# Tecnimap 2007 - TECNIMAP PREMIOS

| | |
|---|---|
| **Fecha Presentación :** | 28-SEPTIEMBRE-2007 |
| **Nº Candidatura :** | TPR-18/2007TG |

## Entidad

**Entidad :** CENTRO CRIPTOLOGICO NACIONAL

**Tipo Entidad :** Administración General del Estado

**Centro Directivo :** AVDA. PADRE HUIDOBRO KM 8,500

**Teléfono :** 913726629

**CIF :** S2800155J

## Datos Evaluación

### Nombre de la iniciativa o proyecto

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

### Antecedentes del proyecto

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, 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.
Asimismo, 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; 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.
Por último, 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. 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.
En este contexto, y teniendo en cuenta además, el continuo incremento de las amenazas y vulnerabilidades, se enmarca la constitución del CCN-CERT (presentado a principios de este 2007). El término CERT proviene de las siglas en inglés Computer Emergency Response Team.

### Objetivos Específicos

Contribuir la mejora del nivel de seguridad en los sistemas de información de las Administraciones Públicas españolas (general, autonómica y local) y afrontar de forma activa las nuevas amenazas a las que hoy en día están expuestos.
Convertirse en el centro de alerta nacional que coopere y ayude a todas las Administraciones a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir.
Divulgar y asesorar a todas las Administraciones en la implantación de medidas tecnológicas que mitiguen el riesgo de sufrir cualquier ataque.
Informar a las distintas Administraciones de las últimas vulnerabilidades y alertar de las nuevas amenazas.
Investigar, divulgar y formar sobre mejores prácticas sobre seguridad de la información entre todas las AAPP.
Brindar soporte ante incidentes mediante la prestación de servicios de apoyo técnico y coordinación.
Ofrecer información, formación y herramientas para que las distintas administraciones puedan desarrollar sus propios CERTs, permitiendo al CCN-CERT actuar de catalizador y coordinador de CERTs gubernamental, tal y como señala el Plan AVANZA.
Participar en los principales foros y organizaciones internacionales (Foro ABUSES, FIRST, TERENA, European Government CERTs Groups, entre otros) en los que se comparte información y se divulgan medidas tecnológicas con el fin de paliar el riesgo y ofrecer soluciones ante hipotéticos ataques informáticos. forma global.
Desarrollar planes de formación para los responsables TIC de las distintas Administraciones.

### Recursos empleados

La constitución, implantación y seguimiento del CCN-CERT ha contado y cuenta con la participación de recursos propios y externos. En este sentido, la organización del trabajo podría dividirse entre:
-Comité de coordinación: encargado de la gestión del proyecto, la coordinación técnica del Equipo y el seguimiento del nivel de servicios.
-Equipo Técnico y de Soporte: responsable de la definición y ejecución técnica de las tareas de consultoría, desarrollo, soporte, formación y comunicación.
De esta forma, y teniendo en cuenta que estamos ante un proyecto de continuidad en el tiempo, durante el primer ejercicio del proyecto (2007) se han destinado al mismo alrededor de un millón de euros. En cuanto a los recursos humanos, se ha contado con quince personas dedicadas al proyecto (entre responsables de proyecto, consultores, analistas, programadores y responsables de comunicación).

### Implementación

El Plan Director está implementado en su conjunto en un 90 por ciento.
-Servicios de Información:
1Dseño y desarrollo de la plataforma de servicios en Internet necesaria (hardware, software y comunicaciones) que soporta los servicios del CCN-CERT.

| | |
|---|---|
| **Fecha Presentación :** | 28-SEPTIEMBRE-2007 |
| **Nº Candidatura :** | TPR-18/2007TG |

2.Mantenimiento y actualización de los contenidos del Portal. 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. 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, pueden 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.
3.Mantenimiento y explotación segura de la Plataforma, realizando una gestión 24x7 de todo el sistema, en coordinación con el proveedor de la infraestructura.
4.Diseño y aprovisionamiento de los sistemas internos de información (back-office) en los que los expertos del Equipo de Respuesta realiza sus labores.
5.Puesta en marcha del laboratorio de investigación y respuesta ante incidentes.
-Plan de Comunicación y Promoción
1.Integración en Organismos Internacionales, tanto a nivel europeo (TERENA TF-CSIRT), como internacional (FIRST).
2.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).
3.Desarrollo de eventos periódicos de comunicación con la prensa.
4.Participación en eventos comerciales de interés.
5.Publicación y envío de estadísticas, noticias, boletines de vulnerabilidades y otros contenidos por feeds RSS.
-Desarrollo de Políticas y Procedimientos
1.Estudio del contexto normativo y regulatorio para el adecuado desarrollo de las políticas y procedimientos y los requerimientos del Servicio de Gestión de Incidentes.
2.Desarrollo de políticas.
3.Desarrollo de procedimientos operativos.
4.Auditoría y revisión periódica de las políticas y los procedimientos.
-Servicios de Gestión de Incidentes
1Desarrollo del Plan de Respuesta a Incidentes
2Diseño y desarrollo de procesos y procedimientos
3Implantación del servicio
4Soporte y mantenimiento del servicio
-Servicios de Formación
1Interna (mantenimiento de los conocimientos del equipo del CCN-CERT de forma continua)
2Formación continua para la Comunidad que permita sensibilizar y mejorar sus capacidades para la detección y gestión de incidentes.

## Resultados

Los resultados de este proyecto están íntimamente ligados a la implementación del CCN-CERT y a la 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 la Comunidad. Así, y en función de los servicios de implementación, encontramos los siguientes resultados:
1-Servicio de información: 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. Del mismo modo, el estudio de las amenazas y vulnerabilidades registradas por el CCN-CERT señala que 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%. 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).
2- Plan de Comunicación y Promoción:
-Acciones con la Comunidad:
Más de 200 noticias publicadas de seguridad TIC (nacionales e internacionales) en el Portal.
Labores de sensibilización e información: emisión de distintos Comunicados Oficiales enviados a medios de comunicación nacionales (generalistas y especializados).
Presentación a responsables TIC de la AGE, Comunidad de Madrid y Ayuntamientos (próximos encuentros en Andalucía, Cantabria y Asturias).
-Acciones con terceros
Rueda de prensa para presentar el proyecto (Difusión OJD: 25 millones de lectores).
Integración en Organismos Internacionales, en los que están presentes todos los CERTs Gubernamentales de nuestro entorno: Europa (TERENA TF-CSIRT) e Internacional (FIRST).
-Participación en eventos comerciales de interés
-Meeting CSIRTs con responsabilidad nacional
-Participación en el Congreso Internacional del FIRST celebrado en Sevilla
-Convenio de colaboración con INTECO para el impulso de los aspectos de seguridad dentro del desarrollo de la Sociedad de la Información, mediante el intercambio de información, formación especializada y el desarrollo de proyectos tecnológicos.
-Colaboración con distintos medios de comunicación en la elaboración de artículos y reportajes de sensibilización.
3 Desarrollo de Políticas y Procedimientos (información confidencial)
4 Gestión de Incidentes (información confidencial)
5 Formación:
1.Seminarios, conferencias y talleres de trabajo realizados tanto para el propio equipo CCN-CERT como para responsables TIC de la AGE.
2.A través de los denominados Cursos STIC se realiza una formación detallada al personal de la Administración especialista en el campo de la seguridad de las TIC, 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.

# Tecnimap 2007 - TECNIMAP PREMIOS

| | |
|---|---|
| **Fecha Presentación :** | 28-SEPTIEMBRE-2007 |
| **Nº Candidatura :** | TPR-18/2007TG |

## Aspectos de mejora de la comunicación

La aportación del CCN-CERT al uso de las comunicaciones electrónicas es fundamental desde el momento en el que dicho uso dependerá de la confianza y seguridad que se genere en los ciudadanos. Así, y tal y como señala la Ley 11/2007, de 22 de junio, el principal reto que tiene la implantación de las Tecnologías de la Información y las Comunicaciones en la sociedad en general, y en la Administración en particular, es la generación de la confianza suficiente que elimine o minimice los riesgos asociados a su utilización.
Para ello, conviene reseñar su labor en una doble vertiente:
Servicio a su Comunidad
A través del citado Plan de Comunicación, este proyecto facilita una comunicación constante entre el CCN-CERT y los responsables TIC de las distintas AAPP que actúan, a su vez, como ciudadanos y como nexo de unión entre el público general y la Administración.
La herramienta clave en este Plan es, sin lugar a dudas, el Portal (www.ccn-cert.cni.es), a través del cual se facilita la comunicación directa con los responsables TIC de las Administraciones (e incluso de los ciudadanos en general). Asimismo, y desde el área restringida del portal, se mantienen los contactos clave (teléfono/correo electrónico) entre el CCN-CERT y los responsables TIC, con el fin de actuar adecuada y rápidamente ante cualquier ataque que se pueda recibir durante las 24 horas de los 365 días del año. La cifra de 25.000 visitas y 600 usuarios registrados, en menos de ocho meses, son una prueba de la magnífica acogida de dicho Portal.
Servicio a los ciudadanos
Tienen acceso a una parte importante del Portal, centrada, sobre todo, en la sensibilización ante la seguridad en la información. Del mismo modo, y a través de las labores del CCN-CERT con los distintos medios de comunicación conocen de primera mano los esfuerzos de la Administración por mantener la seguridad de las comunicaciones y cuáles son las prácticas más recomendables para este objetivo.

## Aspectos de inclusión social

La seguridad en el empleo de nuevas tecnologías y la mejora de los sistemas de información de la Administración Electrónica son dos aspectos fundamentales que facilitan la inclusión social de los ciudadanos. Si un servicio no genera confianza y seguridad a los ciudadanos 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.
Por todo ello, 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.

## Aspectos de transformación del servicio

Tal y como recoge la LEY 11/2007, de 22 de junio, el tiempo actual tiene como uno de sus rasgos característicos la revolución que han supuesto las comunicaciones electrónicas. Por ello, una Administración a la altura de los tiempo en que actúa tiene que acompañar y promover en beneficio de los ciudadanos el uso de estas comunicaciones. No obstante, este uso, depende en gran medida de la confianza y seguridad que se genere en los ciudadanos. Por todo ello, 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.
Si en un primero paso, el principal objetivo fue crear los instrumentos y herramientas necesarios para desarrollar la Sociedad de la Información; la evolución y transformación del servicio creado paso inexorablemente por garantizar la seguridad de todas las (TIC).

## Aspectos de usabilidad,accesibilidad

La implementación del CCN-CERT se ha realizado a través de sistemas que permiten ofrecer todos sus servicios de manera segura y comprensible.
Tanto los desarrollos como la infraestructura de soporte son convenientemente securizados y auditados.

## Aspectos de confianza,seguriada y uso del edni

Confianza y seguridad son dos piezas claves en la misión del CCN-CERT. De hecho, el objetivo principal de este proyecto es contribuir a la mejora del nivel de seguridad de los sistemas de información en las AAPP de España, colaborando con todas ellas en el establecimiento de las medidas necesarias para ofrecer un servicio que genere confianza y, por lo tanto, sea verdaderamente útil a los ciudadanos, al tiempo que eficaz para los intereses nacionales.
De igual forma, su labor fundamental es ser el centro de alerta y respuesta de incidentes de seguridad, ayudando a las Administraciones a responder de forma más rápida y eficiente ante las amenazas de seguridad que afecten a sus sistemas de información.
Sensibilización, formación y divulgación de información y buenas prácticas de seguridad de la información son, por lo tanto, las herramientas claves de este proyecto de colaboración que pretende concienciar a toda la Administración en la necesidad de que la elaboración, conservación y utilización de determinada información se realice de forma segura. Para ello, las propias AAPP deben dotarse de los medios adecuados para la protección y control del acceso a dicha información, y han de regular unos procedimientos eficaces para su almacenamiento, procesamiento y transmisión seguros por medio de sistemas propios. En este sentido, el CCN-CERT cuenta con diversas herramientas puestas a disposición de todos los responsables TIC de las distintas administraciones:
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.
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.
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.
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.
En cuanto al uso del DNI electrónico, el CCN mantiene firmado un convenio de colaboración con INTECO para el desarrollo de la

| | |
|---|---|
| **Fecha Presentación :** | 28-SEPTIEMBRE-2007 |
| **Nº Candidatura :** | TPR-18/2007TG |

Sociedad de la Información y de los requisitos de seguridad de las aplicaciones que empleen el DNI electrónico. En virtud de dicho acuerdo, el CCN realizará labores de certificación de seguridad de los perfiles de protección del DNI para PC y TDT (Televisión Digital Terrestre) elaborados por dicho organismo.

## Aspectos de difusión del servicio

Desde un primer momento, el CCN-CERT ha sido consciente de la necesidad de difundir su servicio hasta alcanzar el reconocimiento y la confianza de su Comunidad (Administración General del Estado, autonómica y local), convirtiéndose en el punto de referencia en cuanto a seguridad se refiere. De igual forma, uno de sus objetivos ha sido, y es, lograr el mayor número de contactos dentro de dicha comunidad con los que mantener un comunicación directa y fluida, adquiriendo una una imagen reforzada en el tiempo, gracias a una periodicidad y frecuencia en las informaciones y una estrecha relación con los gabinetes de prensa de la Administración y los medios de comunicación especializados.
En este sentido, la labor de difusión del equipo hacia la comunidad se ha concretado en las siguientes iniciativas:
Portal/generación de contenidos:
1.Noticias generadas por el departamento de comunicación, así como aquellas seleccionadas entre distintas fuentes de información (prensa, gabinetes de prensa, empresas, organismos nacionales e internacionales...) relativas a la seguridad de la información/seguridad informática, ataques, Administración Pública, ciberseguridad, protección de datos, legislación, etc. Diariamente se genera una noticia que puede ser recibida a través de RSS.
2.Comunicados CCN-CERT: comunicados oficiales que permiten ofrecer una visión continua y pública de la actividad del CCN-CERT, con el fin último de alcanzar el reconocimiento y la confianza de la Comunidad. Con ello se persigue construir una imagen pública de la organización, a través de la frecuencia de estas notas que se dan de alta en el portal y, en algunos casos, se distribuyen entre los gabinetes de prensa de la Administración y los medios de comunicación de referencia (especializados en seguridad, informática y nuevas tecnologías).
Rueda de prensa inicial de presentación del proyecto.
Convocatoria: 46 medios de comunicación de ámbito nacional y 27 gabinetes de prensa de la AGE.
Difusión OJD: 25 millones de personas.
Plan de visitas (roadshow) a la Administración General del Estado, autonómica y local en donde se presenta el proyecto de forma detallada, favoreciendo el contacto directo con los responsables TIC de las distintas administraciones. Hasta el momento se han cursado más de 600 invitaciones a este tipo de actos, y se han realizado presentaciones ante los responsables TIC de la AGE en Madrid, Comunidad de Madrid y Ayuntamientos de la región. Próximamente se llevarán a cabo encuentros ante las comunidades de Andalucía, Asturias y Cantabria.
Elaboración de material de comunicación (trípticos, dossier de prensa, reportajes, etc.)
Presentación en distintas jornadas y congresos (VI Jornadas de Seguridad de la Información de la Defensa, Securmática, Consejo Superior de Administración Electrónica, Jornadas de sensibilización CCN, TECNIMAP 2007...)
Colaboración con distintos medios de comunicación en la elaboración de reportajes y artículos sobre el CCN-CERT y su papel en la seguridad de la información.
Participación en foros nacionales e internacionales:
ABUSES
TERENA Networking Conference
FIRST 19 th Annual Conference
ENISA
Reunión CERTs OTAN
Integración en Organismos Internacionales clave, en los que se echaba en falta la presencia de un CERT gubernamental español que compartiera objetivos, ideas e información sobre la seguridad de las informaciones de forma global:
Integración a nivel europeo (TERENA TF-CSIRT)
Integración a nivel internacional (FIRST)

## Aspectos de incremento de la participación ciudadana

La participación ciudadana en el proyecto se ha canalizado a través del Portal, herramienta de referencia del CCN-CERT. Así, a través de la página web www.ccn-cert.cni.es, los ciudadanos pueden recibir información actualizada diariamente sobre amenazas, vulnerabilidades, guías de configuración de las diferentes tecnologías o mejores prácticas de seguridad. 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.
Dado el incremento constante del número de visitas y del número de registrados, es probable que se concluya este año 2007 con alrededor de mil usuarios registrados en el Portal.

## Lecciones aprendidas y conclusiones

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.
Nadie duda, pues, 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. Unos sistemas que tienen ante sí una lista interminable de amenazas y potenciales delitos que les afectan y que pueden provenir de muy diferentes frentes: hackers, ciberdelincuentes, terroristas, mafias, servicios secretos, usuarios internos malintencionados o despistados, etc.
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, la premisa de la seguridad ha ido marcando las distintas disposiciones provenientes del poder Ejecutivo a la hora de legislar en materia de Tecnologías de la Información (Plan AVANZA, Ley 11/2007, R.D. 421/2004, etc) hasta concluir a principios de este año 2007 en la constitución del CCN-CERT, Equipo de Respuesta ante Incidentes de Seguridad de la Información para las Administraciones Públicas del Centro Criptológico Nacional.
La necesidad de este nuevo servicio queda patente al analizar las estadísticas de amenazas y vulnerabilidades registradas por este equipo. 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%.

| | |
|---|---|
| **Fecha Presentación :** | 28-SEPTIEMBRE-2007 |
| **Nº Candidatura :** | TPR-18/2007TG |

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 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 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.
Del mismo modo, resulta esencial la gestión de incidentes a través de CERTs dedicados a la implantación y gestión de medidas tecnológicas que prevengan, primero, y mitiguen, llegado el caso, el riesgo derivado de los ataques a los que están expuestos los sistemas.
La relación del CCN-CERT con el resto de la Administración será siempre de colaboración, y no se actuará nunca de forma jerárquica, salvo en el caso de información clasificada. Incluso, desde el CCN se ofrecerá información, formación y herramientas para que la comunidad pueda desarrollar sus propios CERTs, permitiendo al CCN-CERT actuar de catalizador y coordinador de CERTs gubernamental, tal y como señala el citado Plan AVANZA.

**Referencias y enlaces**

Las referencias y enlaces fundamentales para esta candidatura se ubican en los siguientes organismos y/o organizaciones:
CCN-CERT www.ccn-cert.cni.es
Centro Criptológico Nacional www.ccn.cni.es
Centro Nacional de Inteligencia www.cni.es
Foro Español de Equipos de Seguridad (ABUSES) www.rediris.es/abuses
European Network and Information Security Agency (ENISA) http://enisa.europa.eu/
Forum of Incident Response and Security Teams (FIRST) http://www.first.org
Instituto Nacional de Tecnologías de la Comunicación (INTECO) http://www.inteco.es
Task Force - Computer Security Incident Response Teams (TERENA TF-CSIRT) http://www.terena.org/activities/tf-csirt/

**Información complementaria**

## Responsables Proyecto

**Apellido 1 :** Jiménez **Apellido 2 :** **Nombre :** Luis
**Nif :** 50706439H **Telefono :** 913726629 **EMAIL :** info@ccn-cert.cni.es
**Puesto Trabajo :** Subdirector General Adjunto del CCN **Información SMS :** NO

**Personas que han intervenido en el proyecto**

Confidencial

**Observaciones**