Presentación de un Framework de Evaluación de la Seguridad de productos y servicios de las Tecnologías de la Información de acuerdo a las normas Common Criteria

Eterovic, Jorge Esteban
Donadello, Domingo
Universidad Nacional de La Matanza,
Departamento de Ingeniería e Investigaciones Tecnológicas

Abstract

La masiva utilización de las Tecnologías de la Información (TI) en particular para los países de la Comunidad Europea, Australia, Canadá y Estados Unidos, obliga a las empresas de software que necesiten exportar a esos países, certificar la seguridad del software bajo el estándar de los COMMON CRITERIA o su equivalente ISO/IEC 15408.
Para la evaluación de la seguridad de productos y servicios de TI, a efectos de garantizar un adecuado nivel de seguridad en su utilización, se debe desarrollar un procedimiento que verifique el cumplimiento de siete niveles de evaluación denominados EAL (Evaluation Assurance Level) que garantizan la seguridad en la operación controlada de los productos y servicios de TI.
En éste artículo se presenta el análisis de un framework para evaluar productos y servicios bajo el estándar ISO/IEC 15408 o Common Criteria.

Palabras Clave

Common Criteria. ISO/IEC 15408; Seguridad de productos y servicios de TI; Evaluación de la Seguridad de las Tecnologías de la Información; Niveles de evaluación de seguridad - EAL.

Introducción

La utilización de las Tecnologías de la Información (TI) en amplias áreas de la actividad de las organizaciones, así como la creciente participación de Argentina en proyectos de desarrollo de la sociedad de la información de carácter internacional, imponen la necesidad de garantizar un adecuado nivel de seguridad en la utilización de las TI.
Por lo tanto, la seguridad que las TI deben poseer, debe abarcar la protección de la confidencialidad, la integridad y la disponibilidad de la información que manejan los sistemas de información, así como la integridad y disponibilidad de los propios sistemas.
La garantía de seguridad de las Tecnologías de la Información debe estar basada en el establecimiento de mecanismos y servicios de seguridad, adecuadamente diseñados, que impidan la realización de funciones no deseadas.
Uno de los métodos, admitido internacionalmente, para garantizar la corrección y efectividad de dichos mecanismos y servicios, consiste en la evaluación de la seguridad de las TI, realizada mediante la utilización de criterios rigurosos tales como los Common Criteria [1] o su equivalente ISO/IEC 15408 [2], con posterior certificación de un Organismo de Certificación legalmente establecido, como por ejemplo el Instituto Argentino de Normalización y Certificación – IRAM [3].
Para ello es necesario contar con un marco que regule los procesos de Evaluación de la Seguridad de las Tecnologías de la Información.
La carencia de un framework de éstas características, es un obstáculo importante para la difusión y aceptación generalizada de la importancia de la evaluación y posterior certificación de los diferentes productos y servicios de las Tecnologías de la Información desarrollados en nuestro país con destino a los mercados de la Comunidad Europea, Australia, Canadá y Estados Unidos.
En el contexto de las naciones no se pueden aceptar criterios de evaluación de la seguridad de las TI que no sean

homologables con los de los otros países participantes. Por ello, es necesaria la adopción de criterios internacionales, que permitan negociar el reconocimiento mutuo de certificados, resultando esencial que los Procedimientos de Evaluación se equiparen a los del resto de los países [4].

Elementos del Trabajo y metodología

El Organismo de Certificación certificará la seguridad de los productos y servicios de Tecnologías de la Información, siguiendo un procedimiento ad-hoc y tras considerar el cumplimiento del procedimiento y los informes de evaluación emitidos por un Laboratorio de Certificación, acreditado conforme a lo establecido en los criterios, métodos y normas de evaluación de la seguridad indicados en las normas Common Criteria.

La certificación de la seguridad de un producto o servicio de las Tecnologías de la Información supone el reconocimiento de la veracidad de las propiedades de seguridad de su correspondiente declaración de seguridad.

La certificación de la seguridad de un producto o servicio no presupone declaración de idoneidad de uso en cualquier escenario o ámbito de aplicación. Para valorar la idoneidad de un producto o servicio deberán tenerse en cuenta otras circunstancias, incluidas las restricciones establecidas en su declaración de seguridad, para la correcta interpretación del certificado.

La certificación, una vez concedida, se mantiene de manera indefinida, salvo cambios en las condiciones que motivaron su concesión, tales como avances tecnológicos, aparición de nuevas vulnerabilidades explotables, incumplimiento de las condiciones de uso del certificado, cambios en el propio producto o renuncia expresa del solicitante.

Para la vigilancia de la vigencia de la certificación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del producto, de su entorno y del uso del certificado.

La certificación se limita mediante el correspondiente alcance, que incluye la definición del producto evaluado y las normas y niveles de evaluación.

El Organismo de Certificación, en la determinación del alcance, realizará la definición más precisa posible del mismo, con el objeto de evitar confusión alguna entre el producto comercial y el producto evaluado, en el supuesto de que ambos no coincidan exactamente.

La certificación deberá hacer referencia, e identificar inequívocamente, al producto evaluado, así como a su declaración de seguridad.

Dicha declaración de seguridad también deberá contener la identificación precisa del producto evaluado, así como la especificación de su entorno de uso, incluyendo las amenazas previstas, políticas de seguridad e hipótesis aplicables al caso, además de los objetivos de seguridad del producto o servicio y la relación de requisitos de seguridad exigibles al mismo.

Los detalles de la declaración de seguridad podrán variar conforme a las normas aplicadas en la evaluación, pero toda declaración deberá ser un reflejo cierto, claro y preciso de las propiedades de seguridad del producto o servicio evaluado.

La certificación incluirá en su alcance los criterios, métodos y normas de evaluación empleados en la evaluación del producto o servicio, así como el nivel que se haya alcanzado, de los definidos en cada norma, y la relación de interpretaciones e instrucciones técnicas aplicadas.

La principal prueba en la instrucción del procedimiento de certificación es el Informe Técnico de Evaluación, emitido por el Laboratorio de Certificación acreditado y realizado cumpliendo en un todo con el procedimiento de certificación.

Se describen los principales conceptos que deberían ser considerados por las entidades públicas o privadas que deseen evaluar y eventualmente luego certificar la seguridad

de un producto o servicio de Tecnologías de la Información.

Procedimientos normalizados

La norma Common Criteria define un criterio estándar a usar como base para la evaluación de las propiedades y características de seguridad de determinado producto o servicio de TI. Ello permite la equiparación entre los resultados de diferentes e independientes evaluaciones, al proporcionar un marco común con el que determinar los niveles de seguridad y confianza que implementa un determinado producto o servicio en base al conjunto de requisitos de seguridad y garantía que satisface respecto a esta norma, obteniendo de esa forma una certificación oficial del nivel de seguridad que satisface.

Por lo tanto, a partir de la norma se han establecido los criterios de evaluación basados en un análisis riguroso del producto o servicio de TI a evaluar y los requisitos que este satisface.

Para ello, se establece una clasificación jerárquica de los requisitos de seguridad y se determinan diferentes tipos de agrupaciones de los requisitos en forma jerárquica, de la siguiente manera:

- **Clase**: conjunto de familias que comparten un mismo objetivo de seguridad.
- **Familia**: un grupo de componentes que comparten objetivos de seguridad pero con diferente énfasis o rigor.
- **Componente**: un pequeño grupo de requisitos muy específicos y detallados. Es el menor elemento seleccionable para incluir en los documentos de Perfiles de Protección (PP) y Especificación de Objetivos de Seguridad (ST).

Si tomamos, por ejemplo, los requisitos de seguridad relacionados con la autenticación [5], la clasificación jerárquica sería:

- **Clase**: Identificación y autenticación
- **Familias de la clase**:
  - Fallos de autenticación
  - Definición de atributos de usuario
  - Autenticación de usuario
  - Identificación de usuario
- **Componentes** de la familia Autenticación de usuario:
  - Tiempo de espera para la autenticación
  - Acciones antes de autenticar
  - Mecanismos de autenticación simple.
  - Mecanismos de autenticación múltiple.

Luego se definen los principios y conceptos generales de la evaluación de la seguridad en tecnologías de la información y se presenta el modelo general de evaluación. También se establece cómo se pueden realizar las especificaciones formales de productos o servicios de TI atendiendo a los aspectos de seguridad de la información [6], y su tratamiento. Éstas pueden ser en función de:

- **Perfil de Protección (PP - Protection Profile):** En un conjunto de requisitos funcionales y de garantías independientes de implementación dirigidos a identificar un conjunto determinado de objetivos de seguridad en un determinado dominio.

  Especifica de forma general qué se desea y necesita respecto a la seguridad de un determinado dominio de seguridad. Ejemplos podrían ser PP sobre un firewall, PP sobre un sistema de control de accesos, etc.
- **Objetivo de Seguridad (ST - Security Target):** Consiste en un conjunto de requisitos funcionales y de garantías usados como especificaciones de seguridad de un producto o servicio concreto.

  Especifica qué requisitos de seguridad proporciona o satisface un producto o servicio, basado en su implementación. Por ejemplo podrían ser ST para CheckPoint Firewall-1, para Oracle v.7, etc.

A continuación se definen los Requisitos Funcionales de Seguridad. Estos Requisitos Funcionales de Seguridad definen un

comportamiento deseado en materia de seguridad de un determinado producto o servicio de TI y se agrupan en clases.
Se consideran las siguientes clases:

- **FAU** - Auditoria
- **FCO** - Comunicaciones
- **FCS** - Soporte criptográfico
- **FDP** - Protección de datos de usuario
- **FIA** - Identificación y autenticación de usuario
- **FMT** - Gestión de la seguridad
- **FPR** - Privacidad
- **FPT** - Protección de las funciones de seguridad del objetivo a evaluar
- **FRU** - Utilización de recursos
- **FTA** - Acceso al objetivo de evaluación
- **FTP** - Canales seguros

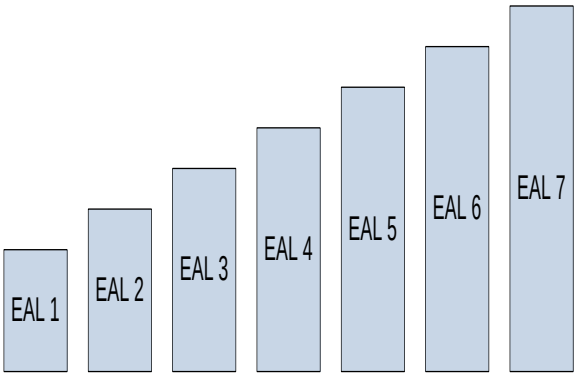
Resulta necesario definir los Requisitos de Garantía de Seguridad. Estos tipos de requisitos de Garantía de Seguridad establecen los niveles de confianza que ofrecen las funciones de seguridad del producto o servicio.
Entonces se trata de evaluar qué garantías proporciona el producto o servicio en base a los requisitos que se satisfacen a lo largo del ciclo de vida del producto o servicio. Contiene las siguientes clases:

- **ACM** - Gestión de la configuración
- **ADO** - Operación y entrega
- **ADV** - Desarrollo
- **AGD** - Documentación y guías
- **ALC** - Ciclo de vida
- **ATE** - Prueba
- **AVA** - Evaluación de vulnerabilidades
- **APE** - Evaluación de Perfiles de Protección (PP)
- **ASE** - Evaluación de Objetivos de Seguridad (ST)
- **AMA** - Mantenimiento de garantías

Finalmente, la norma Common Criteria, proporcionan también los Niveles de Garantía (EAL) como resultado final de la evaluación.
Estos Niveles de Garantía consisten en agrupaciones de los requisitos vistos anteriormente en un paquete, de forma que obtener un cierto Nivel de Garantía equivale a satisfacer por parte del Objetivo de Evaluación (TOE) ciertos paquetes de Requisitos de acuerdo con lo especificado en la norma ISO/IEC 18045 [7].
Se pueden realizar dos tipos diferentes de evaluación:

- **Evaluación de Perfiles de Protección (PP):** El objetivo de esta evaluación es demostrar que un PP es completo, consistente y técnicamente sólido.
  Podrá ser utilizado como base para establecer requisitos destinados a definir un Objetivo de Seguridad (ST). Es una herramienta muy útil, ya que permite definir especificaciones de seguridad independientes de la implementación, que pueden ser utilizadas como base de especificaciones para productos o servicios.
- **Evaluación de los Objetivos de Evaluación (TOE):** Utilizando un Objetivo de Seguridad (ST) previamente evaluado como base, el Objetivo de la Evaluación es demostrar que todos los requisitos establecidos en el ST se encuentran implementados en el producto o servicio de TI.

Como resultado de la evaluación, se pueden certificar distintos Niveles de Seguridad (EAL). Gráficamente podemos representar los siete niveles de seguridad de la siguiente manera:



Los siete niveles de seguridad son:

EAL 1. Probado funcionalmente

Proporciona un nivel básico de seguridad realizado a través del análisis de las funciones de seguridad usando especifica-

ciones informales de aspectos funcionales, de interfaz y las guías y documentación del producto o servicio de TI para entender el comportamiento de seguridad. Es aplicable cuando se requiere confianza en la correcta operación, pero las amenazas de seguridad no se contemplan como un peligro serio.
Este tipo de evaluación proporciona evidencias de que las funciones de seguridad de los Objetivos de Evaluación (TOE) se encuentran implementadas de forma consistente con su documentación y que proporcionan una protección adecuada contra las amenazas identificadas.

EAL 2. Probado estructuralmente

Exige, además de los requisitos del nivel anterior, haber realizado una descripción informal del diseño detallado, haber realizado pruebas en el desarrollo en base a las especificaciones funcionales, una confirmación independiente de esas pruebas, un análisis de la efectividad de las funciones de seguridad implementadas y evidencias de que el desarrollo ha verificado la respuesta del producto o servicio de TI a las vulnerabilidades más comunes.
Requiere de la cooperación del equipo de desarrollo para que entregue información sobre el diseño y resultados de pruebas de testing.
Este tipo de evaluación es adecuado en circunstancias en donde los desarrolladores o usuarios requieren cierto nivel de garantías de seguridad cuando no tienen acceso a toda la documentación generada en la fase de desarrollo.

EAL 3. Probado y comprobado metodológicamente

Este nivel establece unos requisitos que obligan, en la fase de diseño, a un desarrollo metodológico determinando.
Este nivel añade, a los requisitos del nivel anterior, el uso de controles de seguridad en los procesos de desarrollo, para que garanticen que el producto no ha sido manipulado durante su desarrollo.
Por lo tanto, se realiza un análisis de las funciones de seguridad en base a las especificaciones funcional de alto nivel, la documentación, las guías de uso del producto y los test obtenidos en la fase de prueba.

EAL 4. Diseñado, revisado y probado metodológicamente

Requiere, además de los requisitos del nivel anterior, un análisis de vulnerabilidades independiente [8], que demuestre resistencia a intrusos con bajo potencial de ataque y una especificación de bajo nivel del diseño de la implementación.

EAL 5. Diseñado y probado semi-formalmente

Representa un cambio significativo respecto al nivel anterior puesto que requiere de descripciones semi-formales del diseño y la arquitectura, y tener completa la documentación de la implementación.
Además se realiza un completo análisis de vulnerabilidades que pruebe la resistencia frente atacantes de potencial medio y mejora los mecanismos de control para garantizar y demostrar que el producto no es manipulado con respecto a las especificaciones durante el desarrollo.

EAL 6. Diseñado, verificado y probado semi-formalmente

Añade, respecto a los requisitos del nivel anterior, un detallado análisis de las funciones de seguridad, una representación estructurada de su implementación y una semi-formal demostración de la correspondencia entre las especificaciones de alto y bajo nivel con la implementación.
Además, debe demostrarse con un análisis de vulnerabilidades independiente, que en el desarrollo se ha probado la robustez de las funciones de seguridad frente a atacantes de alto potencial de daño.

EAL 7. Diseñado, verificado y probado formalmente

Es el nivel de certificación más alto. Deben probarse formalmente las fases de desarrollo y prueba.

Además se exige una evaluación independiente de la confirmación de los resultados obtenidos, de las pruebas para detectar vulnerabilidades durante la fase de desarrollo, así como sobre la robustez de las funciones de evaluación.

Además, deberá realizarse un análisis independiente de vulnerabilidades para demostrar resistencia frente a un atacante de alto potencial de daño.

Resultados

Para establecer de forma estándar un criterio de evaluación de la seguridad de los productos y servicios de TI, la medición se realiza en base a un conjunto de requisitos y la demostración que éstos son satisfechos.

Los resultados esperados desde las evaluaciones de Perfiles de Protección (PP) y Objetivos de Seguridad / Objetivos de Evaluación (ST/TOE) realizados según la norma ISO/IEC 18045 son:

- Evaluaciones de los Perfiles de Protección que conducen a catálogos de PP evaluados
- Evaluaciones de Objetivos de Seguridad que conducen a resultados intermedios que serán usados en el marco de una evaluación de los Objetivos de Evaluación (TOE).

El Framework del proceso de evaluación, que se muestra en la Figura 1, comienza con la definición de los Perfiles de Protección del objeto a evaluar

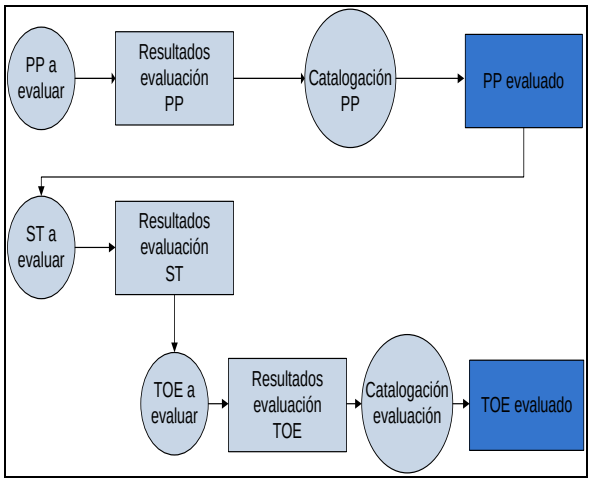


Figura 1

Los resultados de la evaluación producen catálogos de los Perfiles de Protección (PP) evaluados. La norma ISO/IEC 15408-3 contiene los criterios de evaluación que un evaluador está obligado a consultar con el fin de declarar si el PP es completo, coherente y técnicamente correcto y por lo tanto adecuado para su uso en el desarrollo de un Objetivo de Seguridad (ST).

Los Objetivos de Seguridad pueden estar basados en paquetes, en PP evaluados o en PP no evaluados. Las evaluaciones de los Objetivos de Seguridad / Objetivos de Evaluación (ST/TOE) producen catálogos de TOEs evaluados.

En muchos casos estos catálogos se referirán a productos y servicios de TI del cual se deriva el TOE, en lugar de un Objetivo de Evaluación específico.

Por lo tanto, la existencia de un producto o servicio de TI en un catálogo, no debe interpretarse en el sentido de que la totalidad del producto o servicio de TI ha sido evaluado. En su lugar, el alcance real de la evaluación ST/TOE se define por el Objetivo de Seguridad (ST).

Los resultados de esta evaluación también deberán incluir una "declaración de conformidad ISO/IEC 15408" que indica la fuente de la colección de requerimientos que son satisfechos por un Perfil de Protección (PP) o por un Objetivo de Seguridad (ST) que ha pasado la evaluación.

Los resultados de la evaluación se pueden utilizar posteriormente en un proceso de certificación.

Discusión

Los niveles de certificación podrían especificar los mínimos exigibles para la selección y adquisición de productos y servicios de TI.
Por otro lado, la creación de diferentes Perfiles de Protección (PP) para diversos entornos de seguridad proporcionará la información de conjuntos de especificaciones técnicas que permitirán establecer los requisitos mínimos que se deberían incorporar a futuros desarrollos, permitiendo establecer los requisitos de seguridad en las fases de diseño de productos y servicios de TI.
Todo ello contribuirá, seguramente, al incremento de la calidad y seguridad de los diferentes productos y servicios de TI, y por añadidura, al incremento de la confianza que debería depositarse en ellos.

Conclusión

Una conclusión importante a la que se arribó, luego del análisis del Framework para la Evaluación de productos y servicios de TI, es que sería el primer paso necesario para la posterior certificación mediante la norma ISO/IEC 15408, que es el estándar internacional que permite evaluar bajo criterios rigurosos y estrictos qué protecciones en materia de seguridad nos asegura un determinado producto o servicio de TI.
Los acuerdos firmados por diferentes países, permiten el reconocimiento mutuo de las certificaciones realizadas en los diferentes Organismos de Certificación locales reconocidos internacionalmente.
Esto facilita que los principales fabricantes de productos y servicios de TI puedan evaluar y certificar sus productos para proporcionar "valor añadido" en la confianza y seguridad que en ellos se puede depositar, lo que los hace altamente competitivos a nivel mundial.
Finalmente se debe destacar la importancia de contar a futuro con una norma argentina, adoptada a partir de las ISO/IEC 15408, para difundir adecuadamente y promover en el mercado de las empresas locales que exportan, la importancia de certificar sus productos y servicios bajo estos estándares.

Referencias

1. Common Criteria for Information Technology Security Evaluation; Version 3.1; Revision 3 Final; July 2009.
2. Common Criteria for Information Technology Security Evaluation, Evaluation methodology; Version 3.1; Revision 3 Final; July 2009. (Common Evaluation Methodology,) release 3.
3. IRAM – Instituto Argentino de Normalización; www.iram.org.ar
4. International Organization for Standardization ISO/IEC 15408-1; Information Technology — Security techniques — Evaluation criteria for IT security part 1: Security functional requirements; Ginebra, Suiza; ISO, 2005.
   International Organization for Standardization ISO/IEC 15408-2; Information Technology — Security techniques — Evaluation criteria for IT security part 2: Security functional requirements; Ginebra, Suiza; ISO, 2005.
   International Organization for Standardization ISO/IEC 15408-3; Information Technology — Security techniques — Evaluation criteria for IT security part 3: Security assurance requirements Ginebra, Suiza; ISO, 2005.
5. IRAM-ISO/IEC 27002; Tecnología de la Información - Técnicas de Seguridad - Código de práctica para la gestión de la seguridad de la información; Buenos Aires, Argentina; 2006.
6. IRAM-ISO/IEC 27001; Tecnología de la información - Sistemas de gestión de seguridad de la información (SGSI) – Requisitos; Buenos Aires, Argentina; 2007.
7. International Organization for Standardization ISO/IEC 18045; Information technology — Security techniques — Methodology for IT security evaluation; Ginebra, Suiza; ISO, 2008.
8. Computer Security Institute [CSI]; 2011/2012 Computer crime and security survey; New York, NY; CSI; 2012
9. IRAM-ISO/IEC 25005; Tecnología de la Información; Gestión de riesgo de seguridad de la información. Buenos Aires, Argentina; Julio de 2008.

Datos de Contacto:

Mag. Jorge Esteban Eterovic.
Universidad Nacional de La Matanza.
Departamento de Ingeniería e Investigaciones Tecnológicas.
Florencio Varela 1903, (B1754JEC) San Justo, Prov. de Buenos Aires, Argentina.
Tel: (54 11) 4480-8900
E-mail. jeterovic@hotmail.com
jeterovic@ing.unlam.edu.ar

Mag. Domingo Donadello.
Universidad Nacional de La Matanza.
Departamento de Ingeniería e Investigaciones Tecnológicas.
Florencio Varela 1903, (B1754JEC) San Justo, Prov. de Buenos Aires, Argentina.
Tel: (54 11) 4480-8900
E-mail.ddonadel@ing.unlam.edu.ar