UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

POSGRADO EN CIENCIA E INGENIERIA DE LA COMPUTACION

CRITERIOS COMUNES PARA EVALUACION DE SEGURIDAD DE TECNOLOGIA DE LA INFORMACION

T E S I S

QUE PARA OBTENER EL GRADO DE:

MAESTRA EN CIENCIAS

P R E S E N T A:

MARIA JAQUELINA LOPEZ BARRIENTOS

DIRECTOR DE TESIS: DR. ENRIQUE DALTABUIT GODAS

MEXICO, D. F. 2001

Gracias

A Dios por la maravillosa familia que tengo.

A mi esposo Alejandro por su gran apoyo e infinito amor.

A mis dos estrellitas Carol y Alix que con su amor iluminan mi vida.

A mi mamá Elisa por su amor y disposición en todo momento.

Al Dr. Enrique Daltabuit por su tiempo, su dedicación, sus conocimientos, y su confianza en mí para llevar a cabo este trabajo.

ÍNDICE

Prólogo 1

Capítulo 1 5

Antecedentes

1.1 Historia de la seguridad IT 6

1.2 Presentación de los CC 9

Capítulo 2 12

Descripción de la seguridad de la Tecnología de la información

2.1 Presentación 13

2.2 Clasificación según el libro naranja 14

2.2.1 Políticas y Etiquetas 15
2.2.2 Responsabilización 15
2.2.3 Garantías 16
2.2.4 Documentación 16
2.2.5 Niveles 17
2.2.6 Funcionamiento 17

2.3 La serie arcoiris 18

2.4 Uso de los criterios comunes 24

2.4.1 Perfil de Protección 24
a) Propósito 24
b) Definición 24

c) Uso 25

2.5 Estructura 26

2.5.1 Introducción 26
2.5.2 Descripción del objetivo de la evaluación 26
2.5.3 Entorno de seguridad 27
2.5.4 Hipótesis 27
2.5.5 Amenazas 27
2.5.6 Políticas de la organización 28
2.5.7 Nivel de garantía general requerido 28
2.5.8 Objetivos 28
2.5.9 Requerimientos 29
2.5.10 Explicación 30
2.5.11 ¿Cómo se determina que se cumple un pp? 31

Capítulo 3 32

Curso sobre sistemas confiables basado en CC

3.1 Seguridad de tecnología de la información 33

3.2 Contexto de la seguridad 36

3.3 Entorno de seguridad 40

3.3.1 El entorno físico 40
3.3.2 Los bienes 40
3.3.3 El propósito 40

3.4 Políticas de seguridad 40

3.4.1 Hipótesis 41
3.4.2 Amenazas 41
3.4.3 Políticas de seguridad organizacional 41

3.5 Objetivos de seguridad 41

3.5.1 De manera directa por la TOE 42
3.5.2 Por el entorno de la TOE 42

3.6 Requerimientos de seguridad IT 42

3.6.1 Requerimientos funcionales 42
3.6.2 Requerimientos de garantía 43

3.7 Sumario de especificación TOE 44

3.8 Utilización de recursos 44

3.8.1 Tolerancia a fallas 44
3.8.2 Prioridad de servicio 45
3.8.3 Asignación de recursos 45

3.9 Protección de la TSF 45

3.9.1 Prueba de la máquina abstracta subyacente 45
3.9.2 Seguro ante fallas 46
3.9.3 Disponibilidad de datos TSF exportados 46
3.9.4 Confidencialidad de datos TSF exportados 46
3.9.5 Integridad de datos TSF exportados 46
3.9.6 Transferencia interna TOE de datos TSF 46
3.9.7 Protección física de la TSF 46
3.9.8 Recuperación confiable 47
3.9.9 Detección de retransmisión 47
3.9.10 Mediación de referencia 47
3.9.11 Separación de dominio 48
3.9.12 Protocolo de sincronía de estado 49
3.9.13 Sellos de tiempo 49
3.9.14 Consistencia de datos TSF inter- TSF 49
3.9.15 Consistencia de retransmisión de datos TSF de la TOE interna 49
3.9.16 Autoverificación de la TSF 50

3.10 Soporte de cifrado 50

3.10.1 Administración de claves de cifrado 50
3.10.2 Operación de cifrado 51

3.11 Acceso a la TOE 51

3.11.1 Limitación en el ámbito de atributos seleccionables 51

3.11.2Limitación en múltiples sesiones concurrentes 51
3.11.3Cierre de sesión 51
3.11.4Banderas de acceso a la TOE 52
3.11.5Historial de acceso a la TOE 52
3.11.6Establecimiento de sesión TOE 52

3.12 Identificación y autenticación 52

3.12.1 Fallas de autenticación 53
3.12.2Definición de atributos de usuario 53
3.12.3 Especificaciones sobre los secretos 53
3.12.4 Autenticación de usuario 53
3.12.5 Identificación de usuario 53
3.12.6 Enlace usuario-sujeto 54

3.13 Protección de datos de usuario 54

3.13.1 Política de control de acceso 54
3.13.2Funciones de control de acceso 55
3.13.3 Autenticación de datos 55
3.13.4 Exportación al exterior del control TSF 55
3.13.5 Política de control de flujo de información 55
3.13.6 Funciones de control de flujo de información 56
3.13.7 Importación desde el exterior del control TSF 56
3.13.8 Transferencia TOE interna 56
3.13.9 Protección de información residual 57
3.13.10Retroceso 57
3.13.11 Integridad de datos almacenados 57
3.13.12 Protección de transferencia de la confidencialidad de los datos de usuario inter-TSF 58
3.13.13 Protección de transferencia de la integridad de los datos de usuario inter-TSF 58

3.14 Comunicación 58

3.14.1No-repudio de origen 58
3.14.2No-repudio de receptor 58

3.15 Privacía 59

3.15.1Anonimato 59

3.15.2 Pseudonimia 59
3.15.3 Imposibilidad de asociación 59
3.15.4 Inobservabilidad 59

3.16 Caminos/Canales confiables 60

3.16.1 Canal confiable inter-TSF 61
3.16.2 Camino confiable 61

3.17 Administración de la seguridad 61

3.17.1 Administración de funciones en TSF 62
3.17.2 Administración de atributos de seguridad 62
3.17.3 Administración de datos TSF 62
3.17.4 Revocación 62
3.17.5 Vigencia de atributos de seguridad 62
3.17.6 Perfiles de administración de seguridad 62

3.18 Auditoría de seguridad 63

3.18.1 Respuesta automática de auditoría de seguridad 63
3.18.2 Generación de datos de auditoría de seguridad 63
3.18.3 Análisis de auditoría de seguridad 63
3.18.4 Revisión de auditoría de seguridad 63
3.18.5 Selección del evento de auditoría de seguridad 64
3.18.6 Almacenamiento del evento de auditoría de seguridad 64

Capítulo 4 65

Caso práctico: Desarrollo del PP de firewalls de filtrado de paquetes para entornos de bajo riesgo

4.1 Descripción de la TOE 66

4.2 Entorno de seguridad de la TOE 67

4.2.1 Hipótesis 67
4.2.2 Amenazas 68
4.2.2.1 Amenazas referentes a la TOE 68
4.2.2.2 Amenazas referentes al entorno operacional 69

4.3 Objetivos de seguridad 69

4.3.1 Objetivos de seguridad IT 69
4.3.2 Objetivos de seguridad no relacionados a IT 69

4.4 Requerimientos de seguridad IT 70

4.4.1 Requerimientos funcionales de seguridad TOE 71
4.4.2 Requerimientos de garantía de seguridad TOE 80

4.5 Vulnerabilidades identificadas 88

Conclusiones 94

Apéndice "A"
(Glosario de términos) 98

Apéndice "B"
(Autorización del NIST para traducir CC al español) 100

Bibliografía 102

Prólogo

"...la seguridad de los sistemas de información y de las redes es el mayor desafío de la seguridad de esta década y posiblemente del próximo siglo...no se tiene la suficiente conciencia del grave riesgo al que nos enfrentamos en este campo."

Redefining Security, Joint Security Commission /NSA 2000

El uso continuo de equipos de cómputo se ha venido dando desde hace varias décadas, en forma tal que cada día se incrementa de manera considerable el uso de sistemas y/o productos de Tecnología de la Información, y de igual forma cada día son más las funciones vitales para la humanidad que están basando su ejecución, su correcto desempeño, su privacía, su integridad, e inclusive su futuro en la Tecnología de la Información. De manera que conforme en el mundo las sociedades utilicen cada vez más este poderoso recurso y de igual forma dependan de él, más importante y crítica se volverá la seguridad de la información. Así, existe una necesidad real para incrementar el conocimiento de los temas referentes a la seguridad de la información.

Un sistema o producto de Tecnología de la Información (IT) es seguro si se puede confiar en que opere como se espera [9].

Si por ejemplo, se espera que los datos que se ingresan a él permanezcan ahí sin que nadie que no cuente con la debida autorización pueda acceder a ellos, y el sistema o producto IT efectivamente opera así, entonces se puede confiar en su seguridad; lo que conlleva a la necesidad de efectuar pruebas a equipos, programas, etc. que aseguren y garanticen la integridad, la confidencialidad y la disponibilidad de la información, y en este sentido también surge la necesidad de emplear criterios que identifiquen qué es lo que se espera de los productos y/ o sistemas IT en términos de seguridad e igualmente criterios que permitan evaluar la seguridad de éstos.

En este sentido, se sabe que Internet se ha convertido en la red más grande del mundo y el recurso de dominio público y de uso general más difundido, de manera que continuamente se distribuye a través de ella información generada no sólo por universidades, instituciones públicas y centros de investigación, sino también por empresas y hasta por individuos que contribuyen a expandir los servicios de información. En este esquema todos los participantes según sus necesidades hacen uso de sistemas y/o productos de tecnología de la información, y podría decirse que en términos generales la mayoría de los sistemas de cómputo son un objetivo potencial para intrusos maliciosos, lo que conlleva a la apremiante necesidad de contar con sistemas y/o productos seguros y que los criterios para evaluarlos también sean de uso general en el mundo, que sean Criterios Comunes para Evaluación de Seguridad de Tecnología de la Información.

En el esquema planteado participa activamente México, y sin embargo es un tema muy poco tratado y desarrollado en nuestro país, en el cual el uso de las redes de cómputo, así como el desarrollo y uso de sistemas aumenta considerablemente día a día y toma gran relevancia, de manera que el no contar con sistemas seguros, ni profesionales de la seguridad nos hace cada día mas vulnerables, de ahí que la finalidad del presente trabajo es: *realizar una investigación sobre el estado del arte que guarda la seguridad IT, proponer una metodología para describir las características de seguridad necesarias para efectuar licitaciones y con esto desarrollar una guía dirigida a todas aquellas personas que en México requieren adquirir sistemas de cómputo para sus instituciones académicas o de investigación, organizaciones empresariales o gubernamentales etc. con el fin de que utilicen los criterios aquí plasmados para afinar las bases de sus licitaciones enfocadas a sus necesidades muy particulares y que dichos sistemas sean seguros y confiables, y finalmente proponer el temario de un curso sobre sistemas confiables para ser impartido como parte de un programa de estudios avanzados sobre seguridad.*

De manera que el capítulo 1 presenta un recorrido por la historia de la seguridad en tecnología de la información, la cual llega a nuestros días con el desarrollo del estándar "Common Criteria for Information Technology Security Evaluation" (CCITSE) usualmente referido como "Common Criteria" (CC) y publicado a fines de 1999.

Como la información y los sistemas de información son de suma valía para sus propietarios; se considera que deben ser tratados como un recurso estratégico de la organización o la institución que va a hacer uso de ellos, así el capítulo 2 es una guía dirigida a todas aquellas personas que en México requieren adquirir sistemas y/o productos IT con el fin de que utilicen los criterios aquí plasmados y basados en CC.

Buscando incrementar el conocimiento de los profesionales de los temas referentes a la seguridad IT, el capítulo 3 del presente trabajo es un curso sobre sistemas confiables basado en CC con el objeto de proporcionar a los estudiantes de estudios avanzados en seguridad, las herramientas y los lineamientos necesarios para lograr tener sistemas con seguridad IT en sus funciones como evaluadores, desarrolladores y/o consumidores.

Finalmente, en el capítulo 4 se presenta un caso práctico, es la aplicación de CC en la cual se desarrolla el Perfil de Protección para firewalls de filtrado de paquetes, donde se definen los requerimientos de seguridad básicos que éstos deben cubrir para ser utilizados en organizaciones que manejan información en entornos de bajo riesgo, que se cubran los requerimientos y objetivos de seguridad planteados y que el objeto de evaluación (en este caso firewalls) brinde protección contra las vulnerabilidades encontradas.

Adicionalmente el presente trabajo contiene un CD con la traducción del documento "Criterios Comunes para Evaluación de Seguridad de Tecnología de la Información (CC2.1)" el cual se alinea con el Estándar Internacional ISO/IEC 15408:1999. Cabe hacer mención que se trata de un documento extenso el cual cuenta con la aprobación del NIST (National Institute of Standards and Technology) para su traducción y publicación en español con fines académicos (véase Apéndice B) lo cual es de suma importancia para todo el mundo de habla hispana y directamente reportará un beneficio mayúsculo en todos aquellos estudiantes hispanoamericanos que en cualquier parte del mundo se encuentren realizando estudios de doctorado, maestría y/o licenciatura como apoyo para entender el proceso de evaluación y caracterización de la confiabilidad de sistemas en las clases sobre seguridad.

Capítulo 1

Antecedentes

En los primeros años del uso de la información y su tecnología asociada, los usuarios de ésta pertenecían al mundo académico, a comunidades de investigación en cómputo, a organismos gubernamentales y a la misma industria de cómputo; de ahí que en esos ambientes la seguridad de la información solo fuera relevante para las organizaciones gubernamentales (de América y Europa) preocupadas por mantener los secretos de la nación; pero con el paso del tiempo Internet se ha convertido en la red más grande del mundo y el recurso de dominio público más difundido, con lo que muchos tipos de personas pueden acceder a los sistemas de cómputo, y entre ellos intrusos maliciosos que pretenden destruir, robar o bloquear información. A lo largo del último par de décadas muchas han sido las instituciones preocupadas por la seguridad IT y por contar con criterios que operen a nivel mundial, al igual que las redes, y los sistemas y productos IT que las conforman llegando a nuestros días el estándar conocido como "Common Criteria for Information Technology Security Evaluation" (CCITSE) usualmente referido como "Common Criteria" (CC).

1.1 Historia de la seguridad IT

En la década de los 80's el NCSC (National Computer Security Center) de E.E.U.U. emitió una serie de libros clasificados por colores, los cuales abordaban diferentes problemáticas de seguridad. Así, el libro naranja (Orange Book) llamado oficialmente Departament of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC) [10]contiene requerimientos básicos en cuatro categorías para sistemas operativos confiables: política de seguridad, responsabilidad, garantía y documentación. Posteriormente se emitió el libro rojo (Red Book) llamado oficialmente Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria (TCSEC) el cual contiene una interpretación del libro naranja con respecto a los requerimientos para redes, y un sumario de servicios específicos de red: integridad de comunicaciones, denegación de servicio, y protección de compromiso.

En esta serie de libros* se definen las distintas categorías de confiabilidad, integridad, disponibilidad y autenticidad que surgen directamente de las necesidades de las fuerzas armadas de los E.E.U.U., y cuyo uso se ha generalizado debido a su disponibilidad. De manera que se ha publicado esta categorización y a lo largo de los años se han clasificado de esta manera los elementos que conforman los sistemas de información destinados al mercado que no es de índole militar; así en esta serie de documentos se encuentra la información necesaria para especificar con precisión las características de seguridad de cualquier equipo que se piense adquirir o desarrollar (pero desde un punto de vista militar); aunado a esto dichos documentos han quedado obsoletos con el paso del tiempo ya que no avanzaron ni se desarrollaron al ritmo de las necesidades presentes y futuras de su época.

En Europa, los Criterios de Evaluación de Seguridad de Tecnología de la Información (Information Technology Security Evaluation Criteria <ITSEC>) versión 1.2 [5] fueron publicados en 1991 por la Comisión Europea, y posteriormente los trabajos desarrollados por las naciones de Francia, Alemania, los Países Bajos, y el Reino Unido. En Canadá, los Criterios de Evaluación de Productos de Cómputo Confiables Canadienses (Canadian Trusted Computer Product Evaluation Criteria <CTCPEC>) versión 3.0 fueron publicados a principios de 1993 como una combinación de los ITSEC y los TCSEC[11]. En los Estados Unidos, el proyecto de los Criterios Federales

*http://www.radium.ncsc.mil/tpep/ttap/facilities.html

para Seguridad de Tecnología de la Información (Federal Criteria for Information Technology Security <FC>) versión 1.0 fue publicado a principios de 1993 [4], como un segundo planteamiento con la finalidad de fusionar los conceptos de Norte América y Europa y conformar así los criterios de evaluación que operen en todo el mundo[2].

En junio de 1993, las organizaciones responsables de los CTCPEC, FC, TCSEC e ITSEC unieron sus esfuerzos y comenzaron a realizar actividades conjuntas para apegar sus criterios hasta ahora divididos, en un solo conjunto de criterios de seguridad IT que pudieran ser ampliamente usados. Estas actividades fueron nombradas Proyecto CC, cuyo propósito fue resolver las diferencias conceptuales y técnicas encontradas en aquellos primeros criterios y expresar los resultados a la ISO como una contribución a los estándares internacionales en desarrollo[6]. El órgano representativo formado por las organizaciones responsables fue el Consejo Editorial de CC (CC Editorial Board <CCEB>) para desarrollar los CC. Entonces se estableció un vínculo entre el CCEB y el WG 3, y el CCEB contribuyó en el desarrollo de las primeras versiones de los CC a través del WG 3 como su canal de vinculación. Como resultado de la interacción entre WG 3 y el CCEB, estas versiones fueron adoptadas para escribir varias partes de los trabajos sucesivos de los criterios ISO comenzados en 1994**.

Así, en enero de 1996 los Estados Unidos a través del NIST (National Institute of Standards and Technology) y de la NSA (National Security Agency), el Reino Unido a través del CESG (Communications-Electronics Security Group), Alemania a través del BSI (Bundesamt für Sicherheit in der Informationstechnik), Francia a través del SCSSI (Service Central de la Sécurité des Systèmes d'Information), Canadá a través del CSE (Communications Security Establishmente), y Holanda a través de la NNCSA (Netherlands National Communications Security Agency) liberaron conjuntamente los estándares desarrollados para un mercado multi-nacional. Este estándar es conocido como "Common Criteria for Information Technology Security Evaluation" (CCITSE) usualmente referido como "Common Criteria" (CC)***.

El proyecto de CC se concibió en los trabajos cooperativos relacionados con la Organización Internacional de Estándares (ISO), el Comité Técnico Mixto I

** http://www.radium.ncsc.mil/tpep/ttap/facilities.html
*** http://www.commoncriteria.org

"Tecnología de la Información", el Subcomité 27 – "Técnicas de Seguridad", el Grupo de Trabajo 3 – "Criterios de Seguridad" (o solo WG3) para desarrollar y mantener (lo que no se hizo con los libros anteriores y que los llevó a la obsolescencia) un estándar internacional de criterios de seguridad de Tecnología de la Información basado en los Criterios Comunes.

La versión anterior 2.0 de CC fue idéntica en contenido a la Redacción Final del Comité (FCD)15408 sometida a votación dentro de la ISO durante el verano de 1998. Fue entonces que el WG3 hizo algunos cambios al texto (FCD) en octubre del mismo año para crear la Redacción Final del Estándar Internacional (FDIS) 15408, el cual fue sometido a votación y aprobado en ISO el 04 de junio de 1999. Subsecuentemente ISO aprobó y publicó dicho texto como el Estándar Internacional (IS) 15408 el 1° de diciembre de 1999*[v].

La figura 1.1 representa el recorrido histórico que dió por resultado los CC.

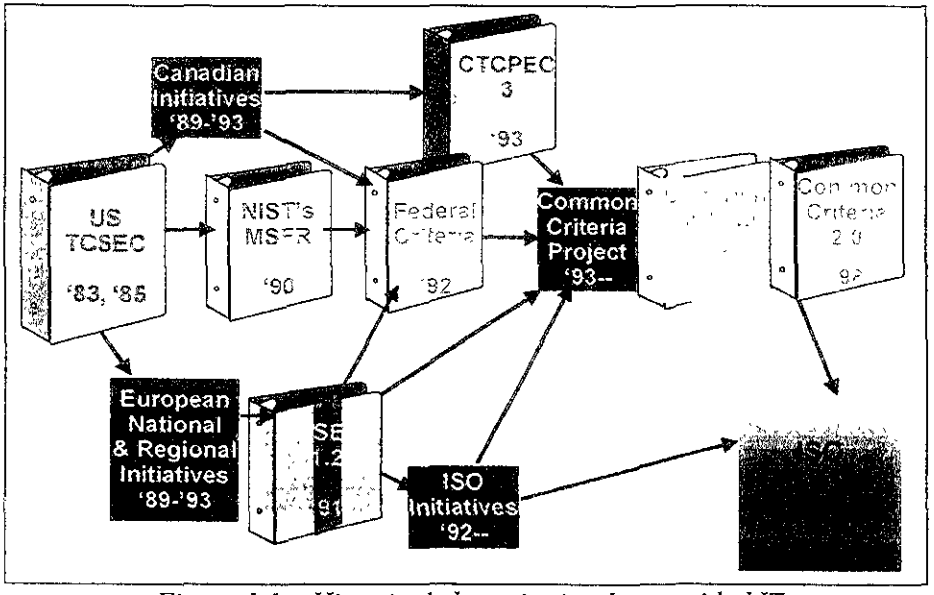

Figura 1.1 – Historia de los criterios de seguridad IT

[v] http://www.commoncriteria.org

1.2 Presentación de los CC

El proyecto de CC versión 2.1 incorpora los últimos cambios hechos por ISO, de manera que esta versión de CC y el IS 15408 ahora son totalmente compatibles y equivalentes.

Los CC tienen como finalidad brindar protección a la información para evitar: la *revelación no autorizada de secretos, modificación, o pérdida de uso*. Las categorías de protección relacionan estos tres tipos de fallas de seguridad, las cuales son llamadas comúnmente *confidencialidad, integridad y disponibilidad*, respectivamente.

Los CC se aplican a medidas de seguridad implementadas en hardware, firmware o software. Donde los aspectos particulares de la evaluación se aplicarán únicamente a métodos seguros de implantación, los cuales estarán indicados dentro de los informes de criterios relevantes.

Los CC permiten hacer comparaciones entre los resultados de evaluaciones de seguridad independientes y son una guía para el desarrollo de productos o sistemas con funciones de seguridad IT y para la procuración de productos y sistemas comerciales con tales funciones.

Se consideran tres grupos con intereses generales en la evaluación de las propiedades de seguridad de productos y sistemas IT*[v]: *consumidores, desarrolladores, y evaluadores.*

Los "Criterios Comunes" pueden ser usados para los siguientes propósitos:

- Encontrar los requerimientos de las características de seguridad que corresponden a la valoración de sus propios riesgos.
- Adquirir los productos que tienen la clasificación de las características deseadas.
- Publicar sus requerimientos de seguridad de manera que los vendedores puedan diseñar productos que reúnan dichos requerimientos.
- Seleccionar los requerimientos de seguridad que desean incluir en sus productos.
- Diseñar y construir productos de tal forma que pueda probar a los evaluadores que el producto reúne los requerimientos.

[v] http://www.commoncriteria.org

- Determinar sus responsabilidades en el soporte y la evaluación de su producto.
- Juzgar si un producto reúne o no sus requerimientos de seguridad.
- Proporcionar un criterio contra el cual pueden llevarse a cabo las evaluaciones.
- Proporcionar entradas cuando se modelan métodos de evaluación específicos.

Bajo los Criterios Comunes, cada nivel de clasificación confiable del TCSEC ahora se puede especificar como un Perfil de Protección (PP). Un Perfil de Protección tiene un aspecto muy similar a aquél nivel de clasificación o categorización pero tiene dos diferencias fundamentales: Primero, cuando el TCSEC vincula conjuntos de características y garantías juntas, los Criterios Comunes permiten que los Perfiles de Protección combinen características y garantías juntas en cualquier combinación[v]. Además, el TCSEC especifica un conjunto fijo de diferentes clasificaciones (perfiles), en tanto que los Criterios Comunes permiten a los consumidores escribir un conjunto específico y muy propio de sus requerimientos particulares en un formato estándar.

En tanto que los CC están orientados hacia la especificación y la evaluación de las propiedades de seguridad IT de la meta u objeto de evaluación, debe además ser de utilidad como material de referencia para todas las partes que estén interesadas en la responsabilidad de la seguridad IT. Algunos de los grupos de interés adicional que pueden beneficiarse de la información contenida en los CC son:

a) custodios de sistemas y oficiales responsables de la seguridad de sistemas para determinar y reunir las políticas de seguridad IT organizacionales y sus requerimientos;

b) auditores internos y externos, responsables de garantizar la adecuación de los sistemas de seguridad;

c) arquitectos y diseñadores de seguridad para la especificación del contenido de seguridad de sistemas y productos IT;

d) acreditadores responsables para la aceptación de sistemas IT para el uso dentro de un medio ambiente particular;

[v] http://www.radium.ncsc.mil/tpep/process/faq-sect1.html

e) patrocinadores o presentadores de evaluaciones responsables de la solicitud y apoyo de una evaluación; y

f) autoridades de evaluación responsables de la administración y la vigilancia de programas de evaluación de seguridad IT.

La versión 2.1 de Criterios Comunes compatible con IS 15408 está conformada por tres partes:

Parte 1, INTRODUCCIÓN Y MODELO GENERAL[*v], es la introducción a los CC. Se definen los conceptos generales y los principios de la evaluación de seguridad IT y se presenta un modelo general de evaluación. La parte 1 además construye éstos para expresar los objetivos de seguridad, para la selección y definición de los requerimientos de seguridad IT, y para escribir especificaciones de alto nivel para productos y sistemas. Adicionalmente, la utilidad de cada parte de los CC está descrita en términos de cada una de las metas del público en general.

Parte 2, REQUERIMIENTOS DE SEGURIDAD FUNCIONAL[*v], establece un conjunto de componentes funcionales como una forma estándar de expresión de los requerimientos funcionales para la TOE (Meta de Evaluación). La parte 2 cataloga un conjunto de componentes funcionales, familias, y clases.

Parte 3, REQUERIMIENTOS DE SEGURIDAD CONFIABLE[*v], establece un conjunto de componentes de seguridad confiables como una forma estándar de expresión de los requerimientos de seguridad confiables para la TOE. La parte 3 cataloga un conjunto de componentes seguros, familias y clases, y asimismo define los criterios de evaluación para los PP (Perfiles de Protección) y las ST (Metas de Seguridad), y presenta los niveles de seguridad de la evaluación que definen los CC establecidos en una escala para evaluar la seguridad de la TOE, a los cuales se les llama Niveles de Seguridad o de Garantía de la Evaluación (EAL)

[*v] *http://www commoncriteria org y http //csrc ncsl nist gov/cc/ccv20/ccv2list*

Capítulo 2

Descripción de la seguridad de la Tecnología de la Información

Uno de los recursos más valiosos con que cuenta una organización es su información, de ahí que se requiera hacer uso de sistemas y/o productos de tecnología de la información para procesarla, producirla, almacenarla y transmitirla; y en cada uno de estos pasos la información debe estar disponible al momento que se le requiera y siempre en forma confidencial e íntegra. Para lo cual es necesario que la especificación del equipo que se va a adquirir para emplear IT tome en cuenta la problemática de la seguridad, y en buena medida esta problemática determinará las características de la tecnología a emplear, por lo que es fundamental contar con un mecanismo preciso y estándar que permita describir la problemática sin hacer referencia a productos específicos. De manera que el material que aquí se presenta en forma concisa y las referencias contenidas son una guía que proporciona lo necesario para desarrollar una descripción adecuada

2.1 Presentación

El desarrollo y uso de sistemas de información se ha venido dando desde hace varias décadas, pero en la actualidad ocupa un lugar importante en todo el mundo, (empresas, organizaciones, institutos, universidades, etc.) donde existe la necesidad de usar, desarrollar y evaluar sistemas de información a la medida de sus necesidades; pero sobre todo en los años recientes cuidando la seguridad de la información concerniente a privacía, confidencialidad, integridad, control de acceso, no repudio y autenticación.

Al término "confiabilidad" se le da un significado técnico que se define en el libro Rojo[v*], y es una precisión del significado del término "confianza" : dícese de las cosas que poseen cualidades recomendables para el fin que se destinan. De manera que se especifican cuáles son las cualidades recomendables de los sistemas de información de una manera sistemática; y en base a conjuntos de cualidades se establecen las categorías que ofrecen diferentes tipos y niveles de confianza.

En el proceso de adquirir un sistema de información es necesario decidir qué confiabilidad debe tener éste para cumplir con su misión de seguridad [7] .

La misión debe definirse en términos de cuatro requerimientos que son:

Preservar:

- la confiabilidad
- la integridad
- la autenticidad
- la disponibilidad

En esta serie de libros se definen las distintas categorías que surgen directamente de las necesidades de las fuerzas armadas de los E.E.U.U., y cuyo uso se ha generalizado de manera extraordinaria y probablemente hasta excesiva debido a su disponibilidad. De manera que se ha publicado esta categorización y a lo largo de los años se han clasificado de esta manera los elementos que conforman los sistemas de información destinados al mercado que no es de índole militar; resultando con ello que la descripción de la confiabilidad que se desea tenga un sistema que se pretende adquirir, en muchos casos esté basada en esta categorización pre-establecida.

[v*] http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-005.txt

En tanto que los Criterios Comunes ofrecen una metodología para poder llevar a cabo una descripción de la confiabilidad que se desea de un sistema que no tiene relación alguna y no requiere de un punto de vista militar, y que además es prácticamente aceptable en todo el mundo. Aunado a esto, los Criterios Comunes constituyen un lenguaje común tanto para fabricantes, proveedores, como para los consumidores, quienes requieren de productos de tecnología de la información que sean precisos y fáciles de usar.

2.2 Clasificación según el libro naranja

Según el Libro Naranja [10], los Criterios de Evaluación de la Confiabilidad de Sistemas de Cómputo se establecen de acuerdo con tres objetivos:

- Las políticas de seguridad y las etiquetas
- La responsabilización
- Las garantías

Y aunado a esto, la existencia de la documentación respectiva.

Un sistema puede ser o no aceptable según algún cierto criterio; o bien, puede tener la capacidad de ser aceptable, y que por causa de una implementación o un uso equivocado, dicho sistema no sea aceptable en base a algún criterio en un caso dado.

Además, un sistema sólo puede ser calificado como seguro o aceptable dentro del contexto de las políticas de seguridad que dicho sistema debe mantener[***], las cuales se determinan en base a la información que se está protegiendo, a una estimación de las amenazas a las que está sujeta y al uso que se le pretende dar a la información.

De manera que para determinar qué sistema de información es el adecuado para garantizar la aplicación de las políticas establecidas, se requiere una metodología de descripción genérica de las salvaguardas que son necesarias.

[***] http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.txt

2.2.1 Políticas y Etiquetas

Las políticas y las etiquetas son el primer objetivo y sus componentes son los que se muestran a continuación : (ver tabla 2.1)

Tabla 2.1 – Componentes de las políticas y las etiquetas[10]

	C1	C2	B1	B2	B3	A1
Control de Acceso Discrecional (DAC)	b	i	i	i	a	a
Reuso de objetos		b	i	i	i	i
Etiquetas			b	i	i	i
Integridad de las etiquetas			b	b	b	b
Exportación de información etiquetada			b	b	b	b
Exportación a dispositivos multinivel			b	b	b	b
Etiquetas en la información legible			b	b	b	b
Control de acceso obligatorio (MAC)			b	i	i	i
Etiquetas de clasificación del contenido				b	b	b
Dispositivos etiquetados				b	b	b

Para que un sistema sea clasificado en alguna de estas categorías deben EXISTIR y estar escritas de manera explícita las políticas respecto a estos encabezados, el sistema debe poder soportarlas, y además, la implementación debe tener activas estas capacidades.

2.2.2 Responsabilización

La responsabilización es el segundo objetivo y sus componentes son los que se muestran a continuación en la tabla 2.2:

Tabla 2.2 – Componentes de la responsabilización[10]

	C1	C2	B1	B2	B3	A1
Identificación y Autenticación	b	i	a	a	a	a
Auditoría		b	i	a	ma	ma
Trayectoria confiable				b	i	i

Para que un sistema sea clasificado en alguna de estas categorías tienen que *existir* y estar funcionando mecanismos para implementar estas funciones.

2.2.3 Garantías

Las garantías son el tercer objetivo y sus componentes son los que se muestran a continuación en la tabla 2.3:

Tabla 2.3 – Componentes de las garantías[10]

	C1	C2	B1	B2	B3	A1
Arquitectura del sistema	b	i	a	ma	e	e
Especificación y verificación del diseño			b	i	a	ma
Análisis de canales encubiertos				b	i	i
Administración confiable del sitio				b	i	i
Administración de la configuración				b	b	i
Recuperación confiable					b	b
Distribución confiable						b

Para que un sistema sea clasificado en alguna de estas categorías, es requisito que el sistema esté diseñado para garantizar una aplicación correcta y precisa de la interpretación de las políticas de seguridad sin que se distorsionen. Estas garantías (típicamente el equipo y el sistema operativo)deben poderse evaluar de manera independiente, y deben identificarse los mecanismos correspondientes en forma explícita. Los mecanismos deben estar protegidos constantemente para evitar alteraciones o modificaciones no autorizadas.

2.2.4 Documentación

La documentación es de suma importancia, e impone las siguientes condiciones: (ver tabla 2.4)

Tabla 2.4 – Documentación[10]

	C1	C2	B1	B2	B3	A1
Guía del usuario de las funciones de seguridad	b	b	b	b	b	b
Manual del sitio confiable	b	i	a	ma	c	c
Documentación de las pruebas	b	b	b	i	i	a
Documentación del diseño	b	b	i	a	ma	c

Para que un sistema sea clasificado en alguna de estas categorías se deben tener y usar los documentos mencionados en la tabla 2.4.

2.2.5 Niveles

En la tabla 2.5 se presenta de qué manera se indica el nivel de la característica considerada:

Tabla 2.5 - Nivel de la característica considerada[10]

b	Básico
i	Intermedio
a	Avanzado
ma	Muy avanzado
e	Extraordinario
ee	Especialmente extraordinario

2.2.6 Funcionamiento

La evaluación realizada a productos a solicitud expresa del proveedor es diferente a la evaluación para certificación[***], que sirve para certificar la confiabilidad de un sistema con respecto a una misión específica.

Debe notarse que en todos los casos, a excepción de los marcados (Control de Acceso discrecional, Reutilización de objetos, Integridad del sistema y Guía del usuario de las funciones de seguridad) los requerimientos de los sistemas clasificados como B3 tienen elementos adicionales a los clasificados como B2. En muchos casos los sistemas clasificados como B1 tienen elementos adicionales a los de la clase C2.

Se dice que la clase B1 es una clase C2 con etiquetas. La diferencia no es trivial pues todos los sujetos (entes activos como usuarios, programas, etc.) y todos los objetos (entes pasivos como archivos, impresoras, listados, etc.) deben tener una jerarquización de seguridad, que esta jerarquización debe permitir establecer una relación de dominancia, y que cada acción de un sujeto sobre un objeto debe estar mediada por un motor de referencia que verifica la relación de dominancia entre el sujeto y el objeto y que según esto, autoriza e impide la acción [10] .

[***] http://nap.nist.gov/

2.3 La serie arcoiris

En la serie arcoiris se extienden los conceptos básicos presentados en el subcapítulo anterior, y se les interpreta en el contexto de otras plataformas de tecnología de la información. Esta serie está conformada por los siguientes documentos:

- 5200.28-STD*[^]
  DoD Trusted Computer System Evaluation Criteria, 26 December 1985 (Supercedes CSC-STD-001-83, dtd 15 Aug 83). *(Orange Book)*

- CSC-STD-002-85*[^]
  DoD Password Management Guideline, 12 April 1985. *(Green Book)*

- CSC-STD-003-85*[^]
  Computer Security Requirements -- Guidance for Applying the DoD TCSEC in Specific Environments, 25 June 1985. *(Light Yellow Book)*

- CSC-STD-004-85*[^]
  Technical Rational Behind CSC-STD-003-85: Computer Security Requirements Guidance for Applying the DoD TCSEC in Specific Environments, 25 June 1985. *(Yellow Book)*

- NTISSAM COMPUSEC/1-87*[^]
  Advisory Memorandum on Office Automation Security Guidelines

- NCSC-TG-001 Ver. 2*[^]
  A Guide to Understanding Audit in Trusted Systems 1 June 1988, Versión 2. *(Tan Book)*

- NCSC-TG-002*[^]
  Trusted Product Evaluations - A Guide for Vendors, 22 June 1990. *(Bright Blue Book)* see also TPEP Procedures which supersedes parts of this document.

*[^]Estos documentos se pueden encontrar en:
http://www.radium.ncs.mil/tpep/library/rainbow/index.html

- NCSC-TG-003*[x]
  A Guide to Understanding Discretionary Access Control in Trusted Systems, 30 September 1987. *(Neon Orange Book)*

- NCSC-TG-004*[x]
  Glossary of Computer Security Terms, 21 October 1988. *(Teal Green Book)* (NCSC-WA-001-85 is obsolete)

- NCSC-TG-005*[x]
  Trusted Network Interpretation of the TCSEC (TNI), 31 July 1987. *(Red Book)*

- NCSC-TG-006*[x]
  A Guide to Understanding Configuration Management in Trusted Systems, 28 March 1988. *(Amber Book)*

- NCSC-TG-007*[x]
  A Guide to Understanding Design Documentation in Trusted Systems, 6 October 1988. *(Burgundy Book)* see also Process Guidelines for Design Documentation which may supercede parts of this document.

- NCSC-TG-008*[x]
  A Guide to Understanding Trusted Distribution in Trusted Systems 15 December 1988. *(Dark Lavender Book)*

- NCSC-TG-009*[x]
  Computer Security Subsystem Interpretation of the TCSEC 16 September 1988. *(Venice Blue Book)*

- NCSC-TG-010*[x]
  A Guide to Understanding Security Modeling in Trusted Systems, October 1992. *(Aqua Book)*

- NCSC-TG-011*[x]
  Trusted Network Interpretation Environments Guideline - Guidance for Applying the TNI, 1 August 1990. *(Red Book)*

*[x] Estos documentos se pueden encontrar en:
http://www.radium.ncs.mil/tpep/library/rainbow/index.html

- NCSC-TG-013 Ver.2*[x]
  RAMP Program Document, 1 March 1995, Versión 2 *(Pink Book)*

- NCSC-TG-014*[x]
  Guidelines for Formal Verification Systems, 1 April 1989. *(Purple Book)*

- NCSC-TG-015*[x]
  A Guide to Understanding Trusted Facility Management, 18 October 1989 *(Brown Book)*

- NCSC-TG-016*[x]
  Guidelines for Writing Trusted Facility Manuals, October 1992. *(Yellow-Green Book)*

- NCSC-TG-017*[x]
  A Guide to Understanding Identification and Authentication in Trusted Systems, September 1991. *(Light Blue Book)*

- NCSC-TG-018*[x]
  A Guide to Understanding Object Reuse in Trusted Systems, July 1992. *(Light Blue Book)*

- NCSC-TG-019 Ver. 2*[x]
  Trusted Product Evaluation Questionaire, 2 May 1992, Versión 2. *(Blue Book)*

- NCSC-TG-020-A*[x]
  Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX® System, 7 July 1989. *(Silver Book)*

- NCSC-TG-021*[x]
  Trusted Database Management System Interpretation of the TCSEC (TDI), April 1991. *(Purple Book)*

*[x]Estos documentos se pueden encontrar en
http://www.radium.ncs.mil/tpep/library/rainbow/index.html

- NCSC-TG-022*[x]
  A Guide to Understanding Trusted Recovery in Trusted Systems, 30 December 1991. *(Yellow Book)*

- NCSC-TG-023*[x]
  A Guide to Understanding Security Testing and Test Documentation in Trusted Systems *(Bright Orange Book)* see also Process Guidelines for Test Documentation which may supercede parts of this document.

- NCSC-TG-024 Vol.1/4*[x]
  A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements, December 1992. *(Purple Book)*

- NCSC-TG-024 Vol. 2/4*[x]
  A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators, 30 June 1993. *(Purple Book)*

- NCSC-TG-024 Vol. 3/4*[x]
  A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial, 28 February 1994. *(Purple Book)*

- NCSC-TG-024 Vol. 4/4*[x]
  A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder's Proposal Document - An Aid to Procurement Initiators and Contractors *(Purple Book)* (publication TBA)

- NCSC-TG-025 Ver. 2*[x]
  A Guide to Understanding Data Remanence in Automated Information Systems, September 1991, Versión 2, (Supercedes CSC-STD-005-85). *(Forest Green Book)*

- NCSC-TG-026*[x]
  A Guide to Writing the Security Features User's Guide for Trusted Systems, September 1991. *(Hot Peach Book)*

*[x] Estos documentos se pueden encontrar en:
http://www.radium.ncs.mil/tpep/library/rainbow/index.html

- NCSC-TG-027*[x]
  A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems, May 1992. *(Turquoise Book)*

- NCSC-TG-028*[x]
  Assessing Controlled Access Protection, 25 May 1992. *(Violet Book)*

- NCSC-TG-029*[x]
  Introduction to Certification and Accreditation Concepts, January 1994. *(Blue Book)*

- NCSC-TG-030*[x]
  A Guide to Understanding Covert Channel Analysis of Trusted Systems, November 1993. *(Light Pink Book)*

En esta serie de documentos se encuentra la información necesaria para especificar con precisión las características de seguridad de cualquier equipo que se piense adquirir (pero desde un punto de vista militar).

Además existe el programa RAMP (Rating Maintenance Phase) que consiste en analizar las actualizaciones de los sistemas de información que han sido categorizados, esto con el fin de poder asegurar si es que mantienen su categoría en la que fueron clasificados, o si requieren ser re-clasificados. Este programa ha traído como ventaja colateral el que se impartan cursos al personal de empresas fabricantes, en las cuales algunos de sus empleados obtienen certificación para ayudar a que los productos mantengan su categoría, y además existe material[x] que se emplea para estos cursos en versión para extranjeros, y mediante el uso de este material se tiene la forma más directa de comprender las categorías establecidas en la serie arcoiris; los módulos que se pueden estudiar se muestran en la tabla 2.6.

---

*[x] Estos documentos se pueden encontrar en:
http://www.radium.ncs.mil/tpep/library/rainbow/index.html
la lista de productos clasificados se encuentran en:
http://www.radium.ncsc.mil/tpep/epl/epl-by-class.html
[x] la información y el material se puede encontrar en:
http://radium.ncsc.mil/tpep/library/ramp-Modulos/index.html

Tabla 2.6 – Módulos de cursos (Serie Arcoiris)[x]

Módulo 1	Panorama de los Sistemas Confiables	
Módulo 2	Certificación y Acreditación	
Módulo 3	Políticas, Instrucciones, Estándares y Guías	
Módulo 4	TCSEC y panorama del proceso de clasificación	Examen
Módulo 5	Políticas y Modelos de Seguridad	Examen
Módulo 6	Monitor de Referencia y Base de Cómputo Confiable	Examen
Módulo 7	Arquitectura y Diseño	Examen
Módulo 8	Control de Acceso Obligatorio y Etiquetas	Examen
Módulo 9	Control de Acceso Discrecional	Examen
Módulo 10	Reutilización de Objetos	Examen
Módulo 11	Identificación y Autenticación	Examen
Módulo 12	Auditoría	Examen
Módulo 13	Garantías	Examen
Módulo 14	Documentación	Examen
Módulo 15	Administración de la Configuración	Examen
Módulo 16	Conservación de la Clasificación	Examen
Interpretación para Bases de Datos (TDI)	Introducción	
TDI Módulos TDI	Introducción	
TDI Módulo 1	Clasificación de Sistemas de Administración de Bases de Datos	
TDI Módulo 2	Políticas y Requerimientos	
TDI Módulo 3	Arquitecturas	
TDI Módulo 4	Problemas de Seguridad	
Interpretación para Redes (TNI)	Introducción	
TNI Módulos	Introducción	
TNI Módulo 1	Conceptos y Términos	
TNI Módulo 2	Evaluación de Sistemas y Redes	
TNI Módulo 3	Evaluación y Constitución de Componentes	
TNI Módulo 4	Otros Servicios de Seguridad	

[x] la información y el material se puede encontrar en.
http://radium.nesc.mil/tpep/library/ramp-Modulos/index.html

2.4 Uso de los criterios comunes

Actualmente, sobre la base de los conceptos planteados hasta ahora y en el catálogo que aparece en los CC, se emplea la metodología de los *Perfiles de Protección* para describir con precisión las propiedades de seguridad de un sistema o de las componentes de un sistema. Ahora bien, quienes adquieren bases de cómputo, tienen entonces una metodología expresada en el **Estándar Internacional ISO/IEC 15408:1999** para describir sus requerimientos, y entonces los proveedores pueden cotizar sus productos con más precisión.

2.4.1 Perfil de Protección

El perfil de protección (PP) contiene un conjunto de requerimientos de seguridad ya sea de los CC, o indicados explícitamente y permite la implantación de expresiones independientes de los requerimientos de seguridad mediante un conjunto de TOEs que cumplirán totalmente con un conjunto de objetivos de seguridad.

Un PP tiene la finalidad de ser reutilizado y definir requerimientos TOE que se sabe son útiles y efectivos en la reunión de los objetivos identificados y contiene además los fundamentos de los objetivos de seguridad y de los requerimientos de seguridad.

a) Propósito

El propósito de un Perfil de Protección es:

- Presentar en forma rigurosa un problema de seguridad que afecte a un conjunto o colección de sistemas o productos llamados TOE;
- Especificar los requerimientos de seguridad que resuelvan ese problema;
- Implementar esos requerimientos sin explicar cómo (o sea que la descripción es independiente de la implementación).

b) Definición

Puede definirse como un conjunto estándar de requerimientos de seguridad que pueden ser satisfechos por uno o más productos, o por sistemas que se usen para un propósito específico dentro de una organización.

Además, puede estar orientado a un objetivo específico (sistema operativo, manejador de bases de datos, tarjeta inteligente, cortafuegos, etc.), o a un conjunto de productos agrupados en un sistema o un producto compuesto.

Así, un Perfil de Protección es:

- Una explicación de lo que quiere un usuario y de lo que quiere lograr,
- Un documento de diseño de un sistema,
- Un camino del "qué" al "cómo".

El lector primario de un PP es el dueño de la misión/organización; pero evidentemente es de gran utilidad a los usuarios, a los desarrolladores, a los evaluadores y a los auditores; ya que los requerimientos corresponden a las necesidades del usuario de tal forma que éste pueda aceptar el PP, y los requerimientos se refinan por etapas hasta llegar a obtener requerimientos específicos.

Además, como se trata principalmente de una explicación de las necesidades del usuario hacia quienes impulsan su desarrollo, en la que se procede solicitando opiniones de los desarrolladores, los evaluadores, los auditores y los reguladores, *el Perfil de Protección le pertenece al dueño de la información.* Ahora bien, por su parte el usuario debe entender la misión de la organización y en este sentido puede decir tanto lo que se espera del objetivo de la evaluación como lo que NO se espera del objetivo de la evaluación. En tanto que a los proveedores les es difícil aseverar qué es lo que la TOE no puede hacer.

c) Uso

Debido a que se trata de una explicación detallada de lo que requiere el usuario, se trata de un lenguaje común entre ellos, los fabricantes, y los proveedores; y cabe aclarar que no se refiere a un lenguaje de productos específicos.

Una necesidad bien explicada y claramente definida puede ser satisfecha mediante una diversidad de productos; de manera que los compradores pueden usar uno o varios PP para buscar soluciones a sus

problemas; pero es requisito indispensable que dichos perfiles sean redactados según se especifica en los Criterios Comunes para que tengan validez generalizada; o bien, si se desea, se pueden examinar los PP que ya han sido acreditados[x*].

2.5 Estructura

Este subcapítulo está basado en los CC V2.1 [*v]

2.5.1 Introducción

a) Resumen ejecutivo (lo que el dueño del dinero tiene que ver)
b) Explicación clara y concisa del problema de seguridad que hay que resolver y de cómo el PP contribuye a la solución del mismo.
c) Es lo único que verán los que tomen decisiones.
d) Debe asegurarse que la introducción sea consistente con el contenido técnico del PP.

2.5.2 Descripción del objetivo de la evaluación

a) Añade detalles a lo que aparece en la Introducción como por ejemplo: ¿Qué es la TOE y cuál es su se entorno?
b) Va dirigido principalmente al técnico administrador.
c) Incluye una descripción funcional, la cual es más detallada y va más allá de una descripción de las características de seguridad de la TOE (a menos que la TOE sea un producto de propósito específico de seguridad).
d) Contiene una descripción de la frontera de la TOE, informando al lector qué es lo que está contenido en la TOE, y qué es lo que está fuera de la TOE.
e) Debe ser consistente técnicamente.

[x*] los PP acreditados se encuentran en:
http://www.radium nesc.mil/tpep/library/protection_profiles/index html
y su registro en: http://niap.nist gov/cc-scheme/PPRegistry.html
[*v] http://www.commoncriteria.org

2.5.3 Entorno de seguridad

a) La descripción se enfoca principalmente a las necesidades del usuario y facilita la definición de requerimientos.
b) Hace explícitas las hipótesis que se plantean al desarrollar el PP y las expectativas sobre el entorno que no se resolverán en otros ámbitos.
c) Hace explícitas las expectativas sobre la naturaleza de la TOE (por ejemplo si está hecho en base a COTS).

2.5.4 Hipótesis

a) Debe identificar las hipótesis y el alcance de los requerimientos relacionados al entorno físico, al personal, a los procedimientos y a la conectividad.
b) Debe evitar, en la medida de lo posible incluir detalles de las funciones de seguridad en la definición de hipótesis.
c) Debe asignarse una etiqueta o nombre a cada hipótesis para facilitar las referencias.

2.5.5 Amenazas

a) Las que sean importantes en términos de desarrollar los requerimientos.
b) Las que los usuarios del PP quieran ver explícitamente tomadas en cuenta.
c) Identificar las amenazas que sean relevantes, determinando cuáles son los bienes IT que requieren protección, contra qué métodos de ataque o contra qué eventos indeseables hay que protegerlos, y quiénes o cuáles son los agentes amenazadores.
d) Asegurar que las descripciones de las amenazas sean explícitas especificando claramente el origen de la amenaza (o del agente amenazador), qué bienes están bajo ataque y cuál es el método de ataque.
e) Asegurar que las descripciones de las amenazas sean concisas evitando el traslape de éstas.
f) Incluir únicamente amenazas que pongan en riesgo a los bienes IT, en lugar de los ataques que se basan en debilidades o fallas de la implementación de la TOE.
g) Debe asignarse una etiqueta o nombre a cada amenaza para facilitar las referencias.

2.5.6 Políticas de la organización

a) Identificar las políticas de seguridad organizacional, así como los requisitos que no se puedan satisfacer sólo mediante el estudio de las amenazas.
b) Definir las políticas como conjuntos de reglas que deben ser implementadas por la TOE y/o por su entorno (por ejemplo reglas de control de acceso).
c) Debe asignarse una etiqueta o nombre a cada política para facilitar las referencias.

2.5.7 Nivel de garantía general requerido

a) Refinamiento del resto del PP a partir de aquí.
b) Comprensión en lo general de lo que es necesario para satisfacer los objetivos del PP.

2.5.8 Objetivos

a) Cómo se hará frente a las amenazas y a las políticas desde el punto de vista de las hipótesis.
b) Naturaleza de los requerimientos.
c) Grado de efectividad esperado.
d) Enfoque del esfuerzo (prevención, detección, reacción, recuperación).
e) Relación entre el objetivo y las políticas y amenazas; la cual puede ser: uno a uno, uno a muchos, o muchos a uno.
f) Explícitos o derivados (implícitos).
g) Si se conocen los requisitos funcionales de seguridad debe identificarse un objetivo de seguridad para cada requisito funcional principal para facilitar el mapeo de los objetivos a los requisitos.
h) Identificar cualquier objetivo de seguridad que deba cumplir del entorno IT (por ejemplo la plataforma de ejecución).
i) Identificar cualquier responsabilidad de procedimientos que se refiera a la administración y uso de medidas de defensa de la TOE como objetivos de seguridad para el entorno.
j) Los objetivos de seguridad de la TOE deben ser afirmaciones concisas de la respuesta esperada para satisfacer los requerimientos de seguridad, y debe incluir hasta qué punto se espera se satisfagan

los requisitos. No es suficiente reiterar las políticas y las amenazas en forma distinta; hay que evitar en lo posible referirse a detalles de implementación.

k) El tipo de cada objetivo debe quedar muy claro, si es de tipo preventivo, detectivo o correctivo.
l) Debe asignarse una etiqueta o nombre a cada objetivo para facilitar las referencias.

2.5.9 Requerimientos

a) Qué funciones debe realizar la TOE.
b) Qué funciones debe realizar el entorno de la TOE, especialmente otras tecnologías de información distintas a la TOE (con la intención de que se pueden integrar).
c) Qué funciones deben realizar juntos el entorno y la TOE.
d) Dando margen a lo que haga precisamente la TOE.
e) Dando flexibilidad al diseño de la TOE.
f) Garantías; motivos para tener confianza.
g) Garantías; la calidad de las tecnologías de la información desde el punto de vista de la seguridad.
h) Medidas de evaluación o auditoría basadas en el PP.
i) La garantía final depende del desarrollador y del operador.
j) Deben identificarse primero los requerimientos funcionales de seguridad que lograrán cada uno de los objetivos de seguridad de la TOE.
k) Debe completarse la lista de requerimientos funcionales identificando aquellos que apoyan a los requerimientos dedicados específicamente a algún objetivo. Deben tomarse en cuenta las dependencias que se mencionan en la Parte 2 de los CC; a menos que se incluyan las razones para no hacerlo.
l) Se debe seleccionar el nivel de auditoría dependiendo de su importancia en el logro de los objetivos y su factibilidad técnica.
m) La iteración se debe emplear cuando se mencionen varias componentes funcionales de las mencionadas en la Parte 2 de los CC.
n) Se debe llevar a cabo, completa o parcialmente, la selección y asignación de las componentes funcionales del PP cuando sea necesario evitar la selección de soluciones que puedan ser inconsistentes con los objetivos de seguridad.

o) Se debe ir refinando paulatinamente cuando se sustituya un término genérico (por ejemplo un atributo de seguridad) por un término que vaya de acuerdo a la TOE, si es que esto hace más legible o comprensible el requerimiento funcional.
p) Se deben emplear letras negritas o cursivas para resaltar las operaciones que se terminan en un PP.
q) Se deben agrupar los requisitos en secciones que ayuden a comprender los requerimientos, si es que los que se mencionan en los CC no son los adecuados.
r) Se deben emplear las etiquetas adecuadas al PP si es que las que se mencionan en los CC no son las adecuadas.
s) Se deben seleccionar los requerimientos de garantía de la tecnología de la información con base en el valor de los activos que se desean proteger, los riesgos a los que están expuestos dichos activos, la factibilidad técnica, los costos probables y los tiempos disponibles.
t) Se deben seleccionar los requerimientos de garantía del entorno IT de acuerdo con los objetivos de seguridad del entorno.
u) Identificar los requerimientos de soporte de seguridad del entorno IT que satisfagan las dependencias de los requisitos funcionales de seguridad de la TOE que no sean alcanzadas por la TOE, y que sean verdaderamente relevantes.
v) Los requerimientos de seguridad del entorno IT deben definirse con un grado de abstracción apropiado en el PP para evitar que se definan en términos de la implementación específica.

2.5.10 Explicación

a) Regularmente se entrega como un documento separado.
b) Muestra por qué el PP está completo, correcto y es internamente consistente.
c) Es necesario mapear los objetivos contra los riesgos, las políticas organizacionales, y las hipótesis, mediante una tabla (u otro método adecuado) que muestre cada riesgo, política e hipótesis está cubierta por al menos un objetivo de seguridad.
d) Para cada riesgo, política e hipótesis, hay que añadir una explicación del porqué los objetivos señalados son los adecuados.
e) Se deben mapear los requerimientos funcionales de seguridad con los objetivos de seguridad mediante una tabla que muestre cómo cada objetivo de seguridad es cubierto por un requerimiento funcional.

f) Se debe añadir una explicación en cada caso del porqué son adecuados los requerimientos de seguridad mencionados.
g) Demostrar que las dependencias de la Parte 2 de los CC se cumplen y que los requerimientos no están en conflicto. Es decir que se ha procurado que un requisito funcional no permita que otro requisito sea evitado, alterado o desactivado.

2.5.11 ¿Cómo se determina que se cumple un PP?

a) Reconocimiento formal del proyecto CC.
b) Evaluación del PP, la ST y la TOE.
c) A través de laboratorios acreditados nacionalmente.
d) Emplear la metodología de evaluación adoptada internacionalmente supervisada por un esquema nacional de vigilancia.
e) Confrontando PP contra CC, ST contra PP, TOE contra ST.
f) Recibe un certificado de validación nacional lo que se evalúa.
g) Evaluación y validación por el sector privado.
h) Primero el PP, y a continuación la ST y la TOE.
i) Laboratorios acreditados sectoriales (o nacionales).
j) El sector acepta la metodología de evaluación.
k) Vigilancia sectorial.
l) El sector emite el certificado de validación.
m) Evaluación y medidas por el sector privado.
n) El sector determina qué medidas se realizarán.
o) Probablemente auditorías contra evaluaciones.
p) Es posible que el PP no se mida independientemente.
q) El sector determina la metodología de medición.
r) El sector emite el certificado de validación.
s) Evaluación independiente.
t) El laboratorio es elegido por el patrocinador (puede ser nacional).
u) La metodología es acordada entre el patrocinador y el laboratorio.

Capítulo 3

Curso sobre sistemas confiables basado en CC

Los sistemas y productos IT se producen y construyen con el fin de reunir requerimientos específicos y por razones económicas, poder utilizar al máximo las ventajas que éstos brindan, y debido a que la información es un recurso de alta valía para las organizaciones es necesario que los sistemas y/o productos se desarrollen con funciones de seguridad IT; para lo cual se requiere de profesionales especializados en seguridad de tecnología de la información y dado que los CC son el enfoque actual y moderno a nivel mundial para llevar a cabo la descripción, el desarrollo y la evaluación de problemas de seguridad en Tecnología de la Información, se ha conformado el presente temario sobre sistemas confiables, el cual deberá cubrirse en un curso avanzado de seguridad de la información; previamente revisado y aprobado por el comité académico de la institución.

3.1 Seguridad de tecnología de la información

En la actualidad muchos de los bienes de las empresas, las industrias, organizaciones y corporativos, así como de los gobiernos, de institutos, de universidades, etc. están en forma de información que es almacenada, procesada y transmitida mediante productos o sistemas IT (Tecnología de la Información) para reunir los requerimientos establecidos por los dueños de la información; así los dueños de la información pueden requerir la diseminación, la modificación y/o la cancelación de toda o parte de la información (datos) en forma tal que el cambio solicitado sea estrictamente controlado; de igual forma pueden demandar que los productos o sistemas IT implementen controles específicos de seguridad IT como parte del conjunto global de contramedidas de seguridad con la finalidad de contraatacar las amenazas a las que se encuentran expuestos sus datos.

La información que es almacenada, procesada y transmitida mediante los productos o sistemas IT es un recurso crítico que permite a las organizaciones tener éxito en su misión [9]. Adicionalmente, existen expectativas razonables individuales en que la información personal que está contenida en productos o sistemas IT permanecerá íntegra y privada, y que estará disponible siempre que ésta sea necesaria, y que no estará sujeta a ningún tipo de modificación sin la debida autorización. Los productos o sistemas IT llevarán a cabo sus funciones manteniendo el control propio de la información para asegurar que está protegida contra riesgos tales como la propagación no deseada o injustificada de la información, modificación o daños. El término seguridad IT se utiliza para prevenir y mitigar este tipo de riesgos y otros similares.

Los sistemas IT se producen y construyen con el fin de reunir requerimientos específicos y por razones económicas, poder utilizar al máximo las ventajas que brindan los productos IT tales como: sistemas operativos, componentes de aplicación de propósito general, plataformas de hardware, etc.. Las contramedidas de seguridad o medidas de defensa IT implantadas por un sistema pueden usar funciones de productos IT subyacentes y depender de la operación correcta de las funciones de seguridad de los productos IT. Los productos IT, pueden de esta manera, ser sujetos a evaluaciones como parte de la *evaluación de seguridad de sistemas IT.*

También se puede dar el caso en que algunos consumidores de Tecnología de la Información requieran juzgar si la confianza en la seguridad de sus productos o sistemas IT es la apropiada y que además probablemente no

deseen depender únicamente de las afirmaciones que hacen los desarrolladores, entonces pueden solicitar un análisis de seguridad, en otras palabras una *evaluación de seguridad de sistemas IT.*

Así, la necesidad de una evaluación de seguridad de sistemas IT podría ser de gran utilidad no solo a consumidores, sino también a usuarios y a los mismos desarrolladores de Tecnología de la Información para mantener, garantizar y/o mejorar la seguridad que ofrecen sus productos y sistemas; en este sentido los CC pueden ser usados para seleccionar las medidas de seguridad IT apropiadas y que contengan criterios para la evaluación de los requerimientos de seguridad.

Para ello es necesario desarrollar de manera clara, completa y concisa el Perfil de Protección(PP) para el sistema o producto IT en cuestión, cuya finalidad es: presentar en forma rigurosa un problema de seguridad que afecte al sistema o producto, especificar los requerimientos de seguridad que resuelvan ese problema y finalmente implementar esos requerimientos, de manera que los requerimientos contenidos en el PP permitan la implantación de expresiones independientes de los requerimientos de seguridad mediante un conjunto de TOEs (metas u objetivos de la evaluación) que cumplirán totalmente con un conjunto de objetivos de seguridad.

El desarrollador del Perfil de Protección debe conjuntar el material en cuatro bloques principales[*v]:

- material del entorno de seguridad
- material de los objetivos de seguridad
- material de requerimientos de seguridad
- material de especificación de la seguridad

Y para ello se requiere establecer:

- el entorno de seguridad,
- los objetivos de seguridad,
- los requerimientos de seguridad; y
- la especificación del sumario TOE.

[*v] http://www.commoncriteria.org

A continuación se da un breve descripción de estos cuatro aspectos fundamentales y las relaciones que guardan entre ellos. (ver figura 3.1)

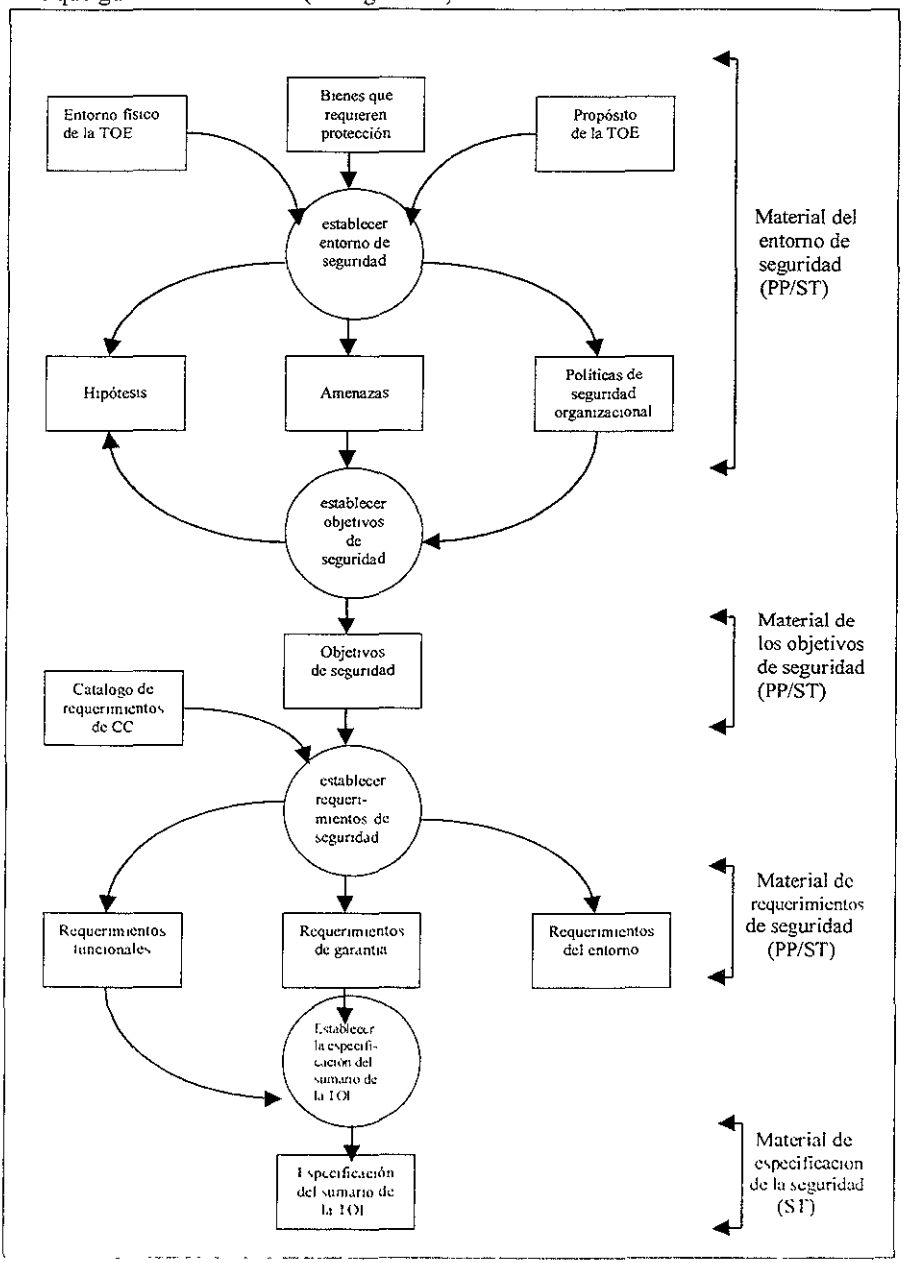

Figura 3.1 – Aspectos fundamentales de la seguridad en Tecnología de la Información (figura tomada de la traducción de CC Parte 1 cláusula 4.3)

El Perfil de Protección requiere que se establezca en primera instancia el ***entorno de seguridad***, el cual depende del conocimiento del entorno físico, los bienes que requieren protección y del propósito de la evaluación, con lo que se podrán establecer hipótesis sobre la seguridad, indicar las amenazas a las que se encuentran expuestos los bienes y determinar las políticas de seguridad organizacional de la empresa o institución propietaria de los bienes.

El Perfil de Protección requiere asimismo que se establezcan el o los ***objetivos de seguridad***, para lo cual necesita conocer las amenazas a las que se está expuesto y cuáles las políticas de seguridad organizacional, lo que permitirá determinar los objetivos de seguridad.

Estos objetivos de seguridad junto con el catálogo de requerimientos ya establecidos por los Criterios Comunes, son los que permiten establecer los ***requerimientos de seguridad***, y al hacerlo, presentar éstos en requerimientos funcionales, de garantía y de entorno.

Finalmente el Perfil de Protección requiere que se establezca la ***especificación del sumario de la TOE***, basándose en los requerimientos de seguridad establecidos (requerimientos funcionales y de garantía).

Cabe hacer notar que todos los conocimientos necesarios para escribir y desarrollar PPs se encuentran en los temas que se mencionan en este documento, y que la propuesta que aquí se plantea forma parte importante del proceso de aprendizaje en cuanto a seguridad IT se refiere, especialmente, a través de la internacionalización de normas y el entrenamiento profesional; y la cual debe ser considerada como el inicio de la preparación formal de un curso en esta disciplina, a través de su análisis y reestructuración (según se considere conveniente) por parte de un cuerpo colegiado que se encargue de formalizar dicho curso; cuyo contexto general es el que se aprecia en la figura 3.1, y en la cual se aprecian los temas que rodean a la seguridad IT, en tanto que los subtemas que refinan cada una de estas áreas se presentan a lo largo del texto que sigue a continuación.

3.2 Contexto de la seguridad

La seguridad se enfoca a brindar protección a los bienes contra posibles riesgos, donde los riesgos son considerados como el potencial que existe para abusar de los bienes protegidos. Todas las categorías de riesgos pueden ser

consideradas; pero en el campo de la seguridad se presta mayor atención a los riesgos que están relacionados con actividades maliciosas o a otro tipo de actividades humanas. (ver figura 3.2)

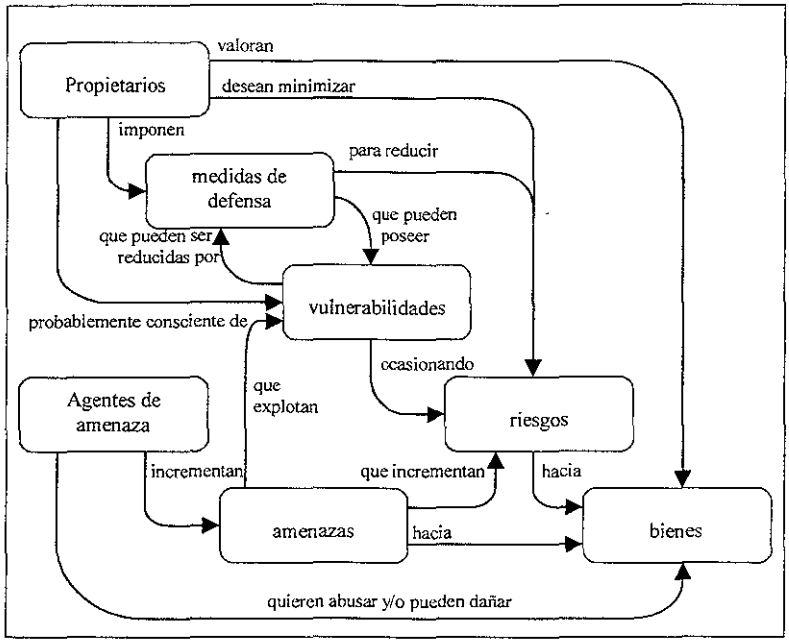

Figura 3.2 – Conceptos de seguridad y sus relaciones
(figura tomada de la traducción de CC Parte I cláusula 4.1)

La salvaguarda y protección de los bienes, y principalmente de aquellos que son de interés primordial *es responsabilidad de los propietarios* quienes estiman y valoran esos bienes. Los agentes actuales o las amenazas presumidas pueden también estimar y valorar los bienes, y buscar la forma de obtenerlos o abusar de ellos de manera contraria a los intereses de los propietarios. De manera que los dueños pueden percibir tales amenazas como un potencial para el deterioro de los bienes, con lo que el valor de éstos (para los dueños) podría reducirse considerablemente. Los daños específicos a la seguridad comúnmente incluyen; daños a los bienes por la revelación de éstos a receptores no autorizados (baja de confidencialidad), daños a los bienes a través de modificaciones no autorizadas (baja de integridad), o privación no autorizada del acceso a los bienes (baja de disponibilidad).

Los dueños de los bienes analizarán todas las posibles amenazas que podrían presentarse para determinar únicamente cuáles son las que aplican a su entorno. Los resultados obtenidos de este análisis se conocen como riesgos, además dicho análisis puede ayudar en la selección de las medidas de defensa para contrarrestar los riesgos y reducir éstos a un nivel aceptable.

Las medidas de defensa deben seleccionarse e implantarse para reducir los puntos vulnerables y cumplir con las políticas de seguridad de los dueños de los bienes (directa o indirectamente encaminados a otras partes). Debe considerarse que aún después de la implantación de las medidas de defensa es posible que permanezcan puntos vulnerables residuales, de manera que tales puntos vulnerables pueden ser explotados por agentes amenazantes que representen un nivel mínimo de riesgo hacia los bienes; no obstante es necesario que los dueños de los bienes busquen minimizar esos riesgos poniendo restricciones adicionales.

Cuando los dueños implantan medidas de defensa, necesitan confiar en que las medidas adoptadas son las adecuadas para contener los riesgos a los cuales están expuestos los bienes antes de que ellos queden expuestos a los riesgos especificados. Ahora bien, es posible que los dueños no posean la capacidad para juzgar todos y cada uno de los aspectos de las medidas de defensa, y es entonces que pueden solicitar la evaluación de las medidas de defensa; el resultado de la evaluación es un documento acerca de la extensión de la seguridad que brindan las medidas de defensa y de su confiabilidad para reducir los riesgos hacia los bienes protegidos. Los informes establecen un rango de garantía de las medidas de defensa, garantizan ser esas propiedades de las medidas de defensa que dan la base para la confidencialidad en sus operaciones apropiadas, de manera que los dueños de los bienes pueden apoyarse en estos informes en la toma de decisiones para aceptar o no los riesgos a los que se verían expuestos sus bienes. La figura 3.3 ilustra estas relaciones.

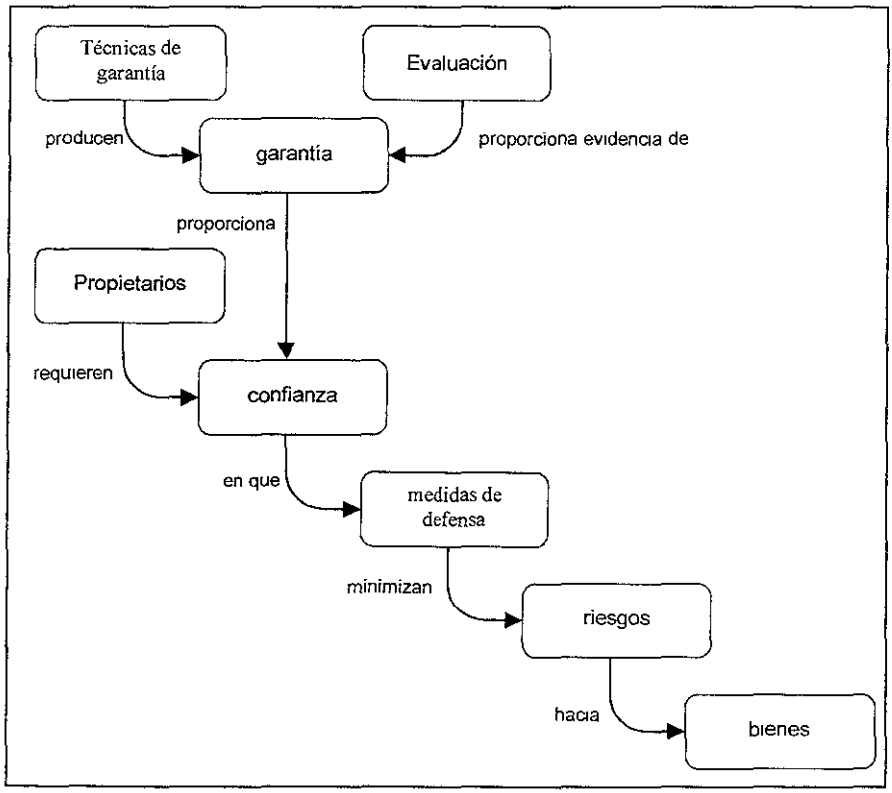

Figura 3.3 – Conceptos de evaluación y sus relaciones
(figura tomada de la traducción de CC Parte I cláusula 4.1)

Los dueños de los bienes normalmente serán los que tengan la responsabilidad de sus bienes y los que podrán tener la capacidad de decidir el aceptar los riesgos de la exposición de los bienes a las amenazas. Esto requiere que los resultados de los informes de la evaluación sean defendibles y de esta manera, la evaluación conducirá a los objetivos y a resultados repetibles que pueden ser citados como evidencia.

3.3 Entorno de seguridad

El entorno de seguridad incluye todas las normas, políticas de seguridad organizacional, costumbres, habilidad y conocimiento que son considerados relevantes. De esta manera se define el contexto en el cual la TOE (Meta u Objetivo de la Evaluación) pretende ser utilizada. El entorno de seguridad además considera las amenazas a la seguridad que están o que podrían estar presentes en el entorno.

Para establecer el entorno de seguridad, el escritor del Perfil de Protección (PP) o de la Meta de Seguridad (ST) tiene que tomar en cuenta los siguientes aspectos:

3.3.1 El entorno físico

El entorno físico de la TOE identifica todos los aspectos relevantes del entorno de operación de la TOE para la seguridad misma de la TOE, incluyendo las medidas de seguridad personal y físicas conocidas.

3.3.2 Los bienes

Los bienes son aquellos que requieren protección del elemento de la TOE para la cual los requerimientos o las políticas de seguridad aplicarán. Esto puede considerar a los bienes que están directamente relacionados, tales como archivos y bases de datos, también a los bienes que indirectamente son requerimientos de seguridad, tales como credenciales de autorización de acceso y la misma implantación de Tecnología de la Información.

3.3.3 El propósito

El propósito de la TOE es identificar a qué tipo de producto se dirigirá y cuál será la intención de la TOE.

3.4 Políticas de seguridad

Se debe llevar a cabo una investigación acerca de las políticas de seguridad, amenazas y riesgos; y dicha investigación debe poder emitir los siguientes informes específicos de seguridad para ser tomados en cuenta por la TOE:

3.4.1 Hipótesis

Las hipótesis deberán ser reunidas por el entorno de la TOE para permitir que la TOE sea considerada segura. Asimismo, el informe que las contiene puede ser aceptado como un axioma para la evaluación de la TOE.

3.4.2 Amenazas

Las amenazas a la seguridad de los bienes identifican todas las amenazas percibidas como relevantes hacia la TOE mediante el análisis de seguridad. Los CC caracterizan una amenaza en términos de un agente amenazador, un método de ataque supuesto, algunas vulnerabilidades que son la base de los ataques, y la identificación de los bienes bajo ataque. Una evaluación de riesgos a la seguridad podría calificar cada amenaza con una evaluación de la probabilidad de que tal amenaza se esté desarrollando dentro de un ataque actual, la probabilidad de que dicho ataque se pueda dar fácilmente, y las consecuencias de algún daño que pueda resultar.

3.4.3 Políticas de seguridad organizacional

Permiten identificar políticas y normas relevantes. Para un sistema IT, tales políticas deben estar referidas de manera explícita, mientras que para un producto IT de propósito general o una clase de producto, puede ser necesario hacer hipótesis acerca del funcionamiento de la política de seguridad organizacional.

3.5 Objetivos de seguridad

Los resultados del análisis del entorno de seguridad pueden ser usados para determinar los objetivos de seguridad que contrarrestan las amenazas identificadas y se refieren a hipótesis y políticas de seguridad organizacional identificadas. Los objetivos de seguridad deberán ser consistentes con la meta operacional determinada o el propósito del producto de la TOE, y cualquier conocimiento acerca de su entorno físico.

3.5.1 De manera directa por la TOE

El propósito de determinar los objetivos de seguridad es tratar todos los asuntos relacionados con la seguridad e informar cuáles aspectos de la seguridad deben ser tratados de manera directa por la TOE.

3.5.2 Por el entorno de la TOE

El propósito de determinar los objetivos de seguridad es tratar todos los asuntos relacionados con la seguridad e informar cuáles aspectos de la seguridad deben ser tratados por el entorno de la TOE.

En cualquiera de los dos casos, esta clasificación está basada en la incorporación de procesos desde el punto de vista ingenieril, políticas de seguridad, factores económicos y decisiones de aceptación de riesgos.

Los objetivos de seguridad para el entorno pueden ser implantados dentro del dominio IT, y por medios procedurales o no técnicos; y únicamente los objetivos de seguridad para la TOE y su entorno IT están dirigidos por los requerimientos de seguridad IT.

3.6 Requerimientos de seguridad IT

Los requerimientos de seguridad IT son el refinamiento de los objetivos de seguridad dentro de un conjunto de requerimientos de seguridad para la TOE y requerimientos de seguridad para el entorno el cual, si los reúne, asegurará que la TOE puede cumplir sus objetivos de seguridad.

Los CC representan requerimientos de seguridad bajo las distintas categorías de *requerimientos funcionales y requerimientos de seguridad.*

3.6.1 Requerimientos funcionales

Se basan en aquellas funciones de la TOE que están específicamente en apoyo de la seguridad IT, y definen la conducta de seguridad deseada. En la Parte 2 de los CC se definen los requerimientos funcionales, los cuales incluyen requerimientos para la identificación, la autenticación, la auditoría de seguridad y el no desconocimiento o no repudio de origen.

Cuando la TOE contiene funciones de seguridad que son realizadas mediante un mecanismo probabilístico o de permutación (p.e. una contraseña o una función de dispersión), los requerimientos de seguridad pueden especificar un nivel mínimo requerido de consistencia con los objetivos de seguridad. En este caso el nivel especificado será uno de los siguientes: SOF-básico, SOF-medio, SOF-elevado. Cada función será requerida para lograr ese nivel mínimo o al menos una métrica específica definida opcionalmente.

El grado de garantía puede ser variado y esto a través de un conjunto dado de requerimientos funcionales; por lo tanto esto se expresa regularmente en términos de ir incrementando niveles de rigor construidos con componentes de garantía. En la Parte 3 de los CC se definen los requerimientos de seguridad y una escala de Niveles de Garantía de Evaluación (EALs) la cual se construyó usando estos componentes.

3.6.2 Requerimientos de garantía

Los requerimientos de garantía se basan en acciones del desarrollador, en la evidencia producida y en las acciones del evaluador. Ejemplos de requerimientos de garantía incluyen condiciones en el rigor del proceso de desarrollo y requerimientos para investigar y analizar el impacto de las vulnerabilidades potenciales de seguridad.

La garantía de que los objetivos de seguridad se logran mediante las funciones de seguridad seleccionadas, se obtiene de los siguientes dos factores:

a) confianza en la exactitud de la implantación de las funciones de seguridad, para lo cual se podría evaluar si están implantadas correctamente;

b) confianza en la eficacia de las funciones de seguridad, para lo cual se puede llevar a cabo una evaluación para saber si realmente se satisfacen los objetivos de seguridad determinados.

Los requerimientos de seguridad generalmente incluyen tanto requerimientos para la presencia de conductas deseadas, como

requerimientos para la ausencia de conductas no deseadas. Normalmente es posible demostrar, mediante el uso o la prueba, la presencia de las conductas deseadas, pero sin embargo no siempre es posible lograr una demostración conclusiva de la ausencia de conductas no deseadas; pero el llevar a cabo pruebas, revisión de diseño y revisión de implantación, contribuye significativamente a reducir el riesgo de que tales conductas no deseadas puedan estar presentes. Los planteamientos racionales proporcionan otro apoyo más para conseguir que dichas conductas no deseadas estén ausentes.

3.7 Sumario de especificación TOE

Debe hacerse una recopilación de las especificaciones TOE, la cual se presenta en un sumario de especificaciones y se proporciona en la ST; dicho sumario define la urgencia de los requerimientos de seguridad para la TOE. Además se proporciona una definición a alto nivel de las funciones de seguridad necesarias para cumplir los requerimientos funcionales, y se indican las medidas necesarias para cumplir con los requerimientos de seguridad.

3.8 Utilización de recursos

Esta clase proporciona tres familias que fundamentan la disponibilidad de recursos requeridos tales como capacidad de procesamiento y/o capacidad de almacenamiento. La familia *Tolerancia a fallas* proporciona protección contra la indisponibilidad de recursos causada por fallas de la TOE. La familia *Prioridad de servicio* garantiza que los recursos serán asignados a las tareas más importantes o tareas de tiempo crítico y no pueden ser monopolizados por tareas de baja prioridad. La familia *Asignación de recursos* proporciona límites en el uso de recursos disponibles, asimismo previene que los usuarios monopolicen los recursos.

3.8.1 Tolerancia a fallas

Los requerimientos de esta familia garantizan que la TOE mantendrá al menos la operación correcta en eventos de fallas.

3.8.2 Prioridad de servicio

Los requerimientos de esta familia permiten a la TSF controlar el uso de los recursos dentro de la TSC por usuarios y sujetos tal que las actividades de alta prioridad dentro de la TSC siempre sean ejecutadas sin interferencia indebida o retrasos causados por actividades de baja prioridad.

3.8.3 Asignación de recursos

Los requerimientos de esta familia permiten a la TSF controlar el uso de recursos por usuarios y sujetos tal que la denegación del servicio no ocurra por causa de la monopolización no autorizada de los recursos.

3.9 Protección de la TSF

Esta clase contiene familias de requerimientos funcionales que relacionan a la integridad y la administración de los mecanismos que proporciona la TSF (independiente de las TSP específicas) y a la integridad de datos TSF (independiente de los contenidos específicos de los datos TSP). En cierto sentido, puede parecer que las familias en esta clase duplican componentes en la clase FDP (Protección de datos de usuario), las cuales pueden ser regularmente implantadas usando los mismos mecanismos. No obstante, FDP se enfoca a la protección de datos de usuario, mientras que FPT se enfoca a la protección de datos TSF. De hecho, los componentes de la clase FPT son necesarios para proporcionar requerimientos que las SFPs en la TOE no pueden ser alterados o eludidos.

3.9.1 Prueba de la máquina abstracta subyacente

Esta familia define los requerimientos de la TSF para llevar a cabo pruebas para demostrar las hipótesis de seguridad hechas con respecto a la máquina abstracta subyacente con respecto a la cual la TSF es liberada. Esta máquina abstracta podría ser una plataforma de hardware/firmware, o podría ser cierto conocimiento y una combinación hardware/software evaluado actuando como una máquina virtual.

3.9.2 Seguro ante fallas

Los requerimientos de esta familia aseguran que la TOE no violará su TSP en el evento de fallas de categorías identificadas en la TSF.

3.9.3 Disponibilidad de datos TSF exportados

Esta familia define las reglas para prevenir la pérdida de disponibilidad de datos TSF viajando entre la TSF y un producto IT remoto y probado. Este dato podría ser por ejemplo, un dato crítico TSF tal como contraseñas, claves, datos de auditoría, o código ejecutable TSF.

3.9.4 Confidencialidad de datos TSF exportados

Esta familia define las reglas para proteger de usuarios no autorizados a descubrir los datos TSF durante la transmisión entre la TSF y un producto IT probado y remoto. Este dato podría, por ejemplo, ser un dato crítico TSF tal como contraseñas, claves, datos de auditoría, o código ejecutable TSF.

3.9.5 Integridad de datos TSF exportados

Esta familia define las reglas para proteger de modificaciones no autorizadas, a datos TSF durante la transmisión entre la TSF y un producto IT probado y remoto. Estos datos podrían, por ejemplo, ser datos críticos tales como contraseñas, claves, datos de auditoría, o código TSF ejecutable.

3.9.6 Transferencia interna TOE de datos TSF

Esta familia proporciona los requerimientos que se refieren a la protección de datos TSF cuando éstos son transferidos entre partes separadas de una TOE a través de un canal interno.

3.9.7 Protección física de la TSF

Los componentes de protección física de la TSF se refieren a las restricciones sobre accesos físicos no autorizados a la TSF, y a la

disuasión de, y resistencia a, modificación física no autorizada, o sustitución de la TSF.

3.9.8 Recuperación confiable

Los requerimientos de esta familia garantizan que la TSF puede determinar que la TOE sea inicializada sin compromiso de protección y pueda recuperarse sin compromiso de protección después de una discontinuidad de operación. Esta familia es importante porque el estado de inicialización de la TSF determina la protección de los estados subsecuentes.

3.9.9 Detección de retransmisión

Esta familia se refiere a la detección de retransmisión por varios tipos de entidades (como: mensajes, solicitudes de servicio, respuestas de servicio) y las acciones subsecuentes para corregirla. En el caso donde la retransmisión puede ser detectada, ésta efectivamente se puede prevenir.

3.9.10 Mediación de referencia

Los requerimientos de esta familia se refieren a los aspectos de las "formas invocadas" de un monitor de referencia tradicional. La meta de esta familia es garantizar con respecto a una SFP dada, que todas las acciones requiriendo la puesta en vigor de la política sean validadas por la TSF contra la SFP. Si la parte de la TSF que aplica la SFP además reúne los requerimientos de componentes apropiados de FPT_SEP (Separación de Dominio) y ADV_INT (TSF internas), entonces esa parte de la TSF proporciona un "monitor de referencia" para esa SFP.

Una TSF que implanta una SFP proporciona protección efectiva contra operaciones no autorizadas si y sólo si todas las acciones aplicables (como: accesos a objetos) solicitadas por sujetos no confiables con respecto a alguno o a todos de esa SFP son validados por la TSF antes de que éstos sucedan. Si una acción que podría ser aplicable por la TSF, es aplicada incorrectamente o eludida incorrectamente, la aplicación total de la SFP podría verse comprometida. Los sujetos podrían entonces desviar la SFP en una variedad de formas no autorizadas

(como: burlar la verificación de acceso para algunos sujetos u objetos, la evasión de la verificación de objetos cuya protección fue asumida por las aplicaciones, retención de los derechos de acceso más allá de su tiempo de vida proyectado, evasión de auditoría de las acciones auditadas o evasión de autenticación). Note que algunos sujetos, a los llamados "sujetos confiables" con respecto a una SFP específica, podría confiárseles aplicar la SFP por ellos mismos, y la desviación de la mediación de la SFP.

3.9.11 Separación de dominio

Los componentes de esta familia garantizan que al menos un dominio de seguridad está disponible para que la TSF haga sus propias ejecuciones y que la TSF esté protegida de interferencias y ataques externos (como: por modificación del código TSF o estructuras de datos) por sujetos no confiables. Satisfaciendo los requerimientos de esta familia, la TSF se protege a sí misma, en el sentido que un sujeto no confiable no puede modificar o dañar la TSF.

Esta familia requiere lo siguiente:

a) Los recursos del dominio seguridad de la TSF ("dominio protegido") y aquellos de los sujetos y entidades libres externas al dominio deben ser separadas de tal forma que las entidades externas para el dominio protegido no puedan observar o modificar datos TSF o código TSF interno para el dominio protegido.
b) Las transferencias entre dominios deben ser controladas de tal forma que el acceso arbitrario a, o el regreso arbitrario de, el dominio protegido no sea posible.
c) Los parámetros de usuario o aplicación pasados al dominio protegido por direcciones debe ser validado con respecto al espacio de direcciones del dominio protegido, y aquellos pasados por valor deben ser validados con respecto a los valores esperados por el dominio de protección.
d) Los dominios de seguridad de sujetos deben ser distintos excepto para la división controlada vía la TSF.

3.9.12 Protocolo de sincronía de estado

Los sistemas distribuidos pueden desarrollarse a mayor grado de complejidad que los sistemas monolíticos a través de las diferencias de potencial de estado entre las partes del sistema, y a través de retrasos en la comunicación. En la mayoría de los casos de sincronización de estado entre funciones distribuidas se involucra un protocolo de intercambio, no una simple acción. Cuando existe malicia en el entorno distribuido de estos protocolos, se requieren protocolos defensivos más complejos.

El *protocolo de sincronía de estado* establece los requerimientos para ciertas funciones de seguridad crítica de la TSF para usar este protocolo confiable. Asimismo garantiza que dos partes distribuidas de la TOE (como: anfitriones) tengan sincronizados sus estados después de una acción de seguridad relevante.

3.9.13 Sellos de tiempo

Esta familia se refiere a los requerimientos para una función de sello de tiempo confiable dentro de una TOE.

3.9.14 Consistencia de datos TSF inter-TSF

En un entorno de sistema distribuido o compuesto, una TOE puede necesitar intercambiar datos TSF (como: atributos asociados a los datos, información de auditoría, información de identificación) con algún otro producto IT confiable. Esta familia define los requerimientos para compartir e interpretar la consistencia de estos atributos entre la TSF de la TOE y un producto IT confiable diferente.

3.9.15 Consistencia de retransmisión de datos TSF de la TOE interna

Los requerimientos de esta familia son necesarios para garantizar la consistencia de datos TSF cuando tales datos son retransmitidos internamente a la TOE. Estos datos pueden volverse inconsistentes si el canal interno entre las partes de la TOE deja de funcionar. Esto puede ocurrir cuando las partes se deshabilitan, si la TOE está estructurada

internamente como una red y las conexiones de la red de la TOE se rompen.

3.9.16 Autoverificación de la TSF

La familia define los requerimientos para que se autoverifique la TSF con respecto a algunas operaciones correctas esperadas. Ejemplos son las interfaces para hacer cumplir funciones, y simples operaciones aritméticas en partes críticas de la TOE. Estas pruebas pueden llevarse a cabo en el arranque, periódicamente, en la solicitud del usuario autorizado, o cuando se reúnan otras condiciones. Las acciones a ser efectuadas por la TOE, así como el resultado de la autoverificación están definidas en otras familias.

Los requerimientos de esta familia son además necesarios para detectar la corrupción de código ejecutable TSF (software TSF) y datos TSF por varias fallas que no necesariamente detienen la operación de la TOE (las cuales podrían ser manejadas por otras familias). Estas verificaciones deben llevarse a cabo porque estas fallas pueden no necesariamente ser prevenidas. Tales fallas pueden ocurrir ya sea por modos de fallas imprevistas o por descuidos asociados en el diseño de hardware, firmware, o software, o por la corrupción maliciosa de la TSF debido a una lógica y/o protección física inadecuadas.

3.10 Soporte de cifrado

La TSF puede emplear funcionalidad de cifrado para ayudar a satisfacer varios objetivos de seguridad de alto-nivel. Estos incluyen (pero no están limitados a: identificación y autenticación, no-repudio, camino confiable, canal confiable y separación de datos. Esta clase es usada cuando la TOE implanta funciones de cifrado, la implantación de las cuales podría ser en hardware, firmware y/o software.

3.10.1 Administración de claves de cifrado

Las claves de cifrado deben ser manejadas a través de sus ciclos de vida. Esta familia tiene el propósito de dar soporte a esos ciclos de vida y definir consecuentemente los requisitos para las siguientes actividades: generación de claves de cifrado, distribución de claves de cifrado,

acceso de claves de cifrado y destrucción de claves de cifrado. Esta familia debe ser incluida no obstante hay requisitos funcionales para la administración de claves de cifrado.

3.10.2 Operación de cifrado

Para que la operación de cifrado funcione correctamente, la operación debe ser ejecutada de acuerdo con un algoritmo específico y con una clave de cifrado de un tamaño específico. Aún cuando hay requisitos para la operación de cifrado que se va a ejecutar esta familia debe estar incluida.

Las operaciones de cifrado típicamente incluyen datos cifrados y/o descifrados, generación de firma digital y/o verificación, generación de suma de validación de cifrado para integridad y/o verificación de la suma de validación, valor de dispersión seguro (resumen del mensaje), clave de cifrado cifrada y/o descifrada, y clave de cifrado convenida.

3.11 Acceso a la TOE

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

3.11.1 Limitación en el ámbito de atributos seleccionables

Esta familia define los requerimientos para limitar el ámbito de atributos de seguridad de sesión que un usuario puede seleccionar para establecer una sesión.

3.11.2 Limitación en sesiones concurrentes múltiples

Esta familia define los requerimientos para poner límites en el número de sesiones concurrentes que pertenecen al mismo usuario.

3.11.3 Cierre de sesión

Esta familia define los requerimientos para que la TSF proporcione la capacidad para cerrar TSF-iniciada y usuario-iniciado y no cerrar sesiones interactivas.

3.11.4 Banderas de acceso a la TOE

Esta familia define los requerimientos para desplegar una advertencia configurable para usuarios que están considerando el uso apropiado de la TOE.

3.11.5 Historial de acceso a la TOE

Esta familia define los requerimientos para que la TSF despliegue a un usuario, un historial de intentos exitosos y sin éxito para acceder a la cuenta de usuario, al momento de establecer exitosamente una sesión.

3.11.6 Establecimiento de sesión TOE

Esta familia define los requerimientos para denegar a un usuario el permiso para establecer una sesión TOE.

3.12 Identificación y autenticación

Las familias en esta clase se refieren a los requerimientos de funciones para establecer y verificar una identidad de usuario pretendida.

La Identificación y Autenticación es un requisito para asegurar que los usuarios están asociados con los atributos de seguridad apropiados (niveles de identidad, grupos, funciones, de seguridad o integridad).

La identificación sin ambigüedades de usuarios autorizados y la asociación correcta de atributos de seguridad con usuarios y sujetos es crítica para la puesta en marcha de las políticas de seguridad proyectadas. Las familias en esta clase tienen que ver con la determinación y verificación de la identidad de los usuarios, determinando su autoridad para interactuar con la TOE, y con la asociación correcta de atributos de seguridad para cada usuario autorizado. Otras clases de requerimientos (como: Protección de Datos de Usuario, Auditoría de Seguridad) dependen de la correcta identificación y autenticación de los usuarios para ser efectivos.

3.12.1 Fallas de autenticación

Esta familia contiene los requerimientos para definir los valores de los intentos de autenticación sin éxito y acciones TSF en caso de fallas de intentos de autenticación. Los parámetros están considerados, pero no limitados a, el número de intentos de autenticación fallidos y umbrales de tiempo.

3.12.2 Definición de atributos de usuario

Todos los usuarios autorizados pueden tener un conjunto de atributos de seguridad, además de la identidad del usuario, que es usada para hacer cumplir la TSP. Esta familia define los requerimientos para la asociación de los atributos de seguridad de usuario con usuarios como una necesidad para soportar la TSP.

3.12.3 Especificaciones sobre los secretos

Esta familia define los requerimientos para los mecanismos que imponen las métricas de calidad definidas sobre los secretos proporcionados y genera secretos para satisfacer las métricas definidas.

3.12.4 Autenticación de usuario

Esta familia define los tipos de mecanismos de autenticación de usuario soportados por la TSF. Esta familia además define los atributos requeridos sobre los cuales los mecanismos de autenticación de usuario deberán basarse.

3.12.5 Identificación de usuario

Esta familia define las condiciones bajo las cuales se requerirá que los usuarios se identifiquen antes de la ejecución de cualquier otra acción que esté siendo mediada por la TSF y la cual requiera identificación de usuario.

3.12.6 Enlace usuario-sujeto

Un usuario autenticado, para usar la TOE, típicamente activa a un sujeto. Los atributos de seguridad de usuario están asociados (total o parcialmente) con este sujeto. Esta familia define los requerimientos para crear y mantener la asociación de los atributos de seguridad del usuario con un sujeto actuando en nombre del usuario.

3.13 Protección de datos de usuario

Esta clase contiene familias relacionadas con los requerimientos para las funciones de seguridad TOE y las políticas de función de seguridad TOE relacionadas a la protección de datos de usuario. FDP está dividido en cuatro grupos o familias (listadas abajo) que se refieren a los datos de usuario dentro de una TOE, durante la importación, exportación, y almacenamiento así también como los atributos de seguridad directamente relacionados a los datos de usuario.

3.13.1 Política de control de acceso

Esta familia identifica el control de acceso (por nombre) y define el ámbito de control de las políticas que forman la parte correspondiente al control de acceso identificado de la TSP. Este ámbito de control está caracterizado por tres conjuntos: los sujetos bajo el control de la política, los objetos bajo el control de la política, y las operaciones entre sujetos controlados y objetos controlados que están cubiertos por la política. Los criterios permiten la existencia de múltiples políticas, cada una con un nombre propio y único. Esto se realiza a través de la iteración de componentes a partir de esta familia una vez para cada política de control de acceso nombrada. Las reglas que definen la funcionalidad de un control de acceso serán definidas por otras familias tales como: *Funciones de control de acceso* e *Integridad de datos almacenados*. Los nombres de control de acceso identificados aquí en *Política de control de acceso* tienen la intención de usarse hasta el final de los componentes funcionales que tienen una operación que hace llamadas a una asignación o selección de un "control de acceso".

3.13.2 Funciones de control de acceso

Esta familia describe las reglas para las funciones específicas que pueden implantar una política de control de acceso nombrada *Política de control de acceso*; la cual especifica el ámbito de control de la política.

3.13.3 Autenticación de datos

La autenticación de datos permite a una entidad aceptar la responsabilidad para la autenticidad de información (por ejemplo: firmando digitalmente). Esta familia proporciona un método para proporcionar una garantía de la validez de una unidad específica de datos que puede ser subsecuentemente usada para verificar que la información contenida no ha sido perdida o modificada fraudulentamente. En contraste con la clase *Auditoría de seguridad*, esta familia pretende ser aplicada más bien a datos "estáticos" que a datos que son transferidos.

3.13.4 Exportación al exterior del control TSF

Esta familia define funciones para la exportación de los datos de usuario desde la TOE tal que sus atributos de seguridad y protección, puedan ser explícitamente preservados o puedan ser ignorados una vez que han sido exportados. Está relacionado con limitaciones de exportación y asociación de atributos de seguridad con los datos de usuario exportados.

3.13.5 Política de control de flujo de información

Esta familia identifica el control de flujo de información (por nombre) y define el ámbito de control de las políticas que forman la porción de control de flujo de información identificada de la TSP. Este ámbito de control está caracterizado por tres conjuntos: los sujetos bajo control de la política, la información bajo control de la política, y las operaciones cuya información controlada causa el flujo Hacia y desde los sujetos controlados cubiertos por la política. Los criterios permiten la existencia de múltiples políticas, cada una con un nombre único. Esto es realizado por la iteración de componentes de esta familia una vez para cada

política de control de flujo de información nombrada. Las reglas que definen la funcionalidad de un control de flujo de información serán definidas por otras familias tales como *Funciones de control de flujo de información* e *Integridad de datos almacenados*. Los nombres del control de flujo de información identificados aquí en *Política de control de flujo de información* tienen la intención de ser usados hasta el final del resto de los componentes funcionales que tienen una operación que hace llamadas para una asignación o selección de un "control de flujo de información".

3.13.6 Funciones de control de flujo de información

Esta familia describe las reglas para las funciones específicas que pueden implantar el control de flujo de información nombrado en *Políticas de control de flujo de información*, las cuales además especifican el ámbito de control de la política. Este consiste de dos tipos de requerimientos: uno es dirigiendo los resultados de flujo de información comunes, y la segunda es dirigiendo el flujo de información ilícito (por ejemplo: canales cubiertos). Esta división es porque los resultados concernientes al flujo ilícito de información son, en algún sentido, ortogonales al resto de un control de flujo de información. Por su naturaleza ellos rodean el control de flujo de información resultando en una violación de la política. Así que ellos requieren funciones especiales ya sea para limitar o para prevenir su ocurrencia.

3.13.7 Importación del control TSF externo

Esta familia define los mecanismos para la introducción de datos de usuario dentro de la TOE tal que éstos tienen los atributos de seguridad apropiados y están protegidos apropiadamente. Esto tiene que ver con las limitaciones sobre importaciones, la determinación de atributos de seguridad deseables, y la interpretación de atributos de seguridad asociados con los datos de usuario.

3.13.8 Transferencia TOE interna

Esta familia proporciona los requerimientos que se refieren a la protección de los datos de usuario cuando éstos son transferidos entre

las partes de una TOE a través de un canal interno. Esto puede ser comparado con las familias *Protección de transferencia de la confidencialidad de datos de usuario Inter-TSF* y *Protección de transferencia de la integridad de datos de usuario Inter-TSF*, las cuales proporcionan protección para los datos de usuario cuando éstos son transferidos entre distintas TSF a través de un canal externo y, *Exportación al exterior del control TSF* e *Importación del control TSF externo*, las cuales se refieren a la transferencia de datos hacia o desde fuera del control de TSF.

3.13.9 Protección de información residual

Esta familia se refiere a lo necesario para que la información borrada no sea accesible por más tiempo, y que los objetos creados nuevamente no contengan información que no deba ser accesible. Este familia requiere protección para la información que tiene que ser lógicamente borrada o liberada, pero que puede estar todavía presente dentro de la TOE.

3.13.10 Retroceso

La operación retroceso involucra el deshacer la última operación o serie de operaciones, con algunos límites, tales como un período de tiempo, y regreso a estados previos del conocimiento. La función de retroceso proporciona la habilidad para deshacer los efectos de una operación o serie de operaciones para preservar la integridad de los datos de usuario.

3.13.11 Integridad de datos almacenados

Esta familia proporciona los requerimientos que se refiere a la protección de los datos de usuario mientras son almacenados dentro de la TSC. Los errores de integridad pueden afectar los datos de usuario almacenados en memoria, o en un dispositivo de almacenamiento. Esta familia difiere de la familia *Transferencia TOE interna* la cual protege los datos de usuario de los errores de integridad mientras son transferidos dentro de la TOE.

3.13.12 Protección de transferencia de la confidencialidad de los datos de usuario inter-TSF

Esta familia define los requerimientos para asegurar la confidencialidad de los datos de usuario cuando son transferidos usando un canal externo entre distintas TOEs o usuarios sobre distintas TOEs.

3.13.13 Protección de transferencia de la integridad de los datos de usuario inter-TSF

Esta familia define los requerimientos para proporcionar integridad a los datos de usuario en tránsito entre la TSF y otro producto IT probado y la recuperación de errores detectables. A lo menos, esta familia monitorea la integridad de los datos de usuario ante modificaciones. Además esta familia soporta diferentes formas de corrección de errores de integridad detectados.

3.14 Comunicación

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

3.14.1 No-repudio de origen

El no-repudio de origen asegura que el creador de la información no puede negar haber enviado la información. Esta familia requiere que la TSF proporcione un método para asegurar que un sujeto que recibe información durante un intercambio de datos se le proporcione evidencia del origen de la información. Esta evidencia puede entonces ser verificada por ambos, este sujeto u otros sujetos.

3.14.2 No-repudio de receptor

El no-repudio de receptor asegura que el receptor de información no puede negar haber recibido la información. Esta familia requiere que la

TSF proporcione un método para asegurar que el sujeto que transmite información durante un intercambio de datos se le proporcione evidencia de receptor de información. Esta evidencia puede ser verificada por ambos, este sujeto u otros sujetos.

3.15 Privacía

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

3.15.1 Anonimato

Esta familia garantiza que un usuario pueda hacer uso de un recurso o servicio sin revelar su identidad. Los requerimientos del Anonimato proporcionan protección a la identidad del usuario. El Anonimato no tiene la intención de proteger la identidad del sujeto.

3.15.2 Pseudonimia

Esta familia garantiza que un usuario puede usar un recurso o servicio sin revelar su identidad de usuario, pero puede continuar siendo responsable de ese uso.

3.15.3 Imposibilidad de asociación

Esta familia garantiza que un usuario puede hacer múltiples usos de recursos o servicios sin que otros sean capaces de ligar estos usos juntos.

3.15.4 Inobservabilidad

Esta familia garantiza que un usuario puede usar un recurso o servicio sin que otros, especialmente terceras partes, sean capaces de observar que los recursos o servicios están siendo usados.

3.16 Caminos/Canales confiables

Las familias en esta clase proporcionan requerimientos para un camino de comunicación confiable entre usuarios y la TSF, y para un canal de comunicación confiable entre la TSF y otros productos IT confiables. Los caminos y los canales confiables tienen las siguientes características generales:

- Para construir caminos de comunicación se utilizan canales de comunicación que pueden ser internos o externos (conforme sea lo mas apropiado para el componente), en los cuales se aislan para un sujeto identificado los datos de la TSF de los comandos de la TSF y los datos del usuario.

- El uso de los caminos de comunicación pueden ser iniciados por el usuario y/o la TSF (como sea apropiado para el componente).

- Los caminos de comunicación son capaces de garantizar que el usuario se está comunicando con la TSF correcta, y que la TSF se está comunicando con el usuario correcto (como sea apropiado para el componente).

En este paradigma, un ***canal confiable*** es un canal de comunicación que puede ser iniciado por ambos extremos del canal, y proporciona características de no-repudio con respecto a la identidad de los extremos del canal.

Un ***camino confiable*** proporciona un medio para que los usuarios ejecuten funciones a través de la interacción directa garantizada con la TSF. El camino confiable es usualmente deseado para acciones de usuario tales como identificación inicial y/o autenticación, pero además puede desearse en otro momento durante de una sesión de usuario. Los intercambios vía un camino confiable pueden ser iniciados por un usuario o la TSF. El usuario responde vía el camino confiable que está garantizado de estar protegido contra modificación, o revelación a aplicaciones no confiables.

3.16.1 Canal confiable inter-TSF

Esta familia define los requerimientos para la creación de un canal confiable entre la TSF y otros productos IT confiables para la ejecución de operaciones críticas de seguridad. Esta familia debe considerarse en cualquier momento que se requiera garantizar la comunicación del usuario o de los datos TSF entre la TOE y otros productos IT confiables.

3.16.2 Camino confiable

Esta familia define los requerimientos para establecer y mantener comunicación confiable hacia, o de usuarios y la TSF. Un camino confiable puede ser requerido para cualquier interacción de seguridad relevante. Los intercambios de camino confiable pueden ser iniciados por un usuario durante una interacción con la TSF, o la TSF puede establecer comunicación con el usuario vía un camino confiable.

3.17 Administración de la seguridad

Esta clase se ha desarrollado para especificar la administración de varios aspectos de la TSF: atributos de seguridad, datos TSF y funciones. Los diferentes perfiles de la administración y su interacción pueden especificarse, tales como la separación de capacidades (acciones posibles).

Esta clase tiene varios objetivos:

a) administración de datos TSF, los cuales consideran por ejemplo, banderas;
b) administración de atributos de seguridad, los cuales consideran, por ejemplo, las Listas de Control de Acceso, y Listas de Posibilidades;
c) administración de funciones de la TSF, las cuales consideran, por ejemplo, la selección de funciones, y reglas o condiciones que influyen sobre el comportamiento de la TSF; y
d) definición de perfiles de seguridad.

3.17.1 Administración de funciones en TSF

Esta familia permite a usuarios autorizados el control sobre la administración de funciones en la TSF. Ejemplos de funciones en la TSF incluyen las funciones de auditoría y las múltiples funciones de autenticación.

3.17.2 Administración de atributos de seguridad

Esta familia permite a usuarios autorizados el control sobre la administración de atributos de seguridad. Esta familia podría incluir posibilidades para ver y modificar atributos de seguridad.

3.17.3 Administración de datos TSF

Esta familia permite a usuarios (perfiles) autorizados el control sobre la administración de datos TSF. Ejemplos de datos TSF incluidos en información de auditoría, reloj, configuración del sistema y otros parámetros de configuración TSF.

3.17.4 Revocación

Esta familia se refiere a la revocación de atributos de seguridad para una variedad de entidades dentro de una TOE.

3.17.5 Vigencia de los atributos de seguridad

Esta familia se refiere a la posibilidad de imponer límites de tiempo sobre la vigencia de los atributos de seguridad.

3.17.6 Perfiles de la administración de seguridad

Esta familia se ha desarrollado para controlar la asignación de diferentes perfiles a usuarios. Las posibilidades de estos perfiles con respecto a la administración de la seguridad se describen en otras familias en esta clase.

3.18 Auditoría de seguridad

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

3.18.1 Respuesta automática de auditoría de seguridad

Esta familia define la respuesta que se tendrá en caso de detectar eventos indicativos de una potencial violación de seguridad.

3.18.2 Generación de datos de auditoría de seguridad

Esta familia define los requerimientos para registrar la ocurrencia de eventos relevantes de seguridad que toman lugar bajo el control TSF. Esta familia identifica el nivel de auditoría, enumera los tipos de eventos que serán auditables por la TSF, e identifica el conjunto mínimo de información relacionada con la auditoría que deberá ser proporcionada dentro de varios tipos de registro de auditoría.

3.18.3 Análisis de auditoría de seguridad

Esta familia define los requerimientos para los medios automatizados que analizan la actividad del sistema y ven la auditoría de los datos para violaciones de seguridad posibles o reales. Este análisis puede trabajar en apoyo a la detección de intrusiones, o respuesta automática a una violación inminente de seguridad.

3.18.4 Revisión de auditoría de seguridad

Esta familia define los requerimientos de las herramientas de auditoría que deben estar disponibles para usuarios autorizados a participar en la revisión de la auditoría de datos.

3.18.5 Selección del evento de auditoría de seguridad

Esta familia define los requerimientos para elegir los eventos a ser auditados durante la operación de la TOE. Se definen los requerimientos para incluir o excluir eventos del conjunto de eventos auditables.

3.18.6 Almacenamiento del evento de auditoría de seguridad

Esta familia define los requerimientos de la TSF para permitir crear y mantener un seguimiento de auditoría confiable.

Capítulo 4

Caso Práctico: Desarrollo del PP de Firewalls de Filtrado de Paquetes para Entornos de Bajo Riesgo

Este PP en firewalls de filtrado de paquetes define los requerimientos de seguridad básicos de las organizaciones que manejan información no clasificada en entornos de bajo riesgo, esto se debe a que se trata de un caso típico de empresas e instituciones en México. Los firewalls pueden consistir de uno o más mecanismos que formen parte de las medidas de seguridad sobre todo en instituciones académicas o ciertas organizaciones empresariales o gubernamentales, esto mediante el aislamiento de la red interna de la organización de la Internet o de otras redes externas. Los firewalls permiten el paso o bloquean el flujo de información hacia la red de la organización, en base a un conjunto de reglas definidas por el administrador autorizado de la red. Este PP en particular aplica a firewalls que son capaces de. proteger el tráfico de la red en las capas correspondientes a los protocolos de red y transporte, autenticar al administrador autorizado para cualquier acción sobre el firewall, y auditar los eventos relevantes de seguridad que se presenten.

4.1 Descripción de la TOE

El propósito de un firewall es proporcionar el acceso controlado y auditado a los servicios, tanto al interior como al exterior de la red de la organización en cuestión, y esto lo hace permitiendo, denegando o redireccionando el flujo de los datos que pasan a través de él. La figura 4.1 muestra la representación lógica de un firewall mediando tráfico o flujos de información entre las redes internas y externas a la organización.

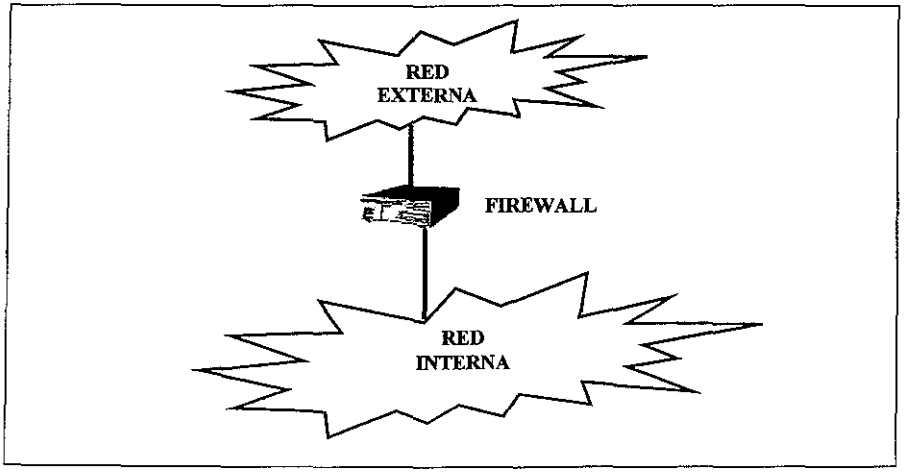

Figura 4.1 – Representación lógica de un firewall

La TOE selecciona los caminos para los flujos de información entre las redes internas y externas de acuerdo a las políticas de seguridad impuestas para la actividad de la organización, y únicamente un administrador autorizado tiene autoridad para cambiar las reglas de las políticas de seguridad.

Las reglas de filtrado deben estar almacenadas en los puertos de la TOE. Cuando los datos llegan al puerto, se analizan los encabezados, incluyendo los campos de dirección fuente y destino, el campo del protocolo de red y el número de puerto de transporte.[8]

Los usuarios de la TOE son usuarios humanos y hosts llamados entidades IT externas; de los usuarios humanos únicamente los administradores autorizados pueden acceder a la TOE a través de medios remotos de una red externa o interna a la organización.

Si un administrador autorizado accede a la TOE remotamente, se debe identificar y autenticar correctamente, y entonces se debe utilizar un canal confiable y cifrado de datos. Si el acceso es local se puede acceder sin el uso del cifrado de datos, lo cual se puede efectuar a través de una terminal en particular (que se puede considerar como parte de la TOE) y para ello se recomienda que usuarios no administradores autorizados: a) no hagan uso de esa terminal en particular, y b) que usuarios/administradores no autorizados que accedan a funciones de la TOE no lo hagan a funciones referentes a la seguridad y que además previamente se identifiquen y autentiquen correctamente.

La TOE puede operar además dentro de una de las dos siguientes políticas por omisión [8]:

- **por omisión = denegar:** todo aquello que no esté permitido expresamente, está prohibido.
- **por omisión = permitir o redireccionar:** todo aquello que no esté prohibido expresamente, está permitido.

El PP que aquí se desarrolla está enfocado a operar en la primera de estas políticas por omisión (denegar).

4.2 Entorno de seguridad de la TOE

El PP que se desarrolla es para TOEs que se pretendan usar en entornos donde la información que se procese, a lo más, sea considerada información delicada pero no clasificada.

4.2.1 Hipótesis

Se considera que estarán presentes las siguientes condiciones en el entorno donde operará la TOE.

- La TOE está segura físicamente.
- La amenaza de ataques maliciosos que pretenden descubrir vulnerabilidades explotables se considera bajo.
- La TOE no es un host de datos públicos.

- El administrador autorizado es una persona honorable y sigue completamente la guía del administrador; pero no se descarta la posibilidad de que cometa algún error.
- La información no puede fluir entre las redes interna y externa a menos que ésta pase a través de la TOE.
- Los usuarios para los que no hay límites de protección física a la TOE, pueden intentar acceder a ella desde alguna conexión directa a la TOE, si es que la conexión es parte de ésta.
- A excepción de la identificación y la autenticación, no hay otras funciones de seguridad para el acceso a la TOE.
- Solamente administradores autorizados pueden acceder a la TOE remotamente desde alguna red interna o externa a la organización.

4.2.2 Amenazas

El análisis de las amenazas se divide en dos grupos; uno que se refiere a amenazas a la TOE, donde los agentes amenaza pueden ser usuarios o entidades IT externas no autorizadas para usar la TOE, y los bienes que son sujetos a ataque son recursos IT que residen en la misma TOE; el otro grupo es el de amenazas referentes al entorno operacional, las cuales deben ser contrarrestadas mediante medidas procedurales y/o métodos administrativos.

4.2.2.1 Amenazas referentes a la TOE [3]

- Un usuario no autorizado puede acceder y usar funciones de seguridad y/o funciones no referentes a seguridad que proporcione la TOE.
- Un usuario autorizado y no autorizado puede intentar repetidamente acertar a los datos correctos de autenticación.
- Después de capturar los datos válidos de identificación y autenticación, un usuario no autorizado puede usar éstos en el futuro para acceder a funciones que proporciona la TOE.
- Un usuario puede emitir información para que fluya a través de la TOE dentro de una red conectada donde la dirección fuente en la información sea falsa.
- Un usuario puede enviar información no permisible a través de la TOE.

- Un usuario puede ser capaz de recoger la información residual de flujos de información previos o de datos internos de la TOE, monitoreando el contenido de los flujos de información provenientes de la TOE.
- Un usuario puede ser capaz de ver la información que se esté transmitiendo entre el administrador autorizado localizado remotamente y la TOE.
- Un usuario autorizado puede leer, modificar o destruir datos internos de la TOE.
- Un usuario puede emitir reportes falsos de auditoría para evitar que los reales sean registrados y sean éstos los que se consideren para acciones futuras referentes a la seguridad.

4.2.2.2 Amenazas referentes al entorno operacional

- La TOE puede ser configurada, usada y administrada de manera insegura, ya sea intencionalmente o no.

4.3 Objetivos de seguridad

Los objetivos de seguridad se dividen en dos grupos:

4.3.1 Objetivos de seguridad IT [3]

- La TOE debe identificar y autenticar la identidad de todos los usuarios antes de que se les permita cualquier tipo de acceso a las funciones de la TOE.
- La TOE debe estar lista para rehusar los datos de autenticación de usuarios que intenten autenticarse desde redes externas.
- La TOE debe mediar el flujo de toda la información de los usuarios que se encuentren conectados a la red hacia usuarios conectados en alguna otra red, y debe asegurar que la información residual de flujos previos no será transmitida de ninguna manera.
- Al momento de la puesta en marcha de la TOE o cuando se esté dando la recuperación después de una interrupción del servicio, la TOE no debe comprometer sus recursos ni aquellos que se encuentren conectados a la red.

- La TOE debe proteger la confidencialidad de su "conversación" con un administrador autorizado a través de mecanismos de cifrado cuando se esté efectuando a través de una conexión remota.
- La TOE debe protegerse a sí misma de usuarios no autorizados que intenten evitar, desactivar o forzar las funciones de seguridad de la TOE.
- La TOE debe proporcionar una cuenta de usuario específica para los tráficos de información con el administrador autorizado con respecto a las funciones de seguridad y relacionadas a eventos de auditoría.
- La TOE debe proporcionar un medio para registrar el seguimiento de auditoría de eventos relacionados a la seguridad que sea legible y que contenga fechas y horas de los eventos registrados; asimismo un medio que busque y seleccione un seguimiento de auditoría basado en atributos relevantes.
- La TOE debe proporcionar la funcionalidad necesaria para permitir a un administrador autorizado hacer uso de las funciones de seguridad, asegurándose de que únicamente administradores autorizados tengan la capacidad de acceder a dicha funcionalidad.
- La TOE debe proporcionar un medio para que el administrador autorizado controle y limite los accesos a las funciones de seguridad de la TOE mediante una entidad IT externa autorizada.

4.3.2 Objetivos de seguridad no relacionados a IT

Para que la TOE pueda cumplir con sus responsabilidades es necesario que ésta sea: entregada, instalada, administrada y operada de manera que mantenga su seguridad.

Es requisito mínimo indispensable que el *administrador autorizado* esté *capacitado* en el establecimiento y mantenimiento de políticas y prácticas de seguridad.

4.4 Requerimientos de seguridad IT

Los requerimientos de seguridad IT se refieren al sistema/producto IT que es el objetivo de esta evaluación, por lo que entonces se hace referencia a requerimientos de seguridad TOE. De manera que aquí se establecen los requerimientos funcionales y de garantía que deben ser satisfechos por el

Perfil de Protección de la TOE; y estos requerimientos consisten de componentes funcionales de la Parte 2 de los CC, así como de un nivel de garantía de evaluación (EAL) que contiene componentes de garantía de la Parte 3 de los CC.

4.4.1 Requerimientos funcionales de seguridad TOE

Los requerimientos de seguridad funcional para este PP consisten de los componentes de la Parte 2 de los CC que se presentan en la tabla 4.1:

Tabla 4.1 – Requerimientos funcionales

Componentes Funcionales	
FMT_SMR.1	Perfiles o funciones de seguridad
FIA_ATD.1	Definición de atributo de usuario
FIA_UID.2	Identificación de usuario antes de cualquier acción
FIA_UAU.1	Coordinación de autenticación
FIA_AFL.1	Manejo de fallas de autenticación
FIA_UAU.4	Mecanismos de autenticación de un solo uso
FDP_IFC.1	Subconjunto de control de flujo de información
FDP_IFF.1	Atributos de seguridad simple
FMT_MSA.3	Inicialización de atributos estáticos
FDP_RIP.2	Protección total de información residual
FCS_COP.1	Operación de cifrado
FPT_RVM.1	Sin evasión de las políticas de seguridad de la TOE
FPT_SEP.1	Separación de dominio de las funciones de seguridad de la TOE
FPT_STM.1	Sellos de tiempo confiables
FAU_GEN.1	Generación de datos de auditoría
FAU_SAR.1	Revisión de auditoría
FAU_SAR.3	Revisión de auditoría seleccionable
FAU_STG.1	Almacenamiento protegido del seguimiento de auditoría
FAU_STG.4	Prevención de pérdida de datos de auditoría
FMT_MOF.1	Administración de la conducta de las funciones de seguridad

El primer componente que aparece en la tabla 4.1 es FMT_SMR.1 ya que es el que define el perfil del administrador autorizado.

FMT_SMR.1 perfiles de seguridad

- FMT_SMR.1.1 – las funciones de seguridad de la TOE mantendrán el perfil del administrador autorizado.
- FMT_SMR.1.2 - las funciones de seguridad de la TOE serán capaces de asociar usuarios (humanos) con el perfil del administrador autorizado.

Los componentes de la clase FIA se listan a continuación porque describen las políticas de identificación y la autenticación que todos los usuarios y entidades IT deben acatar para que se les permita hacer uso de la TOE.

FIA_ATD.1 definición de atributos de usuario

- FIA_ATD.1.1 – las funciones de seguridad de la TOE mantendrán los siguientes atributos de seguridad pertenecientes a usuarios individuales:

  [identidad; asociación del usuario con un perfil del administrador autorizado; cualquier otro atributo de seguridad determinado por el diseñador de la TOE]

FIA_UID.2 identificación del usuario antes de cualquier acción

- FIA_UID.2.1 – las funciones de seguridad de la TOE requerirán que cada usuario se identifique a sí mismo antes de que las funciones de seguridad de la TOE puedan mediar cualquier acción en nombre del usuario

FIA_UAU.1 coordinación de autenticación

- FIA_UAU.1.1 – las funciones de seguridad de la TOE permitirán que primero se lleve a cabo la identificación del usuario (FIA_UID.2) ya sea humano o entidad IT antes de que éste sea autenticado.

- FIA_UAU.1.2 – las funciones de seguridad de la TOE requerirán que cada usuario (humano o entidad IT externa autorizada) sea autenticada exitosamente antes de permitir que las funciones de seguridad de la TOE efectúen cualquier mediación de acciones en nombre del usuario.

FIA_AFL.1 manejo de fallas de autenticación

- FIA_AFL.1.1 – las funciones de seguridad de la TOE detectarán cuando un intento de autenticación no tenga éxito y si este evento está relacionado a una entidad IT externa intentando autenticarse desde una red interna o externa.
- FIA_AFL.1.2 – cuando se haya alcanzado o sobrepasado el número definido de intentos de autenticación sin éxito, las funciones de seguridad de la TOE evitarán que esa entidad IT se pueda autenticar exitosamente hasta que el administrador autorizado decida que medidas o acciones tomar.

FIA_UAU.4 mecanismos de autenticación de uso simple

- FIA_UAU.4.1 – las funciones de seguridad de la TOE prevendrán la reutilización de datos de autenticación relacionados a intentos de autenticación ya sea de redes internas o externas mediante:

  [administradores autorizados; entidades IT externas autorizadas]

Existe una política de función de seguridad (SFP) de control de flujo de información, y se describe a continuación en los componentes FDP; así entonces las reglas que marca la política se deben hacer cumplir como atributos de las entidades definidas.

Nota: a la SFP de control de flujo de información se le llama SFP no autenticada.

FDP_IFC.1 subconjunto de control de flujo de información

- FDP_IFC.1.1 – las funciones de seguridad de la TOE impondrán la SFP no autenticada sobre:

a) subconjuntos: entidades IT externas no autenticadas que envíen y reciban información a través de la TOE hacia alguna otra entidad:
b) información: tráfico enviado de un sujeto a otro a través de la TOE ;
c) operación: información de paso.

FDP_IFF.1 atributos de seguridad simple

- FDP_IFF.1.1 – las funciones de seguridad de la TOE impondrán la SFP no autenticada en base a por lo menos los siguientes tipos de atributos de seguridad de información y sujetos:

  a) sujetos: direcciones, y cualquier otro atributo de seguridad determinado por el diseñador de la TOE;
  b) información: direcciones de sujetos fuente; direcciones de sujetos destino; protocolo de la capa de transporte; interface TOE sobre la cual el tráfico llega y se distribuye; y servicios.

- FDP_IFF.1.2 – las funciones de seguridad de la TOE permitirán un flujo de información entre un sujeto controlado y otro sujeto controlado vía una operación controlado a si se mantienen las siguientes reglas:

  sujetos en una red interna pueden hacer que fluya información a través de la TOE hacia otra red conectada si:

  - todos los valores de los atributos de seguridad de la información están libres de ambigüedades y son permitidos por las reglas de las políticas de seguridad, en cualquier combinación creadas por el administrador autorizado;
  - la dirección del sujeto fuente, en la información, corresponde a una dirección de red interna;
  - y la dirección del sujeto destino, en la información, corresponde a una dirección de alguna red conectada.

- FDP_IFF.1.6 – las funciones de seguridad de la TOE denegarán explícitamente un flujo de información en base a las siguientes reglas:
  a) la TOE rechazará solicitudes de acceso o de servicios cuando la información llegue de una interface TOE externa, y la dirección

del sujeto fuente corresponda a una entidad IT externa de una red interna;

b) la TOE rechazará solicitudes de acceso o de servicios cuando la información llegue de una interface TOE interna, y la dirección del sujeto fuente sea de una entidad IT externa de una red externa;
c) la TOE rechazará solicitudes de acceso o de servicios cuando la información llegue de una interface TOE interna o externa, y la dirección del sujeto fuente sea una dirección broadcast de una entidad IT externa;
d) la TOE rechazará solicitudes de acceso o de servicios cuando la información llegue de una interface TOE interna o externa, y la dirección del sujeto fuente sea una dirección privada de una entidad IT externa, o una dirección reservada de red.

FMT_MSA.3 inicialización de atributos estáticos

- FMT_MSA.3.1 – las funciones de seguridad de la TOE impondrán SFP no autenticada para proporcionar valores *restrictivos* por omisión para los atributos de seguridad del flujo de información que se utilicen para hacer cumplir la SFP.
- FMT_MSA.3.2 – las funciones de seguridad de la TOE permitirán que un administrador autorizado especifique valores iniciales alternativos para omitir los valores por omisión cuando se cree un objeto o se produzca información.

FDP_RIP.2 protección total de información residual

- FDP_RIP.2.1 – las funciones de seguridad de la TOE asegurarán que cualquier contenido de información previa de cualquier recurso se vuelva indisponible para todos los sujetos.

El componente FCS_COP.1 es un requerimiento condicional, ya que solamente será necesario cuando el desarrollador de la TOE permita que pueda darse la administración remota.

FCS_COP.1 operación de cifrado

- FCS_COP.1.1 – las funciones de seguridad de la TOE realizarán el cifrado de sesiones remotas del administrador autorizado de acuerdo con el algoritmo de cifrado que haya sido especificado.

Los componentes que están relacionados con la protección de funciones de seguridad confiables corresponden a la clase FPT.

FPT_RVM.1 sin evasión de las políticas de seguridad de la TOE

- FPT_RVM.1.1 – las funciones de seguridad de la TOE asegurarán que las políticas de seguridad de la TOE harán cumplir las funciones que son invocadas y que ocurran antes de cada función dentro del ámbito de control de las funciones de seguridad que se permitan proceder.

FPT_SEP.1 separación de dominio TSF

- FPT_SEP.1.1 – las funciones de seguridad de la TOE mantendrán un dominio de seguridad para su propia ejecución que proteja de la interferencia y de la destrucción de sujetos no confiables.
- FPT_SEP.1.2 – las funciones de seguridad de la TOE impondrán la separación entre los dominios de seguridad de los sujetos en el ámbito de control TSF.

FPT_STM.1 sellos de tiempo confiables

- FPT_STM.1.1 – las funciones de seguridad de la TOE serán capaces de proporcionar sellos de tiempo confiables para su propio uso.

A partir del componente FAU_GEN.1 se requiere del registro de fecha y hora cuando ocurran eventos de auditoría. Los requerimientos de la clase FAU permiten definir las funciones de seguridad de la auditoría, las cuales deben ser soportadas por la TOE.

FAU_GEN.1 generación de datos de auditoría

- FAU_GEN.1.1 – las funciones de seguridad de la TOE serán capaces de generar un registro de auditoría de los siguientes eventos auditables:

  a) inicialización y cierre de funciones de auditoría;
  b) todos los eventos auditables relevantes para el nivel mínimo o básico de auditoría especificado en la tabla 4.2; y
  c) el evento listado en el nivel "extendido" de la tabla 4.2.

- FAU_GEN.1.2 las funciones de seguridad de la TOE registrarán dentro de cada registro de auditoría al menos la siguiente información:

  a) fecha y hora del evento, tipo de evento, identidades del sujeto, suceso o falla del evento; y
  b) para cada tipo de evento, en base a las definiciones de evento auditable de los componentes funcionales incluidos en el PP/ST, [la información especificada en la columna 4 de la tabla 4.2].

Tabla 4.2 – Eventos auditables

Componente funcional	Nivel	Evento auditable	Contenido adicional del registro de auditoría
FMT_SMR.1	mínimo	Modificaciones para el grupo de usuarios que son parte del perfil del **administrador autorizado**.	La identidad del usuario que está siendo asociada con el perfil del administrador autorizado.
FIA_UID.2	básico	Todos los usos de los mecanismos de identificación de usuario, incluyendo la identidad de usuario proporcionada.	
FIA_UAU.1	básico	Cualquier uso de los mecanismos de autenticación.	
FIA_AFL.1	mínimo	El límite del umbral para los intentos de autenticación sin éxito, las acciones que se ejecuten y la subsecuente **restauración por parte del administrador autorizado**	

		de las capacidades de los usuarios para autenticarse.	
FDP_IFF.1	básico	Todas las decisiones sobre la solicitud de flujos de información.	La dirección origen y destino del sujeto.
FCS_COP.1	mínimo	Éxito y falla, y el tipo de operación de cifrado.	
FPT_STM.1	mínimo	Cambios de tiempo.	
FMT_MOF.1	extendido	Uso de las funciones listadas en este requerimiento concernientes a la auditoría.	

Tabla 4.2 – Eventos auditables (continuación)

FAU_SAR.1 revisión de auditoría

- FAU_SAR.1.1 – las funciones de seguridad de la TOE le darán al administrador autorizado capacidad para leer todos los datos del seguimiento de la auditoría a partir de los registros de auditoría.
- FAU_SAR.1.2 - las funciones de seguridad de la TOE proporcionarán los registros de auditoría en forma clara para que el usuario de éstos pueda interpretar la información.

FAU_SAR.3 revisión de auditoría seleccionable

- FAU_SAR.3.1 las funciones de seguridad de la TOE proporcionarán la posibilidad de ejecutar búsquedas y clasificaciones de datos de auditoría en base a:

  direcciones de sujetos; rangos de datos; rangos de tiempos; y rangos de direcciones.

FAU_STG.1 almacenamiento protegido de seguimiento de auditoría

- FAU_STG.1.1 – las funciones de seguridad de la TOE protegerán los registros de auditoría almacenados, de descubrimientos no autorizados
- FAU_STG.1.2 – las funciones de seguridad de la TOE prevendrán que no haya modificaciones a los registros de auditoría.

FAU_STG.4 prevención de pérdida de datos de auditoría

- FAU_STG.4.1 – las funciones de seguridad de la TOE prevendrán eventos auditables, excepto aquellos que sean ejecutados por el administrador autorizado, y limitará el número de registros de auditoría perdidos si el seguimiento de auditoría está completo.

El último componente del perfil es FMT_MOF.1, y aparece al último porque lista todas las funciones que van a ser proporcionadas por la TOE para uso exclusivo del administrador autorizado, y casi todo de estas funciones se basa en los componentes precedentes.

FMT_MOF.1 administración de la conducta de las funciones de seguridad

- FMT_MOF.1.1 – las funciones de seguridad de la TOE proporcionarán y restringirán la capacidad de ejecutar las siguientes funciones:

  a) inicialización y cierre;
  b) creación, supresión, modificación, y vista de las reglas de la política de seguridad de flujo de información que permitan o denieguen flujos de información;
  c) creación, supresión, modificación, y vista de los valores definidos de atributos de usuario en FIA_ATD.1;
  d) habilitación y des-habilitación de mecanismos de autenticación de uso simple en FIA_UAU.4;
  e) modificación y selección del umbral para el número de intentos permitidos para llevar a cabo la autenticación;
  f) restituir la capacidad de autenticación a usuarios que han alcanzado o superado el umbral de intentos permitidos para llevar a cabo la autenticación;
  g) habilitación y des-habilitación de comunicación de entidades IT externas con la TOE;
  h) modificación y selección de fecha y hora;
  i) archivar, crear, suprimir y vaciar el seguimiento de auditoría;
  j) respaldo de valores de atributos de usuario, reglas de la política de seguridad de flujo de información, y datos de seguimiento de auditoría, donde la capacidad de respaldo será soportada por herramientas automatizadas;
  k) recuperar el estado siguiente al último respaldo;

l) adicionalmente, si se soporta la administración remota:
   - habilitar y des-habilitar la administración remota desde una red interna o externa;
   - restringir las direcciones desde las cuales se pueda ejecutar la administración remota.

m) Otras funciones administrativas relevantes de seguridad que determine el desarrollador de la TOE.

4.4.2 Requerimientos de garantía de seguridad TOE

Los requerimientos de garantía de seguridad para este PP están tomados de la Parte 3 de los CC, EAL2; y estos componentes de garantía están resumidos en la tabla 4.3.

Tabla 4.3 – Requerimientos de garantía: EAL2

Clase de Garantía	**Componentes de Garantía**	
Administración de la configuración	ACM_CAP.2	Elementos de configuración
Entrega y operación	ADO_DEL.1	Procedimientos de entrega
	ADO_IGS.1	Procedimientos de instalación e inicialización
Desarrollo	ADV_FSP.1	Especificación funcional informal
	ADV_HLD.1	Diseño de alto nivel
	ADV_RCR.1	Demostración informal de correspondencia
Documentos guía	AGD_ADM.1	Guía del administrador
	AGD_USR.1	Guía de usuario
Pruebas	ATE_COV.1	Evidencia de transmisión
	ATE_FUN.1	Pruebas funcionales
	ATE_IND.2	Prueba independiente
Evaluación de vulnerabilidades	AVA_SOF.1	Robustez de la evaluación de las funciones de seguridad de la TOE
	AVA_VLA.1	Análisis de vulnerabilidad del desarrollador

ACM_CAP.2 elementos de configuración

Elementos de acción del desarrollador:

- ACM_CAP.2.1D – el desarrollador proporcionará una referencia para la TOE.
- ACM_CAP.2.2D – el desarrollador usará un sistema de administración de la configuración.
- ACM_CAP.2.3D – el desarrollador proporcionará documentación de administración de la configuración.

En cuanto a contenido y presentación de la evidencia:

- ACM_CAP.2.1C – la referencia para la TOE será única para cada versión de la TOE.
- ACM_CAP.2.2C – la TOE será etiquetada con su referencia.
- ACM_CAP.2.3C – la documentación de administración de la configuración incluirá una lista de configuración.
- ACM_CAP.2.4C – la lista de la configuración describirá los elementos de la configuración que comprometan a la TOE.
- ACM_CAP.2.5C – la documentación de la administración de la configuración describirá el método usado para identificar específicamente los elementos de configuración.
- ACM_CAP.2.6C – el sistema de la administración de la configuración identificará específicamente a cada uno de los elementos de la configuración.

ADO_DEL.1 procedimientos de entrega

Elementos de acción del desarrollador:

- ADO_DEL.1.1D – el desarrollador documentará los procedimientos para la entrega de la TOE o partes de ésta para el usuario.
- ADO_DEL.1.2D – el desarrollador usará los procedimientos de entrega.

En cuanto a contenido y presentación de la evidencia:

- ADO_DEL.1.1C – la documentación de entrega describirá todos los procedimientos que son necesarios para mantener la seguridad cuando se distribuyan las versiones de la TOE a cada uno de los sitios de los usuarios.

ADO_IGS.1 procedimientos de instalación e inicialización

Elementos de acción del desarrollador:

- ADO_IGS.1.1D – el desarrollador documentará los procedimientos necesarios para la correcta y segura instalación e inicialización de la TOE.

En cuanto a contenido y presentación de evidencia:

- ADO_IGS.1.1C – la documentación describirá los pasos necesarios para la correcta y segura instalación e inicialización de la TOE.

ADV_FSP.1 especificación funcional informal

Elementos de acción del desarrollador:

- ADV_FSP.1.1D – el desarrollador proporcionará la especificación funcional.

En cuanto a contenido y presentación de evidencia:

- ADV_FSP.1.1C – la especificación funcional describirá la TSF y sus interfaces externas usando un estilo informal.
- ADV_FSP.1.2C – la especificación funcional será consistente internamente.
- ADV_FSP.1.3C – la especificación funcional describirá el propósito y el método de uso de todas las interfaces TSF externas, proporcionando detalles referentes a efectos, excepciones y mensajes de error.
- ADV_FSP.1.4C – la especificación funcional representará completamente la función de seguridad de la TOE.

ADV_HLD.1diseño de alto nivel

Elementos de acción del desarrollador:

- ADV_HLD.1.1D – el desarrollador proporcionará el diseño de alto nivel de la función de seguridad de la TOE.

En cuanto a contenido y presentación de evidencia:

- ADV_HLD.1.1C – la presentación del diseño de alto nivel será informal.
- ADV_HLD.1.2C –el diseño de alto nivel será consistente internamente.
- ADV_HLD.1.3C – el diseño de alto nivel describirá la estructura de la función de seguridad de la TOE en términos de subsistemas.
- ADV_HLD.1.4C – el diseño de alto nivel describirá la funcionalidad de seguridad proporcionada para cada subsistema de la TSF.
- ADV_HLD.1.5C – el diseño de alto nivel identificará cualquier hardware, firmware, y/o software requerido por la función de seguridad de la TOE con una presentación de las funciones proporcionadas por los mecanismos de protección implementados en el hardware, firmware o software.
- ADV_HLD.1.6C – el diseño de alto nivel identificará todas las interfaces a los sistemas de las funciones de seguridad de la TOE.
- ADV_HLD.1.7C – el diseño de alto nivel identificará cuáles de las interfaces a los subsistemas de la TSF son visibles externamente.

ADV_RCR.1 demostración informal de correspondencia

Elementos de acción del desarrollador:

- ADV_RCR.1.1D – el desarrollador proporcionará un análisis de correspondencia entre todos los pares adyacentes de las representaciones TSF que se proporcionan.

En cuanto a contenido y presentación de evidencia:

- ADV_RCR.1.1C – para cada par adyacente de representaciones TSF proporcionadas, el análisis demostrará que todas las funcionalidades

de seguridad relevantes de la representación TSF más abstracta ha sido refinada correcta y completamente en la representación TSF menos abstracta.

AGD_ADM.1 guía del administrador

Elementos de acción del desarrollador:

- AGD_ADM.1.1D – el desarrollador proporcionará una guía de administrador del sistema.

En cuanto a contenido y presentación de evidencia:

- AGD_ADM.1.1C – la guía del administrador describirá las funciones administrativas y las interfaces disponibles para el administrador de la TOE.
- AGD_ADM.1.2C – la guía del administrador describirá cómo administrar la TOE de manera segura.
- AGD_ADM.1.3C – la guía del administrador contendrá advertencias con respecto a funciones y privilegios que deban ser controlados en un entorno de procesamiento seguro.
- AGD_ADM.1.4C – la guía del administrador describirá todas las hipótesis con respecto a la conducta de los usuarios que sean relevantes para asegurar la correcta operación de la TOE.
- AGD_ADM.1.5C – la guía del administrador describirá todos los parámetros de seguridad que estén bajo el control del administrador, indicando cuáles son considerados valores seguros.
- AGD_ADM.1.6C – la guía del administrador describirá cada tipo de eventos relevantes de seguridad relativos a las funciones administrativas que necesitan ser ejecutadas, incluyendo cambios a las características de seguridad de las entidades bajo el control de las funciones de seguridad de la TOE.
- AGD_ADM.1.8C – la guía del administrador describirá todos los requerimientos de seguridad que deberán cumplirse en el entorno IT y que sean relevantes para el administrador.

AGD_USR.1 guía de usuario

Elementos de acción del desarrollador:

- AGD_USR.1.1D – el desarrollador proporcionará la guía de usuario.

En cuanto a contenido y presentación de evidencia:

- AGD_USR.1.1C – la guía de usuario describirá las funciones e interfaces disponibles para los usuarios no administradores de la TOE.
- AGD_USR.1.2C – la guía de usuario describirá el uso de las funciones de seguridad accesibles a los usuarios.
- AGD_USR.1.3C – la guía de usuario contendrá advertencias respecto a las funciones accesibles a usuarios y los privilegios que deberán ser controlados en un entorno de procesamiento seguro.
- AGD_USR.1.4C – la guía de usuario presentará claramente las responsabilidades de los usuarios para una operación segura de la TOE, incluyendo las relacionadas a las especuladas con respecto a las posibles conductas que podrían poner en riesgo la seguridad de la TOE.
- AGD_USR.1.6C – la guía de usuario describirá todos los requerimientos de seguridad que deberán cumplirse en el entorno IT y que sean relevantes para el usuario.

ATE_COV.1 Evidencia de transmisión

Elementos de acción del desarrollador:

- ATE_COV.1.1D el desarrollador proporcionará evidencia de las pruebas de transmisión.

En cuanto a contenido y presentación de evidencia:

- ATE_COV.1.1C – la evidencia de las pruebas de transmisión mostrarán la correspondencia entre las pruebas identificadas en la documentación de las pruebas y las funciones de seguridad de la TOE tal y como se encuentren descritas en la especificación funcional.

ATE_FUN.1 pruebas funcionales

Elementos de acción del desarrollador:

- ATE_FUN.1.1D – el desarrollador probará las funciones de seguridad de la TOE y documentará los resultados.
- ATE_FUN.1.2D – El desarrollador proporcionará la documentación de las pruebas.

En cuanto a contenido y presentación de evidencia:

- ATE_FUN.1.1C – la documentación de las pruebas consistirá de los planes de prueba, descripciones de los procedimientos de prueba, resultados esperados y resultados obtenidos.
- ATE_FUN.1.2C – los planes de las pruebas identificarán las funciones de seguridad que serán probadas y describirán el objetivo de las pruebas.
- ATE_FUN.1.3C – las descripciones de los procedimientos de las pruebas identificarán las pruebas que serán ejecutadas y describirá los escenarios en que se probarán cada una de las funciones de seguridad.
- ATE_FUN.1.4C – los resultados esperados de las pruebas mostrarán por anticipado los resultados que se obtendrán de una prueba exitosa.
- ATE_FUN.1.5C – los resultados de la ejecución de las pruebas del desarrollador demostrarán que cada función de seguridad probada se comporta como se esperaba.

ATE_IND.2 prueba independiente

Elementos de acción del desarrollador:

- ATE_IND.2.1D – el desarrollador proporcionará la TOE de prueba.

En cuanto a contenido y presentación de evidencia:

- ATE_IND.2.1C - la TOE será la apropiada para las pruebas.

- ATE_IND.2.2C – el desarrollador proporcionará un conjunto equivalente de recursos a aquellos que fueron utilizados en las pruebas funcionales del desarrollador.

AVA_SOF.1 robustez de la evaluación de las funciones de seguridad

Elementos de acción del desarrollador:

- AVA_SOF.1.1D – el desarrollador realizará un análisis de robustez de la evaluación de las funciones de seguridad para cada mecanismo identificado en el objetivo de seguridad.

En cuanto a contenido y presentación de evidencia:

- AVA_SOF.1.1C – para cada mecanismo con una robustez de función de seguridad pretendida, el análisis de las funciones de seguridad mostrará que al menos se reúne para cada una el nivel de robustez definido.

AVA_VLA.1 análisis de vulnerabilidades del desarrollador

Elementos de acción del desarrollador:

- AVA_VLA.1.1D – el desarrollador realizará y documentará un análisis concerniente a todas las formas obvias en que un usuario pudiera violar las políticas de seguridad de la TOE.
- AVA_VLA.1.2D – el desarrollador documentará cómo se dispone de esas formas.

En cuanto a contenido y presentación de evidencia:

- AVA_VLA.1.1C – la documentación mostrará, para todas las vulnerabilidades identificadas (ver sección 4.5), que la vulnerabilidad no podrá ser explotada en el entorno de la TOE.

4.5 Vulnerabilidades identificadas

Algunas de las vulnerabilidades encontradas fueron

- **ftp**

Existe una vulnerabilidad que permite a usuarios remotos y locales obtener privilegios de root. Esto se comprueba a través del manejo de rutinas que permiten estos privilegios o a través del comando SITE EXEC[x**].

- **rlogin**

Si durante un intento de rlogin en un sistema vulnerable, el buffer que contiene el valor de la variable de entorno TERM es alcanzado, entonces se puede ejecutar un código arbitrario y utilizarlo como root.

- **Sendmail**

Usuarios remotos pueden ejecutar comandos arbitrariamente con los privilegios de root en sistemas que estén recibiendo correo, siempre que dichos sistemas operen en una versión vulnerable de sendmail que soporte MIME.

Cuando el sendmail no puede distinguir entre una "falla de recurso" y un "id de usuario no encontrado", entonces el sendmail crea sus propios archivos indicando "usuario por omisión" y con esto un usuario mal intencionado puede explotar una cuenta de usuario.[x***]

Cuando se envía correo, se retransmite o se incluyen archivos, es posible que un atacante obtenga los permisos de otro usuario para posteriormente hacer uso de ellos[3].

Cuando el buffer se satura es posible que usuarios no autorizados obtengan accesos tipo root[3].

[x**] http://www.cert.org.
[x***] http://www.phoneboy.com/fw1

➢ **tftp**

Si se permite que un usuario remoto (en Internet) pueda tener acceso a archivos legibles de alguna red interna (en una organización) utilizando un servicio tftp no restringido, los archivos podrían ser recogidos por un adversario que se encuentre en el lado externo del firewall[x**].

➢ **ataques spoofing IP**

Los firewalls son susceptibles a este tipo de ataques incluyendo los ataques por inundación TCP SYN; de manera que los firewalls deben tener mecanismos que manejen este tipo de ataques y que sean capaces de prevenir a la red interna del tráfico entrante que pretenda tener direcciones originarias de la red, direcciones broadcast o reservadas.

➢ **ataques UDP**

Existen herramientas para inundar los puertos UDP con paquetes de información que degradan el desempeño del sistema y congestionan la red, de manera que los firewalls deben poder configurarse para filtrar todos los servicios UDP.

Cuando se permite que un paquete UDP pase a través del firewall en base a las reglas con las que se haya configurado, la entrada se agrega a la tabla de conexiones;. como se puede responder a cualquier paquete UDP en un período determinado (40 segundos por omisión) entonces se relacionan las direcciones de los puertos SRC/DST IP y SRC/DST.

```
Src_IP Src_Prt Dst_IP Dst_Prt  IP_prot Kbuf Type Flags Timeout
192.168.1.10 1111 136.1.1.20 53 17 0 16386 ff01ff00 34/40
192.168.1.10 1111 136.1.1.20  0 17 0 16386 ff01ff00 34/40
192.168.1.10 1111 136.1.1.20 50 17 0 16386 ff01ff00 34/40
192.168.1.10 1111 136.1.1.20  3 17 0 16386 ff01ff00 34/40
```

Aquí se aprecia que el sistema 192.168.1.10 está haciendo un query dns al servidor 136.1.1.20. en los 40 segundos de vigencia el sistema puede estar recibiendo una gran cantidad de paquetes UDP, como se aprecia las entradas son idénticas a excepción de Dst_Prt, el cual es 53, 0, 50, 3, etc., entonces se va quedando en los query's hasta inundarse.

[x**] http://www.cert.org.

- **ICMP**

Si los datagramas ICMP son muy grandes, pueden ocasionar que el sistema se caiga o se paralice, resultando con ello en una denegación de servicio.

Cuando se tienen ICMP's muy grandes y éstos no son inspeccionados antes de que se les permita establecer contacto con las tablas del firewall, sin saberlo el usuario estará permitiendo ciegamente el tráfico ICMP[xxxx], inundando su tráfico de ECHO_REPLIES y con esto paralizándose su sistema.

- **RIP**

Como resultado de la facilidad con la cual los paquetes RIP pueden ser fingidos, es posible que se inyecten a la red paquetes de este tipo para atacar los hosts; y esto ocurre cuando los encaminadores aceptan paquetes RIP debido a que se ejecutan sin ningún tipo de autenticación; de manera que los firewalls deben poder configurarse de tal forma que no permitan el encaminamiento de paquetes en ciertos enlaces (considerados delicados) como enlaces intermedios de una red externa, si los hosts fuente y destino de ese enlace están dentro de la red interna.

- **ARP**

Debido a que cualquier host puede responder a una solicitud ARP, es posible que un host malicioso envíe un ARP falso y tome la respuesta para entonces poder interceptar, modificar o re-enviar tráfico fraudulento; de ahí que los firewalls no deben permitir que solicitudes ARP pasen a través de él.

- **DNS**

Una inundación de respuestas DNS inyectadas a la red puede ocasionar una denegación de servicio desde el servidor DNS que se puede volver confuso; y si un atacante puede contaminar la memoria de reserva de las respuestas DNS antes de que la llamada sea hecha entonces el objetivo puede ser inundado en la creencia de que se está checando una ejecución legítima, y el atacante obtiene el acceso.

[xxxx] http://www.phoneboy.com/fw1

Se trata de la misma prueba que permite encontrar la vulnerabilidad UDP :

```
Src_IP Src_Prt Dst_IP Dst_Prt  IP_prot Kbuf Type Flags Timeout
192.168.1.10 1111 136.1.1.20 53 17 0 16386 ff01ff00 34/40
192.168.1.10 1111 136.1.1.20  0 17 0 16386 ff01ff00 34/40
192.168.1.10 1111 136.1.1.20 50 17 0 16386 ff01ff00 34/40
192.168.1.10 1111 136.1.1.20  3 17 0 16386 ff01ff00 34/40
```

como se aprecia el sistema 192.168.1.10 está haciendo un query dns de manera que el sistema se inunda en la creencia de que se trata de una ejecución legítima.

Una acción que permite asegurar que el sistema no estará siendo usado indebidamente, es la vigilancia de los puertos, explorándolos e identificándolos comúnmente haciendo uso de sistemas de alerta[x**] como el que se muestra:

```
dns zone transfer 53/TCP
portmapper 111/TCP
http 80/TCP
SMB 139/TCP
imap 143/TCP
BackOrrifce 31337/UDP --> Yes, people are STILL scanning for old BO.
```

Algunos scripts empleados en pruebas para identificar vulnerabilidades son:

```
######################################################################
# BEGIN CUSTOMIZING SCRIPT HERE #
######################################################################

# INSTALL DIRECTORY
# Define the directory that this script is in.
# Do NOT put a slash at the end.
# EXAMPLE: dir=/home/fwadmin/alert
dir=

# FW ADMIN
# Define the name of who gets the email alerts
# EXAMPLE: user=fwadmin@example.com
user=

# SCAN LIMIT
# Define maximum number of scans/email alerts
limit=5

# EMAIL REMOTE SYSTEM
# Define as "true" if you want to automatically email
```

[x**] http://www.cert.org

```
# the remote admin when you reach your scan limit.
email=false

# SAM
# Define as "true" if you want to autotmatically block
# the source if you reach your scan limit.
sam=false
# SAM TIMEOUT
# How long do you want the source blocked
# Default is 3600 seconds (1 hour).
timeout=3600
######################################################################
# FINISH CUSTOMIZING SCRIPT HERE #
######################################################################
```

Para definirle las variables al sistema y checar si se alcanzan los límites:

```
### Script variables
message=/tmp/.message_$$
send=/tmp/.send_$$

### Good code is secure code
umask=177
PATH=/usr/bin:/sbin:/usr/sbin:/usr/local/bin
export PATH

if test -a $message
then
        rm $message
fi

if test -a $send
then
        rm $send
fi

### Set trap in case of abrupt exit
trap "rm $send $message ; exit 5" 1 2 15

### Grab User Defined Alert log, pipe to $message.
cat - | tail -1 > $message

### Determine number of scans.
ip=`awk '{print $10}' $message`
number=`grep -c $ip $dir/alert.log`
scan=`expr $number + 1`

### Check number of scans.  If we have reached our limit, lets bail
### now and save CPU cycles.
if [ $scan -gt $limit ];then
        cat $message >> $dir/alert.log
        rm $message
        exit 10
fi
```

```
### Parse log file
date=`awk '{print $1}' $message`
time=`awk '{print $2}' $message`
dst=`awk '{print $12}' $message`

### Determine service (check some variables first)
#Determine if "Valid Address" is in log files for NAT
nat_check=`grep -c "(Valid Address)" $message`

#Determine if protocol is icmp
icmp_check=`grep -c " icmp " $message`

if [ "$nat_check" -eq 0 ];then
        if [ "$icmp_check" -eq 0 ];then
                service=`awk '{print $14}' $message`
        else
                service=`awk '{print $15,$16,$17,$18}' $message`
        fi
else
        if [ "$icmp_check" -eq 0 ];then
                service=`awk '{print $16}' $message`
        else
                service=`awk '{print $17,$18,$19,$20}' $message`
        fi
fi
```

Es posible crear emails de alerta que chequen el send mail, y cuando detecte que hay un husmeador en potencia, envíe un email alert:

```
cat <<EOF > $send

Date: Wed, 14 Jun 2000 15:40:01 -0600 (CST)
From: ids@example.net
To: fwadmin@example.net
Subject: #### Firewall ALERT ####

----- CRITICAL INFORMATION -----
Date: 14Jun2000
Time: 15:39:59
Source: evil.example.org
Destination: ns1
Service: domain-tcp

----- ACTUAL LOG ENTRY -----

14Jun2000 15:39:59 drop fw1 >elx0 mail proto tcp src evil.example.org dst
ns1 service domain-tcp s_port 37401 len 44 rule 6
```

Los CC representan el resultado de una serie de esfuerzos para desarrollar criterios para la evaluación de seguridad IT que sean útiles en términos generales para la comunidad internacional. A principios de la década de 1980's los Criterios de Evaluación de Sistemas de Cómputo Confiables (Trusted Computer System Evaluation Criteria <TCSEC>) se desarrollaron en los Estados Unidos. En la década siguiente, varios países emprendieron iniciativas para desarrollar criterios de evaluación que fueran construidos mediante los conceptos de los TCSEC pero más flexibles y adaptables a la evolución natural de la IT en general. Llegando así a nuestros días con el desarrollo de los CC publicados a finales de 1999.

Como se planteó al inicio del presente trabajo, la evaluación de sistemas y/o productos IT debe llevarse a cabo para determinar el grado de confiabilidad que dicho sistema brinda a los usuarios, para que los desarrolladores puedan garantizar la confiabilidad que el usuario pueda tener en sus productos, y para que dicha evaluación conduzca a objetivos y resultados que sean repetibles y puedan ser citados como evidencia.

No obstante es necesario notar que la aplicación de criterios contiene elementos objetivos y subjetivos, y esto es precisamente porque no son factibles indicadores precisos y universales de la seguridad IT; y de ahí la gran importancia de contar con Criterios Comunes para la Evaluación que permitan hacer uso de la misma métrica en todos los sistemas y productos en los que se requiere seguridad IT, de manera que brinden también mayor confiabilidad a los usuarios, sin tener que preocuparse por un producto de un fabricante en particular sino por un producto que cubra las características de seguridad IT que requiera el usuario o la organización en cuestión a través de un nivel de garantía (EAL).

Por lo que la guía aquí desarrollada resultará en un efectivo y real beneficio para todas aquéllas personas que en México requieren adquirir sistemas seguros y confiables de cómputo, así como para sus instituciones u organizaciones y de igual manera para desarrolladores y distribuidores de los sistemas que les permitirá garantizar la seguridad requerida por parte de sus usuarios y ampliar sus mercados de ventas, no solo en el país sino en el exterior.

Así como es necesario proporcionarles las herramientas necesarias a los que adquieren los sistemas/productos IT, también se requiere brindar a los desarrolladores de los sistemas/productos IT las herramientas que les permitan

desarrollar todo aquello que sus usuarios requieren y con la garantía de que pueden confiar en la seguridad con la que se desarrollan, así el temario propuesto para un curso sobre sistemas confiables, resultará un gran apoyo para todos aquellos profesores y estudiantes de la seguridad IT, así como para todas aquéllas personas interesadas en esta área de estudio en nuestro país, ya que les permitirá estar a la par con estudiantes de otras universidades en el mundo.

Para mostrar la aplicación y la utilidad de los criterios se consideró un caso práctico, para el cual el objeto de evaluación seleccionado fue un firewall, debido a la gran difusión que estos dispositivos tienen en un sinnúmero de instituciones y organizaciones en nuestro país y que al desarrollar el PP se puede apreciar claramente que si no se tienen claramente identificados los objetivos de seguridad que se persiguen, y los requerimientos de seguridad que se pretenden cubrir, entonces el dispositivo (firewall en este caso) no brindará la seguridad que en el entorno se requiere y lejos de brindar protección a la red de la organización, puede caer en alguna de las vulnerabilidades detectadas siendo un puerta de acceso a intrusos maliciosos!

Después de haber aplicado los CC se puede apreciar la flexibilidad que tienen para permitir conjuntar el material necesario estableciendo el entorno y los requerimientos de seguridad, los objetivos de seguridad y la especificación del objeto de estudio (firewall), de manera que desde el punto de vista usuario el contar con este material le permite al comprador adquirir un equipo que efectivamente cumpla con las condiciones que requiere; y desde el punto de vista desarrollador el contar con este material le permite al fabricante construir equipos que resuelvan las problemáticas a las que se enfrentan los usuarios, ganando credibilidad y mercado.

Falta el punto de vista evaluador, para lo cual sería muy interesante el plantear la posibilidad de montar en nuestro país (porque no lo hay) un laboratorio de pruebas y evaluación de sistemas y/o productos de seguridad IT; este puede ser un objetivo a futuro ya que primero se requiere de profesionales capacitados en áreas de seguridad IT que conozcan y aprecien el valor y la responsabilidad que conlleva la seguridad en tecnología de la información para algún día poder contar con un laboratorio de estos alcances.

Finalmente, este trabajo de tesis incluye la traducción del documento "Criterios Comunes para Evaluación de Seguridad de Tecnología de la Información (CC2.1)" la cual representa un beneficio adicional para todos

aquéllos estudiantes hispanoamericanos que se encuentren realizando estudios de doctorado, maestría y/o licenciatura como apoyo para entender el proceso de evaluación y caracterización de la confiabilidad de sistemas; y se sugiere que en la medida de lo posible para estudios minuciosos y refinados se revise la versión original que está en http://csrc.ncsl.nist.gov/cc/ccv20/ccv2list.htm

CC Criterios Comunes (**C**ommon **C**riteria)

EAL Nivel de Garantía de la Evaluación (**E**valuation **A**ssurance **L**evel)

IT Tecnología de la Información (**I**nformation **T**echnology)

PP Perfil de Protección (**P**rotection **P**rofile)

SF Función de Seguridad (**S**ecurity **F**unction)

SFP Política de Función de Seguridad (**S**ecurity **F**unction **P**olicy)

SOF Función de Resistencia (**S**trength **o**f **F**unction)

ST Meta u Objetivo de Seguridad (**S**ecurity **T**arget)

TOE Meta u Objetivo de Evaluación (**T**arget **o**f **E**valuation)

TSC Ámbito de Control TSF (**T**SF **S**cope **o**f **C**ontrol)

TSF Funciones de Seguridad TOE (**T**OE **S**ecurity **F**unctions)

TSFI Interface TSF (**T**SF **I**nterface)

TSP Políticas de Seguridad TOE (**T**OE **S**ecurity **P**olicy)

Este glosario contiene únicamente las principales abreviaturas usadas en los CC.

Date: Mon, 15 May 2000 15:10:32 -0400
From: Ron Ross <ron.ross@mindspring.com> Add to Address Book **Add To Spam Block List**
Subject:RE: cc v 2.1
To:"Dr. Enrique Daltabuit Godas" <enrique@orbis.org.mx>
Cc: Gene Troy <eugene.troy@nist.gov>

You may proceed with an unofficial translation of the Common Criteria into Spanish for academic purposes.

Regards,

Ron Ross

> -----Original Message-----
> From: Dr. Enrique Daltabuit Godas [mailto:enrique@orbis.org.mx]
> Sent: Monday, May 15, 2000 2:50 PM
> To: Gene Troy; RRoss@nist.gov
> Subject: Re: cc v 2.1
>
>
> Thank you very much for your extremely prompt reply.
>
> I have no wish to become involved in the official spanish
> translation of the
> CC. I fully realize that it is a thorny project.
>
> My need derives from teaching a graduate course on Infosec to
> students whose
> grasp of English is at best tenuous. I only propose to produce a
> document that
> students can read to learn. Would it be possible to proceed with
> a translation
> if we labelled every page in an appriopiate way? If we restricted the
> availability to registered students?
>
> Collaborating with the Spanish translators would be a nightmare,
> because the
> spanish "computerese" is very different from the mexican one.
> Sometimes it is
> hard for us to understand papers writen in spanish. Also the National
> University has no authority on Infosec in Mexico.
>
> Thanks for your time.
>
> --
> Enrique Daltabuit
> Coordinador
> Centro Tecnológico Aragón - UNAM
> VOICE 011-525-623-0960
> FAX 011-525-623-0864

1. Canadian Trusted Computer Product Evaluation Criteria, Versión 3.0, Centro de Seguridad del Sistema Canadiense, Personal de Seguridad de Comunicaciones, Gobierno de Canadá, Enero 1993.

2. Connolly, J. L., and B. S. Abramowitz, The Trust Technology Assessment Program and the Benefits to U.S. Evaluations, *Proceedings of the 11th Annual Computer Security Applications Conference*, pp. 157-161, New Orleans, LA, December 1995.

3. Chapman and Zwicky, "Building Internet Firewalls", O'Reilly and Associates, November 1995.

4. Flahavin, E. E., and P. R. Toth, Concept Paper An Overview of the Proposed Trust Technology Assessment Program, *Proceedings of the 15th National Computer Security Conference*, Vol. I, pp. 84-92, Baltimore, MD, October 1992.

5. Information Technology Security Evaluation Criteria, Versión 1.2, Oficina para Publicaciones Oficiales de la Comunidad Europea, Junio 1991.

6. Information processing systems – Open Systems Interconection – Basic Reference Model, Parte 2: Arquitectura de Seguridad.

7. Kou, W., "Networking Security and Standards", Kluwer Academic Publishers, Boston/Dordrecht/London, 1997.

8. Stallings, W., "Network Security Essentials", Prentice Hall, New Jersey, 2000.

9. Rodríguez, L.A., "Seguridad de la Información en Sistemas de Cómputo", Ventura, 1995.

10. Trusted Computer Systems Evaluation Criteria, US DoD, Diciembre 1985.

---

* http://www.radium.ncsc.mil/tpep/ttap/facilities.html
** http://www.radium.ncsc.mil/tpep/ttap/facilities.html
*** http://www.commoncriteria.org
**v http://www.commoncriteria.org
v http://www.radium.ncsc.mil/tpep/process/faq-sectl.html
v* http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-005.txt
v** http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.txt
v*** http://niap.nist.gov/
*X http://www.radium.ncs.mil/tpep/library/rainbow/index.html
x http://radium.ncsc.mil/tpep/library/ramp-Modulos/index html
x* http://www.radium.ncsc.mil/tpep/library/protection_profiles/index.html
y http://niap.nist.gov/cc-scheme/PPRegistry.html
x** http://www.cert.org
x*** http://www.phoneboy.com/fw1