Título: EL ARREGLO DE CERTIFICACIÓN DE CRITERIOS COMUNES DE LA SEGURIDAD DE LA TECNOLOGÍA DE LA INFORMACIÓN

Autor: Francisco López Crespo, Jefe del Área de Sistemas Telemáticos de la Subdirección General de Coordinación de Recursos Tecnológicos de la Administración General del Estado. Ministerio de Administraciones Públicas.

Resumen: Se presenta el estado de situación del Reconocimiento internacional de los Certificados de Seguridad de la Tecnología de la Información.

Biografía: Licenciado en Ciencias Físicas y M.A. en Administración Pública. Secretario del GTA (Grupo de Usuarios de Telecomunicaciones en la Administración) y del Comité Técnico de Seguridad de Sistemas de Información y Protección de Datos, SSITAD, ambos del Consejo Superior de Informática. Director del Proyecto Intranet Administrativa. Secretario de SSITAD. Delegado español en el Comité de Gestión del Arreglo de Reconocimiento de Certificados de Criterios Comunes de Seguridad de la Tecnología de la Información.

EL RECONOCIMIENTO INTERNACIONAL DE LOS CERTIFICADOS.
ARREGLO DE CERTIFICACIÓN DE CRITERIOS DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

1.-Las certificaciones en la seguridad de la información.

La expresión "certificación", cuando se asocia con la seguridad de la información, tiene significados y contenidos muy diferentes. Entre ellos se encuentran los siguientes:

- de la tecnología de la información, en base a evaluaciones realizadas conforme a criterios públicos. Es el caso de los criterios ITSEC/ITSEM y, más recientemente, de acuerdo con la norma ISO/IEC 15408[1], Criterios de evaluación de la seguridad de la tecnología de la información conocida también como *Criterios Comunes.*
- de los servicios de información, por ejemplo respecto a la norma británica BS 7799[2].
- de la autenticidad del autor de un documento electrónico.
- de la autenticidad de los emisores y receptores de las transacciones electrónicas, y de la integridad de las mismas.

Las cuatro manifestaciones de la certificación tienen en la práctica estrechas interrelaciones. Por ejemplo, es difícil que se pueda llegar a confiar en los certificados que emita un determinado prestador de servicios de certificación de firma electrónica si éste, a su vez, no cuenta con productos, sistemas y servicios de seguridad certificados en sus componentes de negocio esenciales.

A pesar que un universo interconectado precisa de armonización y acuerdos internacionales, únicamente la certificación de la seguridad de la tecnología de la información goza de cierto nivel

[1] Información en http://csrc.nist.gov/cc/

[2] Entre las motivaciones de BS 7799, se encontraba inicialmente apoyar el cumplimiento de la ley británica de protección de datos de carácter personal. Pero también las necesidades que se derivan de la creciente interdependencia de las empresas y organizaciones, que posibilita que las agresiones pueden ejecutarse desde otras entidades, distinta de la propia, debido a la mutua dependencia derivada de la interrelación, en particular con respecto a la información común que compartan. Evidentemente, la información, además de exacta, completa y oportunamente disponible, únicamente debe ser accesible por aquellos que tengan legítimo derecho, no importa si se encuentra bajo el control de la propia organización como de otra con la que se tengan asuntos en común. A tal fin, una manera de fundar la confianza mutua entre organizaciones que manejan información compartida es la certificación de dichas organizaciones con respecto a la seguridad del manejo de la información. Puede encontrarse información en http://www.c-cure.org

práctico de consenso. En el segundo de los casos, citado más arriba, se abre camino en el seno de Organización Internacional de Normalización (IS0) la mencionada iniciativa británica.
Por su parte, la certificación de la autenticidad está en plena ebullición de iniciativas nacionales e internacionales, a las que no son ajenas presiones industriales y comerciales, que en ocasiones buscan su imposición de facto. La Directiva sobre firma electrónica es una muestra de armonización, pero está por ver su aplicabilidad práctica, en forma de normas y reconocimiento, por ejemplo respecto a la interoperabilidad entre diferentes prestadores de servicios de certificaciones. Son de relevancia los trabajos en curso de ETSI, que se recogen bajo el título "European Electronic Signature Standard Iniciative" EESSI[3].

En esta ponencia nos referimos únicamente al reconocimiento de la certificación de la seguridad de la tecnología de la información,recogida en el Arreglo de Reconocimiento de los Certificados de Criterios Comunes en el campo de la seguridad de la tecnología de la información. (Arreglo en lo que sigue).

2.-Evaluación y certificación.

Por *evaluación* se entiende el examen detallado, efectuado por un organismo acreditado, de los aspectos de seguridad de un productor o sistema, a fin de comprobar qué requisitos de seguridad cumple y hasta qué nivel.

En el mercado pueden encontrarse cinco tipos principales o modalidades de evaluación:

- Autoevaluación del fabricante o proveedor.
- Pruebas de aceptación, realizadas por el usuario.
- Evaluación indirecta (existencia de otro sistema ya evaluado y de arquitectura común).
- Pruebas de aceptación efectuadas por terceros, sin requisitos formales.
- Evaluación formal por parte de un laboratorio acreditado.

Caben pues evaluaciones no - formales, realizadas por el propio fabricante o entidad y, consecuentemente, una *Declaración* de conformidad de lo evaluado con respecto a criterios estándares o no; sería el caso en que un determinado mecanismo de seguridad garantizado como seguro por el propio fabricante (quien declara el objetivo de la funcionalidad de seguridad y la calidad con la que la consigue) o también el caso de una organización que declara haber establecido internamente determinados controles en relación con la protección de la información.

[3] http://www.ict.etsi.org/eessi/eessi-homepage.htm

Por *certificación de la seguridad* se entiende la *confirmación del resultado de una evaluación, y que los criterios de evaluación utilizados fueron correctamente aplicados*. Presupone pues la existencia de unos *criterios* y de unos procedimientos y métodos de evaluación formales, rigurosos y con sólida base científica; de otro modo, la certificación de un producto, sistema, carecería de fundamento para proporcionar confianza. La *certificación, en* el Arreglo, es un proceso formal, controlado por una entidad independiente, gubernamental, que se emite tras la evaluación formal realizada por organizaciones o laboratorios debidamente acreditados. Las entidades que emiten tales certificados (o validación) reciben el nombre de Órgano *de certificación*. Garantiza los resultados de la evaluación y que ésta ha sido realizada de acuerdo con los criterios y procedimientos formalmente establecidos.

3.-Experiencia previa. El Reconocimiento mutuo de las evaluaciones y las certificaciones de Seguridad de la tecnología de la evaluación en Europa.

El reconocimiento mutuo de las evaluaciones y certificaciones de la seguridad tiene una andadura relativamente corta, pero intensa.

La Recomendación del Consejo de 7 de abril de 1995 (DOCE 26-4-1995) relativa a los criterios comunes de evaluación de la seguridad en las tecnologías de la información sanciona ITSEC a nivel europeo y encarga a SOG IS [4] avanzar hacia el reconocimiento de los certificados que se expidan tras las evaluaciones. SOG IS aprobó el 21 de noviembre de 1997 el Acuerdo de Reconocimiento Mutuo de Certificados de Seguridad de los Sistemas de Información[5] (*Acuerdo* en lo que sigue), cuya finalidad es conseguir que los productos o sistemas con certificado de evaluación de la seguridad de la tecnología de la información de un país puedan ser utilizados en otros sin necesidad de repetir dichos procesos y sin merma de confianza en la fiabilidad de los criterios sobre los que se basa el certificado original.

En el Acuerdo europeo, los Servicios de Evaluación se acreditan conforme con el marco EN45001 ó equivalente. Por su parte, las Autoridades de Certificación han de ser conformes con la norma EN 45011 ó equivalente independiente, gubernamental o no.

[4] SOG IS es el acrónimo de Grupo de Altos Funcionarios responsables de la seguridad de los sistemas de información. Fue establecido como Comité asesor de la Comisión de las Comunidades Europeas por la Decisión de 31-3-1992 (DOCE 8-5-1992) relativa a la seguridad de los sistemas de información.

[5] Documento SOG IS 17/97 final. Se puede consultar en http://www.cordis.lu/infosec/

El Comité de Gestión del Acuerdo se constituyó el día 3 de marzo de 1998. Forman parte del mismo los países de la Unión Europea: Alemania, España, Finlandia, Francia, Grecia, Italia, Países Bajos, Reino Unido y Suecia, además de Noruega y Suiza, del ámbito de la Asociación Europea de Libre Comercio (EFTA).

En virtud del Acuerdo, los países que lo integran se comprometan a reconocer como si fueran propios los certificados que emitan los tres Órganos de Certificación Cualificado reconocidos, a saber, Alemania (BSI), Francia (SCSSI) y Reino Unido (UKITSEC).

Desde el establecimiento del Acuerdo se han certificado 34 productos por países, 21 han sido emitidos por el Reino Unido, 7 por Alemania y 6 por Francia.

4.-La transición hacia los Criterios Comunes

La transición hacia el reconocimiento mutuo internacional de los certificados de la seguridad emitida en base a los Criterios Comunes, partiendo de ITSEC, fue relativamente sencilla, ya que en la mencionada Recomendación del Consejo de 07-04-1995 se recogía la preferencia por criterios internacionales.

La colaboración para armonizar los tres criterios de evaluación de la seguridad de tecnología de la información (CTSEC, Estados Unidos; ITSEC, Unión Europea; CT CPEc, Canadá) se remonta a 1993, bajo los auspicios de SOG IS y NIST. No obstante las diferencias entre unos y otros criterios y los esquemas de evaluación y certificación en los que se aplicaban, las evaluaciones proporcionaban resultados razonablemente comparables, lo que hacía viable una evolución común, desprovista de incertidumbres esenciales, y además rápida.

Las ventajas de esa aproximación común (que recibió el título de “Criterios Comunes”, que subrayaba el ánimo de los promotores de enfatizar lo que les podría unir) son evidentes:

- Eliminar la necesidad de múltiples evaluaciones y certificaciones nacionales, lo que abarata costes y reduce los plazos.

- Apoyar su extensión global, a través de la creación de un estándar internacional, lo que ya es una realidad.

Con independencia de la bondad intrínseca de los Criterios Comunes, esta norma ha permitido establecer el reconocimiento internacional de evaluaciones y certificaciones.

5.-El arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de la Tecnología de la Información.

El día 23 de mayo de 2000 tuvo lugar en Baltimore (Maryland, Estados Unidos) la ratificación de la adhesión de Alemania, Australia, Canadá, España, Estados Unidos, Finlandia, Francia, Grecia, Italia, Noruega, Nueva Zelanda, Países Bajos y Reino Unido, al Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de la Tecnología de la Información[6] (en lo sucesivo Arreglo)
Una idea del impacto previsible del Arreglo viene reflejada en los datos sobre el mercado de la tecnología de la información facilitados por el European Information Technology Observatory(EITO). El conjunto de los países miembro del Arreglo representaban, en 1999, más del 65% del mercado mundial.

El Arreglo se gestiona por un Comité, cuya primera presidencia corresponde a Alemania y del que forman parte todos los Países miembros. En la primera sesión de dicho Comité se eligió un Subcomité Ejecutivo, presidido por Estados Unidos y al que pertenecen Alemania, Australia, Canadá, España, Estados Unidos, Francia, Países Bajos y Reino Unido.

El Arreglo se firmó coincidiendo con la I Conferencia Internacional de Criterios Comunes, a la que asistieron 600 expertos, representantes de la industria, la empresa y las administraciones públicas, de 23 países. Se presentaron y debatieron 61 ponencias, que giraron alrededor de las características de seguridad y garantías necesarias en los productos comerciales que vayan a ser utilizados en los sistemas y redes de información.

5.1. QUÉ ES EL ARREGLO. OBJETIVOS

El Arreglo parte de la premisa de que la utilización de productos y sistemas de la tecnología de la información (TI), cuya seguridad ha sido certificada es una de las salvaguardas principales para proteger la información y los sistemas que la manejan.

Los certificados de la seguridad son expedidos por Organismos de Certificación reconocidos a productos o sistemas de TI (o a perfiles de protección) que hayan sido satisfactoriamente evaluados por Servicios de Evaluación, conforme a los Criterios Comunes. El Arreglo, que consta de 18 artículos, 11 anexos y un apéndice, especifica con detalle, entre otros aspectos, los

[6] Traducción no oficial del Arreglo, se puede encontrar en: http://www.map.es/csi/pg6000.htm).

requisitos que han de cumplir los Certificados de Criterios Comunes, los Organismos de Certificación y los Servicios de Evaluación.

Los Criterios Comunes establecen un conjunto de requisitos para definir las funciones de seguridad de los productos y sistemas de la TI y de los criterios para evaluar su seguridad. El proceso de evaluación, garantiza que las funciones de seguridad de tales productos y sistemas reúnen los requisitos declarados. Los resultados de las evaluaciones realizadas por Servicios de Evaluación independientes entre sí son completamente equiparables.

Por perfil de protección se entiende un conjunto de requisitos de seguridad de productos concretos para una categoría de funcionalidades que cubran necesidades específicas (por ejemplo sistemas operativos, aplicaciones para el campo de la salud, cortafuegos, etc).
Entre los objetivos del Arreglo figuran los siguientes:

- Asegurar que las evaluaciones de los productos y sistemas de TI y de los respectivos perfiles de protección (adecuados a cada caso) se llevan a cabo de acuerdo con normas rigurosas y consistentes.

- Propiciar el aumento del número de los productos y sistemas de TI y de los perfiles de protección evaluados, con nivel de seguridad creciente, disponibles en el mercado.

- Eliminar la carga que supone la duplicación, en distintos países, de las evaluaciones de los productos y sistemas de TI (y de los perfiles de protección), gracias a la aceptación internacional de los certificados.

- Disminuir el gasto del proceso de evaluación y de certificación de los productos y sistemas de TI y de los perfiles de protección, en razón de la economía de escala.

5.2. A QUÉ SE COMPROMETEN LOS SIGNATARIOS

Los Miembros se comprometen a reconocer los Certificados de Criterios Comunes que hayan sido expedidos por cualquier otro participante, que haya actuado de conformidad con las condiciones del Arreglo, y de acuerdo con las leyes y normativas nacionales aplicables en cada caso.

Como salvedad, se establece que en el caso de que el reconocimiento de un certificado de criterios comunes emitido por un Miembro del Arreglo suponga que otro participante haya de

actuar en contra de alguna ley o normativa vigente, ya sea nacional, internacional o de la Comunidad Europea, ese participante podrá declinar el reconocimiento de dicho certificado.

En cualquier caso, conviene hacer notar que el reconocimiento no constituye aval o garantía de los Órganos de Certificación y Servicios de Evaluación que hayan intervenido en los certificados, ni tampoco de los productos o sistemas certificados.

Finalmente, los participantes que además son Miembros del anterior Acuerdo de Reconocimiento Mutuo de Certificados de la Evaluación de la Seguridad de las Tecnologías de la Información mantienen su obligación de apoyar y reconocer los certificados de ITSEC (Information Technology Security Evaluation Criteria) de conformidad con los términos del Acuerdo de Reconocimiento Mutuo y con los del Acuerdo complementario del reconocimiento, que aparece como apéndice del Arreglo.

5.3. A QUIÉNES PUEDE INTERESAR / BENEFICIAR

Entre los beneficiarios directos del Arreglo se encuentran:

Las Administraciones Públicas, para establecer las bases de la seguridad de la información y de las infraestructuras que la manejan.

La industria del sector, que puede encontrar mercados más amplios a los productos y sistemas de la TI que cuenten con el valor añadido del certificado.

Los consumidores (particulares, empresas e instituciones públicas), que pueden contar con mayor oferta de productos y sistemas certificados como seguros para proteger sus activos y transacciones.

En definitiva, es la sociedad en su conjunto la que se beneficia del Arreglo. La evaluación rigurosa e internacionalmente contrastada contribuye a dar confianza en la seguridad de los productos y sistemas de información, que componen la infraestructura y los servicios de TI.

5.4. ACTUACIONES DE ACOMPAÑAMIENTO

El aprovechamiento de los beneficios que proporciona el Arreglo pasa necesariamente por la promoción de la evaluación y de la certificación y la formación y difusión.

Promoción de la evaluación y la certificación

Los beneficios inmediatos que consigue España con su pertenencia al Arreglo se derivan del conocimiento en profundidad de los mecanismos de certificación y evaluación de la seguridad de la tecnología de la información.

El lugar que ocupa nuestro país en el concierto industrial mundial obliga a plantearse objetivos más ambiciosos, como la promoción de la actividad comercial de la evaluación de la seguridad de la tecnología de la información y el establecimiento de un esquema nacional de certificación y de la estructura orgánica que lo ponga en marcha.

En este sentido existen en España dos esquemas parciales de certificación uno en el Ministerio de Defensa y otro en el Ministerio de Ciencia y Tecnología. Este último se crea para cumplir lo dispuesto en el Real Decreto Ley 14/1999 de Firma Electrónica. Conviene tener en cuenta que parece evidente que a nivel europeo o internacional se percibe la preferencia por certificaciones de seguridad únicas, con independencia del campo de aplicación.

Otra actuación tecnológica sería la de promover la evolución de MAGERIT. Los fundamentos de la metodología española y de la herramienta de análisis y de gestión de riesgos aparecen como idóneos para ayudar a definir los objetivos de seguridad y los perfiles de protección previstos en los Criterios Comunes (paso previo obligado para la evaluación de productos y sistemas de tecnologías de la información).

De formación y difusión.

Alcanzar una aceptación efectiva de la certificación de la seguridad de la tecnología de la información, pasa por poner en marcha un conjunto de actuaciones de difusión y formación, entre las que se encuentran:

Interesar a la industria en la certificación de la seguridad de sus productos o sistemas de información, incluso desde el mismo proceso de creación de los productos y sistemas de información.

Promover la formación de técnicos en los criterios comunes

Informar a los consumidores, particulares y empresas, acerca de las ventajas de contar con productos y sistemas certificados.

Promover la aplicación de los perfiles de protección a sectores de especial interés, como la salud, las telecomunicaciones, etc.

Finalmente, para mejor protegerse a sí misma y para educar al mercado, la Administración debería tener en cuenta en sus adquisiciones de tecnología de la información la preferencia por los productos y sistemas certificados.

La I Conferencia Internacional sobre Criterios Comunes [7] ha marcado el principio de un amplio acuerdo internacional, que estimule a la industria a participar en el proceso, no sólo como objeto de la certificación, sino también proporcionando herramientas para la evaluación.

En este sentido es de subrayar la iniciativa de Estados Unidos "National Information Assurance Patertnership[8], que persigue impulsar la actividad de la evaluación. Se orienta con argumentos de negocio tanto a los productores como a los centros o laboratorios de evaluación, en ambos casos con el propósito de avanzar con firmeza hacia una mayor fortaleza del ciberespacio.

6.-El camino por recorrer. El Esquema Nacional de Evaluación y Certificación de la Seguridad de los Sistemas de Información.

En nuestro país, se está trabajando en el Proyecto de Esquema Nacional de Evaluación y Certificación de la Seguridad de los Sistemas de Información, del Consejo Superior de Informática, encargándose de su preparación el Grupo ad hoc 3 del Comité Técnico de Seguridad de los Sistemas de Información y Protección de Datos, SSITAD.

Los actores principales del proyecto de Esquema son la *Oficina Nacional de Seguridad para la certificación de los sistemas de información* (es decir, el Órgano de Certificación) y las *Instalaciones o Laboratorios de evaluación*

La Oficina sería la responsable de la emisión de los correspondientes certificados y de la acreditación de las instalaciones de evaluación. Entre sus cometidos se contemplan la elaboración de procedimientos para la acreditación de las instalaciones de evaluación, procedimientos para la realización de las evaluaciones de los sistemas y productos, procedimientos para la certificación y la elaboración de guías para los diferentes afectados: patrocinadores, productores, instituciones de evaluación, auditores, etc.

[7] Información en http://niap.nist.gov/cc-scheme/iccc/

[8] NIAP es promovido conjuntamente por NIST y NSA. Información en http://niap.nist.gov

Las Instalaciones de Evaluación podrían ser centros públicos o privados acreditados por la Oficina para realizar las evaluaciones de seguridad en el ámbito de aplicación del Esquema.

7.-Confianza y certificación de la seguridad de la tecnología de la información

Parece razonable admitir que en última instancia lo que importa es demostrar que, un producto (por ejemplo, un dispositivo de creación de firma) o una organización (por ejemplo, un prestador de servicios de certificación de firma electrónica) cumple los requisitos que sean de aplicación, sean éstos voluntarios o no. Es obvio que la mera existencia de las normas o la declaración de los interesados de que cumplen las mismas, por si solas, pueden no ser suficientes para generar la *confianza*.

En definitiva, los esquemas de evaluación y certificación de la seguridad de la información responden a la necesidad de fundar sólidamente la confianza que los usuarios reclaman en el uso de la tecnología de la información. Esto es, tener la tranquilidad de que un determinado dispositivo, sistema o servicio hace lo que tiene que hacer y nada más, y que es capaz de resistir la materialización de las amenazas que hayan sido tenidas en cuenta en su evaluación.