Spanish approach
to cybersecurity

CCN-CERT
centro criptológico nacional

Decalogue
CCN-CERT
June 2019

Edit:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

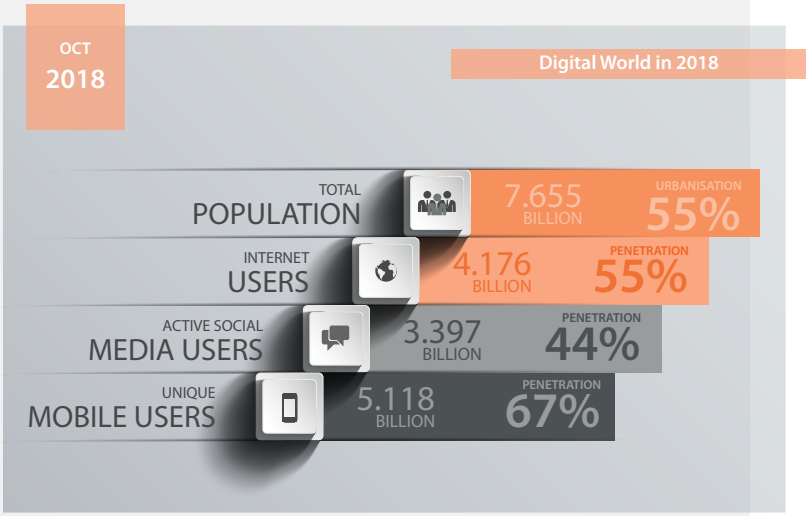
INDEX

Introduction

A new space to protect and new rights to defend

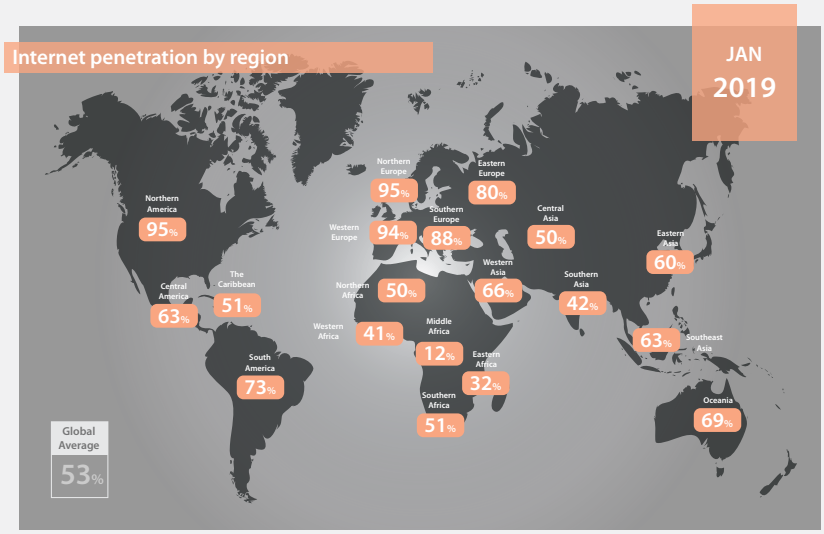
The advance of Information and Communication Technologies (ICT) presents a new paradigm. The expansion of the Internet, with more than 4 billion users' worldwide[1] - or 53% of the world's population - has brought about a profound transformation of global structures. Public services, education, health, media, leisure, transport, culture and, of course, personal relationships have undergone a process of absolute change, due to the influence of technology on society. So much so that there is even a new reality: **cyberspace**.

This global environment presents a scenario of far-reaching economic and social opportunities. However, it also carries a number of risks, which increase day by day. The threats of cyberspace, favoured by economic or political profitability, the low cost of the tools used and the possibility of acting from anywhere in the world anonymously, aim at and transversally affect the public and private sectors, as well as citizens. In this context, cyber-criminals, hackers or states themselves are able to exploit technological vulnerabilities in order to gather information, steal valuable assets and threaten basic services for the normal functioning of a country.



1-. Global Digital Report 2018 (https://digitalreport.wearesocial.com/)

Thus, ensuring and implementing **security in cyberspace**, while **respecting privacy and freedom**, has become one of the strategic priorities of the most developed countries, due to its direct impact on national security, on the competitiveness of enterprises, and on the prosperity of society as a whole. The cyber world demands a **constant commitment** to technological evolution and the increasing sophistication of attacks.



Adapting to this scenario involves improving prevention and surveillance capacities and designing increasingly effective responses to attacks. It also requires a greater degree of coordination and cooperation. On the one hand, at the national level, between all levels of the State Administration and private companies and entities; on the other, at the international level, with countries and multilateral organizations.

Precisely, this document is framed within the framework of both national and **international cooperation**. Only through dialogue and collaboration on cybersecurity, by jointly addressing new challenges, will development and well-being of the states, and therefore of their citizens, be promoted.

CCN-CERT, A SUCCESS CASE IN CYBERSECURITY

The protection and defence of a secure and reliable cyberspace has been put on the agenda of the vast majority of supranational countries and institutions. However, depending on the characteristics of each one of them, the resources available or the degree of maturity of each service, the implementation of the most appropriate measures to achieve this objective will be different.

The purpose of this document is to provide an approach to the development, implementation and improvement of a general framework for National Cybersecurity that will facilitate this task, regardless of the maturity level of each State and of the agents participating in it. Based on the development carried out in Spain in the last 20 years, and with the specific case of the **CCN-CERT**, the aim is to provide a **development** model to face, at a national level, the different challenges arising from the protection of the systems of a country and, by extension, of its administration, companies and citizens. The ability of States to meet the cybersecurity challenges must be a key strategic element, both in protecting themselves and in advancing the current complex geopolitical landscape.

This approach, presented here, is not intended to be a static model, since each country has certain peculiarities and a different maturity level. This document aims to be a reference for the creation of a national programme on cybersecurity that provides a cybersecurity holistic view. To this end, a set of accepted parameters are collected when implementing a national cybersecurity policy, which can be adjusted to the characteristics and needs of each State.

The common challenge of designing policies that preserve national interests in the political, economic and social spheres and the challenge of facing up to the risks and threats that lie ahead in cyberspace require a policy that, encompassed in a National Cybersecurity Strategy, makes it possible to correctly implement all its objectives. It also calls for the regulation of procedures for action in the face of different challenges, the coordination of the different agents responsible for their implementation and the creation of the bodies responsible for such coordination.

This policy must be aligned with the business reality of each country. It must increase capacities for prevention, detection, response and recovery to threats; boost the security and resilience of Information and Communication Technologies in the private sector; and raise awareness of the importance of cybersecurity and the responsible use of technologies. All of this is accompanied by security controls in organizations; technical, organizational and legal controls, both at a global level - to preserve national security - and at an internal level - so that companies can continue operating without affecting their business processes, information assets and clients' assets.

In fact, a decalogue has been drawn up using as an example the steps taken by the National Cryptologic Centre and its Computer Emergency Response Team. Its objective is to guide the action of each State in its response to current challenges through the flexible and efficient use of available resources.

The purpose of this document is to provide an approach to the development, implementation and improvement of a general outline for National Cybersecurity that will facilitate this task, regardless of the maturity level of each State and of the agents participating in it.

The Spanish approach to cybersecurity includes the following ten sections:

1. Establishment of the vision, scope, objectives and priorities: **Cybersecurity Strategy**.

2. Establishing a clear governance structure that identifies and engages stakeholders: **Governance.**

3. To take stock of existing policies, regulations and capacities: **Enabling regulatory development**. Support in an operational and effective legal framework.

4. Increased capacity for prevention, detection and response to cyberthreats, **creating reference and sector CSIRT**.

5. Development and implementation of Early Warning Systems. **Detection capacity** and establishment of incident notification mechanisms.

6. **Increased surveillance**, with a **continuous assessment and cybervigilance service** based on Security Operations Centers (**SOC**), that allow knowing at any time the surface area of exposure to a potential threat and thus allocating resources in an optimal and prioritized manner.

7. **Promotion, development and maintenance of qualified professional profiles** at all levels (management, administration, implementation and users) to protect against cyberthreats. **Talent search** has become a critical element.

8. Actions to strengthen **public-private partnerships** and the security and robustness of ICT networks, products and services used by the industrial sector will be promoted and led. To institutionalize cooperation between public agencies and private enterprise as a key to building community.

9. Implementation of reliable mechanisms for the **exchange of information** between public and private organizations, both for the cyberthreats analysis and for the cyber-incidents' notification, in order to **build trust.**

10. **Communication and promotion,** aimed at achieving strategic objectives. All of this, aware of the need to make themselves known, to disseminate services and to achieve the recognition and trust of the entire community, becoming a reference point in cybersecurity matters.

1 | Need for a National Cybersecurity Strategy

Cybersecurity, over the years, has been introduced into the priorities of a large number of governments, and is now considered a matter of national security and a fundamental pillar of society and its economic systems.

All of this has justified the need for national cybersecurity strategies that, underpinned by security strategies, provide a framework for the objectives and measures to achieve and maintain a high level of security of state networks and information systems.

In the United States, in 2009, the Department of Defense created the US Cyber Command (CYBERCOM) to control the Army's cyber defense and cyberwar capabilities and, in 2011, published its Strategy. In Europe, the European Cybersecurity Agency (ENISA) developed a Good Practice Guide in National Cybersecurity Strategies[2]. In the United Kingdom, the first National Cybersecurity Strategy was published.

Similarly, the Organization of American States (OAS) developed several programs to promote the Inter-American Strategy to Combat Threats to Cybersecurity and, in 2011, Colombia presented its Cybersecurity and Cyber Defense Strategy for the Colombian State.

Thus, in Spain, already in 2011, there was a clear need to develop a national cybersecurity system that would promote the integration of all actors and instruments, public and private, in order to preserve cyberspace from all types of risks and attacks and, therefore, defend national interests and contribute to the Digital Society development. An **integrated cybersecurity model** that, led by the Government, would guarantee the country's security and progress through appropriate coordination of all public administrations with themselves, the private sector and citizens; and that would channel international initiatives and efforts in defense of cyberspace.

As a result, and after several years of intense work through different groups and organizations, in **December 2013** the **National Cybersecurity Strategy**[3] was published, aligned with the National Security Strategy, which included cybersecurity in its twelve areas of action (updated in 2017).

National Cybersecurity Strategy

The National Cybersecurity Strategy, approved on April 30, 2019, develops the provisions of the 2017 National Security Strategy in the field of cybersecurity. Considering the general objectives, the scope and the lines of action established to achieve this, the document is structured in five chapters:

- **Cyberspace, beyond a global common space,** which provides an overview of the field of The following table shows the progress made in the field of cybersecurity since the adoption of the 2013 Strategy, the reasons for this, and the main challenges ahead. that underpin the development of the National Cybersecurity Strategy 2019, as well as the main features that are driving its development.
- **The threats and challenges in cyberspace,** determines the main threats of cyberspace that derive from its condition of common global space, the high technification and the great connectivity that makes possible the amplification of the impact before any attack. It classifies these threats and challenges into two categories: on the one hand, those that threaten assets that are part of cyberspace; and on the other, those that use cyberspace as a means to malicious and illicit activities of all kinds.
- **Purpose, principles and objectives for cybersecurity,** applies the guiding principles of the 2017 National Security Strategy (Unity of Action, Anticipation, Efficiency and Resilience) to five specific objectives
- **Lines of action and measures,** where seven lines of action are established and the measures for the development of every single one of them are identified.
- **Cybersecurity in the National Security System,** which defines the organic architecture of cybersecurity. Under the direction of the President of the Government, the structure is composed of three bodies: the National Security Council, as Government's Delegated Commission for National Security; the National Cybersecurity Council, which supports the Council of National Security and assists the President of the Government in the direction and coordination of the National security policy regarding cybersecurity, and promotes coordination, collaboration and cooperation between Public Administrations and between these and the private sector, and the Situation Committee which, with the support of the National Security Agency, will support the management of crisis situations in any field, which, due to its transversality or dimension, overflows the response capacities of the usual mechanisms.

2.-NCSS Good Practice Guide (https://www.enisa.europa.eu/publications/ncss-good-practice-guide)
3.-National Cybersecurity Strategy https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiber-seguridad.pdf

Overall Objective

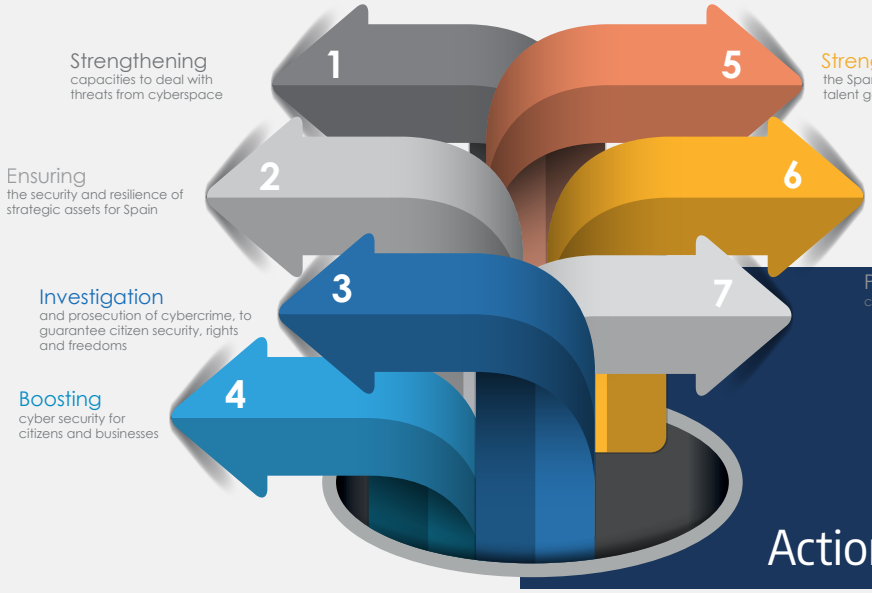
Spain will ensure the safe and reliable use of cyberspace, strengthening the rights and freedom of citizens and promoting socio-economic development.

National Cybersecurity Strategy

Specific Objectives

1. Security and resilience in public sector and essential services
2. Safe and reliable use of cyberspace against illicit or malicious use
3. Protecting the business and social ecosystem and citizens
4. Culture and commitment to cybersecurity and human and technological capacity building
5. International cyberspace security

Action lines



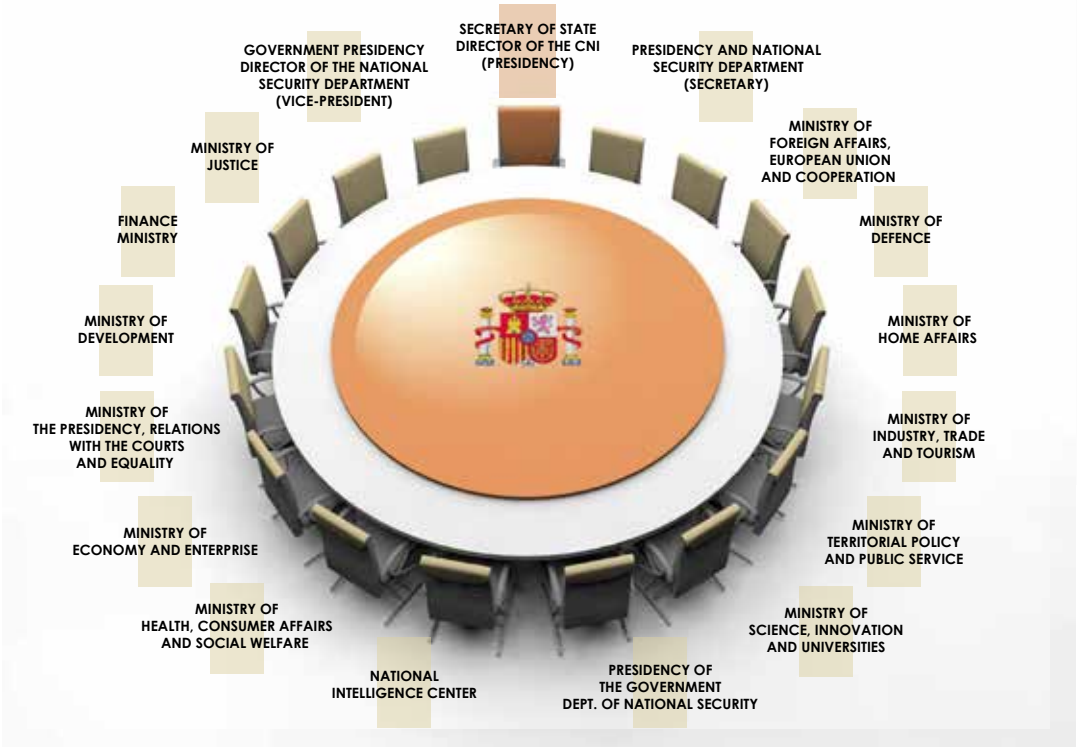
The National Cryptologic Centre (CCN) experience at the head of the National Cybersecurity Council allows the CCN to offer its support and contribution to different States in their efforts to develop their respective cybersecurity strategies.

2 | Cybersecurity Governance

The strategic vision provides a comprehensive overview of the cybersecurity environment and allows for better preparation for potential future risks and threats. However, it is not enough. It is necessary to prioritize available resources and organize decision-making through a centralized institutional system that ensures integrated, effective and, above all, coordinated action.

On the one hand, it is necessary to strengthen the governments' capacities by improving the tools at their disposal and, on the other hand, to identify the **cybersecurity actors** that define the direction to be taken, including the role that each one should play.

The Strategy develops the cybersecurity institutional framework, consisting of the **competent authorities** and the **reference CSIRT**, on the one hand, and **public-private cooperation**, on the other. Thus, in the governance of cybersecurity, a **clear and centralized structure** should be established, defining the different **agents** that make up cybersecurity and their corresponding role.



The composition of the **National Cybersecurity Council (CNCS)**, chaired by the Secretary of State, Director of the National Intelligence Centre (CNI) and Director of the National Cryptologic Centre (CCN), reflects the spectrum of areas of the departments, bodies and agencies of the Public Administrations with competence in cybersecurity matters, although its structure is flexible and provides for the incorporation of other representatives from the autonomous regions and the private sector, depending on the nature of the issues to be dealt with.

In this way, the National Cybersecurity Council contributes to strengthening the relations of coordination, collaboration and cooperation between the different Public Administrations with competences in cybersecurity matters, as well as between the public and private sectors, and facilitates the decision-making of the Council itself through the analysis, study and proposal of initiatives at both national and international levels. This Council is also the **single point of contact** for handling incidents with cross-border impact.

The **competent authorities** exercise the functions of vigilance and apply the sanctioning regime when appropriate, promoting the correction of the infringement rather than its punishment. They are also responsible for promoting the development of the obligations and security measures to be applied, avoiding creating duplicate, unnecessary or excessively onerous obligations.

Finally, the **CSIRT** (Computer Security Incident Response Team) are the gateway to incident notifications, enabling a rapid and timely response to be organized. In addition, provision should be made for the use of a common platform for the notification of incidents to the competent authority, the final addressee of the notifications, via the reference CSIRT.

2.1. Actors in National Cybersecurity

Within the structure developed for the coherent implementation of national cybersecurity, several actors have been trained over the last twelve years.

1 **National Cryptologic Centre (CCN)**, assigned to the **National Intelligence Centre (CNI)**, whose regulatory law (Law 11/2002, of 6 May) entrusts the Centre with the exercise of functions relating to the information security technologies and the protection of classified information, while conferring on its Secretary of State Director the responsibility of running the National Cryptologic Centre. Therefore, the CCN shares with the CNI the means, procedures, regulations and resources. **RD 421/2004** regulates their functions.

a **The National Cryptologic Centre Computer Emergency Response Team (CCN-CERT)**, created in 2006 as a Spanish Governmental/National CERT, whose mission is to contribute to the Spanish cybersecurity improvement, as it is the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively tackle cyber-threats, including the coordination at the state public level of the different Incident Response Capacities or existing Cybersecurity Operations Centres.

b **Certification Body (OC)** for the National Evaluation Scheme and certification of information security technology, to be applied to products and systems (Order PRE/2740/2007). The OC carries out three types of Certification depending on the security aspects being evaluated: Functional certification, Cryptological certification and TEMPEST certification.

2 **INCIBE-CERT: Spanish National Cybersecurity Institute,** formerly the National Institute of Communication Technologies (INTECO), is a society dependent on the Ministry of Economy and Business through the Secretary of State for Digital Advancement. It is the reference entity for the development of cybersecurity and digital trust for citizens, the Spanish academic and research network (RedIRIS) and companies, especially for strategic sectors.

a **INCIBE-CERT,** is the Computer Security Incident Response Team operated by INCIBE. It works to increase the detection and early warning capacity of new threats, the response and analysis of information security incidents, increase the organizations cyber-resilience and the design of preventive measures to meet the society needs in general and, by virtue of the Collaboration Agreement signed between the State Secretariat for Security of the Interior Ministry and the State Secretariat for Telecommunications and the Information Society, for the security needs of critical infrastructures, for support in research and the fight against cybercrime and cyberterrorism.

3 **The National Centre for Infrastructure Protection and Cybersecurity, CNPIC,** is the body responsible for the promotion, coordination and supervision of all policies and activities related to the protection of Spanish critical infrastructure and cybersecurity within the Ministry of Home Affairs, under the protection of the Law /2011 of 28 April (PIC Act) and by the Royal Decree 704/2011 of 20 May 2011, by which critic infrastructure protection is regulated. The CNPIC reports to the Secretary of State of Security, maximum responsible of the National System for the Protection of Critical Infrastructure and Ministry's cyber security.

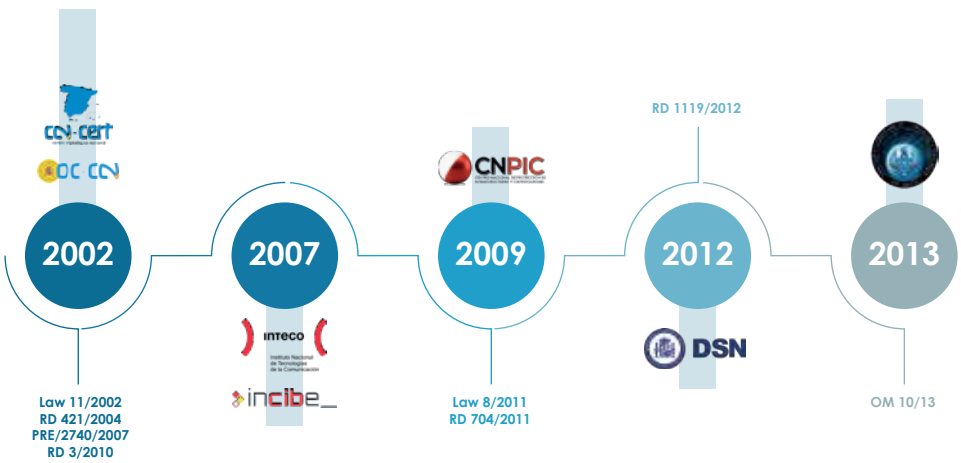
4 **The Department of Homeland Security (DSN)** of the President of the Government Cabinet is the body that advises the President of the Government on matters of Homeland Security. Maintains and ensures the proper functioning of the Situation Centre of the Department of Homeland Security for the exercise of the functions of monitoring and crisis management, as well as special communications of the Presidency of the Government. It was created by Royal Decree 1119/2012 of 20 July, amending Royal Decree 83/2012 of 13 January, restructuring the Presidency of the Government.

5 **Joint Cyber Defence Command** is the body of the operational structure, subordinated to the Chief of Defence Staff (**JEMAD**), responsible for planning and executing actions related to Cyber Defence in the Ministry of Defence's information and telecommunications networks and systems or others that may be entrusted to it, as well as contributing to the appropriate response in cyberspace to threats or aggressions that may affect the National Defence. It was created on 19 February 2013, through the "**Ministerial Order 10/2013**, creating the Joint Cyber Defence Command".

6 **Technological Research Unit (UIT)**, which acts as the E-Crime Prevention and Response Centre of the National Police Force. This unit is responsible for investigating and prosecuting criminal activities involving the use of information and communications technology (ICT) and cybercrime at the national and transnational levels.

7 **Telematics Crime Group (GDT)**, created to investigate, within the Central Operative Unit of the Guardia Civil, all those crimes that use networks and information systems for their commission.

Actors in the National Cybersecurity

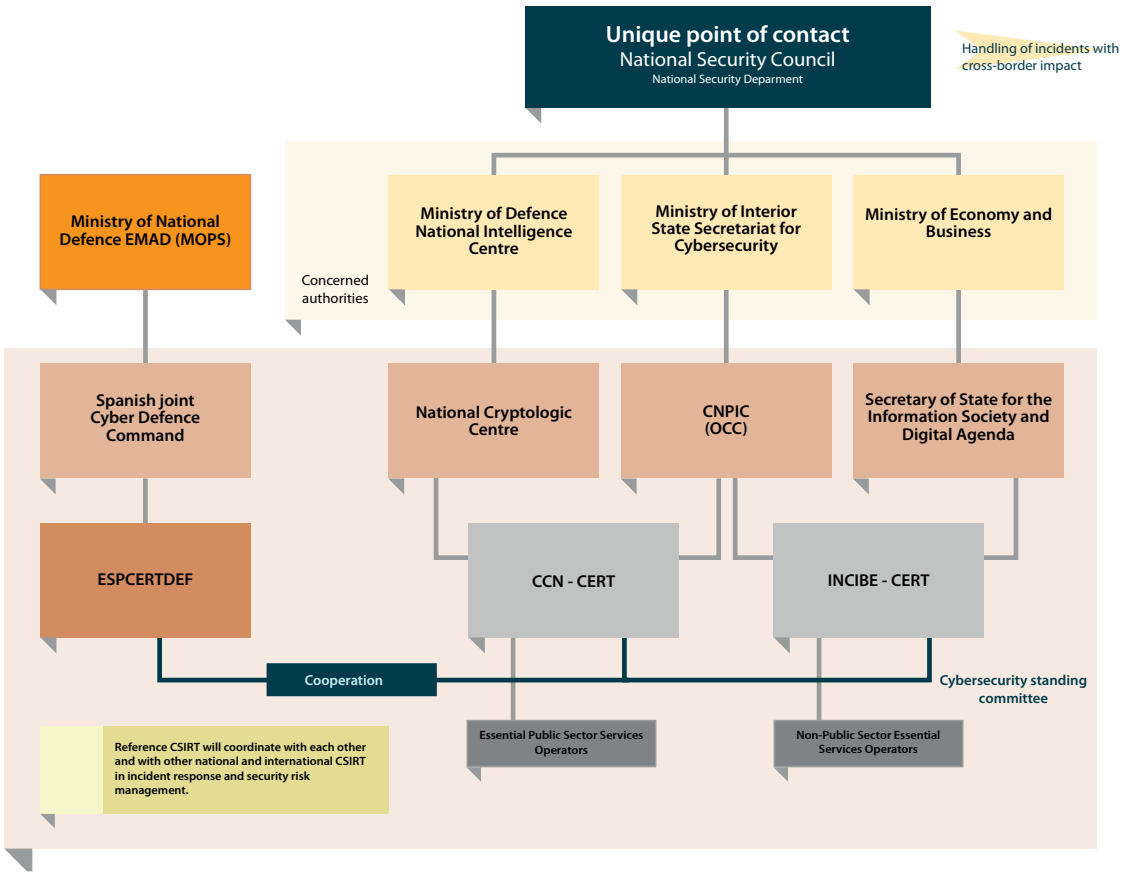


The above-mentioned agencies, each of which is attached to a Competent Authority, operate with a CERT/CSIRT of reference and act as a key component of national capacity for preparedness, information sharing, coordination and response.

The cybersecurity capabilities development, and the accumulated experience over the last decade, has allowed the Spanish state to reach a level of maturity in which the areas of competence of the different actors in the national cybersecurity panorama have been identified, without overlapping.

The transposition of European Parliament and the Council Directive EU 2016/1148 on measures to ensure a high common level of network and information system security in the Union (known as the NIS Directive), which has made it possible to identify operators of essential services, establish security measures and identify the competent authorities and associated CERT/CSIRT reference authorities, has greatly contributed to this.

Actors in National Cybersecurity



3 | Regulatory framework and enabling regulatory development

In all activities in which interactions take place, rules are required to regulate the behaviour of the subjects involved. Rules that not only regulate rights and duties, but also act as catalysts for the sector and promote the creation, growth and strengthening of the activity.

In the case of the ICT sector and its security, it has been necessary for the different existing laws to be adapted to regulate and protect citizens and companies from cyber attacks, as far as possible, also establishing new rules and protocols to regulate new situations not foreseen until now in the physical world.

The approach to this new regulatory framework must include permanent and enabling updating. The body of laws, decrees, royal decrees, ministerial orders and regulations governing cybersecurity must be agile and take advantage of existing situations to achieve a safe and reliable cyberspace, depending on the agencies and entities that make it up.

Therefore, it has been and still is necessary to adapt the legislation to the new reality, both in the criminal field (computer crimes, with specific criminal types), and in the security and protection of personal data.

In Spain, there is a **Code of Cybersecurity Law**[4], published in the Official State Gazette, which cites the main standards to be taken into account in relation to the cyberspace protection and to ensure cybersecurity (some of which, such as the Cybersecurity Strategy, have already been mentioned). The main chapters of this Code are as follows:

1 SPANISH CONSTITUTION

2 NATIONAL SECURITY REGULATIONS

3 CRITICAL INFRASTRUCTURES

4 SECURITY REGULATIONS

5 COMPUTER SECURITY INCIDENT RESPONSE TEAM

6 TELECOMMUNICATIONS AND USERS

7 CYBERCRIME

8 DATA PROTECTION

9 RELATIONS WITH THE ADMINISTRATION

4.- https://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho__de_la_Ciberseguridad. Last modified on 25 May 2018

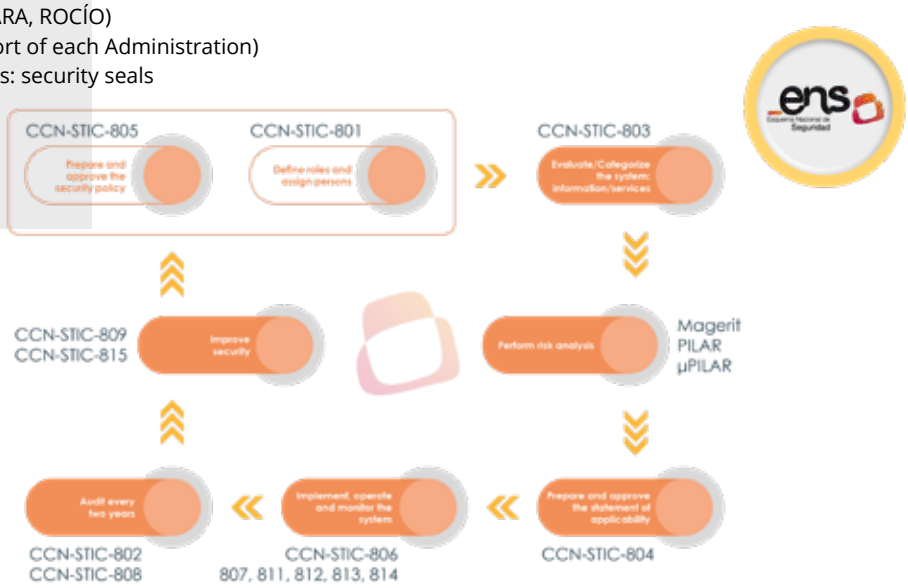
3.1. National Security Framework

Law 11/2007, of 22 June, on citizens' electronic access to Public Services established the **National Security Framework** which, approved by **Royal Decree 3/2010, of 8 January**, aims to determine the security policy for the use of electronic media in the public sector. Its essential mandate is that the entire sector should have a security policy that guarantees access, integrity, availability, authenticity, confidentiality, traceability and conservation of the data, information and services offered. In short, it provides the necessary basis for promoting citizens' confidence in the use of electronic media, while promoting their use.

This Royal Decree, updated in 2015 and in whose development the National Cryptologic Centre (CCN) actively participated, includes **six basic principles** that serve as a guide; **fifteen minimum requirements**, which must be complied and that allow an adequate protection; and **75 information security measures,** which cover both the organizational and operational framework and protection measures. All of this is done **according to different levels of demand**, based on the categorisation of systems determined according to the information handled and the services provided.

The commitment of the CCN to the development and implementation of the ENS has been materialized in the development of solutions and in the necessary support to be carried out. It is not merely a question of setting requirements to be met, but of allowing them to materialise through the adoption of different measures, which are essential for their correct establishment.

- 800 Series CCN-STIC Guides (53 documents)
- Compliance audits
- PILAR (risk analysis and business continuity)
- Compliance analysis solutions (CLARA, ROCÍO)
- INES (National Security Status Report of each Administration)
- Compliance and certification bodies: security seals



The ENS has brought many advantages for both the public and private sectors:

- Public sector
  - It creates a management framework, including the basic principles and minimum requirements necessary, for the adequate protection of citizens' information (residual risk).
  - It helps meeting legal requirements for national, regional or local governments and their suppliers.
  - It allows establishing a common language/taxonomy of danger and incident classification.
  - It establishes a scorecard and metrics, through a system of traceability and incident tracking.
  - It enables integration between digital platforms of the Administration.
- Private sector
  - It helps to develop and demonstrate compliance with legislation (NIS Directive, data protection, critical infrastructure, etc.).
  - It facilitates the services contracting and technological solutions with government agencies.
  - It provides a management framework applicable to an organization.

3.2. NIS Directive

The Spanish legal system is subject to the European Union (EU) legal acts: mainly Regulations and Directives. The purpose of the latter is to set specific objectives, which means that Member States must adapt their national legislation to achieve those objectives, which must be adapted or transposed freely by each Member State.

In the area of cybersecurity, the EU has worked to ensure greater security in networks and information systems. In this regard, The EU Cybersecurity strategy: An open, safe and secure Cyberspace was published in **February 2013**. This document is complemented by the European Parliament and Council EU **Directive 2016/1148** on measures to ensure a high common level of network and information security system in the Union (known as the **NIS Directive**), which entered into force on 9 August 2016 (It was transposed into Spanish law by Royal Decree-Law 12/2018 of 7 September on network and information system security).

The Directive establishes common minimum requirements for capacity building and planning, information exchange, cooperation and common security requirements for operators of essential services and digital service providers, and calls on them to take appropriate measures to manage security risks and to report incidents that would have a significant disruptive effect to the Competent National Authorities, proposing the creation of a network of cooperation between all the different Member States.

The Directive, in one of its most important points, refers to the notification, without undue delay, to the **competent authority through the reference CSIRT** of incidents that have significant effects on the essential services provided so that institutional or national measures can be taken, where appropriate.

In Spain, Royal Decree-Law 12/2018 of 7 September on network and information system security transposes the Spanish legal system this Directive, with the aim of "regulating the security of networks and information systems used for the provision of essential and digital services, while establishing an institutional framework for coordination between competent authorities and with the relevant cooperation bodies at Community level'. The CCN-CERT, according to the provisions of this Royal Decree Law, will exercise national coordination of the technical response of the three Reference CSIRTs established in the cases of special severity determined by regulation and which require a higher level of coordination than is necessary in ordinary situations.

3.3. Cybercrime

Computer/digital crimes and offences are another form of commission of offences already recorded in the physical world (extended, however, by their dissemination and anonymity). However, it is also true that new technologies and the Internet have encouraged the emergence of new forms of crime, which include attacks on pre-established legal assets, such as sexual freedom, property, privacy, honour, etc.

The special nature of this type of crime makes it difficult to investigate and subsequently clarify the facts. In addition, legislation soon becomes obsolete, due to the rapid evolution of new technologies and platforms being created, as well as the absence of borders and, therefore, of common legislation.

In Spain, partial inclusions have been made in the **Criminal Code**, in Organic Law 5/2000, of 12 January, regulating the criminal liability of minors; or in the Royal Decree approving the Criminal Procedure Act. These precepts have taken into account cybercrime such as the possession and dissemination of child pornography, Internet fraud, crimes against privacy, identity theft, industrial espionage or intellectual property rights.

Spain also ratified the **Convention on Cybercrime**, also known as the Budapest Convention, on 23 November 2010. The agreement is the first international treaty, which seeks to tackle cybercrime and Internet crime by harmonizing national laws on substantive criminal law violations and provisions connected to the area of cybercrime, improving investigative techniques and increasing cooperation among nations.

The Convention on Cybercrime was drawn up by the Council of Europe in Strasbourg, with the active participation of the observer states of Canada, Japan, Chile, Costa Rica, the Philippines, the United States and the United States, and further accessions by other non-European states such as Mexico, El Salvador, Argentina, Uruguay and Chile are planned.

3.4. Data protection

In Spain, in 1999, an Organic Law on the Protection of Personal Data was drafted (L.O. 15/1999, of 13 December), the implementing regulations were enshrined in a Royal Decree in 2007 (RD 1720/2007, of 21 December).

However, since 25 May 2018, all countries of the European Union have had to comply with the **General Data Protection Regulation** (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Although it has similarities with the previous standard (LOPD), the new RGPD contains a number of important changes that require the updating of procedures in all organizations. Some of the novel aspects of this Regulation are the figure of the Data Protection Officer; the new rights that the RGPD grants to citizens; risk analysis and impact assessments or the establishment of codes of conduct.

4 | Reference and sectoral CERT/CSIRT

In **1988**, after the first major attack in history (the Morris worm), the U.S. Department of Defense commissioned Carnegie Mellon University in Pittsburgh to create a team capable of dealing with this new type of threat. The result was the constitution of the so-called *Computer Emergency Response Team* (CERT®).

Under the same abbreviation, other groups were formed in various North American universities to study the networks and computers security to provide incident response services to victims of attacks, issue alerts regarding threats and vulnerabilities and provide information to help improve the security of these systems.

At the same time, the term CSIRT (*Computer Security and Incident Response Team*) was consolidated to complete the concept of CERT® and to offer, as an added value, preventive and security management services. Today both terms are used in a similar way.

In Spain, in **2005**, the so-called **Plan Avanza** was approved for the Information Society and Convergence development with Europe and between Autonomous Communities and Autonomous Cities. This plan mentioned the creation of a basic infrastructure of warning and response centres for security incidents, which would respond to the specific demands of different segments of society. Critical sectors, government agencies, Public Administrations, Small and Medium Enterprises (SMEs), large corporations and citizens would receive the appropriate advice from these centers.

In this regard, it the creation of security centres and the establishment of procedures and protocols to coordinate their functions and actions was also discussed. The creation of a CERT for the Administration/Government, a CERT for SMEs and a unit to fight against privacy violations (fight against spam, phishing and other frauds) were also anticipated.

In this context, and taking into account, the continuous increase of threats and vulnerabilities on Information Systems worldwide, in 2004, the Spanish National Government CERT was consolidated, as a result of the aforementioned Royal Decree 421/2004, which regulates the activity of the National Cryptologic Centre (CCN). Thus, and after two years of intense work, in **2006**, the **Information Security Incident Response Capacity** of the CCN (**CCN-CERT**), which depends on the National Intelligence Centre, was presented.

4.1. CCN-CERT. National Governmental CERT

Since its creation, CCN-CERT's mission has been to contribute to the improvement of the Spanish **Public Administrations** information systems' security level (both central, regional and local) and, as its main goal, to become the national alert centre, which cooperates and helps the public sector to respond quickly and efficiently to security incidents that may arise and actively confront the new threats to which they are exposed today.

Similarly, it has assigned the capacity to promote the creation of other CERT/CSIRT, providing the necessary information, training, recommendations and tools so that the rest of the public administrations could develop their own incident response capacities, thus recognising the **CCN-CERT as the state public coordinator**.

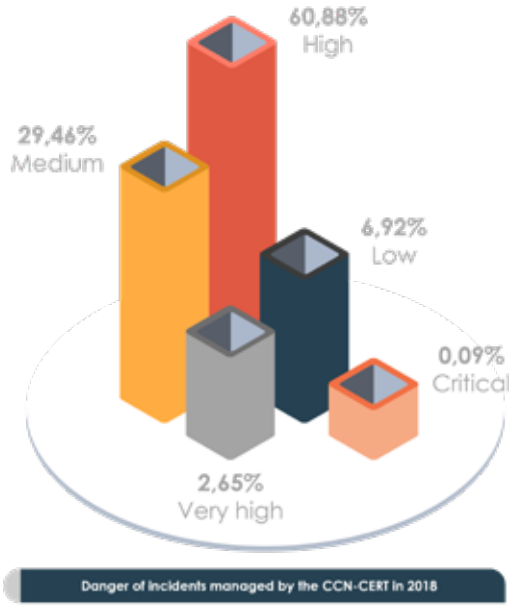
With its creation, the **Spanish National Governmental CERT** was also constituted, in the image and likeness of the existing ones in other countries of its environment, which acts as a fundamental component of the national capacities of preparation, information exchange, coordination and response. It should also participate effectively in cross-border cooperation and information exchange in international fora, encouraging existing organisations such as the EGC Group (European Governmental CERT Group).

The different subsequent regulations outlined its functions -RD 3/2010, of January 8, 2010, regulator of the National Security Scheme (ENS) or Law 40/2015 of the Public Sector Legal Regime- and, at present, its mission includes the **public Incident Response Capacities** or **Cybersecurity Operations Centers coordination**.

All this, with the ultimate aim of achieving a more secure and reliable cyberspace that preserves classified and sensitive information, defending the Spanish technological heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

According to the regulations, the CCN-CERT is responsible for the **management of cyber-incidents affecting any public body or company**. In the case of **critical public sector operators**, the management of cyber-incidents will be carried out by the CCN-CERT in coordination with the CNPIC.

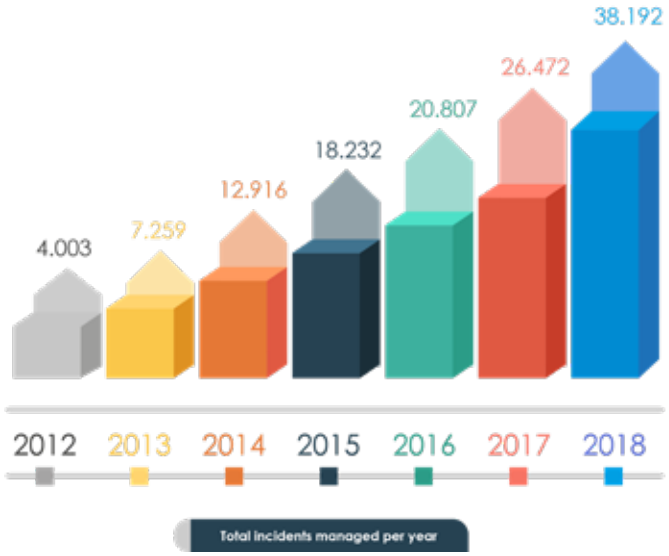
From the beginning, the National Governmental CERT provided all its services, free of charge, to the Spanish public sector. **Some services, easily replicable to other institutions or bodies** and which, following the internationally accepted pattern, could be summarised in the following sections:



Danger of incidents managed by the CCN-CERT in 2018

REACTIVE SERVICES

- Incident Management (about 38,200 in 2018)
- Information on vulnerabilities, alerts and warnings of new threats: 80 alerts and warnings issued in 2018, and 2,928 vulnerabilities
- Malicious code analysis
- Forensic capability and reverse engineering



MANAGEMENT SERVICES

- Risk analysis and management: Pilar
- CCN-STIC guidelines: safety standards, instructions and recommendations: 335 in 2018
- Training and raising awareness- (promoting a culture of cybersecurity)
  1. In-person courses in collaboration with INAP: 14 (620 students in 2018)
  2. Online courses (www.ccn-cert.cni.es): 5 courses. 1,295 teaching hours
  3. Plataforma Vanesa: 13 courses and 1,200 people
- Cybersecurity Reports (Threats, Harmful Code, Good Practices and Technical): 76 in 2018
- Informative articles and press releases for the media: 125 in 2018
- Product Evaluation and Certification

PROACTIVE SERVICES

- Intrusion detection
- Early Warning Systems in IT and OT
- Ongoing security audits and assessments
- Development of security solutions
- Cybervigilance

4.2. National and Sectorial CERT/CSIRT and SOC

In its role as a national cybersecurity catalist, the CCN-CERT has promoted and facilitated the creation and constitution of other public and private organizations› sectoral Incident Response Teams -particularly in the different Public Administrations and Security Operations Centers (SOC)-, with the common goal of maintaining and increasing continuous network surveillance.

To all of them, the CCN-CERT has provided assistance and collaboration, both in its initial constitution and in its subsequent development. Thus, more than 20 CSIRT (FIRST members) and different SOC have been consolidated over the years.

- Other reference CERT/CSIRT:
  - INCIBE-CERT (Security and Industry managed by INCIBE and CNPIC)
  - ESP DEF CERT (CERT Joint Cyber Defense Command)
- CERT/CSIRT sectors that can be cited:
  - RedIRIS: first to be set up in Spain
  - AndaluciaCERT: organizations and entities of the Administration of the Junta de Andalucía
  - CESICAT-CERT: Computer Security Centre of Catalonia
  - CSIRT-CV (Valencian Community)
  - CSIRT.GAL (Government of Galicia)
  - Basque Cibersecuirty Centre CSIRT (Basque Country)

5 | Detection and analysis capability. Early warning system (SAT)

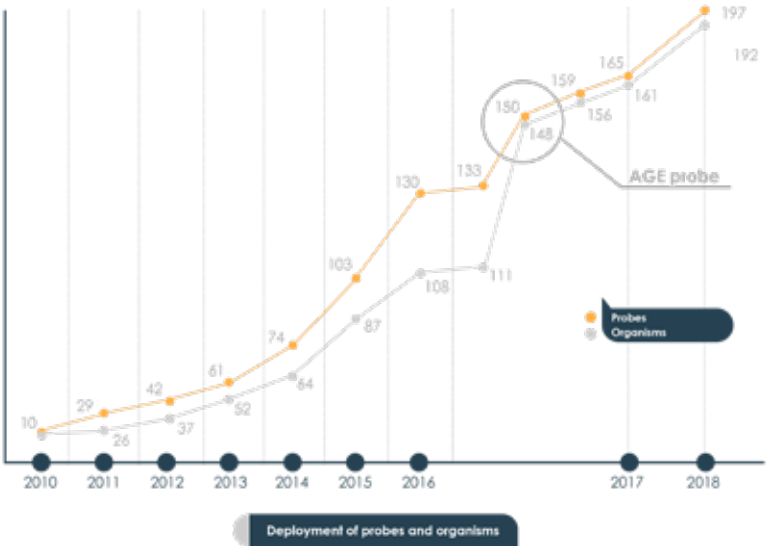
To ensure an adequate the systems security level, it is necessary to act before an incident occurs or at least be able to detect it in the first place to reduce its impact and range.

For this reason, since **2008** the CCN-CERT has developed an Early Warning System (EWS) for the incidents and anomalies rapid detection, which allows preventive, corrective and containment actions. Its main function, therefore, is the incident early detection so the threat containment and elimination necessary measures can be implemented. Thus, the attempted attack can be prevented from being successful or, where appropriate, minimized the possible impact.

This system has three strands: **SAT-SARA** (Monitoring of the Administration Intranet, SARA); **SAT-INET** (Monitoring of the Internet outputs of the agencies assigned to the service) and **SAT-ICS** (Industrial Control Systems).

The EWS, in any of its three modalities, makes possible to detect in real time the existing threats and incidents in the traffic that flows in the the assigned Agency internal network. Its detection systems, through probes, cover all the activities of:

- Detectors deployment and warning systems
- Log collection, traffic monitoring and network monitoring
- Malware analysis, reverse engineering and forensic analysis
- Threat technical characterization and development of technical intelligence on the threat

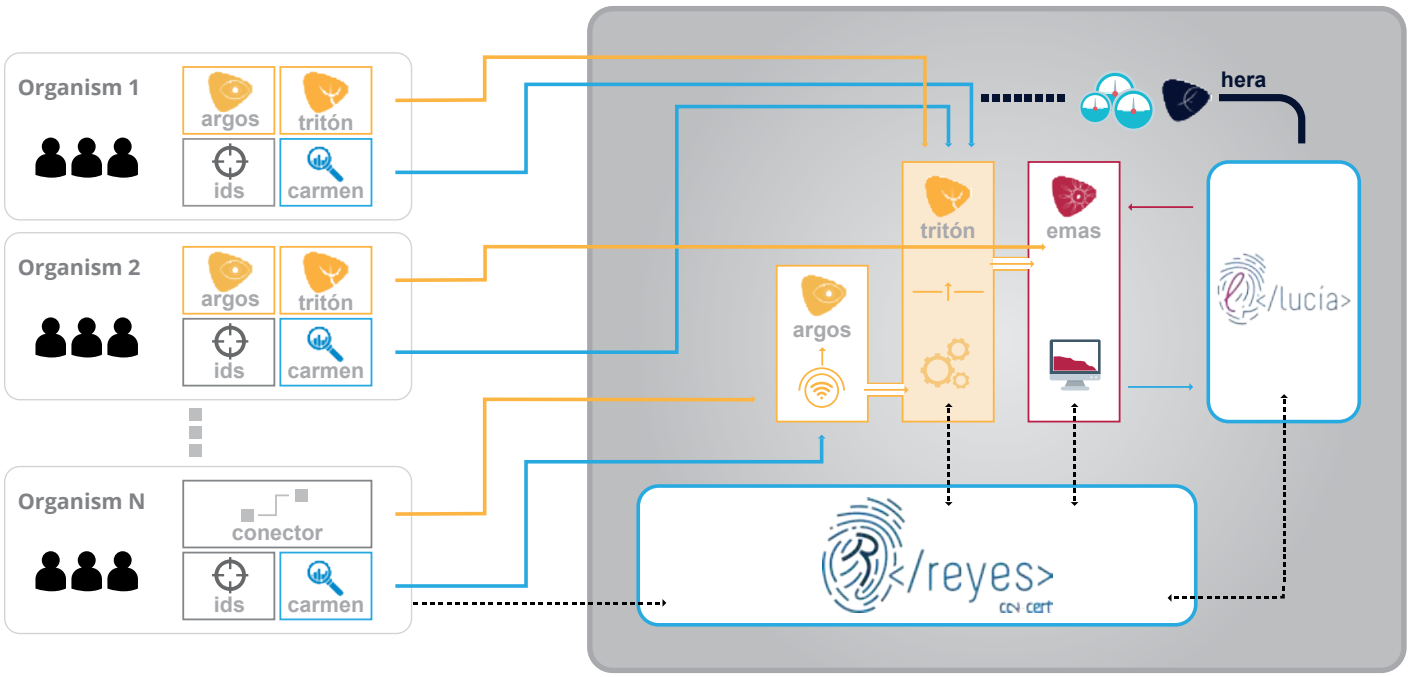


Through this service, the CCN-CERT, in collaboration with the assigned body, has the capacity to detect multitude types of attacks, prevent their expansion, respond quickly to the incident detected and generate rules of action to prevent future incidents. At the same time, and thanks to the storage of a progressive number of events, it is possible to have a complete and truthful overview of the Spanish public administrartions systems situation, which makes possible a preventive action against the threats that hover over them.

In general, the advantages for any organization could be summarized as follows:

- Access to the largest set of **detection rules**, both own and external, integrated by the team of experts of the CCN-CERT, which allows a greater number of threats detection.
- **Detection** of all types of attacks and incidents, including **advanced interdomain detection** (early incident detection that has been replicated in another of the monitored domains).
- **Correlation.** The central system not only detects important incidents individually, but it is also capable of detecting much more complex events that can involve different domains.
- **Information** of great value to the ICT managers of public administrations, who can see in real time their security network status , as well as access to statistical reports.
- **Incident resolution support.** As the Spanish National Governmental CERT, the CCN-CERT offers to all the organizations its collaboration for detection, containment and elimination of any attack that their systems may suffer.
- **Automation and reduction of response times.** To reduce manual and repetitive work by security operators/analysts in incident detection and response processes.

In this regard, the integration of Security Information and Event Management (SIEM), incident notification and cyberintelligence capabilities are particularly needed for improvements in complex event correlation and incident management techniques.



6 | Increased vigilance. Security Operations Centers (SOC)

A CSIRT can provide alerts to entities or manage an incident; however, in different circumstances, organizations themselves do not know how to carry out resource allocation. Sometimes, they are unaware of their systems´ exposure to such alerts or threats issued by the Incident Response Team.

For this reason, in daily work, and as a step forward in cybersecurity, it is necessary to have a continuous assessment service that allows knowing at all times the potential threat exposure area and thus allocate resources in an optimal and prioritized manner.

Through a Cybersecurity Operations Center (SOC), prevention, detection and surveillance tasks are performed, monitoring the people, processes and technology involved in all operational aspects of cybersecurity.

The CCN-CERT has offered surveillance services, at no associated cost, to various Spanish public administration bodies, promoting the creation of this type of centre.

The SOC has three levels:

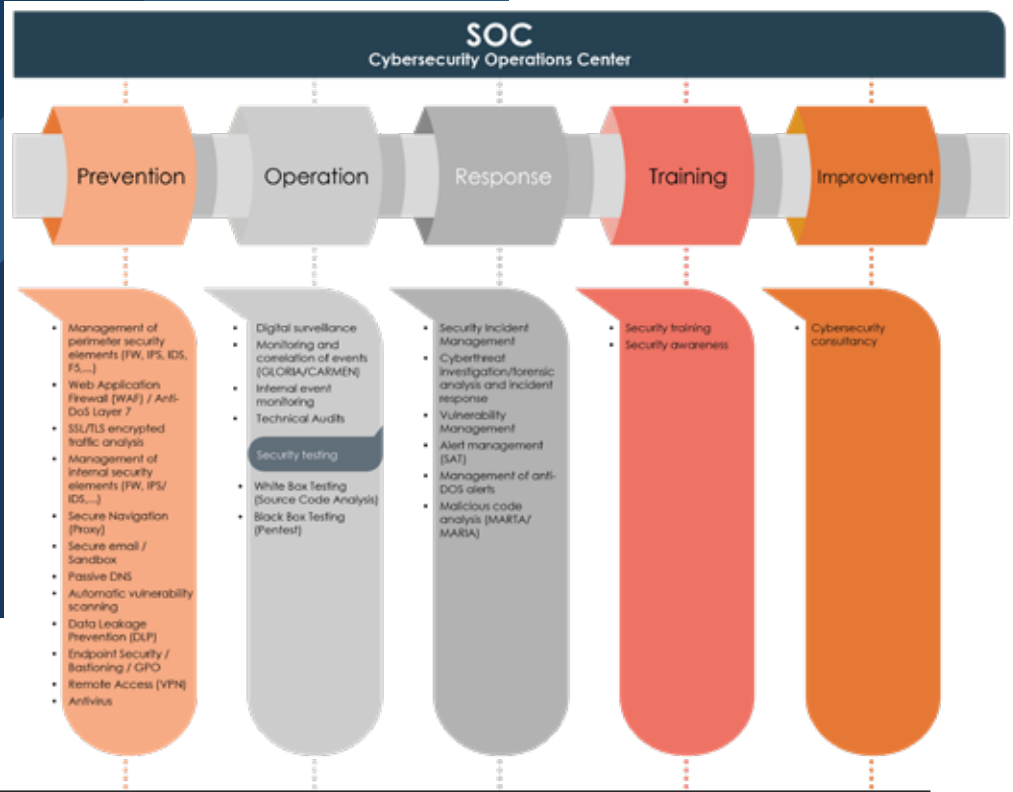
1 OPERATION

2 SURVEILLANCE

3 CYBERSECURITY INTELLIGENCE

Its final objective is to increase the existing surveillance and threat detection capabilities in daily operation, as well as its capacity to respond to any attack, giving priority to the following aspects:

- To continuously monitor and evaluate the safety measures in use, verifying their implementation.
- To act proactively by increasing and expanding capabilities for detection, monitoring, protection and response to incidents.
- To parameterize the threat by means of cybersecurity intelligence, which allows information to be integrated. Accordingly, it is essential to improve the incidents reporting and to increase the information exchange on the threat.

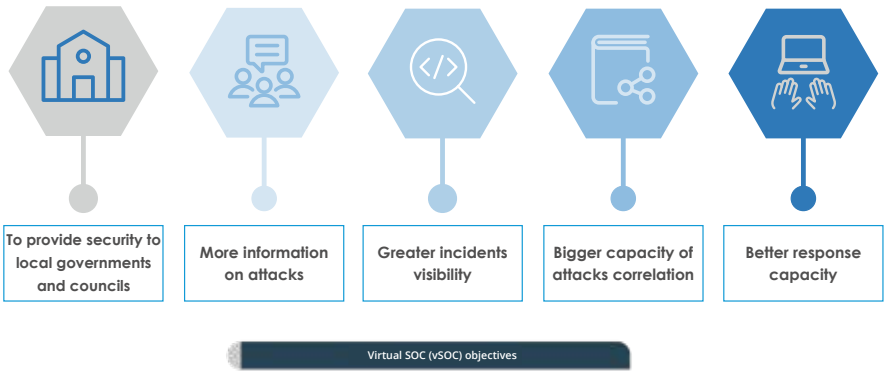


Virtual SOC

The constant increase in cyber-attacks, together with the possible consequences for a country of a security incident affecting their systems lead to the necessity of increasing and improving the prevention, monitoring, surveillance and response capabilities, through **Security Operations Centers (SOC).**

For this reason, the National Cryptologic Centre is working on the implementation of virtual Security Operations Centers (vSOC) in **local entities** to improve their surveillance, detection and monitoring capabilities and response to any possible attack, as well as to optimize its resources based on the information that drive and the services they provide.

In this way, through vSOC, municipalities and councils will have more visibility and information about vulnerabilities, configuration and incident failures, increased deployment, protection and performance capabilities, by having a better understanding of the local environment, and a better understanding of the local situation. (SOC).



Virtual SOC (vSOC) objectives

7 | Training. Skill and Talent

7.1. TRAINING AND CERTIFICATION OF PEOPLE

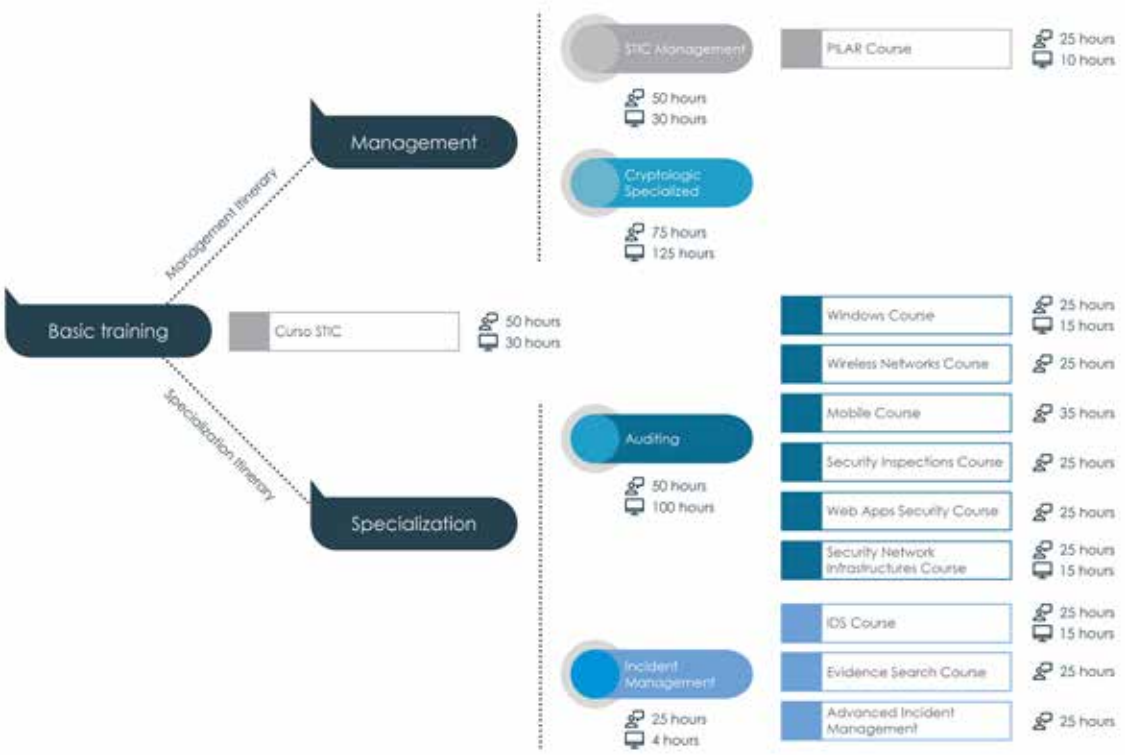
As threats become increasingly complex and sometimes difficult to detect, staff training is needed across all organizations to combat naivety, ignorance of good practices and a lack of awareness of the need to preserve the security of information and services provided to citizens.

The ability to promote, develop and maintain qualified professional profiles at all levels (management, administration, implementation and users) is therefore required to protect against cyber threats. Similarly, the growing knowledge gap and an educational paradigm shift, based on lifelong learning as a potential workforce, need to be addressed.

Historically, one of the National Cryptologic Centre main functions has been to train the Spanish Administration staff through a wide range of courses. A role played with great success that has been expanding, both in the training offered - incorporating online courses and through video streaming - and in the public receiving it - some of its courses are open to the participation of any user.

Thus, the CCN maintains a **Training Plan** with three types of courses that are *easily transferable to other states or organizations:*

- **Attendance:** 20 courses published in the BOE and those developed ad hoc for a national or international organization
- **Online:** The National Critpological Centre website allows users to take different courses through this platform. A 100% online teaching methodology is used, both in the contents of the syllabus and in the exams that are taken after the course. There are currently eight available on the web portal.
    - Linux Basic Course
    - Introduction to the National Security Framework
    - INES Course (National Report on the State of Security)
    - STIC Basic Course - Security in Windows environments
    - STIC Basic Course - Security in Linux environments
    - Risk Analysis and Management of Information Systems Course
    - National Security Scheme Course
    - Information and Communication Technology Security Course
- **VANESA Platform,** with *streaming* training and whose recordings and training material are hosted on the platform itself. The courses that are given, of 4 hours approximate length, deal with the state of the art of technology, as well as the solutions description developed by the CCN-CERT.
- **Curricular design. Persons´ Certification**



The Training Plan of the National Cryptologic Centre has been designed in response to the need to train, both in person and online, qualified professionals with different profiles and levels of training. For this reason, a BASIC training has been established which, through the STIC Course, introduces the student to the field of Information and Communication Technology Security.

Once the basic training has been completed, the professional who wishes to perfect his knowledge can choose between two (2) itineraries designed to achieve this end, the management itinerary and the specialization itinerary (aimed at more technical personnel). The CCN grants those who have successfully completed the course a Certificate, which specifies the subjects and credits partners.

7.2. Search for talent, need for expert personnel

Specialized cybersecurity talent is a skill set of **low supply and high demand**. It could be said that the lack of qualified personnel in this area is one of the greatest problems facing the sector. For this reason, companies or organizations that are able to attract and retain cybersecurity specialists will be more successful in managing risk and leveraging the digital transformation.

Some of the recommendations offered for acquiring and retaining this talent[5] are:

- Apply innovative techniques to find cybersecurity talent
- Look for the spaces where cybersecurity talent spends its time
- Encourage employees to upgrade their digital security skills
- Promote gender inclusion, changing the current perception

Aware of this problem, in 2017 the CCN-CERT launched **ATENEA**, a new platform of cybersecurity challenges, where anyone can demonstrate their knowledge and skills in the face of different challenges in the field. There are different challenge difficulties and very different topics: cryptography and steganography; exploiting, forensics, traffic analysis, reversing and web hacking.

Among its main objectives are:

- To raise awareness among ICT staff of the risks in this field
- To involve experienced cybersecurity professionals so that they can demonstrate their ingenuity and capability
- To demonstrate to people with less experience in ICT security that challenges are fun and that cybersecurity is easier than it seems. It's not a hidden science they would never understand.

ATENEA
Plataforma de desafíos de seguridad

5.-Capgemini. Report 2018 Cybersecurity talent: the big gap in cybersecurity. https://www.capgemini.com/es-es/resources/talento-especializado-en-ciberseguridad-la-gran-brecha-contra-los-ciberataques/

8 | Public-private partnership. Building community

While cybersecurity-related policy development is primarily a State responsability, all public and private actors with responsibility for cybersecurity-related issues, including citizens themselves, must be involved. Strengthening cybersecurity will give the public sector, industry, business, the scientific community and the general public greater confidence in the use of ICTs.

In application of the **shared responsibility principle**, public administrations must maintain close relations with companies that manage information systems relevant to national interests, exchanging knowledge that allows appropriate coordination between them and mutual understanding of the cybersecurity environment.

In this sense, special mention should be made to the actions that ensure the **protection of technological heritage** in cyberspace, understood as those tangible or intangible assets that support the intellectual and industrial property of the business sector, and that shape the present of a country and condition its future.

It is also important to determine the impact that a country may have on the potential systems disruption or systems and networks destruction that provide essential services to society (critical infrastructure), given that, to a large extent, the private sector is the owner of a large part of these systems.

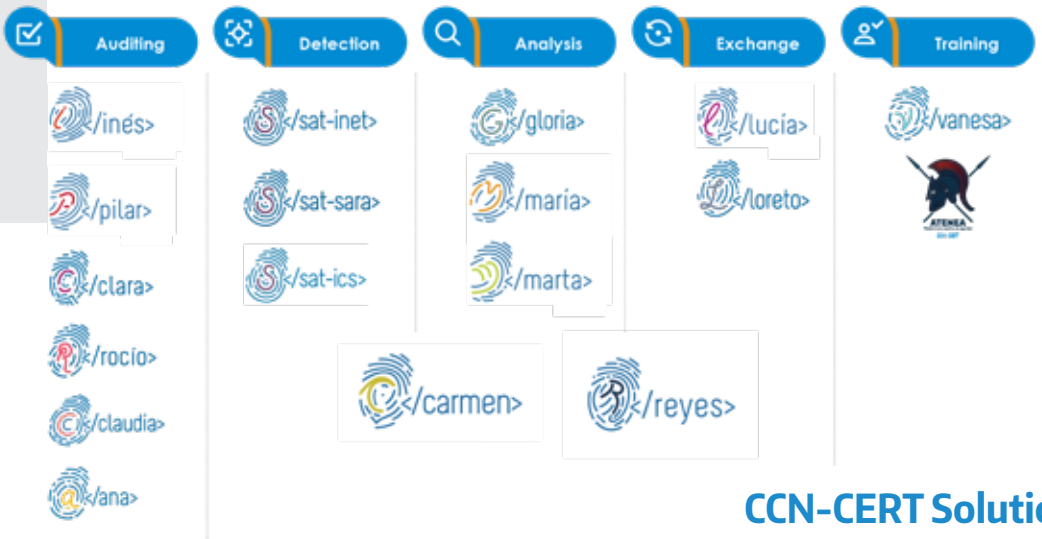
Therefore, one of the objectives is to **improve the networks´ security and resilience**, products and services used by the industrial sector in the development of its activity, strengthening public-private collaboration with the industrial sector and, in particular, with the ICT security sector. The participation of professional associations and associations, among others, will be valued.

The CCN-STIC Guides are freely available to all users. More than 300 documents contain standards, instructions, guidelines and recommendations to improve the level of cybersecurity in organizations.

Its main measures include:

- To foster public-private cooperation by promoting the on vulnerabilities information exchange, cyberthreats and their potential consequences, especially toward to the protection of national interest systems.
- To promote cooperation with the cybersecurity industry and services sectors in order to jointly improve detection, prevention, response and recovery capabilities to cybersecurity risks in cyberspace, by encouraging the active participation of service providers, as well as the development and adoption of conduct codes and good practices.
- To promote the development of standards in cybersecurity, through national and international standardization and certification bodies and entities,and promote their adoption.

In line with these measures, the CCN-CERT has provided a large part of its services to the private sector and, in particular, to companies of strategic interest to the country (its Early Warning System is supported by several companies whose activities require special protection). In this sense, the bulk of the CCN's activity (cyberincident support, early warning services, training, reports, warnings, alerts, vulnerabilities, guides, solutions, etc.) is published on its **website (www.ccn-cert.cni.es)** and is freely available to any user.



The National Cryptologic Centre is doing an important work to improve the technological, intelligence and communication capacities that will allow an effective response. Thus, it is immersed in a solution development plan, in collaboration with the Spanish industry, which, in turn, allows them to be used in all types of organizations (public and private). These are detection, analysis, auditing, information exchange and training solutions.

The **CSIRT.es** platform is another initiative promoted by the CCN-CERT to offer a coordinated response to global attacks. The objectives of this group of **CSIRT which operatein Spain** are the Spanish cyberspace protection, the cybersecurity information exchange and the rapid and coordinated response to any incident that may affect different Spanish entities simultaneously.

CSIRT.es is made up of the main response teams to CERT/CSIRT security incidents, whether public or private, whose sphere of action or community of users in which it operates is within the Spanish territory.

The CCN also maintains a close relationship with companies, ensuring the use of reliable security products. This is how the Certification Body (OC) is constituted, responsible for the products or systems security certification according to certain criteria or regulations (Common Criteria or ISO15408/ISO18045, ITSEC, ISO19790/ISO24759 and the recently created LINCE methodology - National Essential Security Certification).

In addition, it maintains a permanently updated STIC Product Catalogue (CPSTIC) which includes a list of products with contrasted safety guarantees, having certified their fundamental safety functions, in accordance with the criteria established by the CCN. The catalogue consists of:

List of Qualified Products: suitable for use in systems affected by the ENS because it´s a high level of security requirement in any of their dimensions (Confidentiality, Integrity, Availability, Traceability and Authenticity).

List of Approved Products: whose use is approved in systems that handle classified information.

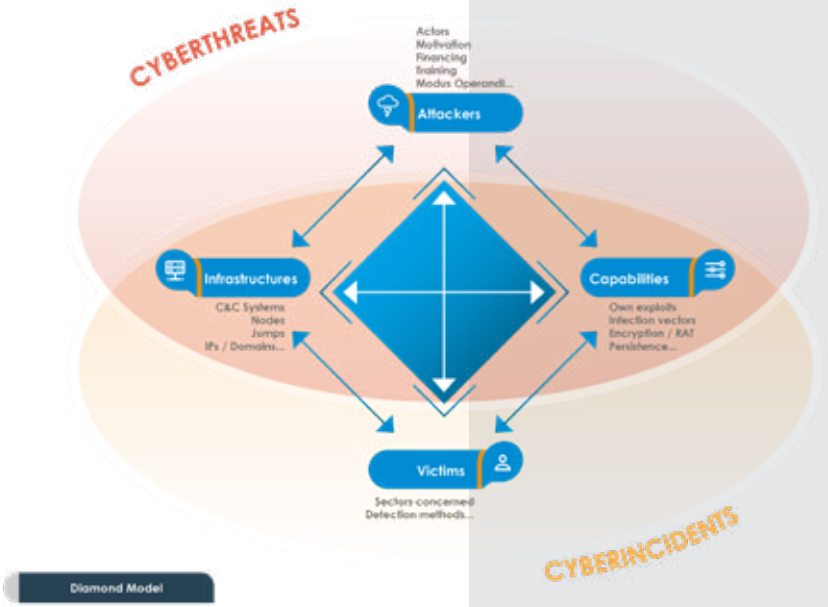
9 | Information exchange, building confidence

The risks and threats of cyberspace have proven to be global and can only be addressed through a joint response. A response that must involve a greater coordination and cooperation level . On the one hand, at the national level, between all levels of the State Administration and private companies and entities; on the other hand, at the international level, with other countries and multilateral organizations.

Any mechanism used for governance will be truly effective if all participants have **reliable information** to enable them to act. This is particularly important for governments, which are responsible for ensuring the safety and well-being of their citizens.

At the **national level**, a model based on the information exchange ofbetween public and private organizations is needed, coming from the analysis of both cyberthreats and cyberincidents, with the aim of improving and speeding up the detection and action against attacks.

This exchange is always more effective through trust between the parties than through regulatory enforcement (although there is some regulation that requires the cyberincident information exchange). This trust will allow all the agents involved to see the benefit of investing time and money in forums and systems exchange, and will also allow reciprocal action to take place, in which the information provided is parallel to the one obtained to optimise their defences.



Diamond Model

To make this model work, the contributions regarding cyberthreats and cyberincidents must be compensated, since both attacker information (his capacities and infrastructures) and victim information (attack procedure, impact suffered and successful detection/resolution techniques) are necessary. In this way, itwill be possible to cover all the vertices of the diamond model and to know the techniques, tactics and procedures (TTP) of the attacker.

The national cybersecurity industry, especially the services industry, must act as a catalyst for this valuable information sharing , with special emphasis on the human factor, and on the training of a good team of analysts and researchers who can provide knowledge and understand the vast amount of information.

In this task, the CCN-CERT offers two of its most outstanding solutions: Lucía and Reyes. The first one, for incident notification and threat contextualization; the second one, for the threat knowledge and parameterization, wich allows the elaboration of cyberintelligence.

9.1. International cooperation

In addition to national cooperation, it is essential that any incident response team maintains contact, in the event of an attack, with other teams in the rest of the world and thus ensure reliable sources of information. Hence the importance of the various existing international fora, both at European and global level. The CCN-CERT participates in the following international meetings and working groups:

- **Forum of Incident Response and Security Teams (FIRST)**, the first and foremost international organizations, with members from Europe, America, Asia and Oceania, from the governmental, economic, educational, business and financial worlds. In fact, since its creation in November 1990, it has grown from nine U.S. and one European security team to its current 440 members.
- **NATO's NCIRC** (*Nato Computer Incident-Response Capability*), in which the various CERTs of NATO member countries analyze and share security information.
- **European Network and Information Security Agency (ENISA)** of the European Union.
- **APWG** (*Anti-Phishing Working Group*), a Europe Council program aimed at eliminating all types of fraud and identity theft through phishing, pharming or phishing emails.
- **Trusted Introducer**, the main European forum in which the continent's leading CERTs collaborate, innovate and share information, is part of TERENA, the Trans-European Association for Research and Network Education.
- **EGC** (*European Goverment CERTs*), organization that brings together the main governmental CERTs in Europe.

10 | Communication Plan and Promotion/Awareness

In 2014, when the work to create the Incident Response Capability (CERT) in the **National Cryptologic Centre (CCN)** started, this kind of team was practically unknown in Spain. The word cybersecurity was not even used and, although the risks and threats posed by new technologies and the Internet were already apparent, there was little awareness of the true nature of the problem.

For this reason, and from the very beginning, the National Governmental CERT decided to carry out an **annual Communication Plan,** conceived as a management tool aimed at achieving the Centre's strategic objectives. All this, aware of the need to make themselves known, to spread their services until they reach the recognition and trust of the whole community, with the aim of becoming the reference point in cybersecurity matters. Similarly, one of its aims has been, and still is, to achieve the greatest number of contacts to maintain direct and fluid communication.

In its first steps, the objectives were clear:

To obtain the CCN-CERT recognition and integration in the main international forums in order to optimize incident management.

To achieve the recognition and trust of its community (Security Officers of the different Spanish public administrations: Central, Regional and Local) to become a point of reference.

Generate a cybersecurity culture, supporting all efforts to raise awareness, train and disseminate information and good practices in information security, both among its community and society in general.


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

Expansión
economíadigital
Así se protege España del ciberespionaje


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

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

To this end, the CCN-CERT carried out a series of relevant actions:

- Integration in the main CERT forums around the world: FIRST, EGC (European Governmental CERT), TI, NCIRC (NATO).
- Roadshows plans to present the CCN-CERT services in different Autonomous Communities.
- Development of periodic communication events with the press.
- Participation and/or sponsorship of Security meetings (fairs, congresses, conferences, etc.).
- Relations with the media. Publication and dispatch of articles and press releases with awareness material and information.
- Monthly and thematic security reports and bulletines dissemination, including some reports on Best Practices (basic security recommendations, HTTPS implementation, mobile devices, safe use of email, etc.), threats or harmful code, as well as its Annual Cyberthreats and Trends Report, which provides an in-depth analysis of the national and international cybersecurity landscape.
- Agreements´signing with various Spanish institutions: Spanish Federation of Municipalities and Provinces (FEMP), INCIBE, Universities, Regional and Local Governments (Andalusia, Catalonia, Valencia, Murcia, etc.).
- Preparation of information and promotional material: leaflets, services catalogue, Activities Report, etc.

10.1. CCN-CERT website and social networks

The CCN-CERT[6] website is the main coordination and support tool for the community. Through this website, users can access to all the services offered by this body. However, given the sensitivity of some content, the site has a restricted access section, which can only be accessed by completing the registration form published on this page.

Likewise, in 2015, the CCN-CERT created its profiles on the main social networks (LinkedIn, Twitter and YouTube), through which it provides information on all its activities, offers warnings and alerts or publishes information of interest to a more general public.

In only two years, it has achieved more than 12,000 followers on Twitter and more than 11,000 on LinkedIn.

10.2. CCN-CERT Conference

The CCN-CERT Conference, held since 2007, is one of the flagship activities of the National Cryptologic Centre. The event has become the main meeting of experts in cybersecurity in Spain, not only because of the great success of the event, but also because of the quality of the topics covered and the experience and knowledge of the speakers.

The last edition, inaugurated by His Majesty the King, brought together 2,464 attendees on 12th and 13th December and was supported by the main companies and associations in the sector.

Spanish approach to cybersecurity