Criterio común para evaluaciones de seguridad en tecnologías de la información

Common criteria for information technology security evaluation

Alina Surós Vicente, Adrián Alberto Machado Cento

Universidad de las Ciencias Informáticas

asuros, amachado@vnz.uci.cu

Resumen

Ante la necesidad de integrar los diferentes criterios que existían con respecto a la certificación de la seguridad en productos informáticos surge el Criterio Común para evaluaciones de seguridad en tecnologías de la información. Como resultado importante de los Criterio Común se encuentran los *Evaluation Assurance Levels*, que avalan a un producto de tecnologías de la información en el cumplimiento de las características de seguridad que corresponden al nivel obtenido (1-7). Para un software representa un valor agregado que se encuentre certificado en un nivel, pero indiscutiblemente los costos y el tiempo que demora alcanzar una certificación son factores que limitan la obtención de una certificación. En este trabajo se introducen los elementos fundamentales del Criterio Común, que pueden servir tanto a los desarrolladores como a los clientes de un sistema para evaluar la factibilidad de que su producto tenga una certificación de Criterio Común.

Palabras clave: Certificación, criterio común, seguridad informática.

Abstract

In spite of the need to integrate various criteria that existed related to certification security in computer products, emerges Common Criteria for information technology security evaluation. The Common Criteria allows comparing independent security evaluations results. Common Criteria is presented as a set of three chapters which include important components that serve to security requirements establishment process and it´s evaluation. It also presents seven pre-defined assurance packages which are called Evaluation Assurance Levels, ASCENDING from level 1 to 7.For software it represents an added value to be certificated at a level, but undeniably costs and time for obtaining a certificate are factors that should be considered to reach a certification. This work introduces the fundamentals of CC, which can serve both developers and customers of a system to evaluate the feasibility of having a certificated CC product.

Key words*: Certification, common criteria, information security.*

Introducción

El Criterio Común para Evaluaciones de Seguridad en Tecnología de la Información (*Common Criteria for Information Technology Security Evaluation*), abreviado como Criterio Común (*Common Criteria*) o CC, es el resultado final de importantes esfuerzos en el desarrollo de criterios de evaluación unificados para la seguridad de los productos de tecnologías de la información (IT) y ampliamente aceptado por la comunidad internacional.

A principios de los años 80, se desarrollaron en Estados Unidos los criterios de seguridad recogidos bajo el nombre de *Trusted Computer System Evaluation Criteria* (TCSEC) por sus siglas en inglés y editados en el famoso "libro naranja". En las décadas posteriores, varios países tomaron como base el TCSEC americano y evolucionaron las especificaciones para hacerlas mas flexibles y adaptables a la constante evolución de los sistemas de IT.De ahí la comisión europea, en el año 1991 publicó el ITSEC (*Information Technology Security Evaluation Criteria*), desarrollado conjuntamente por Francia, Alemania, Holanda y el Reino Unido. En Canadá, igualmente, se desarrollaron en 1993 los criterios CTCPEC (*Canadian Trusted Computer Product Evaluation*)

uniendo los criterios americanos y europeos. En ese mismo año el Gobierno americano publicó los *Federal Criteria* como una aproximación a unificar los criterios europeos y americanos.

Tal escenario comienza a aclararse con la decisión de estandarizar internacionalmente estos criterios para uso general, y en esa labor ISO comienza a trabajar a principios de los años 90 dando como resultado la certificación CC (o ISO-IEC 15408). Es el resultado de una laboriosa e intensa negociación entre países para obtener un acuerdo de reconocimiento mutuo de las certificaciones de seguridad de productos IT.

Establece 7 niveles (1-7), que corresponden a un grado numérico de cumplimiento de las evaluaciones en el ámbito de seguridad que establece el CC, estándar internacional desde 1999. Alcanzar altos niveles garantiza el cumplimiento de principios de seguridad. El nivel *Evaluation Assurance Levels* (EAL) no es una medida de la seguridad que posee el sistema, simplemente expresa el estado del nivel a que fue probado el sistema para determinar si cumple con todos los requerimientos de su *Protection Profile* (PP).

Para alcanzar un EAL particular, el sistema debe garantizar determinados requerimientos, tales como: documentación de diseño, diseño y análisis, pruebas funcionales o pruebas de penetración, a medida que se avanza en estos niveles se requiere de más detalles en la documentación y pruebas que en los niveles inferiores. Alcanzar niveles superiores de certificación EAL cuesta más dinero y tiempo. El número asignado indica que el sistema cumple con todos los requerimientos especificados para dicho nivel.

Aunque cada producto o sistema deba cumplir con los mismos requerimientos para un nivel particular, no significa que tenga los mismos requerimientos funcionales. Las características que deben poseer para cada certificación están establecidas en el *Security Target* (ST), documento adaptado para la evaluación del producto.

En este trabajo se muestran las principales características del CC, niveles de aseguramiento y costos necesarios para obtener una certificación que puedan servir tanto a desarrolladores de productos de tecnologías de información como a los clientes para determinar la factibilidad de obtener una certificación o solicitarla.

Materiales y métodos

Se realizó una búsqueda estructurada de los principales aspectos relacionados con el criterio común (partes integrantes del CC, niveles de garantía, ejemplos de productos certificados y costos) realizando una evaluación de los criterios de distintos autores y la factibilidad y necesidad para una empresa de desarrollo de productos de tecnologías de la información y de los clientes de obtener o exigir una certificación de este tipo.

Criterio común

Los CC están formados por tres partes, en la tabla 1 se muestra, según los tres grupos de audiencia del CC, cuáles son sus intereses en cada una de las partes.

Tabla 1. Intereses de la audiencia en las partes del CC

Parte	Consumidores	Desarrolladores	Evaluadores
1	Es usado a modo de información y como propósito de referencia. Guía para estructurar los PP	Es usado a modo de información y como propósito de referencia. Desarrollo de las especificaciones de seguridad para el TOE	Es usado a modo de información y como propósito de referencia. Guía para estructurar los *Protection Profile* (PP) y ST
2	Es usado par guía y referencia cuando se formulan los requerimientos del TOE	Es usado como referencia cuando se interpretan los requerimientos funcionales y se formulan las especificaciones funcionales para el TOE	Es usado como referencia cuando se interpretan los requerimientos funcionales
3	Es usado como guía cuando se determinan los requerimientos del nivel de garantía	Es usado como referencia cuando se interpretan los requerimientos de seguridad y se determinan los métodos de seguridad del TOE	Es usado cuando se interpretan los requerimientos de seguridad

Parte 1: Introducción y modelo general

Es una introducción al CC. Introduce los conceptos generales y principios de seguridad de las evaluaciones de seguridad y presenta un modelo general de evaluación.

Parte 2: Requerimientos de seguridad funcional

Estos requerimientos están destinados a los usuarios y desarrolladores, están organizados en once componentes, denominadas componentes de requerimientos funcionales y cada una de ellas cubre las necesidades de un área muy particular de la seguridad, a su vez, cada clase funcional se descompone en una o más familias funcionales, las cuales tratan de forma específica los diferentes aspectos que conforman en su totalidad a la clase en cuestión. Así, las familias funcionales contienen uno o más componentes, y cualquiera de ellos puede seleccionarse para incluirlo en el PP.

Componente FAU: Auditoría de seguridad

Auditar la seguridad involucra reconocimiento, registro, almacenamiento y análisis de información relacionada a las actividades relevantes de la seguridad. El resultado de los registros de auditoría puede ser examinado para determinar cuáles actividades relevantes de seguridad ocurrieron y qué usuario es responsable de ellas.

Componente FCO: Comunicación

Esta clase proporciona dos familias que aseguran la identidad de un grupo participante en el intercambio de datos. Estas familias están destinadas a garantizar la identidad del creador de la información transmitida (prueba de origen) y de igual forma, probar la identidad del receptor de la información transmitida (prueba de receptor). Estas familias aseguran que un creador no puede negar haber enviado el mensaje, ni el receptor puede negar haberlo recibido.

Componente FCS: Soporte de cifrado

Las funciones de seguridad del objeto de evaluación pueden emplear operaciones de cifrado para ayudar a satisfacer requerimientos de seguridad de alto-nivel. Estos incluyen: identificación y autenticación, no-repudio,

camino confiable, canal confiable y separación de datos. Esta clase se utiliza cuando el objeto de evaluación implanta funciones de cifrado, la implantación de las cuales podría ser en hardware, firmware y/o software.

Componente FDP: Protección de datos de usuario

Esta clase contiene familias relacionadas con los requisitos para las funciones de seguridad del objeto de evaluación y las políticas de función de seguridad relacionadas a la protección de datos de usuario. FDP está dividida en cuatro grupos que se refieren a los datos de usuario dentro de un objeto de evaluación, durante la importación, exportación, y almacenamiento así también como los atributos de seguridad directamente relacionados a los datos de usuario.

Componente FIA: Identificación y autenticación

Esta clase está dedicada a los requerimientos de funciones para establecer y verificar una identidad de usuario. La identificación y autenticación es un requisito para asegurar que los usuarios están asociados con los atributos de seguridad apropiados (niveles de identidad, grupos, funciones, de seguridad o integridad), por lo que es de suma importancia la identificación sin ambigüedades de usuarios autorizados, y la asociación correcta de atributos de seguridad con usuarios y sujetos, ya que es fundamental para la puesta en marcha de las políticas de seguridad definidas.

Componente FMT: Administración de la seguridad

Esta clase se ha desarrollado para especificar la administración de varios aspectos de las funciones de seguridad de los objetos de evaluación: atributos de seguridad, datos de las funciones de seguridad, y las funciones mismas. Los diferentes perfiles de la administración y su interacción pueden especificarse, tales como la separación de capacidades (acciones posibles). Así, esta clase tiene varios objetivos: administración de datos de las funciones de seguridad, administración de atributos de seguridad, administración de funciones de seguridad, definición de perfiles de seguridad.

Componente FPR: Privacidad

Esta clase contiene los requerimientos de privacidad, los cuales proporcionan a un usuario protección contra la revelación y mal uso de la identidad por parte de otros usuarios.

Componente FPT: Protección de las funciones de seguridad del objeto de evaluación

Esta clase contiene familias de requerimientos funcionales que relacionan la integridad y la administración de los mecanismos que proporcionan las funciones de seguridad del objeto de evaluación (independientemente de las políticas de seguridad específicas) y a la integridad de los datos de las funciones de seguridad (independientemente de los contenidos específicos de los datos de las políticas de seguridad). En cierto sentido, puede parecer que las familias en esta clase duplican componentes de la clase Protección de datos de usuario (FDP), las cuales pueden ser regularmente implantadas usando los mismos mecanismos, no obstante, FDP se enfoca a la protección de datos de usuario, mientras que FPT se enfoca a la protección de datos de las funciones de seguridad del objeto de evaluación, de hecho, los componentes de la clase FPT son necesarios para proporcionar requerimientos de las políticas de seguridad en el objeto de evaluación y que no pueden ser alteradas o eludidas. Los datos de las funciones de seguridad, son la base de los datos administrativos y son éstos los que se refieren a la puesta en vigor de las políticas de seguridad.

Componente FRU: Utilización de recursos

Esta clase proporciona tres familias que fundamentan la disponibilidad de recursos requeridos tales como, capacidad de procesamiento y capacidad de almacenamiento.

Componente FTA: Acceso a la TOE

Esta clase especifica los requerimientos funcionales para controlar el establecimiento de una sesión de usuario.

Componente FTP: Caminos/canales confiables

En esta clase se proporcionan los requerimientos necesarios para establecer un camino de comunicación confiable entre los usuarios y las funciones de seguridad, y de igual forma un canal de comunicación confiable entre las funciones de seguridad y otros productos IT. En este paradigma, un canal confiable es un canal de comunicación que puede ser iniciado por ambos extremos del canal, y proporciona características de no-repudio con respecto a la identidad de los extremos del canal. En tanto que un camino confiable es aquel que proporciona un medio para que los usuarios ejecuten funciones a través de la interacción directa garantizada con las funciones de seguridad. Los caminos confiables usualmente se emplean para que el usuario realice actividades de identificación inicial o autenticación. Además, los intercambios vía un camino confiable pueden ser iniciados por un usuario o por funciones de seguridad.

Parte 3: Requerimientos de garantía de seguridad

Esta parte está destinada a los desarrolladores IT ya que define el criterio de confiabilidad que los evaluadores usan para verificar el desempeño de los desarrolladores y sus productos. Introduce siete niveles de evaluación de garantía (*Evaluation Assurance Level - EAL*) que define la escala de los CC para clasificar la evaluación obtenida por los productos. La evaluación ha sido el medio tradicional de obtener la garantía, y es la base de la aproximación de los CC. Las evaluaciones técnicas pueden incluir, pero no estar limitadas a: análisis y verificación de procesos y procedimientos, verificar qué procesos y procedimientos están siendo aplicados, análisis de la correspondencia entre las representaciones de diseño del objeto de evaluación, análisis de la representación del diseño del objeto de evaluación en comparación con los requerimientos, verificación de demostraciones, análisis de documentos guía, análisis de pruebas funcionales desarrolladas y los resultados proporcionados, prueba funcional independiente, análisis de vulnerabilidades (incluyendo hipótesis sobre defectos).

Los requerimientos de garantía son aquellos que se consideran necesarios para garantizar la seguridad que brinda el objeto de evaluación, estos requerimientos están organizados en siete clases, denominadas clases de garantía y cada clase a su vez se descompone en una o más familias de garantía en una estructura similar a los requerimientos funcionales; adicionalmente, esta parte proporciona niveles de garantía (EALs), de manera que el nivel seleccionado corresponde a uno de los 7 EALs clasificados por CC y al grado de seguridad requerido para el objeto de evaluación.

Componente ACM: Administración de la configuración

Esta clase permite asegurar que se ha preservado la integridad del objeto de evaluación mediante el requerimiento de disciplina y control en los procesos de refinamiento y modificación del objeto de evaluación y cualquier otra información relacionada; asimismo, previene de modificaciones no autorizadas, adiciones o supresiones al objeto de evaluación, y de esta manera, se garantiza que el objeto de evaluación y la documentación empleada para su evaluación están listas para ser distribuidas.

Componente ADO: Distribución y operación

Esta clase define los requerimientos para las medidas, procedimientos y estándares relacionados con la distribución segura, instalación y uso operacional del objeto de evaluación, asegurando que la protección de seguridad ofrecida por el objeto de evaluación no ha sido comprometido durante su transferencia, instalación, inicialización, y operación.

Componente ADV: Desarrollo

Esta clase define los requerimientos para el refinamiento de las funciones de seguridad paso a paso, desde la especificación del objeto de evaluación hasta llegar a su implantación actual. Cada una de las representaciones de las funciones de seguridad resultantes proporciona información para ayudar al evaluador a determinar si los requerimientos funcionales del objeto de evaluación fueron considerados y reunidos.

Componente AGD: Documentos guía

La clase de garantía AGD define requerimientos que se refieren a la comprensión, la cobertura y el completamiento de la documentación operacional proporcionada por el desarrollador. Esta documentación, proporciona dos categorías de información, para usuarios y para administradores, las cuales son un factor importante en la operación segura de un objeto de evaluación.

Componente ALC: Soporte del ciclo de vida

Esta clase define requerimientos de garantía a través de la adopción de un modelo de ciclo de vida bien definido para todos los pasos del desarrollo del objeto de evaluación, incluyendo procedimientos y políticas que permitan solucionar posibles fallas o daños, técnicas para el correcto uso de herramientas y las medidas de seguridad usadas para proteger el entorno de desarrollo.

Componente ATE: Pruebas

La clase de garantía ATE indica los requerimientos de prueba que demuestran que las funciones de seguridad satisfacen los requerimientos funcionales de seguridad del objeto de evaluación.

Componente AVA: Evaluación de la vulnerabilidad

Esta clase define los requerimientos que se refieren a la identificación de vulnerabilidades explotables. Específicamente, se refiere a aquellas vulnerabilidades introducidas en la construcción, operación, mal uso, o configuración incorrecta del objeto de evaluación.

Niveles de garantía

Los niveles de garantía (EALs) proporcionan una escala creciente que compara el nivel de garantía obtenido con el costo y la viabilidad de adquirir ese grado de garantía. Es importante hacer notar que no todas las familias y componentes de la parte 3 de CC están incluidos en los EALs, esto no quiere decir que no proporcionan garantías deseables y significativas, en su lugar, se espera que estas familias y componentes sean considerados para aumentar un EAL en aquellos PPs para los cuales proporcionan utilidad.

Los CC definen siete niveles de garantía de evaluación ordenados jerárquicamente para la valoración de un objeto de evaluación, y los niveles están ordenados jerárquicamente puesto que cada EAL representa una garantía mayor que todos los EALs inferiores. El incremento de garantía de un EAL al siguiente EAL se realiza por sustitución de un componente de garantía jerárquicamente superior de la misma familia de garantía (incrementando rigor, ámbito, o profundidad) y de la adición de componentes de garantía de otras familias de garantía (que adicionen nuevos requerimientos). A continuación se proporcionan definiciones de los EALs.

Los niveles de garantía son:

EAL_1 (Funcionalidad probada): es aplicable donde se requiere tener cierta confianza de la operación correcta y donde además, las amenazas a la seguridad no son vistas como serias. Una evaluación en este nivel debe proporcionar evidencia de que las funciones del objeto de evaluación son consistentes con su documentación, y que proporcionan protección útil contra amenazas identificadas.

EAL_2 (Estructuralmente probado): requiere la cooperación del desarrollador en términos de la distribución de la información del diseño, y los resultados de las pruebas, pero no debe demandar más esfuerzo por parte del desarrollador que el que sea consistente con una buena práctica comercial. De tal manera que no debe requerir una inversión sustancialmente mayor en costo o tiempo.

AL_3 (Probado y verificado metódicamente): permite a un desarrollador aplicado y minucioso, alcanzar una máxima garantía de ingeniería de seguridad positiva en el estado de diseño sin la alteración substancial de prácticas de desarrollo válidas existentes.

EAL_4 (Diseñado, probado y revisado metódicamente): este nivel le permite a un desarrollador alcanzar máxima garantía de ingeniería de seguridad positiva basada en buenas prácticas de desarrollo comercial, las cuales, aunque rigurosas, no requieren del conocimiento especializado substancial, destreza, y otros recursos. Es el nivel menos alto y el más probable de ser económicamente factible para ser utilizado y actualizado por medio de adaptaciones hacia una línea de producto ya existente.

EAL5 (Diseñado y probado semiformalmente): permite a un desarrollador alcanzar máxima garantía de ingeniería de seguridad positiva con base en prácticas rigurosas de desarrollo comercial, esto, mediante la aplicación moderada de técnicas de ingeniería de seguridad. Así un objeto de evaluación probablemente será diseñado y desarrollado con la intención de obtener un nivel EAL_5.

EAL_6 (Diseño verificado y probado semiformalmente): permite a los desarrolladores alcanzar una alta garantía en la aplicación de técnicas de ingeniería de seguridad para un entorno de desarrollo riguroso y donde el objeto de evaluación es considerado de gran valor para la protección del alto costo o estimación de esos bienes contra riesgos significativos. Además, es aplicable para el desarrollo de objetos de evaluación, destinados a resguardar la de seguridad informática en situaciones de alto riesgo donde el valor de los bienes protegidos justifica los costos adicionales.

EAL_7 (Diseño verificado y probado formalmente): es aplicable al desarrollo de objetos de evaluación de seguridad, para su aplicación en situaciones de muy alto riesgo o donde el alto valor de los bienes justifica los más altos costos. La aplicación práctica del nivel EAL_7 está limitada actualmente a objetos de evaluación con seguridad estrechamente enfocada a la funcionalidad, y que es sensible al análisis formal y extenso. Este EAL representa un incremento significativo respecto a la garantía de nivel EAL_6 a través del requerimiento de análisis de gran amplitud, mediante representaciones formales y correspondencia formal y pruebas de gran amplitud.

Ejemplo de certificaciones

Microsoft

Los productos de Microsoft que han obtenido la certificación con nivel EAL4 son *Windows Server* 2003 (cuatro ediciones), *Windows XP* (dos versiones), *MS Exchange Server* SP1, *MS ISA Server* 2004 y *Certificate Server*. Según Héctor Sánchez, director de seguridad corporativa de Microsoft Ibérica, a su juicio, *Comon Criteria* aporta "un criterio de objetividad" al discurso de la seguridad y "demuestra en especial el compromiso de Microsoft con la seguridad informática".

Linux

En enero de 2004 SuSE, que ya en 2002 obtuvo el EAL2, conseguía EAL3. Fue entonces cuando por primera vez un sistema Linux obtuvo esa puntuación de la *Common Criteria Organtization*. La certificación sólo incluía a la distribución SuSE instalada bajo una determinada línea de sistemas IBM. *Red Hat Enterprise Linux* también está certificado bajo servidores IBM.

SecureWave

SecureWave, especializado en seguridad en puntos de acceso, su solución tecnológica Sanctuary® recibió la certificación de criterio común (CC) en Evaluación de Garantía Nivel 2 (EAL). Antes de recibir dicha certificación, Sanctuary de *SecureWave* completó una rigurosa evaluación de parte de *Science Applications International Corporation* (SAIC), un laboratorio independiente acreditado para verificar los requisitos del Estándar de Criterio Común ISO 15408 en cuestiones de evaluaciones de Seguridad en Tecnología de la Información.

Costos

En la segunda mitad de 1990s, vendedores reportaron que gastaron entre 1 y 2,5 millones de dólares en evaluaciones EAL 4.

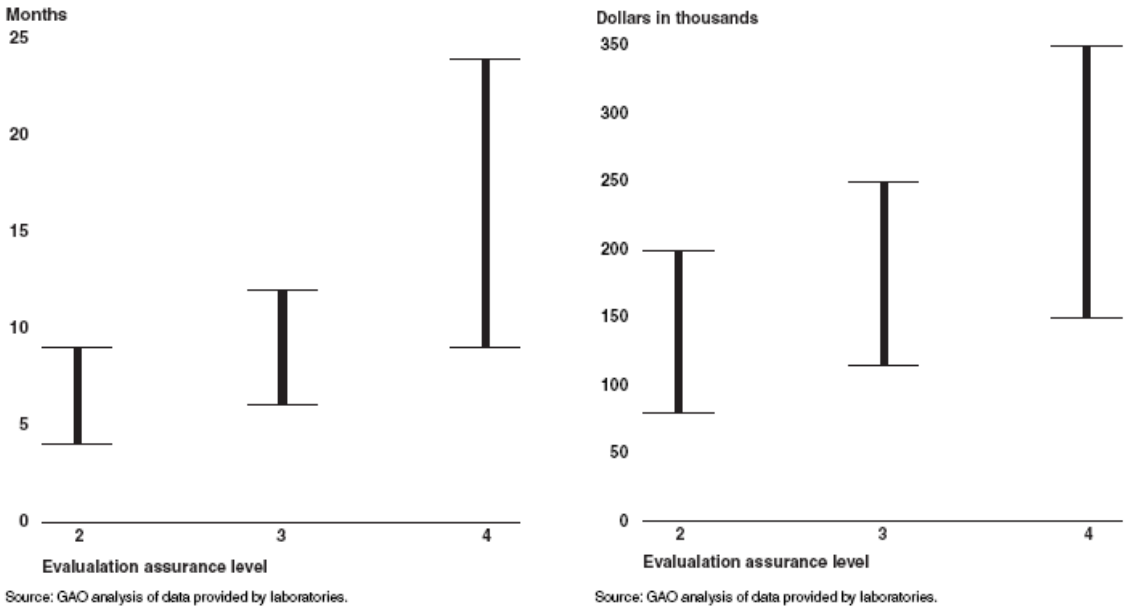

Fig. 1. Costos en tiempo y dinero de la evaluación de los niveles 2 al 4

Conclusiones

El CC proporciona una vía para asegurar que las características de seguridad que contiene un producto de IT, son reales y se corresponden con las declaradas por el fabricante. Contar con esta certificación representa una ventaja competitiva.

Antes de someter a un producto a una certificación CC, es de vital importancia realizar la evaluación de costo beneficio, pues es un proceso costoso en tiempo y dinero. El CC, permite contar con criterios comunes para el desarrollo y la evaluación de esquemas de seguridad informática, que permitan hacer uso de la misma métrica en todos los sistemas y productos en los que se requiere seguridad IT.

Referencias Bibliográficas

http://en.wikipedia.org/wiki/Evaluation_Assurance_Level

http://www.atsec.com/04/index.php?id=06-0001-03

http://www.mtbase.com/contenido/documento.jsp?id=10225

http://www.noticias.info/archivo/2005/200512/20051216/20051216_128841.shtm

http://bulma.net/body.phtml?nIdNoticia=2101

http://www.hispasec.com/unaaldia/2653

http://www.atsec.com/04/index.php?id=06-0002-03

http://www.atsec.com/04/index.php?id=02-0001-01

http://www.fi-p.unam.mx/simposio_investigacion2005/ponencia6_ext.html

http://mx.sun.com/sunnews/press/2005/20051026.html

http://www.microsoft.com/latam/windowsserversystem/hechos/analyses/ccwp.mspx

http://www.financialtech-mag.com/000_estructura/index.php?id=24&idb=64&ntt=4278&sec=8&vn=1

http://en.wikipedia.org/wiki/Common_Criteria

http://www.commoncriteriaportal.org/

http://www.zonagratuita.com/servicios/seguridad/art-esp11.html

http://www.csi.map.es/