Evaluación de la Seguridad de las TIC

DESCRIPCIÓN DE LAS AMENAZAS Y VULNERABILIDADES A QUE ESTÁN SOMETIDOS LOS SISTEMAS DE LAS TIC Y LAS MEDIDAS PARA CONTRARRESTARLAS EN EL CAMPO DE LA EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD TIC

Centro Criptológico Nacional
Centro Nacional de Inteligencia

El hecho de que gran parte de las actividades humanas sean cada vez más dependientes de las Tecnologías de la Información y las Comunicaciones (TIC) hace que la seguridad juegue un papel decisivo en cualquier organización que trabaje con sistemas de información.

La protección de los Sistemas de las Tecnologías de la Información y Comunicaciones (TIC) es una actividad crítica en la consecución de los objetivos de una Organización debido a la importancia que tiene la información que manejan dichos Sistemas.

Ante esta situación, y tal y como se recoge en la Ley 11/2002, el Centro Nacional de Inteligencia, tiene entre otras funciones (artículo 4), coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, así como garantizar la seguridad de las tecnologías de la información en ese ámbito. Esta seguridad viene a denominarse STIC; es decir, el conjunto de medidas de seguridad que se establecen, adoptan o implementan, para proteger la información, procesada, almacenada o transmitida por Sistemas TIC, contra la pérdida de **Confidencialidad** (propiedad por la que la información no está disponible o abierta a usuarios o procesos no autorizados), **Integridad** (propiedad de la información que indica que ésta no es objeto de manipulaciones no autorizadas) o **Disponibilidad** (estar accesible y ser utilizable al requerimiento de un usuario autorizado) ya sea accidental o intencionada, y para impedir la pérdida de la Integridad y Disponibilidad de los propios Sistemas.

> El factor humano suele ser el elemento más vulnerable con relación a la seguridad de los sistemas de información

Conviene asimismo recordar el significado de tres términos de gran importancia en este sentido: amenaza, vulnerabilidad y riesgo. El primero se refiere a cualquier circunstancia susceptible de lograr que la información o los sistemas que la soportan sufran una pérdida de confidencialidad, integridad o disponibilidad. La vulnerabilidad es la debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un activo del sistema, mientras que el riesgo sería la probabilidad de que la amenaza actúe sobre el activo. (Se utiliza para cuantificar el daño -probable- que puede causar la amenaza).

Pero, ¿quiénes son las fuentes de las amenazas actuales frente a la Seguridad TIC? En líneas generales podríamos decir que éstas pueden provenir de servicios de inteligencia, grupos organizados, terroristas, *hackers*, grupos criminales o usuarios internos.

Estas amenazas, además, se pueden manifestar en varios puntos: sistemas de comunicación, en las radiaciones o con software dañino (virus, malware o todo tipo de software malicioso) con un código ejecutable (que dispone, al menos, de un mecanismo de reproducción y una "carga útil") y que puede

disponer, además, de mecanismos de activación y enmascaramiento (troyanos, bombas lógicas, *spam, phishing, farming*, etc.).

En cuanto a los resultados que pueden generar estas amenazas se encuentran: daños físicos; robo, pérdida, destrucción o extracción de dispositivos de almacenamiento; destrucción o modificación de los datos almacenados; encaminamiento de la información a receptores erróneos o interceptación de datos mientras se procesan.

No hay que olvidar tampoco la importancia del factor humano. De hecho, suele ser el elemento más vulnerable con relación a la seguridad de los sistemas de información. Así, podría decir que el *hacker* "amateur" atacaría directamente a un sistema, mientras que el "profesional" aprovecharía las vulnerabilidades que presenta la persona.

Evaluación de la Seguridad

Así pues, la seguridad de la información se asienta en seis grandes pilares: formación, políticas, procedimientos, herramientas, valoración (acreditación) y evaluación (certificación). Esta evaluación, en la que nos vamos a centrar a partir de ahora, es el proceso en el que se contrasta la seguridad de un producto de TI que, con su documentación (manuales de uso/administración), constituye el objeto de evaluación o TOE (*Target Of Evaluation*).

> El ámbito de actuación del Organismo de Certificación comprende, tanto a las entidades públicas como a las privadas

En esta evaluación se distinguen tres apartados: criterios (qué se evalúa), metodología (cómo se evalúa) y esquema (cómo se organiza la evaluación). En el primero de los casos, en los criterios de evaluación, existen tres tipos principales: **criptológica** (evaluación cripto), **radiaciones** (evaluación Tempest) y **funcionales** (evaluación ITSEC y evaluación CC).

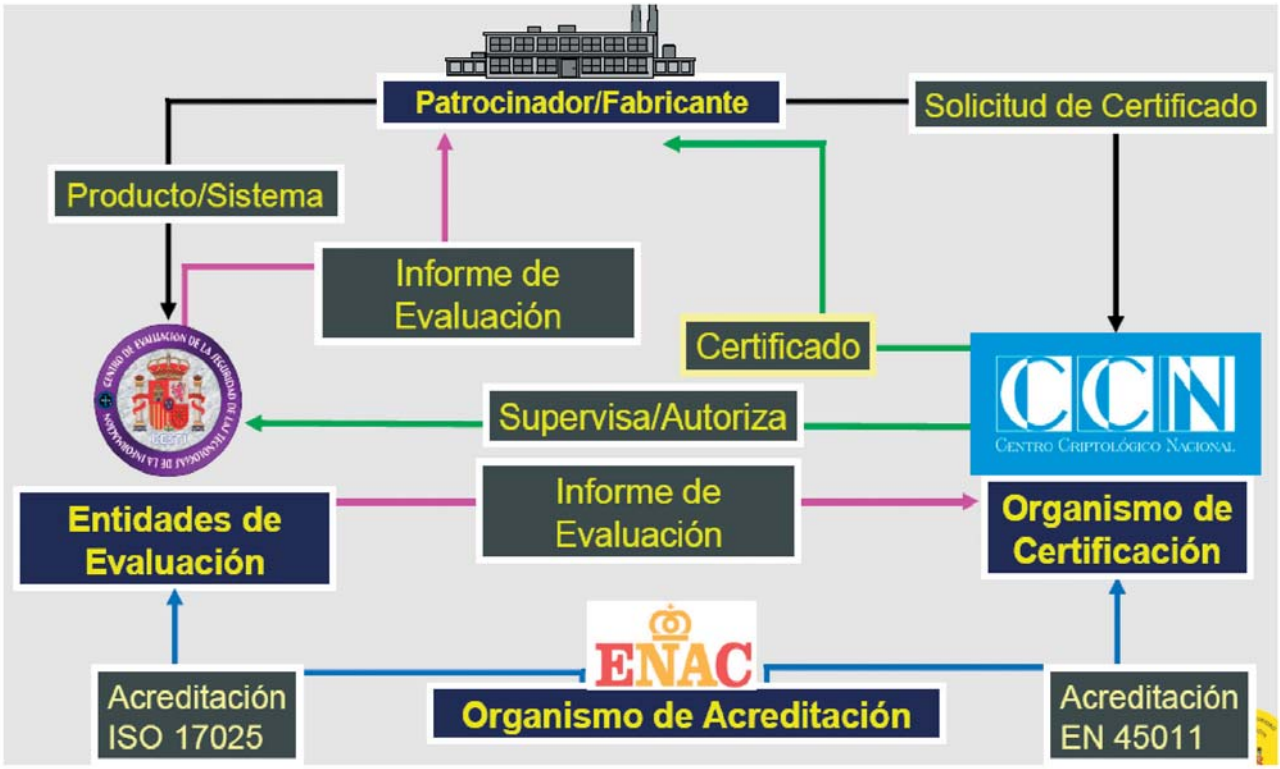
La necesidad de conocer el nivel de seguridad de un producto TIC es tan legítima como la propia necesidad de seguridad. Todo ello debido a que, evidentemente, nunca se puede determinar la seguridad de un producto al cien por cien; aunque sí se pueden determinar grados de confianza en la seguridad de un producto viendo si se ha seguido una metodología de desarrollo o buscando en él vulnerabilidades explotables.

Así pues, el objetivo de la evaluación funcional es adquirir la confianza de que el producto evaluado proporciona las características de seguridad que proclama tener en su **Declaración de Seguridad**, mediante el examen detallado del sistema o producto (objeto a evaluar -TOE-) con el fin de encontrar posibles vulnerabilidades y confirmar el nivel de seguridad establecido.

Los criterios de evaluación funcional se definen como un conjunto de especificaciones funcionales de seguridad y una metodología de evaluación de la seguridad de los productos TIC. Deben contar con dos aspectos clave: **corrección** (las funciones y mecanismos de seguridad están adecuadamente implementados) y **efectividad** (las funciones y mecanismos de seguridad implementados sirven para oponerse a una amenaza y satisfacer un objetivo de seguridad).

En este sentido, conviene reseñar la existencia del Acuerdo de Reconocimiento Mutuo de Certificados *Common Criteria*, del que es signatario el Ministerio de Administraciones Públicas, en representación de la Administración española, y que está reconocido por más de 24 países. A través de este acuerdo se realizan comparaciones de

FUNCIONAMIENTO DEL ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN



evaluaciones independientes, reconocimiento mutuo de los resultados de una evaluación, guías para desarrollar productos TI seguros y una guía para adquirir/solicitar productos seguros.

Common Criteria

Certificación

Como ya hemos señalado, un certificado es la determinación positiva de que un producto tiene capacidad para proteger la información hasta un nivel de seguridad. En España, el marco regulador en el que se realiza la actividad de evaluación y certificación es el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI), del Centro Criptológico Nacional, CCN. Este Organismo se rige por lo dispuesto respectivamente en la **Ley 11/2002, de 6 de mayo**, reguladora del Centro Nacional de Inteligencia, y el **Real Decreto 421/2004, de 12 de marzo**, por el que se regula el Centro Criptológico Nacional, así como la Orden PRE/2740/2007, por la que se aprobó, el 19 de septiembre, el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

> Se pueden determinar grados de confianza en la seguridad de un producto viendo si se ha seguido una metodología de desarrollo o buscando en él vulnerabilidades explotables

Entre otros objetivos, el OC presta los servicios de certificación de la seguridad y soporte a la normalización de la seguridad del DNI-e, de sus aplicaciones y de su sistema de expedición. Su ámbito de actuación comprende a las entidades públicas o privadas que quieran ejercer de laboratorios de evaluación de la seguridad de las TI en el marco del Esquema, y a las entidades públicas o privadas fabricantes de productos o sistemas de TI que quieran certificar la seguridad de dichos productos en el marco del Esquema y cuando dichos productos o sistemas sean susceptibles de ser incluidos en el ámbito de actuación del CCN.