tecnimap Murcia 2004

24

CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Jaime Gotor
Subdirector General Adjunto
Centro Criptológico Nacional

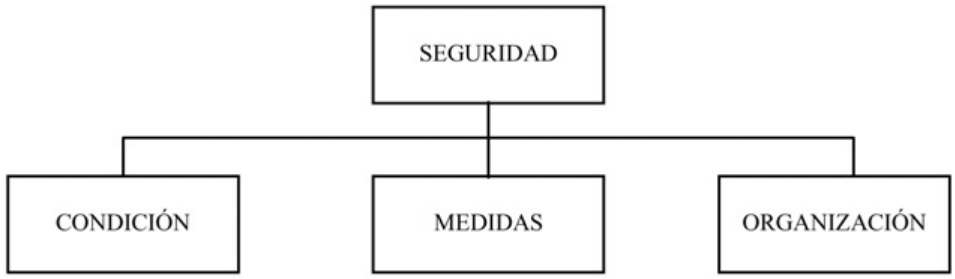
Luis Jiménez
Unidad de Políticas de Seguridad de las TI
Centro Criptológico Nacional

1. LA SEGURIDAD

El concepto de Seguridad de las Tecnologías de la Información deriva del concepto de Seguridad.

Es generalmente aceptado que el término "seguridad" tiene tres significados o acepciones:

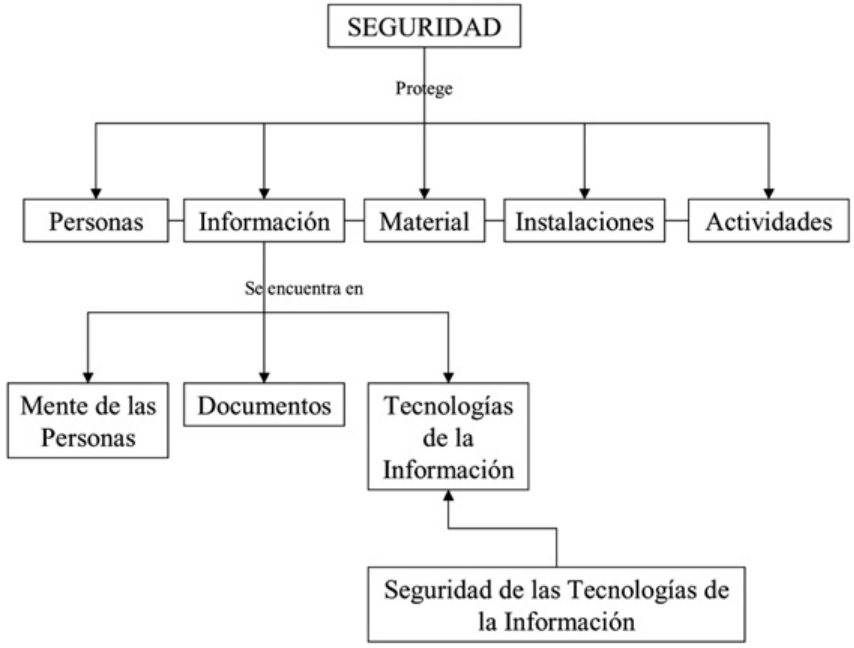
- seguridad como **condición** alcanzada por una entidad cuando es protegida.
- seguridad como **conjunto de medidas** para proteger entidades.
- seguridad como **organización** responsable de proporcionar dicha condición.



Dentro de la protección genérica de entidades, es generalmente aceptado que el objetivo de la seguridad es proteger los recursos (personal, información, material, instalaciones) y las actividades.

Según sea el recurso a proteger se utilizan los términos de seguridad del personal, seguridad de la información, seguridad del material, seguridad de las instalaciones, y seguridad de las actividades u operaciones.

Cuando se trata de proteger la información, a la hora de aplicar las medidas de seguridad, controles o salvaguardas se debe tener en cuenta que la información puede existir en la mente humana, en un documento, o en forma electrónica en un sistema de tecnologías de la información. Por tanto, según quien posea, o según donde resida, la información se utilizan los términos de seguridad del personal, seguridad de la documentación, y seguridad de la información en forma electrónica o Seguridad de las Tecnologías de la Información.



Así pues, en un primer análisis nos encontramos con que el término seguridad del personal tiene dos acepciones:

- protección de las personas (su integridad física).
- protección de la información que conocen las personas mediante medidas de seguridad aplicadas a las personas (determinar su confiabilidad, autorizarlas, habilitarlas, determinar su necesidad de conocer, su formación, etc.).

En relación a la protección de la información cuando reside en un "documento" ha de entenderse el término documento en su sentido más amplio, esto es, "soporte que contiene información", y por tanto la seguridad documental o de la documentación trata aquellas medidas aplicadas a los documentos tales como precintos, sellos, etiquetas, marcas de agua, sobres, contenedores, armarios de seguridad, cajas fuertes, etc.

Por último, la seguridad, entendida como conjunto de medidas destinadas a proteger a algo o a alguien, puede denominarse según la naturaleza de dichas medidas en seguridad física, seguridad de procedimiento o administrativa, y seguridad técnica, cuando las medidas son de naturaleza física, de procedimiento, o técnica respectivamente.

2. LA SEGURIDAD DE LA INFORMACIÓN

Es de sobra conocido que vivimos en la era de la información. Este hecho tiene unas connotaciones inmediatas que también son conocidas universalmente. La primera de ellas es que en la sociedad actual la información tiene un gran valor. Es más, en muchas ocasiones la información es el propio "valor" o, al menos, la información es el valor que marca la diferencia. Como

tal elemento de valor, la información se genera, se compra, se vende, se utiliza y se consume, y toda esa actividad genera ingentes movimientos económicos y de intereses.

Muchas empresas y organizaciones sólo gestionan y negocian con información. Para ellas, la información es el único activo y, por lo tanto, el más valioso. Los propietarios de la información o los responsables de su custodia deben ser conscientes de esta realidad y exigir un tratamiento adecuado a la información, incluyendo su seguridad. Lamentablemente, en algunos casos se pueden encontrar entidades donde el propietario de la información no es plenamente consciente de todos los aspectos que abarca esa responsabilidad.

Como tal elemento de valor, la información debe ser custodiada con el máximo cuidado porque, sin lugar a duda, será deseada y buscada por personas y entidades que no son sus legítimos propietarios. En otras palabras, al ser las diferentes informaciones elementos valiosos que son apetecidos por terceros, decimos que la información está sometida a amenazas.

Por otra parte, en la Sociedad de la Información en la que vivimos, la inmensa mayor parte de la información que es gestionada se transmite, se procesa o se almacena (se maneja) en algún momento en un sistema de información o telecomunicaciones. Estos sistemas de información y comunicaciones reciben las denominaciones de Sistemas de Tecnologías de la Información (TI) y Sistemas de Tecnologías de la Información y de las Comunicaciones (TIC).

Desde hace años hemos conocido la coincidencia de las dos realidades que hemos mencionado: la necesidad de la información y su manejo por los sistemas. En este escenario, muchos expertos señalan que es en los primeros años 90 cuando la rapidez para disponer de la información y su exactitud se convierten en los elementos imprescindibles para la toma de las decisiones que hacen triunfar o fracasar a un negocio.

A partir de esa fecha, la supervivencia para muchas organizaciones depende exclusivamente de que su información, además de ser buena, mantenga las características de confidencialidad, integridad y disponibilidad y que los sistemas que manejan esa información también mantengan siempre su integridad y su disponibilidad.

Para garantizar que la información posee y mantiene esas características tiene que ser adecuadamente protegida. La protección tiene que evitar que la información y los sistemas pierdan las características mencionadas, ya sea por causas accidentales o intencionadas.

Las empresas y organizaciones deben ser conocedoras de esta realidad y cuidar con enorme celo a esos sistemas. Sin embargo, los sistemas de información, aunque están cada vez más presentes en muchas facetas de nuestra vida, son unos grandes desconocidos. El paso del tiempo no hace más que aumentar su presencia y nuestro desconocimiento sobre ellos.

Podemos concluir que hoy en día, la información es un recurso, algunas veces crítico, que debe ser protegido de manera que se garantice su confidencialidad, integridad y disponibilidad, a lo largo de toda su existencia, con independencia del medio, soporte o formato en el que la información permanezca. Además debe garantizarse la integridad y disponibilidad de los servicios y recursos que sustentan dicha información.

Por ello, estamos asistiendo a la aparición de un nuevo ámbito de trabajo en las organizaciones, al cual la Administración tampoco es ajeno, que trata todas aquellas actividades para proporcionar seguridad a la información y para gestionar dichas actividades. Es una nueva cultura de la seguridad de la información en las organizaciones, para la cual están apareciendo nuevos

estándares y códigos de buenas prácticas tales como la norma UNE-ISO 17799:2002 "Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información"; y la norma UNE 71502 "Especificaciones para los Sistemas de Gestión de la Seguridad de la Información".

3. LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Ya se ha señalado que los productos y sistemas de TI deben llevar a cabo sus funciones ejerciendo un control apropiado de la información que manejan para asegurar su protección contra sucesos como revelación no deseada, modificación o pérdida disponibilidad. El término seguridad de TI se utiliza generalmente para referirse tanto a la prevención como a la reducción de este tipo de sucesos.

Por ello, podemos definir la seguridad de las Tecnologías de la Información como la capacidad de las propias TI para evitar, hasta un determinado nivel de confianza, el compromiso de la confidencialidad, integridad y disponibilidad de la información que procesan, almacenan o transmiten (manejan) los sistemas y la integridad y disponibilidad de los propios sistemas.

Un análisis de esta definición nos permite sacar las siguientes conclusiones sobre el alcance de las medidas de seguridad de las TI:

- La Seguridad de las TI agrupa al conjunto de medidas de seguridad (controles, salvaguardas, servicios o funciones, y mecanismos) para proteger la información almacenada, procesada o transmitida (manejada), por productos o sistemas de las tecnologías de la información.
- La Seguridad de las TI también incluye a aquellas medidas que permiten la detección, documentación y contabilidad de las amenazas a la información y a los sistemas, de manera que no sólo se permita detectar los ataques sino también oponerse activamente o, en último caso, recuperarse de ellos.
- De acuerdo con todo lo anterior, la STI abarca los productos o sistemas de tecnologías de la información utilizados en los sistemas de comunicaciones, en los sistemas de información. También se incluyen otro tipo de sistemas electrónicos (como por ejemplo sensores, equipos de medida, sistemas de identificación, de navegación, etc.) que manejan información muy específica.
- La Seguridad de las TI puede conseguirse protegiendo adecuadamente cada uno de los recursos componentes de la configuración de los sistemas de información y comunicaciones.

La seguridad de los productos y sistemas de TI por afectar y preocupar a diversos sectores de la sociedad dispone de una amplia oferta de soluciones. Sin embargo, lo que es difícil realmente es saber si las soluciones de seguridad que existen son adecuadas. Pocas personas o entidades tienen la posibilidad de llegar a valorar la calidad de un sistema de seguridad. De la misma forma que los sistemas que manejan la información, los productos y sistemas de seguridad se han convertido en elementos populares pero, en general, no se conoce gran cosa de su composición ni de su fiabilidad.

4. EVALUACIÓN, CERTIFICACIÓN, VALORACIÓN Y ACREDITACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Muchos usuarios de TI carecen del conocimiento, experiencia y, sobre todo, de los medios necesarios para juzgar si su confianza en la seguridad de los productos o sistemas de TI es justificada y pueden no querer confiar sólo en las afirmaciones de los fabricantes. Los usuarios necesitan cada vez mas incrementar su confianza en las propiedades de seguridad de un producto o sistema de TI ordenando un análisis de su seguridad, es decir, una Evaluación de Seguridad.

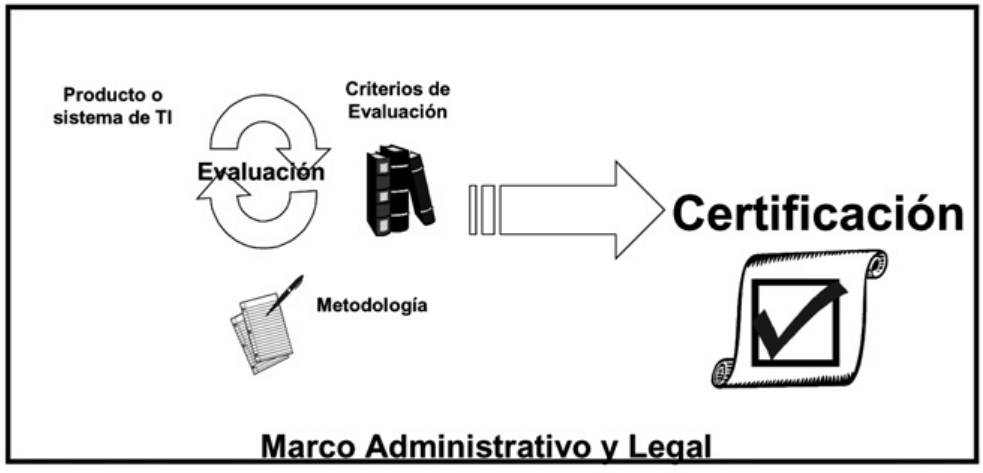
Una Evaluación de la Seguridad de las TI, es un análisis, realizado mediante un proceso metodológico, de la capacidad de un producto o sistema de las tecnologías de la información para proteger las condiciones de la información de acuerdo a unos criterios establecidos, todo ello con objeto de determinar si puede ser certificado.

Una Certificación de la Seguridad de las TI es la determinación, realizada mediante un proceso metodológico, de la capacidad de un producto o sistema de las tecnologías de la información para proteger en profundidad las condiciones de la información de acuerdo a unos criterios preestablecidos.

En este ámbito, se pueden distinguir cuatro tipos de certificaciones:

- Certificación de la Seguridad funcional de las TI
- Certificación de la Seguridad Criptológica
- Certificación de la Seguridad de Emanaciones (TEMPEST)
- Certificación de la Seguridad Física de los propios productos de seguridad de las TI.

La Certificación de la Seguridad de un producto o sistema de TI podrá requerir, dependiendo de la finalidad del propio producto, la obtención de una o varias certificaciones. Aquellos productos que deban ser certificados y no incluyan componentes criptológicas entre sus elementos, no requerirán la obtención de la certificación de la seguridad criptológica. Sin embargo, los productos que incluyan componentes criptológicas deberán obtener ambos certificados y en el orden correlativo en el que se han relacionado. En los casos que se considere necesario, la certificación de la Seguridad de Emanaciones es requerida de forma explícita independientemente de las otras certificaciones.



Por Valoración de la Seguridad de las TI se entiende el análisis de las características de un sistema para resistir, hasta un determinado nivel de confianza, accidentes o acciones maliciosas que pueden comprometer la confidencialidad, integridad, autenticidad y disponibilidad de la información que manejan, almacenan, procesan o transmiten, y la integridad y disponibilidad de los propios sistemas, todo ello con objeto de determinar si ese sistema puede ser acreditado.

La Acreditación de la Seguridad de las TI es la determinación de la capacidad de los sistemas de información y comunicaciones para resistir, hasta un determinado nivel de confianza, accidentes o acciones maliciosas que puedan comprometer la confidencialidad, integridad, autenticidad y disponibilidad de la información que manejan, almacenan, procesan o transmiten, y la integridad y disponibilidad de los propios sistemas.

Esa determinación es la que realmente proporciona confianza al propietario de la información, y se hace en base a la adecuada integración de productos y subsistemas, en algunos casos certificados, correctamente configurados. En general, la acreditación de la seguridad de las TI es el último proceso que se exige a un sistema para que maneje un determinado tipo de información.

Como se ha visto, en el mundo de la seguridad de las TI tiene un gran interés el poseer la capacidad técnica de garantizar que un producto o sistema, que va a manejar información, dispone de determinadas características de seguridad. De forma muy similar, por estar relacionada con lo anterior, también es apreciada la capacidad técnica para discernir si un sistema está configurado de forma que puede manejar de forma segura la información. En definitiva, la posesión de estas capacidades técnicas proporciona la posibilidad de determinar cuales son realmente los productos de seguridad adecuados.

Algunos países avanzados han sabido apreciar desde hace tiempo estos tipos de capacidades técnicas y se han esforzado en obtenerlas. Para ello se han dotado de recursos humanos y han adquirido conocimiento en esa materia. Una vez adquiridas estas capacidades técnicas, se está en

condiciones de valorar con conocimiento de causa si un determinado producto es capaz de evitar algunos de los riesgos a los que está sometida la información. Si el producto merece una valoración positiva, se expide un certificado que determina muy claramente los extremos que abarca la protección que proporciona el producto.

De la misma forma, determinadas organizaciones, principalmente supranacionales, obtienen o se interesan por estas capacidades técnicas. En unos casos, el papel de estas organizaciones internacionales consiste en alcanzar la propia capacidad técnica y expedir certificados de seguridad de productos que son reconocidos por varios países. De esta forma, un grupo de países que normalmente forman parte de esa organización internacional, y que comparten una política de seguridad común, disponen de productos con una contrastada calidad de seguridad. Organizaciones que utilizan y exigen esta forma de trabajo son el Consejo de Europa y la OTAN.

En otros casos, las organizaciones internacionales delegan en los estados miembros la responsabilidad de garantizar la seguridad de sus productos. Lógicamente, únicamente los estados que tengan esa capacidad técnica podrán optar a la posibilidad de satisfacer la petición de la organización. La UE es un ejemplo de una organización internacional que trabaja apoyándose en las capacidades técnicas de sus miembros.

5. ESTÁNDARES DE REFERENCIA PARA LA CERTIFICACIÓN

Certificación de la Seguridad Funcional de las TI

Los estándares de referencia para la evaluación funcional de la seguridad de las TI son:

- ITSEC Information Technology Security Evaluation Criteria, Office for Official Publications of the European Communities.
- ISO/IEC 15408 Evaluation Criteria for IT Security.
- Common Criteria(CC)/Common Evaluation Methodology (CEM).

La Norma Internacional de los Criterios Comunes o CC [Common Criteria] ISO/IEC 15408, tiene como finalidad ser la base para la evaluación de las propiedades de seguridad de los productos y sistemas de Tecnología de la Información.

Los Criterios Comunes permiten la comparación entre los resultados de evaluaciones de seguridad independientes, al proporcionar un conjunto común de requisitos para la funciones de seguridad de los productos y sistemas de TI y para las medidas de garantía (assurance) aplicadas a éstos durante la evaluación de seguridad. El proceso de evaluación establece un nivel de confianza del grado en que las funciones de seguridad de tales productos y sistemas y las medidas de garantía aplicadas coinciden con aquellos requisitos. Los resultados de la evaluación pueden ayudar a los usuarios a determinar si el producto o sistema de TI es suficientemente seguro para la aplicación pretendida y si los riesgos de seguridad implícitos en su uso son aceptables.

Los Criterios Comunes también son útiles como guía para el desarrollo de productos o sistemas con funciones de seguridad de TI y para la adquisición de productos y sistemas comerciales con dichas funciones. Durante la evaluación, el producto o sistema de TI es conocido como el Objeto de Evaluación o TOE [Target Of Evaluation]. Este TOE incluye, por ejemplo, sistemas operativos, redes de ordenadores, sistemas distribuidos y aplicaciones.

Los Criterios Comunes son de aplicación a las medidas de seguridad de TI implementadas en hardware, firmware o software. En este sentido, algunos aspectos, bien porque involucran técnicas especializadas o bien porque son, de alguna manera, adyacentes a la seguridad de TI, son considerados ajenos a la finalidad de los Criterios Comunes. Entre estos aspectos cabe destacar los siguientes:

a) Los Criterios Comunes no contienen criterios de evaluación de la seguridad correspondientes a medidas de seguridad de tipo administrativo o de procedimiento no relacionadas directamente con las medidas de seguridad de TI.
b) La evaluación de los aspectos técnicos de seguridad física de las tecnologías de la información, tales como el control de radiaciones electromagnéticas no se trata específicamente, aunque varios de los conceptos tratados son de aplicación en este área.
c) Los Criterios Comunes no tratan ni la metodología de evaluación ni el marco administrativo y legal –El Esquema de Evaluación y Certificación- bajo el cual los criterios pueden ser aplicados por las autoridades de evaluación. Sin embargo, se supone que los Criterios Comunes serán usados para propósitos de evaluación en el contexto de un determinado marco y con una determinada metodología.
d) Los procedimientos para el uso de los resultados de la evaluación en la acreditación –aprobación de seguridad- de productos o sistemas están fuera del objetivo de los Criterios Comunes. La evaluación, por el contrario, se centra en las partes tecnológicas de seguridad del producto o sistema y en aquellas partes del entorno operativo que pueden afectar directamente al uso seguro de los elementos tecnológicos. Los resultados del proceso de evaluación son, por lo tanto, un dato de valor para el proceso de acreditación.
e) Los criterios para la valoración de las cualidades inherentes de los algoritmos criptográficos no se tratan en los Criterios Comunes. Si se necesita una valoración independiente de las propiedades matemáticas de la criptografía de un producto o sistema de TI, deberá ser proporcionada por el Esquema de Evaluación y Certificación bajo el cual se están aplicando los Criterios Comunes.

Los Criterios Comunes constituyen un punto de encuentro y de consenso científico, técnico, comercial y gubernamental, para la evaluación y certificación de la seguridad de las tecnologías de la información.

Más de 30 países del mundo han adoptado los Criterios Comunes, y 13 de ellos (incluido ESPAÑA a través del Consejo Superior de Informática) firmaron en mayo de 2000, un Arreglo de Reconocimiento Mutuo (ARM) (CCRA) de los certificados expedidos por aquellos países que disponen de Esquema de Evaluación y Certificación reconocido en dicho Arreglo. Es cada vez mas una realidad incuestionable que el establecimiento de un Esquema de Evaluación reconocido por los diferentes países en el marco del CCRA, y la adopción de los Criterios Comunes por parte de dicho Esquema, se convertirá en un futuro próximo en una condición "sine qua non" para que la industria de las TI pueda participar en programas internacionales en condiciones de competitividad.

En muchos casos, se utilizan normas específicas para una determinada finalidad que emanan de los Criterios Comunes. Es el caso de las normas requeridas por el Ministerio de Industria, Comercio y Turismo en la Ley de Firma Electrónica.

Certificación de la Seguridad Criptológica

La certificación de la Seguridad Criptológica determina la capacidad de un sistema de cifra para proteger la información con el nivel de seguridad adecuado en todo momento de su vida útil. Esta certificación incluye verificar que el sistema de cifra implementa un algoritmo de cifra de robustez contrastada, que se manejan claves de calidad adecuada, que el sistema maneja correctamente el algoritmo y las claves y que el sistema mantendrá estas características durante toda su vida útil. Por diversas razones es una tarea compleja verificar todos los extremos mencionados. Además, para hacerlo mas difícil existe muy poca cooperación entre países sobre esta materia. Se considera que es demasiado sensible compartir conocimientos sobre este particular.

Certificación de la Seguridad de Emanaciones (TEMPEST)

La certificación de la Seguridad de Emanaciones determina la capacidad de un producto o sistema de TI de proteger la información que maneja contra la amenaza que supone la captación de la emanaciones electromagnéticas que cualquier producto de TI emite de forma involuntaria en su normal funcionamiento. Esta certificación supone verificar que las emanaciones del producto o sistema de TI están dentro de unos márgenes de seguridad establecidos en los criterios o normas de evaluación, y además que el entorno físico donde el producto o sistema es instalado ofrece una atenuación de dicha emanación también dentro de unos márgenes de seguridad.

En general los criterios que se utilizan para realizar la evaluación de este aspecto específico de la seguridad de las TI son normas que pero tienen una clasificación de seguridad y solo están disponibles para las personas legalmente habilitadas a consultarlas.

Certificación de la Seguridad Física de productos de TI

La certificación de la seguridad Física de los productos de las TI proporciona la evidencias necesarias sobre la seguridad del diseño e implementación hardware de los mecanismos de seguridad de un producto o sistema de TI.

Dichas evidencias son fundamentales para garantizar la integridad de los mecanismos de seguridad, pilar clave en todo el edificio de seguridad asociado a un producto o sistema de TI.

Uno de los estándares de referencia para llevar a cabo la evaluación de este aspecto específico de la STI es la norma americana FIPS Pub. 140-2 (ó ISO 19790 -en desarrollo).

Otras Certificaciones

Existen además otras certificaciones posibles, no relacionadas directamente con la seguridad de las TI, pero sí con la seguridad de la información.

Estas certificaciones se basan en los siguientes estándares:

La norma UNE-ISO/IEC 17799 Código de Buenas Prácticas para la Gestión de la Seguridad de la Información es un conjunto de recomendaciones para gestionar la "seguridad de la información" que trata de proporcionar una base común para "desarrollar normas".

La certificación ISO 17799 supone que la Organización en cuestión establezca y mantenga, al menos, diez controles perfectamente documentados:

- Política de seguridad de la información.
- Asignación de responsabilidades y responsables de la seguridad de la información.

- Programas de formación y sensibilización, entrenamiento del personal respecto a la seguridad de la información.
- Registro de incidentes con respecto a la seguridad.
- Controles de virus informáticos.
- Planes de contingencia para la continuidad de la actividad de la Organización.
- Control de los programas informáticos protegidos por derechos de propiedad.
- Protección de datos personales.
- Conformidad de todas las áreas de la organización respecto de la Política de seguridad y los requisitos legales que sean de aplicación.

Las normas UNE 71501 (Guía para la Gestión de la Seguridad de las TI) y UNE 71502 (Especificaciones para los Sistemas de Gestión de la Seguridad de la Información) también son del ámbito de la seguridad de la información

6. SITUACIÓN DE LA ACREDITACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TI EN LA ADMINISTRACIÓN

Finalmente, cabe hacer una breve valoración de la capacidad técnica en España para garantizar la seguridad de las Tecnologías de la Información y, paralelamente, del uso en nuestro país de la capacidad que se posee.

Cabe decir, que España tiene razonablemente buenas capacidades técnicas en los aspectos mencionados: evaluación Common Criteria de la seguridad, evaluación y certificación de la seguridad criptológica, evaluación y certificación de la seguridad de emisiones y valoración y acreditación de la STI

Básicamente, estas capacidades técnicas se concentran en el INTA, la primera de ellas, y en el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI) el resto.

Sin embargo, la aplicación de estas capacidades y el uso del beneficio que pueden y deben generar en nuestro país no es tan amplio como sería deseable. Las razones de esta baja implantación obedecen a diversas causas. Principalmente se pueden apuntar, a modo de comentario, las siguientes causas:

- Uso reducido de sistemas de manejo de información corporativa sensible en los niveles altos de la Administración y de las empresas.
- Pequeña conciencia de la necesidad de garantizar la seguridad de los productos y sistemas de TI para el manejo de la información.
- En general, escaso nivel de formación técnica de seguridad, principalmente en política y organización de la seguridad.
- Escasa participación en actividades conjuntas con países que exigen la aplicación rigurosa de medidas de seguridad en las TI.
- No disponer de una normas nacionales adaptadas al manejo de la información clasificada nacional y sensible en sistemas de información seguros.
- Desconocimiento de los compromisos que adquiere nuestro país, y que deberá seguir adquiriendo en el futuro, de protección de información suministrada por otros países, organizaciones y empresas.

Posiblemente, muchas de las causas enunciadas pueden tener su origen en una escasa conciencia del valor de la información o de los requisitos establecidos para su manejo. Si el propietario de la información no la llega a considerar como un activo, o como el activo, de valor singular de su organización será difícil que su tratamiento se estructure de una forma adecuada y, finalmente, los sistemas de las TI que manejan la información incorporen medidas de seguridad adecuadas. La misma situación se produce si no se identifica claramente en toda organización a la persona responsable de proporcionar a la información las medidas legal o normativamente exigidas. En esencia, lo que puede estar ocurriendo es que los propietarios o los responsables de la información no exigen o no impulsan la adopción de las medidas de seguridad adecuadas. En algunos casos, lo que puede faltar en realidad es la propia identificación del responsable, o incluso del propietario, de la información en la organización.

En determinadas organizaciones que la información no es amparada por su propietario, si el responsable de seguridad de los sistemas de las TI, por su conocimiento o su concienciación, propone o implementa medidas de seguridad, puede llegar a ser considerado como alguien que "pone pegas" a la libre circulación de la información y hace complejos, y costosos, a los sistemas.

Para finalizar, la conclusión última es apuntar que España debe hacer un esfuerzo en conocer y adoptar sistemas acreditados y productos certificados para manejar la información valiosa de la Administración o que requiere medidas de protección legalmente establecidas. Hay que recordar que este esfuerzo debe ser exigido e impulsado por los propietarios y los responsables de la propia información.