Respuesta a los incidentes de seguridad de la información en las Administraciones Públicas

Autor: CCN-CERT

Resumen: El desarrollo, la adquisición, conservación y utilización segura de las Tecnologías de la Información por parte de las administraciones públicas es imprescindible para garantizar un funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales. La creación de la Capacidad de Respuesta a Incidentes de Seguridad para la Administración por parte del Centro Criptológico Nacional (CCN-CERT) responde a este objetivo y tiene como misión principal ser el centro de alerta nacional que ayude a todas las AAPP a responder de forma rápida y eficiente a cualquier incidente de seguridad que pudiera surgir.

Palabras clave: Seguridad de la Información, Administración Pública, CERT, amenaza, vulnerabilidad.

1. Introducción

Los sistemas que manejan cualquier tipo de datos (información) en formato electrónico reciben indistintamente las denominaciones de "Tecnologías de la Información y las Comunicaciones (TIC)", "Tecnologías de la Información (TI", "Sistemas de Información" o, en terminología inglesa "Communications and Information Systems (CIS)". Estos conceptos quedan englobados en el término genérico "Sistema", que se define como el conjunto de equipos y programas (hardware y software), métodos, procedimientos y personal, organizado de tal forma que permita almacenar, procesar o transmitir información, y que está bajo la responsabilidad de una única autoridad.

El desarrollo de la denominada Sociedad de la Información implica que, cada vez más, la información se transmite, se procesa o se almacena (se maneja) en algún momento en un sistema. Esto, unido al hecho de que los Sistemas son capaces de manejar mayor cantidad de información en menos tiempo, ha contribuido a conferir mayor importancia a la información propiamente dicha, que es considerada como un valor en sí misma.

Como tal valor, la información manejada en un Sistema puede estar sometida a distintos tipos de amenazas que van a introducir, en su manejo, un determinado nivel de riesgo.

Así, existe riesgo cuando se transmite información por un canal de comunicaciones porque

alguien no autorizado podría estar interesado en conocerla (amenaza)[1] y el canal de comunicaciones tiene vulnerabilidades [2] (un canal de comunicaciones es, en la mayoría de los casos, intrínsecamente inseguro) .

También se introduce un nuevo factor de riesgo con la interconexión entre Sistemas. Aunque esto permite que la información sea accesible desde un sistema aunque, físicamente esté almacenado en otro, este acceso se produce, en ocasiones, sin que el propietario de la información tenga conciencia de ello, amenazando la confidencialidad, disponibilidad o integridad de la información. La implantación generalizada de las redes corporativas y el uso de Internet han contribuido a empeorar la situación en este sentido.

De hecho, las amenazas y vulnerabilidades que afectan a los Sistemas de Información han venido aumentando constantemente en los últimos años, llegando incluso a incrementarse un 55% en los dos últimos años, según datos recogidos por el CCN-CERT.

Respecto a los tipos de riesgos que estas vulnerabilidades implican para nuestros Sistemas de Información, según publica el CERT® Coordination Center[3], la mayoría de las amenazas recibidas constituyen casos de cibercrimen o ciberdelincuencia, de tal forma que se han convertido en una debilidad crítica en las naciones occidentales, máxime si tenemos en cuenta que estas amenazas evolucionan continuamente (virus, phising, defacement, etc.) y a una velocidad cada vez mayor.

Dado que las amenazas cada vez son más complejas y, a veces, difíciles de detectar, se hace necesaria una formación del personal responsable de las TIC en todas las Organizaciones (incluidas, por supuesto, todas las Administraciones Públicas) para luchar contra la ingenuidad, la ignorancia de buenas prácticas y la falta de concienciación existente sobre la necesidad de preservar la seguridad de la información (STIC). Una seguridad que debe estar orientada a garantizar o mantener tres cualidades propias de esta última: disponibilidad, integridad y confidencialidad. En algunos entornos, especialmente en los dedicados a la Administración Electrónica, interesan, además, otros aspectos muy importantes de las transacciones on-line como son la autenticidad o la trazabilidad.

---

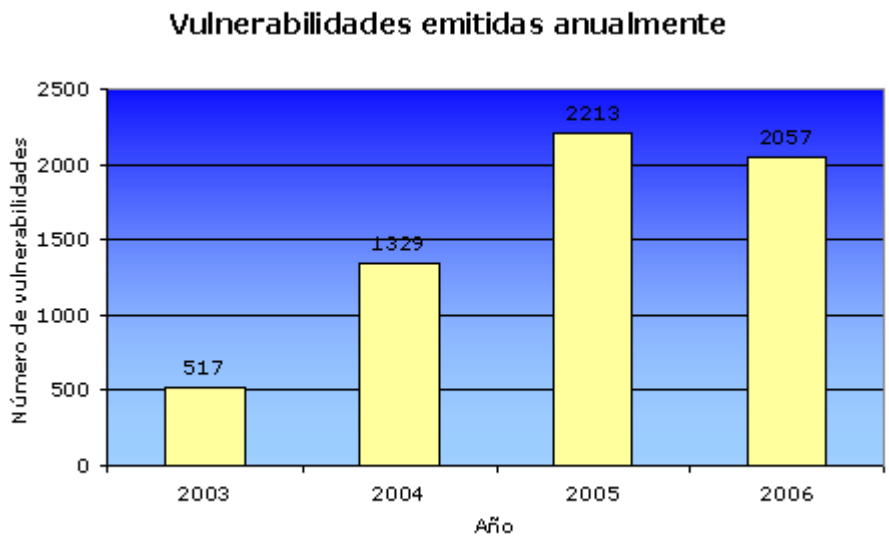
[1] Cualquier circunstancia o evento que puede explotar, intencionadamente o no, una vulnerabilidad específica en un Sistema de las TIC resultando en una pérdida de confidencialidad, integridad o disponibilidad de la información manejada o de la integridad o disponibilidad del propio Sistema.

[2] Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un objetivo o recurso del Sistema.

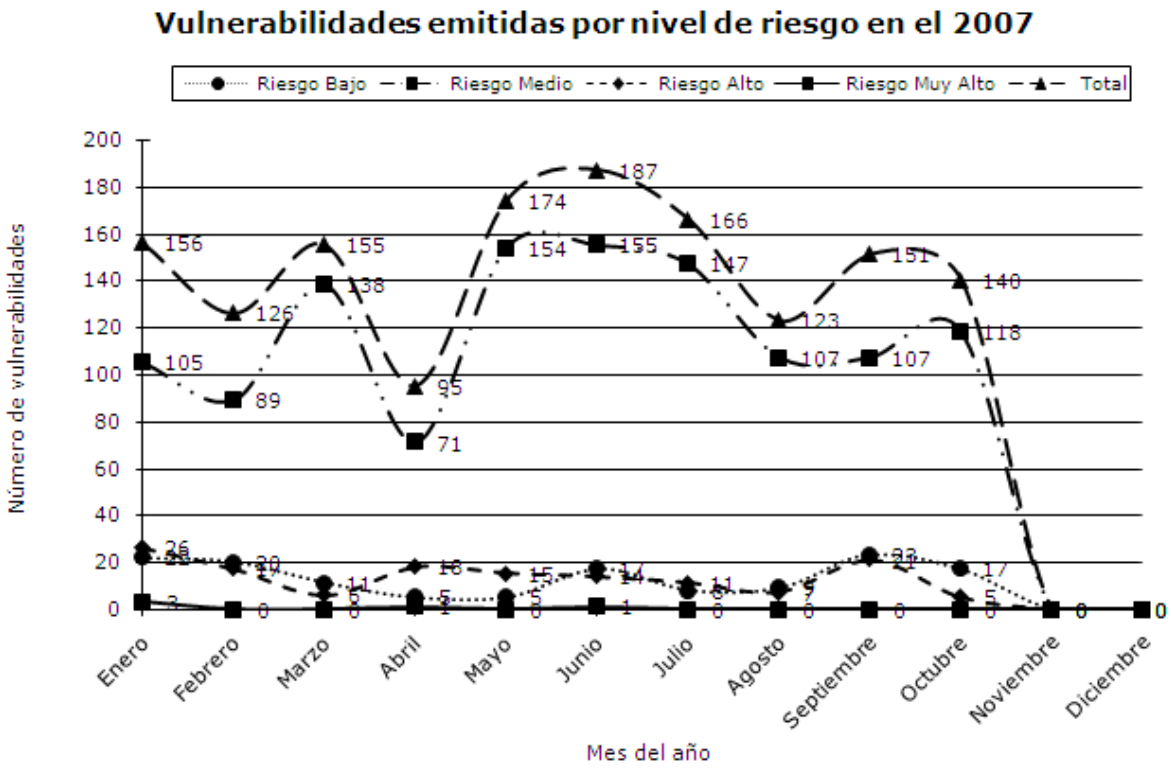
[3] CERT® es una marca de servicios registrada por la Carnegie Mellon University (EEUU)

La Administración en su conjunto no puede ser ajena a este escenario y debe considerar el desarrollo, la adquisición, conservación y utilización segura de las TIC como algo imprescindible que garantice el funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales. Sobre todo, teniendo en cuenta los nuevos retos a los que se enfrenta, procedentes de muy diversas fuentes: Servicios de Inteligencia, Grupos Organizados, Terroristas, Hackers, Grupos Criminales, Empleados deshonestos, etc.

Se hace imprescindible, por tanto, tomar conciencia de los riesgos a través de medidas a todos los niveles (legislativas, organizativas y técnicas) así como de la implentación de herramientas técnicas de seguridad (anti-virus, firewalls, software para autenticación de usuarios o para cifrado de la información) y del empleo de productos certificados, de inspecciones o auditorías de seguridad, etc.



Fuente: CCN-CERT



Fuente: CCN-CERT

2. Marco legislativo

La sociedad española, tal y como recoge la exposición de motivos de la **Ley 11/2002,** de 6 de mayo, que regula las funciones del **Centro Nacional de Inteligencia (CNI)**, demanda unos Servicios de Inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional. No cabe duda de que entre los elementos característicos de este escenario figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización.

La Administración no es ajena a este escenario considerando el desarrollo, adquisición, conservación y utilización segura de las TIC como algo imprescindible para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

La Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC) es tan importante para la seguridad y el bienestar de los ciudadanos como lo es la protección de los propios ciudadanos, sus intereses y su sociedad.

Asimismo, continúa la exposición de motivos, el concepto de seguridad de los sistemas de

información no sólo abarca la protección de la confidencialidad de ésta; en la mayoría de los casos es necesario también que los sistemas permitan el acceso de los usuarios autorizados, funcionen de manera íntegra y garanticen que la información que manejan mantiene su integridad. En consecuencia, la seguridad de los sistemas de información debe garantizar la confidencialidad, la disponibilidad y la integridad de la información que manejan y la disponibilidad y la integridad de los propios sistemas.

En este mismo sentido, el capítulo I, artículo 4º de la citada Ley, sitúa como funciones del CNI, el coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información, informar sobre la adquisición coordinada de material criptológico y formar personal, propio de otros servicios de la administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro. También se cita, dentro de sus funciones, el velar por el cumplimiento de la normativa relativa a la protección de la información clasificada.

Por todo ello, señala la Ley, se hace necesaria la existencia de un Organismo que, partiendo de un conocimiento de las tecnologías de la información y de las amenazas y vulnerabilidades que existen, proporcione una garantía razonable sobre la seguridad de los productos y de los Sistemas de las TIC.

1.1. *Centro Criptológico Nacional*

En el año 2004, a través del Real Decreto 421/2004, se creó el **Centro Criptológico Nacional (CCN),** adscrito al CNI, como Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

Dicho RD fija las funciones y el ámbito de actuación del CCN entre las que figuran la siguientes:

- Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

- Formar al personal de la Administración especialista en el campo de la seguridad de las TIC
- Constituir el organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito
- Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura
- Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas antes mencionados.
- Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.
- Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

1.2. *Plan AVANZA*

El Plan AVANZA 2006-2010 para el desarrollo de la Sociedad de la Información y de Convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas (Ministerio de Industria, Turismo y Comercio), en su Anexo I, menciona la creación de una infraestructura básica de centro de alerta y respuesta ante incidentes de seguridad que atienda a las demandas específicas de los diferentes segmentos de la sociedad. Sectores críticos, agencias gubernamentales, AAPP, PYMEs, grandes corporaciones y ciudadanos recibirán el adecuado asesoramiento por parte de estos centros.

En este sentido, se habla de la creación de centros de seguridad y de establecer los procedimientos y protocolos que permitan coordinar sus funciones y actuaciones. En este mismo texto se adelanta la creación de un **CERT** para la Administración/Gubernamental, un CERT para PYMEs y una unidad de lucha contra la violación de la privacidad (lucha contra el spam, el phising y otros fraudes).

En este contexto, y teniendo en cuenta además, el continuo incremento de las amenazas y vulnerabilidades sobre los Sistemas de Información de todo el mundo citado anteriormente, se

enmarca la constitución de la Capacidad de Respuesta a Incidentes de Seguridad de la Información en la Administración Pública, del Centro Criptológico Nacional (CCN-CERT), dependiente del Centro Nacional de Inteligencia.

3. Contexto internacional

En 1988, tan sólo existían unos 70.000 hosts interconectados y hasta ese momento la seguridad no había sido un aspecto a tener en cuenta. Sin embargo, el 2 de noviembre de 1988 aparece el Gusano de Morris, creado por el estudiante predoctoral, graduado en Harvard, Robert Tappan Morris, de 23 años. El gusano usaba un defecto del sistema operativo Unix para reproducirse hasta bloquear el ordenador. En pocas horas el 10% de los ordenadores conectados dejaron de funcionar correctamente, lo que supuso un coste de 15 millones de dólares. Las copias del virus llegaban a través del correo electrónico que, una vez instalado, realizaba copias repetidas de sí mismo mientras intentaba propagarse, logrando que muchas veces los ordenadores se quedasen sin recursos.

Aunque sus abogados aseguraban que Morris "intentaba ayudar a la seguridad de Internet cuando su programa se salió de su control por accidente", la fiscalía norteamericana argumentó que el gusano "no se trató de un error, sino de un ataque contra el gobierno de los Estados Unidos". Finalmente Morris fue condenado a tres años de libertad condicional, una multa de 10.000 dólares y 400 horas de servicio a la comunidad.

Una de las principales consecuencias de este virus fue que el Departamento de Defensa estadounidense comenzó a tener en cuenta la seguridad informática y encargó a la Universidad Carnegie Mellon, en Pittsburgh, la creación de un equipo capaz de hacer frente a este nuevo tipo de amenazas. El resultado fue la constitución del denominado *Computer Emergency Response Team* (CERT®); es decir, Equipo de Respuesta a Incidentes de Seguridad Informática (www.cert.org).

Bajo estas mismas siglas comenzaron a formarse otros grupos en distintas universidades norteamericanas encargados de estudiar la seguridad de las redes y ordenadores para proporcionar servicios de respuesta ante incidentes a víctimas de ataques, publicar alertas relativas a amenazas y vulnerabilidades y ofrecer información que ayudara a mejorar la seguridad de estos sistemas.

A su vez, empezó a hablarse de CSIRT (*Computer Security and Incident Response Team*) para completar el concepto de CERT® y ofrecer, como valor añadido, los servicios

preventivos y de gestión de seguridad. Hoy en día se emplean de forma similar ambos términos.

Poco tiempo después, a principios de la década de los noventa, la idea se trasladó a Europa y, gracias al apoyo del programa técnico TERENA (www.terena.org), empezaron a crearse los primeros CERTs en el Viejo Continente[4]. De hecho, en la actualidad TERENA continúa siendo el principal foro europeo de CERTs en el que se colabora, innova y comparte información con el fin de "promover y participar en el desarrollo de unas infraestructuras de información y telecomunicaciones de alta calidad en beneficio de la investigación y la educación", tal y como recogen sus estatutos. Asimismo, auspicia un t*ask-force* para promover la cooperación entre CSIRTs en Europa.

De esta forma, y tras la continua proliferación de CERTs en todo el mundo y en todos los ámbitos de la sociedad (Administración, universidad, investigación, empresa, etc.), se ha ido tejiendo en los últimos años una tupida malla de seguridad informática que, necesariamente, ha de estar interconectada, dado que, si existe algún sector globalizado, con ausencia absoluta de fronteras, este es, sin lugar a dudas, el de Internet.

Por ello, se ha constatado la necesidad de compartir objetivos, ideas e información sobre la seguridad de forma global. Del mismo modo, resulta fundamental que cualquier equipo de respuesta a incidentes se mantenga en contacto con otros equipos del resto del mundo en caso de ataque y se asegure de qué fuentes de información son fiables. De ahí, la importancia de los distintos foros internacionales existentes, tanto el citado de ámbito europeo (TERENA), como mundial (FIRST). Este último es, sin lugar a dudas, el primero y más importante por su representatividad mundial.

De hecho, el *Forum of Incident Response and Security Teams* (FIRST), y desde su creación en noviembre de 1990, ha pasado de contar con nueve equipos de seguridad de EEUU y uno europeo, a los 189 miembros que lo componen en la actualidad, procedentes de 41 países y del entorno gubernamental, económico, educativo, empresarial y financiero (a él pertenecen cuatro CERTs españoles, incluido el CCN-CERT).

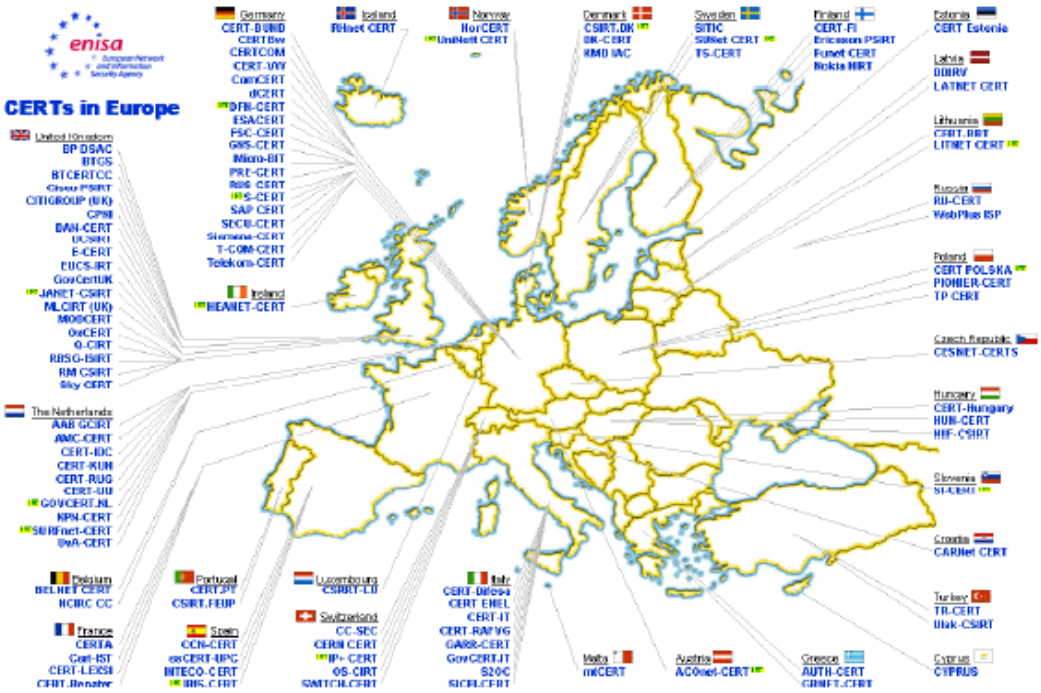
Su objetivo fundamental es coordinar a los diferentes CSIRTs de todo el mundo, compartiendo información sobre vulnerabilidades y ataques a nivel global y divulgando medidas tecnológicas que mitiguen el riesgo de ataques a sistemas y usuarios conectados a

[4] En España el primer equipo de estas características se formó en torno a la Universidad Politécnica de Cataluña en 1994 (esCERT), al que le siguió en 1995, el Iris-CERT (servicio de seguridad de RedIRIS, red académica y de investigación nacional).

Internet, que dan servicio a sus respectivas comunidades. También se encuentra entres sus cometidos, el fomentar la creación de nuevos equipos de coordinación de emergencias, tanto de ámbito nacional como a nivel corporativo.

Conviene reseñar, asimismo, que prácticamente la mitad de los CERTs existentes en el mundo se sitúan en Europa (pese a que Estados Unidos cuenta con un total de 63 equipos). Así, países como Alemania (con 21 CERTs), Reino Unido (17) u Holanda (10) encabezan la lista por número de equipos destinados a asistir a sus respectivas comunidades. Incluso, compañías como Nokia, Ericsson o Siemens, cuentan con su propio CERT.

CERTs en Europa



Fuente: ENISA.

4. Objetivos del CCN-CERT

En este contexto mundial, con un continuo incremento de las amenazas y vulnerabilidades sobre los Sistemas de Información, en el año 2004, empezó a fraguarse lo que sería el CERT® gubernamental español, a raíz del citado Real Decreto 421/2004, que regula la actividad del Centro Criptológico Nacional (CCN). Así, y tras dos años de intenso trabajo, a principios de este 2007, se presentó el CCN-CERT cuyo principal objetivo es contribuir a la mejora del

nivel de seguridad de los sistemas de información de las Administraciones Públicas (tanto la administración general, como la autonómica y local).

Su constitución, además, venía a suplir la ausencia de un CERT gubernamental español, a imagen y semejanza de los existentes en otros países de nuestro entorno, que pudiese estar presente en los principales foros internacionales (caso de los mencionados TERENA y FIRST), en los que compartir objetivos, ideas e información sobre la seguridad de forma global.

Por todo ello, su misión es convertirse en el centro de alerta nacional que coopere y ayude a todas las AAPP a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir y afrontar de forma activa las nuevas amenazas a las que hoy en día están expuestos.

Del mismo modo, el CCN-CERT se compromete a divulgar y asesorar a todas las Administraciones en la implantación de medidas tecnológicas que mitiguen el riesgo de sufrir cualquier ataque y puedan cumplir, de esta forma, con las elevadas exigencias de seguridad que en la actualidad se requieren. Todo ello, en el convencimiento de que el desarrollo, la adquisición, conservación y utilización segura de las Tecnologías de la Información y las Comunicaciones (TIC) por parte de la Administración es imprescindible para garantizar un funcionamiento eficaz al servicio del ciudadano, que genere confianza y, por lo tanto, contribuya a la implantación real de la Sociedad de la Información.

Para contribuir a esta mejora del nivel de seguridad, el CCN-CERT ofrece sus servicios a todos los responsables TIC de las diferentes AAPP a través de tres grandes líneas de actuación:

4.1 Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información.

4.2 Investigación, formación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones Públicas. En este sentido, el CCN-CERT cuenta con diversas herramientas puestas a disposición de todos los responsables TIC de las distintas administraciones:

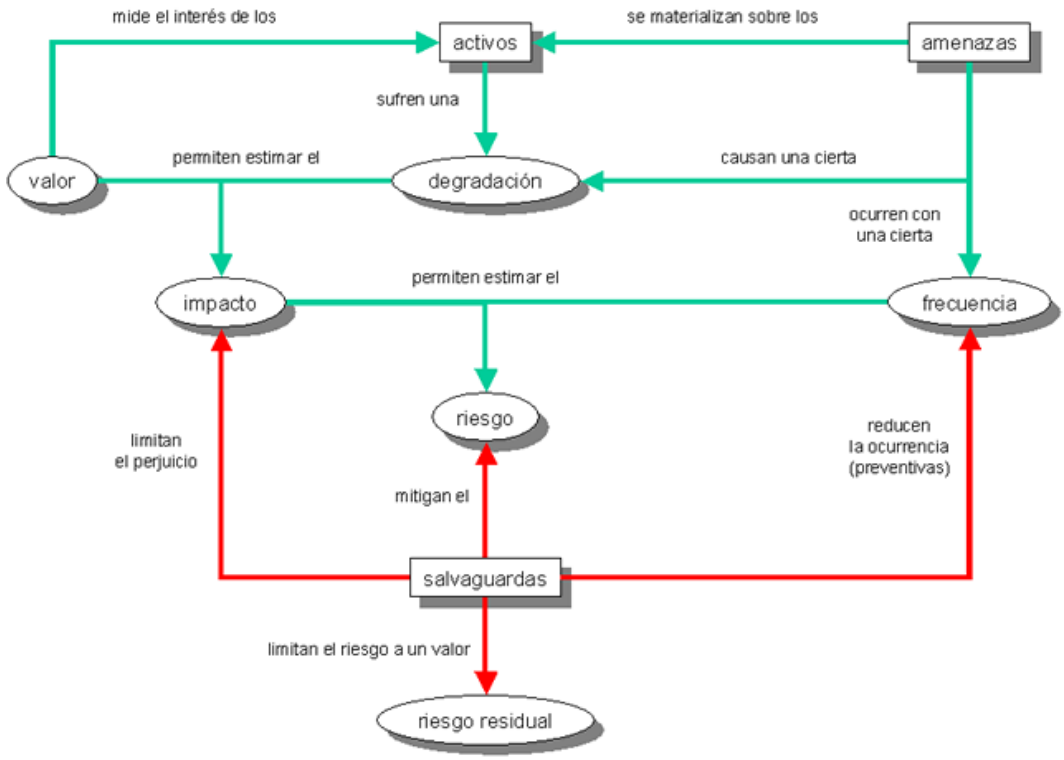
a) Series CCN-STIC: una serie de documentos que incluye normas,

instrucciones, guías y recomendaciones para garantizar la seguridad de los Sistemas de las TIC en la Administración, constituyendo un marco de referencia que sirva de apoyo al personal en su tarea de proporcionar seguridad a los Sistemas bajo su responsabilidad.

b) Cursos STIC: destinados a formar al personal de la Administración especialista en el campo de la seguridad de las TIC y desarrollados a lo largo de todo el año. Su principal objetivo, aparte de mantener el conocimiento del propio equipo, es el de permitir la sensibilización y mejora de las capacidades del personal para la detección y gestión de incidentes. Entre otros, existen cursos informativos y de concienciación en Seguridad, de gestión de seguridad, de especialidades criptológicas o de acreditación STIC en entornos Linux, redes inalámbricas, detección de intrusos o cortafuegos.

c) Herramienta PILAR (Procedimiento Informático Lógico para el Análisis de Riesgos): una herramienta que sigue el modelo MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información desarrollada por el Ministerio de Administraciones Públicas) y que permiten evaluar el estado de seguridad de un sistema, identificando y valorando sus activos e identificando y valorando las amenazas que se ciernen sobre ellos. De este modelado surge una estimación del riesgo potencial al que está expuesto el sistema .

HERRAMIENTA PILAR (PROCEDIMIENTO INFORMÁTICO LÓGICO PARA EL ANÁLISIS DE RIESGOS)



4.3 Soporte ante incidentes y vulnerabilidades mediante servicios de apoyo técnico y coordinación con las distintas Administraciones, con el fin de actuar adecuada y rápidamente ante cualquier ataque que se pueda recibir en los sistemas de información de cualquier AAPP española.

Asimismo, el CCN-CERT ofrece información, formación y herramientas para que las distintas administraciones puedan desarrollar sus propios CERTs, permitiendo a este equipo actuar de catalizador y coordinador de CERTs gubernamentales, tal y como señala el citado Plan AVANZA.

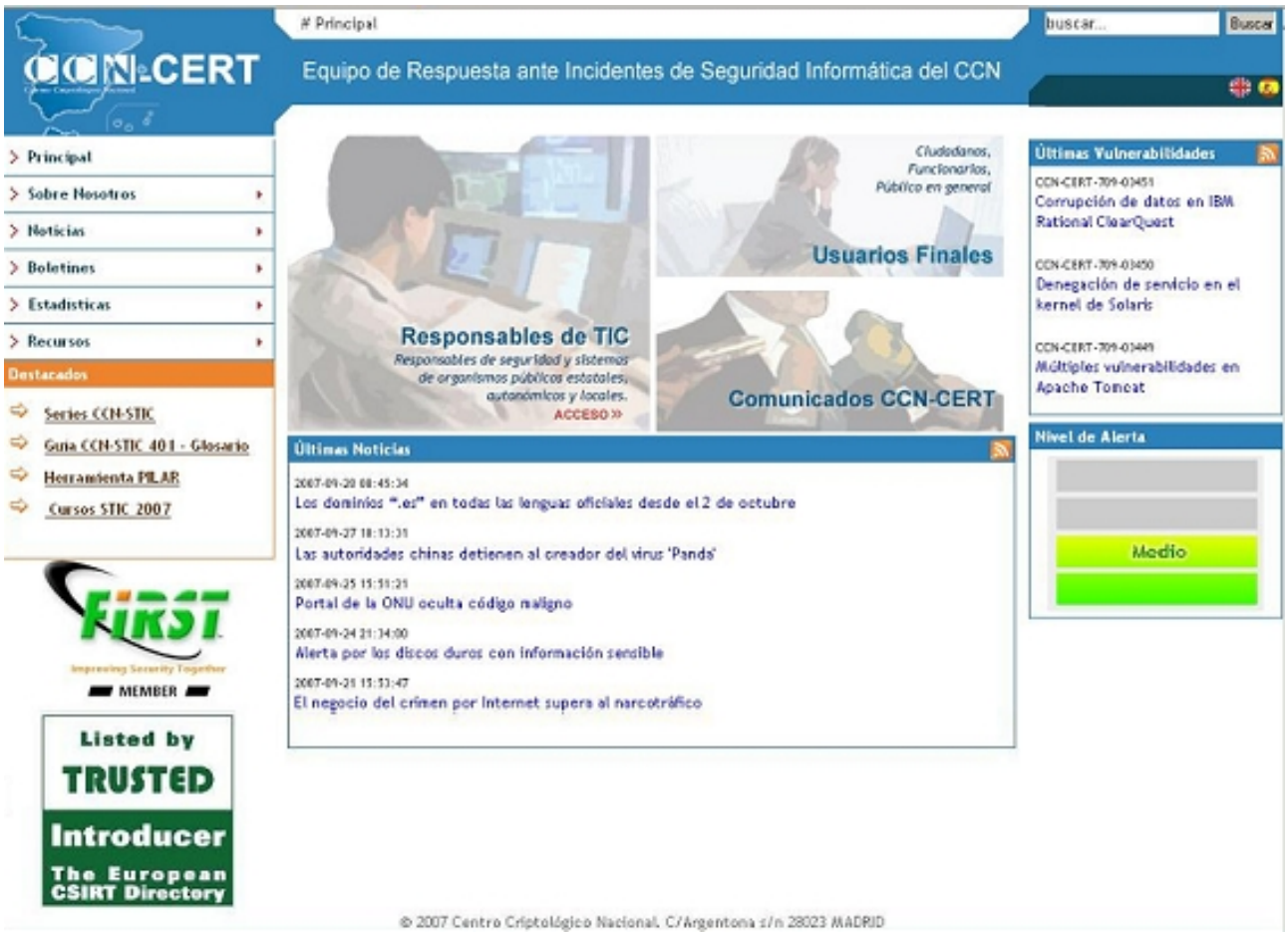
Este servicio, por supuesto, cuenta con un grupo de expertos multidisciplinares, trabajando con unos procesos y plataformas comunes, que operan en estructuras de soporte de 24 horas al día (los siete días de la semana).

5. Portal www.ccn-cert.cni.es

Para una óptima coordinación con toda su Comunidad, el CCN-CERT ha desarrollado un portal en Internet (www.ccn-cert.cni.es) con el que facilitar la comunicación con los responsables TIC de todas y cada una de las Administraciones que así lo deseen. A través de esta página web se ofrece información actualizada diariamente sobre amenazas, vulnerabilidades, guías de configuración de las diferentes tecnologías, las herramientas de seguridad anteriormente mencionadas (PILAR), cursos de formación, mejores prácticas de seguridad o formularios de comunicación de incidentes de seguridad.

Dado el carácter crítico de algunos de los aspectos recogidos en el portal, existe una parte de acceso restringido que exige el registro previo de sus usuarios. Los responsables de seguridad TIC pueden solicitar dicho registro a través de un formulario que se encuentra en la sección "*Responsables TIC*" del portal. De esta forma, y una vez autorizada su alta, podrán acceder a toda la información, productos y servicios puestos a su disposición por el CCN-CERT.

Gracias a este registro, el CCN-CERT pretende conseguir una comunicación directa con su comunidad para poder actuar adecuada y rápidamente ante cualquier hipotético ataque. De hecho, desde la puesta en marcha del portal, en febrero de este año 2007, se han producido más de 25.000 visitas, y se han registrado más de 600 usuarios, todos ellos responsables TIC de las distintas administraciones españolas.



5. Servicio imprescindible

Nadie duda en estos momentos de la trascendencia e importancia de la seguridad de los sistemas y redes de información de los que depende, en gran medida, nuestra sociedad actual. Incluso la mejor infraestructura de seguridad de información no puede garantizar que una intrusión no acabe por afectar a un equipo.

Estos sistemas tienen ante sí una lista interminable de amenazas y potenciales delitos que les afectan y que pueden provenir de muy diferentes frentes: hackers (intrusos que penetran en redes corporativas con diferentes fines), ciberdelincuentes, terroristas, mafias, servicios secretos e, incluso, usuarios internos malintencionados o "despistados".

Además, estas amenazas son cada vez más complejas y difíciles de detectar. Si antaño las técnicas y herramientas de ataque estaban en manos de especialistas, ahora han pasado al gran público y están disponibles en Internet a precios muy asequibles para cualquiera que tenga la motivación suficiente para lanzar un ataque; de manera que la magnitud de los daños que se pueden causar y la velocidad de los mismos se incrementan continuamente.

En estas circunstancias, se hace imprescindible incrementar la formación del personal responsable de las TIC en todas las Organizaciones (incluidas, por supuesto, todas las Administraciones Públicas) para luchar contra la ingenuidad, la ignorancia de buenas prácticas y la falta de concienciación existente sobre la necesidad de preservar la seguridad de la información. Una seguridad que debe estar orientada a garantizar o mantener tres cualidades propias de esta última: disponibilidad, integridad y confidencialidad.

La Administración en su conjunto no puede ser ajena a este escenario y debe considerar el desarrollo, la adquisición, conservación y utilización segura de las tecnologías de la información como algo imprescindible que garantice el funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales. Es, precisamente la Administración, la que debe asegurar que las prácticas de tecnología y gestión de la seguridad son usadas adecuadamente para resistir ataques interconectados, limitar el daño y mantener la continuidad de los servicios críticos a pesar de ataques exitosos, accidentes o fallos.

De hecho, cuando se produce cualquier incidente de seguridad en un ordenador, es crítico para una organización y, por supuesto, para la Administración, contar con un protocolo eficaz de respuesta. La velocidad con la cual se reconozca, analice y responda a un incidente limitará el daño y bajará el coste de la recuperación.

Haciendo un paralelismo, se podría decir que la creación del CCN-CERT representa a la seguridad de la información y las nuevas tecnologías, lo que el 112 ha supuesto para los servicios de urgencia. Su misión de ayuda y cooperación con todas las Administraciones Públicas (estatal, autonómica y local) para que éstas puedan responder ante cualquier ataque a sus sistemas de forma rápida y eficiente, así lo demuestra.

Es, por lo tanto, un paso más y muy necesario, en la lucha por la seguridad de la información y, por ende, de la seguridad nacional.