MODELO PARA LA EVALUACION EN SEGURIDAD INFORMÁTICA A PRODUCTOS SOFTWARE, BASADO EN EL ESTÁNDAR ISO/IEC 15408 COMMON CRITERIA

JOSE ALEJANDRO CHAMORRO LOPEZ

Universidad Icesi
Facultad de Ingeniería
Departamento Académico de Tecnologías de Información y Comunicaciones
Maestría en Gestión de Informática y Telecomunicaciones
Santiago de Cali
2011

MODELO PARA LA EVALUACION EN SEGURIDAD INFORMÁTICA A PRODUCTOS SOFTWARE, BASADO EN EL ESTÁNDAR ISO/IEC 15408 COMMON CRITERIA

JOSE ALEJANDRO CHAMORRO LOPEZ

Trabajo de Grado para optar al título de Magister en Gestión de Informática y Telecomunicaciones con énfasis en Gerencia de Tecnologías de Información y Telecomunicaciones

Director Dr. Francisco Pino

Universidad Icesi
Facultad de Ingeniería
Departamento Académico de Tecnologías de Información y Comunicaciones
Maestría en Gestión de Informática y Telecomunicaciones
Santiago de Cali
2011

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Santiago de Cali, 10 de Diciembre de 2011

DEDICATORIA

A Dios que en una de su tantas manifestaciones de amor, me ha expresado por la Virgen Madre María, todo lo que valgo y puedo llegar a ser. A mis padres José Sídney, Alma Mercedes y hermana Isabel Cristina, quienes son las fortalezas para caminar hacia el sol siempre, y a mí sobrina Ana Sofía que tuvo que nacer para motivarme a alcanzar este sueño y entregarle el diploma antes de su bautizo.

AGRADECIMIENTOS

A Francisco Pino por creer en cosas raras como estas, a la empresa Password por ser una de mis mayores motivaciones y logros profesionales, a la empresa Nexura en su representante James Martínez, a Jason Ceballos, Oscar Mondragon por apoyarme en la ejecución de este proyecto y a Liliana Gómez por compartir su gran conocimiento y amabilidad, a pesar de que yo llegue al final.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

La seguridad en las tecnologías de la información y comunicaciones (TICs), se hace tan indispensable como su funcionalidad misma. Preservar la disponibilidad, integridad y confidencialidad, de sus datos y operaciones, es un reto que se hace cada día más complejo, por su misma evolución y los riesgos que cada día se vuelven más sofisticados, al estar cada vez los usuarios mejor conectados y menos controlados.

Actualmente existen diferentes estándares, modelos, sistemas de gestión y buenas prácticas que promueven la seguridad de la información en las compañías y tecnologías, dentro del más relevante es el estándar ISO/IEC 15408 Common Criteria[1], el cuál es un acuerdo internacional entre diferentes organizaciones de todo el mundo para que con base al cumplimiento de funciones y niveles de evaluación, se garantice diseño, desarrollo y puesta en producción con medidas de seguridad adecuadas para el mercado, entidades vigilantes y la comunidad en general.

En Colombia, este estándar no es muy común y en Latinoamérica no existe hasta el momento un laboratorio o centro de investigación que certifique la aplicación de este estándar, pero que a medida que la globalización y las apuestas productivas del país se enfocan al desarrollo y producción de tecnología, se hace necesario adoptarlo.

Se realizó entonces un análisis de riesgo a un conjunto de sistemas software seleccionados de acuerdo a los requerimientos de ley en Colombia, con el fin de determinar que tan distantes están del cumplimiento del estándar ISO/IEC 15304 y sus falencias generales en seguridad. El resultado no fue bueno, y refleja la falta de documentación y detalle en las funciones de seguridad del software que se desarrolla en las empresas seleccionadas y la no prevención de incidentes de seguridad ante las amenazas reales de un ambiente de producción.

[1] SYMANTEC. Descripción general de la tecnología. http://www.symantec.com/es/es/about/profile/technology.jsp. [Citado el 13 de Noviembre 2011].

A partir de estos resultados se desarrollo un modelo, por el cual un software logre conceptualizarse en un TOE (Target Of Evaluation) que corresponde a una TIC (Tecnologías de la Información y Comunicaciones) en el estándar, y evaluarse de acuerdo a un ST (Secure Target) oficial del portal Common Criteria, bajo las funciones y niveles exigidos, con el fin de especificar un resultado de cumplimiento y las recomendaciones de mejora.

Todo esto esperando motivar iniciativas que acerquen más el desarrollo de Tecnologías de la Información y Comunicaciones al estándar ISO/IEC 15408 y logren a mediano plazo laboratorios y centro de investigación y certificación que apoyen a la región latinoamericana.

1. INTRODUCCION

1.1 Contexto del trabajo

La seguridad en los componentes de las tecnologías de la información (Seguridad Informática)[2], es una de las necesidades que junto con las funcionales es fundamental, debido a que un fallo en ella genera un impacto directo en contra del objetivo por el cual fueron concebidos los componentes.

Para la seguridad de las tecnologías de la información existen los siguientes estándares y buenas prácticas[3]:

- **ISO 27001 [2].** El estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) fue aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Es consistente con las mejores prácticas descritas en ISO/IEC 27002 y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI)[4].
- **Cobit.** Objetivos de Control para Tecnologías de información y relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información,(ISACA, Information Systems Audit and Control

[2] REVISTA DE INGENIERÍA. No.19. Universidad de los Andes. Facultad de Ingeniería. Mayo 2004. ISSN:0121-4993.
[3] ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS. XI Jornadas de Seguridad Informática, presentación III Encuesta Latinoamérica de Seguridad de la Información. http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XI_JornadaSeguridad/Presentacion_Jeimy_Cano_III_ELSI.pdf [Citado el 13 de Noviembre 2011]
[4] PORTAL ISO27001 EN ESPAÑOL. ISO 27000. http://www.iso27000.es/iso27000.html. [Citado el 13 de Noviembre 2011]

Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, IT Governance Institute) en 1992[5].

- **Magerit.** Es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas". Es una metodología de carácter público, perteneciente al Ministerio de Administraciones Públicas en España y fue elaborado por el Consejo superior de administración pública[6].
- **Octave.** Es metodología de evaluación de riesgos desarrollada por el SEI (Software Engineering Institute) de la Carnegie Mellon University[7].
- **Guías NIST (National Institute of Standars and Technology) USA.** Guía de referencia para la medición, diseño y desarrollo de tecnología del Instituto Nacional de Normas y Tecnología de los Estados Unidos[8].
- **Guías de la ENISA (European Network of Information Security Agency).** Son guías generadas por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), que buscan establecer estándares y mejores prácticas para el mejoramiento de las redes y la seguridad de la información en la Unión Europea[9].
- **Top 20 de las fallas de seguridad del SANS.** Son los fallos de seguridad informática más críticos que presenta anualmente el instituto de Auditoría, Redes y Seguridad (SysAdmin Audit, Networking and Securityre Institute) ubicado en Maryland Estados Unidos[10].

---

[5] INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. Control Objectives for Information and related Technology. http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx. [Citado el 13 de Noviembre 2011]

[6] GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL Y ADMINISTRACION PÚBLICA. MAGERIT versión 2. http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184 [Citado el 13 de Noviembre 2011]

[7] SOFTWARE ENGINEERING INSTITUTE CARNEGIE MELLON. Operationally Critical Threat, Asset, and Vulnerability Evaluation. http://www.cert.org/octave/ . [Citado el 13 de Noviembre 2011]

[8] NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY. Computer Security Resource Center. http://csrc.nist.gov/. [Citado el 13 de Noviembre 2011]

[9] EUROPEAN NETWORK OF INFORMATION SECURITY AGENCY. Publications. http://www.enisa.europa.eu/publications. [Citado el 13 de Noviembre 2011]

[10] SYSADMIN AUDIT, NETWORKING AND SECURITYRE INSTITUTE. Cyber Defense Initiative. https://www.sans.org/cyber-defense-initiative-2011/?utm_source=web-sans&utm_medium=text-ad&utm_content=Featured_Links_Homepage_20110810_FE_Links&utm_campaign=SANS_CDI_East_2011_&ref=84139. [Citado el 13 de Noviembre 2011]

- **OSSTMM (Open Standard Security Testing Model) [2].** Manual de la Metodología Abierta de Testeo de Seguridad desarrollado por la ISECOM (Institute for Security and Open Methodologies), el cual da una referencia para realizar análisis de seguridad informática en diferentes niveles[11].
- **ISM3 - Information Security Management Maturiy Model.** Estándar para la creación de sistemas de gestión de la seguridad de la información, basados en ITIL, ISO27001 o Cobit. A través de metodologías de análisis de riesgo que tienen como objetivo garantizar la consecución de los objetivos del negocio[12].
- **ITIL.** Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (Information Technology Infrastructure Library), es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general[13].
- **ISO/IEC 15408 Common Criteria.** Conjunto de estándares sobre seguridad de productos TIC (Tecnologías de Información y Comunicaciones) ya utilizados por diferentes países, el cual genera un resultado de evaluación que establece un nivel de confianza en el grado en el que el producto TIC satisface la funcionalidad de seguridad y ha superado las medidas de evaluación aplicadas[14].

El estándar de Common Criteria, según Symantec "*representa el estándar de seguridad universal*" y es obligatorio por parte del Departamento de Defensa de los EE. UU para sus productos[15].

---

[11] INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES. Open Standard Security Testing Model. http://www.isecom.org/osstmm/. [Citado el 13 de Noviembre 2011]

[12] INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES. Information Security Management Maturity Model. www.isecom.org/ism3/. [Citado el 13 de Noviembre 2011]

[13] APM GROUP LTD. Official ITIL Website. http://www.itil-officialsite.com/home/home.aspx. [Citado el 13 de Noviembre 2011]

[14] THE COMMON CRITERIA RECOGNITION ARRANGEMENT. The Common Criteria. http://www.commoncriteriaportal.org/cc/. [Citado el 13 de Noviembre 2011]

[15] SYMANTEC. Descripción general de la tecnología. http://www.symantec.com/es/es/about/profile/technology.jsp. [Citado el 13 de Noviembre 2011].

En Colombia la aplicación de este estándar es apenas del 2,8% según el estudio de la ACIS[16] y no existen en Latinoamérica laboratorios de testeo y certificación según puede verificarse en la lista oficial[17], lo cual presenta una oportunidad de estudio tesis con el fin de acercar este estándar de seguridad universal al software en Colombia y ayudar a generar mejorar medidas y prevenciones ante los graves incidentes mencionados anteriormente.

1.2 Definición del problema

La complejidad de las medidas requeridas para el aseguramiento de los sistemas de información, se hace mayor cada día, obligando a todos los interesados, a facilitar el desarrollo de esquemas, que tengan en cuenta el carácter globalizado de las Tecnologías de la Información por la conectividad y disponibilidad necesaria y los problemas de delitos informáticos que son cada día más críticos. Por ejemplo, en los Estados Unidos se reportaron en el año 2010, 303.909 incidentes de seguridad informática[18] a través de "The Internet Crime Complaint Center (IC3)" del "Federal Bureau of Investigation (FBI)" y el "National White Collar Crime Center (NW3C)"; y se determinaron pérdidas económicas de gastos directos del 57,6% de acuerdo al COMPUTER SECURITY INSTITUTE[19], donde no se incluyen perdidas de valor en bolsa o ventas futuras.

Esto se suma a los problemas que evidenció la comunidad de crackers más popular en la actualidad "Anonymous", el 30 de Noviembre del 2011, la cual aseguró que accedió a cuentas de clientes importantes en bancos de Estados Unidos como Chase Bank, Bank of America y a tarjetas de crédito de Citibank[20] y

[16] ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS. Seguridad Informática en Colombia Tendencias 2010-2011. http://www.acis.org.co/fileadmin/Revista_119/Investigacion.pdf [Citado el 13 de Noviembre 2011]

[17] THE COMMON CRITERIA RECOGNITION ARRANGEMENT. The Common Criteria labs. http://www.commoncriteriaportal.org/labs/ . [Citado el 13 de Noviembre 2011]

[18] INTERNET CRIME COMPLAINT CENTER. 2010 Internet Crime Report. http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf [Citado el 4 de Diciembre 2011]

[19] COMPUTER SECURITY INSTITUTE. 2010/2011 Computer Crime and Security Survey. New York: 2011. 12 p.

[20] NOTICIERO INTERNACIONAL CM&, 30 de Noviembre 2011. Bogotá: CM& La Noticia, 2011. Video Streaming [FLV] (11:38 min): son.col., español.

que les robará dinero para dárselo a los pobres a través de organizaciones benéficas.

Figura 1 Amenaza de Anonymous contra los bancos

Fuente: NOTICIERO INTERNACIONAL CM&, 30 de Noviembre 2011.
http://www.cmi.com.co/?pr=NOTICIERO%20CMI

En Colombia portales en Internet tales como www.zone-h.org (The Internet Thermometer) ponen al descubierto vulnerabilidades muy graves explotadas en sistemas informáticos de entidades públicas y privadas.

Date	Notifier	H	M	R	L	Domain	OS	View
2011/12/03	Cyber-Crystal					aenigma.co/wp-content/themes/k...	Linux	mirror
2011/12/03	kinG oF coNTroL		M			sindi.co/cgi-sys/suspendedpage...	Linux	mirror
2011/12/03	Hmei7		M			laguminang.co/cgi-sys/movingpa...	Linux	mirror
2011/12/02	Ashiyane Digital Security Team					www.pastojoven.gov.co/media/ku...	Linux	mirror
2011/12/02	a.r.o..slimani	H	M			webinnovations.co	Linux	mirror
2011/12/02	DR-MTMRD		M			www.globizme.co//index.html	Win 2003	mirror
2011/12/02	Cyber-Crystal	H	M			healthyoption.co	Linux	mirror
2011/12/02	9Y3H.511	H	M			agrocolombia.co	Linux	mirror
2011/12/01	Geuks	H				www.eutigutima.edu.co	Linux	mirror
2011/12/01	aBu.HaliL501	H	M			thecorporations.co	Linux	mirror
2011/11/30	HexyL	H	M			www.bakcasus.co	Linux	mirror
2011/11/30	Hepatit	H				zaishengjiao.co	Linux	mirror
2011/11/30	The GreaT TeAm	H	M			fansgoogle.co	Linux	mirror
2011/11/30	aHz-CreW	H	M			aerometric.co	Linux	mirror
2011/11/30	Turkish Energy Team					cevide.cali.gov.co/images/comp...	Linux	mirror
2011/11/30	ar3sw0rmed					reverdecer.com.co/ar3sw0rmed.html	Linux	mirror
2011/11/30	7rb-team	H	M			latingraf.com.co	Linux	mirror
2011/11/30	7rb-team	H	M			latincup.com.co	Linux	mirror
2011/11/30	SLYHACKER	H	M			clasificadosgratis.co	Linux	mirror
2011/11/30	ar3sw0rmed		M			dulcesfiestas.com.co/ar3sw0rme...	Linux	mirror
2011/11/30	Mr.L4iVe		M			www.sugar.seteco.com.co/robots...	Linux	mirror
2011/11/30	Mr.L4iVe		M			www.optipanel.seteco.com.co/ro...	Linux	mirror
2011/11/30	Mr.L4iVe		M			www.jarryscomercializadora.set...	Linux	mirror
2011/11/30	Mr.L4iVe	H	M			www.panelalsacia.co	Linux	mirror
2011/11/30	7rb-team	H	M			www.industechnologies.co	Linux	mirror

Figura 2 Ataques reportados a entidades colombianas
Fuente: http://www.zone-h.org

Tal es el caso de UNE, el 19 de Febrero del 2010, empresa a la que un cracker con el alias de “syskc0”, realizó un ataque de XSS (Cross Site Scripting) a su sitio web principal. Es de tener en cuenta que la empresa UNE fue la encargada de soportar la operación tecnológica de las elecciones en Colombia en el 2010, las cuales tuvieron serios incidentes el día del conteo de la votación para el congreso y consulta de partidos, ocurridos el 14 de Marzo del 2010[21].

[21] UNE, A RENDIR CUENTAS POR IRREGULARIDADES EN DATOS DE ELECCIONES. EL ESPECTADOR. http://www.elespectador.com/noticias/politica/articulo193149-une-rendir-cuentas-irregularidades-datos-de-elecciones [Citado el 4 de diciembre del 2011]

Figura 3 Ataque a UNE el 19 de febrero del 2010
Fuente: http://www.zone-h.org/mirror/id/10272455

También es de anotar el caso presentando en la Alcaldía de Bogotá, donde se manipularon las bases de datos del sistema de información que controla el proceso de impuestos para disminuir el valor de las facturas de una manera fraudulenta[22].

Todo este panorama evidencia que las Tecnologías de la Información y Comunicaciones, se ven afectadas por serios problemas en seguridad que promueven esta materialización de incidentes; en el caso especifico de Colombia, donde, el 92%[23] de las empresas desarrolladoras de software son pequeñas y el 7% medianas, las cuales no cuentan con el personal ni los recursos económicos para garantizar el cumplimiento de protocolos de pruebas de vulnerabilidad exigidos en el contexto internacional. Igualmente, el desarrollo en investigación sobre seguridad informática es incipiente y el número de expertos en seguridad en el país es bajo, aunque existen diversas iniciativas orientadas a la capacitación de profesionales en esta área como diplomados y especializaciones (UPB Bucaramanga, Universidad de los Andes, Universidad Autónoma de Occidente y

[22] FRAUDE EN IMPUESTOS. EL ESPECTADOR. http://www.elespectador.com/impreso/bogota/articulo-314297-fraude-impuestos [Citado el 4 de diciembre del 2011]

[2323] APUESTAS PARA CRECER. Apuestas para Crecer: Las oportunidades en software y servicios. En: Revista Dinero. No 312 (Octubre, 2008).

Universidad Pontificia Bolivariana), así como el salón de Informática y las Jornadas de Seguridad que organiza la ACIS (Asociación Colombiana de Ingenieros de Sistemas), pero que no han logrado hasta el momento un acercamiento de los procesos de desarrollo del software al estándar ISO/IEC 15408 Common Criteria.

1.3 Objetivo general

La presente tesis de grado para optar por el titulo de Maestría en Gestión de Informática y Telecomunicaciones tiene como objetivo general:

Formular y Diseñar un modelo que permita implementar la evaluación en seguridad informática, al software bajo el estándar ISO/IEC 15408 Common Criteria.

1.4 Objetivos específicos

Los objetivos específicos son los siguientes:

- Determinar un conjunto de productos software a los que se les puede aplicar la evaluación en seguridad informática basadas en la ISO/IEC 15408 Common Criteria.
- Realizar un análisis de riesgo en seguridad informática siguiendo Common Criteria a los productos software establecidos.
- Diseñar el modelo para la evaluación en seguridad informática de productos software de acuerdo a la ISO/IEC 15408 Common Criteria.
- Evaluar el modelo en un producto software específico.

1.5 Resumen estrategia propuesta

Se realizó un análisis de riesgo en seguridad informática, basado en la norma ISO/IEC 15408 Common Criteria a productos software pertenecientes a sectores empresariales Financiero, Salud y Gobierno, a los que la ley en Colombia les exige seguridad informática. El resultado en general fue el siguiente:

Crítico para los sistemas de información del muestro realizado en Colombia, con un porcentaje del 84%, en donde la seguridad no es una prioridad que se ajusta a la norma ISO/IEC 15408-3 Common Criteria, y no hay definición de las funciones de seguridad, guías de implementación, prevenciones y pruebas permanente de seguridad, y documentación estricta. Figura 4.

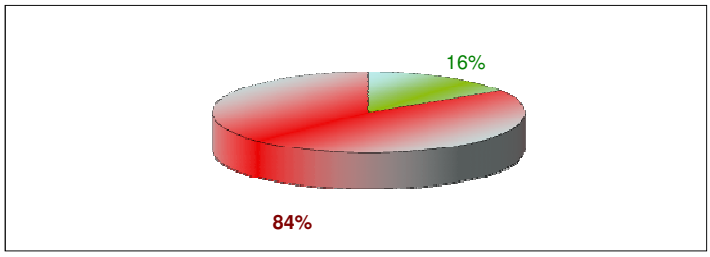


Figura 4 Riesgo general consolidado

De acuerdo a estos resultados se plantea un modelo que permita a los desarrolladores de software, realizar la evaluación de sus productos conceptualizados en un TOE (Target Of Evaluation) en seguridad informática de acuerdo a la norma ISO/IEC 15408-3 Common Criteria en sus dos primeros niveles de evaluación (EAL1 – Probado funcionalmente y EAL2 – Probado estructuralmente) y así identificar las debilidades y sus respectivas recomendaciones de mejora.

Los componentes generales del modelo son los siguientes. Figura 5:

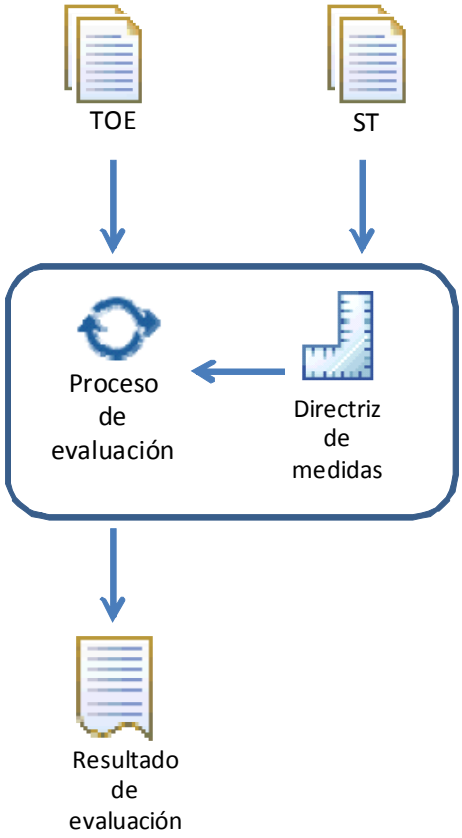


Figura 5 Modelo de ejecución de pruebas

- ST. Objetivo de seguridad. Documento oficial publicado en el Common Criteria, que describe las características de un TOE especifico (Sistema de información, base de datos, sistema operativo o hardware) ideal dividido en:
    - Límites Físicos. Descripción del hardware, en donde implementará el TOE.
    - Limites Lógicos. Descripción del software, que implementará el TOE, basado en sus funciones.
    - Entorno de seguridad del TOE. Es donde se identifican las hipótesis del entorno físico, características de los usuarios autorizados, las

hipótesis del entorno lógico y las amenazas dirigidas al TOE y al ambiente operacional.

  - Objetivos de seguridad. Se especifican los objetivos que cumplirá el TOE en seguridad relacionados a autenticación y gestión de privilegios.

  - Requerimientos de seguridad. Funciones y niveles de garantía de seguridad que cumple el TOE.

- TOE. Objetivo de evaluación. Componente TIC seleccionado para evaluar su seguridad bajo la norma ISO/IEC 15408 Common Criteria ST, dividido en límites físicos, lógicos, entorno de seguridad del TOE, objetivos de seguridad y requerimientos de seguridad.

- Directriz de medidas. De acuerdo a la importancia que se quiera dar a los ítems del ST, se establece una directriz de evaluación con un peso específico para cada ítem que permita generar un valor de calificación al aplicarse.

- Proceso de evaluación. Describe el conjunto de actividades para comparar el TOE con el ST, el cual aplica una directriz de medidas de acuerdo a lo similar que estos dos sean en sus especificaciones de entorno de seguridad, objetivos de seguridad, requerimientos de seguridad y niveles de seguridad.

- Resultado de evaluación. De acuerdo a los ítems del ST y la directriz de medidas, se presentarán un resultado de evaluación cuantitativo que permita establecer el nivel de seguridad del TOE a evaluar.

Cada componente tiene un rol responsable, los cuales son:

NOMBRE	ROL
RTOE	Responsable del TOE al que se le aplicará el modelo y se evaluará
ETOE	Responsable de la evaluación del TOE de acuerdo a las directrices determinadas basadas en la norma ISO/IEC 15408 Common Criteria

Tabla 1 Roles Modelo

Las actividades para cada componente del modelo, se especifican con el siguiente diagrama:

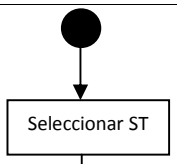
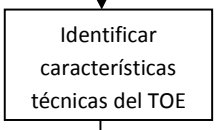
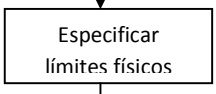
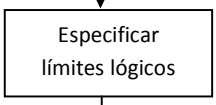
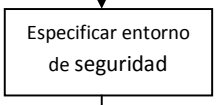
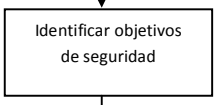
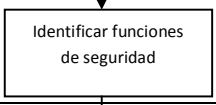
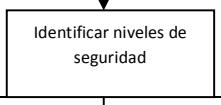
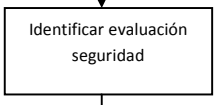
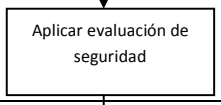
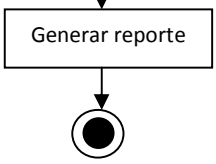
COMPONENTE	ACTIVIDAD	RESPONSABLE
ST		RTOE
TOE		RTOE
TOE		RTOE
TOE		RTOE
TOE		RTOE
TOE		RTOE
TOE		RTOE
TOE		ETOE
Directriz de medidas		ETOE
Proceso de evaluación		ETOE
Reporte		ETOE

Tabla 2 Diagrama y descripción de actividades del modelo

De acuerdo a la directriz de evaluación, se plantea los siguientes rangos de cumplimiento de seguridad informática:

CUMPLIMIENTO PARAMETROS DEL TOE	RANGO	NIVEL DE RIESGO EAL	%
Cumplimiento Ideal	22-21	MUY BAJO	**0.0 – 20**
Cumplimiento Adecuado	20- 16	BAJO	**20 – 40**
Cumplimiento Aceptable	15-11	MEDIO	**41 – 60**
Cumplimiento Regular	10 – 6	ALTO	**61 – 80**
Cumplimiento Critico	5 - 0	MUY ALTO	**81 – 100**

Tabla 3 Rangos de cumplimiento

A partir de esta calificación se plantean recomendaciones necesarias para su mejoramiento en seguridad informática de acuerdo a norma ISO/IEC 15408 Common Criteria.

1.6 Resumen resultados obtenidos

Para aplicar el modelo se seleccionó el producto software Sistema de Información para la Gestión de Activos desarrollado por la empresa Nexura International S.A.S. El cuál es un sistema que es un módulo de un ERP, aplicado a una entidad pública, como la SUPERSALUD. La empresa que evaluará será Password Consulting Services ltda, experta en servicios relacionados con seguridad informática.

Se asignó el ROL de acuerdo al perfil de cada empresa.

NOMBRE	PERFIL ASIGNADO
RTOE	Líder Software Nexura
ETOE	Auditor Password

Tabla 4 ROL con el perfil asignado

El ST (Secure Target) seleccionado fue el “SecureInfo Risk Management System Version 3.2.06.12 Security Target”[24], preparado por COACT Inc.

Los resultados fueron los siguientes

CUMPLIMIENTO PARAMETROS DEL TOE	RANGO	NIVEL DE RIESGO EAL	%	Ubicación TOE Evaluado
Cumplimiento Ideal	22-21	MUY BAJO	**0.0 – 20**	
Cumplimiento Adecuado	20- 16	BAJO	**20 – 40**	TOE
Cumplimiento Aceptable	15-11	MEDIO	**41 – 60**	
Cumplimiento Regular	10 – 6	ALTO	**61 – 80**	
Cumplimiento Critico	5 - 0	MUY ALTO	**81 – 100**	

Tabla 5 Resultados del TOE evaluado

Las recomendaciones en relación a esta evaluación son:

- Especificar Hipótesis del entorno físico y Amenazas, con el fin de prever la protección del hardware y software del TOE antes accesos no autorizados y la ejecución controlada en un ambiente especifico de las diferentes funciones del TOE.

- Planear y ejecutar pruebas de seguridad y análisis de vulnerabilidades, que permitan garantizar un revisión de la seguridad del TOE independiente al desarrollador y determinen cuales son las debilidades que se poseen, con el fin de preparar los ambientes de operación para evitar su explotación.

Con estos resultados se plantea la forma en que se aplica EJECUCIÓN DE PRUEBAS DE SEGURIDAD DE PRODUCTOS SOFTWARE DE ACUERDO A LA ISO/IEC 15408 COMMON CRITERIA.

1.7 Organización del documento

[24] COMMON CRITERIA PORTAL. SecureInfo Risk Management System Version 3.2.06.12 Security Target http://www.commoncriteriaportal.org/files/epfiles/st_vid10042-st.pdf [Citado el 4 de Diciembre 2011]

A continuación se detalla el contenido de cada uno de los capítulos del presente documento.
En el primer capítulo se describe la introducción al documento, la problemática a abordar, los objetivos y el resumen de la estrategia propuesta y los resultados obtenidos.

En el segundo capítulo se encuentra el Marco Teórico, donde se explica que es la norma ISO/IEC 15408 Common Criteria, su origen y la distribución de su estructura en sus tres partes.

En el tercer capítulo, esta la determinación del conjunto de productos software para el análisis de riesgo, de acuerdo a una directriz de selección establecida.

En el cuarto capítulo, se presenta el análisis de riesgo en seguridad informática de los productos software seleccionados, explicando la metodología utilizada, los resultados encontrados por ítem de evaluación y generales.

En el quinto capítulo, está el diseño del modelo para la evaluación de seguridad informático basado en la norma ISO/IEC 15408 Common Criteria, explicando cada uno de sus componentes y directriz de evaluación.

En el sexto capítulo, se encuentra la aplicación del modelo en un producto software específico, detallando las actividades realizadas y los resultados y recomendaciones generadas.

2 MARCO TEORICO

2.1 Definición del ISO/IEC 15408 Common Criteria.

La norma ISO / IEC 15408 Common Criteria para la evaluación de la tecnología de la información regula la evaluación objetiva, repetible y comparable de las propiedades de seguridad de productos y sistemas de información. Generando una declaración de seguridad del producto o sistema evaluado verdadera, la cual procede de una evaluación rigurosa y satisfactoria, generando un alto grado de confianza [3].

2.1.1 Origen

El origen de esta normalización parte desde 1985, en los Estados Unidos donde se desarrollaron los criterios de seguridad recogidos bajo el nombre de TCSEC (Trusted Computer System Evaluation Criteria) y editados en el famoso “libro naranja”. En las décadas posteriores, varios países tomaron como base el TCSEC americano y evolucionaron las especificaciones para hacerlas más flexibles y adaptables a la constante evolución de los sistemas de IT [4].

De ahí la comisión europea, en el año 1.991 publicó el ITSEC (Information Technology Security Evaluation Criteria), desarrollado conjuntamente por Francia, Alemania, Holanda y el Reino Unido. En Canadá, igualmente se desarrollaron en 1.993 los criterios CTCPEC (Canadian Trusted Computer Product Evaluation) uniendo los criterios americanos y europeos. En ese mismo año el Gobierno americano publico los Federal Criteria como una aproximación a unificar los criterios europeos y americanos.

Con la necesidad de estandarizar internacionalmente los criterios de seguridad, la ISO comienza a trabajar a principios de los años 90 dando como resultado la certificación Common Criteria (o ISO-IEC 15408)

Es el resultado de una laboriosa e intensa negociación entre países para obtener un acuerdo de reconocimiento mutuo de las certificaciones de seguridad de productos IT realizadas inicialmente entre un grupo de 14 países.

Figura 6 Evolución de los estándares de Seguridad de IT

Fuente: [3]

2.1.2 Aspectos ajenos a la finalidad.

La norma ISO/IEC 15408 Common Criteria, es de aplicación a las medidas de seguridad de TI implementadas en hardware, firmware o software. En este sentido, algunos aspectos, bien porque involucran técnicas especializadas o bien porque son, de alguna manera, adyacentes a la seguridad de TI, son considerados ajenos a la finalidad de los Criterios Comunes. Entre aspectos claves se pueden destacar los siguientes:

- Criterios de evaluación correspondiente a medidas de seguridad de tipo administrativo o procedimientos relacionadas con la seguridad de TI.

- Aspectos técnicos de la seguridad física como control de radiaciones electromagnéticas.
- No tratan metodologías de evaluación ni el marco administrativo legal.
- Los procedimientos para el uso de los resultados de la evaluación en la acreditación.
- Criterios para la valoración de las cualidades inherentes de los algoritmos criptográficos.

2.1.3 Destinatarios de Criterios Comunes

Existen tres grupos con un interés general por la evaluación de las propiedades de seguridad de los productos o sistemas de TI: usuarios, fabricantes y evaluadores. Los criterios presentados en la norma han sido diseñados para apoyar las necesidades de estos tres grupos:

- Usuarios. Para asegurar que la evaluación satisface sus necesidades al éste el objetivo fundamental y la justificación del proceso de evaluación.
- Fabricantes. La norma pensada para apoyarlos en los procesos de evaluación de sus productos o sistemas y en la identificación de requisitos de seguridad que deben ser satisfechos por cada unos de dichos productos o sistemas.
- Evaluadores. La norma contienen criterios para que los evaluadores emitan veredictos sobre la conformidad del objeto evaluador (TOE) con sus requisitos de seguridad. Aunque los CC no especifican procedimientos a seguir para realizar estas acciones.
- Otros. Oficiales de seguridad, Auditores, Diseñadores de arquitecturas de seguridad, Autoridades de acreditación, Patrocinadores de evaluación y Autoridades de evaluación.

2.1.4 Organización de la norma ISO/IEC 15408 Common Criteria.

La norma se presenta como un conjunto de tres partes distintas pero relacionadas:

1. Parte 1: “Introducción y modelo general”. Define los conceptos generales y principios de la evaluación de seguridad de TI y presenta un modelo general de evaluación. También presenta estructuras para expresar los objetivos de seguridad, para seleccionar y definir los requisitos de seguridad de TI y para escribir las especificaciones de alto nivel de los productos y sistemas. Además, la utilidad de cada parte de los Criterios Comunes se describe para cada tipo de destinatario.
2. Parte 2: “Requisitos funcionales de seguridad”, establece un conjunto de componentes funcionales como una manera estándar de expresar los requisitos funcionales para los TOE. Esta parte cataloga el conjunto de componentes funcionales, familias y clases.
3. Parte 3. “Requisitos de garantía de seguridad”, establece un conjunto de componentes de garantía como una manera estándar de expresar los requisitos de garantía para los TOE. Esta parte cataloga el conjunto de componente de garantía, familias y clases. También define los criterios de evaluación para los Perfiles de Protección (PP) o Declaración de Seguridad (ST).

2.2 Estructuras de requisitos de la norma ISO/IEC 15408 Common Criteria

La norma define las siguientes estructuras de requisitos: TOE, paquete, perfil de protección PP y declaración de seguridad ST.

2.2.1 Target Object Evaluation, Objetivo de Evaluación.

El TOE es un producto o sistema de tecnologías de la información (Por ejemplo medio de almacenamiento electrónico, dispositivos de red, y sistemas operativos) junto a su documentación (manuales) de uso y administración que es objeto de evaluación.

El TOE se define de acuerdo a los siguientes componentes:

- TSP. Políticas de seguridad del TOE (TOE Security Policy). Define las reglas por el cual se accede, gestiona, protege y se distribuyen los recursos, información y servicios controlados por el TOE.
- SFPs. Función de las políticas de seguridad (Security Function Policies). Son las que definen en el TSP. Cada SFP tiene un alcance de control, que define los asuntos, objetos y operaciones.
- SF. La función de seguridad (Security Function SF) implementa la SFP, y son mecanismos que proporcionan las características necesarias de seguridad.
- TSF. Funciones de seguridad del TOE (TSF). El TSF consiste en todo el hardware, software y firmware del TOE que está directamente o indirectamente relacionado con las TSP.
- TSC. Alcance de control del TOE (Scope of Control TSC). La definición de interacciones que pueden ocurrir dentro o por fuera con un TOE y son alcance de las TSP es llamado Alcance de Control del TOE (TSC).
- TSFI. Interfaces de las funciones de seguridad del TOE. Las interfaces por las cuales interactúan los usuarios o aplicaciones, a los recursos (Definidos en las funciones de seguridad TSF) o información, se definen como Interfaces TSF (TSFI).
- Subject. Son las entidades activas del TOE, las cuales son la causa de acciones que ocurren internamente y causan operaciones para ser realizadas sobre la información. Algunos tipos podrían ser:procesos que

actúen desde usuarios autorizados que están definido en los TSF (Procesos UNIX) y procesos internos.

- Object. Esto se definen como las entidades pasivas, que pueden ser los contenedores desde información se origina o a los cuales es almacenada. Puede ser que un object sean los objetivos de operaciones de subjects.
- Atributos de Seguridad (Security Attributes). Atributos necesarios para la definición de las TSP de los usuarios, subject, información y objects.

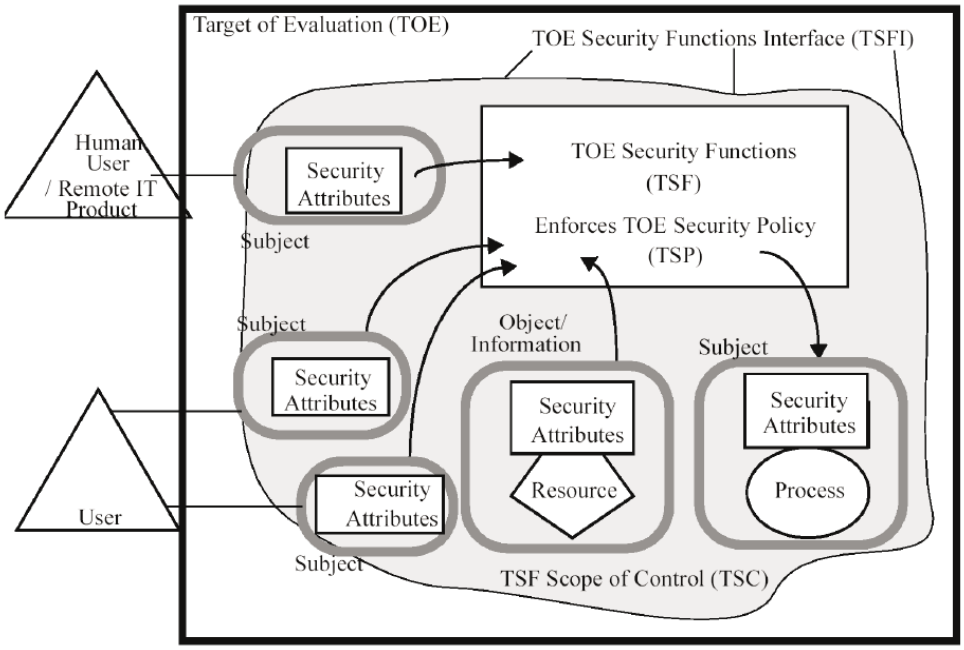


Figura 7 Descripción del TOE

Fuente: [6]

2.2.2 Paquete

Una combinación intermedia de componentes se llama paquete. El paquete permite la expresión de un conjunto de requisitos funcionales o de garantía que cumplen un subconjunto identificable de objetivos de seguridad. Un paquete es reutilizable y define requisitos que se sabe que son útiles y eficaces para cumplir los objetivos establecidos. Un paquete puede usarse en la construcción de paquetes más grandes, PP y ST.

Los niveles de garantía de la evaluación (EAL) son paquetes predefinidos de garantía contenido en la parte 3. Un EAL es conjunto básico de requisitos de garantía para la evaluación. Cada EAL define un conjunto consistente de requisitos de garantía. Juntos, los EAL forman un conjunto ordenado que es la escala de garantía predefinidas de la norma.

2.2.3 Perfil de protección (PP)

El perfil de protección contiene un conjunto de requisitos de seguridad de la norma o declarado explícitamente que debe incluir un EAL.

El perfil de protección permite la expresión, independiente de la implementación, de los requisitos de seguridad para un conjunto de TOE que obedecerán completamente un conjunto de objetivos de seguridad.

Un perfil de protección es reutilizable y define los requisitos del TOE que se sabe son útiles y eficaces para cumplir los objetivos establecidos, tanto para las funciones como para la garantía. Un perfil de protección también, contiene la razón de objetivos de seguridad y requisitos de seguridad.

Un perfil de protección puede desarrollarse por comunidades de usuarios, diseñadores de productos de TI u otras partes interesadas en definir un conjunto común de requisitos. Un perfil de protección da a los consumidores un medio de referirse a un conjunto específico de necesidades de seguridad y facilita la evaluación futura de esas necesidades.

2.2.4 Declaración de seguridad (ST)

Una declaración de seguridad contiene un conjunto de requisitos de seguridad que pueden establecerse por referencia a un perfil de protección, directamente por

referencia a componentes de la norma funcionales o de garantía, o declarada explícitamente.

La declaración de seguridad permite la expresión de requisitos de seguridad para un TOE específico que se demuestran, por la evaluación, útiles y eficaces al cumplir los objetivos establecidos.

Esta también especifica un resumen del TOE, junto con los requisitos y objetivos de seguridad y la razón para cada uno. Una declaración de seguridad es la base para el acuerdo entre todas las partes acerca de qué seguridad ofrece el TOE.

2.2.5 Expresión de los requisitos

Para expresar los requisitos de seguridad de un producto o sistemas de TI, la norma define un conjunto de estructuras que se combinan en grupos significativos de requisitos de seguridad de validez conocida.

Los requisitos se organizan en una jerarquía de “clase” – “familia” – “componente”. Esta organización se proporciona para ayudar a los consumidores a localizar los requisitos específicos de seguridad.

Los requisitos describen el comportamiento de seguridad deseado que se espera de TOE con objeto de satisfacer los objetivos de seguridad expresados en un perfil de protección o en una declaración de seguridad. Estos requisitos describen las propiedades de seguridad que los usuarios pueden detectar con la interacción directa con el TOE (ej. Entradas, salidas) o a través de la respuesta del TOE a estímulos.

La norma presenta los requisitos para aspectos funcionales y de garantía en el mismo estilo general y usa la misma organización y terminología para cada uno [6].

2.2.5.1 Clase.

El termino clase se usa para la agrupación más general de requisitos de seguridad. Todos los miembros de una clase comparten un enfoque común, aunque difieren en la protección de los objetivos de seguridad.

En la norma cada clase funcional se presenta con un nombre de clase, una introducción y una o más familias funcionales.

El nombre de clase da la información necesaria para identificar y catalogar una clase funcional. Cada clase funcional tiene un único nombre. La información consiste en un nombre corto de tres caracteres que se usará en la especificación de los nombres cortos de las familias de cada clase.

La introducción expresa la aproximación común de las familias de la clase para satisfacer los objetivos de seguridad. La definición de la clase funcional no refleja ninguna taxonomía formal en la especificación de los requisitos.

La introducción de una descripción de las familias de la clase y de la jerarquía de los componentes de cada familia. Los miembros de una clase se llaman familias.

2.2.5.2 Familia.

Una familia es una agrupación de conjuntos de requisitos de seguridad que comparten los objetivos de seguridad pero pueden diferir en énfasis o rigor.

Los miembros de una familia son los componentes.

2.2.5.3 Componente

Un componente describe un conjunto específico de requisitos de seguridad y es el conjunto más pequeño de requisitos de seguridad seleccionable para su inclusión en las estructuras definidas en la norma. El conjunto de componentes dentro de una familia puede estar ordenado para representar fortaleza o capacidad creciente de requisitos de seguridad que comparten un propósito común. También puede estar parcialmente ordenado para representar otros conjuntos no relacionados

jerárquicamente. En algunos casos, hay sólo un componente en una familia luego la ordenación no es posible.

Los componentes se construyen con elementos individuales. El elemento es la expresión de requisito de seguridad de más bajo nivel, y es el requisito de seguridad indivisible que puede verificarse en la evaluación.

Por ejemplo, el nombre del requisito, FDP_IFF.4.2 se lee como sigue:

- F = requisito funcional
- DP = clase “protección de datos usuario”
- _IIF = familia “funciones de control del flujo de información”
- .4 = cuarto componente llamado eliminación parcial de flujos de información ilícitos
- .2 = segundo elemento del componente.

2.2.5.4 Clases y familias de requisitos funcionales de seguridad

Clase FAU: Auditoría de seguridad

La auditoría de seguridad implica el reconocimiento, grabación, almacenamiento, y análisis de la información relacionada con las actividades relevantes de seguridad, es decir, actividades controladas por la política de seguridad cuyo cumplimiento debe forzar el TOE (TOE Acurity Policy – TSP). Los archivos de auditoría resultantes pueden examinarse para determinar qué actividades relevantes de seguridad tuvieron lugar y quién (qué usuario) es responsable de ellas.

Clase FCO: Comunicación

Esta clase proporciona dos familias específicamente comprometidas a asegurar la identidad de una de las partes que participa en un intercambio de datos. Estas familias están relacionadas con asegurar la identidad del emisor de la información

transmitida (prueba de origen) y con asegurar la identidad del destinatario de la información transmitida (prueba de recepción). Estas familias aseguran que un emisor no pueda negar haber enviado el mensaje y que un destinatario no pueda negar haberlo recibido.

Clase FCS: Soporte criptográfico

La TSF puede emplear la funcionalidad criptográfica para ayudar a satisfacer varios objetivos de seguridad de alto nivel. Éstos incluyen (pero no se limitan a) identificación y autenticación, no-repudio, camino confiable, canal confiable y separación de datos.

Esta clase se usa cuando el objeto de evaluación (TOE) realiza funciones criptográficas, cuya implementación puede venir en hardware, *firmware* y/o software.

La clase FCS está compuesta de dos familias:FCS_CKM, gestión de claves criptográficas y FCS_COP, operación criptográfica. La familia FCS_CKM se refiere a los aspectos de gestión de claves criptográficas. Mientras la familia FCS_COP se preocupa del uso operativo de esas claves criptográficas.

Clase FDP: Protección de datos de usuario

Esta clase contiene familias que especifican los requisitos para las funciones de seguridad del TOE y las políticas asociadas a éstas relacionadas con la protección de los datos de usuario. La clase FDP se divide en cuatro grupos de familias dirigidas a los datos de usuarios, dentro de un TOE, durante su importación, exportación y almacenamiento, así como a los atributos de seguridad directamente relacionados con dichos datos.

Las familias en esta clase se organizan en cuatro grupos:

- Políticas de las funciones de seguridad de protección de datos de usuario.
- Formas de protección al usuario:

- Almacenamiento, importación y exportación *off-line:*
- Comunicación inter-TSF

Clase FIA: Identificación y autenticación

Las familias de esta clase se dirigen a los requisitos de las funciones que establecen y verifican la identidad reivindicada por un usuario.

La identificación y la autenticación son necesarias para asegurar que los usuarios son asociados con los atributos de seguridad apropiados (por ejemplo, identidad, grupos, roles, niveles de seguridad o e integridad).

La identificación inequívoca de usuarios autorizados y la asociación correcta de los atributos de seguridad con los usuarios y con los sujetos son factores críticos para la aplicación de las políticas de seguridad previstas. Las familias en esta clase tratan de determinar y verificar la identidad de los usuarios, determinado su autorización para interactuar con el TOE y con la asociación correcta de atributos de seguridad para cada usuario autorizado. Otras clases de requisitos (por ejemplo, protección de datos de usuario, auditoría de seguridad) dependen de la identificación correcta y autenticación de los usuarios para ser eficaces.

Clase FMT: Gestión de seguridad

La intención de esta clase es especificar la gestión de varios aspectos de la TSF: atributos de seguridad, datos y funciones. Se pueden especificar los diferentes roles de gestión y su interacción así como la separación de aptitudes.

Esta clase tiene varios objetivos:

La gestión de datos de TSF que incluyen, por ejemplo, mensajes de aviso.

La gestión de atributos de seguridad que incluyen, por ejemplo, las listas de control de acceso y las listas de aptitud.

La gestión de funciones de la TSF que incluye, por ejemplo, la selección de funciones y reglas o condiciones que influyen en el comportamiento de la TSF.

La definición de roles de seguridad.

Clase FPR: Privacidad

Esta clase contiene requisitos de confidencialidad. Estos requisitos proporcionan al usuario protección contra la revelación y el uso indebido de su identidad por parte de otros usuarios.

Clase FPT: Protección de la TSF

Esta clase contiene las familias de requisitos funcionales relacionadas con la integridad y gestión de los mecanismos que proporcionan la TSF (independiente de TSP) y con la integridad de los datos de TSF (independientemente de los contenidos específicos de los datos de TSP). En algún sentido, puede que parezca que las familias de esta clase duplican los componentes de la clase FDP (protección de datos de usuario); incluso pueden implementarse usando los mismos mecanismos. Sin embargo, FDP se entra en la protección de datos de usuario, mientras FPT se centra en la protección de datos de TSF. De hecho, se necesitan componentes de la clase FPT para proporcionar requisitos que las SFP no pueden forzar o desviar en el TOE.

Clase de FRU: Utilización del recurso

Esta clase proporciona tres familias que apoyan la disponibilidad de los recursos necesarios como la capacidad de proceso y/o la capacidad de almacenamiento. La familia tolerancia al fallo proporciona protección contra la disponibilidad de capacidades causadas por el fallo de TOE. La familia prioridad de servicio asegura que los recursos se asignarán a las tareas más importantes o urgentes no pudieron ser monopolizados por las tareas de prioridad menor. La familia

asignación del recurso proporciona límites al uso de los recursos disponibles, evitando, de este modo, que los usuarios los monopolicen.

Clase FTA: Acceso al TOE

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

Clase FTP: Ruta/ canales confiables

Las familias de esta clase proporcionan los requisitos para una ruta de comunicación confiable entre los usuarios y la TFS y para un canal de comunicación confiable entre la TSF y otros productos de TI confiables. Las rutas y canales confiables tienen las siguientes características generales:

- La ruta de comunicaciones se construye usando canales de comunicaciones internos y externos (como sea más apropiado para cada componente) que aíslan a un subconjunto determinado de datos y órdenes de TSF del resto de datos de TSF y de datos de usuario.
- El uso de la ruta de comunicaciones puede iniciarse por el usuario y/o por la TSF (como sea más apropiado para cada componente).

2.2.5.5 Clases y familias de requisitos de garantía de seguridad

Las clases y familias de requisitos de garantía de seguridad así como las abreviaturas de cada familia se muestran en la Tabla 1[3].

Los Criterios Comunes incluyen además una clase específica para los requisitos que tienen por objeto el mantenimiento de la garantía.

Asimismo, y como complemento y apoyo a la evaluación, los Criterios Comunes incluyen una clase de requisitos específicos para la evaluación de los Perfiles de

Protección, y otra clase de requisitos específicos para la evaluación de las declaraciones de seguridad [7].

Clase ACM: Gestión de la configuración

La clase de "gestión de la configuración" sirve para asegurar que se mantiene la integridad del TOE, exigiendo disciplina y control en los procesos de refinamiento y modificación del TOE y de cualquier otra información relacionada. La gestión de la configuración impide modificaciones, inclusiones o eliminaciones no autorizadas el TOE, garantizando así que el TOE y la documentación usados para la evaluación son los preparados para la distribución.

Clase ADO: Distribución y operación

La clase de garantía ADO define los requisitos para las medidas, procedimientos y normas relacionadas con la distribución, instalación y uso operacional seguros del TOE, asegurando que la protección de seguridad ofrecida por el TOE no se ve comprometida durante el traslado, instalación, arranque ni funcionamiento del mismo.

CLASE DE GARANTÍA	FAMILIA DE GARANTÍA	ABREVIATURA
ACM-Gestión de la configuración	Automatización	ACM_AUT
	Capacidades	ACM_CAP
	Alcance	ACM_SCP
ADO-Distribución y operación	Distribución	ADO_DEL
	Instalación, generación y puesta en marcha	ADO_IGS
ADV-Desarrollo	Especificación funcional	ADV_FSP
	Diseño de alto nivel	ADV_HLD
	Representación de la implementación	ADV_IMP
	TSF internos	ADV_INT
	Diseño de bajo nivel	ADV_LLD
	Correspondencia de la representación	ADV_RCR
	Modelo de política de seguridad	ADV_SPM
AGD-Manuales	Manuales de administrador	AGD_ADM
	Manuales de usuario	AGD_USR
ALC-Apoyo al ciclo de vida	Seguridad del desarrollo	ALC_DVS
	Resolución de fallos	ALC_FLR
	Definición de ciclo de vida	ALC_LCD

	Herramientas y técnicas	ALC_TAT
ATE-Pruebas	Cobertura	ATE_COV
	Profundidad	ATE_DPT
	Pruebas funcionales	ATE_FUN
	Pruebas independientes	ATE_IND
AVA-Evaluación de vulnerabilidades	Análisis de canales encubiertos	AVA_CCA
	Mal uso	AVA_MSU
	Fortaleza de las TSF	AVA_SOF
	Análisis de vulnerabilidades	AVA_VLA

Tabla 6 Clases y familias con sus abreviaturas

Clase ADV: Desarrollo

La clase de garantía ADV define los requisitos para el refinamiento, por etapas, de la TSF a partir de la especificación resumen del TOE de la declaración de seguridad hasta la implementación final. Cada una de las representaciones de TSF resultantes proporciona información para ayudar el evaluador a determinar si se han reunido los requisitos funcionales del TOE.

Clase AGD: Manuales

La clase de garantía AGD define requisitos dirigidos a los comprensión, a la cobertura y a la integridad de la documentación operacional proporcionada por el fabricante. Esta documentación que proporciona dos categorías de información, para los usuarios y para los administradores, es un factor importante en el funcionamiento seguro del objetivo de evaluación (TOE).

Clase ALC: Apoyo al ciclo de vida

La clase de garantía ALC define los requisitos de garantía a través de la adopción de un modelo de ciclo de vida bien definido para todos los pasos del desarrollo del objeto de evaluación (TOE), incluyendo los procedimientos y políticas de

resolución de fallos, el uso correcto de herramientas y técnicas y las medidas de seguridad utilizadas para proteger el entorno de desarrollo.

Clase ATE: Pruebas

La clase de garantía ATE establece los requisitos de las pruebas que demuestren que la TSF satisface los requisitos funcionales de seguridad del objeto de evaluación (TOE).

Clase AVA: Evaluación de vulnerabilidad

La clase de garantía AVA define los requisitos dirigidos a la identificación de las vulnerabilidades explotables. Específicamente, se ocupa de aquellas vulnerabilidades introducidas en la construcción, operación, mal uso configuración incorrecta del objeto de evaluación (TOE).

Clase AMA: Mantenimiento de garantía

La clase de garantía AMA pretende mantener el nivel de garantía de que el objeto de evaluación (TOE) continuará cumpliendo su declaración de seguridad conforme se vayan haciendo cambios en el TOE o en su entorno. Cada una de las familias de esta clase identifica las acciones que el fabricante y el evaluador deberán realizar después de que el TOE haya sido evaluado con éxito, aunque algunos requisitos pueden aplicarse en el momento de la evaluación.

2.3 Evaluación

La garantía es la base para confiar en que un producto o sistema de TI cumple sus objetivos de seguridad. La garantía puede derivarse de la referencia a fuentes como afirmaciones sin confirmar, previas a la experiencia, o de la propia

experiencia. Sin embargo, la ISO/IEC 15408 Common Criteria proporciona garantía a través de la investigación activa que implica una evaluación del producto o sistema de TI para determinar sus propiedades de seguridad [7].

La evaluación ha sido el medio tradicional de dar garantía y es la base del enfoque de la ISO/IEC 15408 Common Criteria. Las técnicas de evaluación pueden incluir, pero no se limitan a:

- El análisis y verificación de procesos y procedimientos.
- La verificación de que los procesos y los procedimientos están siendo aplicados.
- El análisis de la correspondencia entre las representaciones del objeto de evaluación (TOE).
- El análisis de la representación de diseño del objeto de evaluación (TOE) frente a los requisitos.
- La comprobación de las pruebas
- El análisis de los manuales
- El análisis de las pruebas funcionales desarrolladas y los resultados proporcionados
- Pruebas funcionales independientes
- El análisis de vulnerabilidades (incluyendo hipótesis de fallo)
- Test de penetración.

2.3.1 La escala de garantía de evaluación de los criterios comunes

La filosofía de los Criterios Comunes afirma que se consigue mayor garantía al aplicar un mayor esfuerzo en la evaluación y que el objetivo es aplicar el mínimo esfuerzo necesario para proporcionar el nivel de garantía requerido. El nivel creciente de esfuerzo está basado en:

- El alcance, es decir, el esfuerzo es mayor cuando se incluye una parte mayor del producto o sistema TI.
- La profundidad, es decir, el esfuerzo es mayor cuando se despliega hasta un nivel más fino del diseño y del detalle de la implementación.
- El rigor, es decir, el esfuerzo es mayor cuando es aplicado de una manera más estructurada y formal.

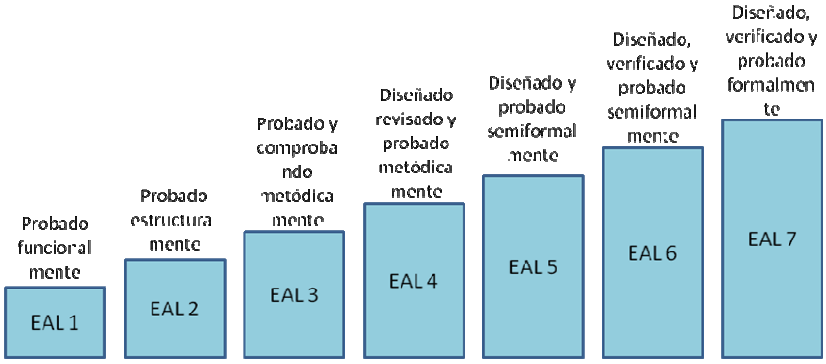


Figura 8 Escala de garantía de evaluación de los criterios comunes

Fuente: [3]

2.3.2 Evaluación del perfil de protección

La evaluación de un perfil de protección se lleva a cabo con los criterios de evaluación para PP contenidos en la parte 3 de la norma. La meta de esta evaluación es demostrar que el perfil de protección es completo, consistente, técnicamente sólido y conveniente para su uso como una declaración de requisitos para un TOE evaluable.

2.3.3 Evaluación de la declaración de seguridad

La evaluación de la declaración de seguridad para el TOE se lleva a cabo con los criterios de evaluación para ST contenido en la parte 3 de la norma. La meta de esta evaluación es doble: primero para demostrar que la declaración de seguridad es completa, consistente, técnicamente sólida y conveniente para su uso como base para la evaluación del TOE correspondiente; segundo, cuando una

declaración de seguridad afirma (o exige) su conformidad con un perfil de protección, para demostrar que la declaración de seguridad reúne apropiadamente los requisitos del perfil de protección.

2.3.4 Evaluación del TOE

La evaluación del objeto de evaluación (TOE) se lleva a cabo con los criterios de evaluación contenidos en la parte 3 usando una declaración de seguridad evaluada como base. La meta de esta evaluación es demostrar que el TOE reúne los requisitos de seguridad contenidos en la declaración de seguridad.

2.3.5 Resultados de evaluación

La evaluación debe conseguir resultados objetivos y repetibles que puedan citarse como pruebas, aun cuando no haya ninguna escala totalmente objetiva para representar los resultados de una evaluación de seguridad TI.

La existencia de un conjunto de criterios de evaluación es una precondición necesaria para que la evaluación llegue a un resultado significativo y proporcione una base técnica para el reconocimiento mutuo de resultados de evaluación entre autoridades de evaluación. Pero hay que advertir que la aplicación de los criterios contiene tanto elementos objetivos como subjetivos, por eso no son factibles evaluaciones precisas y universales para la seguridad de TI.

Una evaluación realizada en relación con la ISO/IEC 15408 Common Criteria representa los resultados de un tipo específico de investigación de las propiedades de seguridad de un TOE. Esta evaluación no garantiza la aptitud para su uso en cualquier entorno particular de aplicación específico está basado en la consideración de muchos aspectos de seguridad además de los resultados de la evaluación.

2.3.6 Resultados de la evaluación de un perfil de protección

Los Criterios Comunes definen un conjunto de criterios de seguridad de TI que pueden dirigirse a las necesidades de muchos colectivos. La ISO/IEC 15408 Common Criteria se ha desarrollado alrededor de la noción central de que el uso de los componentes funcionales de seguridad contenidos en la parte 2, y los niveles de garantía de evaluación EAL, y componentes de garantía contenidos en la parte 3, representan la forma de proceder preferida para a expresión de requisitos TOE en los perfiles de protección y en las declaraciones de seguridad, ya que representan un dominio muy conocido y entendido.

Sin embargo la propia norma reconoce la posibilidad de que se necesiten requisitos funcionales y de garantía no incluidos en los catálogos proporcionados, para establecer un conjunto completo de requisitos de seguridad de TI.

En este caso, la norma establece lo siguiente para la inclusión de estos requisitos funcionales o de garantía adicionales:

- Cualquier requisito funcional o de garantía adicional incluido en un perfil de protección o en una declaración de seguridad será clara e inequívocamente expresado de forma que la evaluación y la demostración de conformidad sean factibles. El nivel de detalle y manera de expresión de los componentes funcionales o de garantía existentes en la ISO/IEC 15408 Common Criteria se usarán como modelo.

- Se advertirá expresamente de los resultados de la evaluación obtenidos usando requisitos funcionales o de garantía adicionales.

- La incorporación de requisitos funcionales o de garantía en un perfil de protección o en una declaración de seguridad serán conformes a las clases APE o ASE de la parte 3, según el caso.

Con todo ello, la ISO/IEC 15408 Common Criteria contienen los criterios de evaluación que permiten a un evaluador declarar si un perfil de protección es

completo, consistente, técnicamente sólido y, por tanto, conveniente para su uso como una declaración de requisitos para un TOE evaluable.

La evaluación de un perfil de protección producirá una declaración de apto/ no-apto. Un perfil de protección para el que la evaluación produce una declaración de apto será elegible para su inclusión dentro de un registro de perfiles de protección.

2.3.7 Resultados de la evaluación del TOE

La ISO/IEC 15408 Common Criteria contiene los criterios de evaluación que permiten a un evaluador determinar si el objeto de evaluación (TOE) satisface los requisitos de seguridad expresados en la declaración de seguridad. Usando la ISO/IEC 15408 Common Criteria en la evaluación del TOE, el evaluador puede hacer declaraciones acerca de:

Si las funciones de seguridad del TOE especificadas reúnen los requisitos funcionales y son, por tanto, eficaces para cumplir los objetivos de seguridad del TOE.

Si las funciones de seguridad del TOE especificadas están correctamente implementadas.

Los requisitos de seguridad expresados en la ISO/IEC 15408 Common Criteria definen el dominio de trabajo conocido de aplicación de los criterios de evaluación de seguridad de TI. Un TOE con los requisitos de seguridad expresados sólo en forma de requisitos funcionales y de garantía deducidos de la ISO/IEC 15408 Common Criteria será evaluable con la ISO/IEC 15408 Common Criteria.

Sin embargo, puede existir la necesidad para un TOE en particular de reunir requisitos de seguridad no expresados directamente en la ISO/IEC 15408 Common Criteria. La norma reconoce la necesidad de evaluar este tipo de TOE pero, como los requisitos adicionales quedan fuera del dominio conocido de aplicación de la ISO/IEC 15408 Common Criteria, se debe advertir apropiadamente de esta circunstancia en los resultados de esta evaluación.

Los resultados de la evaluación de un objeto de evaluación (TOE) incluyen una declaración de conformidad con la norma ISO 15408 Criterios Comunes. El uso de términos de la ISO/IEC 15408 Common Criteria para describir la seguridad de un TOE permite la comparación de las características de seguridad de los TOE en general.

El resultado de la evaluación TOE es, por tanto, una declaración que describe hasta qué punto se puede confiar en el TOE para cumplir los requisitos. La evaluación del TOE producirá una declaración de apto/no-apto. Un TOE cuya evaluación produce una declaración de apto será elegible para su inclusión dentro de un registro de TOE evaluados.

2.4 Producto Final del proceso de Certificación

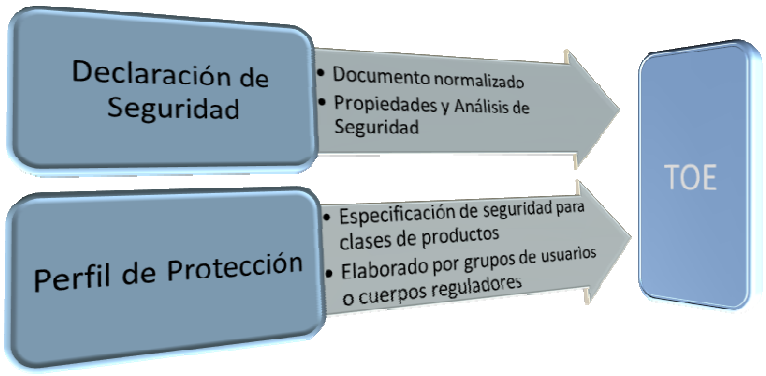


Figura 9 Producto final de certificación del TOE

Al finalizar el proceso de certificación se debe generar un documento llamado Declaración de Seguridad, el cuál es un documento con un contenido normalizado, que refleja el análisis y propiedades de seguridad del objeto a evaluar, relacionado con el cumplimiento de un Perfil de Protección (PP), el cuál es una especificación

de seguridad aplicable a una clase de productos con objetivos de seguridad comunes. Elaborados por grupos de usuarios o cuerpos reguladores.

Tomando como ejemplo la Declaración de Seguridad de ADVANTIS CRYPTO 3.1 Versión 1.2[25], el contenido tipo es el siguiente:

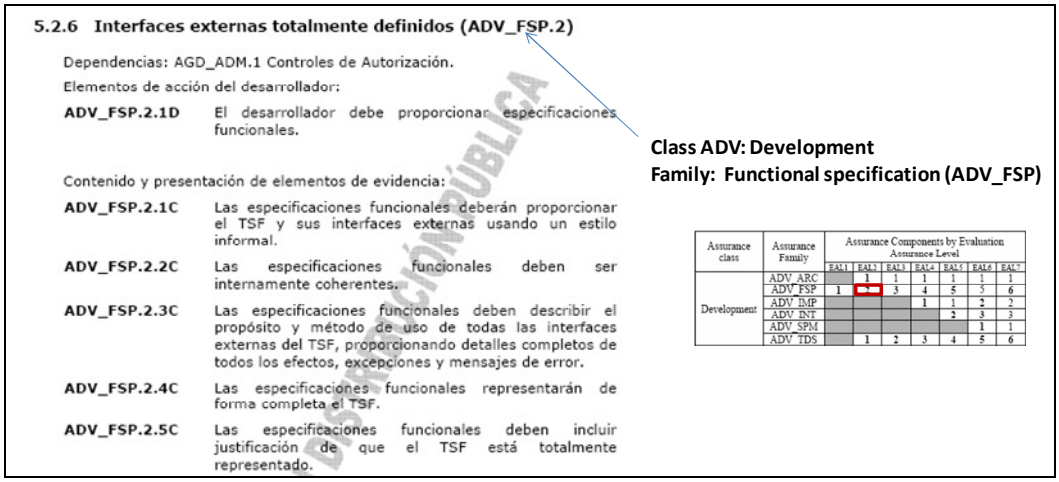
- Introducción
- Descripción del producto a evaluar
- Entorno de seguridad
- Objetivos de seguridad
- Requisitos de seguridad
  - Funciones de seguridad
  - Requisitos de garantía
- Síntesis de la especificación del producto
- Cumplimiento perfiles de protección
  - CAWA14169
- Justificaciones
- Acrónimos
- Referencias

La Descripción en términos generales describe el siguiente alcance:
"Esta declaración de seguridad cumple con los requisitos de la norma CC versión 2.3, partes 2 y 3, y define un nivel de garantía de evaluación EAL4, aumentado por los componentes Análisis y pruebas sobre los estados inseguros (AVA_MSU.3) y Alta resistencia (AVA_VLA.4)*" "La selección del nivel de evaluación se justifica por la necesidad de garantía de las propiedades de seguridad del producto, que vienen fijadas por CWA 14169:2004. Protection Profile – Secure Signature-Creation Device, Type 3, version 1.05 (Perfil de Protección - Dispositivo Seguro de

[25] COMMON CRITERIA PORTAL. Advantis Crypto 3.1 Declaración de seguridad versión pública Versión: 1.2 18/08/2008. http://www.commoncriteriaportal.org/files/epfiles/2006-01-DS.pdf [Citado el 4 de Diciembre 2011]

Creación de Firma) y que determina un producto altamente resistente a diferentes ataques."[8]

Uno de sus apartes relacionados con la estructura del Common Criteria es el siguiente:



5.2.6 Interfaces externas totalmente definidos (ADV_FSP.2)

Dependencias: AGD_ADM.1 Controles de Autorización.

Elementos de acción del desarrollador:

ADV_FSP.2.1D El desarrollador debe proporcionar especificaciones funcionales.

Contenido y presentación de elementos de evidencia:

ADV_FSP.2.1C Las especificaciones funcionales deberán proporcionar el TSF y sus interfaces externas usando un estilo informal.

ADV_FSP.2.2C Las especificaciones funcionales deben ser internamente coherentes.

ADV_FSP.2.3C Las especificaciones funcionales deben describir el propósito y método de uso de todas las interfaces externas del TSF, proporcionando detalles completos de todos los efectos, excepciones y mensajes de error.

ADV_FSP.2.4C Las especificaciones funcionales representarán de forma completa el TSF.

ADV_FSP.2.5C Las especificaciones funcionales deben incluir justificación de que el TSF está totalmente representado.

Class ADV: Development
Family: Functional specification (ADV_FSP)

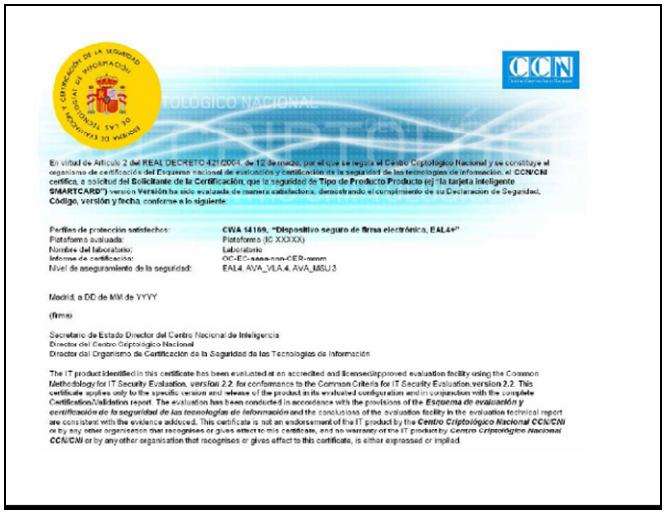
Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6

Figura 10 Apartes de la declaración de seguridad del Advantis Crypto 3.1

Fuente: [5]

En donde la clase en Desarrollo (ADV) y la familia Especificaciones Funcionales.

La certificación dada por un ente certificador como el Centro de Certificación Nacional de España (CCN) en Common Criteria es el siguiente:



En virtud de Artículo 2 del REAL DECRETO 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional y se constituye el organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, el **CCN/CNI certifica**, a solicitud del **Solicitante de la Certificación**, que la seguridad de **Tipo de Producto Producto [c]** "la tarjeta inteligente **SMARTCARD**") versión **Versión** ha sido evaluada de manera satisfactoria, demostrando el cumplimiento de su Declaración de Seguridad, **Código, versión y fecha**, conforme a lo siguiente:

Perfiles de protección satisfechos:	**CWA 14169, "Dispositivo seguro de firma electrónica, EAL4+"**
Plataforma evaluada:	Plataforma (IC XXXXX)
Nombre del laboratorio:	Laboratorio
Informe de certificación:	OC-EC-aaa-aaa-CER-aaaa
Nivel de aseguramiento de la seguridad:	EAL4 AVA_VLA.4 AVA_MSU.3

Madrid, a DD de MM de YYYY

(firma)

Secretario de Estado Director del Centro Nacional de Inteligencia
Directa del Centro Criptológico Nacional
Directa del Organismo de Certificación de la Seguridad de las Tecnologías de Información

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation, version 2.2, for conformance to the Common Criteria for IT Security Evaluation, version 2.2. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification/Validation report. The evaluation has been conducted in accordance with the provisions of the *Esquema de evaluación y certificación de la seguridad de las tecnologías de información* and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by the *Centro Criptológico Nacional CCN/CNI* or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by *Centro Criptológico Nacional CCN/CNI* or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Figura 11 Certificación del CCN para el producto Advantis Crypto, versión 3.1

Fuente: [5]

Este es el objetivo a largo plazo para las TICs desarrolladas en Colombia.

3 DETERMINACION DE UN CONJUNTO DE PRODUCTOS SOFTWARE A LOS QUE SE LES PUEDE APLICAR LA EVALUACIÓN EN SEGURIDAD INFORMÁTICA BASADAS EN LA ISO/IEC 15408 COMMON CRITERIA

3.1 Directrices de determinación

Para Colombia las directrices que se asumirán para la determinación de los conjuntos de productos software serán las siguientes:

- Requerimientos de ley. De acuerdo a la normatividad legal colombiana, estas son las resoluciones o decretos que se exigen seguridad de la información:
    - Para el sector financiero la Superintendencia Financiera de Colombia, publicó la Circular Externa 052 de 2007 "Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios". Con el cuál le exige a todas sus entidades reguladas, una serie de requerimientos mínimos para sus transacciones y procesos.[26]
    - Para el sector salud, el Ministerio de Salud publico la resolución número 1995 de 1999 (Julio 8) por la cual se establecen normas para el manejo de la Historia Clínica, donde el componente de seguridad es fundamental.[27]
    - En el sector Gobierno presenta el "Manual para la implementación de la Estrategia de Gobierno En Línea" el cuál determina los

[26] SUPERINTENDENCIA DE SALUD. Resolución 052 de 2007. http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce052_07.rtf [Citado el 13 de Noviembre 2011]

[27] MINISTERIO DE SALUD. Resolución 1995 de 1997. http://www.minproteccionsocial.gov.co/Normatividad/RESOLUCI%C3%93N%201995%20DE%201999.pdf [Citado el 13 de Noviembre 2011]

lineamientos para cumplir con lo establecido en el Decreto 1151 del 14 de abril de 2008, en todas las entidades públicas, y presenta la Seguridad de la Información como algún indispensable en cada una de sus cinco fases.[28]

- Entrevistas con entidades a los sectores con exigencias legales en seguridad de la información, en donde se identifique cuales son los software que deben tener un nivel de seguridad critico y a los cuáles se puede y debe aplicar pruebas en la ISO/IEC 15408 Common Criteria. Las preguntas fueron las siguientes:
    - ¿Cuál es el sistema de información software más crítico de la entidad?
    - ¿Cuál es su objetivo general?
    - ¿En qué lenguaje esta desarrollado?
    - ¿En qué motor de base de datos esta implementado?

3.2Identificación de las empresas con sus software respectivos

La selección de las empresas de acuerdo a los sectores identificados, se realizó debido a la relación comercial y laboral que se tiene con anterioridad con ellas.

SECTOR	EMPRESA	SOFTWARE
Público	Ideam	Sistema de Información Ambiental
Público	Ministerio de Transporte	Sistema de Gestión Documental
Público	Gobernación del Cauca	ERP
Público	Alcaldía de Santiago de Cali	ERP
Salud	Servicio de Salud Inmediato	ERP
Salud	Hospital del Sur Bogotá	Sistema de Historias

[28] GOBIERNO EN LINEA. Manual para la implementación de la estrategia de Gobierno en Línea. http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ManualGEL2008.pdf [Citado el 13 de Noviembre 2011]

	D.C	clínicas
Salud	Asmet Salud	ERP
Salud	Clínica Comfacauca	Sistema de Historias Clínicas
Financiero	Banco de Occidente	ERP
Financiero	Coomeva	ERP
Financiero	Supergiros	Sistema de Giros y Envíos
Financiero	Macrofinanciera	ERP

Tabla 7 Empresas seleccionadas con su software identificado

El sistema de información con mayor selección fue el ERP (Enterprise Resource Planning), debido a la importancia en los procesos de negocio de cada entidad.

Las fichas técnicas de los encuestados están en el Anexo, es de anotar que los detalles de cada encuesta no serán publicados en este documento por acuerdos de confidencialidad con las entidades. Solo serán publicados los resultados generales. Se anexo formato de acuerdo de confidencialidad que se diligencio con las entidades.

4 ANÁLISIS DE RIESGO EN SEGURIDAD INFORMÁTICA A LOS PRODUCTOS SOFTWARE ESTABLECIDOS SIGUIENDO EL COMMON CRITERIA

4.1 Análisis de riesgo en seguridad informática al software de cada empresa.

4.1.1 Criterios de evaluación

Los criterios de evaluación para el análisis de riesgo a los sistemas software a analizar se basaron en los 2 niveles de seguridad del ISO/IEC 15408-3 Common Criteria EAL1 – Probado funcionalmente y EAL2 – Probado estructuralmente, en su controles agremiados en las clases Administración de la configuración, Entrega y funcionamiento, Desarrollo, Documentos Guía, Pruebas y Evaluación de la vulnerabilidad, aplicados de la siguiente manera:

CLASES DE ASEGURAMIENTO	FAMILIA DE ASEGURAMIENTO	Componentes EAL1	Componentes EAL2
Administración de la configuración	ACM_AUT		
	ACM_CAP	1	2
	ACM_SCP		
Entrega y funcionamiento	ADO_DEL		1
	ADO_IGS	1	1
Desarrollo	ADV_FSP	1	1
	ADV_HLD		1
	ADV_IMP		
	ADV_INT		
	ADV_LLD		
	ADV_RCR	1	1
	ADV_SPM		
Documentos Guia	AGD_ADM	1	1
	AGD_USR	1	1
Pruebas	ATE_COV		1
	ATE_DPT		
	ATE_FUN		1

	ATE_IND	1	2
Evaluación de la vulnerabilidad	AVA_CCA		
	AVA_MSU		
	AVA_SOFT		1
	AVA_VLA		1

Tabla 8 Distribución de los componentes de acuerdo al EAL1 y EAL2

A cada componente se le formuló una pregunta que indaga sobre el cumplimiento de los requisitos del TOE bajo evaluación. Basado en los resultados obtenidos de estas preguntas se genero un nivel de riesgo en seguridad, asociado a dicho TOE. Las preguntas identificadas para cada componente son las siguientes:

	COMPONENTES	**CLASE ADMINISTRACIÓN DE LA CONFIGURACIÓN**
EAL1	ACM_CAP.1.1D	El desarrollador presentó una referencia para el TOE
	ACM_CAP.1.1C	La referencia para el TOE es única para cada versión
	ACM_CAP.1.2C	El TOE es etiquetado con su referencia.
	ACM_CAP.1.1E	El evaluador confirma que la información suministrada reúne todos los requerimientos para contenido y presentación de evidencia.
EAL2	ACM_CAP.2.1D	El desarrollador provee una referencia para el TOE.
	ACM_CAP.2.2D	El desarrollador usa un sistema de administración de configuración.
	ACM_CAP.2.3D	El desarrollador provee documentación del administrador de configuración.
	ACM_CAP.2.1C	La referencia para el TOE es única para cada versión.
	ACM_CAP.2.2C	El TOE es etiquetado con su referencia.
	ACM_CAP.2.3C	La documentación del administrador de configuración incluye una lista de configuración.
	ACM_CAP.2.4C	La lista de configuración identifica únicamente todos los ítems de configuración que abarca el TOE.
	ACM_CAP.2.5C	La lista de configuración describe los ítems de configuración que abarca el TOE.
	ACM_CAP.2.6C	La documentación del administrador de configuración describe el método utilizado para identificar únicamente los ítems de configuración.
	ACM_CAP.2.7C	El sistema de administrador de configuración identifica únicamente todos los ítems de configuración.
	ACM_CAP.2.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	COMPONENTES	**CLASE ENTREGA Y FUNCIONAMIENTO**
EAL1	ADO_IGS.1.1D	El desarrollador documenta los procedimientos necesarios para la instalación segura, generación y puesta en marcha del TOE.
	ADO_IGS.1.1C	La documentación indica los pasos necesarios para garantizar la instalación, generación y puesta en marcha del TOE.
	ADO_IGS.1.1E	El evaluador confirma que la información proporcionada cumple con todos los requisitos de contenido y la presentación de pruebas.

	ADO_IGS.1.2E	El evaluador determina que los procedimientos de instalación, generación y puesta en marcha son resultado de una configuración segura.
EAL2	ADO_DEL.1.1D	El desarrollador documenta los procedimientos de entrega del TOE ó partes de este al usuario al usuario.
	ADO_DEL.1.2D	El desarrollador utiliza los procedimientos de entrega.
	ADO_DEL.1.1C	La documentación entregada describe todos los procedimientos necesarios para mantener la seguridad cuando se distribuyen versiones del TOE a los usuarios.
	ADO_DEL.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	ADO_IGS.1.1D	El desarrollador provee una referencia para el TOE.
	ADO_IGS.1.1C	La referencia para el TOE es única para cada versión.
	ADO_IGS.1.1E	El TOE es etiquetado con su referencia.
	ADO_IGS.1.2E	El evaluador determina que los procedimientos de instalación, generación y puesta en marcha son resultado de una configuración segura.
	COMPONENTES	**CLASE DESARROLLO**
EAL1	ADV_FSP.1.1D	El desarrollador provee una especificación funcional.
	ADV_FSP.1.1C	La especificación funcional describe el TSF y sus interfaces externas usando un lenguaje informal.
	ADV_FSP.1.2C	La especificación funcional es consistente internamente.
	ADV_FSP.1.3C	La especificación funcional describe el propósito y método de uso de todas las interfaces externas TSF, proveer detalles de los efectos, excepciones y mensajes de error.
	ADV_FSP.1.4C	La especificación funcional representa completamente la TSF.
	ADV_FSP.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	ADV_FSP.1.2E	El evaluador determina que la especificación funcional sea una exacta y completa instanciación de los requisitos funcionales de seguridad del TOE.
	ADV_RCR.1.1D	El desarrollador presenta un análisis de la correspondencia entre todos los pares adyacentes de representaciones de TSF que se ofrece.
	ADV_RCR.1.1C	Para cada par adyacente de representaciones TSF entregadas, el análisis demuestra que toda la funcionalidad de seguridad relevante de la representación TSF más abstracta está correctamente y completamente refinada en la representación TSF menos abstracta.
	ADV_RCR.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
EAL2	ADV_FSP.1.1D	El desarrolador provee una especificación funcional.
	ADV_FSP.1.1C	La especificación funcional describe el TSF y sus interfaces externas usando un estilo informal.
	ADV_FSP.1.2C	La especificación funcional es internamente consistente.
	ADV_FSP.1.3C	La especificación funcional describe el objetivo y el método de uso de todas las interfaces externas de TSF, se facilitan detalles de los efectos, las excepciones y mensajes de error.
	ADV_FSP.1.4C	La especificación funcional representa completamente la TSF.
	ADV_FSP.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.

	ADV_FSP.1.2E	El evaluador determina que la especificación funcional sea una exacta y completa instanciación de los requisitos funcionales de seguridad del TOE.
	ADV_RCR.1.1D	El desarrollador presenta un análisis de la correspondencia entre todos los pares adyacentes de representaciones de TSF que se ofrece.
	ADV_RCR.1.1C	Para cada par adyacente de representaciones TSF entregadas, el análisis demuestra que toda la funcionalidad de seguridad relevante de la representación TSF más abstracta está correctamente y completamente refinada en la representación TSF menos abstracta.
	ADV_RCR.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	ADV_HLD.1.1D	El desarrollador entrega el diseño de alto nivel de la TSF.
	ADV_HLD.1.1C	La presentación del diseño de alto nivel es informal.
	ADV_HLD.1.2C	El diseño de alto nivel es internamente consistente.
	ADV_HLD.1.3C	El diseño de alto nivel describe la estructura de la TSF en términos de subsistemas.
	ADV_HLD.1.4C	El diseño de alto nivel describe la funcionalidad de seguridad suministrada por cada subsistema de la TSF.
	ADV_HLD.1.5C	El diseño de alto nivel debe identificar cualquier tipo de software requerido por la TSF, con una presentación de las funciones que ofrece el soporte a los mecanismos de protección aplicados en ese software.
	ADV_HLD.1.6C	El diseño de alto nivel identifica todas las interfaces para los subsistemas de la TSF.
	ADV_HLD.1.7C	El diseño de alto nivel identifica cuál de las interfaces para los subsistemas de las TSF son visibles externamente.
	ADV_HLD.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	ADV_HLD.1.2E	El evaluador determina que el diseño de alto nivel sea una exacta y completa instanciación de los requisitos funcionales de seguridad del TOE.
	COMPONENTES	**CLASE DOCUMENTOS GUIA**
EAL1	AGD_ADM.1.1D	El desarrollador proporciona la guía del administrador dirigida al personal administrativo del sistema.
	AGD_ADM.1.1C	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE.
	AGD_ADM.1.2C	La guía del administrador describe cómo administrar el TOE de una manera segura.
	AGD_ADM.1.3C	La guía del administrador contiene advertencias acerca de las funciones y privilegios que deben ser controlados en un ambiente seguro de procesamiento.
	AGD_ADM.1.4C	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son relevantes para el funcionamiento seguro del TOE.
	AGD_ADM.1.5C	La guía del administrador describe todos los parámetros de seguridad bajo el control del administrador, indicando los valores de seguridad apropiados.
	AGD_ADM.1.6C	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF.
	AGD_ADM.1.7C	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación.
	AGD_ADM.1.8C	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de

		tecnología de la información.
	AGD_ADM.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	AGD_USR.1.1D	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE.
	AGD_USR.1.1C	La guía del administrador describe cómo administrar el TOE de forma segura.
	AGD_USR.1.2C	La guía del administrador contiene advertencias acerca de funciones y privilegios que deben ser controladas en un ambiente de procesamiento seguro.
	AGD_USR.1.3C	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son relevantes para el funcionamiento seguro del TOE.
	AGD_USR.1.4C	La guía del administrador describe todos los parámetros bajo el control del administrador indicando los valores seguros apropiados.
	AGD_USR.1.5C	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF.
	AGD_USR.1.6C	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación.
	AGD_USR.1.1E	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de tecnología de la información que son relevantes al administrador.
EAL2	AGD_ADM.1.1D	El desarrollador proporciona la guía del administrador dirigida al personal administrativo del sistema.
	AGD_ADM.1.1C	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE.
	AGD_ADM.1.2C	La guía del administrador describe cómo administrar el TOE de forma segura.
	AGD_ADM.1.3C	La guía del administrador contiene advertencias acerca de las funciones y privilegios que deben ser controlados en un ambiente seguro de procesamiento.
	AGD_ADM.1.4C	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son relevantes para el funcionamiento seguro del TOE.
	AGD_ADM.1.5C	La guía del administrador describe todos los parámetros de seguridad bajo el control del administrador, indicando los valores de seguridad apropiados.
	AGD_ADM.1.6C	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF.
	AGD_ADM.1.7C	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación.
	AGD_ADM.1.8C	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de tecnología de la información.
	AGD_ADM.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	AGD_USR.1.1D	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE.
	AGD_USR.1.1C	La guía del administrador describe cómo administrar el TOE de forma segura.

	AGD_USR.1.2C	La guía del administrador contiene advertencias acerca de funciones y privilegios que deben ser controladas en un ambiente de procesamiento seguro.
	AGD_USR.1.3C	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son relevantes para el funcionamiento seguro del TOE.
	AGD_USR.1.4C	La guía del administrador describe todos los parámetros bajo el control del administrador indicando los valores seguros apropiados.
	AGD_USR.1.5C	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF.
	AGD_USR.1.6C	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación.
	AGD_USR.1.1E	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de tecnología de la información que son relevantes al administrador.
	COMPONENTES	**CLASE PRUEBAS**
EAL1	ATE_IND.1.1D	El desarrollador provee el TOE para pruebas.
	ATE_IND.1.1C	El TOE se adecua para pruebas
	ATE_IND.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	ATE_IND.1.2E	El evaluador prueba un subconjunto de la TSF apropiadamente para confirmar que el TOE funciona como se especificó.
EAL2	ATE_COV.1.1D	El desarrollador provee evidencia del cubrimiento de la prueba.
	ATE_COV.1.1C	La evidencia del cubrimiento de la prueba muestra la correspondencia entre las pruebas identificadas en la documentación de pruebas y la TSF descrita en la especificación funcional.
	ATE_COV.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	ATE_FUN.1.1D	El desarrollador prueba el TSF y documenta los resultados.
	ATE_FUN.1.2D	El desarrollador provee la documentación de pruebas.
	ATE_FUN.1.1C	La documentación de pruebas consiste en planes de pruebas, descripción de los procedimientos de pruebas, resultados esperados de la prueba y resultados actuales de la prueba.
	ATE_FUN.1.2C	Los planes de prueba identifican las funciones de seguridad para ser probadas y describe las metas de las pruebas a desarrollar.
	ATE_FUN.1.3C	Las descripciones del procedimiento de prueba identifican las pruebas a desarrollarse y describe los escenarios para probar cada función de seguridad. Estos escenarios incluyen cualquier orden dependiendo de los resultados de otras pruebas.
	ATE_FUN.1.4C	Los resultados de las pruebas esperadas muestran las salidas anticipadas de una ejecución exitosa de las pruebas.
	ATE_FUN.1.5C	Los resultados de las pruebas de la ejecución del desarrollador demuestran que cada función de seguridad probada se comportó como se especificó.
	ATE_FUN.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	ATE_IND.2.1D	El desarrollador provee el TOE para pruebas.
	ATE_IND.2.1C	El TOE se adecua para pruebas

	ATE_IND.2.2C	El desarrollador provee un conjunto equivalente de recursos para esos que fueron usados en la prueba funcional del desarrollador de la TSF.
	ATE_IND.2.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	ATE_IND.2.2E	El evaluador prueba un subconjunto de la TSF apropiadamente para confirmar que el TOE funciona como se especificó.
	ATE_IND.2.3E	El evaluador ejecuta un ejemplo de pruebas en la documentación de pruebas para verificar los resultados de pruebas del desarrollador.
	COMPONENTES	**EVALUACIÓN DE LA VULNERABILIDAD**
EAL2	AVA_SOF.1.1D	El desarrollador realiza un fuerte análisis de función de seguridad del TOE para cada mecanismo identificado en el ST como una fuerza que demanda función de seguridad del TOE.
	AVA_SOF.1.1C	Para cada uno de los mecanismos con una dotación de función de seguridad del TOE demanda la fuerza del análisis de función de seguridad del TOE que cumple o supera el nivel de fortaleza mínimo definido en el PP / ST.
	AVA_SOF.1.2C	Para cada uno de los mecanismos con una fortaeza específica de función de seguridad del TOE reclama la fortaleza del análisis de función de seguridad del TOE muestra que reúne o excede la fortaleza específica de funciones metricas definidas en el PP/ST.
	AVA_SOF.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	AVA_SOF.1.2E	El evaluador confirma que las solicitudes estrictas son correctos.
	AVA_VLA.1.1D	El desarrollador lleva a cabo y documenta un análisis de lo que se puede entregar del TOE buscando la manera evidente en la cual un usuario puede violar la TSP.
	AVA_VLA.1.2D	El desarrollador documenta la disposición de las vulnerabilidades evidentes.
	AVA_VLA.1.1C	La documentación presenta que para todas las vulnerabilidades identificadas, que la vulnerabilidad no puede ser explotada en el medio ambiente para el TOE.
	AVA_VLA.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.
	AVA_VLA.1.2E	El evaluador realiza pruebas de penetración, sobre la base del análisis de vulnerabilidad de los desarrolladores, para garantizar las vulnerabilidades evidentes que se han abordado.

Tabla 9 Preguntas desarrolladas para los componentes de EAL1 y EAL2

4.1.2 Cuantificación de la valoración del riesgo aplicado

La forma de cuantificar las preguntas y obtener el nivel de riesgos, se describe a continuación. Para cada una de las preguntas, al ser verdadera cumple el requisito y se le da un valor de uno (1), sino el valor es de cero (0). El riesgo de cada una de las clases que tiene el TOE se determina de la siguiente manera:

(Cantidad de controles implementados por clase)*100 / (Cantidad de controles por clase) - 100

El valor del riesgo total del TOE se determina considerando todas las clases evaluados, de la siguiente manera:
(Cantidad de controles implementados en total)*100 / (Cantidad de controles por clase en total) - 100

Los valores de riesgo se han asociado a los siguientes niveles:

NIVEL DE RIESGO	%
MUY ALTO	**80 – 100**
ALTO	**60 – 80**
MEDIO	**40 – 60**
BAJO	**20 – 40**
MUY BAJO	**0.0 – 20**

Tabla 10 Porcentaje de niveles de riesgo

4.1.3 Resultados de la evaluación

Por acuerdos de confidencialidad, y protección de los sistemas de información de las entidades que amablemente se prestaron para ejecutar el análisis de seguridad, solo se presentarán los resultados en general.

Con el fin de evidenciar que los datos fueron recolectados, se adjuntan las fichas de información general de cada encuesta.

Los resultados fueron los siguientes de acuerdo a cada clase de evaluación de la norma ISO/IEC 15408-3:

- Administración de la Configuración. Riesgo 73%. Se tiene un alto riesgo donde la integridad del TOE no está prevenida ante modificaciones,

eliminación o adiciones no autorizadas. Un requerimiento para esta clase se refiere a que el TOE tiene que tener documentadas las medidas de prevención ante modificaciones, eliminación o adiciones no autorizadas. Sin embargo las organizaciones carecen de esta documentación. Es importante que las entidades cumplan con esta clase debido a que sirve para asegurar que se mantiene la integridad del TOE, exigiendo disciplina y control en los procesos de refinamiento y modificación del TOE y de cualquier otra información relacionada. Figura 10.

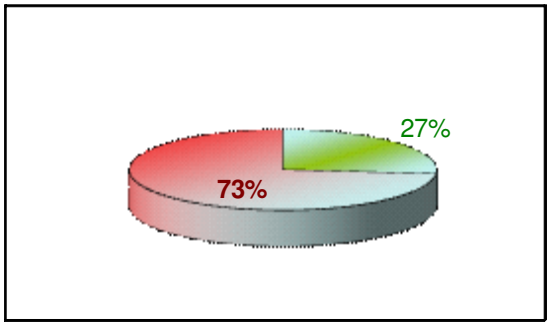


Figura 12 Riesgo en la Administración de la Configuración

- Entrega y Funcionamiento. Riesgo del 71%. Se tiene un alto riesgo al no estar definidos los requerimientos que estandaricen medidas y procedimientos, para la entrega, instalación y operación segura del TOE. Esta clase se hace necesaria debido a que define los requisitos para las medidas, procedimientos y normas relacionadas con la distribución, instalación y uso operacional seguros del TOE, con el fin de garantizar que la protección de seguridad ofrecida por el TOE no se ve comprometida durante el traslado, instalación, arranque ni funcionamiento del mismo. Figura 11.

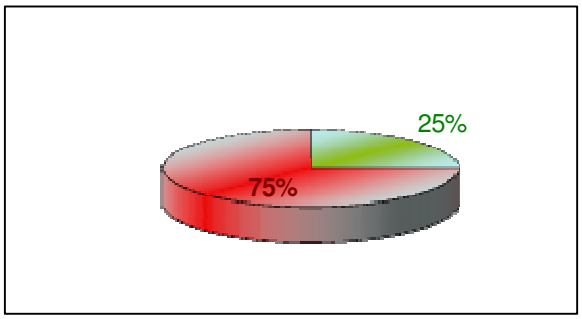


Figura 13 Entrega y Funcionamiento

- Desarrollo 83%. Existe un alto riesgo al no estar definidos los requerimientos necesarios para la implementación de una forma estructurada de las funciones de seguridad (TSF) del TOE. Teniendo en cuenta que no hay un Secure Target guía para los sistemas de información. Esto indica que los desarrolladores no consideran la seguridad en el ciclo de desarrollo del TOE, lo cual puede conllevar a la generación de riesgos de seguridad considerables en producción. Figura 12.

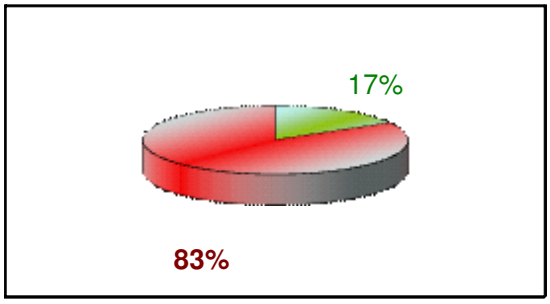


Figura 14 Desarrollo

- Documentos Guía 89%. Existe un alto riesgo en la documentación entregada por el desarrollador al administrador y usuario del TOE, en donde si está clasificada para usuario y administradores, pero no tiene especificaciones de seguridad suficientes que describan funciones del TOE (TSF) y sus restricciones. Figura 13.

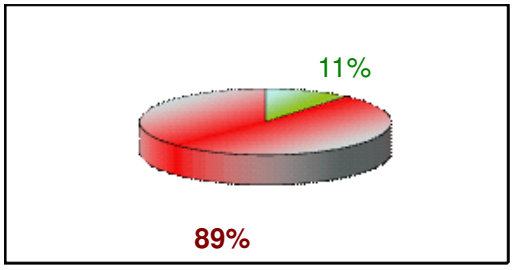


Figura 15 Documentos Guía

- Pruebas 86%. Se presente un riesgo alto, al no realizar las pruebas necesarias que evidencien el nivel de seguridad de las funciones de seguridad del TOE. Generando un alto grado de incertidumbre sobre el comportamiento del TOE ante un evento e incidente de seguridad y los ambientes que se deberían preparar para la producción del TOE, que eviten estos incidentes. Figura 14.

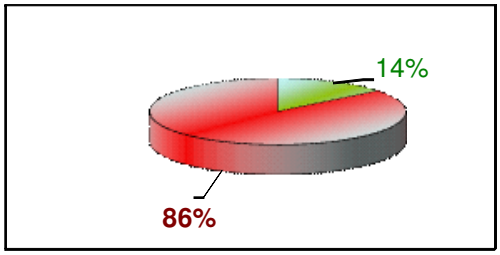


Figura 16 Pruebas

- Evaluación de vulnerabilidad 90%. Hay un riesgo alto de que no exista un análisis previo de las posibles vulnerabilidades relacionadas con la construcción, operación abuso o incorrecta configuración del TOE, que permita prevenir eventos e incidentes de seguridad. Un análisis previo de vulnerabilidades permite identificar las condiciones de seguridad necesarias para la correcta operación del TOE. Figura 15.

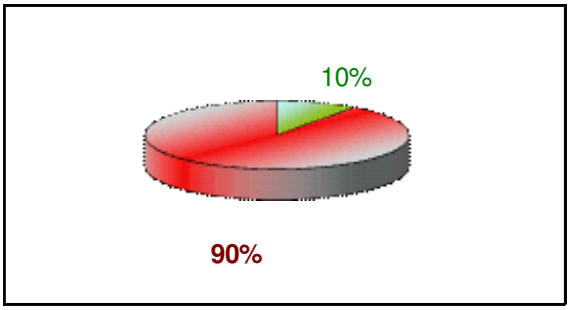


Figura 17 Evaluación de Vulnerabilidad

Resultado general consolidado

Con base en la información descrita anteriormente, es posible determinar que el resultado de seguridad es crítico para los sistemas de información del muestro realizado en Colombia, con un porcentaje del 84%, en donde la seguridad no es una prioridad que se ajusta a la norma ISO/IEC 15408-3 (Common Criteria), y no hay definición de las funciones de seguridad, guías de implementación, prevenciones y pruebas permanente de seguridad, y documentación estricta. Figura 16.

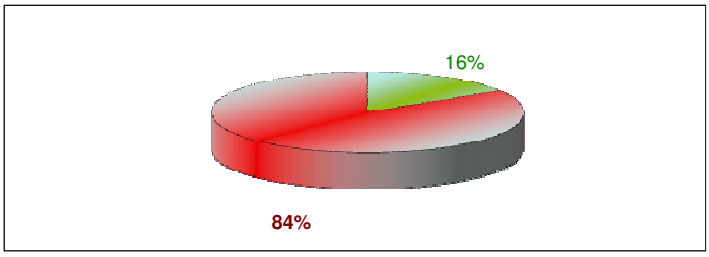


Figura 18 Riesgo general consolidado

5 DISEÑO DEL MODELO PARA LA EVALUACIÓN EN SEGURIDAD INFORMÁTICA DE PRODUCTOS SOFTWARE DE ACUERDO A LA ISO/IEC 15408 COMMON CRITERIA

Se describirá un modelo para la ejecución de pruebas de seguridad basado en la norma ISO/IEC 15408 para sistemas de información software [11].

5.1 Propósito y objetivos del modelo

El propósito de este modelo es el de mejorar los procesos de desarrollo de software en cuanto a seguridad, a través de un cumplimiento de funciones y niveles de evaluación, de acuerdo a una directriz de medidas basadas en la norma ISO/IEC 15408. Los objetivos que se plantean en el modelo son los siguientes:

- Lograr la mejora de procesos de desarrollo de software mediante el cumplimiento y realización sistemática de actividades de aseguramiento, detección y prevención de riesgos.
- Evaluar los resultados de desarrollo con respecto a las funciones de seguridad implementadas o proyectadas
- Monitorear y supervisar el desarrollo de los productos software, evaluando frecuentemente su seguridad de acuerdo a los niveles de seguridad de la norma ISO/IEC 15408-3.
- Identificar nuevas estrategias para mejorar los procesos de desarrollo de software y lecciones aprendidas, con el fin de mejorarlo constantemente y avanzar hacia posibles certificaciones.

El alcance del modelo está dirigido a controlar el acceso de cualquier usuario que este permitido y su respectiva gestión de privilegios a los recursos del TOE. El objetivo del alcance de definir el alcance descrito es alivianar la evaluación en los primeros dos niveles de la norma ISO/IEC 15408-3, con el fin de que las

organizaciones logren las habilidades para hacer una evaluación de seguridad. Con estas habilidades las organizaciones pueden seguir avanzando en otros niveles de seguridad de la norma ISO/IEC 15408 [12].

5.2 Descripción del modelo

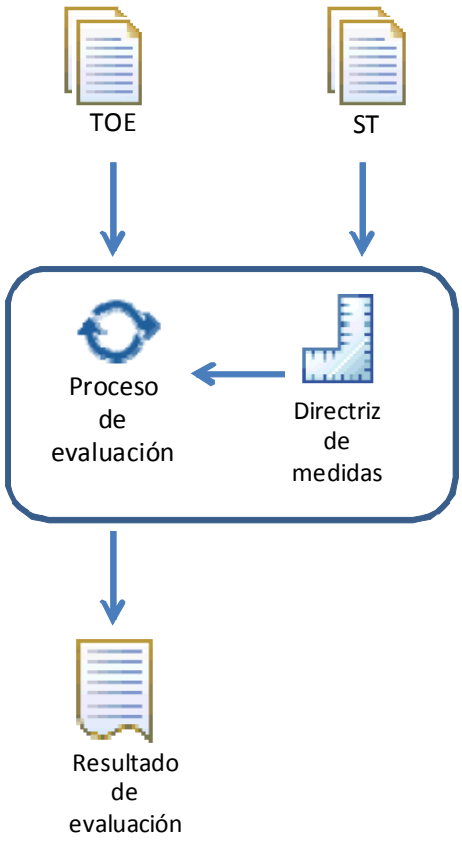


Figura 19 Modelo de ejecución de pruebas

Los componentes del modelo son los siguientes:

- ST. Objetivo de seguridad. Documento oficial publicado en el Common Criteria, que describe las características de un TOE especifico (Sistema de información, base de datos, sistema operativo o hardware) ideal dividido en:

- Límites Físicos. Descripción del hardware, en donde implementará el TOE.
- Limites Lógicos. Descripción del software, que implementará el TOE, basado en sus funciones.
- Entorno de seguridad del TOE. Es donde se identifican las hipótesis del entorno físico, características de los usuarios autorizados, las hipótesis del entorno lógico y las amenazas dirigidas al TOE y al ambiente operacional.
- Objetivos de seguridad. Se especifican los objetivos que cumplirá el TOE en seguridad relacionados a autenticación y gestión de privilegios.
- Requerimientos de seguridad. Funciones y niveles de garantía de seguridad que cumple el TOE.

- TOE. Objetivo de evaluación. Componente TIC seleccionado para evaluar su seguridad bajo la norma ISO/IEC 15408 Common Criteria ST, dividido en límites físicos, lógicos, entorno de seguridad del TOE, objetivos de seguridad y requerimientos de seguridad.
- Directriz de medidas. De acuerdo a la importancia que se quiera dar a los ítems del ST, se establece una directriz de evaluación con un peso específico para cada ítem que permita generar un valor de calificación al aplicarse.
- Proceso de evaluación. Describe el conjunto de actividades para comparar el TOE con el ST, el cual aplica una directriz de medidas de acuerdo a lo similar que estos dos sean en sus especificaciones de entorno de seguridad, objetivos de seguridad, requerimientos de seguridad y niveles de seguridad.

- Resultado de evaluación. De acuerdo a los ítems del ST y la directriz de medidas, se presentarán un resultado de evaluación cuantitativo que permita establecer el nivel de seguridad del TOE a evaluar.

5.3 Roles del modelo

Los roles del modelo son los siguientes:

NOMBRE	ROL	COMPETENCIAS
RTOE	Responsable del TOE al que se le aplicará el modelo y se evaluará	Conocimiento del TOE a evaluar, de la norma ISO/IEC 15408 Common Criteria y capacidad para implementar las mejoras generadas de la aplicación del modelo de evaluación al TOE
ETOE	Responsable de la evaluación del TOE de acuerdo a las directrices determinadas basadas en la norma ISO/IEC 15408 Common Criteria	Conocimiento de la norma ISO/IEC 15408 Common Criteria y capacidad de análisis que permitan generar una evaluación objetiva del TOE

Tabla 11 Roles del modelo

5.4 Descripción de las actividades del modelo

El diagrama de actividades es el siguiente:

COMPONENTE	ACTIVIDAD	RESPONSABLE
ST	Seleccionar ST	RTOE
TOE	Identificar características técnicas del TOE	RTOE
TOE	Especificar límites físicos	RTOE
TOE	Especificar límites lógicos	RTOE
TOE	Especificar entorno de seguridad	RTOE
TOE	Identificar objetivos de seguridad	RTOE
TOE	Identificar funciones de seguridad	RTOE
TOE	Identificar niveles de seguridad	ETOE
Directriz de medidas	Identificar evaluación seguridad	ETOE
Proceso de evaluación	Aplicar evaluación de seguridad	ETOE
Reporte	Generar reporte	ETOE

Tabla 12 Diagrama y descripción de actividades del modelo

5.4.1 Seleccionar ST

El sitio oficial del Common Criteria tiene un repositorio de ST (Security Target) y PP (Protection Profile), del cual se toma el más apropiado para la evaluación del software TOE. Para este tipo es necesario escoger en la sección "Other Devices and Systems" ST referentes a Sistemas de Información.

Este modelo de evaluación se basará en el ST "SecureInfo Risk Management System Version 3.2.06.12 Security Target" [29].

El responsable de esta actividad es el Responsable del TOE (RTOE).

5.4.2 Identificar características técnicas generales del TOE

Se identifican el TOE (Target Of Evaluation), con los siguientes componentes:

- TSC (Scope of Control TSC). Alcance de control del TOE, es el conjunto de interacciones que pueden ocurrir dentro o por fuera con un TOE y son alcance de las TSP.
- TSP (TOE Security Policy). Política de seguridad del TOE, por la cual se dirigen las reglas para acceder, gestionar, proteger y distribuir los recursos, información y servicios controlados por el TOE.
- SFPs (Security Function Policies). Políticas de Seguridad en Funciones componen al TSP que contienen un alcance y operaciones.
- SF (Security Function SF). Funciones de seguridad que implementan las SFP.

[29] COMMON CRITERIA PORTAL. SecureInfo Risk Management System Version 3.2.06.12 Security Target http://www.commoncriteriaportal.org/files/epfiles/st_vid10042-st.pdf [Citado el 4 de Diciembre 2011]

- TSF (TOE Security Functions). Funciones de seguridad del TOE, las cuales corresponden a las interacciones con todo el hardware, software y firmware del TOE que está directamente o indirectamente relacionado con las TSP.
- TSFI (TSF Interface). Interfaces de las funciones de seguridad del TOE, por las cuales interactúan los usuarios o aplicaciones, a los recursos.
- Subjects. Entidades activas como procesos o usuarios que están sujetos al TSP.
- Objects. Objetivos de seguridad que se pueden realizar con “Subjects”
- Security Attributes. Atributos necesarios para la definición de las TSP de los usuarios, subject y objects.

La distribución del TOE de acuerdo a sus componentes es la siguiente:

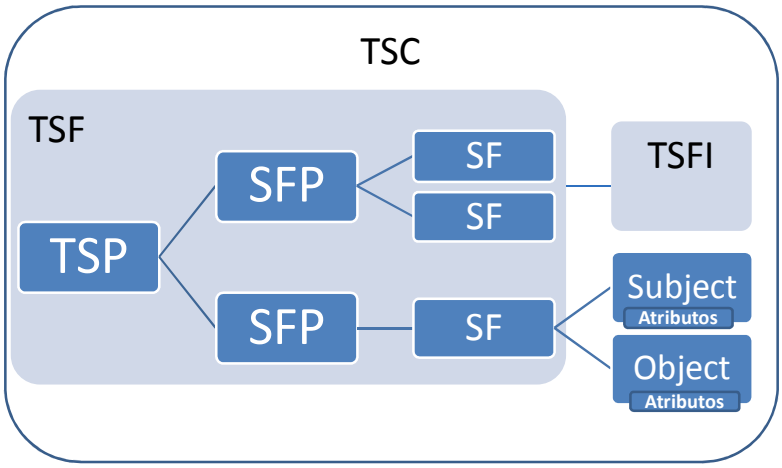


Figura 20 Distribución del TOE de acuerdo a sus componentes

5.4.3 Especificar límites Físicos

En esta actividad se especifican los componentes en el hardware que soportará el TOE, y la forma en que se conectarán. El responsable de esta actividad es el Responsable del TOE (RTOE). Su ID de identificación es LF1.

5.4.4 Límites Lógicos

Se definen las funciones de seguridad implementadas por el software que compone el TOE, las cuales son:

- Identificación y autenticación. Se requiere la identificación y autenticación de los usuarios antes de acceder al TOE. No se debe iniciar ninguna modificación y/o eliminación sin previa identificación y autenticación. Cada usuario tiene asociado perfiles de seguridad con su cuenta que define las funcionalidades.

- Control de acceso. El TOE usa controles de acceso según las políticas establecidas por el área de TI.

El responsable de esta actividad es el Responsable del TOE (RTOE).

Sus ID de identificación son:

LIMITE LÓGICO	ID DE IDENTIFICACIÓN
Identificación y autenticación	LL2
Control de acceso	LL3

Tabla 13 ID de Límites Lógicos

5.4.5 Especificar entorno de seguridad

Se definen tres ítems en el TOE:

- Hipótesis del entorno físico. Se describen las características que previenen el acceso físico no autorizado. En donde los recursos de procesamiento deben contar con entornos seguros que posean controles preventivos de accesos físicos no autorizados.

- Hipótesis del entorno de las TI. Describe las características de operación del TOE. Teniendo en cuenta la conexión controlada de sistemas externos

al TOE que interactúan con él, la protección del hardware y software del TOE antes accesos no autorizados y la ejecución controlada de las diferentes aplicaciones del TOE.

- Amenazas. Se describen las amenazas relacionadas con el TOE y el ambiente de TI. Las amenazas pueden ser de ACCESO al TOE donde un usuario puede tener permisos por un error de un usuario y/o de un sistema o un ataque sofisticado y de ACCESO al AMBIENTE OPERACIONAL donde gane privilegios para realizar modificaciones no autorizadas.

El responsable de esta actividad es el Responsable del TOE (RTOE).

Los ID de identificación son los siguientes:

ENTORNO DE SEGURIDAD DEL TOE	ID DE IDENTIFICACIÓN
Hipótesis del entorno físico	EST1
Hipótesis del entorno de las TI	EST2
Amenazas	EST3

Tabla 14 ID de Entorno de seguridad del TOE

5.4.6 Identificar objetivos de seguridad del TOE

Se especifican los objetivos de seguridad del TOE, los cuales deben ser dirigidos a controlar el acceso de cualquier usuario que este permitido para ingresar y su respectiva gestión de privilegios a los recursos.

El responsable de esta actividad es el Responsable del TOE (RTOE).

Su identificación es OS1.

5.4.7 Identificar funciones de seguridad

Se aplican las funciones de seguridad de referencia al TOE de acuerdo al ST escogido, las cuales para un sistema de información son las siguientes con su respectivo ID de identificación:

CLASE	ID DE IDENTIFICACION DE FUNCION	DESCRIPCIÓN DE IMPLEMENTACIÓN
FDP_ACC.1 Política control de acceso a un subconjunto	FS1	La función de seguridad debe asegurar la política de control de acceso a subconjuntos de usuarios, objetivos y operaciones específicas.
FDP_ACF.1 Perfiles de seguridad basados en los controles de acceso	FS2	Control de seguridad del acceso basado en los atributos jerárquicos.
	FS3	La función de seguridad del TOE debe aplicar el control de acceso de las políticas de las funciones de seguridad basándose en Permisos y/o dominios.
	FS4	La función de seguridad del TOE debe aplicar reglas para determinar si una operación entre sujetos y objetos controlados está permitida.
FIA_SOS.1 Verificación de datos de alta confidencialidad	FS5	La función de seguridad del TOE debe proporcionar un mecanismo para verificar que se debe cumplir con las políticas y limitaciones de contraseña definidas por los siguientes atributos: a. Las contraseñas deben tener una longitud mínima de ocho (8) caracteres y que se incluya al menos un carácter alfabético, un carácter numérico y un carácter especial. b. Las contraseñas no se deben reutilizar por el usuario. c. La función de seguridad del TOE no debe indicar que la contraseña elegida por él o ella está siendo usada por otro usuario. d. La función de seguridad del TOE por defecto, debe prohibir contraseñas nulas durante la operación normal.
FIA_UAU.2 Autenticación de usuarios antes de cualquier acción.	FS6	La función de seguridad del TOE debe exigir que cada usuario se autentique correctamente antes de permitir que cualquier otra función de seguridad del TOE realice acciones mediante el nombre de ese usuario.
FIA_UAU.7 Protección de la información de autenticación.	FS7	La función de seguridad del TOE debe proporcionar solo información oculta para el usuario, mientras que la autenticación está en curso.
FIA_UID.2 Identificación del usuario antes de	FS8	La función de seguridad del TOE debe exigir que cada usuario se identifique antes de permitir que cualquier otra función de seguridad del TOE realice acciones en nombre de dicho usuario.

cualquier acción.		
FMT_MSA.1 Gestión de los perfiles de seguridad	FS9	La función de seguridad del TOE debe aplicar el control de acceso de la política de función de la seguridad para restringir la capacidad de cambio por defecto, consultar, modificar, eliminar y crear los atributos de seguridad: permisos del administrador del sistema del sistema de gestión y el administrador de dominio.
FMT_MSA.3 Inicialización de atributos estáticos	FS10	La función de seguridad del TOE debe aplicar el control de acceso a la configuración del sistema, para hacer cumplir la SFP.
	FS11	La función de seguridad del TOE debe permitir que el administrador del sistema de gestión y el administrador del dominio especifique valores iniciales para anular los valores por defecto cuando un objeto o la información es creada.
FMT_MTD.1 Gestión de los datos de las funciones de seguridad del TOE	FS12	La función de seguridad del TOE debe restringir la capacidad de crear, consultar, modificar y eliminar los siguientes datos del TSF: a. Grupo del sistema de gestión. b. Permisos para grupos del sistema de gestión. c. Cuenta de cliente de un grupo del sistema de gestión. d. Permisos para una cuenta de cliente del sistema de gestión.
	FS13	La función de seguridad del TOE debe restringir la capacidad de crear, modificar y eliminar en ese dominio especifico los siguientes datos relevantes para la función de seguridad del TOE: a. Grupo del sistema de gestión. b. Permisos para grupos del sistema de gestión. c. Cuenta de cliente de un grupo del sistema de gestión.
FMT_SMF.1 Especificación de funciones de gestión	FS14	La función de seguridad del TOE debe ser capaz de realizar las siguientes funciones de gestión de seguridad: a. Gestión de grupos del sistema de gestión. b. Gestión de los permisos para cada grupo del sistema de gestión. c. Gestión de cuentas de clientes en los grupos del Sistema de gestión. d. Gestión de permisos para cada cuenta del sistema de gestión.
FMT_SMR.1	FS15	La función de seguridad del TOE debe mantener las funciones: a. Administrador autorizado del sistema de gestión. b. Los administradores de dominio. c. Los usuarios autorizados.
	FS16	La función de seguridad del TOE debe ser capaz de asociar a los usuarios los perfiles.

Tabla 15 Descripción de las funciones de seguridad con su ID

El responsable de esta actividad es el Responsable del TOE (RTOE).

5.4.8 Identificar niveles de seguridad

Los niveles de seguridad que se aplicarán de acuerdo a la norma ISO/IEC 15408-3 (Common Criteria), serán los descritos en el ítem “2.2.1 Criterios de evaluación”, basados en los niveles: EAL1 – Probado funcionalmente y EAL2 – Probado estructuralmente.

El EAL1 – Probado funcionalmente, evaluará si las funcionalidades del TOE corresponden a su documentación y no requiere una identificación detallada de riesgos.

El EAL2 – Probado estructuralmente, evaluará la entrega de la documentación del diseño y los resultados de las pruebas del TOE.

El responsable de esta actividad es el Evaluador del TOE (ETOE).

Para cada pregunta y componente de la evaluación se realizará una descripción de su cumplimiento, en donde el responsable a través de una revisión documental lo evidenciará.

Sus ID de identificación son los siguientes:

	COMPONENTES	ID DE IDENTIFICACIÓN
EAL1	ACM_CAP.1.1D	NE17
	ACM_CAP.1.1C	NE18
	ACM_CAP.1.2C	NE19
	ACM_CAP.1.1E	NE20
EAL2	ACM_CAP.2.1D	NE21
	ACM_CAP.2.2D	NE22
	ACM_CAP.2.3D	NE23
	ACM_CAP.2.1C	NE24

	ACM_CAP.2.2C	NE25
	ACM_CAP.2.3C	NE26
	ACM_CAP.2.4C	NE27
	ACM_CAP.2.5C	NE28
	ACM_CAP.2.6C	NE29
	ACM_CAP.2.7C	NE30
	ACM_CAP.2.1E	NE31
	COMPONENTES	**ID DE IDENTIFICACIÓN**
EAL1	ADO_IGS.1.1D	NE32
	ADO_IGS.1.1C	NE33
	ADO_IGS.1.1E	NE34
	ADO_IGS.1.2E	NE35
EAL2	ADO_DEL.1.1D	NE36
	ADO_DEL.1.2D	NE37
	ADO_DEL.1.1C	NE38
	ADO_DEL.1.1E	NE39
	ADO_IGS.1.1D	NE40
	ADO_IGS.1.1C	NE41
	ADO_IGS.1.1E	NE42
	ADO_IGS.1.2E	NE43
	COMPONENTES	**ID DE IDENTIFICACIÓN**
EAL1	ADV_FSP.1.1D	NE44
	ADV_FSP.1.1C	NE45
	ADV_FSP.1.2C	NE46
	ADV_FSP.1.3C	NE47
	ADV_FSP.1.4C	NE48
	ADV_FSP.1.1E	NE49
	ADV_FSP.1.2E	NE50
	ADV_RCR.1.1D	NE51

	ADV_RCR.1.1C	NE52
	ADV_RCR.1.1E	NE53
EAL2	ADV_FSP.1.1D	NE54
	ADV_FSP.1.1C	NE55
	ADV_FSP.1.2C	NE56
	ADV_FSP.1.3C	NE57
	ADV_FSP.1.4C	NE58
	ADV_FSP.1.1E	NE59
	ADV_FSP.1.2E	NE60
	ADV_RCR.1.1D	NE61
	ADV_RCR.1.1C	NE62
	ADV_RCR.1.1E	NE63
	ADV_HLD.1.1D	NE64
	ADV_HLD.1.1C	NE65
	ADV_HLD.1.2C	NE66
	ADV_HLD.1.3C	NE67
	ADV_HLD.1.4C	NE68
	ADV_HLD.1.5C	NE69
	ADV_HLD.1.6C	NE70
	ADV_HLD.1.7C	NE71
	ADV_HLD.1.1E	NE72
	ADV_HLD.1.2E	NE73
	COMPONENTES	**ID DE IDENTIFICACIÓN**
EAL1	AGD_ADM.1.1D	NE74
	AGD_ADM.1.1C	NE75
	AGD_ADM.1.2C	NE76

	AGD_ADM.1.3C	NE77
	AGD_ADM.1.4C	NE78
	AGD_ADM.1.5C	NE79
	AGD_ADM.1.6C	NE80
	AGD_ADM.1.7C	NE81
	AGD_ADM.1.8C	NE82
	AGD_ADM.1.1E	NE83
	AGD_USR.1.1D	NE84
	AGD_USR.1.1C	NE85
	AGD_USR.1.2C	NE86
	AGD_USR.1.3C	NE87
	AGD_USR.1.4C	NE88
	AGD_USR.1.5C	NE89
	AGD_USR.1.6C	NE90
	AGD_USR.1.1E	NE91
EAL2	AGD_ADM.1.1D	NE92
	AGD_ADM.1.1C	NE93
	AGD_ADM.1.2C	NE94
	AGD_ADM.1.3C	NE95
	AGD_ADM.1.4C	NE96
	AGD_ADM.1.5C	NE97
	AGD_ADM.1.6C	NE98
	AGD_ADM.1.7C	NE99
	AGD_ADM.1.8C	NE100
	AGD_ADM.1.1E	NE101

	AGD_USR.1.1D	NE102
	AGD_USR.1.1C	NE103
	AGD_USR.1.2C	NE104
	AGD_USR.1.3C	NE105
	AGD_USR.1.4C	NE106
	AGD_USR.1.5C	NE107
	AGD_USR.1.6C	NE108
	AGD_USR.1.1E	NE109
	COMPONENTES	**ID DE IDENTIFICACIÓN**
EAL1	ATE_IND.1.1D	NE110
	ATE_IND.1.1C	NE111
	ATE_IND.1.1E	NE112
	ATE_IND.1.2E	NE113
EAL2	ATE_COV.1.1D	NE114
	ATE_COV.1.1C	NE115
	ATE_COV.1.1E	NE116
	ATE_FUN.1.1D	NE117
	ATE_FUN.1.2D	NE118
	ATE_FUN.1.1C	NE119
	ATE_FUN.1.2C	NE120
	ATE_FUN.1.3C	NE121
	ATE_FUN.1.4C	NE122
	ATE_FUN.1.5C	NE123
	ATE_FUN.1.1E	NE124
	ATE_IND.2.1D	NE125
	ATE_IND.2.1C	NE126

	ATE_IND.2.2C	NE127
	ATE_IND.2.1E	NE128
	ATE_IND.2.2E	NE129
	ATE_IND.2.3E	NE130
	COMPONENTES	**ID DE IDENTIFICACIÓN**
EAL2	AVA_SOF.1.1D	NE131
	AVA_SOF.1.1C	NE132
	AVA_SOF.1.2C	NE133
	AVA_SOF.1.1E	NE134
	AVA_SOF.1.2E	NE135
	AVA_VLA.1.1D	NE136
	AVA_VLA.1.2D	NE137
	AVA_VLA.1.1C	NE138
	AVA_VLA.1.1E	NE139
	AVA_VLA.1.2E	NE140

Tabla 16 ID de identificación de los niveles de seguridad

5.4.9 Identificar Evaluación Seguridad

De acuerdo a las actividades anteriores se fija una evaluación y se aplica al TOE seleccionado. Las ponderaciones recomendadas son las siguientes:

- Límites físicos. El cumplimiento de la disposición de los límites físicos da un valor de 1.
- Límites lógicos. El cumplimiento de la disposición de los límites lógicos da un valor de 1.

- Entorno de seguridad del TOE. El no cumplimiento de los ítems da un puntaje de 0, el cumplimiento de un ítem da un puntaje de 2, el cumplimiento de dos ítems da un puntaje de 3, el cumplimiento de los 3 item da un puntaje de 5.
- Objetivos de seguridad. El cumplimiento de esta disposición da un valor de 1, si no es así el valor de cumplimiento es 0.
- Funciones de seguridad. El cumplimiento de cada una de las disposiciones da un valor de 1, si no es así el valor de cumplimiento es 0.

5.4.10 Aplicar evaluación de seguridad

Se aplicará la evaluación Para cada ID de identificación de los Límites Físicos, Limites Lógicos, Entorno de seguridad del TOE, Objetivos de seguridad y Funciones de seguridad. De acuerdo a la sumatoria los resultados son los siguientes:

CUMPLIMIENTO	RANGO	DESCRIPCIÓN DE CUMPLIMIENTO
Cumplimiento Ideal	22-21	Las funciones de seguridad están definidas completamente, junto con los límites y entorno de seguridad.
Cumplimiento Adecuado	20- 16	Hay funciones de seguridad definido en su mayoría definidas, junto con los límites y entorno de seguridad
Cumplimiento Aceptable	15-11	Existen límites, entorno de seguridad y más de la mitad de funciones de seguridad
Cumplimiento Regular	10 – 6	Existen límites, entorno de seguridad definidos y ciertas funciones
Cumplimiento Critico	5 – 0	Las funciones de seguridad no están completamente definidas junto con el entorno

Tabla 17 Rango de cumplimiento TOE

Estos se agruparan en **PARAMETROS del TOE.**

La evaluación de acuerdo a niveles de seguridad de Evaluación será de acuerdo a lo descrito en el ítem 2.2.2 Tabla 5, en el cuál se revisará su cumplimiento

Los valores tienen que ser consistentes de los PARAMETROS DEL TOE y LOS NIVELES DE SEGURIDAD. Por ejemplo si el valor es de CUMPLIMIENTO IDEAL, el valor de riesgo tiene que estar en el rango de MUY BAJO.

La correspondencia de los rangos es la siguiente:

CUMPLIMIENTO PARAMETROS DEL TOE	RANGO	NIVEL DE RIESGO EAL	%
Cumplimiento Ideal	22-21	MUY BAJO	**0.0 – 20**
Cumplimiento Adecuado	20- 16	BAJO	**20 – 40**
Cumplimiento Aceptable	15-11	MEDIO	**41 – 60**
Cumplimiento Regular	10 – 6	ALTO	**61 – 80**
Cumplimiento Critico	5 - 0	MUY ALTO	**81 – 100**

Tabla 18 Rango de cumplimiento de los parámetros del TOE con el Nivel de Riesgo EAL

5.4.11 Generar reporte

De acuerdo a los cumplimientos del TOE, se genera un reporte con el resultado en general, donde se genere un compendio por cada ID su evaluación.

6 EVALUACION DEL MODELO EN UN PRODUCTO SOFTWARE ESPECÍFICO

Para aplicar el modelo se seleccionó el producto software Sistema de Información para la Gestión de Activos desarrollado por la empresa Nexura International S.A.S. El cuál es un sistema que es un módulo de un ERP, aplicado a una entidad pública, como la SUPERSALUD. La empresa que evaluará será Password Consulting Services ltda, experta en servicios relacionados con seguridad informática.

6.1 Selección de los roles para la aplicación del modelo

Para ROL se le asignará un perfil de acuerdo a cada empresa.

NOMBRE	PERFIL ASIGNADO
RTOE	Líder Software Nexura
ETOE	Auditor Password

Tabla 19 ROL con el perfil asignado

6.2 Selección del Secure Target

Para aplicar el modelo se selecciono el ST "SecureInfo Risk Management System Version 3.2.06.12 Security Target"[30], preparado por COACT Inc. El cuál proporciona las bases para una evaluación de un Sistema de Información que permite la gestión de riesgos, el TOE en este caso, y define los aspectos del ambiente físico y lógico, el listado de amenazas, los objetivos, requerimientos y funciones de seguridad. Las características técnicas generales son:

- Sistema Operativo del servidor. Windows Server.
- Sistema de Base de Datos. MS SQL Server.

[30] COMMON CRITERIA PORTAL. SecureInfo Risk Management System Version 3.2.06.12 Security Target http://www.commoncriteriaportal.org/files/epfiles/st_vid10042-st.pdf [Citado el 4 de Diciembre 2011]

- Sistema servidor web. Apache Tomcat Web Server.
- Lenguaje de programación. Java soportado por Java Runtime Enviroment SE.

6.3TOE a evaluar

El TOE a evaluar de acuerdo al Sistema de Información para la Gestión de Activos tendrá los siguientes componentes:

- **TSC (Scope of Control TSC).** El Alcance del TOE, será todo el conjunto de operaciones que puedan ocurrir con la identificación, autenticación y control de acceso de usuarios al Sistema de Información para la Gestión de Activos.
- **TSP (TOE Security Policy).** Política de seguridad del TOE, es identificar, autenticar y controlar el acceso de los usuarios al Sistema de Información para la Gestión de Activos.
- **SFPs (Security Function Policies).** Las Políticas de Seguridad en Funciones son las siguientes:
    - **SFP1 Identificación y autenticación.** Se requiere la identificación y autenticación de los usuarios antes de acceder al TOE, donde no se debe iniciar ninguna modificación y/o eliminación sin previa identificación
    - **SFP2 Asignación de sesión y privilegios.** Cada usuario tiene asociado perfiles de seguridad con su cuenta que define las funcionalidades y privilegios dentro del TOE.

- **SFP3 Control de acceso.** El TOE usa controles de acceso, con el fin de tener un registro sobre las acciones realizadas por los usuarios identificados y autenticados.

- **SF (Security Function SF).** Funciones de seguridad que implementan cada una de las SFPs son las siguientes:

  - **SFP1 Identificación y autenticación.** Funciones de seguridad de implementación:

    - **SFP1 SF1.** Adquirir el nombre y la contraseña del usuario que requiere autenticarse. Se realiza con la implementación de una Clase llamada “Afiliacion” que contiene los métodos “nombre_autenti”, el cuál captura el nombre y la contraseña a través de la interfaz gráfica “GUI_Autentica”, e interactúa con el método “get_usuarios”, el cuál consulta a las tabla de la Base de Datos “Usuarios”. Si el usuario y la contraseña no se identifica se devuelve un dato de no válido por el método “get_usuarios” y se despliega la interfz gráfica “GUI_NoValido”. Si se identifica como valido se asigna su rol para establecer su sesión correspondiente.

  - **SFP2 Asignación de sesión y privilegios.** Funciones de seguridad de implementación:

    - **SFP2 SF1.** Adquirir el rol de usuario autenticado. El método “nombre_autenti” llama al método “rol_establecido” que invoca al método “get_rol”, el cuál llama a la tabla de la Base de Datos “Roles”, en esta tabla está el rol del usuario autenticado, que devuelve los datos al método “rol_asignado”. Es obligatorio que si un usuario esta autenticado debe tener un rol.

        - **SFP2 SF2.** Asignar la sesión al usuario con sus privilegios correspondientes. los privilegios de la sesión que se le asignará al usuario. Cuando se tiene el rol del usuario el método “rol_establecido”, llama al método “sesion”, el cuál con el método “get_sesion”, consulta en la tabla de la Base de Datos “Sesion” los privilegios que tiene ese rol y los carga en un objeto llamado sesion_(nombre_rol_id), a través del método “sesion” que invoca la interfaz “GUI_Sesion” con los recursos de la Base Datos y funciones que tiene permitido el usuario.

    - **SFP3 Control de acceso.** Funciones de seguridad de implementación:

        - **SFP3 SF1.** Cada vez que el objeto “sesion_(nombre_rol_id)” tiene alguna acción por el usuario, se llama al método “insert_registro” de la clase “RegistroAccion”, con el fin de insertar el tipo de acción (Variable TipoAccion), la hora, la fecha (Variable HoraFecha) y el Usuario (Variable usuario) que realizo la acción, en la Tabla de la Base de Datos “Historico_Acciones”.

- **TSF (TOE Security Functions).** Funciones de seguridad del TOE que corresponde a las interacciones con todo el hardware, software y firmware del TOE que está directamente o indirectamente relacionado con las TSP.

    - **TSF 1.** Interacción base de datos. Son las interacciones que tiene el TOE cuando requiere llamar tablas de la base de datos para consultas o modificaciones.

- **TSF 2.** Interacción Tomcat. Interacciones por las cuales el TOE funciona, al igual que todo el Sistema de Información, debido a que esta desarrollado en java con jsp.
- **TSF 3.** Interacción Sistema Operativo. Interacción en donde el sistema operativo almacena en memoria los archivos del TOE.

- **TSFI (TSF Interface).** Interfaces de las funciones de seguridad del TOE, por las cuales interactúan los usuarios o aplicaciones, a los recursos.
  - **TSFI1.** La interfaz de conexión es el objeto "conexionBD", que interactúa con las librerías JDBC.
  - **TSFI2**. La interfaz de conexión es la librería "Common" que interactúa con las clases del TOE.
  - **TSFI3**. La interfaz son los directorios en la memoria del servidor c:\Apache-Tomca/webroot/webapps/TOE.

- **Subjects.** Se identificaron los siguientes:
  - **Subject 1.** El proceso de validación, el cuál verifica que el usuario exista y que las credenciales sean validas. Se relaciona con SFP1 SF1
  - **Subject 2.** Generación de sesión, el cual genera la sesión del usuario en el momento en que este identificado. Se relaciona con SFP2 SF1 y SFP2 SF2.
  - **Subject 3.** Registro de actividades, el cual registra las actividades de los usuarios dentro del TOE. Se relaciona con SFP3 SF1.
  - **Subject 4.** El usuario Administrador, que crea los demás usuarios. Se relaciona con SFP1 SF1, SFP2 SF1, SFP2 SF2 y SFP3 SF1.

- **Subject 5.** El usuario Auditor de tecnología, el cuál configura la lógica de negocio. Se relaciona con SFP1 SF1, SFP2 SF1, SFP2 SF2 y SFP3 SF1.
- **Subject 6.** El usuario Auditor que genera reportes. Se relaciona con SFP1 SF1, SFP2 SF1, SFP2 SF2 y SFP3 SF1.
- **Subject 7.** El Usuario externo que presenta informes. Se relaciona con SFP1 SF1, SFP2 SF1, SFP2 SF2 y SFP3 SF1.

- **Objects.** Se identificaron los siguientes:
  - **Object 1.** La sesión como un objeto, que guarda la información del usuario, rol y privilegios. Se relaciona con SFP2 SF1, SFP2 SF2 y SFP3 SF1.

- **Security Attributes.** El atributo identificado es el siguiente:
  - **Atribute 1.** Cifrado MD5. Este atributo pertenece al Subject 1, Subject 3, Subject 4, Subject 5, Subject 6 , Subject 7 y Object 1
  - **Atribute 2.** Proceso Nativos que no es posible descifrarlos desde afuera del TOE. Este atributo pertenece al Subject 2.
  - **Atribute 3.** Longitud de contraseñas mayor a ocho caracteres. Este atributo pertenece al Subject 1, Subject 3, Subject 4, Subject 5, Subject 6 , Subject 7 y Object 1
  - **Atribute 4.** Contraseñas con caracteres especiales no alfa numéricos. Este atributo pertenece al Subject 1, Subject 3, Subject 4, Subject 5, Subject 6 , Subject 7 y Object 1
  - **Atribute 5.** Parámetros no nulos. Este atributo pertenece al Subject 1, Subject 3, Subject 4, Subject 5, Subject 6 , Subject 7 y Object 1

La distribución del TOE es la siguiente:

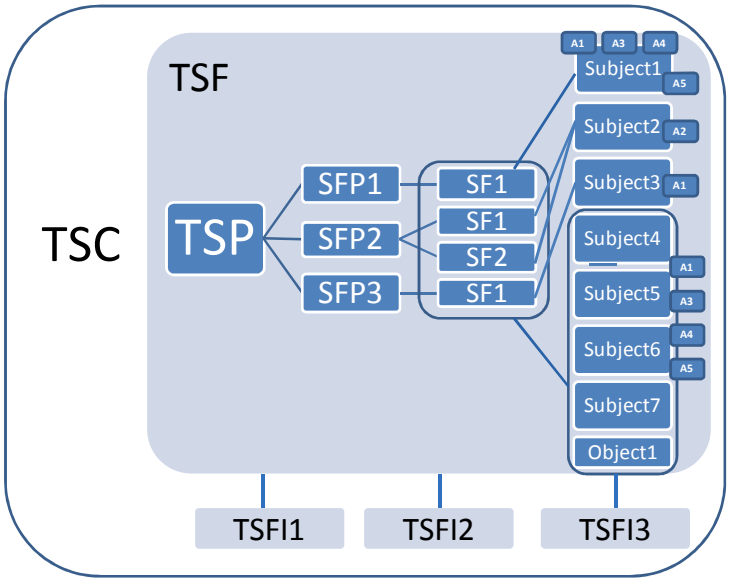


Figura 21 Conceptualización del TOE evaluado

6.4 Especificar límites físicos

Los límites físicos del TOE a evaluar, se encuentran dentro del equipo servidor, el cual tendrá los siguientes componentes con los que se conectará:

- Sistema operativo Windows 2003 Server. Se conectará de acuerdo a la interfaz TSFI 3.
- Apache Tomcat web server 6.0.13. Se conectará de acuerdo a la interfaz TSFI 2
- MS SQL Server 2005. Se conectará de acuerdo a la interfaz TSFI 1

El responsable de esta actividad es el Responsable del TOE (RTOE).

6.5 Especificar límites lógicos

Las funciones de seguridad implementadas en el TOE son:

- SFP1 Identificación y autenticación.
- SFP2 Asignación de sesión y privilegios.
- SFP3 Control de acceso.

El responsable de esta actividad es el Responsable del TOE (RTOE).

6.6 Entorno de seguridad del TOE

La Hipótesis del entorno de las TI, la describe los componentes del TOE: SFP1, SFP2, SFP3, Subjec 1, Subject 2, Subject 3, Subject 4, Subject 5, Subject 6 y Subject 7.

El responsable de esta actividad es el Responsable del TOE (RTOE).

6.7 Objetivos de seguridad

Los objetivos de seguridad del TOE se especifican en:

- SFP1 Identificación y autenticación.
- SFP2 Asignación de sesión y privilegios.
- SFP3 Control de acceso.

El responsable de esta actividad es el Responsable del TOE (RTOE).

6.8 Funciones de seguridad

Las funciones de seguridad implementadas fueron las siguientes:

CLASE	ID DE IDENTIFICACION DE FUNCION	IMPLEMENTACION EN EL TOE
FDP_ACC.1 Política control de acceso a un subconjunto	FS1	SFP1. Identificación y autenticación. SFP2. Asignación de sesión y privilegios
FDP_ACF.1 Perfiles de seguridad basados en	FS2	SFP2. Asignación de sesión y privilegios.

los controles de acceso	FS3	SFP2. Asignación de sesión y privilegios.
	FS4	SFP3. Control de acceso
FIA_SOS.1 Verificación de datos de alta confidencialidad	FS5	No se implemento: b. Las contraseñas no se deben reutilizar por el usuario. c. La función de seguridad del TOE no debe indicar que la contraseña elegida por él o ella está siendo usada por otro usuario.
FIA_UAU.2 Autenticación de usuarios antes de cualquier acción.	FS6	SFP1 Identificación y autenticación.
FIA_UAU.7 Protección de la información de autenticación.	FS7	Atribute 2, relacionado con el Subject 2 y este con SFP2 Asignación de sesión y privilegios.
FIA_UID.2 Identificación del usuario antes de cualquier acción.	FS8	SFP1 Identificación y autenticación.
FMT_MSA.1 Gestión de los perfiles de seguridad	FS9	SFP2. Asignación de sesión y privilegios
FMT_MSA.3 Inicialización de atributos estáticos	FS10	SFP1 Identificación y autenticación. SFP2 Asignación de sesión y privilegios. SFP3 Control de acceso.
	FS11	No implementado

FMT_MTD.1 Gestión de los datos de las funciones de seguridad del TOE	FS12	SFP1 y SFP2 de acuerdo a los subjetc 4, subject 5, subject 6 y subject 7.
	FS13	FSP 1 y FSP 2, relacionadas con el subject 4.
FMT_SMF.1 Especificación de funciones de gestión	FS14	No está documentada esta función
FMT_SMR.1	FS15	Subject 4, Subject 5, Subject 6 y Subject 7 asociados a SFP1, SFP2 y SFP3.
	FS16	SFP2. Asignación de sesión y privilegios

Tabla 20 Implementación en el TOE de las funciones

El responsable de esta actividad es el Responsable del TOE (RTOE).

6.9 Niveles de seguridad de evaluación

La revisión de los niveles de seguridad fue la siguiente:

	COMPONENTES	CLASE ADMINISTRACIÓN DE LA CONFIGURACIÓN	CUMPLIMIENTO	DESCRIPCION DE CUMPLIMIENTO
EAL1	ACM_CAP. 1.1D	El desarrollador presentó una referencia para el TOE	1	El TOE esta referenciado en un ítem descripción
	ACM_CAP. 1.1C	La referencia para el TOE es única para cada versión	1	Es única para cada versión, es la 1.0
	ACM_CAP. 1.2C	El TOE es etiquetado con su referencia.	1	Tiene un código de etiqueta NXSGSS007.TOE1

	ACM_CAP. 1.1E	El evaluador confirma que la información suministrada reúne todos los requerimientos para contenido y presentación de evidencia.	1	Confirmado
EAL2	ACM_CAP. 2.1D	El desarrollador provee una referencia para el TOE.	1	El TOE esta referenciado en un ítem descripción
	ACM_CAP. 2.2D	El desarrollador usa un sistema de administración de configuración.	1	Existe un Sistema de Configuración que configura los parámetros de cada perfil y de seguridad
	ACM_CAP. 2.3D	El desarrollador provee documentación del administrador de configuración.	1	El manual de SISTEMA DE GESTION describe la administración de configuración NXSGSS012
	ACM_CAP. 2.1C	La referencia para el TOE es única para cada versión.	1	Es única para cada versión, es la 1.0
	ACM_CAP. 2.2C	El TOE es etiquetado con su referencia.	1	Tiene un código de etiqueta NXSGSS007.TOE1
	ACM_CAP. 2.3C	La documentación del administrador de configuración incluye una lista de configuración.	1	Se incluye una lista de configuración en la documentación del administrador
	ACM_CAP. 2.4C	La lista de configuración identifica únicamente todos los ítems de configuración que abarca el TOE.	1	Se identifica en la lista todos los parámetros del TOE
	ACM_CAP. 2.5C	La lista de configuración describe los ítems de configuración que abarca el TOE.	1	Se identifica en la lista todos los parámetros del TOE
	ACM_CAP. 2.6C	La documentación del administrador de configuración describe el método utilizado para identificar únicamente los ítems de configuración.	0	No está cumpliendo
	ACM_CAP. 2.7C	El sistema de administrador de configuración identifica únicamente todos los ítems de configuración.	1	El sistema de administrador solo identifica los ítems de configuración del TOE
	ACM_CAP. 2.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	1	Confirmado

Tabla 21 Descripción de cumplimiento del TOE Clase Administración de la Configuración

	COMPONENTES	CLASE ENTREGA Y FUNCIONAMIENTO	CUMPLIMIENTO	DESCRIPCION DE CUMPLIMIENTO
EAL1	ADO_IGS.1.1D	El desarrollador documenta los procedimientos necesarios para la instalación segura, generación y puesta en marcha del TOE.	1	Están documentados los procedimientos en NXSGSS112, NXSGSS113 y NXSGSS114

	ADO_IGS.1.1C	La documentación indica los pasos necesarios para garantizar la instalación, generación y puesta en marcha del TOE.	1	Están documentados los procedimientos en NXSGSS112, NXSGSS113 y NXSGSS114
	ADO_IGS.1.1E	El evaluador confirma que la información proporcionada cumple con todos los requisitos de contenido y la presentación de pruebas.	1	Confirmado
	ADO_IGS.1.2E	El evaluador determina que los procedimientos de instalación, generación y puesta en marcha son resultado de una configuración segura.	1	Confirmado
EAL2	ADO_DEL.1.1D	El desarrollador documenta los procedimientos de entrega del TOE ó partes de este al usuario al usuario.	1	Están documentados los procedimientos en NXSGSS212 y NXSGSS213
	ADO_DEL.1.2D	El desarrollador utiliza los procedimientos de entrega.	1	Se utiliza los procedimientos NXSGSS212 y NXSGSS213
	ADO_DEL.1.1C	La documentación entregada describe todos los procedimientos necesarios para mantener la seguridad cuando se distribuyen versiones del TOE a los usuarios.	0	No describe todos los procedimientos
	ADO_DEL.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	1	Confirmado
	ADO_IGS.1.1D	El desarrollador provee una referencia para el TOE.	1	El TOE esta referenciado en un ítem descripción
	ADO_IGS.1.1C	La referencia para el TOE es única para cada versión.	1	Es única para cada versión, es la 1.0
	ADO_IGS.1.1E	El TOE es etiquetado con su referencia.	1	Tiene un código de etiqueta NXSGSS007.TOE1
	ADO_IGS.1.2E	El evaluador determina que los procedimientos de instalación, generación y puesta en marcha son resultado de una configuración segura.	1	Determinado

Tabla 22 Descripción de cumplimiento del TOE Clase Entrega y Funcionamiento

	COMPONENTES	**CLASE DESARROLLO**	**CUMPLIMIENTO**	**DESCRIPCION DE CUMPLIMIENTO**
EA	ADV_FSP.1.1D	El desarrollador provee una	1	Las funciones de seguridad se

		especificación funcional.		especifican en el documento NXSGSS007.TOE1
	ADV_FSP.1.1C	La especificación funcional describe el TSF y sus interfaces externas usando un lenguaje informal.	1	En el documento NXSGSS007.TOE1 se especifican las interfaces.
	ADV_FSP.1.2C	La especificación funcional es consistente internamente.	1	Si es consistente
	ADV_FSP.1.3C	La especificación funcional describe el propósito y método de uso de todas las interfaces externas TSF, proveer detalles de los efectos, excepciones y mensajes de error.	1	Se describe los efectos excepcionales y mensajes de error.
	ADV_FSP.1.4C	La especificación funcional representa completamente la TSF.	1	Las funciones de seguridad se especifican en el documento NXSGSS007.TOE1
	ADV_FSP.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	1	Confirmado
	ADV_FSP.1.2E	El evaluador determina que la especificación funcional sea una exacta y completa instanciación de los requisitos funcionales de seguridad del TOE.	1	Determinado
	ADV_RCR.1.1D	El desarrollador presenta un análisis de la correspondencia entre todos los pares adyacentes de representaciones de TSF que se ofrece.	0	No hay un análisis de correspondencia
	ADV_RCR.1.1C	Para cada par adyacente de representaciones TSF entregadas, el análisis demuestra que toda la funcionalidad de seguridad relevante de la representación TSF más abstracta está correctamente y completamente refinada en la representación TSF menos abstracta.	0	No hay un análisis de correspondencia
	ADV_RCR.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	1	Confirmado
EAL2	ADV_FSP.1.1D	El desarrollador provee una especificación funcional.	1	Las especificaciones funcionales están el documento NXSGSS007.TOE1

	ADV_FSP.1.1C	La especificación funcional describe el TSF y sus interfaces externas usando un estilo informal.	1	Son descritas las TSF en el documento NXSGSS007.TOE1
	ADV_FSP.1.2C	La especificación funcional es internamente consistente.	1	Es consistente
	ADV_FSP.1.3C	La especificación funcional describe el objetivo y el método de uso de todas las interfaces externas de TSF, se facilitan detalles de los efectos, las excepciones y mensajes de error.	1	Son descritas las TSF en el documento NXSGSS007.TOE1
	ADV_FSP.1.4C	La especificación funcional representa completamente la TSF.	1	Las TSF están descritas las en el documento NXSGSS007.TOE1
	ADV_FSP.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	1	Confirmado
	ADV_FSP.1.2E	El evaluador determina que la especificación funcional sea una exacta y completa instanciación de los requisitos funcionales de seguridad del TOE.	1	Determinado
	ADV_RCR.1.1D	El desarrollador presenta un análisis de la correspondencia entre todos los pares adyacentes de representaciones de TSF que se ofrece.	0	No hay pares adyacentes referenciados
	ADV_RCR.1.1C	Para cada par adyacente de representaciones TSF entregadas, el análisis demuestra que toda la funcionalidad de seguridad relevante de la representación TSF más abstracta está correctamente y completamente refinada en la representación TSF menos abstracta.	0	No hay pares adyacentes referenciados
	ADV_RCR.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	1	Confirmado
	ADV_HLD.1.1D	El desarrollador entrega el diseño de alto nivel de la TSF.	1	El diseño de alto nivel esta en NXSGSS214
	ADV_HLD.1.1C	La presentación del diseño de alto nivel es informal.	1	Es semiformal descrita con UML
	ADV_HLD.1.2C	El diseño de alto nivel es internamente consistente.	1	Es consistente de acuerdo a la documentación entregada

	ADV_HLD.1.3C	El diseño de alto nivel describe la estructura de la TSF en términos de subsistemas.	1	Se describen las TSF en el diseño de alto nivel
	ADV_HLD.1.4C	El diseño de alto nivel describe la funcionalidad de seguridad suministrada por cada subsistema de la TSF.	1	Se describen las TSF en el diseño de alto nivel de cada subsistema
	ADV_HLD.1.5C	El diseño de alto nivel debe identificar cualquier tipo de software requerido por la TSF, con una presentación de las funciones que ofrece el soporte a los mecanismos de protección aplicados en ese software.	1	Se identifican el software requerido por cada TSF en el documento NXSGSS214
	ADV_HLD.1.6C	El diseño de alto nivel identifica todas las interfaces para los subsistemas de la TSF.	1	Se identifican las interfaces para todo subsistema de las TSF en el documento NXSGSS214
	ADV_HLD.1.7C	El diseño de alto nivel identifica cuál de las interfaces para los subsistemas de las TSF son visibles externamente.	1	Se identifican estas interfaces en NXSGSS214
	ADV_HLD.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	1	Confirmado
	ADV_HLD.1.2E	El evaluador determina que el diseño de alto nivel sea una exacta y completa instanciación de los requisitos funcionales de seguridad del TOE.	1	Confirmado

Tabla 23 Descripción de cumplimiento del TOE Clase Desarrollo

	COMPONENTES	**CLASE DOCUMENTOS GUIA**	**CUMPLIMIENTO**	**DESCRIPCION DE CUMPLIMIENTO**
EAL1	AGD_ADM.1.1D	El desarrollador proporciona la guía del administrador dirigida al personal administrativo del sistema.	1	El desarrollador en el documento NXSGSS012 proporciona la guía
	AGD_ADM.1.1C	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE.	1	En el documento NXSGSS012 se describen las funciones administrativas e interfaces
	AGD_ADM.1.2C	La guía del administrador describe cómo administrar el TOE de una manera segura.	1	En el documento NXSGSS012 están los procedimientos de administrar el sistema de una

				forma segura
	AGD_ADM.1.3C	La guía del administrador contiene advertencias acerca de las funciones y privilegios que deben ser controlados en un ambiente seguro de procesamiento.	0	No se describe
	AGD_ADM.1.4C	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son relevantes para el funcionamiento seguro del TOE.	0	No se describen las hipótesis
	AGD_ADM.1.5C	La guía del administrador describe todos los parámetros de seguridad bajo el control del administrador, indicando los valores de seguridad apropiados.	1	Se describe en la guía del administrador todos los valores de seguridad apropiados
	AGD_ADM.1.6C	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF.	0	No se describe
	AGD_ADM.1.7C	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación.	1	Es consistente
	AGD_ADM.1.8C	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de tecnología de la información.	0	No se describe
	AGD_ADM.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	1	Confirmado
	AGD_USR.1.1D	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE.	1	Se describe las funciones e interfaces en la guía del administrador NXSGSS012
	AGD_USR.1.1C	La guía del administrador describe cómo administrar el TOE de forma segura.	1	Se describe en el NXSGSS012 la forma de administración segura
	AGD_USR.1.2C	La guía del administrador contiene advertencias acerca de funciones y	0	No se tienen descritas estas advertencias

		privilegios que deben ser controladas en un ambiente de procesamiento seguro.		
	AGD_USR.1.3C	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son relevantes para el funcionamiento seguro del TOE.	0	No están descritas estas hipótesis
	AGD_USR.1.4C	La guía del administrador describe todos los parámetros bajo el control del administrador indicando los valores seguros apropiados.	1	Si están descritas en el manual NXSGSS012
	AGD_USR.1.5C	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF.	0	No están descritos estos eventos de seguridad
	AGD_USR.1.6C	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación.	1	Es consistente
	AGD_USR.1.1E	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de tecnología de la información que son relevantes al administrador.	1	Se describen todos los requerimientos para el ambiente necesario
EAL2	AGD_ADM.1.1D	El desarrollador proporciona la guía del administrador dirigida al personal administrativo del sistema.	1	El desarrollador en el documento NXSGSS012 proporciona la guía
	AGD_ADM.1.1C	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE.	1	En el documento NXSGSS012 se describen las funciones administrativas e interfaces
	AGD_ADM.1.2C	La guía del administrador describe cómo administrar el TOE de forma segura.	1	En el documento NXSGSS012 están los procedimientos de administrar el sistema de una forma segura
	AGD_ADM.1.3C	La guía del administrador contiene advertencias acerca de las funciones y privilegios que deben ser controlados en un ambiente seguro de procesamiento.	1	Se encuentran estas advertencias

	AGD_ADM.1.4C	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son relevantes para el funcionamiento seguro del TOE.	0	No se describen las hipótesis
	AGD_ADM.1.5C	La guía del administrador describe todos los parámetros de seguridad bajo el control del administrador, indicando los valores de seguridad apropiados.	1	Se describe en la guía del administrador todos los valores de seguridad apropiados
	AGD_ADM.1.6C	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF.	0	No se describen eventos de seguridad
	AGD_ADM.1.7C	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación.	1	Es consistente
	AGD_ADM.1.8C	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de tecnología de la información.	0	No se describen
	AGD_ADM.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	1	Confirmado
	AGD_USR.1.1D	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE.	1	Se describe las funciones e interfaces en la guía del administrador NXSGSS012l
	AGD_USR.1.1C	La guía del administrador describe cómo administrar el TOE de forma segura.	1	Se describe en el NXSGSS012 la forma de administración segura
	AGD_USR.1.2C	La guía del administrador contiene advertencias acerca de funciones y privilegios que deben ser controladas en un ambiente de procesamiento seguro.	0	No se tienen estas advertencias
	AGD_USR.1.3C	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son	0	No son descritas estas hipótesis

		relevantes para el funcionamiento seguro del TOE.		
	AGD_USR.1.4C	La guía del administrador describe todos los parámetros bajo el control del administrador indicando los valores seguros apropiados.	1	En el documento NXSGSS012 se describen las funciones administrativas e interfaces
	AGD_USR.1.5C	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF.	0	No se describe
	AGD_USR.1.6C	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación.	1	Es consistente
	AGD_USR.1.1E	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de tecnología de la información que son relevantes al administrador.	No	No se hace esta descripción

Tabla 24 Descripción de cumplimiento del TOE Clase Documentos Guía

	COMPONENTES	CLASE PRUEBAS	CUMPLIMIENTO	DESCRIPCION DE CUMPLIMIENTO
EAL1	ATE_IND.1.1D	El desarrollador provee el TOE para pruebas.	0	No hay pruebas realizadas
	ATE_IND.1.1C	El TOE se adecua para pruebas	0	No hay pruebas realizadas
	ATE_IND.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	0	No hay pruebas realizadas
	ATE_IND.1.2E	El evaluador prueba un subconjunto de la TSF apropiadamente para confirmar que el TOE funciona como se especificó.	0	No hay pruebas realizadas
EAL2	ATE_COV.1.1D	El desarrollador provee evidencia del cubrimiento de la prueba.	0	No hay pruebas realizadas
	ATE_COV.1.1C	La evidencia del cubrimiento de la prueba muestra la correspondencia entre las pruebas identificadas en la	0	No hay pruebas realizadas

		documentación de pruebas y la TSF descrita en la especificación funcional.		
	ATE_COV.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	0	No hay pruebas realizadas
	ATE_FUN.1.1D	El desarrollador prueba el TSF y documenta los resultados.	0	No hay pruebas realizadas
	ATE_FUN.1.2D	El desarrollador provee la documentación de pruebas.	0	No hay pruebas realizadas
	ATE_FUN.1.1C	La documentación de pruebas consiste en planes de pruebas, descripción de los procedimientos de pruebas, resultados esperados de la prueba y resultados actuales de la prueba.	0	No hay pruebas realizadas
	ATE_FUN.1.2C	Los planes de prueba identifican las funciones de seguridad para ser probadas y describe las metas de las pruebas a desarrollar.	0	No hay pruebas realizadas
	ATE_FUN.1.3C	Las descripciones del procedimiento de prueba identifican las pruebas a desarrollarse y describe los escenarios para probar cada función de seguridad. Estos escenarios incluyen cualquier orden dependiendo de los resultados de otras pruebas.	0	No hay pruebas realizadas
	ATE_FUN.1.4C	Los resultados de las pruebas esperadas muestran las salidas anticipadas de una ejecución exitosa de las pruebas.	0	No hay pruebas realizadas
	ATE_FUN.1.5C	Los resultados de las pruebas de la ejecución del desarrollador demuestran que cada función de seguridad probada se comportó como se especificó.	0	No hay pruebas realizadas
	ATE_FUN.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	0	No hay pruebas realizadas
	ATE_IND.2.1D	El desarrollador provee el TOE para pruebas.	0	No hay pruebas realizadas
	ATE_IND.2.1C	El TOE se adecua para pruebas	0	No hay pruebas realizadas

	ATE_IND.2.2C	El desarrollador provee un conjunto equivalente de recursos para esos que fueron usados en la prueba funcional del desarrollador de la TSF.	0	No hay pruebas realizadas
	ATE_IND.2.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	0	No hay pruebas realizadas
	ATE_IND.2.2E	El evaluador prueba un subconjunto de la TSF apropiadamente para confirmar que el TOE funciona como se especificó.	0	No hay pruebas realizadas
	ATE_IND.2.3E	El evaluador ejecuta un ejemplo de pruebas en la documentación de pruebas para verificar los resultados de pruebas del desarrollador.	0	No hay pruebas realizadas

Tabla 25 Descripción de cumplimiento del TOE Clase Pruebas

	COMPONENTES	**EVALUACIÓN DE LA VULNERABILIDAD**	**CUMPLIMIENTO**	**DESCRIPCION DE CUMPLIMIENTO**
EAL2	AVA_SOF.1.1D	El desarrollador realiza un estricto análisis de función de seguridad del TOE para cada mecanismo identificado en el ST como un requerimiento que demanda función de seguridad del TOE.	0	No existe un estricto análisis
	AVA_SOF.1.1C	Para cada uno de los mecanismos con una dotación de función de seguridad del TOE demanda un estricto análisis para cada función de seguridad del TOE que cumple o supera el nivel de fortaleza mínimo definido en el PP / ST.	0	No existe estricto análisis
	AVA_SOF.1.2C	Para cada uno de los mecanismos con una característica de seguridad específica de función de seguridad del TOE reclama las características de seguridad en el análisis de función de seguridad del TOE muestra que reúne o excede la fortaleza específica de funciones métricas definidas en el PP/ST.	0	No alcanza a cumplir el ST

	AVA_SOF.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	0	No cumple
	AVA_SOF.1.2E	El evaluador confirma que las solicitudes son correctas.	0	No cumple
	AVA_VLA.1.1D	El desarrollador lleva a cabo y documenta un análisis de lo que se puede entregar del TOE buscando la manera evidente en la cual un usuario puede violar la TSP.	0	No lo realiza
	AVA_VLA.1.2D	El desarrollador documenta la disposición de las vulnerabilidades evidentes.	0	No las documenta
	AVA_VLA.1.1C	La documentación presenta que para todas las vulnerabilidades identificadas, que la vulnerabilidad no puede ser explotada en el medio ambiente para el TOE.	0	No hay documentación
	AVA_VLA.1.1E	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia.	0	No hay evidencia
	AVA_VLA.1.2E	El evaluador realiza pruebas de penetración, sobre la base del análisis de vulnerabilidad de los desarrolladores, para garantizar las vulnerabilidades evidentes que se han abordado.	0	No se realizaron pruebas

Tabla 26 Descripción de cumplimiento del TOE Clase Evaluación de la Vulnerabilidad

El responsable de esta actividad es el ETOE

6.10 Identificar evaluación de seguridad

De acuerdo al cumplimiento de los anteriores ID de identificación del TOE , se aplicará la evaluación descrita en el ítem 4.4.9, de este documento.

6.11 Aplicar evaluación de seguridad

El resultado de la evaluación en Limites Físicos, Limites Lógicos, Entorno de seguridad del TOE, Objetivos de seguridad y Funciones de seguridad son los siguientes:

ID de evaluación	Cumplimiento
LF1	1
LL1	1
LL2	1
EST1	1
EST2	1
EST3	0
OS1	1
FS1	1
FS2	1
FS3	1
FS4	1
FS5	0
FS6	1
FS7	1
FS8	1
FS9	1
FS10	1
FS11	0
FS12	1
FS13	1
FS14	0
FS15	1
FS16	1
Resultado Total	**19**

Tabla 27 Resultado de cumplimiento de Límites Físicos, Limites Lógicos, Entorno de seguridad del TOE, Objetivos de seguridad y Funciones de seguridad

De acuerdo a la Evaluación identificada, el resultado es un **Cumplimiento Adecuado**.

La ejecución de los niveles de seguridad aplicados de acuerdo a la norma ISO/IEC 15408-3 (Common Criteria), serán los siguientes:

	COMPONENTES	ID DE IDENTIFICACIÓN	CUMPLIMIENTO
EAL1	ACM_CAP.1.1D	NE17	1
	ACM_CAP.1.1C	NE18	1
	ACM_CAP.1.2C	NE19	1
	ACM_CAP.1.1E	NE20	1
EAL2	ACM_CAP.2.1D	NE21	1
	ACM_CAP.2.2D	NE22	1
	ACM_CAP.2.3D	NE23	1
	ACM_CAP.2.1C	NE24	1
	ACM_CAP.2.2C	NE25	1
	ACM_CAP.2.3C	NE26	1
	ACM_CAP.2.4C	NE27	1
	ACM_CAP.2.5C	NE28	1
	ACM_CAP.2.6C	NE29	0
	ACM_CAP.2.7C	NE30	1
	ACM_CAP.2.1E	NE31	1
EAL1	ADO_IGS.1.1D	NE32	1
	ADO_IGS.1.1C	NE33	1
	ADO_IGS.1.1E	NE34	1
	ADO_IGS.1.2E	NE35	1
EAL2	ADO_DEL.1.1D	NE36	1
	ADO_DEL.1.2D	NE37	1
	ADO_DEL.1.1C	NE38	0
	ADO_DEL.1.1E	NE39	1
	ADO_IGS.1.1D	NE40	1
	ADO_IGS.1.1C	NE41	1

	ADO_IGS.1.1E	NE42	1
	ADO_IGS.1.2E	NE43	1
EAL1	ADV_FSP.1.1D	NE44	1
	ADV_FSP.1.1C	NE45	1
	ADV_FSP.1.2C	NE46	1
	ADV_FSP.1.3C	NE47	1
	ADV_FSP.1.4C	NE48	1
	ADV_FSP.1.1E	NE49	1
	ADV_FSP.1.2E	NE50	1
	ADV_RCR.1.1D	NE51	0
	ADV_RCR.1.1C	NE52	0
	ADV_RCR.1.1E	NE53	1
EAL2	ADV_FSP.1.1D	NE54	1
	ADV_FSP.1.1C	NE55	1
	ADV_FSP.1.2C	NE56	1
	ADV_FSP.1.3C	NE57	1
	ADV_FSP.1.4C	NE58	1
	ADV_FSP.1.1E	NE59	1
	ADV_FSP.1.2E	NE60	1
	ADV_RCR.1.1D	NE61	0
	ADV_RCR.1.1C	NE62	0
	ADV_RCR.1.1E	NE63	1
	ADV_HLD.1.1D	NE64	1
	ADV_HLD.1.1C	NE65	1
	ADV_HLD.1.2C	NE66	1
	ADV_HLD.1.3C	NE67	1
	ADV_HLD.1.4C	NE68	1
	ADV_HLD.1.5C	NE69	1
	ADV_HLD.1.6C	NE70	1

	ADV_HLD.1.7C	NE71	1
	ADV_HLD.1.1E	NE72	1
	ADV_HLD.1.2E	NE73	1
EAL1	AGD_ADM.1.1D	NE74	1
	AGD_ADM.1.1C	NE75	1
	AGD_ADM.1.2C	NE76	1
	AGD_ADM.1.3C	NE77	0
	AGD_ADM.1.4C	NE78	0
	AGD_ADM.1.5C	NE79	1
	AGD_ADM.1.6C	NE80	0
	AGD_ADM.1.7C	NE81	1
	AGD_ADM.1.8C	NE82	0
	AGD_ADM.1.1E	NE83	1
	AGD_USR.1.1D	NE84	1
	AGD_USR.1.1C	NE85	1
	AGD_USR.1.2C	NE86	0
	AGD_USR.1.3C	NE87	0
	AGD_USR.1.4C	NE88	1
	AGD_USR.1.5C	NE89	0
	AGD_USR.1.6C	NE90	1
	AGD_USR.1.1E	NE91	1
EAL2	AGD_ADM.1.1D	NE92	1
	AGD_ADM.1.1C	NE93	1
	AGD_ADM.1.2C	NE94	1

	AGD_ADM.1.3C	NE95	1
	AGD_ADM.1.4C	NE96	0
	AGD_ADM.1.5C	NE97	1
	AGD_ADM.1.6C	NE98	0
	AGD_ADM.1.7C	NE99	1
	AGD_ADM.1.8C	NE100	0
	AGD_ADM.1.1E	NE101	1
	AGD_USR.1.1D	NE102	1
	AGD_USR.1.1C	NE103	1
	AGD_USR.1.2C	NE104	0
	AGD_USR.1.3C	NE105	0
	AGD_USR.1.4C	NE106	1
	AGD_USR.1.5C	NE107	0
	AGD_USR.1.6C	NE108	1
	AGD_USR.1.1E	NE109	0
EAL1	ATE_IND.1.1D	NE110	0
	ATE_IND.1.1C	NE111	0
	ATE_IND.1.1E	NE112	0
	ATE_IND.1.2E	NE113	0
EAL2	ATE_COV.1.1D	NE114	0
	ATE_COV.1.1C	NE115	0
	ATE_COV.1.1E	NE116	0
	ATE_FUN.1.1D	NE117	0
	ATE_FUN.1.2D	NE118	0
	ATE_FUN.1.1C	NE119	0
	ATE_FUN.1.2C	NE120	0

	ATE_FUN.1.3C	NE121	0
	ATE_FUN.1.4C	NE122	0
	ATE_FUN.1.5C	NE123	0
	ATE_FUN.1.1E	NE124	0
	ATE_IND.2.1D	NE125	0
	ATE_IND.2.1C	NE126	0
	ATE_IND.2.2C	NE127	0
	ATE_IND.2.1E	NE128	0
	ATE_IND.2.2E	NE129	0
	ATE_IND.2.3E	NE130	0
EAL2	AVA_SOF.1.1D	NE131	0
	AVA_SOF.1.1C	NE132	0
	AVA_SOF.1.2C	NE133	0
	AVA_SOF.1.1E	NE134	0
	AVA_SOF.1.2E	NE135	0
	AVA_VLA.1.1D	NE136	0
	AVA_VLA.1.2D	NE137	0
	AVA_VLA.1.1C	NE138	0
	AVA_VLA.1.1E	NE139	0
	AVA_VLA.1.2E	NE140	0

Tabla 28 Resultado de cumplimiento de acuerdo a los niveles EAL1 y EAL2

El Riesgo en General es del 40%

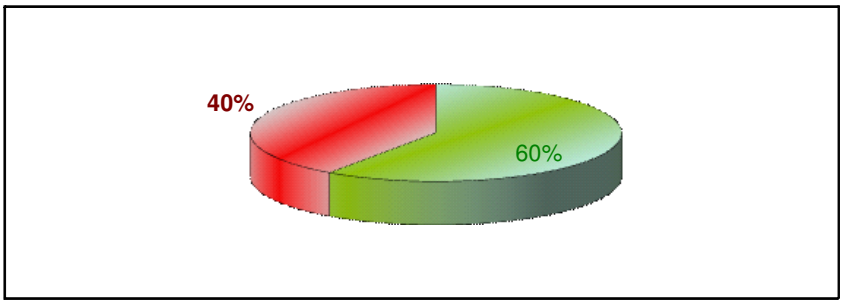


Figura 22 Resultado del Riesgo en general

El riesgo de acuerdo a la Evaluación identificada es **Medio**, por lo tanto teniendo en cuenta el valor anterior de **Cumplimiento Adecuado,** existe una correspondencia para determina que el **Cumplimiento de los parámetros del TOE** de acuerdo a la norma ISO/IECA15408 es **ADECUADO**.

6.12 Generar reporte

6.12.1 Resultado

El TOE evaluado el cuál corresponde a todo el conjunto de operaciones que puedan ocurrir con la identificación, autenticación y control de acceso de usuarios al Sistema de Información para la Gestión de Activos de la empresa Nexura International S.A.S, presento los siguientes resultados:

La evaluación en Limites Físicos, Limites Lógicos, Entorno de seguridad del TOE, Objetivos de seguridad y Funciones de seguridad es de **Cumplimiento Adecuado.**

La evaluación de acuerdo a los niveles de seguridad de la norma ISO/IEC 15408-3 (Common Criteria), es de un riesgo en general del 40%, identificado como **Medio.**

Por lo tanto se determina que el **Cumplimiento de los parámetros del TOE** de acuerdo a la norma ISO/IECA15408 es **ADECUADO.**

CUMPLIMIENTO PARAMETROS DEL TOE	RANGO	NIVEL DE RIESGO EAL	%	Ubicación TOE Evaluado
Cumplimiento Ideal	22-21	MUY BAJO	**0.0 – 20**	
Cumplimiento Adecuado	20- 16	BAJO	**20 – 40**	TOE
Cumplimiento Aceptable	15-11	MEDIO	**41 – 60**	
Cumplimiento Regular	10 – 6	ALTO	**61 – 80**	
Cumplimiento Critico	5 - 0	MUY ALTO	**81 – 100**	

Tabla 29 Resultado Evaluación TOE

6.12.2 Recomendaciones

En el desarrollo del TOE se hace necesario la realización de las siguientes recomendaciones:

- Especificar Hipótesis del entorno físico y Amenazas, con el fin de prever la protección del hardware y software del TOE antes accesos no autorizados y la ejecución controlada en un ambiente especifico de las diferentes funciones del TOE.

- Planear y ejecutar pruebas de seguridad y análisis de vulnerabilidades, que permitan garantizar un revisión de la seguridad del TOE independiente al desarrollador y determinen cuales son las debilidades que se poseen, con el fin de preparar los ambientes de operación para evitar su explotación.

CONCLUSIONES

Algunas conclusiones importantes derivadas del proyecto son:

Las empresas clientes y proveedoras de Tecnologías de la Información, deben ser más rigurosas con respecto a la documentación en el diseño del software, que permita mejorar el control y la gestión de la seguridad de sus componentes, además de presentar manuales detallados para la configuración, y operación en ambientes seguros.

De acuerdo a los resultados del análisis de riesgo en a los productos software seleccionados y al TOE evaluado, la identificación de amenazas, debilidades y riesgos debe realizarse, y así prevenir eventos e incidentes de seguridad. Se recomienda desarrollar análisis basándose en la Manual de la Metodología Abierta de Testeo de Seguridad desarrollado por la ISECOM (Institute for Security and Open Methodologies), el cual da una referencia para realizar análisis de seguridad informática en diferentes niveles, que al ser cubiertos se da el cumplimiento de las especificaciones del Entorno de Seguridad y los niveles Pruebas y Evaluación de la vulnerabilidad de la ISO/IEC 15408-3 Common Criteria.

Para mejorar la seguridad del software a evaluar TOE, la formalización en el lenguaje de expresión (Natural, semi formal y formal), es necesaria, con el fin de lograr escalar los niveles de seguridad, permitiendo posibilidades de certificación en el estándar ISO/IEC 15408 Common Criteria.

Ejecutar procesos de evaluación del software de la ISO/IEC 15408 permite complementar procesos en la compañías de implementación y certificación de ISO27001, en el cuál en su Anexo "A.12 adquisición, desarrollo y mantenimiento de sistemas"[31] exige requisitos de seguridad, seguridad en los procesos de

[31] COLOMBIA. ICONTEC. Norma Técnica NTC-ISO-IEC 27001:2005, Anexo A. Santafé de Bogotá: ICONTEC, 2006. 50 p.

desarrollo y gestión de las vulnerabilidades a los productos software que estén en el alcance del Sistema de Gestión de Seguridad de la Información.

Los riesgos de seguridad contra los productos software se vuelven cada día más sofisticados, y los clientes requieren garantías confiables; si Colombia tiene el "Software & TI" como un sector de clase mundial para su desarrollo[32], es necesaria una estrategia Estado – Empresa privada – Universidad, que promueva la adopción de estándares de seguridad como la ISO/IEC 15408 Common Criteria, y su certificación, con el fin de lograr diferenciadores relevantes en el mercado mundial.

Un centro de certificación en la ISO/IEC 15408 Common Criteria, proyectaría a Colombia como un país gestor del mejoramiento de la seguridad de las TIC producidas en Latinoamérica, debido a que en la región no existe; lo cual se presenta como una oportunidad de liderar procesos de competitividad, desarrollo e innovación en Tecnologías de la Información en la región.

Por último es de concluir que el problema de los incidentes de seguridad en los sistemas de información de una entidad pública o privada, no se soluciona completamente con la implementación y certificación de estándares, debido a que al final la decisión del usuario que opera es la que define en gran medida si ocurre o no un incidente. Sin embargo la adopción de estándares permite obstaculizar y rastrear para futuras investigaciones, esta clase de situaciones.

[32] TRANSFORMACION PRODUCTIVA SECTOR SOFTWARE & TI. Ministerio de Comercio, Industria Y Turismo. http://www.transformacionproductiva.gov.co/publicacones.php?id=18293. [Citado el 4 de Diciembre 2011]

BIBLIOGRAFIA

[1] INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES. Information Security Management Maturity Model. www.isecom.org/ism3/.

[2] COLOMBIA. ICONTEC. Norma Técnica NTC-ISO-IEC 27001:2005. Santafé de Bogotá: ICONTEC.

[3] FERNANDEZ, Eduardo. MOYA, Roberto. PIATTINI, Mario. Seguridad de las Tecnologías de la Información: La construcción de la confianza para una sociedad conectada. Madrid: Ediciones Aenor, 2003. 619 p. ISBN 84-8143-367-5

[4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security part 1: Security functional requirements. Switzerland: 2005.

[5] COMMON CRITERIA PORTAL. Advantis Crypto 3.1 Declaración de seguridad versión pública Versión: 1.2 18/08/2008. http://www.commoncriteriaportal.org/files/epfiles/2006-01-DS.pdf

[6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security part 2: Security functional requirements. Switzerland: 2005.

[7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security part 3: Security assurance requirements. Switzerland: 2005.

[8] ESPAÑA. CENTRO CRIPTOLOGICO NACIONAL, RESOLUCIÓN 1A0/38248/2008, de 29 de octubre. Madrid: 2008.

[9] INTERNET CRIME COMPLAINT CENTER. 2010 Internet Crime Report. http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf

[10] COMPUTER SECURITY INSTITUTE. 2010/2011 Computer Crime and Security Survey. New York: 2011. 12 p.

[11] PINO, F., GARCÍA, F., RUIZ, F., Y PIATTINI, M.; Modelo para la Implementación de Mejora de Procesos en Pequeñas Organizaciones Software, European Systems & Software Process Improvement and Innovation (EuroSPI 2006), Joensuu, Finland. Proceedings EuroSPI 2006. October 2006.

ANEXO

NOMBRE DE LA EMPRESA	IDEAM
DIRECCION	Carrera 10 No. 20-30 BOGOTA D.C
NOMBRE DEL CONTACTO	Alicia Barón
CARGO	Jefe de Tecnología
CORREO	
NUMERO DE CONTACTO	(1)3527160

NOMBRE DE LA EMPRESA	Ministerio de Transporte
DIRECCION	Transversal 45 No. 47-14 BOGOTA D.C
NOMBRE DEL CONTACTO	Luis Fernando Avila
CARGO	Director de Tecnología
CORREO	favila@mintransporte.gov.co
NUMERO DE CONTACTO	(1) 3240800

NOMBRE DE LA EMPRESA	Gobernación del Cauca
DIRECCION	Cra 7 calle 4 esquina, Edificio de la Gobernación del Cauca. Popayán - Cauca
NOMBRE DEL	Danilo Velasco

CONTACTO	
CARGO	Jefe de Sistemas
CORREO	sistemas@cauca.gov.co
NUMERO DE CONTACTO	(2) 8244201

NOMBRE DE LA EMPRESA	Alcaldía Santiago de Cali
DIRECCION	Torre Alcaldía Av 2N Cll 10-11 - Santiago de Cali ()
NOMBRE DEL CONTACTO	Andrés Cruz
CARGO	Analista
CORREO	andres.cruz@cali.gov.co
NUMERO DE CONTACTO	(2) 89820000

NOMBRE DE LA EMPRESA	Servicio de Salud Inmediato S.A
DIRECCION	Carrera 42 Nº 5C-107 - Santiago de Cali (Valle)
NOMBRE DEL CONTACTO	Guido Garzón Peña
CARGO	Jefe de Sistemas
CORREO	sistemas@ssicolombia.com
NUMERO DE CONTACTO	(2) 5528282

NOMBRE DE LA EMPRESA	Hospital del sur de Bogota D.C

DIRECCION	Carrera 78 No. 35-71 Sur Bogotá D.C
NOMBRE DEL CONTACTO	Gustavo Camacho Russy
CARGO	Jefe de Sistemas
CORREO	
NUMERO DE CONTACTO	(1) 273 1819

NOMBRE DE LA EMPRESA	Asmet Salud EPS EPS-S
DIRECCION	Cra. 4 No. 18N-46 - Popayan (Cauca)
NOMBRE DEL CONTACTO	Guillermo Jurado
CARGO	Analista Seguridad de la Información
CORREO	guillermojurado@asmetsalud.org.co
NUMERO DE CONTACTO	(2) 8312002

NOMBRE DE LA EMPRESA	Banco de Occidente
DIRECCION	Cr 4 No 7-61 - Cali (Valle)
NOMBRE DEL CONTACTO	Jorge Velez
CARGO	Arquitecto de Seguridad de la información
CORREO	Jorge.velez@bancodeoccidente.com
NUMERO DE	(2) 8861111

CONTACTO	

NOMBRE DE LA EMPRESA	Clínica Comfacauca
DIRECCION	Calle 2N No. 7-74
NOMBRE DEL CONTACTO	Nelson Portela
CARGO	Jefe de Sistemas
CORREO	nelson.portela@comfacauca.com.co
NUMERO DE CONTACTO	(2) 8231868

NOMBRE DE LA EMPRESA	Coomeva
DIRECCION	Av Pasoancho 57-50 - Cali (Valle)
NOMBRE DEL CONTACTO	Jaime Torres
CARGO	Jefe de Riesgo Tecnológico
CORREO	Jaimea.torres@coomeva.com.co
NUMERO DE CONTACTO	(2)3330000

NOMBRE DE LA EMPRESA	Supergiros
DIRECCION	Calle 13 No 18a-23 - Cali (Valle)
NOMBRE DEL CONTACTO	Oscar eduardo Mondragon
CARGO	Coordinador Seguridad de la Información
CORREO	oscar.eduardo@supergiros.com

NUMERO DE CONTACTO	018000 221321

NOMBRE DE LA EMPRESA	Macrofinanciera
DIRECCION	Carrera 7 No. 73 – 47 – Piso 6
NOMBRE DEL CONTACTO	Edwin Eduardo Orozco López
CARGO	Oficial de Seguridad Informática
CORREO	edwin.orozco@macrofinanciera.com
NUMERO DE CONTACTO	(1)6080033