MINISTERIO
DE ADMINISTRACIONES
PÚBLICAS

SECRETARÍA GENERAL PARA LA ADMINISTRACIÓN PÚBLICA

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA

Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la seguridad de la Tecnología de la Información

Nipo: 326-07-019-4

1ª edición internet
Mayo de 2007

Catálogo general de publicaciones oficiales
http://www.060.es/

ÍNDICE

Portal de Criterios Comunes (Common Criteria Portal)

Organismo de Certificación

Texto completo del Arreglo

PREÁMBULO

La generalización del uso de los medios electrónicos, informáticos y telemáticos, proporciona unos beneficios evidentes para los ciudadanos y la sociedad. Al mismo tiempo, implica una dependencia de la tecnología de la información, cuyo correcto funcionamiento es cada vez más crítico para que las organizaciones puedan realizar su misión. Por lo tanto, adquiere crucial importancia la adopción de especificaciones y de normas comunes de seguridad para las distintas clases de productos y sistemas de información.

La evaluación rigurosa de la seguridad de los sistemas y productos de información y su certificación por órganos competentes, de acuerdo con la norma ISO / IEC 15408 de criterios comunes, es una de las mejores garantías de que la tecnología de la información realiza su cometido con el menor riesgo posible, y en condiciones de economía.

1. QUÉ ES EL ARREGLO

El *Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de la Tecnología de la Información* (en lo sucesivo *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* (que tienen la marca que se muestra a continuación) 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* (norma ISO / IEC 15408). El *Arreglo* especifica con detalle, entre otros aspectos, los requisitos que han de cumplir los *Certificados de Criterios Comunes*, los *Organismos de Certificación* y los *Centros 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, que se ciñe a lo prescrito en los *Criterios Comunes*, garantiza que las funciones de seguridad de tales productos y sistemas reúnen los requisitos declarados y que sus resultados son equivalentes, siempre que las evaluaciones hayan sido realizadas por *Servicios de Evaluación* en los términos del *Arreglo*.

Entre los objetivos que motivan el *Arreglo* figuran los siguientes:

a) 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.

b) 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.

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

d) 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*.

Información sobre el Proyecto de Criterios Comunes y listas de los certificados pueden encontrarse en la página web http://www.commoncriteriaportal.org, así como en las páginas web de los Organismos de Certificación.

2. CONSTITUCIÓN DEL ARREGLO Y ESTATUS DE ESPAÑA

El día 23 de mayo de 2000 tuvo lugar en Baltimore (Maryland, Estados Unidos) la ratificación de la adhesión al *Arreglo* de Alemania, Australia, Canadá, España, Estados Unidos, Finlandia, Francia, Grecia, Italia, Noruega, Nueva Zelanda, Países Bajos y Reino Unido. Posteriormente, se han incorporado Israel, Suecia, Austria, Turquía, Hungría, Japón, República Checa, Singapur, India, República de Corea y Dinamarca.

En representación del Reino de España suscribió el *Arreglo* el Ministerio de Administraciones Públicas, por orden de su Titular, previo informe favorable del Consejo Superior de Administración Electrónica, en su décimo cuarta Sesión Plenaria, celebrada el día 11 de mayo del año 2000, así como tras los oportunos informes jurídicos favorables del Departamento y del Ministerio de Asuntos Exteriores.

A partir del 17 de agosto de 2006, España cambia su estatus en el *Arreglo* y se convierte en participante acreditado para emitir certificados de seguridad de la tecnología de la información.

El *Arreglo*, en sus cuarenta páginas, 18 artículos, 11 anexos y un apéndice, especifica con detalle, entre otros aspectos, los requisitos que han de cumplir, los objetivos, compromisos, los requisitos

de los participantes y su forma de gobierno.

Una idea del impacto previsible del *Arreglo* la proporciona el que el conjunto de los países miembros del *Arreglo* representaban, en 2000, más del 67% del mercado mundial de la tecnología de la información (*European Information Technology Observatory* -EITO).

Precursor del *Arreglo* es el *Acuerdo de Reconocimiento Mutuo de Certificados de la Evaluación de la Seguridad de las Tecnologías de la Información*, cuyo ámbito geográfico se ceñía inicialmente a países europeos y cuya norma de referencia primera fue ITSEC, a la que posteriormente se añadió Criterios Comunes.

3. ORGANIZACIÓN DEL ARREGLO

La dirección máxima del *Arreglo* corresponde al *Comité de Gestión*, en el cual España está representada por el MAP. En su seno se elige a un Presidente.

Dicho Comité administra el *Arreglo*, lo que conlleva el actuar en cualquier asunto relativo a los términos y funcionamiento, admitir a los nuevos participantes, cambiar el estatus de los miembros, decidir si los Organismos de Certificación cumplen o no con los requisitos y realizar los cambios relativos al ámbito del *Arreglo*, en los casos previstos.

Dependiente del Comité de Gestión, existe un *Subcomité Ejecutivo*, compuesto por aquellos países que cuentan con órganos reconocidos de certificación de la seguridad de la tecnología de la información, además de otros Países miembros cuando así lo acuerde el Comité de Gestión. De la primera categoría son Alemania, Australia (junto a nueva Zelanda), Canadá, Estados Unidos, Francia, Japón y Reino Unido. España ha sido elegida para formar parte del Subcomité Ejecutivo en el periodo 2000 – 2001, a través del MAP, y desde el año 2003, a través del Centro Nacional de Inteligencia – Centro Criptológico Nacional.

Parte de la actividad del *Arreglo* se realiza mediante Grupos de Trabajo, que se encargan de aspectos tales como la interpretación de las normas como de su evolución internacional.

4. A QUÉ SE COMPROMETEN LOS SIGNATARIOS

Los Miembros se comprometen a *reconocer los Certificados de Criterios Comunes* hasta el nivel EAL4 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.

Conviene hacer notar, no obstante, que el reconocimiento no constituye aval o garantía de los *Órganos de Certificación* y *Servicios de Evaluación* que hayan intervenido en la evaluación o certificación, ni tampoco de los productos o sistemas certificados.

Por otra parte, sigue vigente el anterior *Acuerdo de Reconocimiento Mutuo de Certificados de la Evaluación de la Seguridad de las Tecnologías de la Información*, que no limita el nivel máximo de seguridad que se reconoce.

5. 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.

6. PERSPECTIVAS DEL ARREGLO

Desde su creación, el *Arreglo* no ha cesado de extenderse. Entre los signos de su vitalidad se pueden mencionar:

- En seis años transcurridos desde su creación, a los trece Países miembros signatarios se han sumado Austria, Dinamarca, Hungría, India, Israel, Japón (con la categoría de emisor de certificados), República Checa, República de Corea (con la categoría de emisor de certificados), República de Singapur, Suecia y Turquía.

  Así mismo, tres Países Miembros (España, Noruega y Países Bajos) han cambiado de su condición, para pasar a convertirse en países emisores de certificados.

- La aceptación de la industria, crece ininterrumpidamente, y de productos muy variados. Por ejemplo, entre las empresas que han obtenido certificados para sus productos en Alemania se encuentran Philips Semiconductors, Infineon Technologies, IBM como promotor de la certificación de Suse Linux Products, Microsoft Corporation, Sony Corporation y Sharp Corporation

- En adquisiciones públicas ciertos países imponen la certificación de la seguridad, como medio de cumplir ciertos requisitos legales (sobre protección de infraestructuras o servicios críticos o de protección de la privacidad).

  En nuestro país, los Criterios SNC se establecen a nivel de recomendación, por ejemplo para proteger la disponibilidad, integridad y la autenticación.

- Además de las administraciones públicas, la investigación, la docencia, la industria y los usuarios en general el interés es creciente.

  Así se pone de manifiesto en la nutrida asistencia a la Conferencia Internacional de Criterios Comunes, que se celebra cada año a continuación de la reunión del Comité de Gestión. Brece Schneier, experto mundial en seguridad, afirma que el *Arreglo* es "un paso en la dirección correcta", después de revisar las amenazas, vulnerabilidades de nuestra tecnología y de las políticas.

Reflejo del interés es también la aceptación del Portal en Internet del *Arreglo* (http://www.commoncriteriaportal.org) que junto a los enlaces a páginas de los Países miembros, supone una importante fuente de información.

7. PAÍSES PARTICIPANTES

- ALEMANIA
  Bundesamt für Sicherheit in der Informationstechnik

- AUSTRALIA Y NUEVA ZELANDA
  Defence Signals Directorate y Government Communication Security Bureau

- AUSTRIA
  Federal Ministry of Public Servic and Sports

- CANADÁ
  Communications Security Establishment

- DINAMARCA
  National IT-and Telecom. Agency

- ESPAÑA
  Ministerio de Administraciones Públicas y Centro Criptológico Nacional/Centro Nacional de Inteligencia

- ESTADOS UNIDOS DE AMÉRICA
  National Institute of Standards and Technology y National Security Agency

- FINLANDIA
  Ministry of Finance

- FRANCIA
  Direction Centrale de la Sécurité des Systèmes d'Information

- GRECIA
  Ministry of Interior

- HUNGRÍA
  Ministry of IT and Telecommunication

- INDIA
  Government of India Department of information technology

- ISRAEL
  Ministry of Industry and Trade

- ITALIA
  Autorità Nazionale per las Sicurezza
  OCSI – Organismo di Certificazione della Sicurezza Informatica

- JAPÓN
  Information Security Certification Office y Information Technology Promotion Agency (IPA)

- NORUEGA

HQ Defence Command Norway/ Security Division

- PAÍSES BAJOS
  Ministry of the Interior y Kingdom Relations

- REINO UNIDO
  Communications-Electronics Security Group y Department of Trade and Industry

- REPÚBLICA CHECA
  National Security Authority of the Czech Republic

- REPÚBLICA DE COREA
  The National Intelligence Service (NIS)

- SINGAPUR
  Infocomm Development Authority of Singapore (IDA)

- SUECIA
  SWEDAC (Swedish Board for Accreditation and Conformity Assessment)

- TURQUÍA
  TSE (Turkish Standards Institution)

8. ORGANISMOS DE CERTIFICACIÓN QUE CUMPLEN LOS REQUISITOS

Alemania
Bundesamt für Sicherheit in der Informationstechnik (Zertifizierungsstelle)
http://www.bsi.bund.de

Australia y Nueva Zelanda
Australasian Information Security Evaluation Programme
http://www.dsd.gov.au/infosec

Canadá
Canadian Common Criteria Evaluation and Certification Scheme
http://www.cse-cst.gc.ca/services/common-criteria/common-criteria-e.html

España
Organismo de Certificación de la Seguridad de las Tecnologías de la Información
Centro Criptológico Nacional - Centro Nacional de Inteligencia
http://www.oc.ccn.cni.es

Estados Unidos de América
National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme
http://niap.nist.gov/cc-scheme

Francia
Schema d'Evaluation et Certification Francais
http://www.ssi.gouv.fr

Japón
Japan Information Technology Security Evaluation and Certification Scheme (JISEC)
http://www.ipa.go.jp/security/jisec/jisec_e/index.html

Noruega
SERTIT (Norwegian Certification Authority for IT Security)
http://www.sertit.no

Países Bajos
TNO Certification
http://www.tno-certification.nl

Reino Unido
UK ITSec Scheme
http://www.cesg.gov.uk

República de Corea
IT Security Certification Center (ITSCC) - Korea IT Security Evaluation and Certification Scheme (KECS)
http://www.kecs.go.kr

Para solicitar información adicional puede dirigirse a:
Secretaría de SSITAD
secretaria.ssitad@map.es