

# 'Criterios Comunes' para la seguridad

La certificación que vela por la excelencia

SIETE NIVELES DE GARANTÍA -EAL- SON LOS QUE CERTIFICAN LOS ORGANISMOS AUTORIZADOS DE DOCE PAÍSES EN TODO EL MUNDO, ESPAÑA ENTRE ELLOS, POR MEDIO DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN). ACTUALMENTE, LA ISO-IEC 15408, O MÁS CONOCIDA COMO CERTIFICACIÓN 'COMMON CRITERIA' (CC) CUENTA CON EL RECONOCIMIENTO DE 25 ESTADOS. CIENTOS DE PRODUCTOS Y SISTEMAS DE TODO TIPO DE FABRICANTES HAN CONSEGUIDO YA LA CC, TRAS EL PROCESO DE EVALUACIÓN EN ALGUNO DE LOS 48 LABORATORIOS CERTIFICADOS.

Tx: Mercedes Oriol Vico.  
Ft: CCN y Getty Images.

**TODO EMPEZÓ** a principios de los años 80, cuando Estados Unidos plasmó una serie de criterios de seguridad informática, recogidos en el *Trusted Computer System Evaluation Criteria* (TCSEC), que más tarde se publicaron en el "libro naranja". A partir de ahí, distintos países seguirían el ejemplo norteamericano para valorar y certificar, de alguna manera, la seguridad de sus productos y sistemas tecnológicos.

En 1991, la Comisión Europea (CE) hizo público su *Information Technology Security Evaluation Criteria* (ITSEC), desarrollado principalmente por Francia, Alemania, Holanda y Reino Unido.

Canadá, por su parte, intentó aunar los criterios americanos y europeos, en 1993, en su documento *Canadian*

*Trusted Computer Product Evaluation* (TCPEEC), intención que igualmente persiguió Estados Unidos, en el mismo año, en la evolución de su primer paso -el TCSEC- hacia el *Federal Criteria*.

En estos primeros años 90, es cuando la Organización Internacional para la Estandarización (ISO) también comienza su interés y trabajo en esta materia, que le llevará a dar como fruto, en 1999, lo que hoy conocemos como ISO-IEC 15408 o certificación *Common Criteria* (CC) -*Common Criteria for Information Technology Security Evaluation*-.

#### Acercamiento más explicativo

Pero, ¿qué es exactamente *Common Criteria*? Según el Centro Criptológico Nacional (CCN), perteneciente al Centro Nacional de Inteligencia (CNI) del Ministerio de Defensa, que es el organismo oficial de certificación en nuestro país, los Criterios Comunes



hacen tanto énfasis en las propiedades de seguridad del producto, como en el proceso de su desarrollo. Dependiendo del nivel de garantía exigido, las empresas deben implementar un sistema que desarrolle un modelo de ciclo de vida de desarrollo y mantenimiento del objeto a evaluar con sus fases, controles, herramientas y técnicas adecuadas, un sistema de gestión de configuración que garantice la integridad del producto, procedimientos para la realización del seguimiento de fallos de seguridad post-certificación, etc. Además, las propias áreas de desarrollo y el proceso de distribución del producto, pueden estar sujetos a

## El sistema de 'Common Criteria' está formado por siete niveles, los EAL, por medio de los que se contrasta el nivel de seguridad real de los aspectos requeridos con lo que el fabricante afirma

medidas de seguridad físicas, procedimentales, personales y técnicas orientadas a garantizar la confidencialidad e integridad del producto y de su documentación. El CCN asegura que, en cuanto al producto, las empresas deben mentalizarse de que el resultado de la evaluación está orientado a la mejora de sus prestaciones de seguridad y, por tanto, una consecuencia normal del proceso, es la detección de alguna vulnerabilidad que el fabricante deberá corregir como cualquier otro aspecto que pudiera surgir como resultado de las actividades de evaluación.

El sistema de *Common Criteria* está formado por siete niveles, los *Evaluation Assurance Level* (EAL), por medio de los que se contrasta el nivel de seguridad real de los aspectos anteriormente indicados con lo que el fabricante afirma. Los cuatro primeros niveles (EAL1, EAL2, EAL3 y EAL4) están pensados para productos y sistemas comerciales y los dos últimos (EAL6 y EAL7) están destinados sólo para productos y sistemas de Defensa, no comerciales.

### Acuerdo de reconocimiento

En mayo de 2000, se firmó el *Common Criteria Recognition Agreement* (CCRA), un acuerdo de reconocimiento mutuo de certificados, hasta el nivel EAL4. Desde entonces hasta hoy, 25 países se han unido al CCRA para reconocer la *Methodology for Information Technology Security Evaluation* (CEM), bases técnicas de esta certificación. En este mapa, los miembros se diferencian en países emisores de certificados (Australia,

Nueva Zelanda, Canadá, Francia, Alemania, Japón, República de Corea, Holanda, Noruega, España, Suecia, Reino Unido y Estados Unidos) y países consumidores de certificados (Austria, República Checa, Dinamarca, Finlandia, Grecia, Hungría, India, Israel, Italia, Malasia, Singapur y Turquía).

En 2006, el esquema español, tras pasar una auditoría de capacitación técnica, entró a formar parte de los esquemas de países emisores de certificados CC dentro del CCRA. Éstos cuentan un organismo de certificación (OC) que es el que aprueba la certificación, tras una evaluación exhaustiva realizada por laboratorios autorizados.

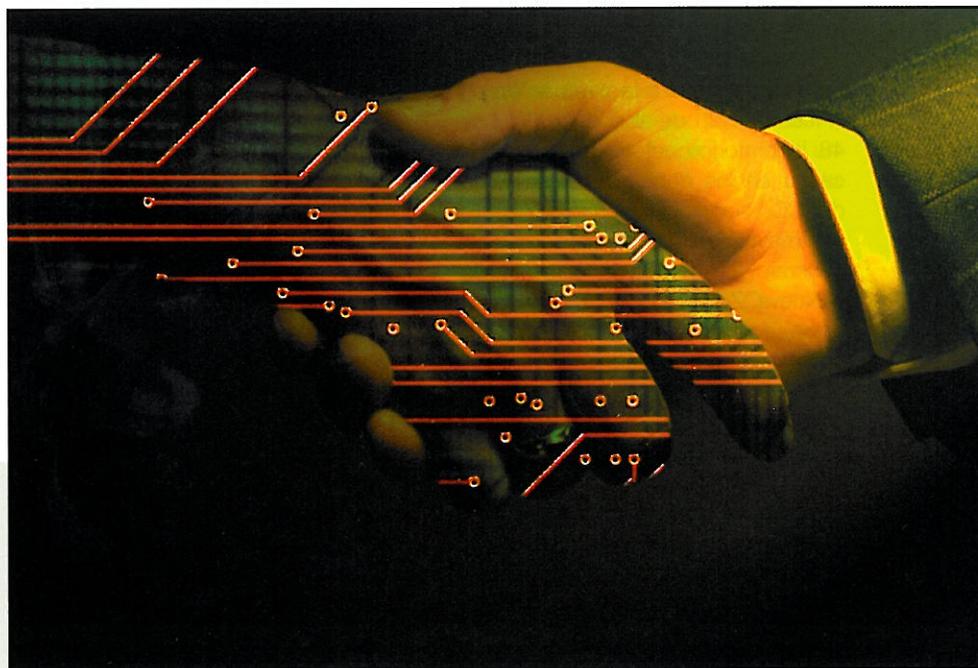
### CCN, organismo de certificación

Ya desde los orígenes del CCN -con la publicación en el Boletín Oficial del Estado (BOE) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (CCN)-, se marca dentro del ámbito de actuación y funciones del

centro (en el artículo 2, apartado c) la constitución del "organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de la información, de aplicación a productos y sistemas en su ámbito". Y la función de "valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura" (artículo 2, apartado d).

Pero no es hasta tres años después -con la Orden Pre/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, cuando comienza a funcionar. Sin embargo, España estuvo presente en el CCRA desde su creación, a través del Ministerio de Administraciones Públicas (MAP).

A partir de entonces, los certificados que emite el esquema español, a través del CCN (hasta ese cuarto



El CCRA es un acuerdo de reconocimiento mutuo de certificados que se firmó en mayo del año 2000. Desde entonces, 25 países se han unido a este foro.

nivel) son reconocidos internacionalmente dentro de los firmantes del CCRA. Asimismo, el CCN también reconoce cualquier certificado emitido por un esquema extranjero -reconocido como emisor en dicho ámbito-.

Este sistema permite, por tanto, que cualquier empresa extranjera pueda perfectamente certificar sus productos en el esquema español.

Los portavoces del CCN explican que el centro basa la decisión de conceder o denegar el certificado CC, principalmente, en un análisis de seguridad formalizado conforme a la metodología CC, que recibe el nombre de evaluación de seguridad y que sólo puede realizar alguno de los laboratorios acreditados por el CCN a tal efecto. El CCN tiene la obligación,

la Seguridad de las Tecnologías de la Información (CESTI) del Instituto Nacional de Técnica Aeroespacial (INTA); Applus y Epoche & Espri.

Según fuentes del CCN, dentro del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información se establecen los requisitos para la acreditación de los laboratorios que quieran participar en este esquema. No hay una actividad de selección de laboratorios, sino que son los propios laboratorios que quieren participar en el esquema los que solicitan ser acreditados. Para ello, deberán cumplir con los requisitos previstos en el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, apro-

supone. En ello influyen los siguientes factores:

- La tecnología del objeto a evaluar (por ejemplo, tarjeta inteligente versus aplicación web).
- Sus características de seguridad: en número y en complejidad.
- El nivel de garantía: profundidad y rigor de la evaluación (pruebas de caja negra versus pruebas de caja blanca; inspección de código versus diseño de alto nivel; resistente a atacantes con alto potencial versus bajo potencial; etc...).

Desde el punto de vista de la evaluación, el CCN calcula, grosso modo, que se podría hacer una aproximación media de un esfuerzo aproximado de diez meses/hombre para una evaluación EAL4. Sin embargo, esta institución deja claro que este no es el único parámetro que debe ser tenido en cuenta por parte de la empresa. Los responsables deberán hacer una provisión de recursos/gastos internos: consultoría, adaptación de los procesos, planificación de recursos para las correcciones del producto, etc. En algunos casos, la empresa dedica recursos exclusivos para cumplir los requisitos de documentación de la norma aunque, en general, el propio grupo de desarrollo y un responsable de certificación ayudados por un consultor CC externo, abordan con éxito el proceso completo.

#### Certificados emitidos

Según el CCN, en España, hasta la fecha se han abierto 26 expedientes de certificación CC, aunque la mayoría de ellos se encuentran todavía en evaluación. Se han emitido, de momento, seis certificados CC y hay cuatro expedientes cuya evaluación ya ha terminado satisfactoriamente y cuyos certificados serán emitidos próximamente.

Los certificados emitidos, con indicación de su nivel, corresponden a los siguientes productos:

- Keyone 2.1 (EAL2) y Keyone 3.0 (EAL4+), de la empresa Safelayer.
- Tarjeta electrónica del Ministerio de Defensa 1.0 (EAL4+), de la empresa Microelectrónica Española.
- DNle (EAL4+), de la Fábrica Nacional de Moneda y Timbre (FNMT).

## Hoy hay 48 laboratorios autorizados en todo el mundo para realizar la evaluación CC

y el derecho, de realizar un seguimiento del proceso de evaluación que le permita validar el trabajo realizado por el laboratorio. Es, por tanto, el CCN el que, en última instancia, tiene la potestad de decidir, basándose en las conclusiones del laboratorio, la estimación o no del certificado.

#### Laboratorios para la evaluación

A fecha de 28 de abril de 2008, hay 48 laboratorios autorizados y certificados en los doce países emisores de CC, siendo Alemania el estado con mayor cantidad de ellos, doce en concreto. El resto: tres, en Australia y Nueva Zelanda; tres, en Canadá; cinco, en Francia; cuatro, en Japón; uno en Holanda; dos, en Noruega; dos, en Suecia; cuatro, en Reino Unido; y nueve en Estados Unidos.

Actualmente, en España, hay tres laboratorios acreditados por el Centro Criptológico Nacional (CCN) para realizar la evaluación de la seguridad de las tecnologías de LA información: el Centro de Evaluación de

bado por la Orden PRE/2740/2007, de 19 de septiembre. Estos requisitos se refieren, fundamentalmente, a tres aspectos: seguridad (del personal, de las instalaciones y en el manejo y custodia de la información de las evaluaciones), competencia técnica para realizar este tipo de evaluaciones y, por último, requisitos de información y coordinación con el Organismo de Certificación.

En cuanto al número de laboratorios acreditados, esto no depende del CCN, que aceptará cualquier solicitud de cualquier entidad, pública o privada, que quiera establecerse como laboratorio en este esquema. Aunque, hasta la fecha, no se ha recibido ninguna solicitud nueva al respecto.

#### Requisitos de la evaluación

Hay varios factores que afectan al coste de una evaluación, que exponen claramente los portavoces del CCN a continuación, y que, en todo caso, se presupuesta simplemente conforme a la carga de trabajo que

- ✦ Crypto Token USB (EAL3), de la Datatech.
- ✦ Cifrador EP430S (EAL4+), de la empresa Epicom.
- ✦ ASF 4.1 (EAL3), de la empresa TB Solutions.

La información sobre las evaluaciones en curso y, sobre todo, sobre los certificados emitidos, se puede consultar en la página web del Organismo de Certificación: [www.oc.ccn.cni.es](http://www.oc.ccn.cni.es).

A nivel internacional, son cientos los productos y sistemas de compañías que ya tienen la certificación CC, según los perfiles a los que se hayan sometido: sistemas y dispositivos de control de accesos (algunos de Oracle, Hitachi, Citrix, Boeing, IBM, Siebel, Computer Associates (CA), entre otros), sistemas y dispositivos de protección perimetral (algunos de SonicWall, APPGate Network, Tutus Data AB, Avocent, Symantec, Fujitsu, Microsoft, Cisco, NexG, Check Point Software Technologies, Lucent Technologies, Juniper Networks, CyberGuard, SurfControl, Nokia, Nortel, WatchGuard, Secure Computing, Netasq, Fortinet, Stonesoft, y muchos más), protección de datos (algunos de Innovation Data Processing, Senforce Technologies, Sterling Commerce, Control Break Internacional, EMC, SafeNet, Bull, etc.), bases de datos (algunos de Intersystems, Sybase, etc.), sistemas y dispositivos de detección (algunos de Third Brigade, McAfee, Cryptek, TippingPoint...), sistemas y dispositivos relativos a *smart cards* (algunos de T-Systems Enterprise Services, Infineon Technologies, Gieseck&Devrient, Siemens AG, Sagem Défense Sécurité, Samsung Electronics, Oberthur Card System, etc.), sistemas de gestión de claves (algunos de Entrust Incorporated, CoreStreet, SecureNet, y más), sistemas y dispositivos de red (algunos de F5 Networks, Blue Coat Systems, Still Secure, BMC Software, Bea Systems, HP, LANDesk Software, EADS Telecom, etc.), sistemas operativos (de Aruba Networks, IBM, Microsoft, HP, Sun Microsystems, Oracle, Network Appliance, VMware, Apple, Nokia, Silicon Graphics...),

otros sistemas y dispositivos, y productos para la firma digital.

Se puede acceder al listado completo en: [www.commoncriteriaportal.org/products\\_ALL.html](http://www.commoncriteriaportal.org/products_ALL.html).

### Nuevos intentos

Los plazos del proceso de certificación de un producto se derivan de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, de 26 de noviembre, tal y como explica el CCN.

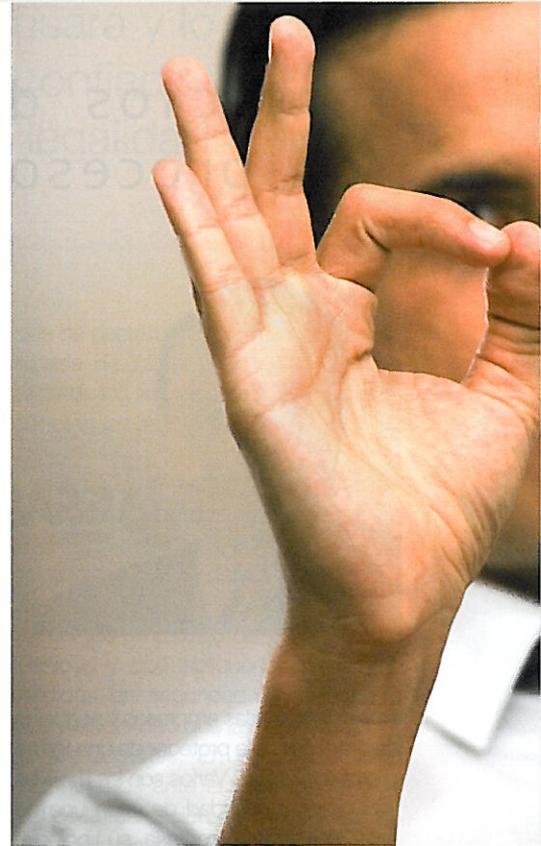
Hay empresas que no han conseguido la certificación, a pesar de haber realizado la evaluación en un laboratorio autorizado, bien por deficiencias en la documentación del producto o por aspectos relacionados con la resistencia técnica de dicho producto, es decir, por sus propiedades de seguridad. En estos casos en los que el dictamen del OC es desestimatorio, el fabricante puede volver a solicitar la certificación de su producto tras haber corregido las deficiencias por las que se desestimó su primera solicitud.

Independientemente de este punto, el CCN como organismo de certificación aconseja a las empresas que aborden el proceso empezando por niveles de garantía bajos, que no les requiera un gran esfuerzo para la adaptación de sus procesos, y vayan ampliando, de manera gradual, el alcance de sus certificaciones. Es decir, llegar al EAL4, tras haber pasado antes por un nivel EAL2, por ejemplo.

Otra recomendación del CCN es contar con una consultoría que proporcione a la empresa un curso de capacitación CC y una ayuda en el desarrollo de la documentación requerida.

### Beneficios y ventajas de la CC

Entre los beneficios y ventajas de conseguir una certificación *Common Criteria* está, en primer lugar, el prestigio internacional en materia de seguridad que este sello posee. Por otra parte, el CCN destaca que el propio proceso de evaluación conlleva, por un lado, la mejora de las características de seguridad del producto y, en ocasiones, incluso la mejora



La certificación ofrece, además de prestigio por el reconocimiento internacional que tiene, mejora de las propias características del producto o sistema a analizar, incluso en los procesos.

de los procesos de desarrollo del fabricante. También supone un factor de diferenciación que puede hacerse valer en determinados procesos de adquisición de productos de TI. Desde el punto de vista de la organización usuaria de productos de TI, esta certificación le proporciona un nivel de garantía de la seguridad de los productos que utiliza.

Durante los próximos 23 al 25 de septiembre, se celebra la 9ª Conferencia Internacional *Common Criteria* (I0CC), en Korea. España estará presente una vez más, aparte de con la participación activa en las reuniones de los grupos de trabajo de CC, por parte del OC, presidiendo una de las reuniones temáticas y uno de los paneles de discusión, así como en las ponencias de los laboratorios, de la Universidad Carlos III y del propio OC. ■