**Desarrollo de un laboratorio para la Evaluación y Certificación de la Seguridad de las Tecnologías de la Información de acuerdo a las normas internacionales Common Criteria**

Eterovic, Jorge; Donadello, Domingo; Downar, Alejandro; Galera, Santiago;

Pomar, Pablo; Zeballos, Martín; Kiryczun, Hernán Darío; Ureta, Walter; Petrini,

Gisela; Eterovic, Silvina; D´Arano, Facundo; Bevilcqua, Ricardo.

*jeterovic@ing.unlam.edu.ar****;*** *ddonadel@ing.unlam.edu.ar*

**Resumen**

La utilización de las Tecnologías de la Información (TI) impone como estándar los COMMON CRITERIA o su equivalente ISO/IEC 15408 para la evaluación y la certificación de la seguridad de productos y sistemas de TI, a efectos de garantizar un nivel de seguridad que permita a las organizaciones confiar en los sistemas adquiridos a empresas proveedoras de software.

El proyecto consiste en la traducción de las normas ISO/IEC 15408 para ser cedidas al IRAM a efectos de su adopción como norma nacional y desarrollar las especificaciones para el armado de un laboratorio que estaría en capacidad de evaluar la seguridad de los productos y sistemas de TI, siguiendo el procedimiento establecido en la norma internacional ISO/IEC 18045, que establece una metodología de evaluación de la seguridad de TI.

El laboratorio, para poder evaluar la seguridad de los productos y sistemas de TI de terceros, deberá ser acreditado por un organismo de certificación, por ejemplo el INTI o el OAA (Organismo Argentino de Acreditación).

Este proyecto no sólo permitirá formar investigadores y alumnos en la interpretación de las normas, sino también trabajar en el armado de especificaciones técnicas. El impacto será importante para el grupo de investigación y también para la Universidad, pudiendo hacer uso de éstas especificaciones para el montaje de un laboratorio.

**Descriptores**

Common Criteria - ISO/IEC 15408; Seguridad de productos y sistemas de TI; Laboratorio de Certificación de Seguridad.

**Planteo del problema**

La utilización de las Tecnologías de la Información (TI) en particular el software, en prácticamente todas las actividades 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 nivel de seguridad en la utilización de las TI equiparable, como mínimo, al conseguido en el tratamiento tradicional de la información en soporte papel.

Por tanto, la seguridad que las TI deben poseer, debe comprender 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, en particular preservar sobre la corrupción de la información.

Una de los métodos más reconocidos 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 como los establecidos en la Comunidad Europea, Canadá, Estados Unidos y Australia denominado Common Criteria, cuyo cumplimiento es exigido a todo proveedor externo al momento de adquirir una solución de software. Demostrado mediante una certificación por parte de un Organismo de Certificación legalmente establecido. Como comentario adicional, cabe destacar que los laboratorios que certifican el Common Criteria se encuentran instalados en España principalmente.

Para poder evaluar y certificar la seguridad de los productos y sistemas de TI es necesario desarrollar las Metodologías y Procedimientos de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información que regulen el marco de los procesos de evaluación y certificación.

La carencia actual de un esquema de éstas características es un obstáculo importante para la difusión y aceptación generalizada, tanto a nivel nacional como internacional, de los diferentes productos y sistemas de las Tecnologías de la Información desarrollados en nuestro país.

En el contexto de las naciones no se pueden aceptar criterios de evaluación y certificación de la seguridad de las TI que no sean homologables con los de los demás países participantes. Por ello, es necesaria la adopción de criterios internacionales que permitan negociar el reconocimiento mutuo de certificados, resultando esencial que las Metodologías y Procedimientos de Evaluación y Certificación se equiparen a los del resto de los países.

El marco normativo son las Common Criteria, que han sido adoptados por distintas organizaciones de normalización como por ejemplo ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que las han codificado como ISO/IEC 15408. Nuestro Instituto Argentino de Normalización y Certificación (IRAM) es el representante argentino ante estas organizaciones internacionales y el encargado de la adopción de las normas internacional mediante un proceso de nacionalización.

**Breve descripción del proyecto de investigación**

El desarrollo del proyecto está fuertemente relacionado con la aceptación por parte del IRAM de incluir en su agenda de trabajo el tratamiento de las normas traducidas por el grupo de investigación, ISO/IEC 15408 para su adopción como norma nacional.

Sin este requisito es imposible poder desarrollar localmente un esquema de evaluación y certificación de la seguridad de las TI.

El proyecto de investigación tuvo por objetivo desarrollar las especificaciones para el armado de un laboratorio para la Evaluación de la Seguridad de las Tecnologías de la Información, de acuerdo a las normas internacionales Common Criteria.

En cumplimiento de este objetivo, el proyecto de investigación se ha desarrollado según siguientes etapas:

1. Identificar, obtener y traducir las normas de referencia al castellano
2. Definir el alcance del ámbito de certificación del laboratorio.
3. Definir los Procedimientos de Evaluación y Certificación donde se describa sistemáticamente la actividad de certificación.
4. Estudio y análisis de las normas de referencia.
5. Desarrollar las especificaciones para el armado de un laboratorio para la Evaluación de la Seguridad de las Tecnologías de la Información
6. Establecer convenios con el IRAM, para que se desempeñe como Organismo de Certificación y para cederle las normas traducidas y a futuro sea quien acredite el Laboratorio de Evaluación.

**Conceptos teóricos que sirven de marco a la investigación**

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).

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, 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.

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.

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.
* 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 7 Niveles de Seguridad (EAL). Ellos son:

* EAL 1. Probado funcionalmente
* EAL 2. Probado estructuralmente
* EAL 3. Probado y comprobado metodológicamente
* EAL 4. Diseñado, revisado y probado metodológicamente
* EAL 5. Diseñado y probado semiformalmente
* EAL 6. Diseñado, verificado y probado semiformalmente
* EAL 7. Diseñado, verificado y probado formalmente

**Aspectos relevantes de la investigación**

Se realizó la búsqueda y selección de las normas relacionadas con la temática de la norma Common Criteria:

* ISO/IEC 15408-1/2/3:2005 - Information technology — Security techniques — Evaluation criteria for IT security — (Part 1: Introduction and general model (15408-1); Part 2: Security functional requirements (15408-2); Part 3: Security assurance requirements (15408-3).
* ISO/IEC 18045:2008 - Information technology -- Security techniques -- Methodology for IT security evaluation.

Se tradujeron todas las partes de las normas y fueron cedidas al subcomité de Seguridad de la Información del IRAM.

Se trabajó en diseño de un Laboratorio de prueba de Software y en la Metodología para las Evaluación de Seguridad.

**Aportes alcanzados en relación con el problema planteado**

Se ha logrado que el IRAM acepte el tratamiento de las normas traducidas por los integrantes del equipo de investigación, por parte del Subcomité de Seguridad en Tecnologías de la Información para su posterior adopción como norma argentina IRAM – ISO/IEC. La existencia de una norma argentina es fundamental para poder implementar un proceso de evaluación y certificación de la seguridad de productos y sistemas de Tecnologías de la Información.

Se ha desarrollado un Procedimiento para la acreditación de un laboratorio de evaluación de la seguridad de productos y sistemas de Tecnologías de la Información.

Se ha desarrollado un Procedimiento para la certificación de productos y sistemas de Tecnologías de la Información.

Se han desarrollado los Criterios y Metodologías de evaluación.

Los resultados del proyecto de investigación fueron presentados en el 1er. Congreso Nacional de Ingeniería Informática / Sistema de Información (CoNaIISI 2013), realizado en el mes de noviembre de 2013 y se incorporaron como material de estudio de la materia Auditoría y Seguridad Informática de la carrera de Ingeniería en Informática de la UNLaM.