>> Jorge Dávila

La certificación de la seguridad

En la sociedad de la información las cosas no están tan bien como podría pensarse y hay que seguir dándole vueltas a cuáles pueden ser las causas y soluciones de ese problema. Si el *e-commerce* no se anima por desconfianza, habrá que conseguirla y eso suele hacerse a través de certificaciones, homologaciones o normalizaciones imparciales. La sociedad americana ha montado en el NIST la correspondiente iniciativa, mientras que en España no pasa de una oscura "infraestructura" del MAP y una oferta del Ministerio de Defensa. El arco fundamental ya está establecido bajo el paraguas de los "*Common Criteria*" y el acuerdo internacional de reconocimiento mutuo; ahora bien, ¿por qué nadie nos ofrece productos e instalaciones "certificadas"?

Pasamos por tiempos en los que las cosas no van especialmente bien para la Sociedad de la Información y, sobre todo, para el negocio electrónico en cualquiera de sus formas. Sin embargo, tampoco podemos decir que se trate de una situación realmente desastrosa y todavía mucha gente sabe que la red va a dar mucho juego, aunque no es fácil imaginar cómo. Una de las causas que se esgrimen para explicar la parálisis de las empresas para lanzarse al ruedo del mercado de siempre sobre tecnologías de ahora, es la falta de confianza en esa misma tecnología. Muchas son las noticias sobre virus y códigos maliciosos, muchas las referencias a personajes tan manidos como los *hackers* que todos mencionan y nadie conoce, pero pocas noticias se refieren a los intentos, un tanto tradicionales, de dar motivos para la confianza y que no son otros que la *normalización*, *certificación* u *homologación* de los sistemas en cuanto a su seguridad se refiere.

Las normas hoy conocidas como *"Common Criteria"* son el resultado de una serie de esfuerzos para desarrollar criterios para la evaluación de la seguridad en las tecnologías de la información y tienen vetustos antecedentes. A principios de los años 80 se desarrolló en Estados Unidos el *Trusted Computer System Evaluation Criteria* **(TCSEC)**. En la siguiente década, otros países tomaron iniciativas análogas y dirigidas a desarrollar nuevos criterios de evaluación, construidos sobre los conceptos del TCSEC americano pero siendo más flexibles y adaptables a la evolución natural de las TI. Diez años después, en 1991, en Europa se publica el *Information Technology Security Evaluation Criteria* **(ITSEC)** por parte de la Comisión Europea después del esfuerzo conjunto de Francia, Alemania, Holanda, y Reino Unido. Por otra parte, en 1993 y en Canadá, se publica *la Canadian Trusted Computer Product Evaluation Criteria* **(CTCPEC)** como una continuación de las aproximaciones de ITSEC y TCSEC.

En Estados Unidos y también en 1993, se publica el borrador de los *Federal Criteria for Information Technology Security* (**FCITS**) como una segunda aproximación que combina los conceptos americanos y europeos en lo que a criterios de evaluación se refiere. Paralelamente y desde 1990, en la *International Organization for Standardization* (**ISO**) se habían iniciado algunos trabajos para desarrollar un conjunto de estándares internacionales, con ámbito general, para los criterios de evaluación (ISO/IEC 15408) de la seguridad de los sistemas de información. En mayo de 2002, tras dos años de negociaciones entre administraciones e industria, los gobiernos de EEUU, Canadá, Francia, Alemania y Reino Unido firman un acuerdo histórico[1] por el que se comprometen a reconocer los resultados de todas aquellas evaluaciones que se hiciesen siguiendo las directrices de los Criterios Comunes en la forma de los denominados *"Protection Profiles"*.

> ***Estamos ante más de veinte años de esfuerzos para normalizar, homologar, o certificar eso tan etéreo que denominamos "seguridad" y cuya apreciación siempre resulta tan subjetiva; a pesar de ello son pocos los resultados tangibles que pueden mencionarse.***

Los objetivos de estas medidas son:

– Asegurar que la evaluación de productos TI se realiza según estándares de calidad y son vistos como argumentos para fundamentar la confianza en la seguridad de dichos productos.

– Aumentar la disponibilidad de productos TI de calidad y de seguridad probada, así como la existencia de *"Protection Profiles"* de uso nacional.

– Eliminar las dobles evaluaciones; es decir, que los productos TI y los *"Protection Profiles"* que tienen un *"Common Criteria Certificate"* pueden obtenerse de una vez por todas.

– Mejorar continuamente la eficiencia, efectividad y los costes de las evaluaciones de seguridad y de los procesos de validación / certificación.

El acuerdo especifica las condiciones en las que los participantes aceptarán los resultados de las evaluaciones de la seguridad en productos TI y define un comité de gestión compuesto por representantes de cada país firmante, cuya misión es desarrollar el acuerdo y dar guía a los subordinados esquemas nacionales relacionados con la evaluación y validación de los productos TI.

Sin embargo, la complejidad de los sistemas de información y productos a evaluar es ya tan significativa, que un criterio de evaluación ideal y

una metodología humanamente perfecta no podrían atender a todos los riesgos o eventualidades posibles por lo que, en muchos casos, los criterios proponen *la consulta a expertos profesionales*. El objetivo de cualquier evaluación es poder asegurar que los productos estudiados satisfacen sus objetivos de seguridad o que los *"Protection Profiles"* propuestos son completos y están bien diseñados.

Así pues, estamos ante más de veinte años de esfuerzos para normalizar, homologar, o certificar eso tan etéreo que denominamos *"seguridad"* y cuya apreciación siempre resulta tan subjetiva. A pesar de ello son pocos los resultados tangibles que pueden mencionarse.

El NIST de los EEUU, a través de su división CSRC[2] centra su trabajo con la administración y empresas americanas en conseguir sistemas y redes de información con una mayor seguridad mediante el desarrollo, gestión y promoción de la seguridad a través de herramientas[3,4], técnicas específicas, nuevos servicios, y apoyando programas de evaluación y validación[5].

A través de la *National Information Assurance Partnership* **(NIAP)**, el NIST junto con la oculta NSA[6], han anunciado su estrecha colaboración para definir los requisitos y especificaciones de seguridad aplicables a tecnología críticas utilizadas en la construcción de los sistemas de información de sus agencias federales, dentro del marco que representan los Criterios Comunes. Para ello se proponen el establecimiento de Perfiles de Protección *("Protection Profiles")* en áreas clave como los sistemas operativos, los cortafuegos, las tarjetas inteligentes, sistemas biométricos, bases de datos, componentes de PKI, equipos de red, VPNs, IDSs, navegadores, etc.

A este lado del océano y refiriéndonos a nuestro país, encontramos dentro del Ministerio de Administraciones Públicas al *"Consejo Superior de Informática"* que se ocupa, entre otras cosas, de la *"Evaluación y Certificación de la Seguridad de las Tecnologías de la Información"* y habla de un *"Esquema nacional de evaluación y certificación de los Sistemas de Información"*[7] dirigido por el indefinido y desconocido *"Grupo ad hoc 3"*[8] del Comité Técnico del SSITAD[9].

El objetivo principal de esta propuesta es, según sus representantes, el de cubrir las necesidades de todos los sectores implicados, Industria y Administración, ofreciendo sus servicios de evaluación y certificación a productores, proveedores, y usuarios de las tecnologías de la información. El esquema nacional español se compone de:

(1) Comisión de Dirección, que es responsable de su funcionamiento y que asegurará la provisión de servicios.

(2) Oficina Nacional de Certificación (**ONC**), que será responsable de la emisión de los correspondientes certificados y de la acreditación de las instalaciones de evaluación. Esta oficina tendrá que elaborar procedimientos para la acreditación de las instalaciones de evaluación, procedimientos para ello en sistemas y productos, procedimientos para la certificación, elaboración de guías para los diferentes agentes, etc.

(3) Instalaciones de Evaluación. En un principio serán centros públicos o privados acreditados por la ONC para realizar las evaluaciones de seguridad.

El 27 de noviembre de 2000 el Ministerio de Defensa acreditó al CESTI[10] como Entidad Evaluadora de la Seguridad en el ámbito del Ministerio de Defensa y emite los correspondientes dictámenes, de acuerdo con la normativa IT-SEC-ITSEM, cuando le son solicitados. Este centro es parte del Esquema de Evaluación y Certificación de la Seguridad de las TIs de ese Ministerio. El CESTI está organizado en tres unidades y cuatro laboratorios de evaluación que mantienen distintas líneas de actuación en sistemas aeronáuticos, comunicaciones y redes, firma electrónica y tarjetas inteligentes.

Según la información facilitada por el INTA en Internet, el CESTI *"representa y defiende los intereses del Ministerio de Defensa"* cuando le sea requerida, aunque también lo puede hacer con *"empresas relacionadas con el mismo y por otras entidades que lo requieran"*, pero a partir del 22 de junio de 2001 se corrige este elitismo y el CESTI se acreditó también en el ámbito civil ante la Entidad Nacional de Acreditación (ENAC).

Por el momento no parece que entre sus clientes cuente con importantes productores españoles de software ni que su actividad haya sido frenética hasta el momento. Si la normalización pretendía poner un poco de orden en esto de la seguridad, la verdad es que no parece haberlo conseguido ya que, a pesar de contar con antecedentes de más de veinte años, acuerdos internacionales de gran calado, e iniciativas razonables como la del Ministerio de Defensa, nadie somete y nadie exige que se someta a certificación fiable los productos que componen los sistemas que les dan cabida en la sociedad de la información.

Así pues, cada vez está más claro que la tan cacareada inseguridad del negocio Internet, entre otros, no es algo inevitable, sino que no se tienen intenciones reales de hacerlo. Si alguien conoce la explicación, a muchos nos encantaría saberla. **I**

> ***Si la normalización pretendía poner un poco de orden en esto de la seguridad, la verdad es que no parece haberlo conseguido***

(1) "Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security"

(2) **CSRC** = **C**omputer **S**ecurity **R**esource **C**enter http://csrc.nist.gov/index.html

(3) **CMVP** = **C**ryptographic **M**odule **V**alidation **P**rogram <http://csrc.nist.gov/cryptval/>

(4) **ASSET** = **A**utomated **S**ystem **S**ecurity **E**valuation **T**ool <http://csrc.nist.gov/asset/>

(5) **NIAP** = **N**ational **I**nformation **A**ssurance **P**artnership <http://niap.nist.gov/>

(6) **NSA** = **N**ational **S**ecurity **A**gency <http://nsa.gov/>

(7) <http://www.map.es/csi/pg3432.htm>

(8) <http://www.map.es/csi/pg3405.htm>

(9) **SSITAD** = Seguridad de los Sistemas de Información y Protección de Datos

(10) **CESTI** = **C**entro de **E**valuación de la **S**eguridad de las **T**ecnologías de la **I**nformación como parte del INTA <http://www.inta.es/es unidad.asp?IDunidad=1992&barra=UNIDAD>

Jorge Dávila Muro
Director
Laborfatorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es