VERY HIGH

CASTELLANO
ENGLISH
CATALÀ
EUSKARA
GALEGO
VALENCIÀ

OPEN SESSION

HOME
ABOUT US
MISSION AND GOALS
CCN-CERT SERVICES
FAQ
ANNUAL REPORT
CCN
OC
ONS
CNI
CONTACT
INCIDENTS
CCN-CERT NOW
ALERTS AND NOTICES
TOOLS
TRAINING
LEGAL FRAMEWORK
REPORTS
S.A.T.
ENS
CRITICAL INFR.
NEWS
INTERESTING LINKS
PREFERENCES

ACCREDITATIONS

EGC group

GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA

What services offer CCN-CERT?

The CCN-CERT is the CCN's Computer Emergency Response Team. This service was created at the end of 2006 as the Government Spanish CERT and its functions are specified in chapter VII of RD 3/2010, of January 8. This chapter includes the services the CCN-CERT has offered since its creation (which are in part specified in RD 421/2004), and that are now contained in article 37 of this RD:

- Support and coordination for vulnerabilities management and for the resolution of security incidents suffered by the State's General Administration, by the regional and local administrations and the public-sector bodies with their own legal personality or dependent on any of the aforementioned administrations. The CCN-CERT, through its technical support and coordination service, will act quickly to face any targeted attack against the Public Administration's Information Systems. For the fulfillment of these objectives the CCN-CERT can gather the audit reports for the affected systems.

- Research and diffusion of the best practices on information security among all the members of Public Administrations. To this end, the CCN-STIC Series will offer standards, instructions, guidelines and recommendations to implement the ENS and to ensure the security of ICT systems within the

- Training aimed at specialised Public Administration staff in the area of ICT security in order to update the staff's knowledge and to raise awareness and improve the staff's ability to detect and handle incidents.

- Information about vulnerabilities, alerts and advice on new threats targeted at Information Systems, compiled from different renowned and prestigious sources, including their own.

In particular the specific services offered by CCN-CERT are:

- Incident management: Any public organization that suffers an attack against its system can request the CCN-CERT's collaboration. This team will provide direct technical support or will put the organization in contact with other affected systems, or will provide it with relevant technical documents or will suggest it to adopt certain measures to restore the security of their systems. The CCN-CERT receives incident reports from all parts of the world, and sometimes, these incidents have similar characteristics or involve the same attackers, so by centralizing its incident management capabilities, CCN-CERT can provide a faster and more efficient response. CCN-CERT's policy is to keep the confidentiality on the information provided by the public administration that asks for its help.

- Information, alerts, advice and vulnerabilities: CCN-CERT offers all type of information to all its Community, among which we can highlight vulnerabilities, alerts and advice on new threats targeted at Information Systems, based on the work of their own analysts and on the work of different renowned and prestigious collaborating sources, both at a national and international level. These vulnerabilities are classified according to their risk, confidence level, the impact they may have or the difficulty of its resolution.

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

- Early warning system:In order to guarantee an appropriate security level in the systems of public administrations it is necessary to act before incidents occur or, at least, to detect them as soon as possible in order to minimize its impact and scope. Therefore, since 2008, the CCN-CERT has been developing an Early Warning System (SAT) for the rapid detection of incidents and anomalies within the Administration's scope, a system which allows the implementation of preventive, corrective and containment action.

  - Early Warning System of SARA network: This system is based in log correlation (data registry) for the areas of connection of the SARA network that provides a constant commitment to security and t issues alerts for all types of incidents. The system allows the proactive detection of anomalies and attacks on traffic that flows among Ministries and Organizations connected to the aforementioned network and offers a real time vision of the network security level, using different sensors.

  - Internet Early Alert System (individual probes): This system consists of the introduction of an individual probe in the Organization's Internet output which is responsible for collecting relevant security information, and, after a first filtrate, it sends the security events to the Central System which performs a correlation among the different elements and domains.Multiantivirus System / Malicious Code Analysis: The multiantivirus system (MAV) can perform analysis for all kinds of code, by using different antivirus engines, updated in real time. This way, any agency within the Public Administration (general, regional or local) which has a suspicious file that may be infected, can upload it to the web interface. After a while the analysis, the user will receive an e-mail including a report about the suspicious file.

  - Web Analysis System: The Web Analysis System (SAW) is a service developed and implemented by the CCN-CERT, which provides ICT managers with a real time overview of the security level of its webs, detecting possible incidents. In order to achieve it, it performs an analysis of the contents included in the Administration webs.

Back