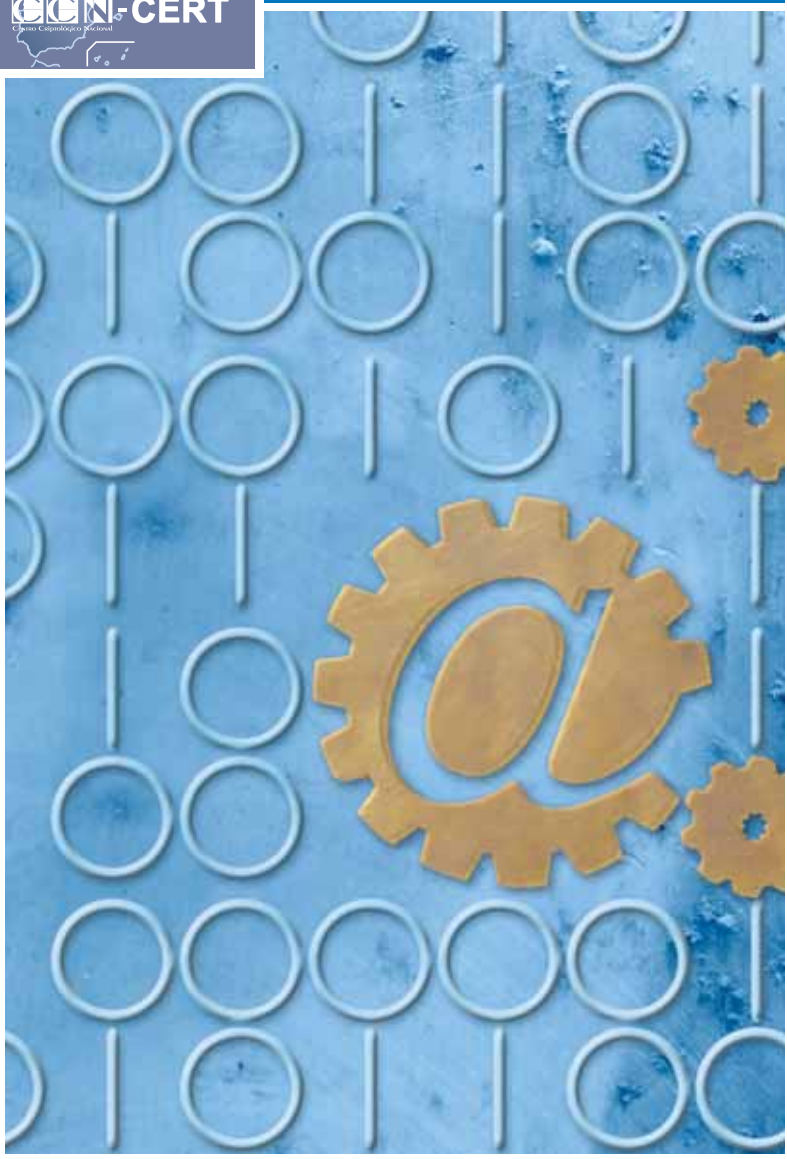
SPANISH GOVERNMENT CERT SERVICES CATALOGUE

Information Security in Public Administration

CCN-CERT
Centro Criptológico Nacional



INFORMATION SECURITY,
a challenge to the Administrations

One of the main challenges to current society is the ever-increasing number of vulnerabilities in systems and threats/attacks to information communications and technologies (ICT). These threats, which may not always be deliberate (consider, for example, mistakes and omissions made by authorized and well-intentioned staff who are not aware of good practices in IT systems, or other types of disasters such as fires or floods), are in constant development and pose a real threat to society.

The challenge is even bigger in the case of deliberate attacks, as the tools used to execute them get more and more sophisticated and are easily available on the Internet. Furthermore, attacks can be carried out from any part of the world and there is little chance of discovering their origin, or even their existence.

In fact no system, including that of Public Administrations is safe from receiving a serious attack, such as theft, loss, destruction or extraction from storage devices, destruction or modification of stored data, information redirection for fraudulent uses; data interception while being processed, junk mail, etc.

Given this situation, even the best security infrastructure cannot guarantee the prevention of damages to the system when an intrusion occurs. Therefore, when a security incident takes place, it is essential to depend on an appropriate and

efficient response protocol. The speed with which an incident is detected, analyzed and responded to, can limit damages and decrease recovery costs.

The National Cryptology Centre, CCN, under the auspices of the National Intelligence Centre is the Organization responsible for the ICT security of Public Administrations and for the training of specialist administration staff in this area, as established by the Spanish Royal Decree 421/2004, and by which means the CCN was created.

The National Cryptology Centre's Computer Emergency Response Team was created at the beginning of 2007 (CCN-CERT), with the aim of improving the security level of the Spanish Public Administration's information systems (general, autonomous and local). This CERT Team acts as the national alert centre which cooperates and helps all the administrations in preventing security incidents, or if need be to help them to respond quickly and efficiently to any problem that may arise. Especially at the present time, when Administrations must promote the use of new technologies in the public interest, and must become an electronic administration in order to offer citizens all the advantages and services of an information society, as obliged by the Spanish Act 11/2007 of May 22: electronic access to Public Services.

This Services Guide details the functions and services rendered by CCN-CERT to all Spanish Public Administration staff and the means to access them. These resources which are free, will gradually be expanded and are expected to contribute to the smooth running of the administrations and their services, for the benefit of the public.

PORTAL

www.ccn-cert.cni.es

The main tool developed by the CCN-CERT to coordinate and support all persons responsible for the security of ICT from different administrations, is the portal: www.ccn-cert.cni.es. Through this website, it is possible to access all services offered by the Team and described in this Catalogue. Given the critical nature of some of the information given on the website, there is an area of restrictive use aimed at Administration staff, which can be accessed by completing a form which appears on the web page.

Services RENDERED BY THE CCN-CERT TO THE Administration

All services offered by the CCN-CERT can be divided into three large areas, depending on the time and methods used in facing an incident. For these reasons we have the following groups: REACTIVE SERVICES, MANAGEMENT and PROACTIVE SERVICES. At the same time, these services as described below, are differentiated following the needs of the *Constituency*(*) or *Public* which accesses the portal.

1. REACTIVE SERVICES

These services are designed to respond to a threat or an incident that a computer or information system used by the Administration may suffer and minimize their impact. Among the services rendered by the CCN-CERT, the following stand out:

(*) In the CERTs field, the term Constituency refers to the group members to whom the service is provided, that is, all those people responsible for Spanish public administration's information security

INCIDENT MANAGEMENT (constituency)

Any public body that suffers an attack can request the assistance of CCN-CERT to respond to it. This team will provide direct technical assistance or will put the victims in touch with other sites involved in the same incident, will show them relevant technical documents or will suggest how to restore their security systems. It should be borne in mind that the Team reports of incidents from all over the world which in many cases, have similar characteristics or involve the same attackers, and therefore management is much faster and more effective.

In this sense, the policy of CCN-CERT is, to at all times keep confidential all particular information pertaining to the Administration which has asked for help

When and how to report an incident?

Reports sent shortly after an incident occurs will almost certainly contain valuable information for both the applicant for assistance and the CCN-CERT. However, even if an incident took place in the past, it may still be pertinent to report it as it may be useful to other organizations or investigations.

The recommended method to report these incidents is to use the form available in the restricted area of the portal www.ccn-cert.cni.es (Incidents). It can also be made by through the following email address: incidents@ccn-cert.cni.es

Priority incident for the CCN-CERT

- Incidents that affect "classified" information
- Attacks against Public Administration's Internet infrastructures
- Distributed and automatic attacks against Internet sites
- New types of attacks or new vulnerabilities
- Attack with malicious code
- Forensic analysis of compromised machine
- Attacks against Critical Infrastructures Systems

ADVICE, WARNINGS AND VULNERABILITIES (public)

The CCN-CERT provides daily information on vulnerabilities, gives advice and warnings of new threats to information systems, based on both the work done by its own analysts and on contributions from many different and prestigious national and international sources. These vulnerabilities are classified according to their risk and/or confidential level, the possible impact they may have or the difficulty of its solution.

Through the portal www.ccn-cert.cni.es any user of internet can access:

- Daily vulnerabilities bulletins. These bulletins may help them confront failures observed in their systems or applications
- Incident statistics.
- Daily news on ICT security (policy and legislation, cyber security, personal data protection, privacy, online fraud, phishing, spam, viruses, Trojans or events of interest).
- Reports/articles/notices of interest released by the CCN-CERT.

MALICIOUS CODE ANALYSIS (constituency)

The CCN-CERT analyzes all kinds of malicious codes (malware) reported by Public Administration staff, with the ultimate aim of preventing any incidents in their information systems.Thus, the ICT head, may send the team specimens of malicious codes for analysis to the e-mail address malware@ccn-cert.cni.es or through the corresponding link included in the portal

Malicious codes will be analyzed by the CCN-CERT and a report will be sent regarding behaviour, capabilities and the process for elimination. Likewise, the Team will report on the capacity of the different antivirus tools available on the market to detect malicious codes (please see the following complete list of antiviruses in use).

Antivirus analyzed by CCN-CERT

AhnLab	Kaspersky
Antivir	McAfee
Avast	NOD32
AVG	Norman
BitDefender	Panda
ETrust-Vet	QuickHeal
ClamAV	Rising
DrWeb	Sophos
eSafe	Sunbelt
Ewido	Symantec
Fortinet	TheHacker
F-Prot	VBA32
Ikarus	VirusBuster

2. PROACTIVE SERVICES

These services are those whose functions are to reduce security risks to the Administrations by distributing information and implementing protection and detection systems.

The proactive services are designed to improve the infrastructure and security processes of the *Constituency* members before an incident occurs or is detected. The main objective is to prevent incidents and reduce their impact and scope should an incident occur.

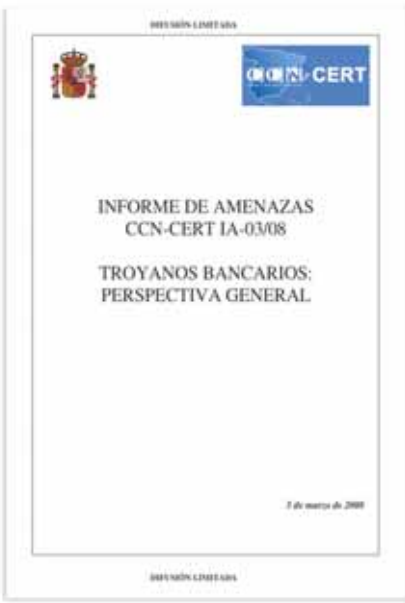
ADVICE AND WARNINGS TO AUTHORIZED USERS (constituency)

The CCN-CERT provides its "constituency" the following information on a daily basis, compiled from different renowned and prestigious sources.

- **Restricted Daily vulnerabilities bulletins.** Those which may help them confront failures observed in their systems or applications. RESTRICTED AREA: www.ccn-cert.cni.es (Alerts).
- **Weekly reports,** on published articles regarding security and level of threats. These reports contain specific sections on hacking, critical infrastructure, threat scene in different countries, government iniciatives, etc. RESTRICTED AREA: www.ccn-cert.cni.es (Resources/Weekly Reports).
- **Reports on malicious code** regarding identified malicious code activity, risk level and where code analysis reports are referred to. RESTRICTED AREA: www.ccn-cert.cni.es (Resources/Malicious Code Reports).

- **Threat reports, classified as Restricted or higher,** which focus on a certain security aspect such as zero-day vulnerabilities, banking Trojans, areas/countries (comprehensive analysis of the position of a given country, in which, for example, the penetration level of broadband communications, cybercrime, security measures at government level, incident response capability take place, etc.). RESTRICTED AREA: www.ccn-cert.cni.es (Resources/ Threat reports).
- **Updates of malicious code signatures** with the aim of obtaining a more efficient detection in the devices for perimeter protection.

Likewise, people who are responsible for security and who are registered in the portal will automatically receive, by e-mail, comprehensive details on threats reviewed by the CCN-CERT with the most relevant information (latest identified threats, updates to the portal…).



AUDITS / SECURITY ASSESSMENTS (constituency)

Revision and detailed analysis of the systems within the Organ which requests it. Such security assessments (STIC inspections) are obligatory for those systems dealing with Classified Information and voluntary for the remaining systems. These assessments allow analysis of the systems and processes in search of potential risks and vulnerabilities, in order to establish appropriate procedures and technical measures to reduce or eliminate them.

The CCN-CERT performs annual security audits in order to detect vulnerabilities within the web services offered by the different Public Administrations. Furthermore, it performs specific penetration tests on request or in the wake of a security incident.

DEVELOPMENT / ASSESSMENT OF SECURITY TOOLS (constituency)

The CCN develops various support tools for security management and makes them available to any Administration ICT staff member who may request them. These tools provide different functional capabilities:

- **Security management:** those used for certification and accreditation, such as analysis and risk management, vulnerability analysis, periodic inspections or response to incidents.
- **Administration of security systems and/or management:** security tools used by Administrations, such as configuration checks, integrity checks, filtering or monitoring of resources.

The CCN facilitate the following tools:

- **CCN-Windows:** tools for management and administration of security regarding:
  - AUDIT: analysis of vulnerabilities, scanners, generating packages, proxies, recognition of the Internet, wireless networks, users and passwords and local checks.
  - PROTECTION: encryption, firewall and intrusion detection.
  - DETECTION: traffic analysis, analysis and monitoring and spyware.
  - REACTION: forensic analysis.

  RESTRICTED AREA: www.ccn-cert.cni.es (Tools).

- **CCN-STIC series:** rules, instructions, guidelines and recommendations for the exclusive use by administration staff. All tools are developed by the CCN with the aim of cooperating in the implemention of projects to improve information security.This comprehensive policy is aimed at those responsible for the Administration's security with the purpose of providing them with the necessary references to help them comply with the security requirements of their systems.

  Some of the guides are classified as Restricted or even higher and their treatment must meet the stipulated regulations established for this classification level.

  RESTRICTED AREA: www.ccn-cert.cni.es (Tools/Series CCN-STIC).

PILAR Tool: Logical Information Procedure for Risk Analysis to evaluate the security status of a system, identify and assess assets and threats posed to it.This tool, which follows the MAGERIT model (Methodology for Analysis and Risk Management of information systems, developed by the Higher Council for Electronic Administration), allows for the classification of assets, value them, establish a map of risks based on a catalogue of threats and determine the effect of safeguards on the state of the risk

Depending on the level of maturity of these safeguards, the tool allows assessment of the level of compliance of the organization with the international standards of personal data protection such as ISO27002 or the national standards such as RD1720 for the protection of personal data and the security, normalization and preservation of the Public Administration Ministry criteria.

RESTRICTED AREA: www.ccn-cert.cni.es (PILAR).

- **Other security tools developed by CCN are:** safety erasure, security tools for e-mail, virtual private networks (VPN) and data diode.

It is worth mentioning that the CCN evaluates commercial and free tools used to perform analysis of vulnerabilities, software damage detection, passwords analysis or anti-spam tools.

INTRUSION DETECTION (constituency)

One of the fundamental keys in the CCN method to solve security incidents is the early detection of intrusions (any set of actions that might compromise the integrity, confidentiality or availability of information or of a computer resource), which can both reduce the response time to these problems and solve them before the situation becomes critical.

In this regard, the CCN-CERT has developed the following early warning services:

- A system based on the correlation of logs (data logging) on the network S.A.R.A. (Application and Networks Systems for the Administrations), which provides a constant index of security compromise and issues warnings before any incident. The aim of this monitoring is to enable the system to obtain information of high value which may help it to enhance the capacity to respond to incidents, adjust its security policy in light of the risks identified and resolve the identified incidents.
- A system based on the analysis of perimeter traffic which protects Internet access within Public Administrations. This service requires an agreement between the Organization and the CCN-CERT.
- A service to monitor non-authorised changes and infections by different types of malicious codes within the Public Adminstration web services.

3. MANAGEMENT SERVICES

The management services are those which seek to improve work processes of both the Public Administration and the CCN-CERT itself. Among others, these services include:

RISK ANALYSIS (constituency)

The CCN-CERT, as already mentioned, provides the latest version of the PILAR to any Administration staff who request it. The main objective of this tool is to conduct an intuitive risk analysis in a short period of time. At the same time, consultancy support is provided for the performance of risk analysis and is adaptable to different environments, among which the following are noteworthy:

- Security profile for classified systems.
- Adaptation of the risk assessment tools to calculate the different types of attacks and security profiles for critical national infrastructures.
- Security profile for Administration.

RESTRICTED AREA: www.ccn-cert.cni.es (PILAR)

AWARENESS AND TRAINING (constituency)

One of the basic pilars of information security is the sensitivity of its users, as well as the continual update of their knowledge. Only in this way, we can proactively confront the increasing threats which grow more and more complex and much harder to detect.

It is therefore essential that ICT staff in all organizations are properly trained, including, of course, the Administration, to combat naivety, ignorance of good practices and the lack of awareness which exists, for the need to preserve security information.

In this sense, and as pointed out by Royal Decree 421/2004, the National Cryptology Centre has the power to train Administration staff specializing in the security field of information technology. For this reason, and by means of STIC courses (free of charge), provided throughout the entire year (in classroom setting and online) through INAP (National Institute of Public Administration) and published in the BOE and by the Ministry of Defence through the BOD. The courses are structured in four different categories.

RESTRICTED AREA: www.ccn-cert.cni.es (Resources)

1. **Information and Security Awareness courses** (Course on Security of the Information Technologies and Communications-STIC-).
2. **Basic Security Courses** (Windows, Linux, Database and Network Infrastructure).
3. **Specific Courses on Security Management** (STIC management, cryptology specialities).
4. **Security Specialization Courses** (STIC accreditation in Unix, Windows or Linux environment; wireless networks, firewall, intrusion detection, security tools, security inspections, Common Criteria and Evidence Search and Integrity Control).

The CCN offers custom designed or complementary courses to those offered by INAP. In this case costs are paid by the applying organisation.

On the other hand, and with the same objective, the CCN conducts seminars and workshops on raising awareness, aimed at training and upgrading administration staff knowledge in the field of information security. All general, autonomous and local administration staff can attend these workshops should they wish to do so.

RESTRICTED AREA: www.ccn-cert.cni.es (Resources).

PRODUCT EVALUATION AND CERTIFICATION (public)

To implant the adequate security level in the Administration systems, it must rely on those products that provide security assurances. In addition, they must be sure that the design of these products is appropriate and that they will not perform unwanted functions. In this regard, the CCN, an organization legally established for this purpose, conducts assessment of the information system or any of its teams, using strict criteria, with the subsequent quality certification based on the security aspects it evaluates. These certifications are, among others, the *Common Criteria*, *Tempest or Cryptology* certifications.

Cryptology Certification

The CCN is responsible for the creation of the Catalogue of Products with Cryptology Certification, which include the products capable of protecting National Classified Information. This way, the encrypted system which has been evaluated and which has obtained the said certification provided by the CCN will be considered a national encryptor, with cryptology certification. For further information you can visit the Centre's web page http://www.ccn.cni.es

Tempest Certification

With regard to Tempest certification, the CCN is the Tempest certifying authority in the Ministry of Defence and, as such it is responsible for developing the necessary training for the protection of equipment / systems and facilities where classified information is processed. As in other NATO member states, national standards are based or are developed to be compatible with NATO's standards. In some cases, these norms are distinguished and extended to adapt themselves to the needs of the Spanish Administration, mainly in those aspects regarding the evaluation of the encryption equipments or the evaluation of the risk coming from the facilities due to its little minimization of the undesired radiations, which are the object of the TEMPEST study.

Common Criteria Certification

The Organization of Certification of the National Evaluation Outline and Certification of the Security of the Information Technologies issues this functional certification in accordance with the standard international criteria, the so-called "Information Technology Security Evaluation Criteria" (ITSEC) and "Common Criteria for Information Technology Security Evaluation", the latter ones were published also as the ISO/IEC 15408 regulation.

This certification is the culmination of an assessment process on the security features of a product or system (under evaluation), which, following a standard methodology and performed by an independent laboratory, accredited and technically trained for this purpose. The aim is to check that the object of the evaluation performs correctly and effectively the security function described in its documentation. For more information, please visit: http://www.oc.ccn.cni.es

Argentona, s/n - 28023 Madrid, Spain

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

MINISTERIO
DE DEFENSA