



Crerios comunes para Monitorear y Evolucionar la Seguridad Informática en Colombia

José Alejandro Chamorro López
Password S.A – Seguridad Informática
jose.chamorro@password.com.co





Agenda

- Problemática
- Una solución: Criterios Comunes
- A sumergirse en Criterios Comunes
- Acercamiento para Colombia
- Comparativa con otros estándares.



Problemática

- Productos Software Inseguros.
 - Salón de la fama:

Time	Attacker	H	M	R	★ Domain	OS	View
2009/06/12	D4NB4R			R	www.ideam.gov.co/cuencas.asp?id=1	Win 2000	mirror
2009/06/12	1923Turk				intranet.minipak.com.co/porta...	Win 2003	mirror
2009/06/12	m0sted			★	www.suzuku.com.co/especificaci...	Win 2003	mirror
2009/06/10	Plexnum Team			★	www.transitoenvidado.gov.co/nt...	Win 2003	mirror
2009/06/08	KHG			★	usrt242.hospitalsegovia.gov.co...	Linux	mirror
2009/06/06	Dz Geniuses				www.ciac.gov.co	Linux	mirror
2009/06/03	DATA ir Security Group			★	www.invisbu.gov.co	Linux	mirror
2009/06/02	Busindre		M		vallasavisos.com.co/sibocons...	Linux	mirror
2009/06/02	Busindre		M		imancorp.com.co/siboconsolas/...	Linux	mirror
2009/06/02	Busindre		M		frutasprimavera.com.co/sitoco...	Linux	mirror
2009/06/02	Busindre		M		naturalworld.com.co/siboconso...	Linux	mirror
2009/06/02	Busindre		M		holasa.com.co/ingles/imagenes/ba...	Linux	mirror
2009/06/02	Busindre		M		kent.com.co/siticoconsolas/imag...	Linux	mirror
2009/05/29	D4NB4R			H	www.abakos.com.co	Linux	mirror
2009/05/28	SecurityBus			M	fundacionesramirezmoreno.org.c...	MacOSX	mirror
2009/05/28	SecurityBus			H.M	www.eneroeticos.com.co	MacOSX	mirror



Problemática

- Casos concretos sin compromisos con marcas:
 - ERP 1
 - ERP 2
 - ERP 3
 - Aplicación de Logística
 - Gestor de Contenidos Web



Problemática

- Cuadro Patológico ERP 1:
 - Archivos de configuración sin protección e identificables por el nombre de su función.
 - No hay políticas estrictas de autenticación.
 - No hay encriptación de la información crítica.
 - No hay encriptación en el tráfico de los datos.
 - No hay control de las aplicaciones de mantenimiento.



Problemática

- Problemas de seguridad ERP 1:
 - Volcado de memoria en los archivos de usuarios y contraseñas.
 - Replica de la aplicación.
 - Captura de información en el transporte de red.
 - Modificación de los archivos de configuración.
 - Modificación de las tablas de datos.
 - Generación y/o eliminación de información falsa (Por ejemplo: Facturas, Informes, etc.).



Problemática

- Cuadro Patológico ERP 2:
 - La Base de Datos que está en SQL Server, tiene el usuario y contraseña por defecto.
 - No hay protección de los archivos de configuración.
 - No hay políticas estrictas de autenticación.
 - No hay encriptación en el tráfico de los datos



Problemática

- Problemas de seguridad ERP 2:
 - Acceso no autorizado a las base de datos.
 - Inyección de código malicioso a las dll.
 - Captura de información en el transporte de red.
 - Autenticación no autorizada a la aplicación.
 - Técnicas de ingeniería inversa a los .exe.



Problemática

- Cuadro Patológico ERP 3:
 - Aplicación en Visual Fox Pro 6.0 con base de datos sin control de acceso.
 - Utiliza unidades de red compartidas sin control de acceso.
 - Unidades de red con el nombre de la aplicación.



Problemática

- Problemas de seguridad ERP3:
 - Acceso no autorizado a la base de datos.
 - Modificación y/o eliminación de los archivos de configuración.
 - Etc...



Problemática

- Cuadro Patológico Aplicación de Logística:
 - Aplicación con SQL server y .Net que utiliza los nombres de NETBIOS para identificación de los equipos computacionales.



Problemática

- Problemas de seguridad Aplicación de Logística:
 - Puertos 135 y 137 abiertos, utilizados para generar sesiones nulas en Windows.
 - Puerto 445 RPC abierto, utilizado por virus informáticos como Sasser, Blaster y Lsas, para accesos no autorizados.



- Cuadro Patológico Gestor de Contenidos Web



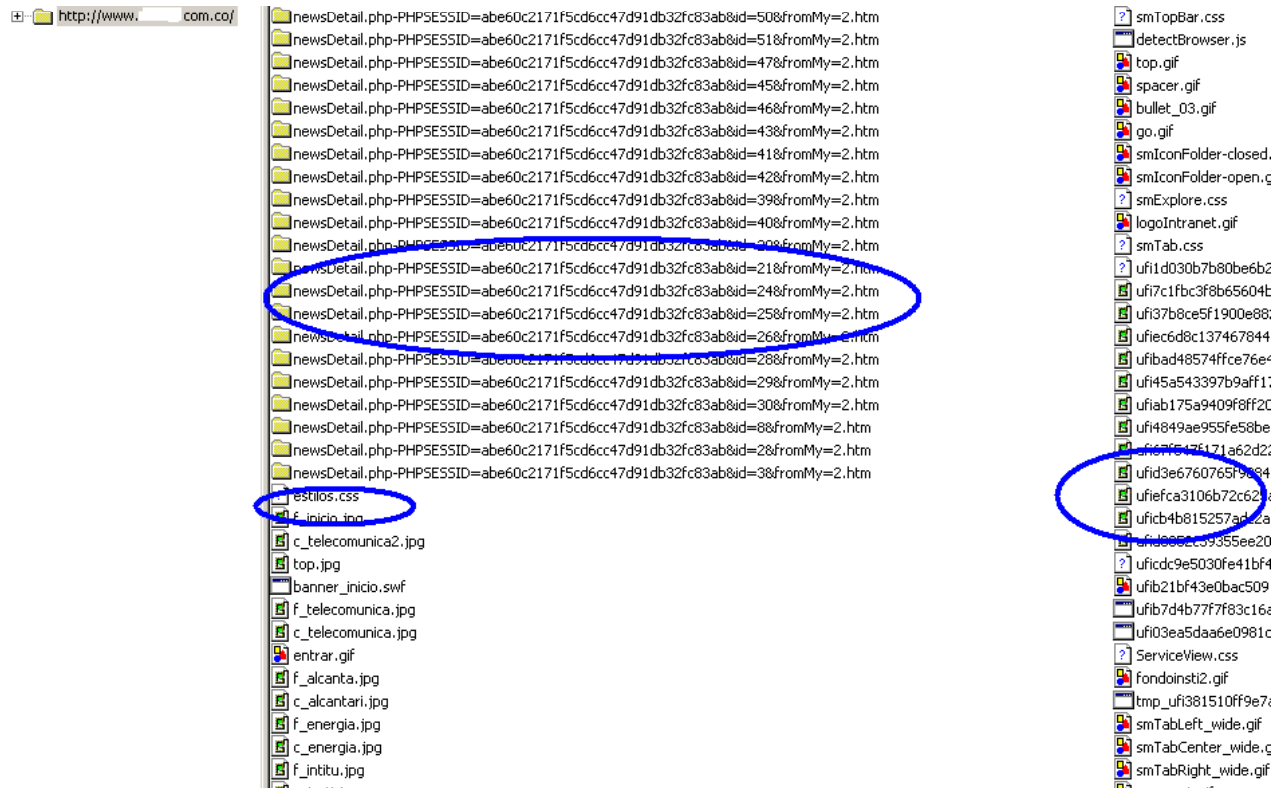


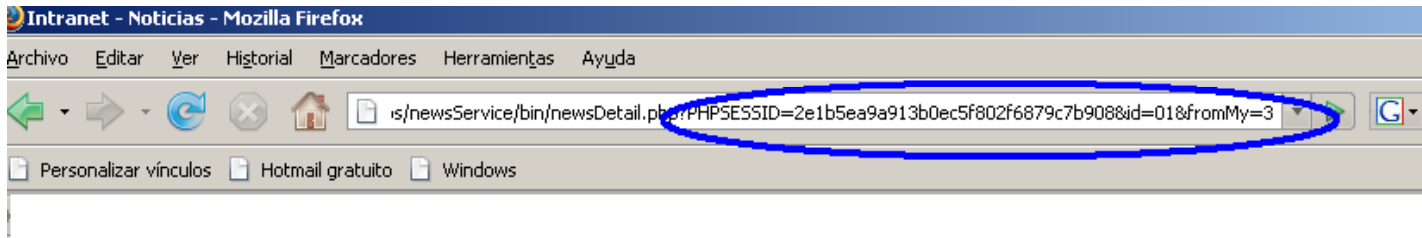
Problemática





Problemática





NewsGetNewItem: No matching record found

Centro de Noticias
Encuentre la Información Detallada de la Noticia

Noticia

2006/10/29

[Ver más Noticias](#)

Fecha de Publicación: //
Vigencia de la Noticia hasta : //
Publicada Por:
smGetUserName: You have an error in your SQL syntax near ' ' at line 1
smGetUserLastName: You have an error in your SQL syntax near ' ' at line 1
Default user
Fuente:



SOLUCION

¿?



ISO/IEC 15408





¿Qué es?

- **Acuerdo internacional sobre el método de desarrollo seguro**, y sobre **7 niveles** discretos de la **gama de esfuerzo**, incluyendo la especificación del trabajo de los evaluadores en cada nivel.
- **Paradigma de arquitectura de seguridad** sobre el que se aplica un catálogo coherente y relacionado de funciones de seguridad que permiten establecer un **lenguaje común** para la **expresión de la seguridad** de los productos y sistemas de las TI.



Origen





¿Que responde CC?

Common Criteria da respuesta a tres preguntas importantes:

¿Qué hace el producto?

CC determina claramente cuales son las funciones de seguridad del producto y en qué entorno aplican.

¿Cómo se ha validado el producto?

CC especifica diferentes niveles de confianza (EAL) que determinan el nivel de ensayo (en tiempo y complejidad) requeridos para probar la seguridad del producto y el nivel exigencia a seguir en el desarrollo de este.

¿Quién ha validado el producto?

Sólo laboratorios acreditados por un esquema de certificación nacional de cada país del CCRA.



Beneficios

Common Criteria aporta diferentes beneficios para el desarrollador de productos IT:

- ✓ Argumento de ventas frente a un producto de la competencia que no lo tenga.
- ✓ Demuestra que su producto cumple íntegramente con las funcionalidades requeridas por su cliente final.
- ✓ Los certificados CC están reconocidos a nivel mundial, lo que permite que su inversión sirva para clientes de cualquier parte del mundo.
- ✓ Permite detectar los puntos fuertes y débiles de la seguridad del producto, lo que ayuda al desarrollador a mejorarlo.



Divisiones

- Parte 1 – Introducción y modelo general
- Parte 2 – Requisitos funcionales de seguridad
- Parte 3 – Requisitos de garantía de seguridad



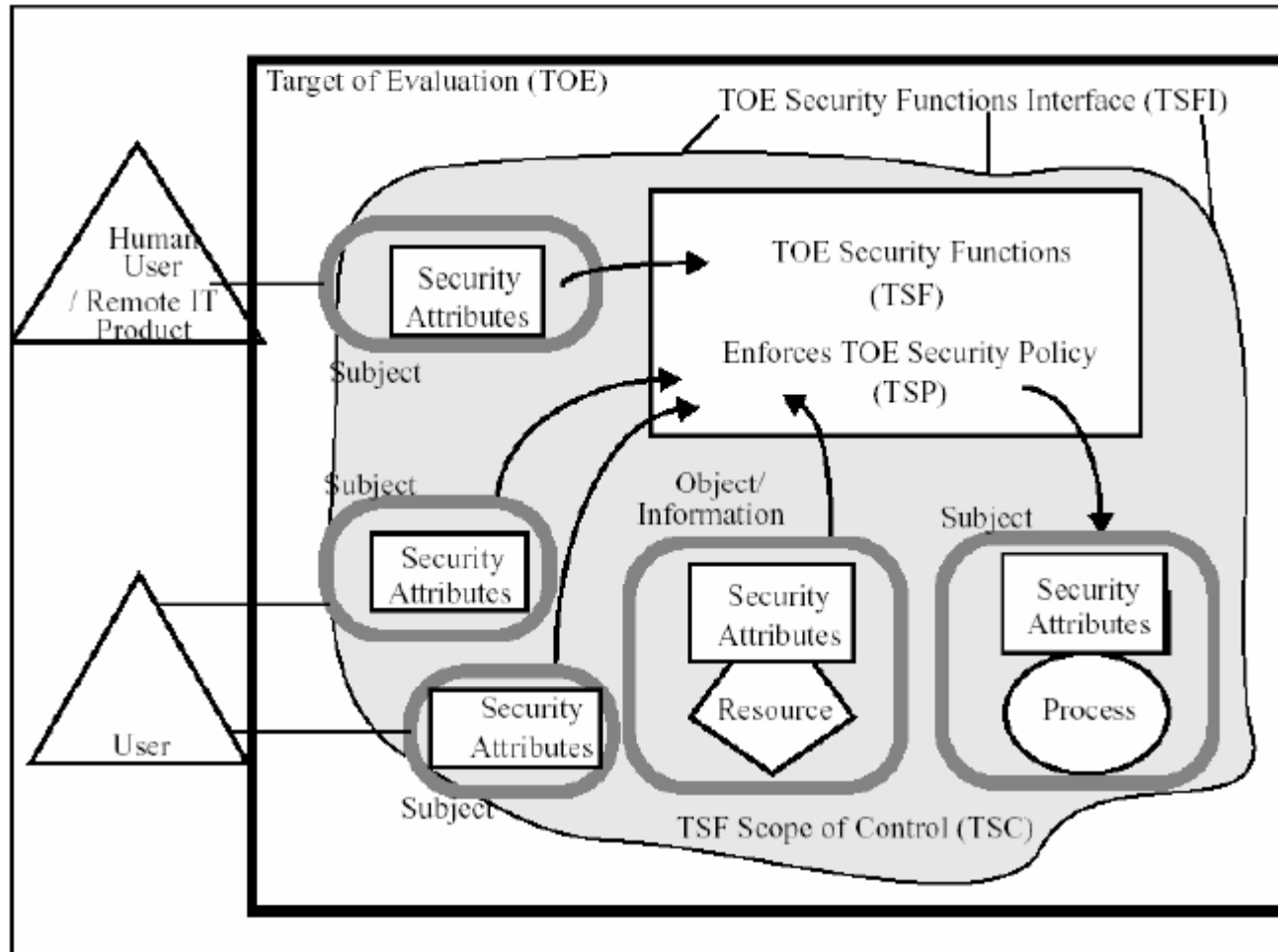
A SUMERGIRSE EN CRITERIOS





IX JORNADA de SEGURIDAD INFORMATICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2005



IX JORNADA
de SEGURIDAD
INFORMÁTICA
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

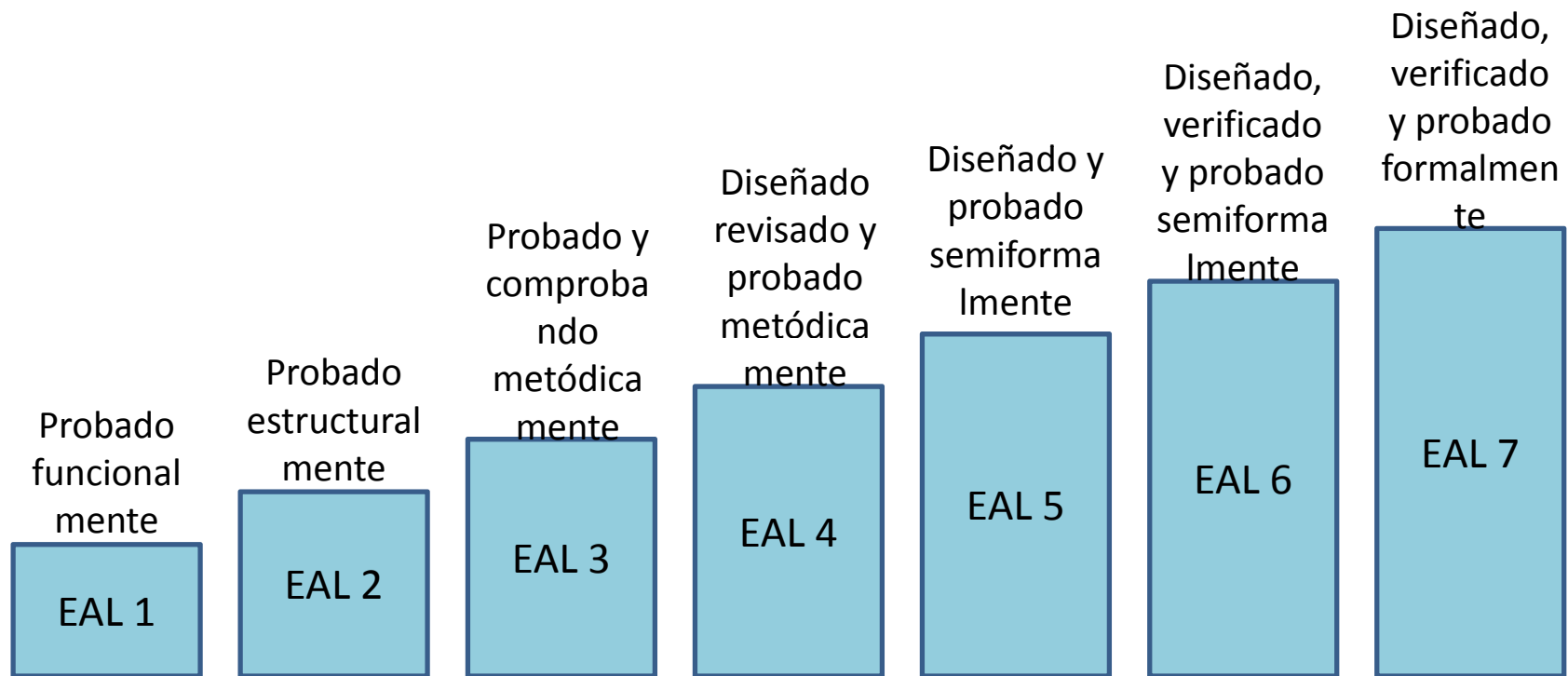
Declaración de Seguridad (ST)

El documento, de contenido normalizado, que refleja el análisis y propiedades de seguridad del **objeto a evaluar**.

Puede incluir el cumplimiento de un Perfil de Protección (PP); especificación de seguridad aplicable a una clase de productos con objetivos de seguridad comunes. Elaborados por grupos de usuarios o cuerpos reguladores.



Niveles de aseguramiento EAL





Niveles de aseguramiento EAL

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
Guidance documents	AGD OPE	1	1	1	1	1	1	1
	AGD PRE	1	1	1	1	1	1	1
Life-cycle support	ALC CMC	1	2	3	4	4	5	5
	ALC CMS	1	2	3	4	5	5	5
	ALC DEL		1	1	1	1	1	1
	ALC DVS			1	1	1	2	2
	ALC FLR							
	ALC LCD			1	1	1	1	2
Security Target evaluation	ASE CCL	1	1	1	1	1	1	1
	ASE ECD	1	1	1	1	1	1	1
	ASE INT	1	1	1	1	1	1	1
	ASE OBJ	1	2	2	2	2	2	2
	ASE REQ	1	2	2	2	2	2	2
	ASE SPD		1	1	1	1	1	1
	ASE TSS	1	1	1	1	1	1	1
Tests	ATE COV		1	2	2	2	3	3
	ATE DPT			1	2	3	3	4
	ATE FUN		1	1	1	1	2	2
	ATE IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA VAN	1	2	2	3	4	5	5

Common Criteria v3.1

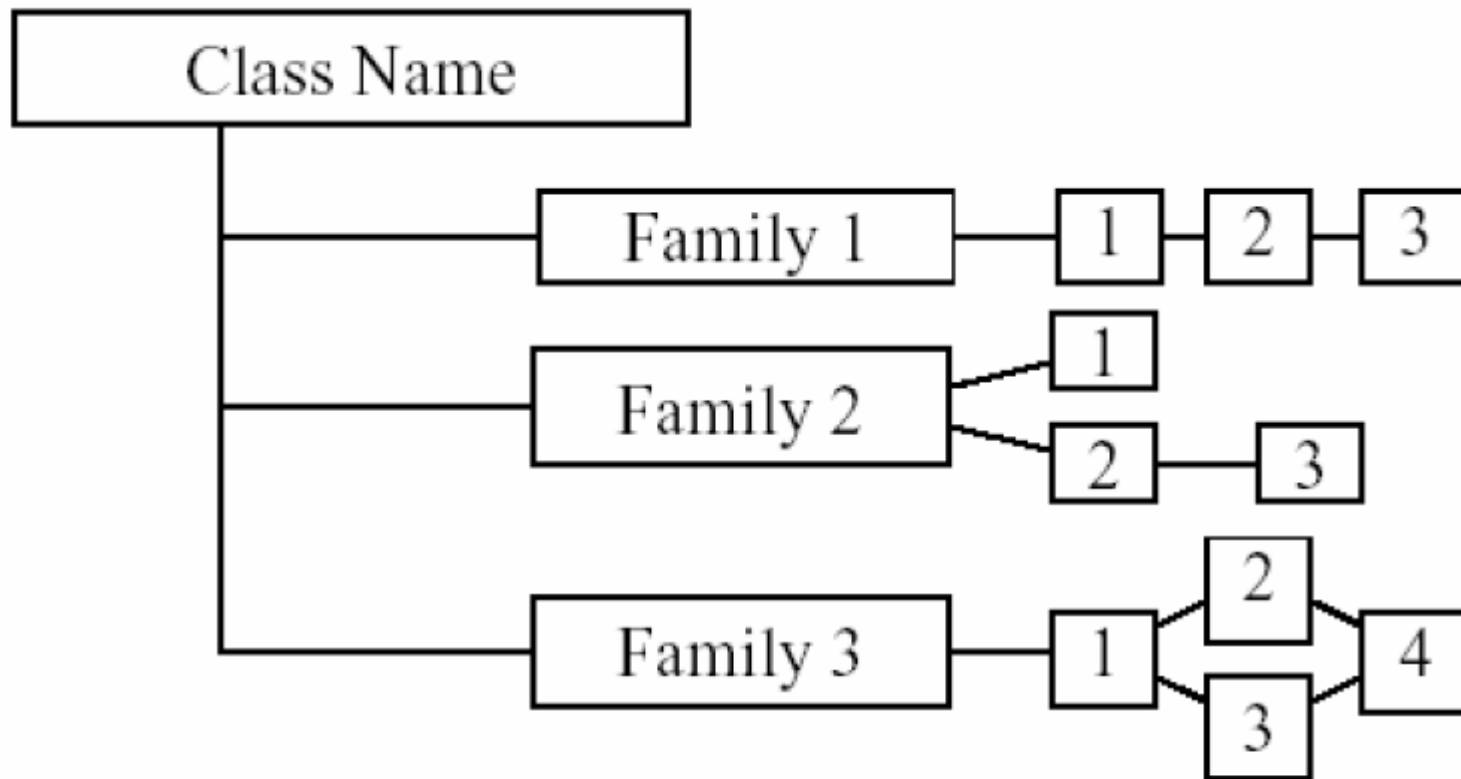


Requisitos funcionales

Con este paradigma de IT y su seguridad, se establece un catálogo de requisitos funcionales de seguridad, basados en la parte 2.

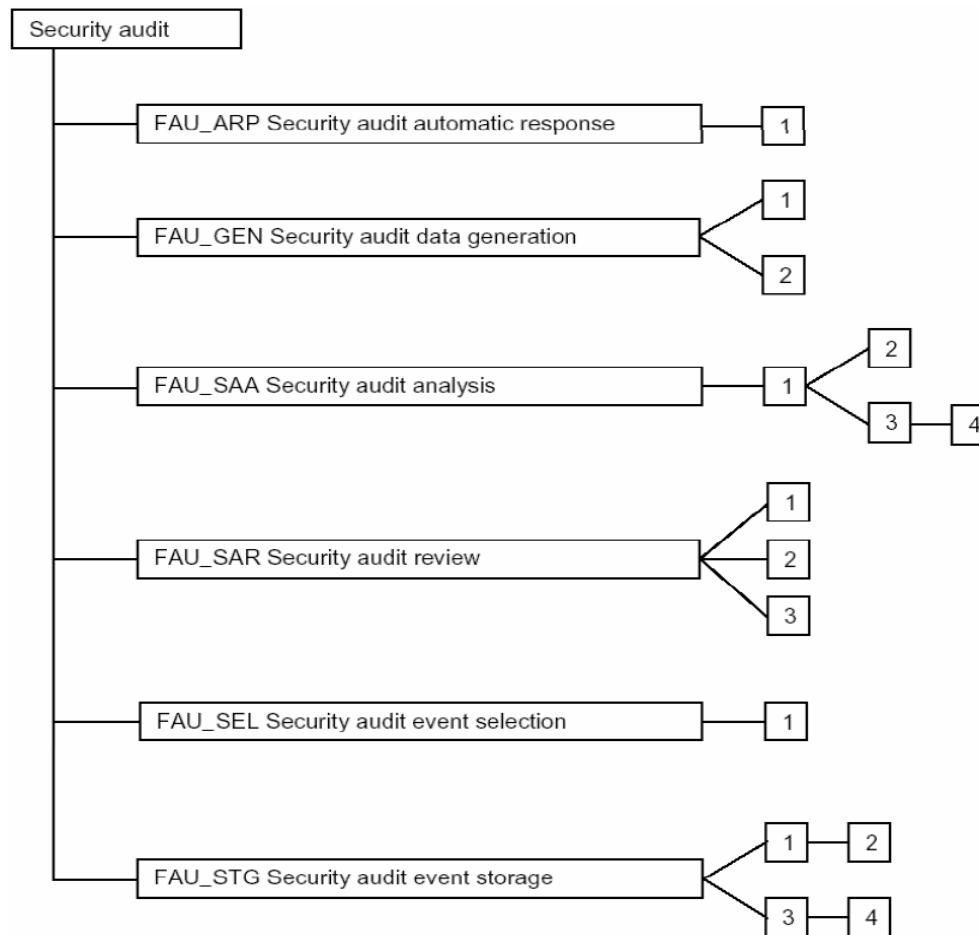


Requisitos funcionales





Requisitos funcionales





Requisitos funcionales

Security audit automatic response (FAU_ARP)

Family Behaviour

This family defines the response to be taken in case of detected events indicative of a potential security violation.

At FAU_ARP.1 Security alarms, the TSF shall take actions in case a potential security violation is detected.

Management: FAU_ARP.1

The following actions could be considered for the management functions in FMT:

the management (addition, removal, or modification) of actions.

Audit: FAU_ARP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

Minimal: Actions taken due to imminent security violations.

FAU_ARP.1 **Security alarms**
Hierarchical to: No other components.
Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 **The TSF shall take [assignment: *list of the least disruptive actions*] upon detection of a potential security violation**

Ejemplo Declaración de Seguridad



ADVANTIS CRYPTO 3.1 DECLARACIÓN DE SEGURIDAD VERSIÓN PÚBLICA

Versión: 1.2

18/08/2008

Referencia TI345



The banner features a wooden background with a compass on the left. The text reads: "IX JORNADA de SEGURIDAD INFORMÁTICA", "Monitoreo y Evolución de la Inseguridad Informática", and "Junio 17, 18 y 19 de 2009".

Ejemplo Declaración de Seguridad

Contenido:

- 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



Ejemplo Declaración de Seguridad

“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 Creación de Firma) y que determina un producto altamente resistente a diferentes ataques.”

*Common Criteria V.2.3

Ejemplo Declaración de Seguridad



5.1.1 Soporte Criptográfico (FCS)

5.1.1.1 Generación de claves criptográficas (FCS_CKM.1)

FCS_CKM.1.1 La TSF debe generar las claves criptográficas de acuerdo con el algoritmo de generación de claves criptográficas especificado [**rsagen1**]¹ ([10]) y con un tamaño de claves criptográficas especificado [**de 768 a 1984 bits**] que cumpla lo siguiente: [**requisitos de generación de número aleatorio trueran**] ([10])

5.1.1.2 Destrucción de claves criptográficas (FCS_CKM.4)

FCS_CKM.4.1 La TSF debe destruir las claves criptográficas en caso de regeneración de un nuevo SCD, de acuerdo con un método de destrucción de claves criptográficas especificado [**sobrescribir las claves con el valor 0**] que cumpla lo siguiente: [**ningún requisito especial**].

Ejemplo Declaración de Seguridad

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

Ejemplo Declaración de Seguridad

Certificado de Seguridad



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 (ej. "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-aaaa-aaaa-CER-nmm
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
Director del Centro Criptológico Nacional
Director 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.



Acercamiento para Colombia

Con el apoyo de Colciencias, el objetivo es:
Generar un modelo de acercamiento a Criterios Comunes para los productos software de Colombia, con el fin de mejorar su competitividad.



Acercamiento para Colombia

- Brecha de los producto software con EAL 1 y EAL 2.
 - Lista de Chequeo
<http://www.password.com.co/cc>
 - Modelo de implementación Criterios Comunes EAL1 y EAL2.



Comparativa con otros estándares





IX JORNADA de SEGURIDAD INFORMATICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2008

Organizational Innovation and Deployment Causal Analysis and Resolution	ML 5 Optimizing		Plus Critical Subprocesses	Plus Critical Subprocesses	
Organizational Process Performance Quantitative Project Management	ML 4 Quantitatively Managed				
Requirements Development Technical Solution Product Integration Verification Validation	ML 3 Defined				
Organizational Process Focus Organizational Process Definition +IPPD Organizational Training Integrated Project Management +IPPD Risk Management Decision Analysis and Resolution	ML 3 Defined				
Requirements Management Project Planning Project Monitoring and Control Supplier Agreement Management Measurement and Analysis Process and Product Quality Assurance Configuration Management	ML 2 Managed				
Generic Goal / Capability Level	1	2	3	4	5

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
Guidance documents	AGD OPE	1	1	1	1	1	1	1
	AGD PRE	1	1	1	1	1	1	1
Life-cycle support	ALC CMC	1	2	3	4	4	5	5
	ALC CMS	1	2	3	4	5	5	5
	ALC DEL		1	1	1	1	1	1
	ALC DVS			1	1	1	2	2
	ALC FLR							
	ALC LCD			1	1	1	1	2
	ALC TAT				1	2	3	3
Security Target evaluation	ASE CCL	1	1	1	1	1	1	1
	ASE ECD	1	1	1	1	1	1	1
	ASE INT	1	1	1	1	1	1	1
	ASE OBJ	1	2	2	2	2	2	2
	ASE REQ	1	2	2	2	2	2	2
	ASE SPD		1	1	1	1	1	1
Tests	ASE TSS	1	1	1	1	1	1	1
	ATE COV		1	2	2	2	3	3
	ATE DPT			1	2	3	3	4
	ATE FUN		1	1	1	1	2	2
Vulnerability assessment	AVA VAN	1	2	2	3	4	5	5



Nuestra Compañía

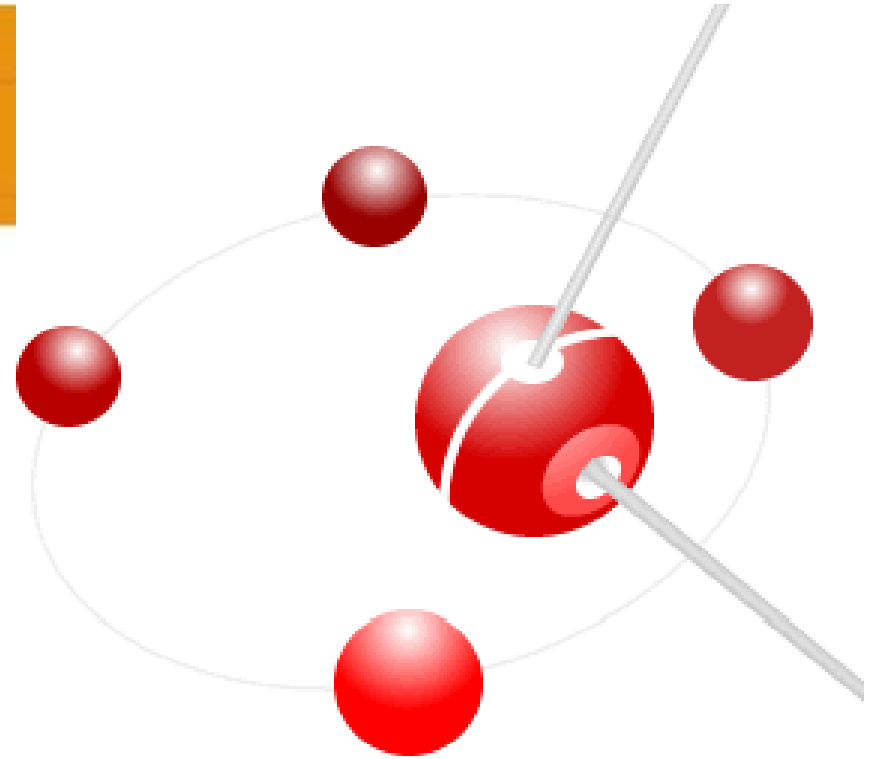


Consultoría en Seguridad Informática:

- ✓ Software
- ✓ Servidores
- ✓ Redes de Telecomunicaciones

- ✓ Acompañamiento en la implementación y certificación de Criterios Comunes





JOSE ALEJANDRO CHAMORRO LOPEZ
Consultor Seguridad de la Información
jose.chamorro@password.com.co
Móvil: 300 6611727



PASSWORD
SEGURIDAD INFORMÁTICA

SEGURIDAD INFORMÁTICA

