Capacidad de Respuesta ante Incidentes de Seguridad de la Información en la Administración Pública del Centro Criptológico Nacional (CCN-CERT)

- **Cooperar con todas las Administraciones Públicas (estatal, autonómica y local) para responder ante cualquier ataque informático de forma rápida y eficiente, máxima prioridad de este servicio gubernamental.**

- **El desarrollo, la adquisición, conservación y utilización segura de las 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.**

En el punto cuarto de la Exposición de Motivos de la **Ley 11/2007**, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos se asegura que: "*El principal reto que tiene la implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en la sociedad en general y en la Administración en particular es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización*". Del mismo modo, en el Título Preliminar y dentro de los principios generales de dicha Ley, se recogen los de seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas; accesibilidad a la información a través de sistemas que permitan obtenerlos de manera segura y comprensible; así como cooperación en la utilización de medios electrónicos por las AAPP.

Por otro lado, el **Real Decreto 421/2004**, que regula el **Centro Criptológico Nacional** (CCN), dependiente del **Centro Nacional de Inteligencia** (CNI), señala entre sus funciones las de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de las TIC en la Administración. De igual forma, el R.D. le asigna la formación del personal de la Administración especialista en el campo de la seguridad de las TIC; constitución del Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito; así como la coordinación, promoción, desarrollo, obtención, adquisición y utilización de la tecnología de seguridad de los Sistemas antes mencionados.

De igual forma, 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 el desarrollo de una red de centros de seguridad cuyo principal objetivo sea crear una infraestructura básica de centros de alerta y repuesta ante incidentes

de seguridad que atienda a las demandas específicas de los diferentes segmentos de la sociedad. Sectores críticos, agencias gubernamentales, Administración Pública, PYMEs, Grandes Corporaciones y ciudadanos deberían recibir, según el citado Plan, 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.

En este contexto, y teniendo en cuenta además, el continuo incremento de las amenazas y vulnerabilidades sobre los Sistemas de Información, se enmarca la reciente constitución del **CCN-CERT** (presentado a principios de este 2007); la Capacidad de Respuesta ante Incidentes de Seguridad de la Información para las Administraciones Públicas del Centro Criptológico Nacional.

El término CERT proviene de las siglas en inglés *Computer Emergency Response Team* y viene a definir a una organización que estudia 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 para ofrecer información que ayude a mejorar la seguridad de estos sistemas. A estos servicios, y como valor añadido, suele unirse, bajo la denominación CSIRT (*Computer Security and Incidente Response Team*) los servicios preventivos y de gestión de seguridad.

1. OBJETIVOS DEL CCN-CERT

Así pues, la creación del CCN-CERT tiene como principal objetivo contribuir a la mejora del nivel de seguridad en los sistemas de información de las AAPP y afrontar de forma activa las nuevas amenazas a las que hoy en día están expuestos.

Para ello, su misión es convertirse en el **centro de alerta nacional** que coopere y ayude a todas las AAPP (general, autonómica y local) 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:

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

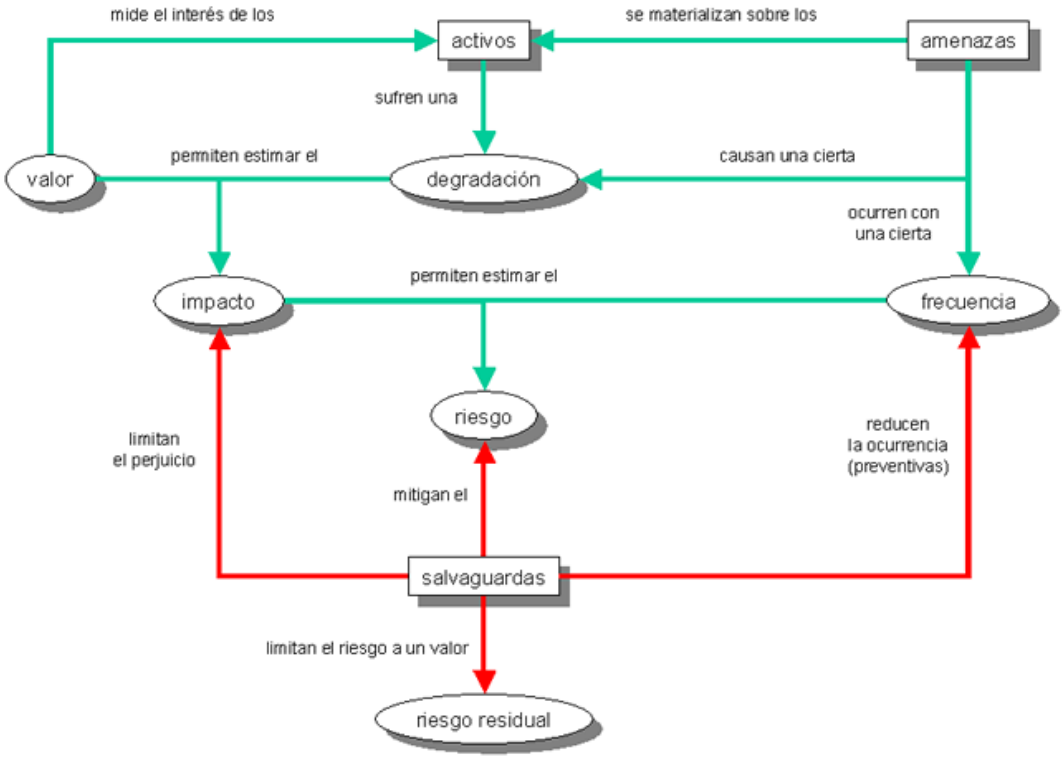
-Investigación, formación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones Públicas. En este sentido, el CCN-CERT cuenta con diversas herramientas puestas a disposición de todos los responsables TIC de las distintas administraciones:

1. 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.

2. 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. 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.

3. 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 *(véase **Figura. 1**)*

Figura 1. **HERRAMIENTA PILAR (PROCEDIMIENTO INFORMÁTICO LÓGICO PARA EL ANÁLISIS DE RIESGOS)**



-**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 los distintos organismos de la Administración puedan desarrollar sus propios CERTs, permitiendo a este equipo actuar de catalizador y coordinador de los CERTs que vayan surgiendo, tal y como señala el citado Plan AVANZA.

2. PORTAL www.ccn-cert.cni.es

Para una óptima coordinación, 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.

De hecho, y 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 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 17.200 visitas, y se han registrado más de 480 usuarios, todos ellos responsables TIC de las distintas administraciones españolas.

3. IMPLEMENTACIÓN DEL PROYECTO

La constitución, implantación y seguimiento del CCN-CERT es un proyecto con continuidad en el tiempo que, desde su puesta en marcha (principios de este año 2007), ha contado con la participación activa de quince personas entre responsables de proyecto, consultores, analistas, programadores y responsables de comunicación. Entre las labores ya realizadas destacan las siguientes:

1. Servicios de Información

a) Diseño y desarrollo de la plataforma de servicios en Internet necesaria (hardware, software y comunicaciones) que soporta los servicios del CCN-CERT hacia su Comunidad.
b) Mantenimiento y actualización de los contenidos del Portal (www-ccn-cert.cni.es). En él, 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. La mayor parte de estos servicios requieren el registro previo de los usuarios.

c) Mantenimiento y explotación segura de la Plataforma, realizando una gestión 24x7 de todo el sistema, en coordinación con el proveedor de la infraestructura.
d) Diseño y aprovisionamiento de los sistemas internos de información (back-office) en los que los expertos del Equipo de Respuesta realiza sus labores.
e) Puesta en marcha del laboratorio de investigación y respuesta ante incidentes

2. Plan de Comunicación y Promoción

a) Integración en Organismos Internacionales, tanto a nivel europeo (TERENA TF-CSIRT), como internacional (FIRST).
b) Plan de visitas (roadshow) por las distintas autonomías para la presentación del servicio a los responsables TIC de las distintas Administraciones (general, autonómica y local).
c) Desarrollo de eventos periódicos de comunicación con la prensa.
d) Participación en eventos comerciales de interés.
e) Publicación y envío de estadísticas, noticias, boletines de vulnerabilidades y otros contenidos por feeds RSS.

3. Desarrollo de Políticas y Procedimientos

a) Estudio del contexto normativo y regulatorio para el adecuado desarrollo de las políticas y procedimientos y los requerimientos del Servicio de Gestión de Incidentes.
b) Desarrollo de políticas.
c) Desarrollo de procedimientos operativos.
d) Auditoría y revisión periódica de las políticas y los procedimientos.

4. Servicios de Gestión de Incidentes

a) Desarrollo del Plan de Respuesta a Incidentes.
b) Diseño y desarrollo de procesos y procedimientos.
c) Implantación del servicio.
d) Soporte y mantenimiento del servicio.

5. Servicios de Formación

a) Interna (mantenimiento de los conocimientos del equipo del CCN-CERT de forma continua).
b) Formación continua para la Comunidad que permita sensibilizar y mejorar sus capacidades para la detección y gestión de incidentes.

Conviene reseñar que, hasta la fecha, el proyecto está ejecutado en su conjunto en un 90 por ciento, aproximadamente, con unos resultados altamente positivos, teniendo en cuenta el grado de implementación, sensibilización y acogida que dicho proyecto está teniendo entre los responsables TIC de las distintas Administraciones Públicas españolas, así como el grado de conocimiento del mismo entre su Comunidad. Así, por ejemplo, tras la puesta en marcha del Portal y toda la plataforma de servicios que conlleva, 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.

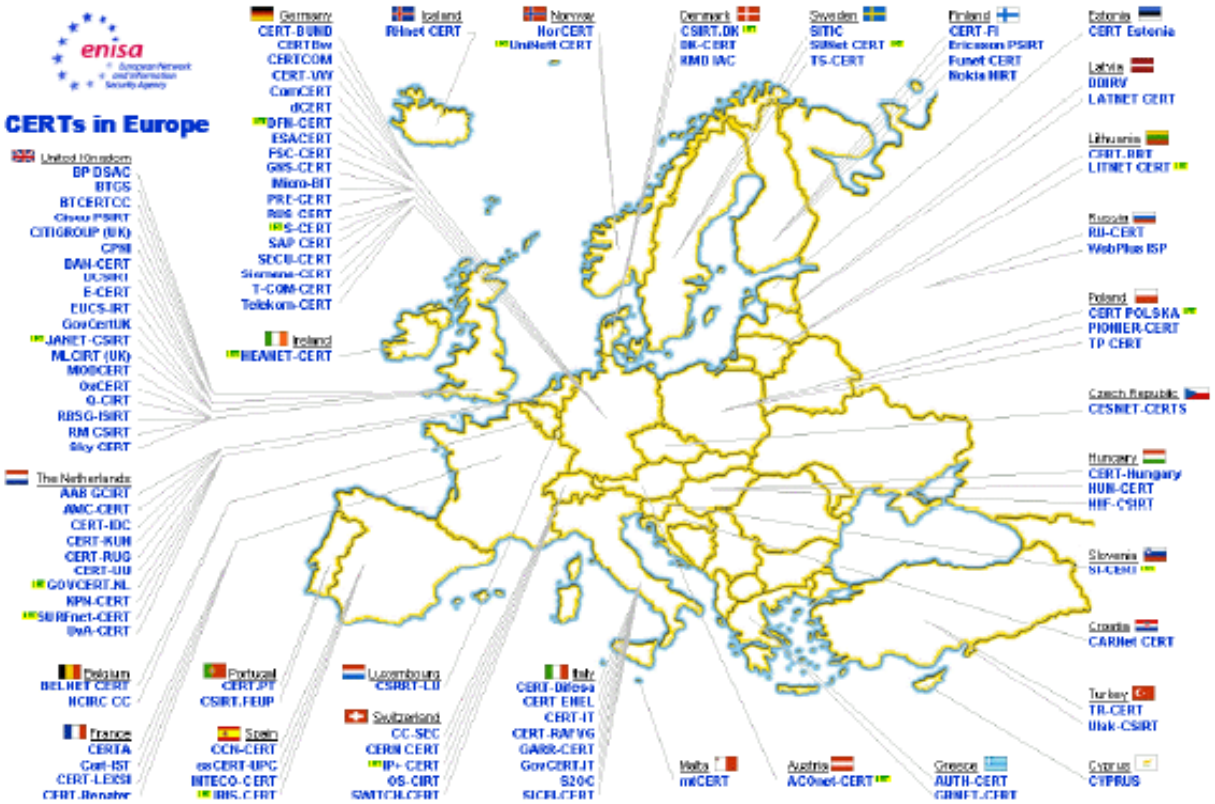
También se ha observado una excelente acogida entre los medios de comunicación nacionales que se han venido haciendo eco de los distintos comunicados de prensa emitidos por CCN-CERT, en particular sobre su presentación el pasado mes de abril (difusión estimada sobre OJD de 25 millones de lectores), que redunda en beneficio del proceso de sensibilización necesario para tomar conciencia de la importancia de la Seguridad de la Información y las Comunicaciones.

4. PROYECCIÓN INTERNACIONAL

La creación de este servicio ha venido a suplir la ausencia de un CERT gubernamental español, a imagen y semejanza de los existentes en todos los países de nuestro entorno, que pueda participar en los principales foros y organizaciones internacionales, en los que se comparten objetivos, ideas e información sobre la seguridad de forma global.

De hecho, desde que en 1988 se creara el primer CERT perteneciente la Universidad Carnegie Mellon, en Pittsburg (Estados Unidos), la proliferación de este tipo de equipos en todo el mundo y en todos los ámbitos de la sociedad (Administración, Universidad, Investigación, Empresa, etc...) ha sido continuo. Poco a poco, se ha ido tejiendo una tupida malla de seguridad informática que, necesariamente, está interconectada y que cuenta con protocolos de respuesta ante cualquier incidente de seguridad. No en vano, la velocidad con la cual se reconozca, analice y responda a un incidente limitará el daño y bajará el coste de recuperación. De ahí, la importancia de los distintos foros internacionales existentes, tanto en el ámbito europeo (**TERENA**), como mundial (**FIRST**), a los cuales se ha adherido el CCN-CERT. *(**véase Figura 2.**).*

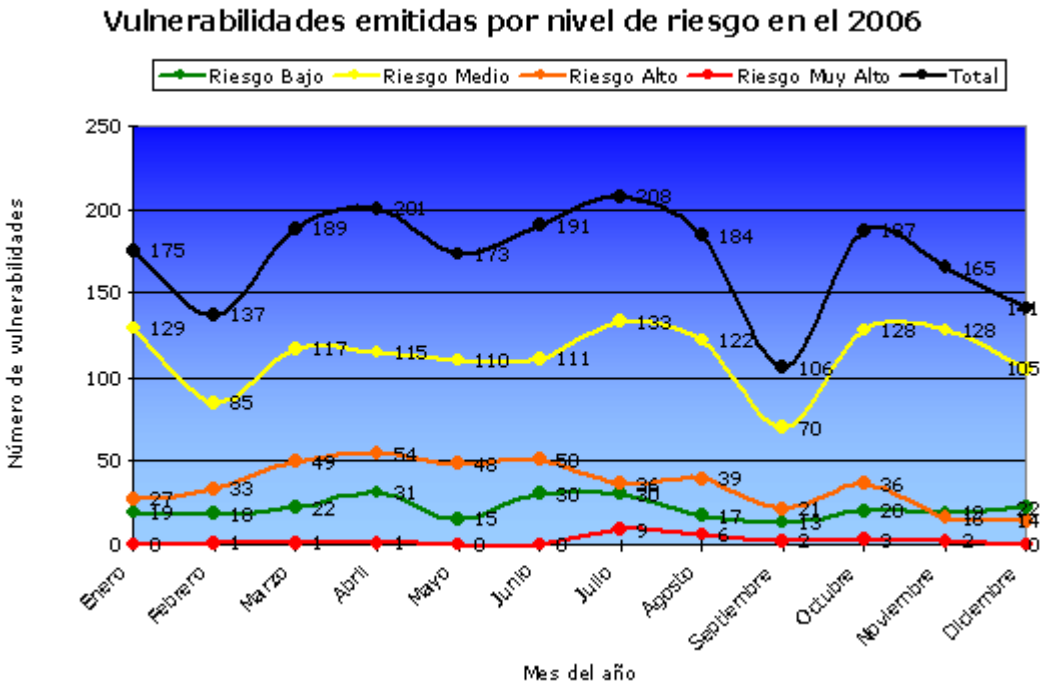
Figura 2. CERTs en Europa



5. SERVICIO IMPRESCINDIBLE

La necesidad de este nuevo servicio queda patente al analizar las estadísticas de amenazas y vulnerabilidades registradas por el CCN-CERT. Éstas se incrementaron en un 55% en los dos últimos años. Así, de las 1.329 publicadas en 2004 (obviamente, no todas explotadas) se pasó a 2.057 en 2006, lo que representa un incremento del 54,7%. *(**véase Figura 3.**).*

Figura 3



Si bien es cierto que en los ocho primeros meses del año 2007 se observa un descenso del 18 por ciento en el número de amenazas y/o vulnerabilidades registradas frente al mismo período del ejercicio 2006 (1.182 frente a las 1.458 registradas hasta agosto del pasado año) *(**véase Figura 4.**)*, basta un repaso a la serie de datos de los últimos cuatro años para observar que el ritmo de crecimiento de las mismas que afectan a los Sistemas de Información ha sido prácticamente exponencial en este período de tiempo. De hecho, de estos intentos de ataques, un 20 por ciento se materializaron.

La nota más preocupante es que estas amenazas son cada vez más complejas y difíciles de detectar. Si antaño las técnicas de ataque estaban en manos de especialistas, ahora han pasado al gran público y el daño y la velocidad de los mismos se incrementan continuamente.

Dado el carácter de estas amenazas, se hace necesaria por tanto 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

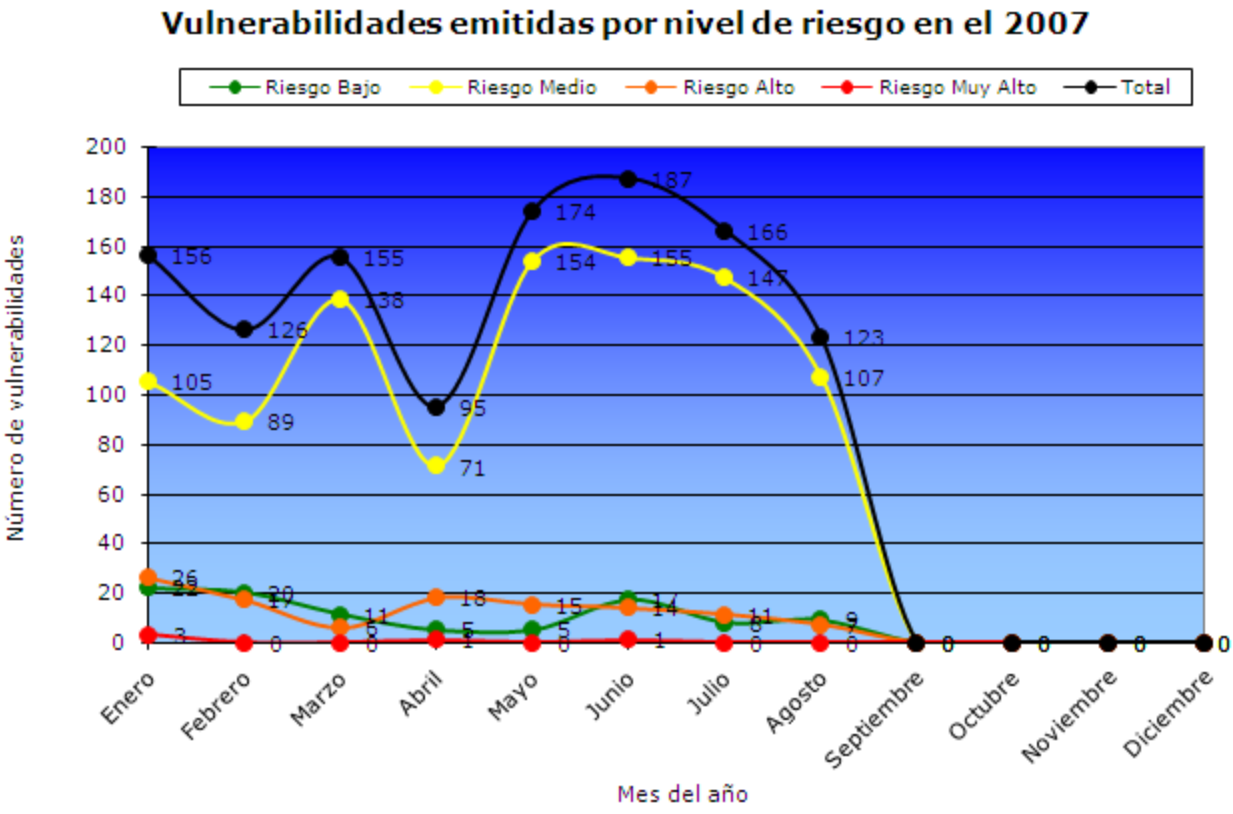
debe estar orientada a garantizar o mantener tres cualidades propias de esta última: disponibilidad, integridad y confidencialidad.

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 implementación 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.

Tampoco conviene olvidar que la Sociedad de la Información será segura o no será. Si los ciudadanos no perciben seguridad en el empleo de las Tecnologías de la Información, cualquier intento por conseguir su implantación universal y definitiva se verá abocado al fracaso. Así lo pone de manifiesto la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos que señala que la generalización del uso de las comunicaciones electrónicas "depende de la confianza y seguridad que genere en los ciudadanos" y, por supuesto, también de "los servicios que ofrezca".

Figura 4



Incluso la mejor infraestructura de seguridad de información no puede garantizar que una intrusión no acabe por afectar a un equipo. 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.

Por todo ello, si cualquier Administración presta un servicio que no genera confianza y seguridad, la posibilidad de incrementar la brecha digital se agranda, sobre todo entre aquellos colectivos más "desconfiados". Una desconfianza que nace de la percepción, muchas veces injustificada, de una mayor fragilidad de la información en soporte electrónico, de posibles riesgos de pérdida de privacidad y de la escasa transparencia de estas tecnologías. Asimismo, el incremento paulatino del número de amenazas y vulnerabilidades (ampliamente recogidas en los medios de comunicación) acrecienta esta percepción de "inseguridad" entre los ciudadanos.

La seguridad que brinda el CCN-CERT a todas las AAPP es un arma poderosa para eliminar esta posible barrera a la inclusión de todos los ciudadanos en el empleo de las tecnologías de la información.