Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

SEGURIDAD DEL *SOFTWARE* Y CRITERIOS DE EVALUACIÓN

Alfredo Eulalio Ochoa Reyes

Asesorado por Ing. Raúl Gaitán García

Guatemala, noviembre de 2003

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

SEGURIDAD DEL *SOFTWARE* Y CRITERIOS DE EVALUACIÓN

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA FACULTAD DE INGENIERÍA

POR

ALFREDO EULALIO OCHOA REYES

ASESORADO POR EL ING. RAÚL GAITÁN GARCÍA

AL CONFERÍRSELE EL TÌTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, NOVIEMBRE DE 2003

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERIA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Sydney Alexander Samuels Milson
VOCAL I	Ing. Murphy Olympo Paiz Recinos
VOCAL II	Lic. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. Ricardo Morales Prado
EXAMINADOR	Ing.. Edgar Rene Ornelyz Hoil
EXAMINADOR	Inga. Virginia Victoria Tala Ayerdi
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

SEGURIDAD DEL *SOFTWARE* Y CRITERIOS DE EVALUACIÓN

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha mayo de 2001.

Alfredo Eulalio Ochoa Reyes

AGRADECIMIENTOS

A MI SALVADOR JESUCRISTO	Por darme la vida, la inteligencia, la sabiduría y mi salvación.
A MIS PADRES	Eulalio Ochoa y Odilia de Ochoa, por su amor, confianza, comprensión, esfuerzo y apoyo.
A MIS HERMANOS	Por todo el apoyo durante el transcurso de mi carrera.
A MI ESPOSA	Naty, por el amor, la comprensión, y la paciencia.
A MIS HIJOS	Jonathan, Jeniffer, Josué y Emily, por su amor y comprensión.
A MIS COMPAÑEROS Y AMIGOS	Por todo su apoyo y amistad.

DEDICATORIA

Este trabajo de graduación lo dedico a Jesucristo, ya que sin él no hubiera sido posible alcanzar esta meta. A mis padres formadores de mi vida y ejemplo a seguir ya que con esfuerzos, trabajo, paciencia, comprensión y sobre todo amor me han llevado a obtener este triunfo. A mis hermanos por su apoyo, a mi esposa y mis hijos por todo su amor y comprensión, y cada uno de mis compañeros y amigos.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLA

GLOSARIO

Common criteria(cc)	Criterios de evaluación.
Evaluation	Valoración de un PP, ST o un TOE, contra criterios definidos.
Evaluation Assurance Level (EAL)	Los componentes de los niveles de aseguramiento del paquete que consistían en tres partes, que representa un punto en la CC que predefinieron el nivel de aseguramiento.
Firewall	Es un sistema o grupo de sistemas que establece una política de control de acceso entre dos redes.
Information Tecnology(IT)	Tecnología de información.
Pretty good privacy(PGP)	PGP es un *software* de encripcion de alta seguridad disponible para varios sistemas operacionales.
Protection Profile (PP)	Un sistema puesta en práctica-independiente de los requisitos de la seguridad para una categoría de los TOE que satisfacen lo que necesita un consumidor específico.
Secure Socket Layer(SSL)	E un protocolo diseñado para proveer privacidad sobre Internet.
Security Target (ST)	Un sistema de requisitos y de especificaciones de la seguridad para ser utilizado como la base para la evaluación del TOE identificado.

Target of Evaluation (TOE)	Un producto IT o sistema asociado con la documentación de la dirección que le dan el administrador y el usuario del tema de una evaluación.

RESUMEN

El trabajo presenta una metodología para la evaluación de la seguridad del *software*, tanto de bases de datos como de sistemas operativos, y con la revolución tecnológica del Internet, seguridad en el desarrollo de páginas. La evaluación de seguridad para organizaciones independientes provee una garantía en la seguridad de la tecnología de información (IT por sus siglas en Ingles *Information Techcnology*). De productos y sistemas comerciales, gubernamentales e instituciones militares

Se definen conceptos que son necesarios de entender ante la vulnerabilidad de que se puede ser objeto por la falta de seguridad en todos los niveles de desarrollo de *software* y administración de sistema operativo.

Además se define el concepto de los criterios comunes los cuales no son una lista finita de los requisitos que los productos y el sistema deben resolver. Mas bien los criterios comunes para la evaluación de seguridad de la tecnología de información, presentan un lenguaje para definir los sistemas y los productos de la seguridad de la tecnología de información.

Finalmente se logra conocer la importancia del concepto de seguridad del *software* y de cómo aplicar métodos para su utilización y de como aplicar una metodología para su evaluación.

OBJETIVOS

- **General**

Dar a conocer métodos que se puedan poner en practica para la evaluación de *software* a niveles de bases de datos, sistemas operativos y desarrollo y utilización en la Internet.

- **Especificos**

1. Dar a conocer los criterios de evaluación que nos permitan tener la certeza de la confidencialidad de la Información (IT).

2. Dar a conocer metodologías, que permita ayudar a las personas o entes gubernamentales, y privadas en la evaluación de la seguridad del *software*.

3. Dar a conocer los criterios de evaluación que pueden ser utilizados en el desarrollo de bases de datos, así como en sistemas operativos y desarrollo en la *web*.

4. Dar a conocer los conceptos básicos para mantener la seguridad dentro de los sitios de la Internet.

INTRODUCCIÓN

Actualmente las innovaciones tecnológicas que han tenido lugar en el ámbito computacional, han promovido un cambio en la manera de ver los sistemas de información, en general, a las aplicaciones realizadas con la ayuda de las computadoras. Dentro de algunas ramas de la computación, como lo son las bases de datos, sistemas operativos y la Internet, han surgido avances tecnológicos que se han desarrollan sobre circuitos, dispositivos de almacenamiento, programas y metodologías. Sin embargo, los cambios tecnológicos van de la mano con la demanda de los usuarios y programas para extraer el máximo provecho de dichos dispositivos. Actualmente, existen compañías e instituciones académicas dedicadas al desarrollo de productos donde se incorporan ideas nuevas.

En la actualidad aunque es posible que un usuario común no perciba el desarrollo que conlleva el realizar nuevos productos, existe una gran demanda por mayor funcionalidad, mayor número de servicios, más flexibilidad y mejor rendimiento al momento de desarrollar nuevos sistemas. La utilización de una metodología para el desarrollo, análisis y diseño de sistema de información es de suma importación ya que se debe buscar siempre formas para enlazar las soluciones ofrecidas por la tecnología y las necesidades de los usuarios**.**

Si bien es cierto el *software* es inmaterial y su calidad difícil de medir, tenemos algunos indicadores que nos ayudan a diferenciar los productos de calidad de los que carecen de el acercamiento a cero defectos, el cumplimiento de los requisitos intrínsecos y expresos. Y la satisfacción del cliente

Sobre todo la satisfacción del cliente. Ya se sabe que un suministrador puede engañar a todos alguna vez o a alguno muchas veces, pero no puede engañar a muchos durante largo tiempo. El cliente casi siempre tiene razón y para eso están las encuestas de satisfacción. El *software* de calidad es el que resulta en los primeros puestos de la tabla de satisfacción de los usuarios.

Para lograr el *software* de calidad es necesario tener en cuenta un factor importante como lo es la seguridad, aunque esto parecería ser tarea de la administración de los sistemas, se deben utilizar ciertos mecanismos y técnicas que se encarguen de garantizar una efectiva aplicación de seguridad en los sistemas de computadoras.

1. CONCEPTOS BÁSICOS

1.1. ¿Qué es una base de datos?

La cantidad de innovaciones tecnológicas que ha habido en los últimos años ha promovido un cambio en la forma de observar a los sistemas de información y, en general, a las aplicaciones computacionales. Existen avances tecnológicos que se realizan continuamente en circuitos, dispositivos de almacenamiento, programas y metodologías. Sin embargo, los cambios tecnológicos van de la mano con la demanda de los usuarios y programas para la explotación exhaustiva de tales dispositivos mejorados. Por tanto, existe un continuo desarrollo de nuevos productos los cuales incorporan ideas nuevas desarrolladas por compañías e instituciones académicas.

Aún cuando es posible que un usuario común no perciba los desarrollos relevantes de nuevos productos, para las aplicaciones existe una demanda permanente a mayor funcionalidad, mayor número de servicios, más flexibilidad y mejor rendimiento. Así, al diseñar un nuevo sistema de información o al prolongar la vida de uno ya existente, se debe buscar siempre formas para enlazar las soluciones ofrecidas por la tecnología disponible a las necesidades de las aplicaciones de los usuarios.

Un área en la cual las soluciones están integrando tecnología con nuevas arquitecturas o formas de hacer las cosas es, sin lugar a dudas, el área de los sistemas distribuidos de información. Ellos se refieren al manejo de datos almacenados en facilidades de cómputo localizadas en muchos sitios ligados a través de una red de comunicaciones.

Un caso específico de estos sistemas distribuidos es lo que se conoce como bases de datos distribuidas, tópico a estudiar en estas notas.

1.1.1. Motivación

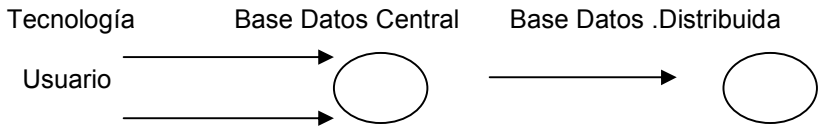
Existen dos fuerzas que han impulsado la evolución de los sistemas de bases de datos. Por un lado los usuarios como parte de organizaciones más complejas han demandado una serie de capacidades que se han ido incorporando en los sistemas de bases de datos (Figura 1.1). Un ejemplo de esto es la necesidad de integrar información proveniente de fuentes diversas. Por otro lado, la tecnología ha hecho posible que algunas facilidades inicialmente imaginadas solo en sueños se conviertan en realidad. Por ejemplo, las transacciones en línea que permite el sistema bancario actual no hubieran sido posibles sin el desarrollo de los equipos de comunicación. Los sistemas de cómputo distribuidos son ejemplos claros en donde presiones organizacionales se combinan con la disponibilidad de nuevas tecnologías para hacer realidad tales aplicaciones.

1.1.2 La presión por datos distribuidos

1.1.2.1 La presión de los usuarios

Las bases de datos permiten organizar la información relevante a alguna parte de la operación de una organización como por ejemplo servicios de salud, corporaciones industriales o bancos. Casi cualquier organización que ha incorporado sistemas de información para su funcionamiento ha experimentado dos fases.

Figura 1. Fuerzas evolucionarías en los sistemas de bases de datos



En la primera fase, se ha agrupando toda la información en un solo lugar. La idea original era que todos los accesos a datos podrían ser integrados en un solo lugar usando herramientas de bases de datos tales como lenguajes de descripción de datos, lenguajes de manipulación de datos, mecanismos de acceso, verificadores de restricciones y lenguajes de alto nivel. Para poder tener estos mecanismos de almacenamiento y recuperación de información, las organizaciones hicieron fuertes inversiones en equipos computacionales sofisticados y con grandes capacidades. Sin embargo, después de experimentar por un tiempo con este enfoque, muchas organizaciones encontraron que el sistema completo era satisfactorio, en algún grado, para un buen número de usuarios pero muy pocos obtenían un servicio óptimo.

Más aún, bajo este esquema centralizado los propietarios de la información específica, perdieron el control sobre el manejo de su información ya que ésta no se almacenaba en sus lugares de trabajo.

Algunos experimentos mostraron que el 90% de las operaciones de entrada y salida de información eran locales (correspondientes al departamento que las generaba) y solo el 10% de tales operaciones involucraba información cruzada (información proveniente de más de un departamento). Así, en la segunda fase se promovió la descentralización de los sistemas de bases de datos corporativos. Entonces, se empezaron a adquirir sistemas de *software* y *hardware* departamentales. Este enfoque presentó grandes beneficios para el control de la seguridad[2] de la información y la disponibilidad de la misma. Permitió que los esquemas de mantenimiento y planeación de los sistemas de información afectara en menor medida al funcionamiento general de la organización.

Sin embargo, muy pronto empezaron a aparecer inconvenientes con este enfoque. Se presentaron problemas de consistencia de la información entre los sistemas locales y central y se hallaron dificultados al transferir información entre departamentos diferentes de una corporación.

De esta manera, en una tercera fase se ha tratado de formalizar la descentralización de las bases de datos y de sus funciones manteniendo la integridad de la información y quizá algún tipo de control centralizado o distribuido.

1.1.2.2. La presión de la tecnología

Existen buenas razones técnicas para distribuir datos. La más obvia es la referente a la sobrecarga de los canales de entrada y salida a los discos en donde se almacena finalmente la información. Es mucho mejor distribuir los accesos a la información sobre diferentes canales que concentrarlos en uno solo. Otra razón de peso es que las redes de computadoras empezaron a trabajar a velocidades razonables abriendo la puerta a la distribución del trabajo y la información.

El hacer una descentralización de la información se justifica desde el punto de vista tecnológico por las siguientes razones:

- Para permitir autonomía local y promover la evolución de los sistemas y los cambios en los requerimientos de usuario.
- Para proveer una arquitectura de sistemas simple, flexible y tolerante a fallas.
- Para ofrecer un buen rendimiento.

Existen aplicaciones que nacieron distribuidas. Para ellas ha sido necesario el uso de nuevas tecnologías para integrar sistemas de información diferentes, de forma que, no se afecte de manera sustancial el estilo de trabajo o de hacer las cosas de los usuarios.

Aunque la idea de distribución de datos es bastante atractiva, su realización conlleva la superación de una serie de dificultades tecnológicas entre las que se pueden mencionar:

- Asegurar que el acceso entre diferentes sitios o nodos y el procesamiento de datos se realice de manera eficiente, presumiblemente óptima.
- Transformar datos e integrar diferentes tipos de procesamiento entre nodos de un ambiente distribuido.
- Distribuir datos en los nodos del ambiente distribuido de una manera óptima.
- Controlar el acceso a los datos disponibles en el ambiente distribuido.
- Soportar la recuperación de errores de diferentes módulos del sistema de manera segura y eficiente.
- Asegurar que los sistemas locales y globales permanezcan como una imagen fiel del mundo real evitando la interferencia destructiva que pueden ocasionar diferentes transacciones en el sistema.

Así también, la aplicación de técnicas de distribución de información requiere de superar algunas dificultades de índole organizacional y algunas otras relacionadas con los usuarios; entre ellas se puede mencionar:

- El desarrollo de modelos para estimar la capacidad y el tráfico esperado en el sistema distribuido.

- Soportar el diseño de sistemas de información distribuidos. Por ejemplo, ayudar a decidir donde localizar algún dato particular o donde es mejor ejecutar un programa de aplicación.

- Considerar la competencia que habrá por el uso de los recursos entre nodos diferentes.

Aun cuando las dificultades mencionadas son importantes, las ventajas de la distribución de información han promovido su aplicación en ambientes del presente y del futuro.

1.1.3 Heterogeneidad y la presión para integrar datos

La descentralización de los sistemas de información y el advenimiento de los sistemas distribuidos están bien justificados[1]

.

[1] Los sistemas de bases de datos distribuidas son un caso particular de los ***sistemas de cómputo distribuido*** en los cuales un conjunto de elementos de procesamiento autónomos (no necesariamente homogéneos) se interconectan por una red de comunicaciones y cooperan entre ellos para realizar sus tareas asignadas. Históricamente, el cómputo distribuido se ha estudiado desde muchos puntos de vista. Así, es común encontrar en la literatura un gran número de términos que se han usado para identificarlo. Entre los términos más comunes que se utilizan para referirse al cómputo distribuido podemos encontrar: funciones distribuidas, procesamiento distribuido de datos, multiprocesadores, multicomputadoras, procesamiento satelital, procesamiento tipo "backend", computadoras dedicadas y de propósito específico, sistemas de tiempo compartido, sistemas funcionalmente modulares.

Sin embargo, existe todavía un argumento importante para el desarrollo de sistemas de bases de datos distribuidas; éste se refiere a la integración de necesidades de procesamiento *no locales* en donde es necesario intercambiar información proveniente de otras áreas o departamentos.

La descentralización de la información promueve la heterogeneidad en su manejo. La heterogeneidad se puede dar a muchos niveles, desde la forma y significado de cada dato hasta el formato y el medio de almacenamiento que se elige para guardarlo. La integración de la información es de importancia mayor para el funcionamiento de una organización.

En resumen, en los sistemas de bases de datos distribuidas se persigue la integración de sistemas de bases de datos diversos no necesariamente homogéneos para dar a los usuarios una visión global de la información disponible. Este proceso de integración no implica la centralización de la información, más bien, con la ayuda de la tecnología de redes de computadoras disponible, la información se mantiene distribuida (localizada en diversos lugares) y los sistemas de bases de datos distribuidos permiten el acceso a ella como si estuviera localizada en un solo lugar. La distribución de la información permite, entre otras cosas, tener accesos rápidos a la información, tener copias de la información para accesos más rápidos y para tener respaldo en caso de fallas.

Existen muchas componentes a distribuir para realizar una tarea. En computación distribuida los elementos que se pueden distribuir son:

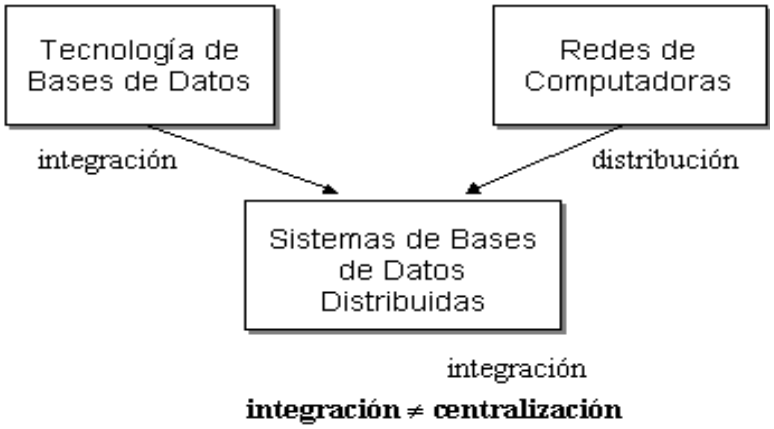
- Control, las actividades relacionadas con el manejo o administración del sistema.

- Datos, la información que maneja el sistema.

- Funciones, las actividades que cada elemento del sistema realiza.

- Procesamiento lógico, las tareas específicas involucradas en una actividad de procesamiento de información.

Figura 2. Justificación de los sistemas de bases de datos distribuidos



1.2 ¿Qué es un sistema operativo?

Un Sistema Operativo (SO) es una colección organizada de extensiones de *software* y de *hardware*, consiente en rutinas de control que hacen funcionar una computadora y proporcionan un entorno para la ejecución de los programas.

Existen otros programas que se apoyan en el SO para poder acceder a los recursos que necesitan. Esto se lleva a cabo a través de llamadas sistema operativo. También el SO debe brindar una forma de que el usuario se pueda comunicar con él a través de una interfaz que le brinde una vía de comunicación con el *hardware* del sistema informático.

El objetivo principal del SO es lograr que los recursos de *hardware* se manejen de forma eficiente para atender al sistema informático.

El SO debe asegurar el correcto funcionamiento del sistema informático. Para lograr esto el *hardware* debe brindar algún mecanismo apropiado que impida que los usuarios intervengan en el funcionamiento del sistema y así mismo el SO debe poder utilizar este recurso de *hardware* de modo que esto se cumpla.

El SO debe ofrecer servicios a los programas y sus usuarios para facilitar la tarea de programación.

1.2.1. Clases de sistema operativos

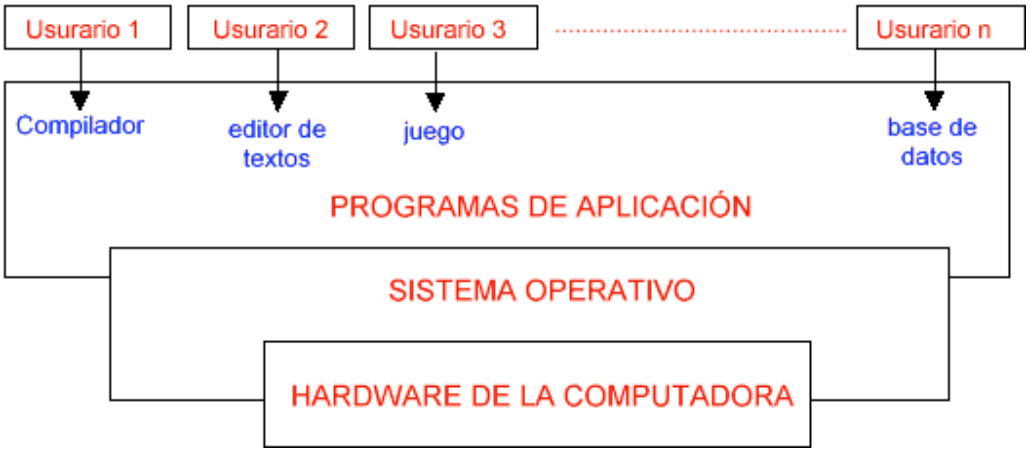
Las clases de sistemas operativos en la que nos basáremos serán los denominador multiusuarios y de multiprogramación es decir que varios usuarios podrán correr concurrentemente múltiples programas.

Un SO es una parte importante de casi cualquier sistema informático.

Para entender mejor esto veremos que un sistema informático puede separar en cuatro partes

- El *hardware*.
- El Sistema operativo.
- Los programas de aplicación.
- Los usuarios.

Figura 3. **Sistema operativo separado en partes**



Estas partes consiste de capas, cada una de las cuales acerca mas al usuario a utilizar los recursos del *hardware*, el *hardware* (CPU, memoria y dispositivos) proporciona los recursos de computación básicos sobre los que se agregaran estas capas sucesivas.

Los programas de aplicación como los compiladores, juegos, aplicaciones de negocios, definen la forma en que estos recursos se emplearán para solucionar los problemas del usuario.

Puede haber varias clases de usuarios usando el sistema (personas, programas y otras computadoras) tratando de resolver diversos problemas.

El SO controla y coordina el uso del *hardware* entre los diversos programas de aplicación y los distintos usuarios. Administra todos los recursos como discos, memoria, impresoras, monitor, etc.

El sistema operativo determina los tiempos en que un determinado programa utilizara un recurso dado.

Al comienzo de la era informática, los sistemas no utilizaban SO's, estas computadoras de hace 40 años ejecutaban un programa a la ves que era cargado por un programador. Este cargaba el programa y lo ejecutaba. Si existía algún error que hiciera que el programa se detuviera antes de lo esperado, se tenía que comenzar de nuevo con todo el proceso.

Recordemos que en esa época no existían muchas computadoras en funcionamiento, así que el programador tendría que esperar seguramente de varios días hasta que nuevamente tuviera su turno enfrente de la computadora de aquella época.

Los SO's existen porque son una manera razonable de solucionar el problema de crear un sistema informático utilizable. El objetivo fundamental de los sistemas informáticos es ejecutar los programas de los usuarios y facilitar la resolución de sus problemas.

Todo esto se realizaba a través de tarjetas perforadas que una persona cargaba en la computadora y luego de algunas horas daba como resultado la salida impresa al programador.

Al avanzar la tecnología informática, muchos de estos programas se cargaban en una sola cinta, otro programa residente en la memoria de la computadora, cargaba y manipulaba los programas de esa cinta. Este es el ancestro de los SO's de hoy en día.

En la década del 60 la tecnología de SO's avanzo de tal forma que se podían tener múltiples programas al mismo tiempo en la memoria. Así surgió el concepto de multiprogramación. Si un programa necesitaba esperas a que ocurriera algún evento externo, como que una cinta se rebobinara, otro podría tener acceso a la CPU para así poder utilizar el 100 % del poder de procesamiento con que contaba la computadora. Esto ahorraba mucho dinero ya que en aquel entonces todo en lo referente a computo (memoria, espacio en disco, etc) costaba cientos de miles de dólares.

Una definición para los SO que nos compete en estos momentos seria que el SO es el programa que ejecuta todo el tiempo en la computadora (conocido usualmente como KERNEL o núcleo), siendo los programas de aplicación todo lo demás.

En general un SO intenta incrementar la productividad de un recurso de proceso tal como el *hardware* de la computadora, o de los usuarios de los sistemas informáticos.

Ahora bien en lo referente a la utilización eficiente de un sistema informático no siempre se puede lograr que un SO lo logre. Casi siempre resulta contradictorio la comodidad y la eficiencia.

1.3. ¿Qué es la Internet?

Internet ha hecho una revolución sin precedentes en el mundo de la informática y de las comunicaciones. Los inventos del telégrafo, teléfono, radio y ordenador sentaron las bases para esta integración de capacidades nunca antes vivida. Internet es a la vez una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus computadoras independientemente de su localización geográfica.

Internet representa uno de los ejemplos más exitosos de los beneficios de la inversión sostenida y del compromiso de investigación y desarrollo en infraestructuras informáticas. A raíz de la primitiva investigación en conmutación de paquetes, el gobierno, la industria y el mundo académico han sido copartícipes de la evolución y desarrollo de esta nueva y excitante tecnología. Hoy en día, términos como *leiner@mcc.com y http: www.acm.org* fluyen fácilmente en el lenguaje común de las personas.

Existe actualmente una gran cantidad de material sobre la historia, tecnología y uso de Internet. Un paseo por casi cualquier librería nos descubrirá un montón de estanterías con material escrito sobre Internet.

En este artículo, varios de nosotros, implicados en el desarrollo y evolución de Internet, compartimos nuestros puntos de vista sobre sus orígenes e historia.

Esta historia gira en torno a cuatro aspectos distintos. Existe una evolución tecnológica que comienza con la primitiva investigación en conmutación de paquetes, ARPANET y tecnologías relacionadas en virtud de la cual la investigación actual continúa tratando de expandir los horizontes de la infraestructura en dimensiones tales como escala, rendimiento y funcionalidades de alto nivel. Hay aspectos de operación y gestión de una infraestructura operacional global y compleja. Existen aspectos sociales, que tuvieron como consecuencia el nacimiento de una amplia comunidad de ínter nautas trabajando juntos para crear y hacer evolucionar la tecnología.

Y finalmente, el aspecto de comercialización que desemboca en una transición enormemente efectiva desde los resultados de la investigación hacia una infraestructura informática ampliamente desarrollada y disponible.

Internet hoy en día es una infraestructura informática ampliamente extendida.

Su primer prototipo es a menudo denominado *National Global or Galactic Information Infrastructure* (Infraestructura de Información Nacional Global o Galáctica). Su historia es compleja y comprende muchos aspectos: tecnológico, organizacional y comunitario. Y su influencia alcanza no solamente al campo técnico de las comunicaciones computacionales sino también a toda la sociedad en la medida en que nos movemos hacia el incremento del uso de las herramientas *online* para llevar a cabo el comercio electrónico, la adquisición de información y la acción en comunidad.

1.3.1. Comercialización de la tecnología

En los últimos años hemos vivido una nueva fase en la comercialización. Originalmente, los esfuerzos invertidos en esta tarea consistían fundamentalmente en fabricantes que ofrecían productos básicos para trabajar en la red y proveedores de servicio que ofrecían conectividad y servicios básicos. Internet se ha convertido en una ***"commodity"***, un servicio de disponibilidad generalizada para usuarios finales, y buena parte de la atención se ha centrado en el uso de la GII (*Global Information Infraestructure*) para el soporte de servicios comerciales. Este hecho se ha acelerado tremendamente por la rápida y amplia adopción de visualizadores y de la tecnología del *World Wide Web*, permitiendo a los usuarios acceder fácilmente a información distribuida a través del mundo. Están disponibles productos que facilitan el acceso a esta información y buena parte de los últimos desarrollos tecnológicos están dirigidos a obtener servicios de información cada vez más sofisticados sobre comunicaciones de datos básicas de Internet.

1.3.2. Historia del futuro

El 24 de octubre de 1995, el FNC (*Federal Networking Council*, Consejo Federal de la Red) aceptó unánimemente una resolución definiendo el término *Internet*. La definición se elaboró de acuerdo con personas de las áreas de Internet y los derechos de propiedad intelectual.

La resolución: "el FNC acuerda que lo siguiente refleja nuestra definición del término *Internet*. *Internet* hace referencia a un sistema global de información que está relacionado lógicamente por un único espacio de direcciones globales basado en el protocolo de Internet (IP) o en sus extensiones, es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones u otros protocolos compatibles con IP, y emplea, provee, o hace accesible, privada o públicamente, servicios de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas aquí descritas".

Internet ha cambiado en sus dos décadas de existencia. Fue concebida en la era del tiempo compartido y ha sobrevivido en la era de los ordenadores personales, cliente-servidor, y los *network computers*. Se ideó antes de que existieran las LAN, pero ha acomodado tanto a esa tecnología como a ATM y la conmutación de tramas. Ha dado soporte a un buen número de funciones desde compartir ficheros, y el acceso remoto, hasta compartir recursos y colaboración, pasando por el correo electrónico y, recientemente, el World Wide Web. Pero, lo que es más importante, comenzó como una creación de un pequeño grupo de investigadores y ha crecido hasta convertirse en un éxito comercial con miles de millones de dólares anuales en inversiones.

No se puede concluir diciendo que Internet ha acabado su proceso de cambio. Aunque es una red por su propia denominación y por su dispersión geográfica, su origen está en los ordenadores, no en la industria de la telefonía o la televisión. Puede -o mejor, debe- continuar cambiando y evolucionando a la velocidad de la industria del computador si quiere mantenerse como un elemento relevante.

Ahora está cambiando para proveer nuevos servicios como el transporte en tiempo real con vistas a soportar, por ejemplo, audio y vídeo. La disponibilidad de redes penetrantes y omnipresentes, como Internet, junto con la disponibilidad de potencia de cálculo y comunicaciones asequibles en máquinas como las computadoras portátiles, los PDA y los teléfonos celulares, está posibilitando un nuevo paradigma de informática y comunicaciones "nómadas".

Esta evolución nos traerá una nueva aplicación: telefonía Internet y, puede que poco después, televisión por Internet. Está permitiendo formas más sofisticadas de valoración y recuperación de costes, un requisito fundamental en la aplicación comercial. Está cambiando para acomodar una nueva generación de tecnologías de red con distintas características y requisitos: desde ancho de banda doméstico a satélites. Y nuevos modos de acceso y nuevas formas de servicio que dará lugar a nuevas aplicaciones, que, a su vez, harán evolucionar a la propia red.

La cuestión más importante sobre el futuro de Internet no es cómo cambiará la tecnología, sino cómo se gestionará esa evolución.

En este capítulo se ha contado cómo un grupo de diseñadores dirigió la arquitectura de Internet y cómo la naturaleza de ese grupo varió a medida que creció el número de partes interesadas. Con el éxito de Internet ha llegado una proliferación de inversores que tienen intereses tanto económicos como intelectuales en la red. Se puede ver en los debates sobre el control del espacio de nombres y en la nueva generación de direcciones IP una pugna por encontrar la nueva estructura social que guiará a Internet en el futuro.

Será difícil encontrar la forma de esta estructura dado el gran número de interés que concurre en la red. Al mismo tiempo, la industria busca la forma de movilizar y aplicar las enormes inversiones necesarias para el crecimiento futuro, por ejemplo para mejorar el acceso del sector residencial. Si Internet sufre un traspié no será debido a la falta de tecnología, visión o motivación. Será debido a que no podemos hallar la dirección justa por la que marchar unidos hacia el futuro.

2. *SOFTWARE* Y SEGURIDAD

2.1. Características del *software*

Para poder comprender lo que es el *software*, es importante examinar las características que lo diferencian de otras cosas que los hombres pueden construir. Cuando se construye hardware, por ejemplo, el proceso creativo humano (análisis, diseño, construcción, prueba) se traduce finalmente en una forma física. Si se construye una nueva computadora, el boceto inicial, diagramas formales de diseño y prototipo de prueba, evolucionan hacia un producto físico (tarjetas de circuitos impresos, fuentes de potencia, etc.). Sin embargo, el *software* es un elemento del sistema que es lógico, en lugar de físico. Por tanto, tiene características considerablemente distintas a las del *hardware*.

2.1.1. El *software* se desarrolla, no se fabrica en un sentido clásico

Aunque existen algunas similitudes entre el desarrollo del *software* y la construcción del *hardware*, ambas actividades son fundamentalmente diferentes. En ambas actividades la buena calidad se adquiere mediante un buen diseño, pero la fase de construcción del hardware puede introducir problemas de calidad que no existen (o son fácilmente corregibles) en el *software*. Ambas actividades dependen de las personas, pero la relación entre la gente dedicada y el trabajo realizado es completamente diferente para el *software*.

2.1.2. El *software* no se *estropea*

Los defectos no detectados harán que falle el programa durante las primeras etapas de su vida. Sin embargo, una vez que se corrigen, suponiendo que no se introducen nuevos errores, el índice de fallos disminuye y se estabiliza.

2.1.3. *Software* a la medida

Con unas pocas excepciones, no existen catálogos de componentes de *software*. Se puede comprar *software* ya desarrollado, pero sólo como una unidad completa, no como componentes que puedan reensamblarse de nuevo.

Si se tuviera que elegir una característica que pudiera considerarse como la mejor de cualquier producto de *software*, esta probablemente sería la homogeneidad o estandarización de la interfaz, aspecto o forma de empleo.

Esto no constituye un mero detalle técnico, sino que para los usuarios de cualquier nivel de conocimientos significa una mayor facilidad de manejo, mayor eficiencia y ahorro de tiempo.

La escalabilidad es más que una propiedad deseable en el *software* que usted puede adquirir. Un producto o servicio escalable le permite expandir o contraer sus operaciones de acuerdo a las necesidades del momento sin incurrir en costos innecesarios.

Adquirir productos escalables resulta ser una mejor inversión en cualquier caso que la adquisición de productos y servicios provistos por fabricantes que carecen de una política semejante.

2.1.4. Problemas que afectan al desarrollo del *software*

Los problemas que afectan al desarrollo del *software* se pueden caracterizar bajo muchas perspectivas diferentes, pero los especialistas en esta actividad se centran en los siguientes aspectos:

- La planificación y estimación de los costes son frecuentemente muy imprecisas.
- La productividad de la comunidad del *software* no se corresponde con la demanda de sus servicios.
- La calidad del *software* no llega a ser a veces ni aceptable.

2.1.5. Ventajas y aplicaciones del *software*

El desarrollo de *software* tiene como base la necesidad de automatizar un proceso que se realice manualmente, añadiéndole rapidez, seguridad y exactitud; características que incrementan considerablemente la calidad en los resultados, humanizan el trabajo y aumentan la cultura informática de la sociedad en su conjunto.

El *software* puede aplicarse en cualquier situación en la que se hayan definido previamente un conjunto específico de pasos procedí mentales (es decir, un algoritmo).

Las primeras aplicaciones del *software* estuvieron relacionadas con la automatización de funciones vinculadas con el control administrativo empresarial con alto grado de formalismo, tales como las nóminas, el inventario y la contabilidad. De ahí que hoy en el mundo sean éstas las experiencias más difundidas, aunque las posibilidades de su aplicación tienen una gran amplitud, entre muchas otras se destacan:

- *Software* de sistemas: conjunto de programas que han sido escritos para servir a otros programas.
  Ejemplo: MS DOS, Windows´95, Windows´98, etc.

- *Software* de tiempo real: es aquel que mide/analiza/controla sucesos del mundo real conforme ocurren.

- *Software* de gestión: sistemas de procesamiento de información comercial.
  Ejemplo: nóminas, cuentas de haberes/débitos, inventarios, etc.

- *Software* de ingeniería y científico: se caracteriza por los algoritmos de manejo de números. El diseño asistido por computadoras (CAD por sus siglas en ingles de *Computer Aided Design*), la simulación de sistemas y otras aplicaciones interactivas (características de esta rama), han comenzado a tomar características del *software* de tiempo real e incluso del *software* de sistemas.

Finalizando el siglo XX –sin dudas el abanderado del conocimiento y el avance tecnológico en la historia de la humanidad- las aplicaciones de *software* se han hecho indispensables para el hombre, evidencia del desarrollo progresivo de su pensamiento y del ritmo acelerado de su tiempo.

En Cuba, se aprovechan eficazmente las magníficas reservas de talento de los especialistas, los cuales mancomunan esfuerzos y tratan de hacer del *software* un rubro que aporte eficiencia a la sociedad cubana.

Lograr que el conocimiento engrandezca al ser humano, no sólo desde el índice de sus posesiones, sino desde su alcance moral y humanista, hacer que cada uno de sus descubrimientos en la ciencia –entre ellos el avance incontrolado de la informática- devenga atributo de su inteligencia y de su capacidad genética de amar, ayudar o salvar al resto de sus semejantes, constituye el reto más importante de este nuevo siglo, aquel del cual depende la continuidad sobre este planeta de ese ser increíblemente valioso que es el hombre.

2.2. Evaluación de calidad del *software*

2.2.1. ¿Qué entendemos por calidad del *software*?

El *software* es inmaterial y la calidad del *software* difícil de medir, pero tenemos algunas pautas, algunos indicadores que nos ayudan a diferenciar los productos de calidad de los que carecen de ella:

- El acercamiento a cero defectos.

- El cumplimiento de los requisitos intrínsecos y expresos.

- La satisfacción del cliente.

Sobre todo la satisfacción del cliente. Ya se sabe que un suministrador puede engañar a todos alguna vez o a alguno muchas veces, pero no puede engañar a muchos durante largo tiempo. El cliente casi siempre tiene razón y para eso están las encuestas de satisfacción. El *software* de calidad es el que resulta en los primeros puestos de la tabla por "aclamación" de los usuarios.

El argumento de la calidad es exhibido por las empresas como un factor diferenciador, como clave de sus procesos de negocio y como eslogan de competitividad empresarial. De hecho, la exigencia cada vez mayor por parte del mercado de la certificación ISO 9000 o el interés creciente por los modelos de calidad de gestión empresarial de tipo EFQM son indicadores de la percepción de la calidad como un elemento cada vez más necesario.

La calidad del *software* debe ser una disciplina más dentro de la Ingeniería del s*oftware*. El principal instrumento para garantizar la calidad de las aplicaciones sigue siendo el plan de calidad. El plan se basa en unas normas o estándares genéricos y en unos procedimientos particulares.

Las normas, directivas, modelos y estándares son básicamente las siguientes:

- Familia de normas ISO 9000 y en especial, la ISO 9001 y la ISO 9000-3.2: 1996 *Quality Management and Quality Assurance Standards*.
- ISO 8402: 1994.
- IEEE 730/1984, *Standard for Software Quality Assurance Plans*.
- IEEE Std 1028: 1989, IEEE *Standard for Software Reviews and Audits*.
- El Plan General de Garantía de Calidad del Consejo Superior de Informática. MAP.
- CMM. *Capability Maturity Model.*
- ISO/IEC JTC1 15504. SPICE. *Software Process Improvement and Capability Determination*.
- Modelo de EFQM. Modelo de la Fundación Europea de Gestión de Calidad.

Los procedimientos pueden variar en cada organización, pero lo importante es que estén escritos, personalizados, adaptados a los procesos de la organización y, lo que es más importante, que se cumplan. La calidad del *software* debe implementarse a lo largo de todo el ciclo de vida, debe correr paralelo desde la planificación del producto hasta la fase de producción del mismo.

Para ello se cuenta con una serie de ayudas, a las que el grupo dedica su atención y trabajo, a través de distintas actividades:

- Para la fase de planificación se pueden utilizar elementos y herramientas propias de la gestión de proyectos, como la:
    - Estimación de la duración, coste y esfuerzo para la construcción del producto. En lo referido a la estimación habrá que tener presentes las métricas de *software*.
    - Planificación de tareas que hay que realizar, asignación de personas, tiempo, coste y otros parámetros para construcción del producto.
- Para los procesos de análisis y diseño deberemos contar con:
    - Conjunto de métodos, utilidades y técnicas que facilitan la automatización del ciclo de vida del desarrollo de sistemas de información, completamente o en alguna de sus fases.
    - Sistemas de obtención de requisitos.
    - Métricas de *software*.
    - Herramientas de generación de datos.
    - Casos de pruebas.
- En los procesos de construcción y pruebas deberíamos echar mano de:
    - Herramientas de gestión de la configuración.
    - Herramientas de simulación.
    - Casos de pruebas.

- Y, finalmente, para el proceso de producción, básicamente habremos de utilizar:
  - Herramientas de monitorización de resultados.
  - Pruebas de producción.

2.3. Seguridad

2.3.1. Introducción y antecedentes

La filosofía con la que creció Internet, permitir la máxima conectividad, ha admitido que cualquier persona pueda tener acceso tanto a la información que permanece en los diferentes nodos de la red como a la información que viaja por los canales de comunicación. Es precisamente esta filosofía la que ha empezado a ser un verdadero problema para el almacenamiento y/o transferencia de cierto tipo de información sensible a ser observada, capturada o deteriorada por personas diferentes a los verdaderos propietarios de ella. Como resultado de estas necesidades que surgen día a día por la introducción de ciertos servicios en la red (e.g. servicios bancarios, pagos por la red, *software* propietario en la red, etc.), surge un concepto que es la seguridad en Internet. Para ofrecer seguridad en la red de redes, es necesario realizar modificaciones a los protocolos o bien adicionar *software* o hardware especializado. Estos procesos muy probablemente afecten un aspecto crítico en Internet como por ejemplo, el desempeño. La seguridad dentro de Internet es tan nueva en nuestro medio como el inicio masivo de la utilización de los servicios que ofrece la red, es por eso que simplemente podemos decir que Internet aún no es segura.

Únicamente existe hoy en día una proliferación de productos que ofrecen seguridad para la Internet que se encuentran en etapa de desarrollo y en donde se han realizado medidas (muy empíricamente) encaminadas a optimizarlos de tal forma que una posible degradación en el desempeño de la red no sea crítico; por ejemplo, PGP es una aplicación que nació como un producto de seguridad para correo electrónico y ha sido optimizado para que las funciones de seguridad finalmente se traduzcan no en archivos binarios, sino en simples textos muy manejables desde cualquier aplicación de correo; por otro lado, la naturaleza misma de los correos electrónicos no define una eventual necesidad de "tiempo real" para la entrega de la información.

Así, una vez justificada la necesidad de seguridad para Internet, los mecanismos introducidos deben permitir garantizar que las diferentes amenazas que sucedieran sean eliminadas, o por lo menos, disminuidas, permitiendo un aprovechamiento más confiable de los servicios que nos ofrece la red.

2.3.2. Seguridad en redes de computadoras y seguridad en Internet

Antes de emprender cualquier estudio sobre seguridad en Internet es necesario tener claros los siguientes conceptos que permiten comprender qué es seguridad y cuales son las acciones a llevar a cabo para garantizar seguridad.

2.3.3. Amenazas

Cualquier acción que comprometa la seguridad de la información que se encuentra en una red se considera una amenaza. Existen varias clasificaciones de amenazas (prácticamente tantas como autores sobre seguridad en redes);

Las amenazas se pueden clasificar en cuatro categorías: naturales, accidentales, activas deliberadas y pasivas deliberadas. Las naturales no están dirigidas a los elementos de la red ni sistemas de información, e incluyen principalmente cambios naturales que pueden afectar de una manera u otra el normal desempeño de la red; las accidentales se dividen en errores de: usuario, administración, sistema, salida, datos mal preparados, entre otras; finalmente, las deliberadas son amenazas intencionales generalmente perpetuadas por *hackers*.

2.3.4. Servicios de seguridad

Luego de identificar las amenazas que atacan al sistema que se este analizando, se debe entender que es necesario implementar unos servicios de seguridad apropiados para prevenir y controlar dichas amenazas. Los principales servicios de seguridad que se deben ofrecer en una red de computadores son: autenticación, integridad, confidencialidad, control de acceso y no rechazo [STA 90].

2.3.5. Mecanismos de seguridad

Para la implementación de servicios de seguridad, se deben utilizar ciertos mecanismos y técnicas que se encargan de garantizar una efectiva aplicación de seguridad en los sistemas computacionales involucrados. Los principales mecanismos de seguridad son: criptografía, firmas digitales, funciones de transformación y técnicas de control de acceso [STA 95] [COR 97].

2.3.4. TCP/IP y seguridad en Internet

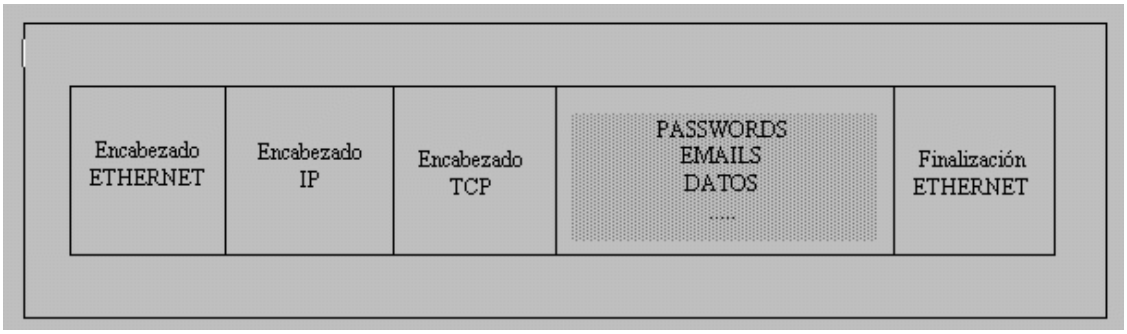
TCP/IP puede ser utilizado para comunicarse a través de cualquier grupo de redes interconectadas físicamente. Es una tecnología especialmente interesante pues su viabilidad ha sido demostrada a gran escala. Los protocolos soportan la tecnología base que permite obtener una Internet, brindando conectividad a organizaciones, hogares, universidades, corporaciones, laboratorios, etc.

Los protocolos TCP/IP contienen los detalles referentes a los formatos de los mensajes, a las reacciones de los equipos cuando llegan mensajes o las acciones que se deben llevar a cabo cuando se desea enviarlos; además, especifica los comportamientos de las máquinas respecto de errores o condiciones anormales.

El protocolo de Internet fue diseñado para que la interconexión de computadoras y redes fuera posible de una manera fácil; pero, qué pasa con la seguridad de la información que viaja entre estas computadoras y redes.

Una trama (paquete) que finalmente viaja por una red *ethernet* cuyo protocolo de "comunicación" es TCP/IP tiene el aspecto que muestra la figura 4.

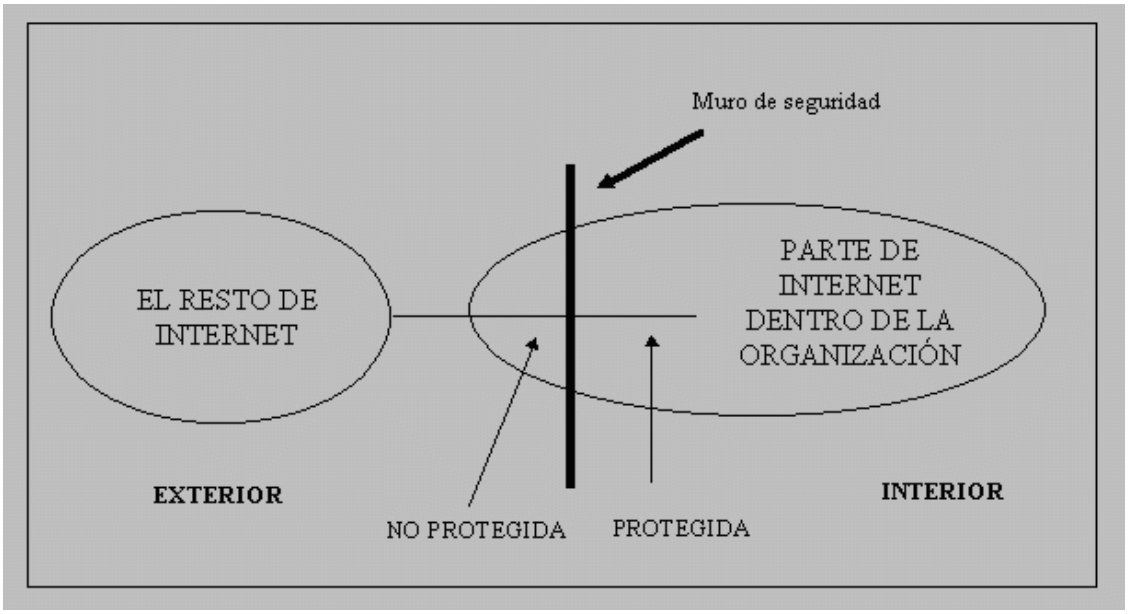
Figura 4: Un paquete que viaja por una red *ethernet* con TCP/IP



Los datos de control que preceden a los datos de usuario se conocen como encabezados. Cada uno de dichos encabezados proporciona información sobre los datos que siguen; así, si un usuario transmite datos hacia otra máquina, esto sucede a nivel de aplicación, TCP (servicio de transmisión confiable) o UDP (servicio de data grama de usuario) recibe los datos y los encapsula en un paquete TCP que contiene un encabezado TCP (valga la redundancia); sigue IP que hace algo similar, hasta que finalmente obtenemos el paquete que se muestra en la figura 5.

Este paquete viaja por la red y cuando llega a su destino sucede algo muy similar pero se inicia desencapsulando la información de nivel a nivel (utilizando las interfaces de cada servicio) hasta conseguir los datos que la aplicación del destino requiere. Para ver que la información que viaja "sin protección" es importante, por ejemplo un encabezado IP contiene información acerca del protocolo de nivel de transporte que debe recibir el data grama (TCP o UDP) o por ejemplo el número del puerto donde entregar los datos finalmente.

Figura 5: El esquema más general de un *firewall*



Adicionalmente, los encabezados IP contienen el origen y destino de los datos (en forma de direcciones IP) que pueden ser examinados por cualquier vía *Internet Network Information Center* (InterNIC), lo que permitirá conocer con mayor exactitud quien es el emisor y receptor de un paquete.

Adicionalmente a la información que viaja en los encabezados, se encuentra el protocolo de control de mensajes de Internet *Internet Control Message Protocol* (ICMP) que es inseguro por naturaleza. Por ejemplo, existe un mensaje que pueden recibir los enrutadores y que permite "desviar" el tráfico de un destino hacia otro; así, la falsificación de un mensaje ICMP puede hacer que un atacante gane acceso a toda la información que pertenecía a otro destino.

3. CRITERIOS DE EVALUACIÓN

3.1. ¿Qué es un criterio de evaluación?

Mientras que mucha gente utilizará la terminología criterios comunes (CC) certificados, los criterios comunes no son una lista finita de los requisitos que los productos y el sistema deben resolver. Los criterios comunes para la evaluación de seguridad de la tecnología de información, la CC definen un lenguaje para definir los sistemas y los productos de la seguridad de la tecnología de información de la evaluación. El marco proporcionado por los criterios comunes permite que las agencias estatales y otros grupos definan los sistemas de requisitos funcionales y del aseguramiento específicos, llamados los perfiles de la protección. El CC también provee de los laboratorios de la evaluación los procedimientos para evaluar los productos o los sistemas contra los requisitos especificados.

3.1.1. Orígenes de los criterios comunes

El CC representa el resultado de una serie de esfuerzos de desarrollar los criterios para la evaluación de la seguridad de la Tecnología de la Información (TI) los cuales son ampliamente útiles dentro de la comunidad internacional.

A principio de los años 80 la evaluación se confiaba al *Trusted Computer System Evaluation Criteria* (TCSEC por sus siglas en ingles) del sistema informático el cual fue desarrollado en los Estados Unidos. En la década de los 80 cuando esta evaluación tenía éxito, varios países comenzaron iniciativas para desarrollar los criterios de la evaluación que construyeron sobre los

conceptos del TCSEC pero eran más flexibles y adaptables a la naturaleza de desarrollo de IT en general.

En Europa, la versión 1,2 de los criterios de la evaluación de seguridad de la tecnología de información *Information Technology Security Evaluation Criteria* (ITSEC) fue publicada en 1991 por la Comisión de las Comunidades Europeas después del desarrollo común por las naciones de Francia, de Alemania, de los Países Bajos, y del reino unido. En Canadá, la versión confiada en canadiense 3,0 de los criterios de la evaluación del producto de computadora *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC) fue publicada en 1993 como una combinación de los acercamientos de ITSEC y de TCSEC.

En los Estados Unidos, los criterios federales para la versión 1,0 de la seguridad de la tecnología de información *Federal Criteria* (FC) también fueron publicados a principios de 1993, como segundo acercamiento a combinar los conceptos norteamericanos y europeos para los criterios de la evaluación.

El trabajo había comenzado en 1990 en el Organización internacional para la estandarización (ISO *International Organsation for Standardisation*) a desarrollar un sistema de los criterios estándares internacionales de la evaluación para el uso general. Los nuevos criterios son la respuesta a la necesidad del reconocimiento mutuo de los resultados estandarizados de la evaluación de seguridad en una forma global para el mercado.

3.2. Criterios de evaluación

El Criterio de Evaluación es presentado como un conjunto de partes relacionadas las cuales se dividen en tres partes.

Parte uno

Introducción y modelo general, es la introducción del criterio de evaluación. Son las definiciones generales, conceptos y principios de la IT, este se refiere a la evaluación de la seguridad y presentación de un modelo general de evaluación.

También presenta construcciones para expresar los objetivos de seguridad de la IT, para seleccionar y definir requerimientos de seguridad y para escribir especificaciones de alto nivel para productos y sistemas. Además, la utilización de cada parte del criterio de evaluación describe términos de cada uno de los consumidores

Parte dos

Requerimientos funcionales de seguridad, establecen un conjunto de componentes funcionales de seguridad como una forma estándar de expresar los requerimientos de seguridad para los destinos de evaluación *Targets of Evaluation (*TOEs). Parte 2 se catalogo como el conjunto de componentes funcionales, familias y clases.

Parte tres

Certificar los requerimientos de seguridad, se establece como un conjunto de componentes de seguridad como una forma estándar de expresar los

requerimientos de seguridad para los TOEs. La parte tres cataloga el conjunto de seguridad, en componentes, familias y clases.

La parte tres también define criterios de evaluación para *Protection Profiles*(PPs) y *Security Targets* (STs) y evitan evaluar los niveles de seguridad definidos y predefinidos en la escala CC para evaluar la seguridad para TOEs, los cuales son llamados Evaluación de los niveles de seguridad *Evaluation Assurance Levels* (EALs).

Los siguientes elementos se presentan como las tres partes de la CC los cuales se podrían involucrar en los tres grupos de usuarios para la CC.

- Consumidor
- Desarrolladores
- Evaluadores

3.3. Criterios comunes internacionales

Los criterios comunes internacionales para la evaluación de seguridad de la tecnología de información (referenciada como criterios comunes) son un esfuerzo común entre Norteamérica y la unión europea de desarrollar un solo sistema de criterios internacionalmente reconocidos de la seguridad. Concluido recientemente como estándar de ISO (número 15408), los criterios comunes reemplazan los existentes de los estados unidos TCSEC, el ITSEC europeo, y el CTCPEC canadiense. Porque el CC reemplaza los US. TCSEC y el ITSEC europeo, y se ha convertido en un estándar de ISO, todas las evaluaciones actuales y futuras de los productos del servidor de la base de datos del orácle serán perseguidas contra el CC.

3.3.1. Hacia la armonización internacional de los criterios

Como los criterios de la evaluación de seguridad se desarrollaron en la última década, se movieron hacia mayor flexibilidad en la especificación de qué puede ser evaluada, mayor importancia para los ambientes del comercio y de la industria, y mayor concentración en las ediciones del análisis de las prestaciones del sistema donde un número de componentes seguros se pueden integrar en cierto ambiente. Éstas son las tendencias valiosas que ayudarán a asegurar la disponibilidad de tecnologías seguras funcionales e independientemente aseguradas a los números más grandes de usuarios.

Mientras que la proliferación de criterios ha estimulado la discusión y el progreso técnico importante y metodología publica, de los criterios del libro ITSEC CC Alemania Francia CTCPEC MSFR de los CRITERIOS de la SEGURIDAD también ha puesto una carga en los compradores internacionales

y los vendedores. Puede requerir a compradores que sean consientes de la seguridad y estar familiarizados con un numero diverso de criterios. También requiere que los vendedores este consientes de la seguridad para emprender evaluaciones de los mismos productos contra varios criterios y bajo diversos esquemas de la evaluación. Por lo tanto, el *Oracle* ha trabajado para animar a los patrocinadores de los diversos criterios hacia la armonización internacional de criterios, y reconocimiento mutuo de la certificación para garantizar a los compradores y/o vendedores que los sistemas sean seguros.

El CC ha emergido como estándar mundial con el objetivo principal del reconocimiento mutuo de los certificados de la evaluación del CC por los países participantes. A este efecto, un arreglo en el reconocimiento mutuo de los certificados comunes de los criterios en el campo de la tecnología de la información (IT) fue firmado formalmente en octubre de 1998. El propósito de este arreglo era avanzar ese objetivo teniendo la nación.

3.3.2. El CC son los criterios estándares de la evaluación de seguridad internacional.

Los firmantes aceptan cada uno de los certificados del CC sin la necesidad de la nueva evaluación de un producto en cada país, de tal modo que se prevé la duplicación de los esfuerzos de la evaluación.

El arreglo indica los argumentos para la confianza de cada nación en la confiabilidad de los juicios en los cuales el certificado original fue basado declarando que los cuerpos de la certificación (o validación) asociados a las naciones signatarias al arreglo resuelven estándares altos y constantes de las evaluaciones de seguridad. Especifica las condiciones por las cuales cada participante acepta resultados de las evaluaciones de seguridad y las

certificaciones asociadas conducidas por otros participantes, y prevé otras actividades cooperativas relacionadas.

Durante el desarrollo del CC, el oráculo participó en todas las conferencias de la revisión y respondió a todas las solicitaciones para los comentarios sobre versiones provisionales a la ayuda asegura los requisitos para la evaluación de los usos acordados del software como los servidores del DBMS fueron tratados por el CC. Al igual que ITSEC, el CC trata una vista ampliada del secreto, de la integridad y de la disponibilidad con la puntería más explícitamente de tratar requisitos militares y comerciales. El CC es evaluaciones dirigidas de ambos productos y sistemas (que se puedan componer de productos y de componentes individualmente evaluados). Al igual que el ITSEC, el CC separa funcionalidad y aseguramiento. Un producto o un sistema se evalúan contra un blanco específico de la seguridad (ST) o el perfil de la protección (PP) que especifiquen la funcionalidad de la seguridad del producto o sistema así como un nivel demandado del aseguramiento.

3.3.2.1. La funcionalidad

El patrocinador o el vendedor definen en un blanco de la seguridad o un perfil de la protección la funcionalidad de la seguridad del producto. La parte 2 del CC define el sistema de los requisitos por los cuales uno puede definir la funcionalidad de la seguridad para un producto o un sistema. Como en el ITSEC, la funcionalidad de la seguridad se desempareja del nivel del aseguramiento, no obstante los criterios comunes no asignan ninguna agrupación de la funcionalidad por mandato, como en el ITSEC y el TCSEC.

3.3.2.2. Aseguramiento

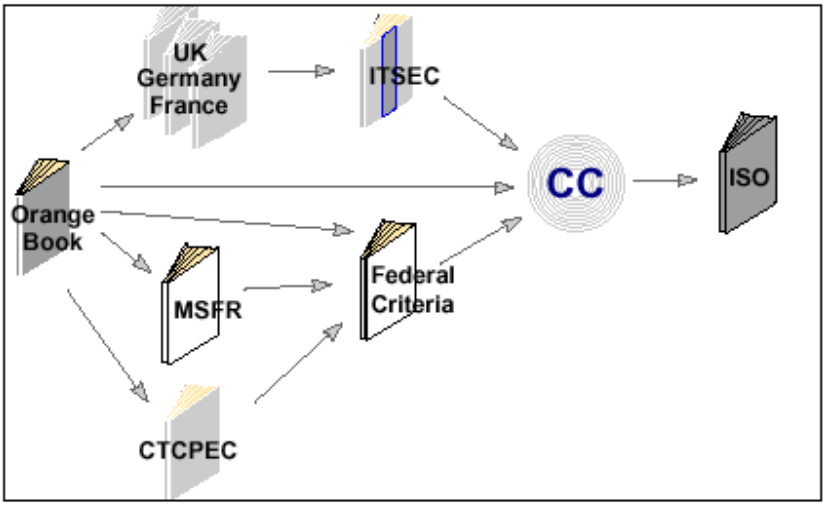
El CC define que el aseguramiento está ganado con asegurar la corrección de la puesta en práctica así como la eficacia de las funciones y de los mecanismos de la seguridad. La corrección de un producto o de un sistema se determina a un solo nivel de la confianza del diseño y del desarrollo, a través a la distribución y a la operación. La parte 3 del CC define siete niveles de la evaluación de EAL1 con EAL7, representando grados de confianza en la corrección del producto o del sistema. El nivel EAL1 asigna un mínimo por mandato de prueba funcional. El nivel EAL4 requiere la especificación de una blanco de la seguridad, una descripción informal del diseño detallado, prueba funcional, análisis del código de fuente, prueba de los mecanismos de la seguridad, El CC separa funcionalidad y aseguramiento, al igual que el ITSEC.

3.3.3. Sistema de control de configuración, y procedimientos

El nivel EAL7 representa el nivel más alto de la confianza y requiere el desarrollo, la verificación, y métodos formales muy rigurosos de la distribución perceptiblemente más allá del alcance de cualesquiera productos o sistema disponibles en el comercio actual. Como con el ITSEC, la eficacia de un producto o el sistema se determina con una variedad de análisis que investiguen, por ejemplo, la conveniencia de mecanismos en el producto o el sistema para los objetivos de la seguridad del producto o del sistema.

También, basado en un análisis de la fuerza de todos los mecanismos críticos de seguridad que se deben cumplir (como mecanismos de la contraseña), el producto o el sistema se da una fuerza mínima del grado del mecanismo. Por lo tanto, en evaluaciones del CC un producto o un sistema se dan una evaluación o el aseguramiento llano (EAL4) que representa el nivel de los usuarios de la confianza puede tener en la disposición del producto o del sistema de la funcionalidad demandada en su perfil de la blanco o de la protección de la seguridad. El diagrama esquemático siguiente demuestra una comparación de los diversos esquemas del grado usados por los US. TCSEC, el ITSEC europeo, y el CC internacional

Figura. 6. Evolución de criterios de seguridad



3.3.4. Esquema de evaluación

El proceso de realizar que las evaluaciones de seguridad contra criterios de la evaluación diferencian según el cuerpo de sanción relevante. Las diferencias en estos procesos afectan el papel de los evaluadores, de los patrocinadores, y de los desarrolladores; el coste y la duración de las evaluaciones; y los recursos requeridos para realizar y para apoyar las evaluaciones. El esquema de la evaluación de US TCSEC el centro nacional de la seguridad de la computadora de US. (NCSC), la tarea de la agencia de la seguridad nacional (NSA), realiza evaluaciones de seguridad en los Estados unidos de América. Estas evaluaciones se realizan bajo la égida del programa confiado en de la evaluación del producto (TPEP). El proceso confiado en de la evaluación del producto (TPEP) en el TPEP, cada evaluación consiste en dos fases distintas: 1) la fase de la pre-evaluación, y 2) la fase de la evaluación.

El proceso entero toma a menudo varios años. Los productos que se evalúan con éxito se dan un grado y se colocan en la lista evaluada de los productos (EPL). Durante la fase de la pre-evaluación, el equipo de la evaluación trabaja con el vendedor para contestar de la documentación, preguntas de los criterios y las interpretaciones mientras que el vendedor termina el desarrollo del producto, y de otros materiales requeridos por el NCSC. Se firma una revisión técnica preliminar intensiva (IPTR) y si la preparación del vendedor es completa, un acuerdo de la evaluación. En la fase de la evaluación el equipo de la evaluación de NCSC repasa la documentación del vendedor.

Una vez que este análisis sea completo, el equipo de NCSC escribe el informe inicial del análisis de producto (IPAR) que es presentado y repasado por el comité examinador técnico de NCSC.s (TRB). Después de la aceptación del IPAR por el TRB, el equipo de NCSC realiza la prueba intensiva y análisis de los productos. En el final de este proceso, se produce un informe final de la evaluación (FER) y el producto se enumera en el EPL con el grado asignado.

El NCSC también ha establecido un programa de mantenimiento de los grados (RAMPA) como el proceso para el mantenimiento de los grados de producto a través de lanzamientos subsecuentes. Este programa requiere procedimientos especiales ser puesto en ejecución por el vendedor usando NCSC-*trained* y los analistas de seguridad certificados del vendedor. Estos procedimientos se centran sobre todo en la gerencia de la configuración y cambian controles.

Todos los cambios subsecuentes a las especificaciones del diseño, a la documentación, a la codificación, y a las habitaciones de la prueba de la

configuración evaluada se deben seguir y analizar para las implicaciones de la seguridad y divulgar posteriormente al NCSC. El proceso de la RAMPA se puede también utilizar para facilitar evaluaciones de componentes en configuraciones adicionales. Por ejemplo, la RAMPA se puede utilizar para evaluar un servidor previamente evaluado del DBMS en un sistema operativo diverso, pero previamente evaluado.

El centro nacional de la seguridad de la computadora (NCSC) realiza evaluaciones de seguridad en los Estados Unidos de América.

En el final del proceso de TPEP, se publica un informe final de la evaluación y el producto se enumera en la lista evaluada de los productos.

Solamente los productos se evalúan bajo el TPEP, así que las aplicaciones componentes y productos que integran en un sistema son la responsabilidad de las autoridades de la certificación y de la acreditación que deben aprobar el sistema antes de uso. El esquema europeo de la evaluación de ITSEC en las instalaciones BRITÁNICAS, comerciales de la evaluación (CLEFs) realiza evaluaciones dentro del Reino Unido La tecnología de la información realiza la evaluación de seguridad y esquema de la certificación.

La parte final del esquema es conducido por un cuerpo del gobierno conocido como el cuerpo de la certificación (CB) que es funcionado por el grupo de la seguridad de la Comunicación-Electrónica (CESG).

En la fase I de una evaluación de ITSEC, un CLEF es contraído por el patrocinador para determinar la aptitud para la evaluación del producto y para producir un programa de trabajo para la evaluación. El cuerpo de la certificación

repasa este programa de trabajo y las metas de la evaluación para asegurarse de que la evaluación sería certificable si estuvo terminada con éxito. En la fase II de una evaluación de ITSEC, un CLEF se contrae para realizar el programa de trabajo de la evaluación (EWP).

Todos los devuelven los resultados de la evaluación realizados por el CLEF, incluyendo los informes técnicos de la evaluación (ETRs), son repasados por el cuerpo de la certificación para asegurarlos resuelven los requisitos del esquema y para asegurar el secreto de las técnicas usadas en la evaluación. Durante la evaluación, el CLEF informa al cuerpo de la certificación todos los problemas encontrados en el producto o el sistema. El cuerpo de la certificación discute estos problemas con el desarrollador para resolverlos en un primero tiempo y para asegurarse de que la certificación subsiguiente no está afectada. El esquema de ITSEC también define claramente el proceso de cómo evaluar productos, y se publica en ÉL la metodología de la evaluación de seguridad (ITSEM). En la terminación de una evaluación acertada de ITSEC, el cuerpo de la certificación publicará un informe de la certificación y un certificado basados en los resultados del CLEF y de su propio análisis.

La meta final del esfuerzo de la armonización de ITSEC de la gran importación a los vendedores y a los compradores igualmente, es alcanzar el reconocimiento mutuo internacional de estos certificados para asegurarse de que una evaluación se realizó con éxito en Alemania, por ejemplo, será reconocido en el Reino Unido. Ya que el Reino Unido y Alemania tienen actualmente el único reconocimiento mutuo formal de cada uno, certificados de ITSEC.

Sin embargo, en abril de 1996, el *National Institute of Standards and Technology* de los E.E.U.U. (NIST) publicó las pautas (boletín del NIST, abril de 1996) que permiten que las agencias de gobierno de los Estados Unidos de

América obtenga o. compren ITSEC F-c2/e2 (o mejorar), o CTCPEC C2/T1 evaluar el sistemas en lugar de un sistema evaluado por nosotros si no hay producto disponible en la lista evaluada los Estados Unidos de América.

Además, en noviembre de 1997, los altos funcionarios para la seguridad de la información de la comisión de las comunidades europeas aprobaron el acuerdo del reconocimiento de los certificados de la evaluación de seguridad de la tecnología de información basados en ITSEC.

El acuerdo vino con fuerza y en marcha desde 1998, y ahora cubre Francia, Finlandia, las instalaciones comerciales de la evaluación (CLEFs) realizan estimaciones contra ITSEC, con la ayuda de un cuerpo del gobierno, la terminación acertada de una evaluación, el cuerpo de la certificación pública un informe y un certificado de la evaluación.

Alemania, Grecia, Italia, los Países Bajos, Noruega, España, Suecia, Suiza y el Reino Unido. Estas naciones acuerdan reconocer certificados de ITSEC de los cuerpos calificativos de la certificación, que son inicialmente SCSSI de Francia, del BSI de Alemania y de CESG del Reino Unido. El esquema internacional de la evaluación del CC

El CC sigue un esquema similar a el de ITSEC europeo. Es supervisado por el CESG en el Reino Unido, por el NSA en los E.E.U.U., y por los cuerpos que gobiernan respectivos de cada uno de los países que participan en el CC. Uno de los dogmas iniciales del desarrollo del CC era el reconocimiento mundial de certificados.

3.4. Esquemas de Evaluación

3.4.1. Requisitos funcionales de la seguridad

Los requisitos funcionales de la seguridad se agrupan en clases. Las clases son el conjunto más general de la seguridad, y todos los miembros de una clase comparten un enfoque común. En cuanto a la funcionalidad de las clases que se contienen dentro del CC. Éstas son como sigue:

- Intervención
- Ayuda criptográfica
- Comunicaciones
- Protección de los datos del usuario
- Identificación y autentificación
- Gerencia de la seguridad
- Aislamiento
- Protección de las funciones de la seguridad del TOE
- Utilización del recurso
- Acceso del TOE

- *Path*/Canal Confiado (**Trusted Path/Channels**)

Cada uno de estas clases contiene a un número de familias. Los requisitos dentro de cada familia comparten objetivos de la seguridad, pero diferencian en énfasis o rigor. Por ejemplo, la clase de la intervención contiene a seis familias que se ocupan de varios aspectos de la revisión (e.g. generación de los datos de la intervención, análisis de la intervención y almacenaje del acontecimiento de la intervención).

Cada familia contiene unos o más componentes, y estos componentes pueden o no pueden estar en una jerarquía. Por ejemplo, la familia de la generación de los datos de la intervención contiene dos componentes no-jerárquicos, el uno que se ocupa de la generación de los expedientes de la intervención, y el otro ocuparse de la asociación de un usuario de un acontecimiento auditable.

3.4.2 Requisitos del aseguramiento de la seguridad

Los requisitos del aseguramiento de la seguridad se agrupan en clases. Las clases son el agrupar más general de los requisitos de la seguridad, y todos los miembros de una clase comparten un foco común. Ocho clases del aseguramiento se contienen dentro del CC. Éstos son como sigue:

- Mantenimiento de la configuración

- Entrega y operación

- Desarrollo y operación
- Guía de documentos
- Soporte del ciclo de vida
- Pruebas
- Evaluación de la vulnerabilidad
- Mantenimiento de seguridad

Dos clases adicionales contienen el aseguramiento para los perfiles de la protección (PPs *Protection Profiles*) y los blancos de la seguridad (STs *Security Targets*).

Cada uno de estas clases contiene a un número de familias. Los requisitos dentro de cada familia comparten objetivos de la seguridad, pero diferencian en énfasis o rigor. Por ejemplo, la clase del desarrollo contiene a siete familias que se ocupan de varios aspectos de la documentación del diseño (especificación funcional, diseño de alto nivel y correspondencia de la representación).

Cada familia contiene unos o más componentes, y estos componentes están en una jerarquía terminante. Por ejemplo, la familia funcional de la especificación contiene cuatro componentes jerárquicos, repartiendo con el aumento de lo completo y de formalidad en la presentación de la especificación funcional.

El CC ha proporcionado aseguramiento predefinido siete paquetes, sobre una escala de aseguramiento, Los niveles de aseguramiento de la evaluación (EALs). Proporcionan las agrupaciones equilibradas de los componentes del aseguramiento que se piensan para ser generalmente aplicables. Los siete EALs son como sigue:

- EAL1 - probado funcionalmente
- EAL2 - probado estructural
- EAL3 - probado y comprobado metódicamente
- EAL4 - diseñado, probado y repasado metódicamente
- EAL5 - semiformalmente diseñado y probado
- EAL6 - diseño semiformalmente verificado y probado
- EAL7 - diseño formalmente verificado y probado

La declaración de los requisitos del aseguramiento de la seguridad del TOE en el ST, debe indicar los requisitos del aseguramiento como uno del EALs aumentado opcionalmente por los componentes del aseguramiento.

EAL1 es el nivel de entrada. Hasta EAL4 el rigor y el detalle de aumento se introducen, pero sin profundizar en técnicas especializadas significativas de

la ingeniería de la seguridad. EAL4 se puede aplicar generalmente a los productos y a los sistemas no desarrollados con la evaluación en mente.

Sobre EAL4, el uso de aumento de las técnicas especializadas de la ingeniería de la seguridad se requiere. Los dedos del pie que resuelven los requisitos de estos niveles del aseguramiento habrán sido diseñados y desarrollados probablemente con ése objetivo. En el nivel superior (EAL7) hay limitaciones significativas en la factibilidad de resolver los requisitos, en parte debido al impacto substancial del coste en las actividades del revelador y de la evaluación, y también porque cualquier cosa con excepción del más simple de productos es probable ser demasiado complejo someter a las técnicas avanzadas para el análisis formal

3.4.3 Niveles del aseguramiento de la evaluación

3.4.3.1. EAL1 - probado funcionalmente

EAL1 es aplicable donde una cierta confianza en la operación correcta se requiere, pero las amenazas para la seguridad no se ven como serias. Será del valor donde el aseguramiento independiente se requiere para apoyar la contención que el cuidado debido se ha ejercitado con respecto a la protección de la información personal o similar.

Este nivel proporciona una evaluación deL destino de la evaluación (TOE) como hecho disponible al consumidor, incluyendo la prueba independiente contra una especificación, y una evaluación de la documentación de la dirección proporcionada.

3.4.3.2. EAL2 - probado estructural

EAL2 requiere la cooperación del desarrollador en los términos de la entrega de los resultados de la información y de la prueba del diseño, pero no debe exigir más esfuerzo de parte del desarrollador que constante con buena práctica comercial. Puesto que pueden requerir de una inversión substancialmente creciente del coste o del tiempo.

EAL2 es aplicable en esas circunstancias donde los desarrolladores o los usuarios requieren un punto moderado de seguridad independientemente asegurada o en ausencia de la disponibilidad del expediente completo del desarrollo. Tal situación puede presentarse el asegurar sistemas de la herencia, o donde el acceso al desarrollador puede ser limitado.

3.4.3.3. EAL3 - probado y comprobado metódicamente

EAL3 permite que un desarrollador concienzudo gane aseguramiento máximo de la ingeniería positiva de la seguridad en la etapa del diseño sin la alteración substancial de las prácticas sanas existentes del desarrollo. Es aplicable en esas circunstancias donde los desarrolladores o los usuarios requieren un nivel moderado de la seguridad independientemente asegurada, y requiere una investigación cuidadosa del TOE y de su desarrollo sin incurrir en costes substanciales de la reingeniería

Una evaluación EAL3 proporciona un análisis apoyado por la caja gris que prueba, confirmación selectiva de los resultados de la prueba del desarrollador, y evidencia de una búsqueda del desarrollador para las vulnerabilidades obvias.

Los controles del medio ambiente del desarrollo y gerencia de la configuración del TOE también se requieren.

3.4.3.4. EAL4 - diseñado, probado y repasado metódicamente

EAL4 permite que un desarrollador maximice la utilización de la ingeniería positiva de la seguridad basada en buenas prácticas comerciales del desarrollo. Aunque son rigurosas, estas prácticas no requieren conocimiento de especialista substancial, habilidades, y otros recursos. EAL4 es el nivel más alto en el cual es probable ser económicamente factible adaptar a una línea de productos existente.

Es aplicable en esas circunstancias donde los desarrolladores o los usuarios requieren un nivel medio a alto de la seguridad independientemente asegurada en TOE convencionales de la materia, y está preparado para incurrir en costes seguridad-específicos adicionales de la ingeniería.

Una evaluación EAL4 proporciona un análisis apoyado por el diseño bajo de los módulos del TOE, y un subconjunto de la puesta en práctica. La prueba es apoyada por una búsqueda independiente para las vulnerabilidades. Los controles del desarrollo son apoyados por un modelo del ciclo de vida, la identificación de herramientas, y la gerencia automatizada de la configuración.

3.4.3.5. EAL5 - semiformalmente diseñado y probado

EAL5 permite que un desarrollador gane aseguramiento máximo de la ingeniería de la seguridad, basada sobre las prácticas comerciales rigurosas del desarrollo, apoyadas por el uso moderado de las técnicas de la ingeniería de la seguridad. Tal TOE será diseñado y desarrollado probablemente con el intento de alcanzar el aseguramiento EAL5. Es probable que los costes adicionales atribuibles a los requisitos EAL5, concerniente al desarrollo riguroso sin el uso de técnicas especializadas, no sean grandes.

EAL5 es por lo tanto aplicable en esas circunstancias donde los desarrolladores o los usuarios requieren un alto nivel de la seguridad y que requieren de un acercamiento riguroso del desarrollo sin incurrir en los costes desrazonables atribuibles a las técnicas de la seguridad del especialista.

Una evaluación EAL5 proporciona un análisis que incluya toda la puesta en práctica. Se asegura de suplir un modelo formal y uno semiformal los cuales representan la especificación y de un diseño de alto nivel, y uno semiformal que muestra correspondencia. La búsqueda para las vulnerabilidades debe asegurar resistencia a los atacantes con un potencial moderado. Un diseño del canal secreto es requerido (*Covert channel analysis and design*)

3.4.3.6. EAL6 - diseño semiformal verificado y probado

EAL6 permite que los desarrolladores ganen alto aseguramiento del uso de las técnicas de la ingeniería de la seguridad a un ambiente riguroso del desarrollo para producir un TOE superior para proteger el valor de los activos contra riesgos significativos.

EAL6 es por lo tanto aplicable al desarrollo de los TOE de la seguridad para el uso en las situaciones del alto riesgo donde el valor de los activos protegidos justifica el coste adicional.

Una evaluación EAL6 proporciona un análisis que sea apoyado por un acercamiento modular y acodado para diseñar, y una presentación estructurada de la puesta en práctica. La búsqueda independiente para las vulnerabilidades debe asegurar resistencia a los intrusos con un alto potencial del ataque. La búsqueda para los canales secretos debe ser sistemática. El ambiente de desarrollo y la configuración debe estar controlado fuertemente.

3.4.3.7. EAL7 - diseño formalmente verificado y probado

EAL7 es aplicable al desarrollo de los TOE de la seguridad para el uso en situaciones del riesgo extremadamente alto y/o donde el alto valor de los activos justifica los costes más altos. El uso práctico de EAL7 se limita actualmente a los TOE con la funcionalidad firmemente enfocada de la seguridad que es favorable al análisis formal extenso.

Para una evaluación EAL7 el modelo formal es suplementado por una presentación formal de las especificaciones funcionales y de diseño de alto nivel, mostrando su correspondencia. La evidencia de la comprobación de la caja-blanca y una completa e independiente confirmación del examen del desarrollador son requeridas. La complejidad del diseño debe ser minimizada.

Para una evaluación EAL7, el modelo formal es suplementario por una presentación formal de la especificación funcional y del diseño de alto nivel,

demostrando correspondencia. La evidencia del desarrollador o caja-blanca que prueba y confirmación independiente de los resultados de la prueba del desarrollador cuanto estos ser requieren. La complejidad del diseño debe ser reducida al mínimo.

4. METODOLOGÍA DE CRITERIOS DE EVALUACIÓN

4.1. Valuación de seguridad del sistema operativo

4.1.1. Servicios de seguridad

La seguridad de un sistema depende de una combinación equilibrada de tecnología y políticas de control. El sistema operativo ofrece un resistente modelo de seguridad que hace hincapié en un control de acceso a todos los recursos y facilita el uso consistente de normas para nivelar las protecciones tecnológicas.

Una completa estructura de seguridad, se debe dotar de una amplia gama de normas y permisos, para la utilización de las herramientas integradas para lograr el nivel de seguridad apropiado para sus entornos informáticos.

Una preocupación fundamental de los gestores de sitios *Web* es la seguridad de sus sitios y la información clave en ellos. La misma protección disponible con *Microsoft Windows NT Server* para archivos y aplicaciones está ahora a su disposición con *Microsoft Internet Information Server* 4.0 (IIS), sin ningún trabajo adicional para los administradores de sistemas.

4.1.2. Características del sistema de seguridad

Aunque sean sólo algunos departamentos gubernamentales de Estados Unidos de América los que demanden expresamente una seguridad de nivel C2, las ventajas de este nivel excepcional de seguridad son reconocidas ya por casi todas las empresas que desean la confidencialidad de su información.

Un sistema de redes seguro tiene muchas características definitorias, pero la medida básica la establece el criterio de nivel C2 de la NSA estadounidense. Y es que aunque sean sólo algunos departamentos Gubernamentales de Estados unidos de América los que demanden expresamente una seguridad de nivel C2, las ventajas de ésta son reconocidas ya por casi todas las empresas que buscan la confidencialidad de su información.

4.1.3. Reutilización de objetos

El sistema operativo debe proteger la información almacenada en su memoria durante un proceso, para evitar que sea reutilizada al azar durante otras operaciones en proceso. Por ejemplo, el sistema operativo *Microsoft® Windows NT® Server* protege la memoria para que sus contenidos no puedan ser leídos tras ser utilizados en un proceso. Además, si un archivo es borrado, los usuarios no podrán acceder a sus contenidos incluso aunque el espacio usado por ese archivo haya sido cubierto por otro. Esta protección deberá extenderse también al disco duro, al monitor, al teclado, al ratón, y al resto de dispositivos del sistema.

4.1.4. Identificación y autentificación

Cada usuario deberá poder identificarse así mismo, para poder acceder al sistema operativo, ya que al momento de ingresar, tendrá que introducir el nombre del usuario y la contraseña; el sistema utilizará esta identificación individual para mantener un registro de las actividades del usuario.

4.1.5. Auditoría

El administrador del sistema (y sólo éste) será el encargado de controlar todos los eventos relacionados con la seguridad, así como las acciones de los usuarios individuales.

Además de los requisitos del nivel C2 de seguridad impuestos por el gobierno estadounidense, existen diversos problemas reales de seguridad que un sistema informático deberá saber resolver. Estos problemas suelen dividirse en dos categorías: la gestión y el uso de la seguridad. Windows NT Server ha sido diseñado tanto para cumplir con los requisitos del nivel C2 como para ofrecer las mejores herramientas para gestionar y usar los completos dispositivos de seguridad del sistema.

4.1.6. Definición de los requerimientos de seguridad de nivel C2

Los requerimientos de seguridad de nivel C2 son definidos por el Centro de Seguridad Informática del Ministerio de Defensa estadounidense, y aparecen publicados en el *Trusted Computer System Evaluation Criteria*, llamado también Libro Naranja.

Todos los sistemas operativos, tanto si son de redes como si son individuales, son evaluados según los criterios definidos en este Libro Naranja. Microsoft y el NCSC han colaborado estrechamente durante todo el proceso de desarrollo de *Windows NT Workstation y Windows NT Server* para asegurarse de que cumplan los requerimientos de seguridad del nivel C2.

El NCSC ha publicado distintas versiones de su Libro Naranja, para especificar los requerimientos específicos de cada sistema. Por ejemplo, la versión sobre redes seguras del *Trusted Computer System Evaluation Criteria*, denominada Libro Rojo, es una adaptación de los requerimientos de seguridad del Libro Naranja para aplicarlos a los componentes de redes del sistema, sin modificar los requerimientos básicos, simplemente especificando como debe operar un sistema de redes para cumplirlos y poder ser considerado de nivel C2 de seguridad.

EL NCSC ha publicado un completo conjunto de versiones de su Libro Naranja para ayudar a los distribuidores a asegurarse de que sus sistemas cumplan con estos requerimientos de seguridad.

Además del libro rojo, existe un libro azul que aplica las directrices del libro naranja a los componentes del subsistema, y así completar todo un esquema de seguridad, recordemos por último que los productos incluidos en la lista de productos evaluados de cara a la obtención del nivel C2 del NCSC fueron sometidos a un proceso extenso y excesivo de evaluación, el cual fue detallado y minucioso.

4.2 .Valuación de seguridad para bases de datos

4.2.1. Características de la seguridad

Las tres principales características de la seguridad que se deben mantener en una base de datos son la confidencialidad, la integridad y la disponibilidad de la información. - Los datos contenidos en una base de datos pueden ser individuales o de una organización. Sean de un tipo o de otro, a no ser que su propietario lo autorice, no deben ser desvelados. Si esta revelación es autorizada por dicho propietario la confidencialidad se mantiene. Es decir, asegurar la confidencialidad significa prevenir, detectar e impedir la revelación impropia de la información.

4.2.2. Políticas, modelos y mecanismos de seguridad en base de datos

Para proteger la base de datos es preciso proteger los recursos, concretamente los datos almacenados, de lecturas y/o actualizaciones accidentales o malintencionadas. Concretamente, los requisitos de protección que pueden establecerse son:

- **Protección de accesos indebidos**

- **Protección de inferencias**
- **Integridad de la base de datos**
- **Integridad operacional de los datos**
- **Integridad semántica de los datos**
- **Contabilidad y auditoría**
- **Autenticación del usuario**
- **Gestión y protección de datos sensibles**
- **Protección multinivel**

Para cumplir con ellos, es preciso que en cada organización que contenga una base de datos, se establezca lo que se denomina políticas, modelos y mecanismos de protección: Las políticas son las directrices generales que definen las líneas que deben guiar la seguridad de la información. Estas políticas son marcadas, unas veces, por los niveles de mayor responsabilidad de la empresa dependiendo del tipo de actividad de la misma. Otras veces, vienen impuestas por obligaciones legales. Los modelos son formulaciones matemáticas abstractas de las políticas de seguridad.

Los mecanismos son conjuntos de funciones que implantan los modelos de seguridad previamente definidos. En algunos casos estos mecanismos se materializan en *hardware* o en *software*, y otras veces en procedimientos administrativos.

Las políticas, modelos y mecanismos están encaminadas a determinar la forma de restringir el acceso de los usuarios a los recursos del sistema dependiendo de la protección que se necesite suministrar.

4.2.3. La comisión mundial de seguridad

Oracle esta comprometido a proveer a sus usuarios los productos seguros independiente del servidor de la base de datos, con este fin, el *oracle* ha trabajado con los patrocinadores de los varios criterios de la evaluación para asegurarse de que sus criterios son apropiados para los productos de *software*,

Oracle también ha apoyado esfuerzos hacia la armonización y el reconocimiento mutuo de los criterios y de los esquemas de la evaluación lo cual proporcionaría ventajas a los usuarios y a los vendedores, por supuesto, la mejor evidencia de la comisión de *oracle* con los estándares y las evaluaciones de la seguridad es que la misma empresa amplia sus costos para evaluar sus productos.

O*racle* eligió tener productos del servidor de la base de datos evaluados de modo que los clientes tengan un servidor seguro independientemente de la base de datos si sus requisitos están para la seguridad de niveles múltiples de *oracle* 7 o para la seguridad discrecional ofrecida por *oracle* 7, *oracle* 8 y oracle8i, la decisión de *oracle* de hacer que sus productos sean evaluados en las plataformas de los sistemas abiertos, que son exigidas cada vez más por el gobierno, los militares, y la industria, también muestra su compromiso ante los sistemas abiertos seguros;.en resumen, la corporación *oracle* ha obtenido con éxito más certificados de criterios mundiales de la evaluación de seguridad que cualquier otro vendedor de la base de datos.

4.3. Valuación de seguridad en Internet

A menudo se cuestionan los problemas de seguridad que existen en la extensa cantidad de computadoras interconectados a nivel mundial, que hoy llamamos Internet. Estos problemas no son sino el fruto de una red que ha ido creciendo de forma desordenada, descentralizada y caótica, sin ningún mecanismo de control o diseño previo. Aunque probablemente hayan sido estos factores lo que ha permitido y favorecido su rápida expansión, así como su aceptación mundial más allá de fronteras.

Hace unos años los mecanismos existentes para garantizar la seguridad en este tipo de redes eran escasos, sólo había servicios de autenticación para el acceso a un recurso determinado y la posibilidad de encriptación. En los últimos años se han ido incorporando mecanismos más avanzados para proporcionar seguridad a nuestras comunicaciones. Aunque aún están muy verdes, el futuro que nos aguarda pasará indiscutiblemente por utilizarlos como parte esencial en nuestras relaciones electrónicas a distancia.

Veamos cuáles son los principales problemas de seguridad en Internet. En primer lugar, se debe garantizar la confidencialidad de la información, es decir, nadie no autorizado debería ser capaz de averiguar el contenido de nuestra comunicación.

En segundo lugar, se debe garantizar la integridad de la información que se esta recibiendo, esto simplemente consiste en que nadie pueda manipular nuestra comunicación de tal forma que cambie el contenido o el significado de ella.

Se debe tener un mecanismo por el cual, se controle el envió y recepción de información para no negar la llegada de ningún mensaje. Este aspecto se conoce como no repudiación, tanto en envío como en recepción.

Se debe tener un mecanismo por el cual, se controle el problema de la autenticación. En toda transacción importante o acceso a recursos, es necesario saber que la persona que está al otro lado es quien dice ser y evitar así la suplantación en la comunicación o el acceso a nuestro sistema por parte de personas ajenas.

En la actualidad todos estos problemas son aceptablemente resueltos gracias a las técnicas de claves asimétricas (pares de claves pública y privada), funciones *hash* y terceras partes fiables.

Actualmente se tiene problemas relacionados con la seguridad en los sistemas informáticos, en los cuales personas totalmente ajenas a ellos son capaces de introducirse y causar daños u obtener información comprometida.

Este aspecto está más relacionado con el sistema y su administrador que con las personas que lo usan. Aunque lógicamente la entrada de un intruso en un servidor puede ocasionar muchos trastornos y quebraderos de cabeza a la persona encargada de mantener su funcionamiento, también puede provocar la suspensión del servicio durante horas, incluso días.

Hoy en día hay cientos de agujeros o debilidades bien conocidas, que se emplean para atacar nuestros sistemas informáticos. La misión del administrador es evitar estos errores en la configuración del *software* con el que se trabaja y estar al tanto de las nuevas posibilidades de ataque.

Es el eterno esfuerzo de construir un castillo inexpugnable para los invasores, esfuerzo que consume mucho tiempo, energía y dinero, para los frutos que cosecharemos.

Una de estas grietas o fallo es la mala elección de la clave de acceso que permite a un usuario entrar en el sistema. A la hora de efectuar un ataque, el pirata opta por los sistemas protegidos con contraseñas fáciles de descubrir.

Existen programas destinados a este propósito, son los denominados cazadores de contraseñas. Podríamos quedar sorprendidos de la efectividad de estos, de la misma manera que un amigo mío quedó ante unas pruebas que realizó con una de estas aplicaciones sobre un fichero de claves encriptadas. Descubrió que dicho programa había conseguido averiguar más del 80% de las claves que él consideraba seguras.

Veamos algunas estimaciones sobre el tiempo que se tardaría en descubrir nuestras contraseñas, según su complejidad y con un ordenador más bien modesto de hoy en día. Nuestra primera clave vamos a formarla con 4 caracteres de longitud y usando sólo minúsculas. Una contraseña muy sencilla que duraría 30 segundos en dejar de ser válida. Haremos otra más compleja, esta vez usaremos seis caracteres con minúsculas y mayúsculas. En este caso nuestro ordenador tardaría unos 15 días en dar con ella. Por último, construyamos una con 8 caracteres en la que incluimos mayúsculas, minúsculas y dígitos. Ahora nuestro modesto ordenador se quedará obsoleto en el intento, ya que necesitaría más de mil años.

Por ello es necesario tener una política de suministro de claves con cierta robustez, para que en el caso de que alguna persona ajena y no deseable consigan entrar y capturar los ficheros de claves encriptadas, la cosa le resulte un poco más difícil.

Es esta la razón por la que el Centro Servidor del IIE nos ha dado una contraseña tan larga (ocho caracteres) que combina letras (en este caso sólo minúsculas), con dígitos y de forma aleatoria, resultando molesta y caprichosa.

La política del Centro es seguir con estas contraseñas tan molestas, aunque se plantea implementar un mecanismo para poder cambiarla, debido entre otras cosas al tiempo de vida tan largo que tienen, hecho que se contradice con las normas de seguridad referentes a claves.

En el próximo artículo se intentará profundizar un poco más en los mecanismos actuales para garantizar los aspectos vistos aquí de confidencialidad, integridad, no repudiación y autenticación.

4.3.1. Un modelo de seguridad para Internet

Antes de realizar las pruebas de desempeño, es necesario conocer por qué se eligieron ciertos mecanismos y/o productos para afirmar que la seguridad puede ser ofrecida con la introducción de ellos en la red. Este capítulo trata un modelo de seguridad encaminado a demostrar que con la adecuada elección de tecnología de seguridad actual es posible ofrecer servicios fundamentales de seguridad en Internet.

Luego de la presentación del modelo, en el siguiente capítulo se describen dichos mecanismos o productos elegidos para proseguir con las pruebas de desempeño y el resto del desarrollo de la investigación.

4.3.1.1. Clasificación de ataques propuesta

Se presenta a continuación una clasificación de ataques basada en **riesgos,** que consiste esencialmente en tomar una categorización de amenazas de acuerdo a un gran número de instancias reportadas de los ataques actuales en Internet. Una taxonomía de ataques basada en riesgos debe proponer los ataques y presentar un(os) ejemplo(s) que respalden la decisión de incluir una clase. De esta manera, propongo que las clases de ataques para el modelo propuesto sean:

Ataques a la integridad de información externa (información que está siendo transmitida) a los sistemas computacionales involucrados (en el canal). Por ejemplo, por medio de la técnica de **engaño IP** se pueden alterar los datos en curso hacia un destino.

Robo o revelación de información externa a los sistemas computacionales involucrados (en el canal). Por ejemplo, por medio de la técnica de **husmear** se pueden adquirir datos que no tienen como destino al atacante.

Ataques a la integridad de información contenida en los sistemas computacionales involucrados (interna a una máquina). Por ejemplo, un *hacker* que gana acceso a una máquina puede alterar el archivo de contraseñas del sistema o archivos de configuración de red, otro ejemplo claro son los virus y caballos de troya.

Robo o revelación de información contenida en los sistemas computacionales involucrados (interna a una máquina). Muy similar al anterior, en este caso pueden no dañarse dichos archivos pero si, por ejemplo, robar el archivo de contraseñas para intentar **desencriptarlo** y ganar acceso de usuario o superusuario a la(s) máquina (s) atacadas.

Negación de servicios externos a las máquinas (integridad de la red). Por ejemplo, dañando la configuración de un enrutador puede quedar aislada una red o subredes entre si. Otro ejemplo claro lo encontramos en ataques físicos a los medios de transmisión: cables cortados, microondas o canales satelitales interferidos, etc.

Negación de servicios internos a las máquinas (virus, sabotaje, caballos de troya, programas "peste"). Por ejemplo, un famoso virus que viaja por Internet es conocido como: "*The Internet worm*". Este virus se aprovecha de las fallas de los programas de utilidad en sistemas BSD (*Berkeley Software Distribution*). El virus se propago por Internet muy rápidamente en noviembre de 1988, cuando su creador Robert Morris lo introdujo en la red.

Violación de autenticación y autorización (maquinas, canal, etc.). Por ejemplo, la primera etapa de un **engaño IP** consta de violación a la autenticación del supuesto origen de los paquetes. Otro ejemplo claro en la **telaraña mundial** los encontramos cuando un servidor WWW es suplantado para recibir información sensible como números de tarjeta de crédito de propiedad del cliente.

Faltas de acción de los responsables de la seguridad (fallas accidentales e intencionales de administración, son amenazas internas). Por ejemplo, dejar mal configurado un servicio como FTP puede ser fatal para el sistema local, un *hacker* podría ingresar al sistema inclusive con privilegios de superusuario y hacer su voluntad.

4.3.1.2. Los mecanismos propuestos

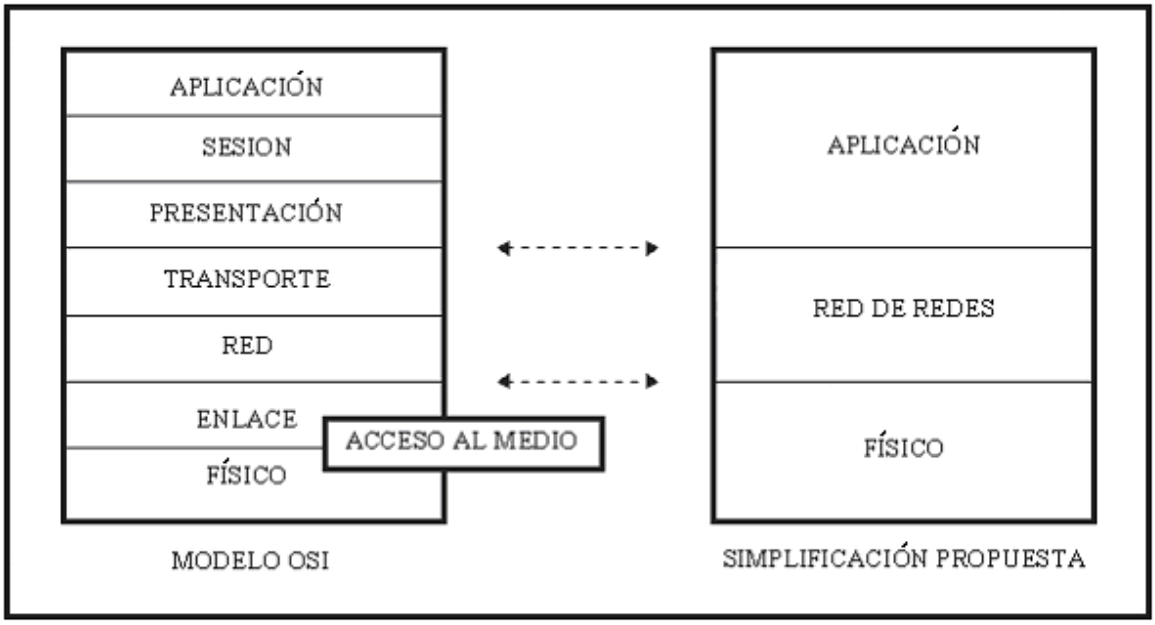
Recordemos que los **servicios de seguridad** que se deberían ofrecer en una red de computadores son: autenticación, confidencialidad,, control de acceso, integridad y no repudio.

Y los mecanismos de seguridad para poder ofrecer dichos servicios son: encripción, firmas digitales, funciones de transformación y control de acceso.

Los mecanismos que serán elegidos para las pruebas de desempeño pueden ser ubicados en algún nivel (o varios) del modelo OSI dependiendo del objetivo del mecanismo y de la factibilidad de su implementación; por ejemplo, si encontramos un mecanismo que garantice privacidad realizando encripción de paquetes IP, podemos decir que se encuentra en el nivel de red. Para efectos de este estudio se han resumido los 7 niveles del modelo OSI en 3 niveles que se denominarán: aplicación que comprende desde la interfaz del usuario hasta el nivel de transporte (sin incluirlo), red de redes que comprende el nivel de red y transporte y físico donde se quedan el físico, de acceso al medio y enlace inclusive.

Se tomó la decisión de no incluir ninguna evaluación a nivel físico en el modelo de seguridad, los otros niveles se verán bien representados por los mecanismos que se proponen. Adicionalmente se toman decisiones de la forma de evaluación de desempeño de los mecanismos; esto es, se decide si se realizaran pruebas directas o se utilizara una herramienta de simulación.

Figura 7: Una simplificación del modelo OSI para proponer mecanismos de seguridad



4.3.1.3. Modelo definitivo de seguridad en Internet

Se han designado con las siguientes convenciones para condensar el modelo en una sola figura:

Los rótulos *SEG* indican sitios donde se deben implementar mecanismos de seguridad para ofrecer los servicios de seguridad fundamentales (confidencialidad, integridad, autenticación, control de acceso y no rechazo).

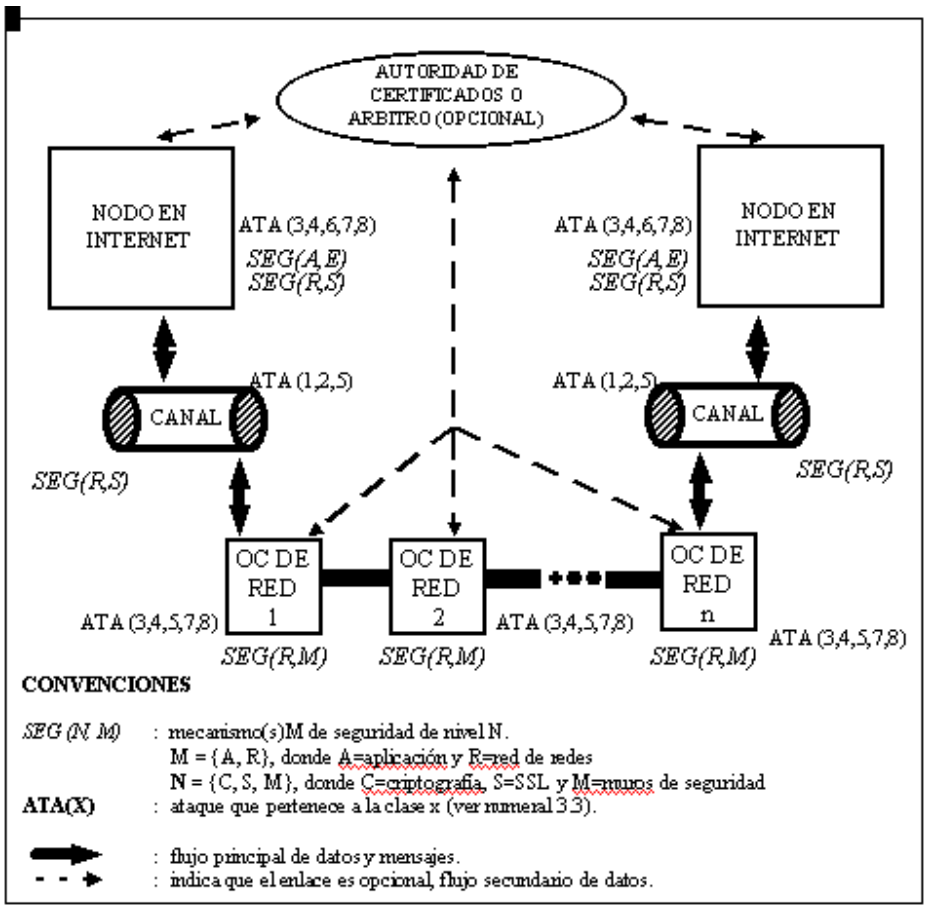
Los rótulos ATA sitúan a los posibles atacantes **ATA**, agrupados según la taxonomía propuesta del numeral anterior (8 clases de amenazas); es decir, ATA(x1, x2, ..., xn) representa ataques de la clase xi, 1 <= xi <= 8 y 1 <= i <= n en el componente de red que contiene el rótulo.

Otros elementos importantes dentro del modelo fueron rotulados con OC (otro componente) de red y son los componentes, diferentes de las estaciones de trabajo, que permiten la conformación de redes de computadoras: enrutadores, conmutadores de red LAN (*LAN Switches*), puentes, compuertas, concentradores, etc; y que, adicionalmente, pueden ofrecen mecanismos de seguridad muy poderosos como los muros de seguridad.

Finalmente se presentan los canales de comunicación (líneas gruesas y los cilindros) y opcionalmente algunos caminos que puede seguir la información para llegar desde un origen hasta un destino.

Se presenta el modelo (figura 8) donde se indican los ataques y se especifica cuál de los componentes del modelo implementa o necesita la implementación de un mecanismo elegido correspondiente a uno de los niveles del modelo OSI simplificado. Se designó el rótulo SEG(N, M), que indica que para un elemento en particular, se debe implementar seguridad a nivel N y con el mecanismo M propuesto.

Figura 8: Un modelo general para seguridad en Internet con la localización de los mecanismos de seguridad planteados



4.3.2. PGP, muros de seguridad

En el numeral anterior se planteó un modelo para la seguridad en Internet. Además, se propusieron tres mecanismos de seguridad concretos que en este capítulo serán explicados (muy brevemente a manera de información general), antes de describir el proceso de pruebas de desempeño de dichos mecanismos.

4.3.2.1. PGP (*Pretty Good Privacy*)

PGP es un *software* de encripción de alta seguridad disponible para varios sistemas operacionales (MS-DOS/Windows, UNIX, Macintosh, entre otros). PGP es el resultado del esfuerzo individual de Phil Zimmermann, su creador. Básicamente ofrece los servicios de confidencialidad y autenticación aunque además, tiene posibilidades para ofrecer compresión de datos (algoritmo ZIP) y gran compatibilidad con el funcionamiento y manejo de mensajes de correo electrónico; en resumen PGP permite a los usuarios intercambiar archivos o mensajes con privacidad y autenticación de una manera conveniente.

Respecto de **confidencialidad** PGP utiliza encripción de mensajes; la encripción convencional es una implementación de IDEA (*International Data Encription Algorithm*) y la encripción de llaves públicas es una implementación del famoso algoritmo RSA (*Rivest-Shamir-Adleman*). Para prestar el servicio de **autenticación (y privacidad)** se ha implementado una combinación de RSA (para encripción de llaves públicas) y una función de transformación (*hash code*) MD5 (*Message Digest Algorithm*). Todos estos algoritmos han sido examinados para corroborar su seguridad efectiva y además fueron expuestos a revisión pública exhaustiva lo que en últimas garantiza la eficacia misma del producto.

Hoy en día el hecho de no tener problemas para el intercambio de llaves sobre canales inseguros y el excelente manejo de llaves de PGP, han colocado al producto como uno de los favoritos para envío de correo electrónico secreto y del correo electrónico certificado.

Además existen muchas aproximaciones para ofrecer seguridad en Internet sobre aplicaciones como WWW utilizando el conocido protocolo para transporte de hipertextos HTTP o modificaciones del mismo.

4.3.2.2. Muros de seguridad (*firewalls*)

Estrictamente hablando un muro de seguridad puede ser definido como una colección de componentes que se colocan entre dos redes. Las siguientes propiedades se cumplen: todo el tráfico en cualquier dirección debe pasar a través del muro de seguridad, únicamente al tráfico autorizado por las políticas locales de seguridad se le permitirá el paso y el muro de seguridad por si mismo es inmune a penetración.

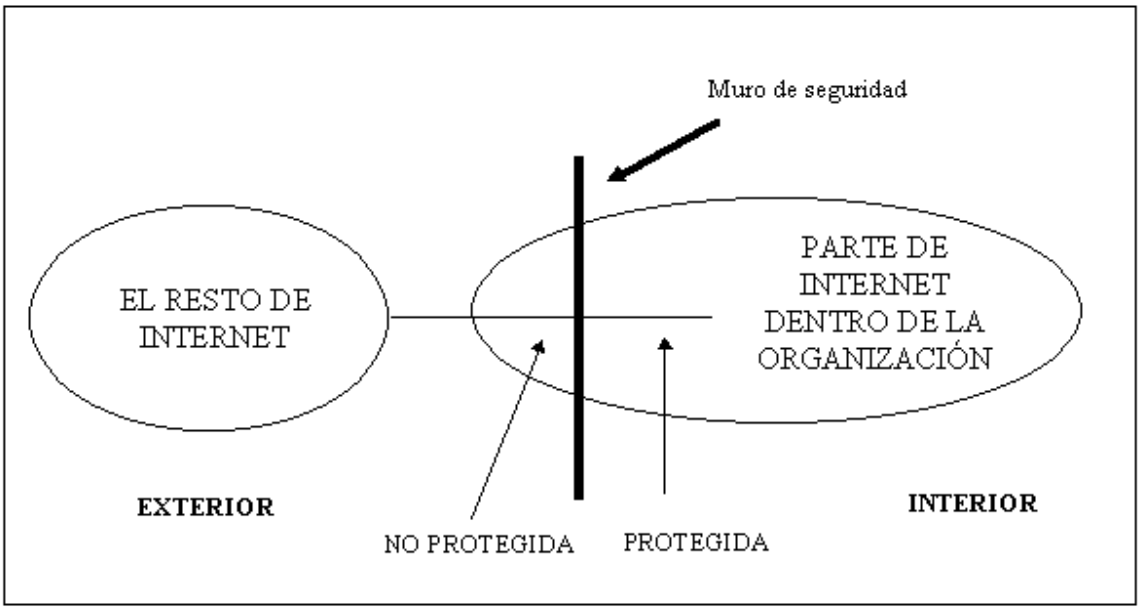
A nivel de red de redes la tendencia de seguridad son los *firewalls*, que de una u otra forma necesitan una modificación de la infraestructura de Internet en la organización que se desea proteger. En términos generales este mecanismo de seguridad permite proveer un cierto grado de aislamiento entre dos redes; además, cuando se elige el *muro de seguridad* apropiado, se configura y se mantiene correctamente, puede proveer un determinado nivel de seguridad. Específicamente y en teoría el *firewall* sencillamente bloquea o restringe cierto tipo de comunicaciones no autorizadas entre computadoras en la organización y computadoras en las organizaciones externas.

Para identificar con mayor claridad el funcionamiento práctico de los muros de seguridad miremos las clases de *muros de seguridad* que existen, junto con algunas modificaciones en la estructura y organización de la red

Esto permite llevar a cabo los objetivos de seguridad planteados y elegir el tipo de mecanismo específico de acuerdo con las necesidades de seguridad identificadas en una red en particular. El esquema más general de un muro de seguridad se muestra en la figura 9.

En esta gráfica, la línea central que representa el muro de seguridad puede cobijar solo una porción de la organización que se desea proteger y no necesariamente debe aislarse la red totalmente. Por esto existe una parte de Internet que aparece desprotegida (conocida como zona desmilitarizada).

Figura 9. El esquema más general de un *firewall*



4.3.2.3. SSL (*Secure Socket Layer*)

Secure Socket Layer (SSL), es un protocolo diseñado para proveer privacidad sobre Internet. El protocolo permite que aplicaciones cliente/servidor se comuniquen de tal forma que no exista riesgo de ser espiados. El servidor es autenticado siempre y los clientes opcionalmente.

SSL requiere un protocolo de transporte confiable (TCP) para transmisión y recepción de datos. La ventaja del protocolo es que es independiente de la aplicación; esto es, un protocolo de aplicación de "nivel superior" (HTTP, FTP, TELNET, etc) puede colocarse arriba de SSL de manera transparente. El protocolo se encarga de negociar el algoritmo de encripcion y una llave de sesión, también se autentica el servidor antes de que el protocolo de aplicación transmita o reciba el primer *byte* de datos. Todos los datos del protocolo de aplicación a transmitir son encriptados; así, asegurando privacidad.

4.4. Metodología CEM

4.4.1. Principios universales de la evaluación

Estos principios son la fundación para la evaluación. La metodología de la evaluación no solamente hace cumplir los principios; las asunciones en los las partes implicados en la evaluación y el esquema que maneja el uso de esta metodología deben también contribuir a la aplicación de los principios.

4.4.1.1. La declaración y la discusión

La declaración y la discusión de principios universales de esta sección indican los principios universales de la evaluación, en cada subdivisión, el principio es indicado y seguido por una breve discusión.

4.4.1.2. Principio de la conveniencia

Las actividades de la evaluación empleadas en la realización de un nivel previsto del aseguramiento serán apropiadas; todas las partes implicados en una evaluación realizarán sus tareas requeridas a un grado del rigor constante con la dirección y los requisitos del nivel del aseguramiento de la evaluación de (EAL).

4.4.1.3. Imparcialidad

Principio: todas las evaluaciones estarán libres de prejuicios, ninguna de las partes implicadas en la evaluación tendrá prejuicios sobre cualquier Objetivo de la evaluación (TOE) o del perfil de la protección (PP) que es evaluado, el descuido técnico apropiado juntado con un esquema que elimine conflictos del interés debe reducir a un nivel nominal de cualquier prejuicio residual; el reconocimiento mutuo y el esquema deben tratar detalladamente el concepto del conflicto inaceptable que son de interés.

4.4.1.4. Objetividad

Principio: los resultados de la evaluación serán obtenidos con un mínimo de juicio u opinión subjetivo, los individuos no pueden estar totalmente libres de la opinión o de juicios, el descuido técnico apropiado basado en la metodología e interpretaciones bien definidas debe reducir opiniones y juicios a un nivel aceptable.

4.4.1.5. Repetición y reproducibilidad

Principio: la evaluación repetida del TOE o PP a los mismos requisitos con la misma evidencia de la evaluación rendirá los mismos resultados; los resultados de cada elemento de la acción del evaluador deben rendir el mismo resultado sin importar quién realiza la evaluación, los requisitos se deben interpretar de una manera constante a través de evaluaciones, la reproducibilidad diferencia de la capacidad de repetición en que el anterior está referido a consistencia a través de evaluadores, y el último es referido a la consistencia de resultados por los mismos evaluadores.

4.4.1.6. Validez de los resultados

Principio: los resultados de la evaluación estarán completos y técnicamente correctos. La salida de la evaluación demostrará el buen juicio y un gravamen técnico exacto del TOE o de los PP. El proceso y los resultados de la evaluación deben estar conforme al olvido técnico para asegurarse de que los requisitos del CC, del CEM, y del esquema están resueltos.

4.4.2. Asunciones

Los principios subyacentes universales son un número de asunciones con respecto al ambiente de la evaluación y de las actividades de todos los las partes implicados; los principios dependen de la validez de estas asunciones.

4.4.2.2. Costo y rentabilidad

El valor de una evaluación debe compensar la hora, los recursos, y el dinero gastado por todas las partes interesados. Un equilibrio se debe mantener continuamente entre el valor, y el gasto del tiempo y de los recursos en la evaluación del TOE y del PPs.

4.4.2.3. Metodología de evaluación

Asunción: el impacto de factores ambientales y técnicos que cambian en evaluaciones se debe reflejar en la metodología de la evaluación de una manera bien considerada y constante. Los ambientes que cambian y la tecnología de desarrollo pueden afectar la eficacia de las técnicas que se utilizan para evaluar un TOE o los PP. además, la metodología de la evaluación deben tomar el ambiente en cuenta y ser aplicables a la tecnología de desarrollo asegurar la aptitud para el propósito del TOE o de los PP evaluados.

4.4.2.4. Reutilidad

Asunción: las evaluaciones deben hacer el uso eficaz de resultados anteriores de la evaluación.

Los resultados de evaluar un TOE o los PP, y las interpretaciones que se presentan en el curso de la evaluación, son útiles en evaluaciones subsecuentes si las mismas condiciones se aplican. La reutilidad es especialmente útil para las evaluaciones donde el TOE o los PP evaluados se incorpora en otro TOE o PP, el contenido y la estructura de los resultados de la evaluación y de la metodología de la evaluación deben apoyar reutilidad.

4.4.2.5. Terminología

Asunción: una nomenclatura común se debe utilizar por todos los las partes implicados en la evaluación. Para asegurar la calidad técnica constante de los resultados de la evaluación y para proporcionar una base constante para comprender y mantener la comunicación a través de evaluaciones, todos los las partes interesados deben compartir una nomenclatura común y una comprensión del significado de los términos en la práctica.

4.5. Modelo general

El modelo general de la metodología se identifica como:

Roles y responsabilidades de los las partes implicados en el proceso de la evaluación.

Un proceso de alto nivel de la evaluación incluyendo una caracterización de alto nivel de los resultados de la evaluación.

El modelo general no prescribe ningún esquema particular; sin embargo, incluye requisitos que cualquier esquema debe conformarse para satisfacer el reconocimiento mutuo de una evaluación.

4.5.1. Responsabilidades de los roles

El modelo general define los roles siguientes: patrocinador, desarrollador, evaluador, y supervisor. Cada papel tiene responsabilidades identificadas dentro de la metodología. El modelo general no imposibilita la organización o la otra entidad de si se asume unos o más roles, conforme a la adherencia a los principios universales, específicamente el principio universal de imparcialidad. Un esquema puede imponer requisitos adicionales para asegurar conformidad con leyes nacionales y regulaciones.

4.5.1.1. Patrocinador

Las responsabilidades del patrocinador incluyen:

Establecer los acuerdos necesarios para la evaluación asegurando que el evaluador proporcione la evaluación (evidencia, entrenamiento, y ayuda de la evaluación).

4.5.1.2. Desarrollador

Las responsabilidades del desarrollador incluyen:

- Soporte de la evaluación.
- Evidencia del desarrollo y de la evaluación.

4.5.1.3. Evaluador

Las responsabilidades del evaluador incluyen:

- Recepción de la evidencia de la evaluación (documentación, PP, ST, una copia del TOE), realizando las acciones requeridas por el CC.

- Requerir y recibir soporte de la evaluación si es necesario.

- Suplir con los descuidos de quien entrega documentando y justificando el veredicto total y cualquier veredicto del interino al supervisor; conformándose con los principios universales y el esquema relevante.

4.5.1.3. Supervisor

Las responsabilidades del supervisor incluyen:

- Supervisión de evaluaciones según los requisitos del esquema, recibiendo y revisando los descuidos de quien entrega.

- Creando las condiciones que aseguran que las evaluaciones se conforman con los principios universales y ponen el CEM en ejecución.

- Evaluaciones de soporte proporcionando el esquema y la interpretación y la dirección de los criterios.

- Aprobando o desaprobando el veredicto total.

- Documentando y justificando el veredicto del descuido a la autoridad de la evaluación.

4.5.2. La relación de los roles

La tabla I describe la separación requerida de los roles de la perspectiva de la influencia indebida en una sola evaluación; la influencia impropia es definida como violación de los principios universales por el individuo que satisface un rol en una sola evaluación.

Un no en la intersección de una fila y de una columna indica que el rol de esa fila no está permitido para influenciar indebidamente en el papel de esa columna.

Tabla I. Influencias impropias permitidas entres roles y durante una simple evaluación

	Desarrollador	Patrocinador	Evaluador	Supervisor
Desarrollador		Si	No	No
Patrocinador	Si		No	No
Evaluador	No		No	No
Supervisor	No	No	No	

4.5.3. La descripción de proceso de la evaluación

A continuación se presenta una descripción de alto nivel del proceso de la evaluación del CEM. El proceso de la evaluación se puede dividir en tres etapas que puedan traslaparse:

- Preparación – Se realiza el contacto entre el patrocinador y el evaluador.
- Conducta - se realiza la evaluación.
- Conclusión - se entregan los resultados de la evaluación, las interacciones entre estos roles durante cada etapa de la evaluación.

4.5.3.1. Preparación

En la etapa de la preparación, el patrocinador aprovecha el esquema para iniciar la evaluación del los PP o un TOE, provee al evaluador de los PP o el ST. el cual realiza un análisis de la viabilidad para determinar la probabilidad de una evaluación acertada, solicitando la información relevante. El desarrollador provee de un subconjunto de resultados de la evaluación (posiblemente en forma de bosquejo); el evaluador puede repasar los PP o el ST y aconsejar al patrocinador sobre los cambios necesitados para asegurar una base firme para la evaluación. si los requisitos del esquema para la evaluación están satisfechos, la evaluación procederá a la etapa siguiente. La salida de la viabilidad debe incluir la lista de los resultados de la evaluación, una lista pedida de las actividades de la evaluación y la información sobre requisitos del muestreo en la CC será tratada.

La salida de la viabilidad se debe convenir por todos los roles, los detalles de la salida de la viabilidad dependen de una variedad de factores, particularmente si la evaluación es de PP o de un TOE todos los roles son responsables de identificar y de proteger la información propietaria.

De acuerdo con el esquema, el patrocinador y el evaluador firman un acuerdo durante esta etapa en la que se define el marco de la evaluación. El acuerdo se toma en cuenta por el esquema, las leyes nacionales y de regulaciones que son aplicables.

4.5.3.2. Conducta

La etapa de la conducta es la parte principal del proceso de la evaluación, durante la etapa de la conducta, el evaluador repasa los resultados de la evaluación recibidos del patrocinador o del desarrollador y realiza las acciones requeridas por los criterios del aseguramiento; durante la evaluación, el se pueden generar informes de la observación, además puede solicitar la clarificación en el uso de un requisito del supervisor usando un informe de la observación. Esta petición podría dar lugar a una interpretación de un requisito para asegurar el uso constante de las evaluaciones futuras. El evaluador puede también utilizar el informe de la observación para identificar una vulnerabilidad o una deficiencia potencial y para solicitar la información adicional del patrocinador o del desarrollador.

La distribución de los informes de la observación se puede especificar más a fondo en el esquema. El supervisor supervisa la evaluación según los requisitos del esquema.

El evaluador produce el informe técnico de la evaluación (ETR) que contiene el veredicto total y la justificación para el veredicto.

4.5.3.3. Conclusión

En la etapa de la conclusión, el evaluador entrega el ETR al supervisor, los requisitos para los controles en la dirección del ETR son establecidos por el esquema que puede incluir la entrega al patrocinador o al desarrollador.

El ETR puede incluir la información sensible o propietaria y puede necesitar ser esterilizado antes de que se dé al patrocinador puesto que el patrocinador puede no tener acceso a los datos del propietario del desarrollador. Las revisiones y los análisis del supervisor el ETR para determinar conformidad al cc, al CEM, y a los requisitos del esquema. El supervisor toma una decisión para convenir o para discrepar con el veredicto total en el ETR (veredicto del descuido), y prepara un informe sumario de la evaluación (ESR). El supervisor utiliza el ETR como la entrada primaria al ESR. El evaluador podría ser requerido para proporcionar la ayuda y/o la dirección técnicas en requisitos no expuestos al supervisor para la preparación del ESR.

En el extremo de la etapa de la conclusión, el supervisor entrega el ESR a la autoridad de la evaluación. El patrocinador, el desarrollador y el evaluador deben tener la capacidad de repasar el ESR para asegurar su evaluación.

5. INVESTIGACIÓN DE CAMPO

Las entrevistas constituyen una técnica de recopilación de información que permite recoger opiniones, posturas, conductas y características de diversas personas, que se encuentran involucradas en el desarrollo de sistemas de información.

Para el diagnóstico se desarrolló una entrevista para recopilar datos, los cuales permitieron mostrar las tendencias en la utilización de la calidad de *software* que se desarrolla, evaluar la seguridad y la utilización de una metodología para la evaluación del *software* en Guatemala.

5.1. Objetivo de la entrevista

Se establecieron los siguientes objetivos para la realización de la entrevista:

- Identificar el sistema operativo que utilizan cada una de las empresas que representan los entrevistados.
- Identificar el manejador de base de datos que utilizan cada una de las empresas que representan los entrevistados.
- Identificar si desarrollan *software* para Internet.
- Identificar si las empresas conocen el concepto de criterios de evaluación.

- Identificar si las empresas utilizan una metodología para la evaluación de su *software*.

5.2. Metodología de la entrevista

Para la elección del tipo de pregunta se utilizó una combinación de preguntas abiertas y cerradas.

Se seleccionaron un grupo de empresas del sector público y privado de Guatemala, empresas que se encargan de desarrollar productos de *software* para la venta y/o utilización en las empresas.

La entrevista se dirigió a personas profesionales en informática, las cuales de alguna manera son responsables del desarrollo del *software* y manejo de la información de sus empresas.

La mayor parte de las entrevistas fueron enviadas por correo electrónico; y otra parte fueron de manera personal.

5.3. Contenido de la entrevista

La entrevista consta de siete preguntas que se responderán a criterio del entrevistado y en forma breve, y seis preguntas de selección múltiple.

Figura 10. Encuesta

Nombre de la empresa: _____

Puesto que desempeña: _____

Escolaridad: Diversificado ____ Universidad ____ Otro ____

1. ¿Qué sistema operativo utiliza?

_____
_____
_____
_____

2. ¿Qué manejador de base de datos utiliza?

_____
_____
_____
_____

3. ¿Qué entiende por calidad del *software*?

_____
_____
_____
_____

4. ¿Que es para usted la seguridad de *software*?

_____
_____
_____
_____

5. ¿Que mecanismos utiliza para manejar la seguridad del *software*?

_____
_____
_____
_____

6. ¿Qué mecanismos conoce para la seguridad de transmisión de datos por Internet?

_____
_____
_____
_____

7. ¿A qué mecanismos recurre para los servicios de seguridad de su red?

_____
_____
_____
_____

8. ¿Cree que es conveniente la utilización de la seguridad en el *software*?

Si _____ no _____

¿Por qué?

_____

9. ¿Cree que es conveniente la utilización de la seguridad dentro de su red?

Si _____ no _____

¿Por qué?

_____

10. ¿Cree que es conveniente la utilización de la seguridad en Internet?

Si _____ No _____

¿Explique su respuesta?

_____

11. ¿Conoce el concepto de Criterios de Evaluación?

Si _____ No _____

12. ¿Conoce el concepto de criterios comunes (*common criteria*) para la evaluación del *software*?

Si _____ No _____

13. ¿Conoce alguna metodología para la evaluación de *software*?

Si _____ No _____

Si la respuesta es afirmativa, ¿mencione cuáles?

_____

_____

_____

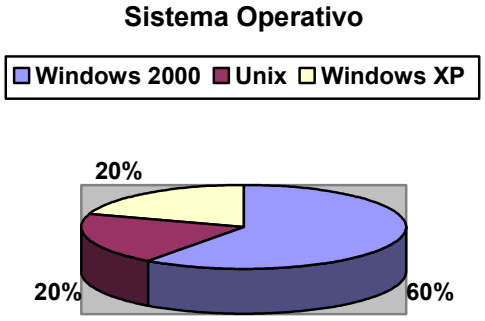
_____

5.4. Presentación de resultados

A continuación se presentan los resultados obtenidos de las entrevistas realizadas. Se tomaron empresas del sector público y privado de la ciudad capital de Guatemala en un porcentaje del 80% de las empresas correspondieron al sector privado y el 20% del sector público, empresas cuya actividad principal es el desarrollo de *software*.

1. ¿Qué sistema operativo utiliza?

Figura 11. Respuesta a pregunta número 1



Interpretación del total de la población entrevistada la tendencia actual de utilización de sistemas operativos se tiene el 60% utilizan sistema operativo *Windows 2000*, un porcentaje menor corresponde a la utilización de *Unix* y de sistema operativo W*indows Xp*.

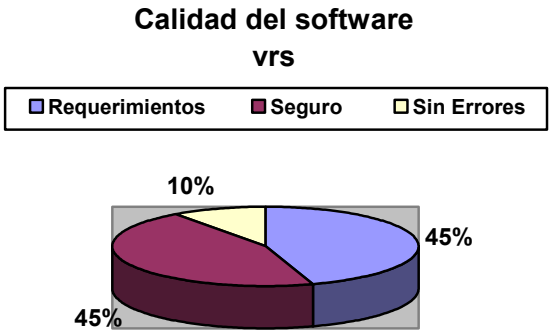
2. ¿Qué manejador de base de datos utiliza?

Oracle	*Sqlserver*
90%	10%

Interpretación según los resultados de dicha pregunta un porcentaje mayor de la población entrevistada utiliza el manejador de base de datos *Oracle*.

3. ¿Que entiende por calidad del *software*?

Figura 12. Respuesta a pregunta número 3



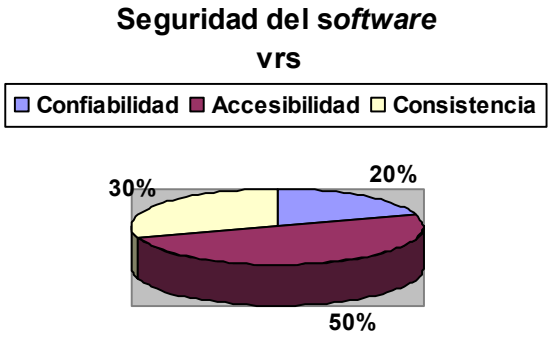
Calidad de *software* vrs. Sin errores, requerimientos y seguro

	Sin errores	Cumpla con los requerimientos	Seguro
Calidad del *software*	10%	45%	45%

Interpretación de acuerdo con la respuesta obtenidas sobre que se entiende por calidad del *software*, se considera que los parámetros seguridad del *software* y cumplir con los requerimientos son los factores mas preponderantes para definir la calidad del *software*.

4. ¿Qué es para usted la seguridad de *software*?

Figura 13. Respuesta a pregunta número 4



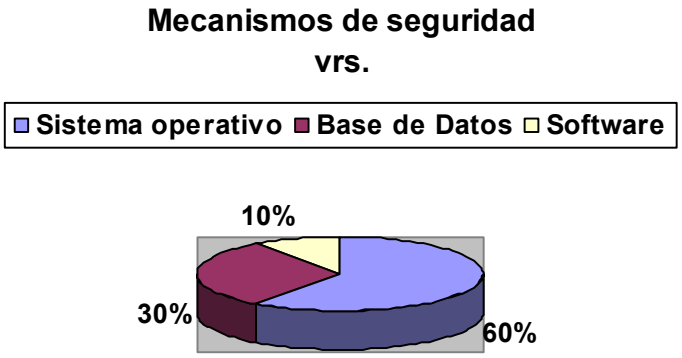
Seguridad del *software* vrs confiabilidad, accesibilidad y consistencia

	Confiabilidad	Accesibilidad de la información	Consistencia
Seguridad del *software*	20%	50%	30%

Interpretación de acuerdo con las respuestas obtenidas sobre que se entiende por seguridad del *software*, se considera que el parámetros accesibilidad según la muestra posee una ponderación alta sobre la confiabilidad y consistencia.

5. ¿Qué mecanismos utiliza para manejar la seguridad del *software*?

Figura 14. Respuesta a pregunta número 5



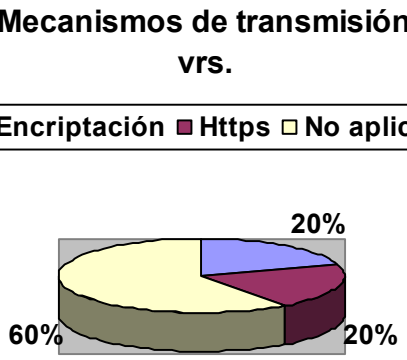
Mecanismos de seguridad vrs sistema operativo, accesos y *software*

	Sistema operativo	Base de datos	A nivel de *software*
Mecanismos de Seguridad	60%	30%	10%

Interpretación de acuerdo con las respuestas obtenidas sobre que mecanismos de seguridad a nivel de base de datos, sistema operativo y a nivel del *software* la mayor parte de muestra opta porque los mecanismos de seguridad son mejores a nivel de sistema operativo que a nivel de base de datos y a nivel de el mismo *software*.

6. ¿Qué mecanismos conoce para la seguridad de transmisión de datos por Internet?

Figura 15. Respuesta a pregunta número 6



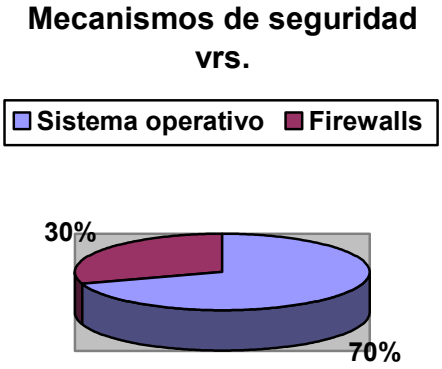
Mecanismos de transmisión vrs encripción protocolo https y no aplica

	Encriptación	Protocolo https	No aplicable
Mecanismos de Transmisión	20%	20%	60%

Interpretación de acuerdo a las respuestas obtenidas una gran parte de la muestra desconoce el concepto de mecanismos para la transmisión de la información, ya que la mayoría indicaba que desconoce el concepto de envió de la información a través de Internet.

7. ¿A que mecanismos recurre para los servicios de seguridad de su red?

Figura 16. Respuesta a pregunta número 7



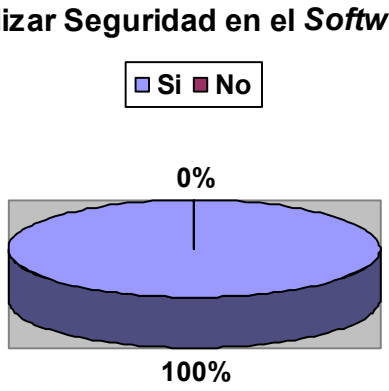
Seguridad de red vrs sistema operativo y *firewalls*

	Sistema operativo	*Firewalls*
Seguridad de red	70%	30%

Interpretación de acuerdo con las respuestas obtenidas se coincide en utilizar esquemas de seguridad a través de usuarios y *passwords*, a nivel de sistema operativo, y no utilizar herramientas externas como lo son *firewalls*.

8. ¿Cree qué es conveniente la utilización de la seguridad en el *software*?

Figura 17. Respuesta a pregunta número 8



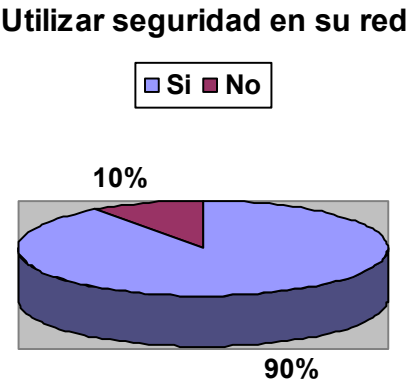
Seguridad del *software*

	Si	No
¿Utilizar Seguridad?	100%	0%

Interpretación el total de la población entrevista coincide que es necesaria la utilización de la seguridad en el *software* esto garantiza la conservación de la información ya sea que se utilice dentro o fuera de la organización.

9. ¿Cree qué es conveniente la utilización de la seguridad dentro de su red?

Figura 18. Respuesta a pregunta número 9



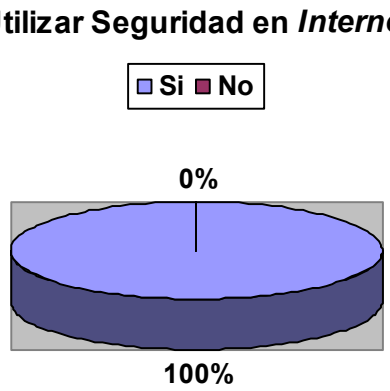
Seguridad en la red

	Si	No
¿Utilizar Seguridad?	90%	10%

Interpretación el 90% de la población entrevistada coincide en que es necesario utilizar seguridad dentro de la red, ya que esto evitaría que la información que se utiliza en la organización sea manejada por todos los usuarios, evitando con ello mal uso de la información, aunque un 10% cree que no es correcto ya que se debe confiar en el personal que maneja la red.

10. ¿Cree que es conveniente la utilización de la seguridad en Internet?

Figura 19. Respuesta a pregunta número 10



Seguridad en Internet

	Si	No
¿Utilizar Seguridad?	100%	0%

Interpretación el total de la población entrevistada coincide en que es necesario utilizar seguridad en Internet, para evitar intrusos en la red, para evitar manipulación de los datos de la organización y para mantener la confidencialidad de los datos.

11. ¿Conoce el concepto de criterios de evaluación?

Figura 20. Respuesta a pregunta número 11

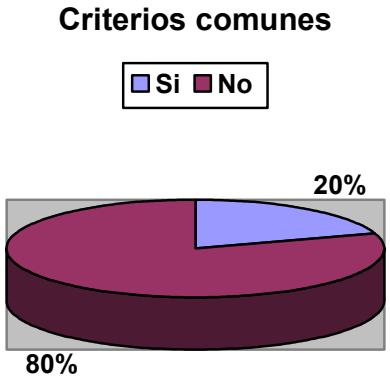
Conocimiento sobre criterios de evaluación

	Si	No
¿Conoce sobre Criterios evaluación?	100%	0%

Interpretación del total de la población entrevistada el 50% de la población conoce el concepto de criterios de evaluación.

12. ¿Conoce el concepto de criterios comunes (*common criteria*) para la evaluación del *software*?

Figura 20. Respuesta a pregunta número 12



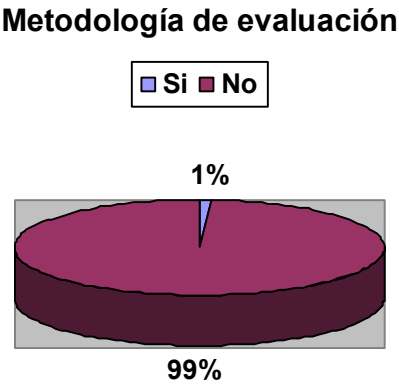
Conocimientos sobre criterios comunes

	Si	No
¿Conoce sobre Criterios Comunes?	80%	20%

Interpretación del total de la población entrevistada el 80% de la población no conoce el concepto de criterios comunes para la evaluación del *software*.

13. ¿Conoce alguna metodología para la evaluación de *software*?

Figura 21. Respuesta a pregunta número 13



Metodología de evaluación

	Si	No
¿Conoce sobre metodología de evaluación?	1%	99%

Interpretación del total de la población entrevistada solamente uno definió alguna metodología para la evaluación del *software* y el resto de la población no la conoce.

5.5. Análisis de resultados

De acuerdo con los resultados obtenidos en la recopilación de datos efectuada por medio de las encuestas se determinó que lo mas sobresaliente e importante es que todas las empresas se encuentran consientes de lo que la seguridad significa para su información; así como de los mecanismos a utilizar para evitar de que tanto personas propias de su organización como personas externas puedan manipular o generar inconsistencias en sus datos.

Se determinó además que las empresas entrevistadas están conscientes en utilizar la Internet para realizar transacciones con su información, ya que es necesario utilizar métodos de encriptación o utilizar protocolos de seguridad, para que los elementos viajen seguros y mantener la confidencialidad necesaria.

Se comprobó que la calidad en el *software* es clara y necesaria en el desarrollo del *software* ya que esto nos garantiza *software* robusto y que cumpla con los objetivos por los cuales fue desarrollado.

Se comprobó que son pocas las empresas que conocen el concepto de criterios de evaluación, aunque están conscientes de que es necesario la seguridad no conocen alguna metodología para realizar evaluaciones y además de que el concepto de criterios comunes es poco conocido y mucho menos la metodología para la evaluación del *software*.

En resumen, del grupo de empresas que fueron entrevistadas conocen la importancia del concepto de seguridad del *software* y cómo aplicar métodos para su utilización pero como aplicar una metodología para su evaluación es poco probable.

CONCLUSIONES

1. El proceso de desarrollo de los criterios de evaluación para la tecnología de información, son un esfuerzo común entre países de Norteamérica y la unión europea para desarrollar un solo sistema de criterios internacionales de evaluación para el reconocimiento de la seguridad.

2. La metodología de evaluación aplica sus principios, los cuales deben emplearse por las partes involucradas en la evaluación y el esquema que utiliza dicha metodología para la aplicación oportuna de sus principios.

3. Los servicios de seguridad que se deberían ofrecer en una red de computadoras son autenticación, confidencialidad, control de acceso e integridad; para los servicios de seguridad de Internet implementar los servicios de encriptación, firmas digitales, funciones de transformación y control de accesos.

4. Reforzar en las diferentes universidades del país en las que se forman a los futuros profesionales de la informática, la necesidad de utilizar métodos para la evaluación de su *software*, seguridad en la red, accesos a Internet y en los manejadores de bases de datos.

5. El 80% de las empresas entrevistadas desconocen de la metodología para la evaluación de la seguridad del *software*, aunque si utilizan métodos de seguridad que les proporcionan el sistema operativo y su manejador de base de datos.

RECOMENDACIONES

1. Fomentar la importancia que se debe tener sobre la seguridad en los productos de *software* que se desarrollan por las organizaciones, y aplicarlos a través de una metodología de evaluación del *software*.

2. Dar énfasis en que la seguridad no solo se debe enfocar a nivel del *software*, también debe contemplarse el sistema operativo y todas aquellas herramientas necesarias que se requieran para asegurarse de la confiabilidad de la información.

3. Reforzar a las partes que desarrollan *software* para Internet sobre las medidas preventivas para la seguridad al momento de transmitir información por la red, ya que esto ocasionaría que intrusos puedan acceder a su información y consecuencia de ello perder la inconsistente de los mismos.

4. De los resultados de las entrevistadas a las empresas en la ciudad capital de Guatemala, están conscientes de la importancia que se le debe dar a la seguridad del *software*, ya que de ella depende la consistencia de la información que manejan.

5. Sin importar la metodología que se utilice para el desarrollo de productos de *software,* es necesario que los analistas y desarrolladores, generen *software* seguro, tomando en cuenta todo su entorno para evitar que la información sea manipulada por agentes externos.

BIBLIOGRAFÍA

1. Agencia de seguridad federal <http://csrc.nist.gov/fasp/ febrero 2003.

2. Calidad del *software* <http://www.ati.es/gt/calidad-software/presentacion.htm noviembre 2002.

3. Características del *software* <http://projects.openresources.com/libresoft-notes/libresoft-notes-es/node14.html julio 2002.

4. Claver, E**. Los sistemas y tecnologías de la información. Su repercusión en las estructuras Empresariales**. 2ª ed. Zaragoza: Alta Dirección, 1998.

5. Date,C.J. **Sistemas de base de datos**. 5ª ed. (volumen 1) Estados Unidos de América: Addison Wesley Iberoamericana, 1993.

6. Datos distribuidos <http://www.cs.cinvestav.mx/SC/prof_ personal /adiaz/ Disdb/Cap_1.html mayo 2002.

7. Deitel, Harvey. **Sistemas Operativos**. 2ª ed. Estados Unidos de América: Addison Wesley Iberoamerica, 1993. 150 pp.

8. Estudio del impacto de seguridad en el desempeño de Internet <http://wwwisc.uniandes.edu.co/~revista/articulos/seguridad/memtes.htm septiembre 2002.

9. Implementación de servidor de seguridad <http://www.microsoft.com/latam/ technet/articulos/200104/art02/default.asp julio 2003.

10. Organización de criterios comunes <www.commoncriteria.org marzo 2003.

11. Orígenes de criterios comunes http://www.commoncriteria.org/docs/origins .html julio 2003.

12. Pérez. I. Investigación del Mercado de *Software* en la Provincia Granma. Tesis de Maestría, España, Facultad de Ingeniería, 1999. 120 pp.