




**El estándar de seguridad ISO 15408 –
“Criterios Comunes”**

Ing. Eduardo Giménez, PhD



Agenda

- Que es y para que sirve este estándar
- Como se originó
- El proceso de evaluación
- Modelo de seguridad de los CC:
 - Perfil de Protección
 - Declaración de Seguridad
- Zoom sobre las exigencias de seguridad
 - Requisitos funcionales de seguridad
 - Garantías de seguridad
- Conclusiones



¿Que son los Criterios Comunes?

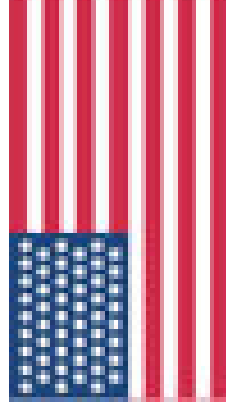
- Un estándar público para evaluar el nivel de seguridad que ofrece un producto vinculado a tecnologías de la información (software, hardware, firmware).
- Centrado en productos, más que en procesos.
- Centrado en lo técnico, más que en lo organizacional.
- Con vocación internacional: adaptable a diferentes métodos de evaluación y marcos legales.

¿Para que se utilizan los Criterios Comunes?

- Desarrollador de tecnología:
 - Ganar confianza en su producto de TI.
 - Argumento de marketing indispensable en ciertas áreas.
 - Tarjetas de crédito con microchip.
 - Pasaportes electrónicos.
 - Productos de criptografía (HSM, software de firma digital, etc).
- Comprador de tecnología:
 - Describir garantías mínimas de seguridad.
 - Poder comparar productos en licitaciones.
 - Base de requerimientos y exigencias estándar.
 - Reconocimiento internacional de certificados.
- Evaluador: una metodología para realizar evaluaciones de seguridad.

Un largo camino...

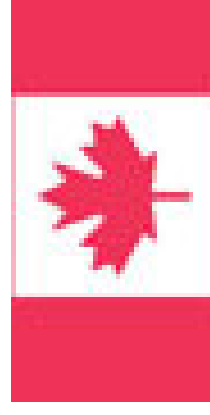
- **TCSEC (1985)**
 - Trusted Computer System Evaluation Criteria (U.S.)



- **ITSEC (1991)**
 - Information Technology Security Evaluation and Certification Scheme (Europe)



- **CTCPEC (1993)**
 - Canadian Trusted Computer Product Evaluation Criteria (Canada)



...hasta converger en los Criterios Comunes

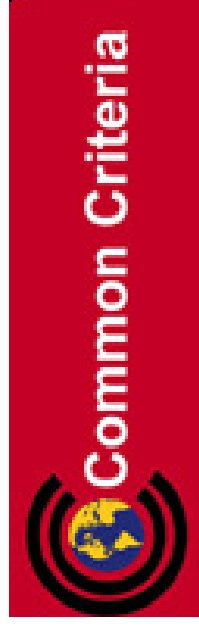
○ **TCSEC (1985)**



○ **ITSEC (1991)**



○ **CTCPEC (1993)**



(1998)

Acuerdo de reconocimiento mutuo



Ventajas:

- Evita pasar múltiples certificaciones en diferentes países.
- Simplifica la comparación de productos.
- Estandariza la expresión de requerimientos industriales.

Países integrados (Julio 2010):

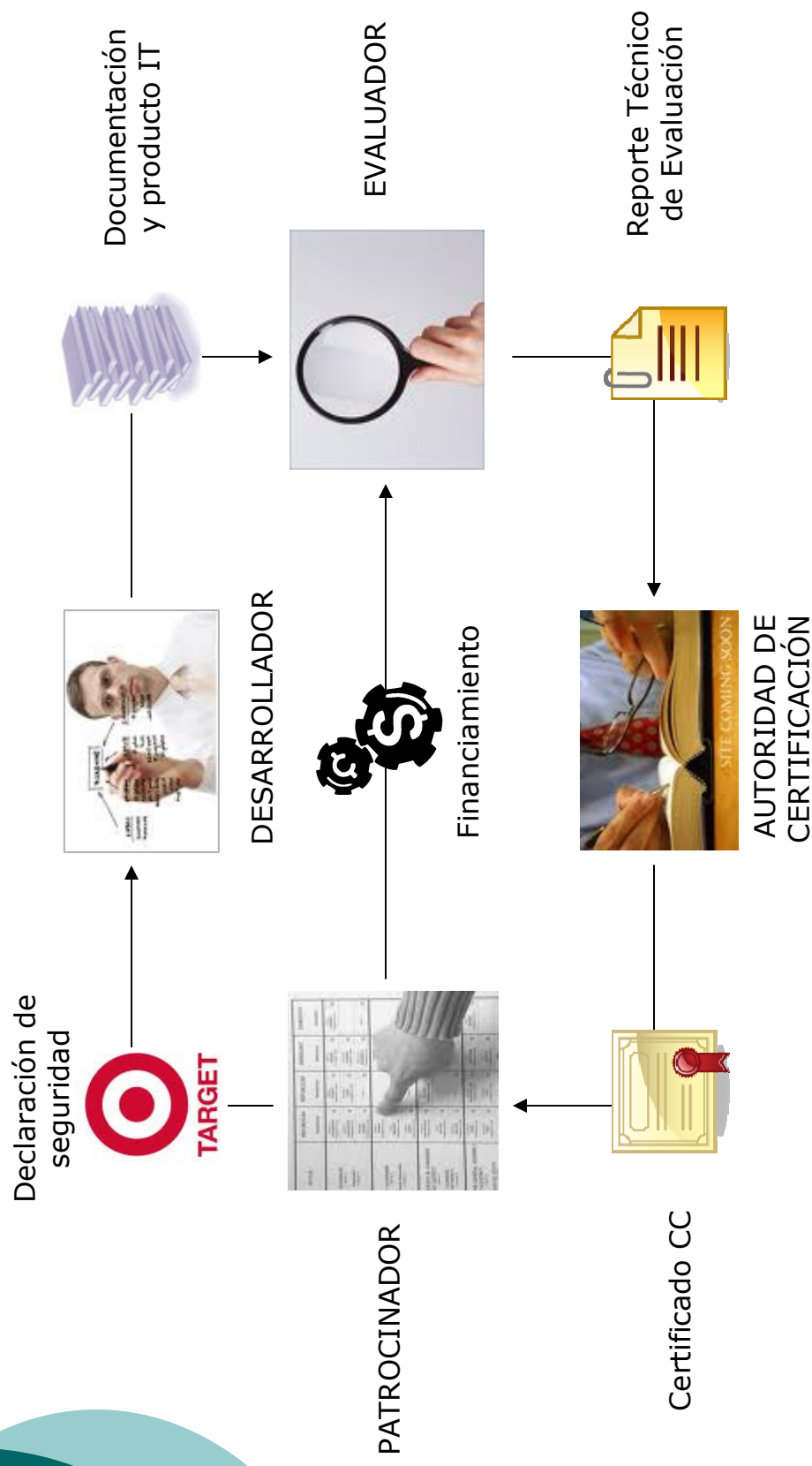
- Productores de certificados: Australia, Canadá, Francia, Alemania, Italia, Japón, Corea del Sur, Nueva Zelanda, Holanda, Noruega, España, Suecia, Reino Unido, Estados Unidos de América.
- Consumidores de certificados: Austria, República Checa, Dinamarca, Finlandia, Grecia, Hungría, India, Israel, Italia, Japón, Corea del Sur, Malasia, Holanda, Noruega, Pakistán, Singapur, España, Suecia, Turquía, Reino Unido, Estados Unidos de América.



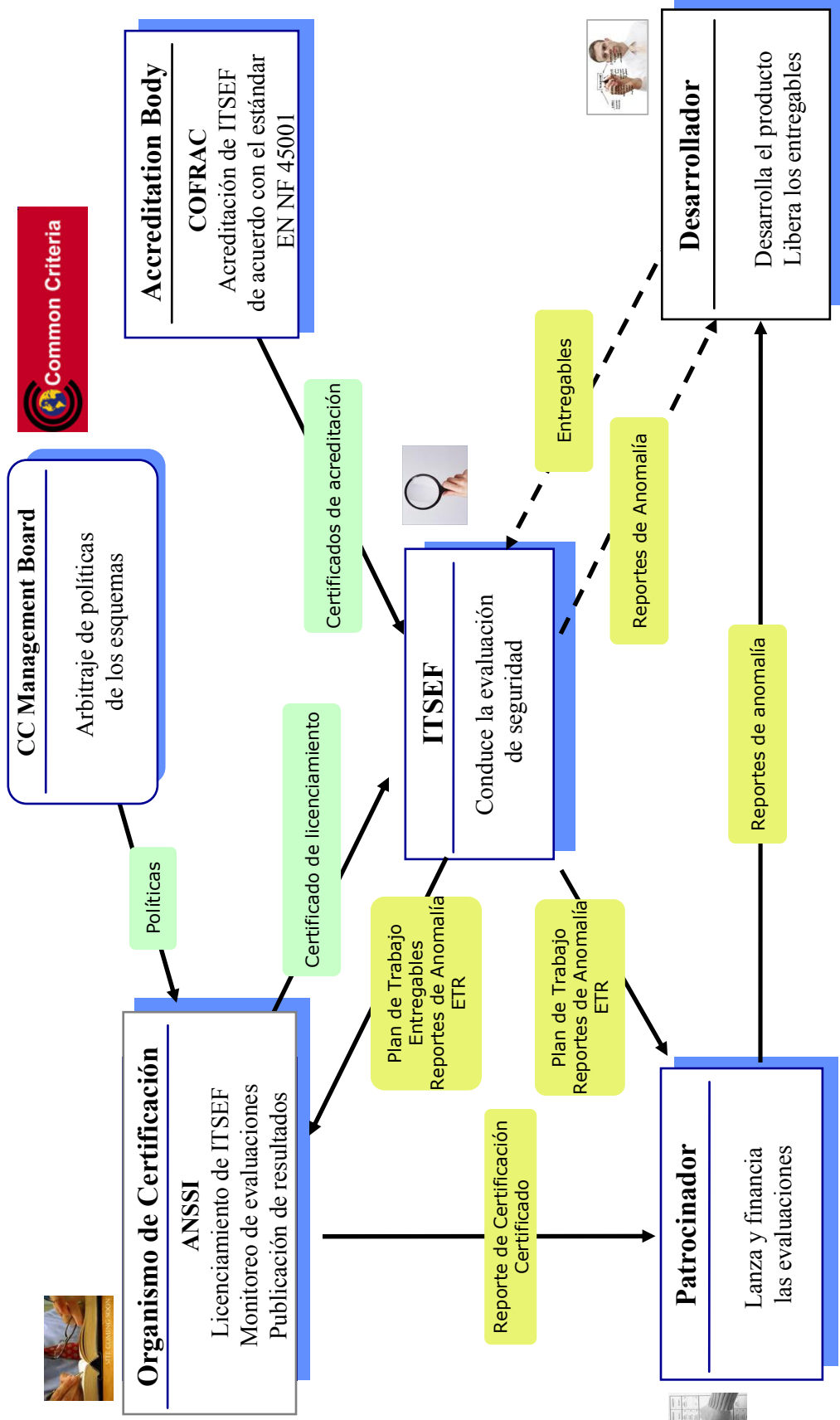
Agenda

- Que es y para que sirve este estándar
- Una breve historia del estándar
- El proceso de evaluación
- Modelo de seguridad de los CC:
 - Perfil de Protección
 - Declaración de Seguridad
- Zoom sobre las exigencias de seguridad
 - Requisitos funcionales de seguridad
 - Garantías de seguridad
- Conclusiones

Roles en una evaluación CC



Ejemplo: Esquema de certificación francés





Etapas en el proceso de certificación

1. Ajustar la seguridad del producto.
2. Elegir un esquema de certificación
3. Elegir un centro de evaluación del esquema.
4. Preparar la documentación y las evidencias de prueba.
5. Lanzar el proceso de evaluación
6. Hacer validar el Reporte de Evaluación por la Autoridad de Certificación y obtener el certificado.



¿Cuanto cuesta una certificación CC?

Tarea	Costo	Duración
Preparación	24 mes/h	10 meses
Evaluación	100k a 150k €	10 a 18 meses
Emisión del certificado	0 a 10% del costo de la evaluación	1 mes

Datos aproximados relativos a una aplicación Java Card para tarjeta inteligente comportando unas 30.000 líneas de código, utilizando un equipo desarrollo entrenado en evaluaciones CC y un laboratorio que conocía la plataforma de ejecución Java Card a través de evaluaciones previas.

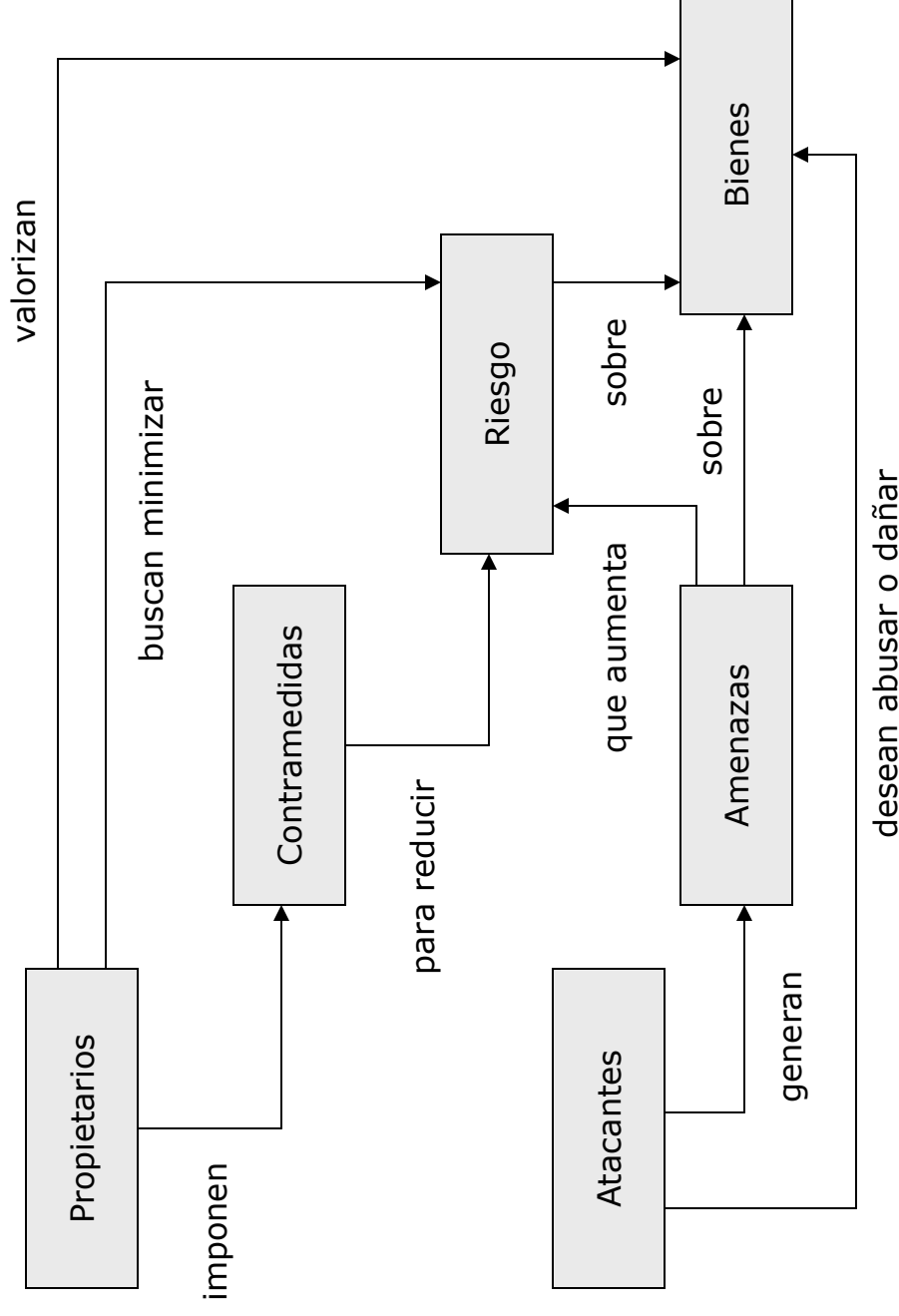


Agenda

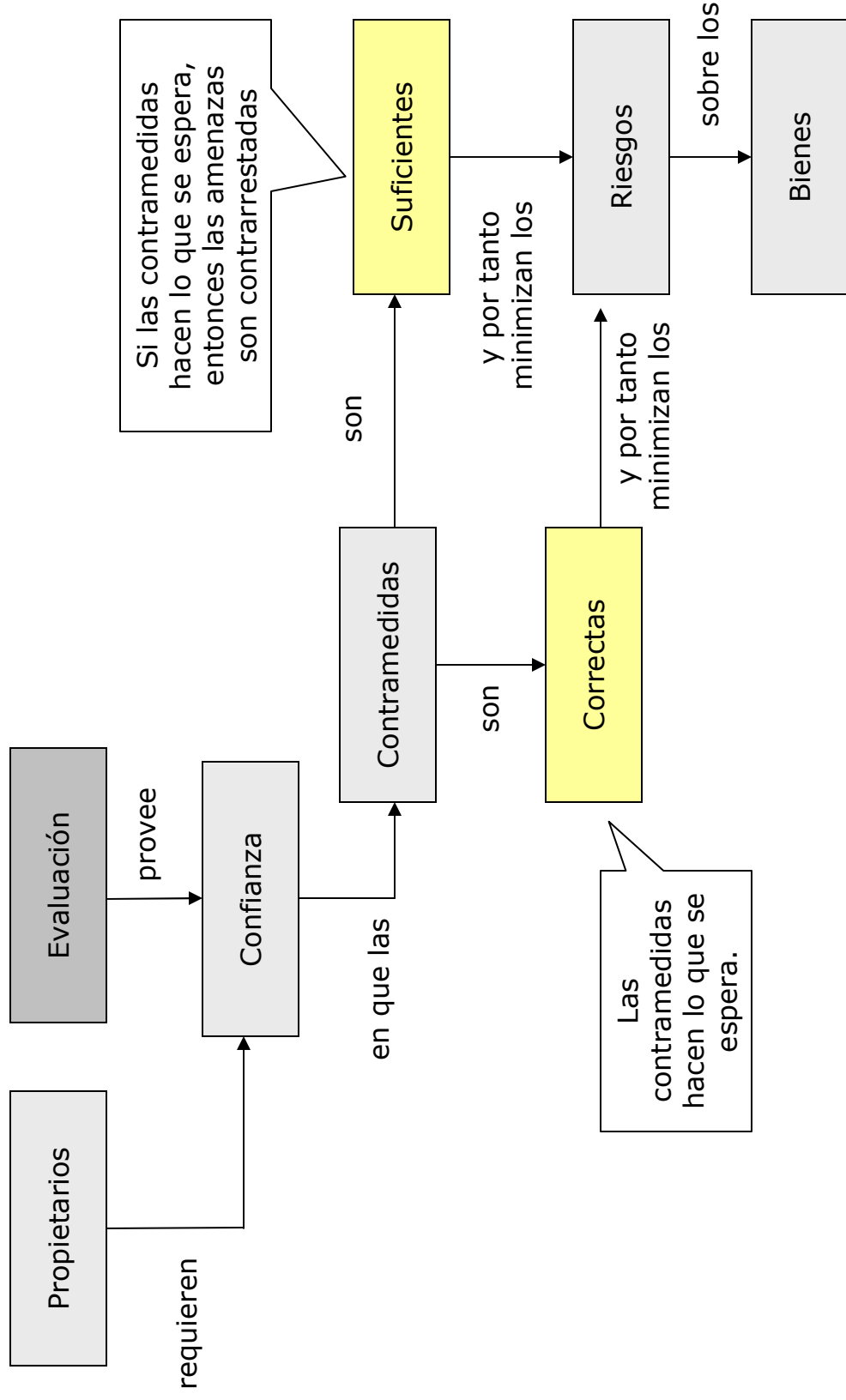
- Que es y para que sirve este estándar
- Una breve historia del estándar
- El proceso de evaluación
- Modelo de seguridad de los CC:
 - Perfil de Protección
 - Declaración de Seguridad
- Zoom sobre las exigencias de seguridad
 - Requisitos funcionales de seguridad
 - Garantías de seguridad
- Conclusiones



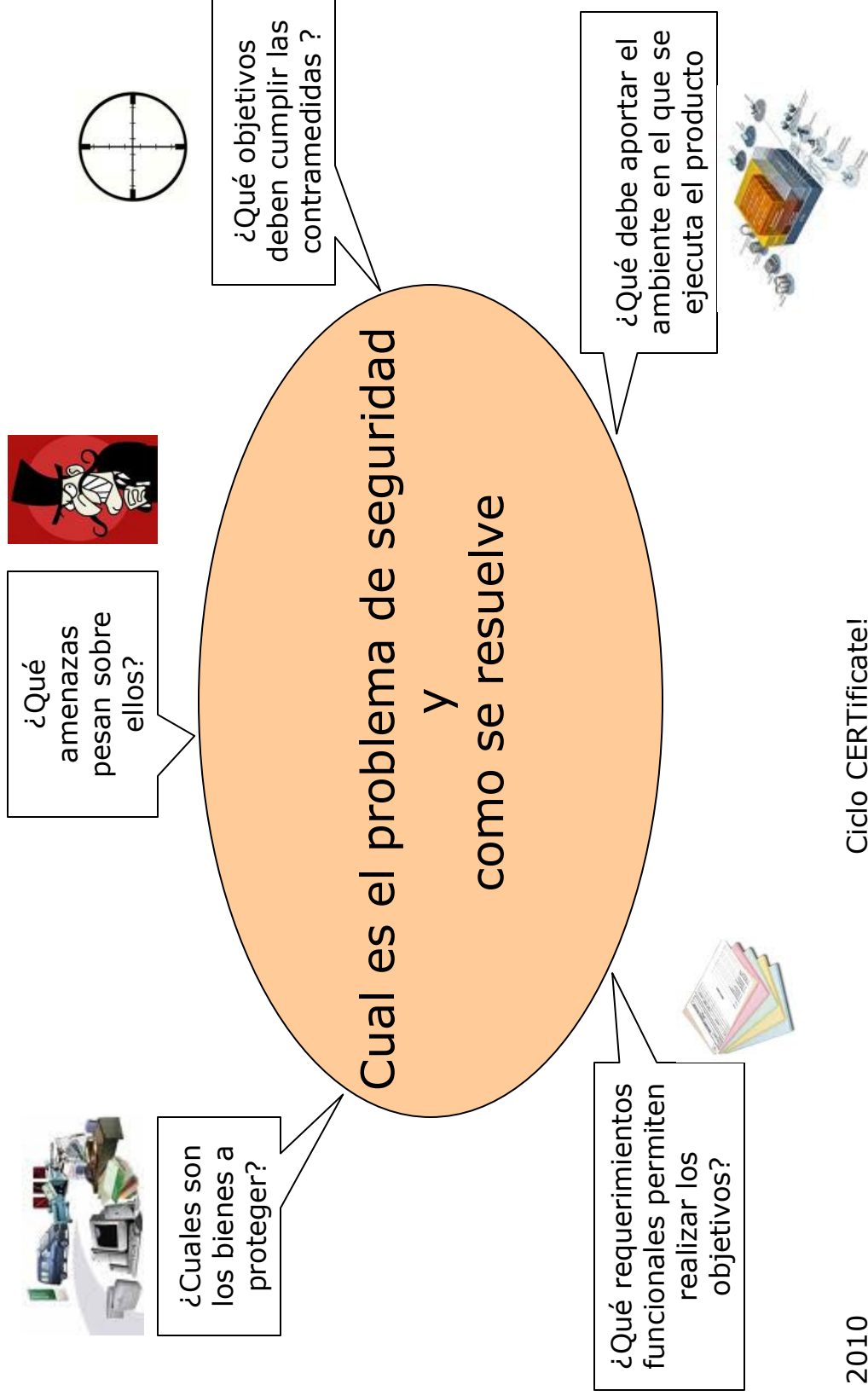
El modelo de seguridad de los CC



El modelo de seguridad de los CC



1: Suficiencia de las contramedidas



2: Corrección de las contramedidas

Como se gana confianza en su corrección:



- Examinando las diferentes representaciones del producto.



- Testeando el producto.



- Examinando la seguridad física del ambiente de desarrollo.



- Examinando los procedimientos de desarrollo, generación, liberación e instalación del producto.

Perfil de Protección (PP)



- Descripción de un problema de seguridad al cual responden una familia de productos.
- Resolución del problema independiente de toda implementación.
- Introduce las contramedidas necesarias y los requerimientos que pesan sobre ellas.
- Estructura, contenido y terminología altamente estandarizados.



Declaración de Seguridad (ST)

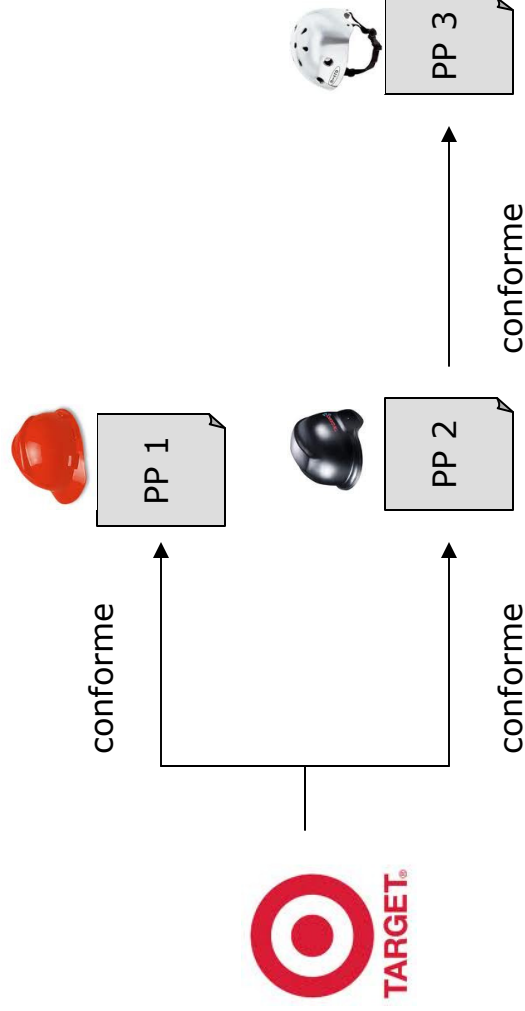


- Descripción de un problema de seguridad que es solucionado por un producto concreto.
- Demuestra que las contramedidas del producto son suficientes.
- Es el punto de partida de la evaluación de un producto.

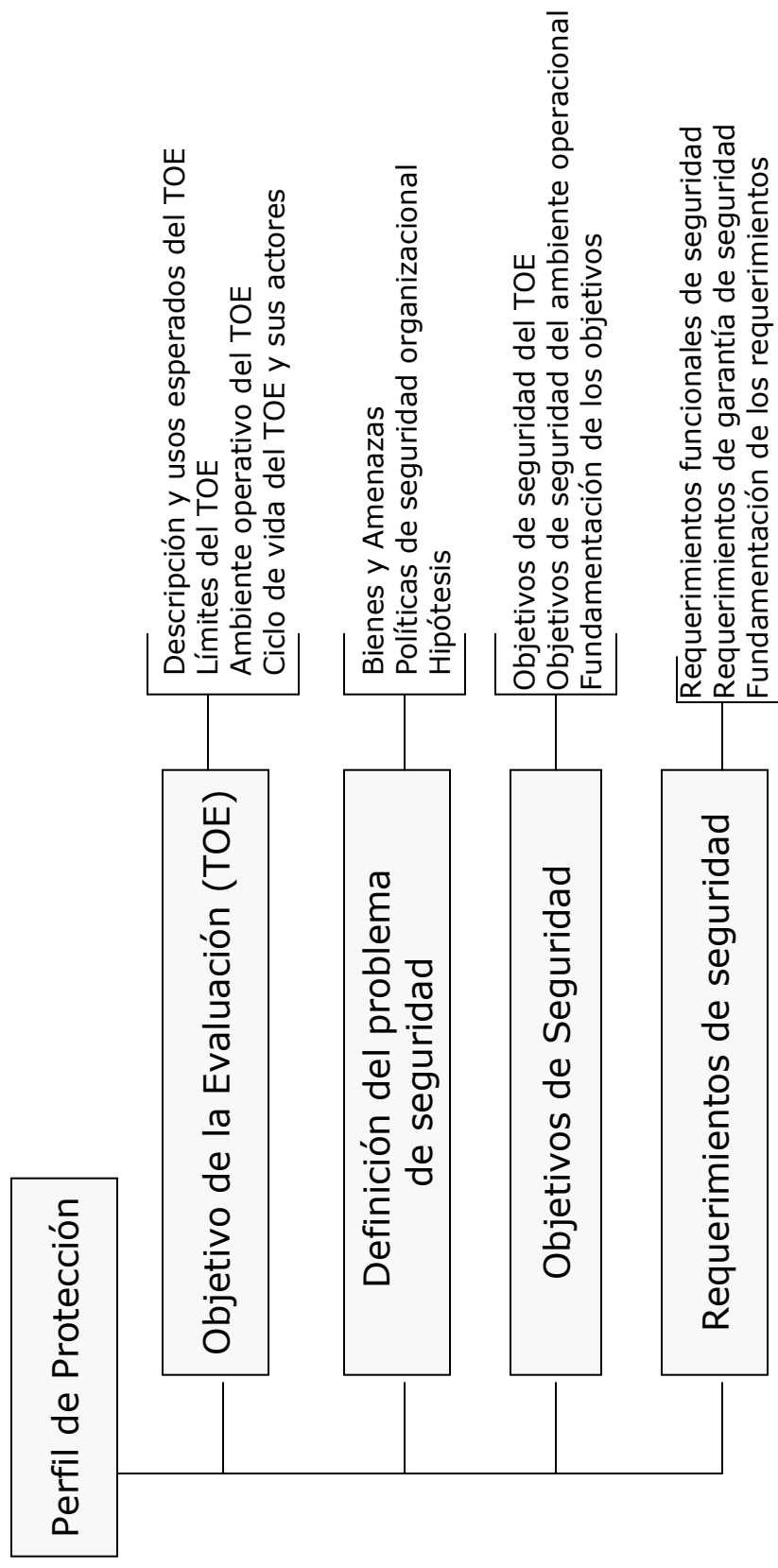


Relación entre ST y PP

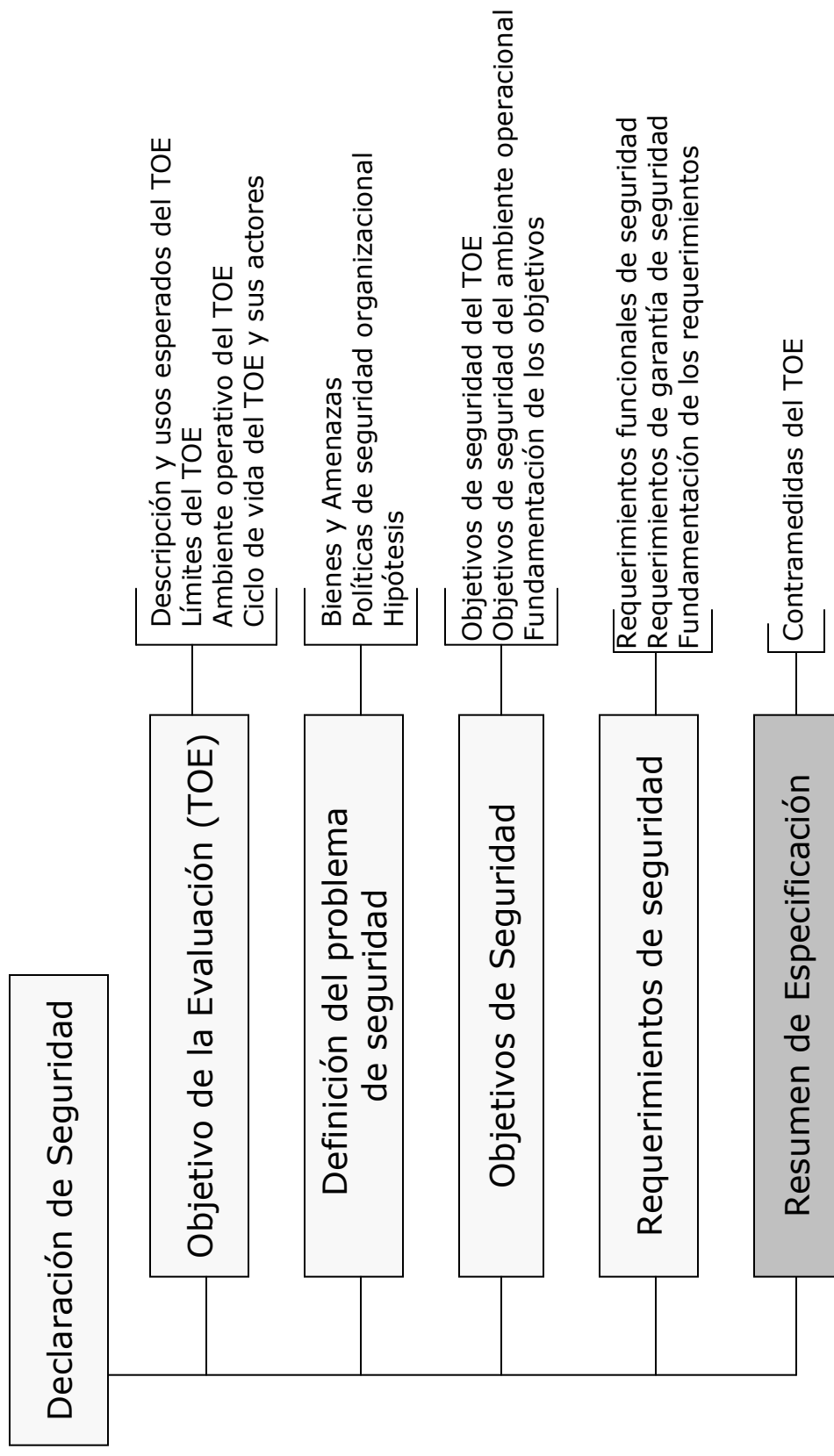
La Declaración de Seguridad de un producto puede reclamar la conformidad con uno varios Perfiles de Protección.



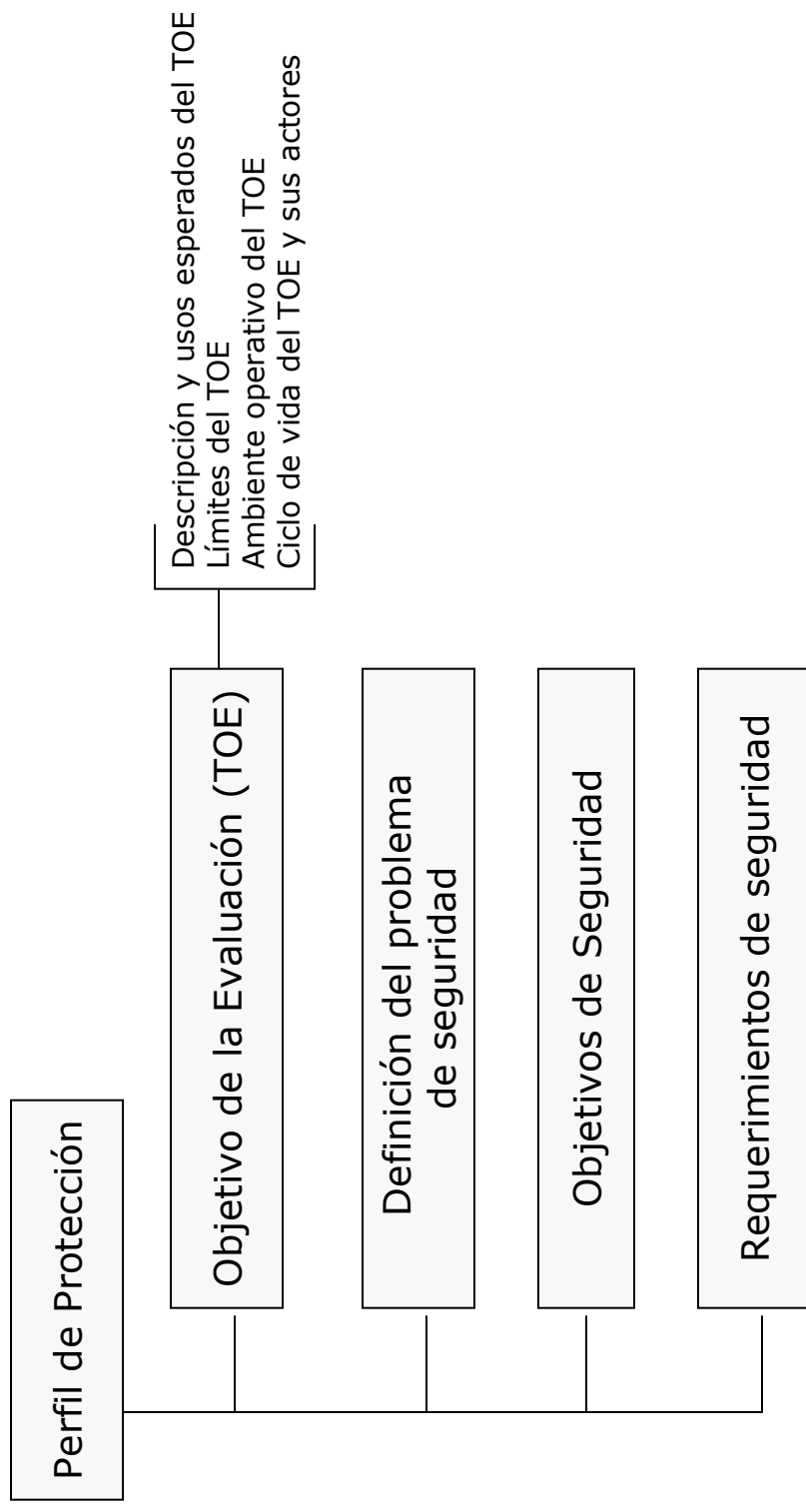
Contenido de un Perfil de Protección



Contenido de una Declaración de Seguridad



Contenido de un Perfil de Protección



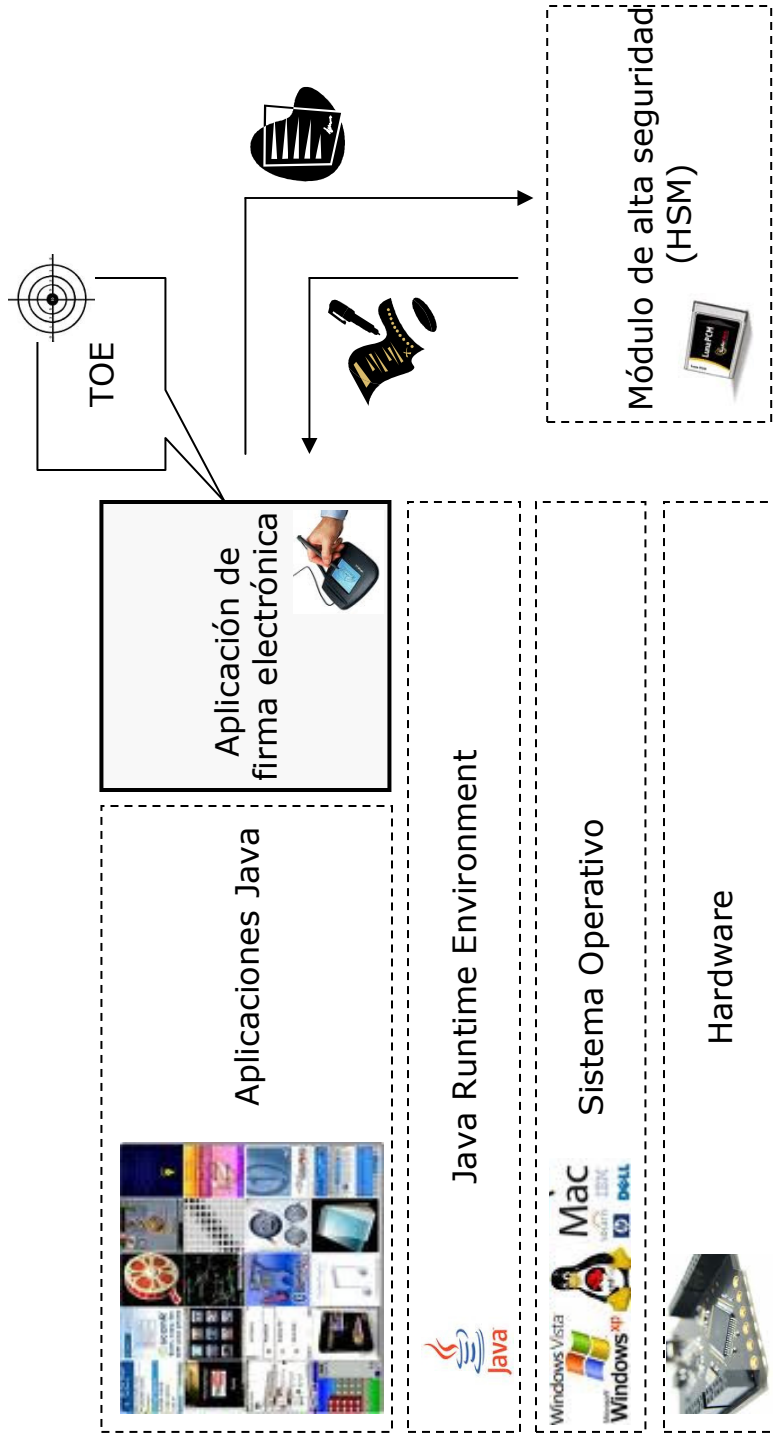


Objetivo de evaluación (TOE)



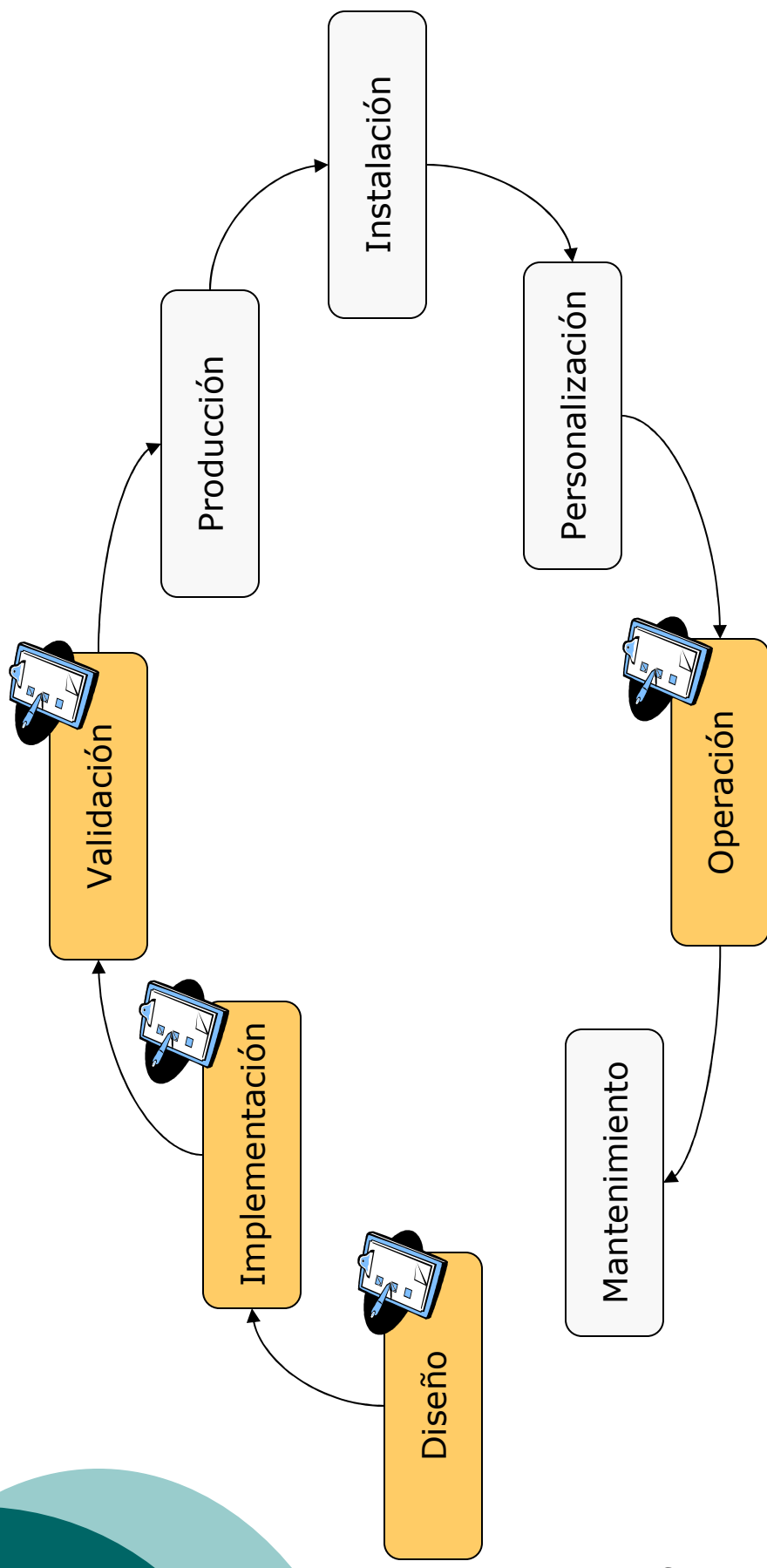
- Define cual es el alcance de la evaluación
- ¿Para que sirve el producto y como se utiliza?
- ¿Que parte del producto va a ser evaluada?
- ¿Cual es el ambiente operacional IT en el que se inscribe el producto?
- ¿En que fases de su ciclo de vida va a ser evaluado?
- ¿Que actores intervienen en ese ciclo de vida?

Ejemplo: aplicación de firma electrónica



Perfil de protección PP-ACSE-CCv3.1 de la ANSSI francesa

Ejemplo: ciclo de vida y evaluación



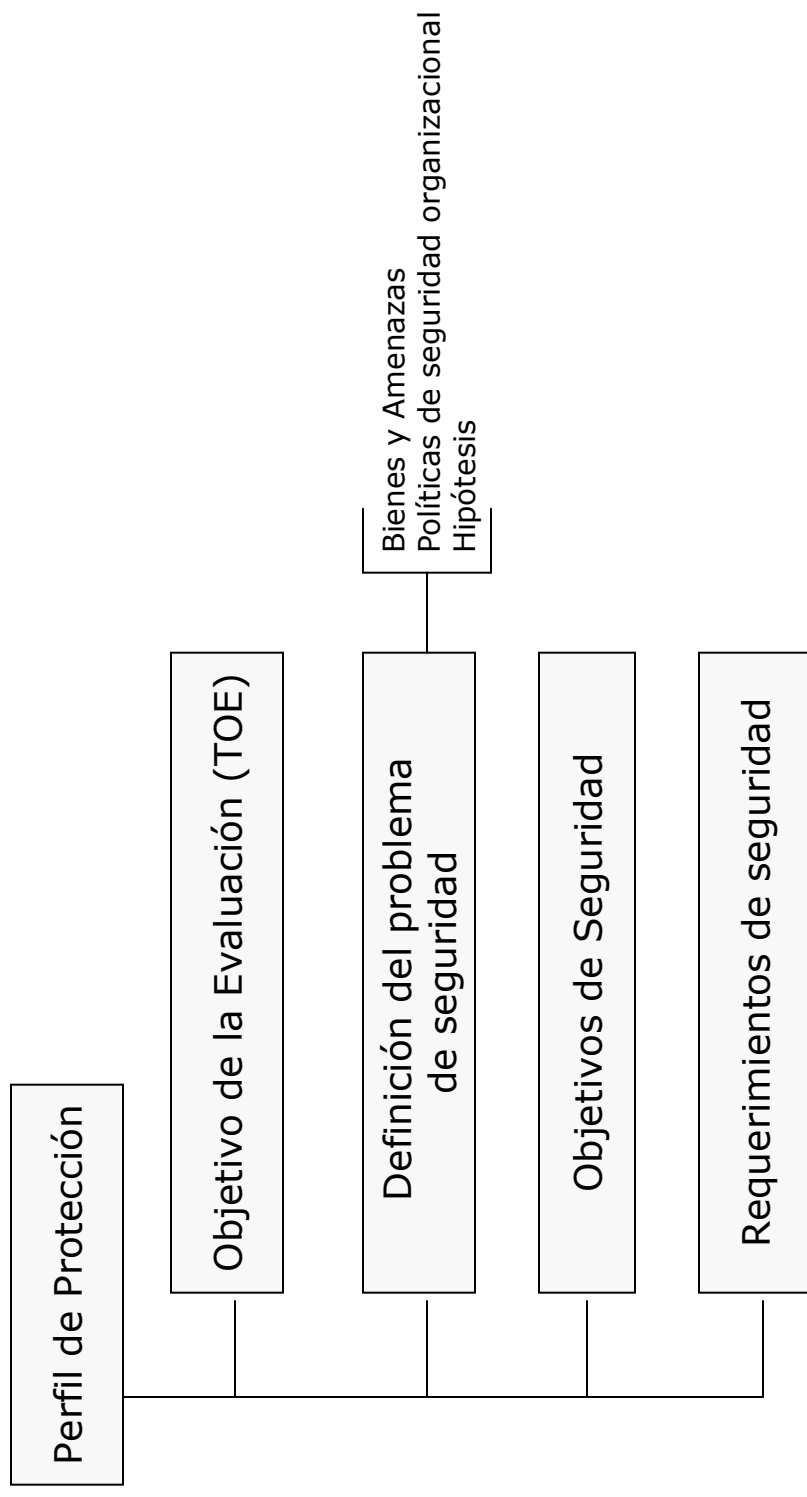
© Dr. Ing. Eduardo Giménez

Julio 2010

Ciclo CERTificate!



Contenido de un Perfil de Protección



Definición del problema de seguridad: Bienes

- Un bien es información que el TOE debe proteger.
- Ejemplos en nuestro caso de estudio:
 - Documento a ser firmado
 - Fecha y hora de la firma
 - Hash del documento y sus atributos
 - Firma electrónica



Definición del problema de seguridad: Amenazas

- Son acciones adversas realizadas por un atacante sobre los bienes.
- Ejemplos en nuestro caso de estudio:
 - “Un operador malicioso podría engañar al usuario acerca del documento que se le propone firmar.”
 - “El atacante podría interceptar el hash del documento a firmar cuando es transmitido al HSM, y reemplazarlo por el de otro documento.”



Definición del problema de seguridad:

Hipótesis

- Permiten acotar el alcance del problema a resolver.
- Ejemplos en nuestro caso de estudio:
 - “La plataforma sobre la que reposa la aplicación de firma (HW, OS, JRE) está bajo el control del firmante o de la organización a la que pertenece.”
 - “El HSM es capaz de autenticar a la aplicación de firma.”



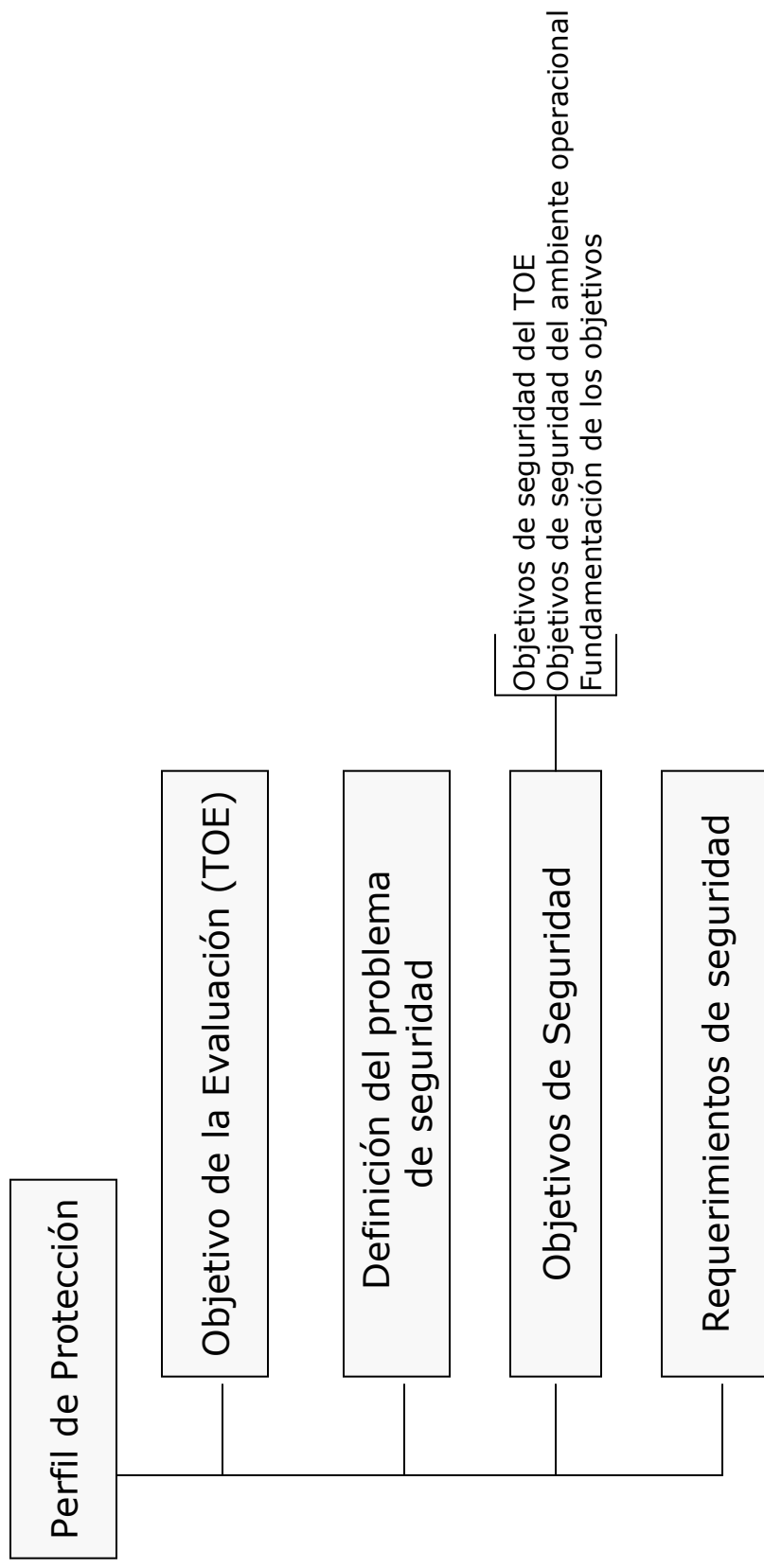
Definición del problema de seguridad: Políticas Organizacionales

- Describen reglas y procedimientos impuestos por una organización al ambiente operativo.
- Ejemplos en nuestro caso de estudio:
 - “Si la organización del signatario mantiene copias de su clave privada fuera del HSM, las mismas deben ser almacenadas en un lugar físico que asegure el mismo nivel de confidencialidad, y al que solo debe tener acceso dicha organización.”





Contenido de un Perfil de Protección



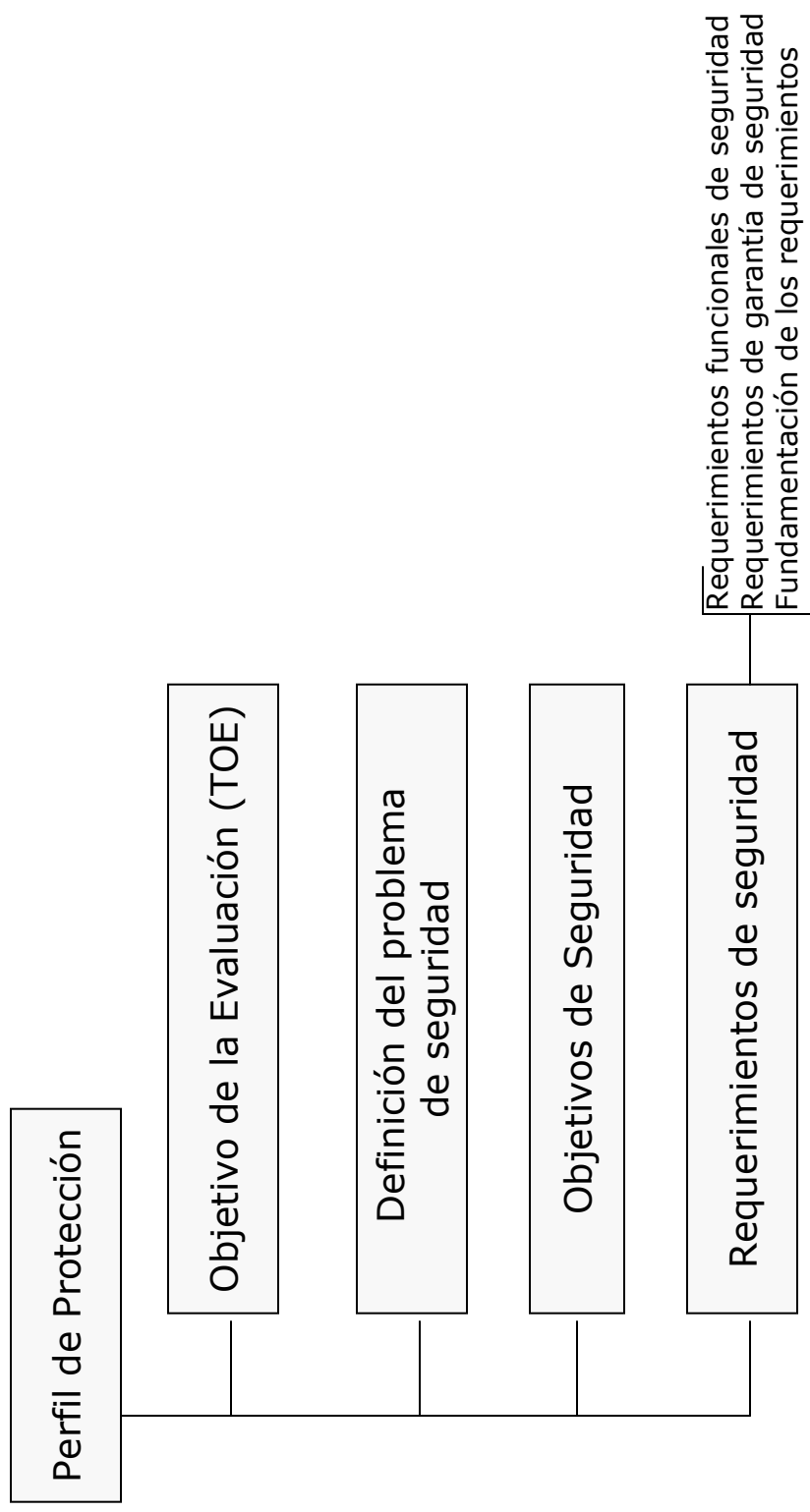


Objetivos de seguridad

- Son un enunciado conciso y abstracto de las propiedades que debe satisfacer la solución al problema de seguridad.
- Ejemplos en nuestro caso de estudio:
 - “El TOE debe presentar al signatario una representación exacta del documento a firmar.”
 - “El HSM y el TOE deben comunicar a través de un canal seguro que asegure autenticación mutua e integridad de los mensajes.”
- Debe fundamentarse que son consistentes y suficientes para contrarrestar las amenazas y resolver el problema de seguridad.



Contenido de un Perfil de Protección



Requerimientos de seguridad



- Requerimientos funcionales de seguridad (SFR)
 - Conciernen las funcionalidades del TOE.
 - Traducción de los objetivos del TOE en un lenguaje estandarizado.
 - Los CC proveen un amplio catálogo de requerimientos.
- Requerimientos de garantía de seguridad (SAR)
 - Conciernen el proceso de desarrollo del TOE.
 - Describen cómo la TOE debe ser evaluada.
 - Permiten ganar confianza en que los requerimientos funcionales han sido correctamente implantados.
- Fundamentación respecto a los objetivos de seguridad.

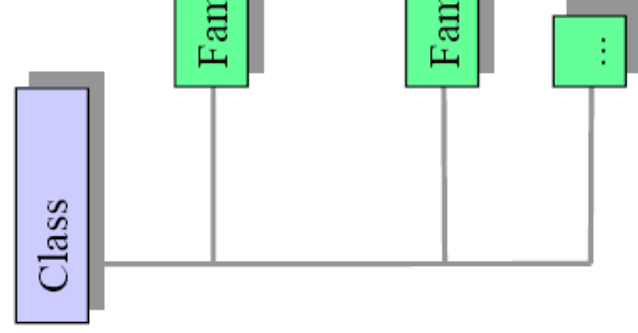


Agenda

- Que es y para que sirve este estándar
- Como se originó
- El proceso de evaluación
- Modelo de seguridad de los CC:
 - Perfil de Protección
 - Declaración de Seguridad
- Zoom sobre las exigencias de seguridad
 - Requisitos funcionales de seguridad
 - Garantías de seguridad
- Conclusiones

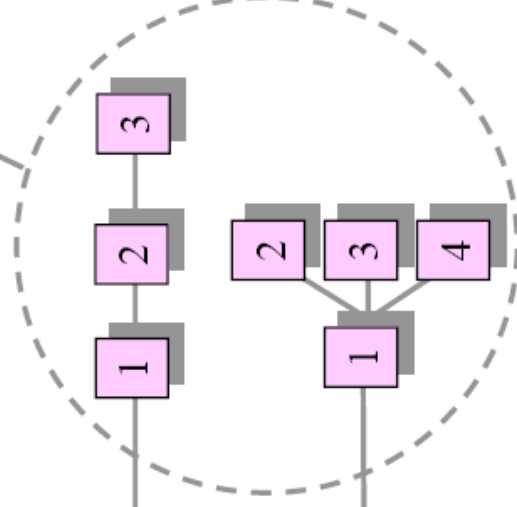
Requerimientos: estructura jerárquica

Un grupo de familias que comparten una misma temática.

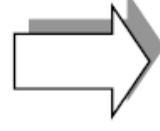


Un grupo de componentes que comparten los mismos objetivos de seguridad pero difieren en énfasis o fortaleza.

Components
↳ Dependencies
↳ Operations



El conjunto de elementos seleccionables que pueden ser incluidos en un PP o ST.

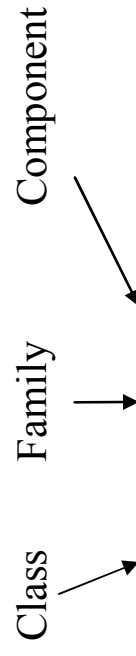


Aplica para requerimientos funcionales y garantías de seguridad

Las 11 clases de SFR

- FAU: Audit
- FCS: Cryptographic support
- FCO: Communications
- FDP: User data protection
- FIA: Identification and Authentication
- FMT: Security Management
- FPR: Privacy
- FPT: Protection of the TOE security functions
- FRU: Resource Utilisation
- FTA: TOE access
- FTP: Trusted Paths/Channels

Requerimiento funcional de seguridad



FDP_UIT.1 Data Exchange Integrity

Dependencies:

(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)

Component Element

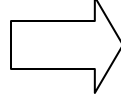


FDP_UIT.1.1 The TSF shall enforce the [assignment: access or information control policy] to be able to [selection: transmit, receive] user data in a manner protected from [selection: modification, deletion, insertion, replay] errors.

Requerimiento funcional de seguridad:

Ejemplo

- El HSM y el TOE deben comunicar a través de un canal seguro que asegure autenticación mutua e integridad de los mensajes.



- **FDP_UIT.1.1/SC** The TSF shall enforce the **signature generation information flow control policy** to be able to **transmit and receive** user data in a manner protected from **modification, insertion and replay** errors.

Requerimiento funcional de seguridad: Ejemplo de refinamiento

- FCS_COP.1 The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].
- FCS_COP.1/DocHash The TSF shall perform computation of the document's hash in accordance with a specified cryptographic algorithm [selection: SHA256 or RIPEMD160] and cryptographic key sizes (none) that meet the following: [selection: FIPS 180-2 or ISO/IEC10118:2003].



Agenda

- Que es y para que sirve este estándar
- Como se originó
- El proceso de evaluación
- Modelo de seguridad de los CC:
 - Perfil de Protección
 - Declaración de Seguridad
- Zoom sobre las exigencias de seguridad
 - Requisitos funcionales de seguridad
 - Garantías de seguridad
- Conclusiones

El paradigma de la confianza

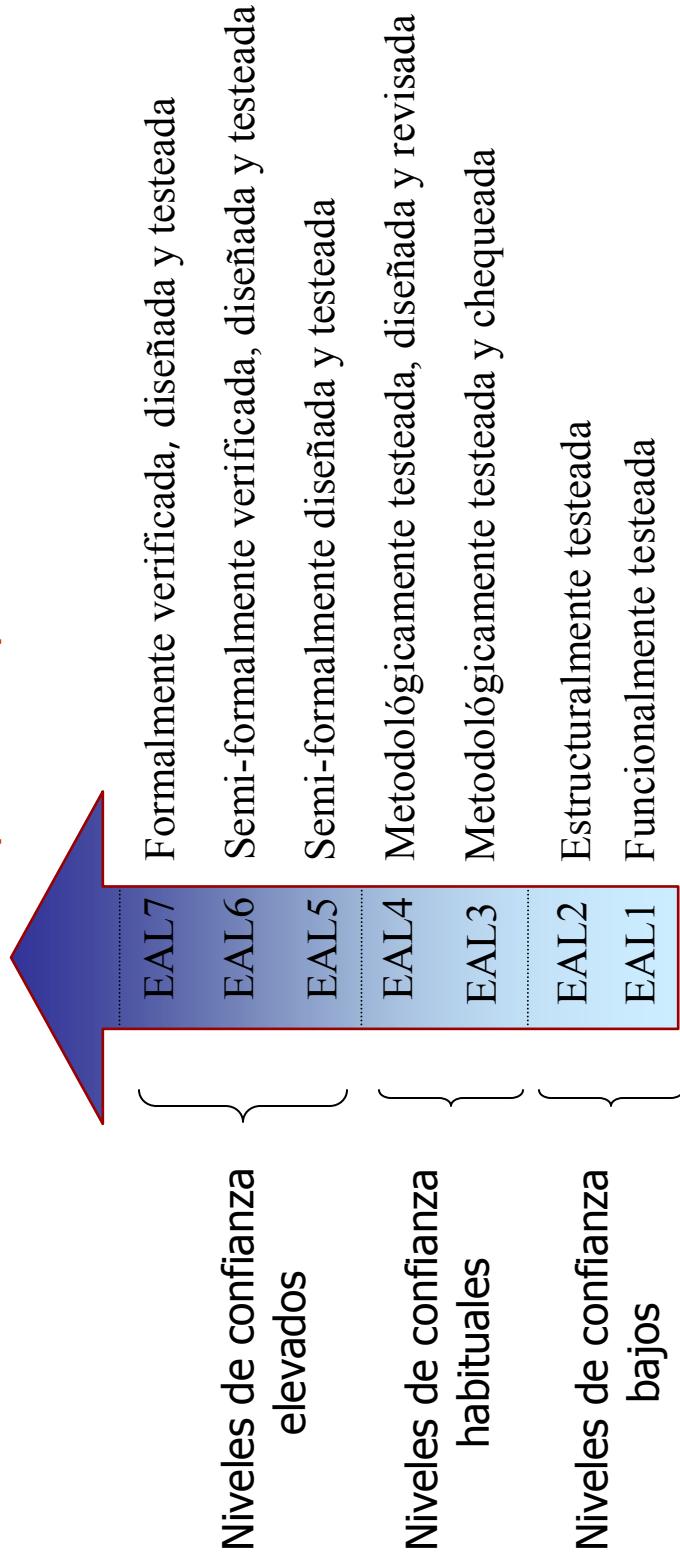



- Objetivos: ganar confianza en que la implementación de las contramedidas es correcta, reducir vulnerabilidades.
- La confianza se gana mediante la evaluación del producto IT y de su documentación (evaluación = investigación activa)
- A mayor esfuerzo de evaluación, mayor confianza.
- Nivel de esfuerzo depende de tres variables:
 - **Alcance:** porción de producto que es inspeccionada
 - **Profundidad:** nivel de detalle requerido para la evidencia
 - **Rigor:** tipo de lenguaje utilizado para describir el TOE

Niveles de confianza predefinidos

Una escala incremental, construida a partir de componentes de confianza.

Objetivo: balancear el nivel de confianza con el costo y la factibilidad para adquirirla.





Requerimientos de garantía de seguridad (SAR)

- Cada componente de confianza está formado por un conjunto de elementos de confianza que constituyen el requerimiento de seguridad.
- Un elemento de confianza puede ser de tres tipos:
 - **Acción del desarrollador (D)**: lo que debe de hacer el Desarrollador par aumentar la confianza.
 - **Contenido y presentación de evidencia (C)**: el tipo de evidencia requerida para la evaluación, lo que la misma debe demostrar, que información debe contener.
 - **Acción del Evaluador (E)**: las actividades de investigación que debe realizar el Evaluador.



Componentes de confianza



- Clase ADV: Desarrollo
- Clase ATE: Testeo Funcional
- Clase AGD: Manuales
- Clase ALC: Soporte al ciclo de vida del producto
- Clase AVA: Análisis de Vulnerabilidades

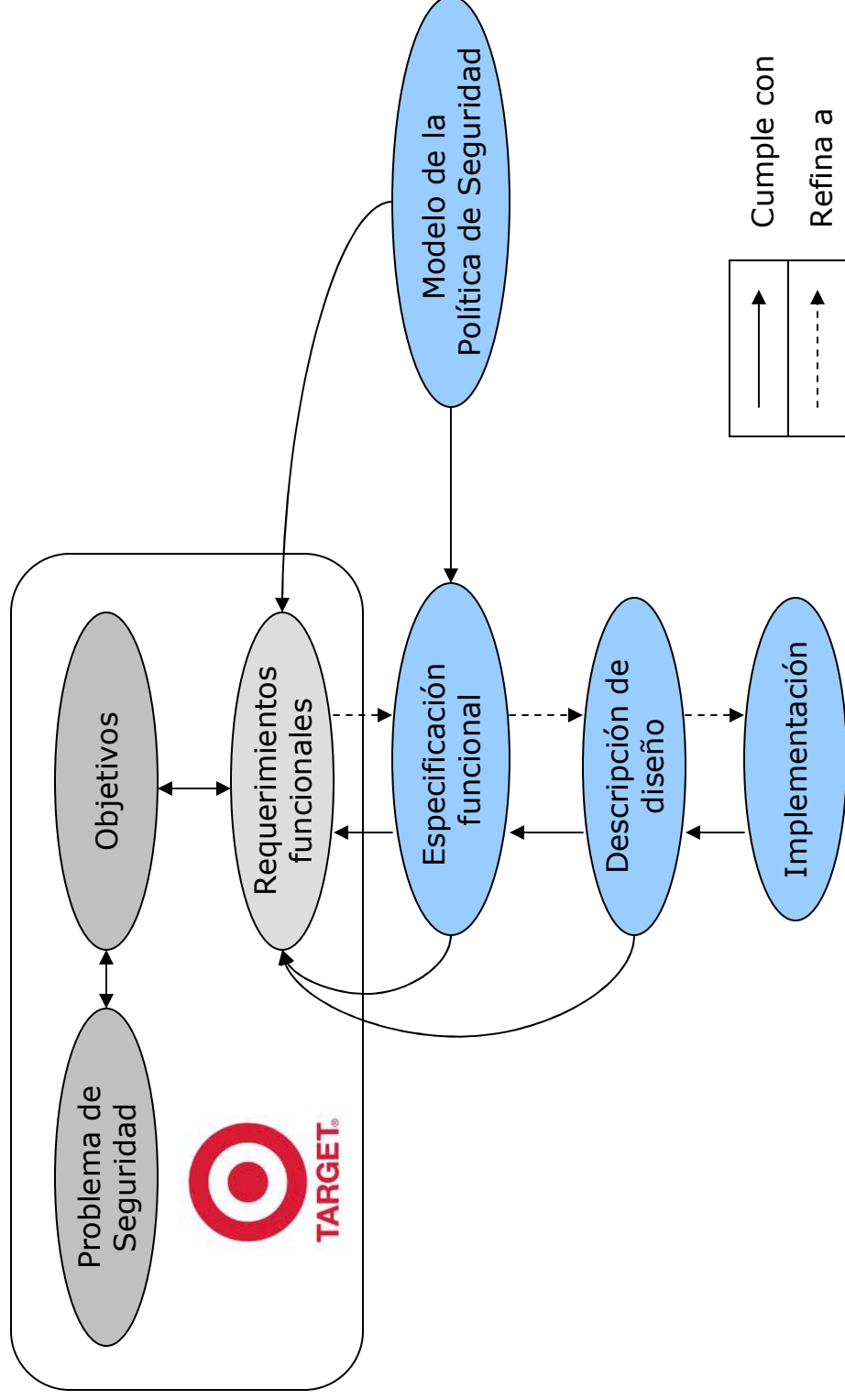
Componentes de confianza: Desarrollo (ADV)

- Familias de requerimientos:
 - ADV_SPM: Modelado de Políticas de Seguridad
 - ADV_FSP: Especificación Funcional
 - ADV_TDS: Diseño del TOE
 - ADV_IMP: Implementación
 - ADV_ARC: Arquitectura de Seguridad
 - ADV_INT: Estructura interna de las TSF

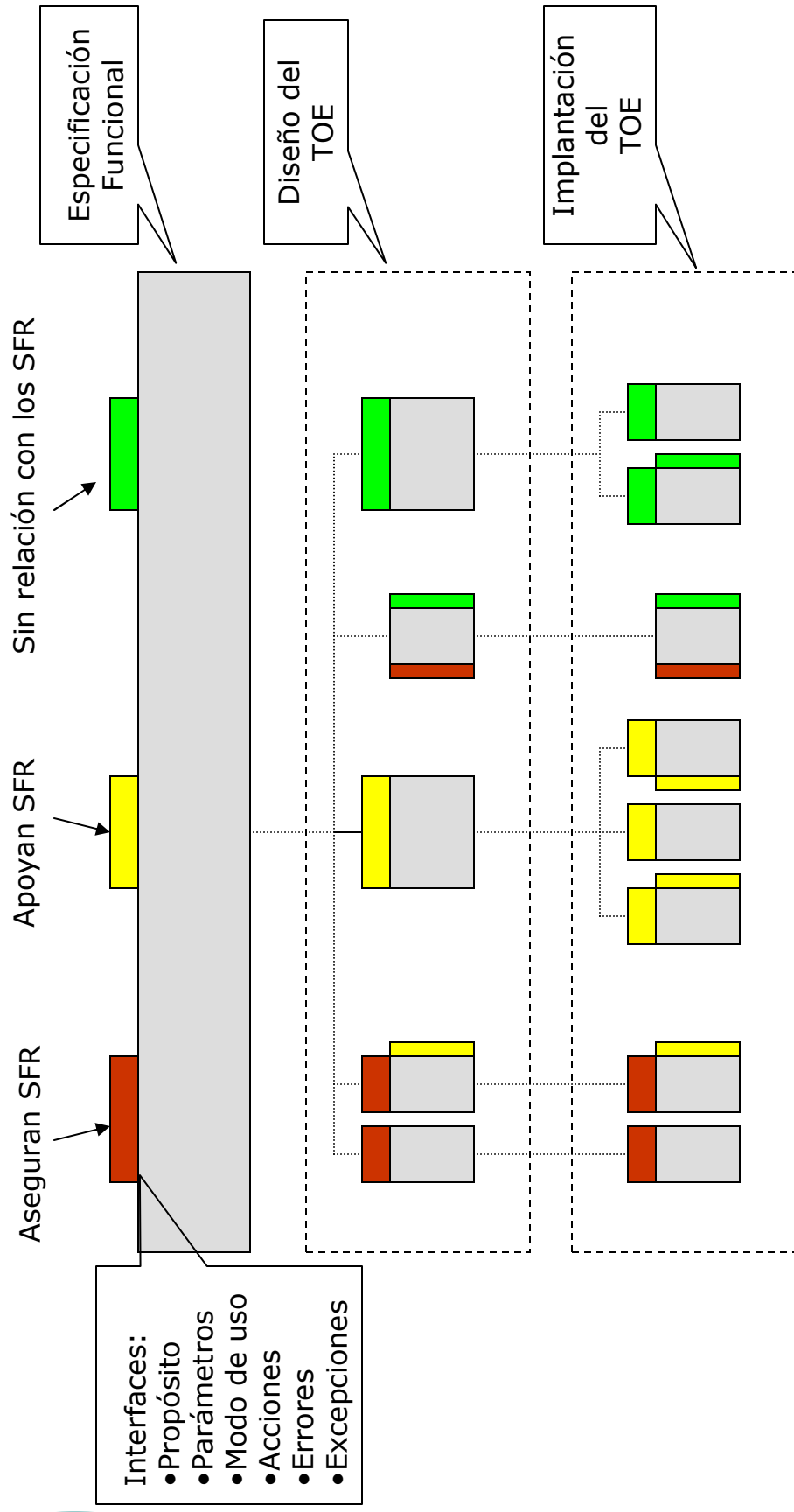


- Dos objetivos:
 - Las contramedidas funcionan como se especificó.
 - Las contramedidas no pueden ser evitadas o corrompidas.

Desarrollo (ADV): Relaciones entre representaciones



Desarrollo (ADV): Representaciones del código del TOE





Desarrollo (ADV): Nivel de confianza en la evaluación

- Alcance:
 - Evaluación en caja negra (especificación funcional)
 - Evaluación en caja gris (arquitectura en sistemas)
 - Evaluación en caja blanca (fuentes del programa)
- Detalle:
 - Todos los errores o solo los relevantes para seguridad
 - Solo las interfaces que aseguran SFR o todas
- Rigor:
 - Lenguaje informal, semi-formal o formal.



Desarrollo (ADV): Arquitectura de Seguridad

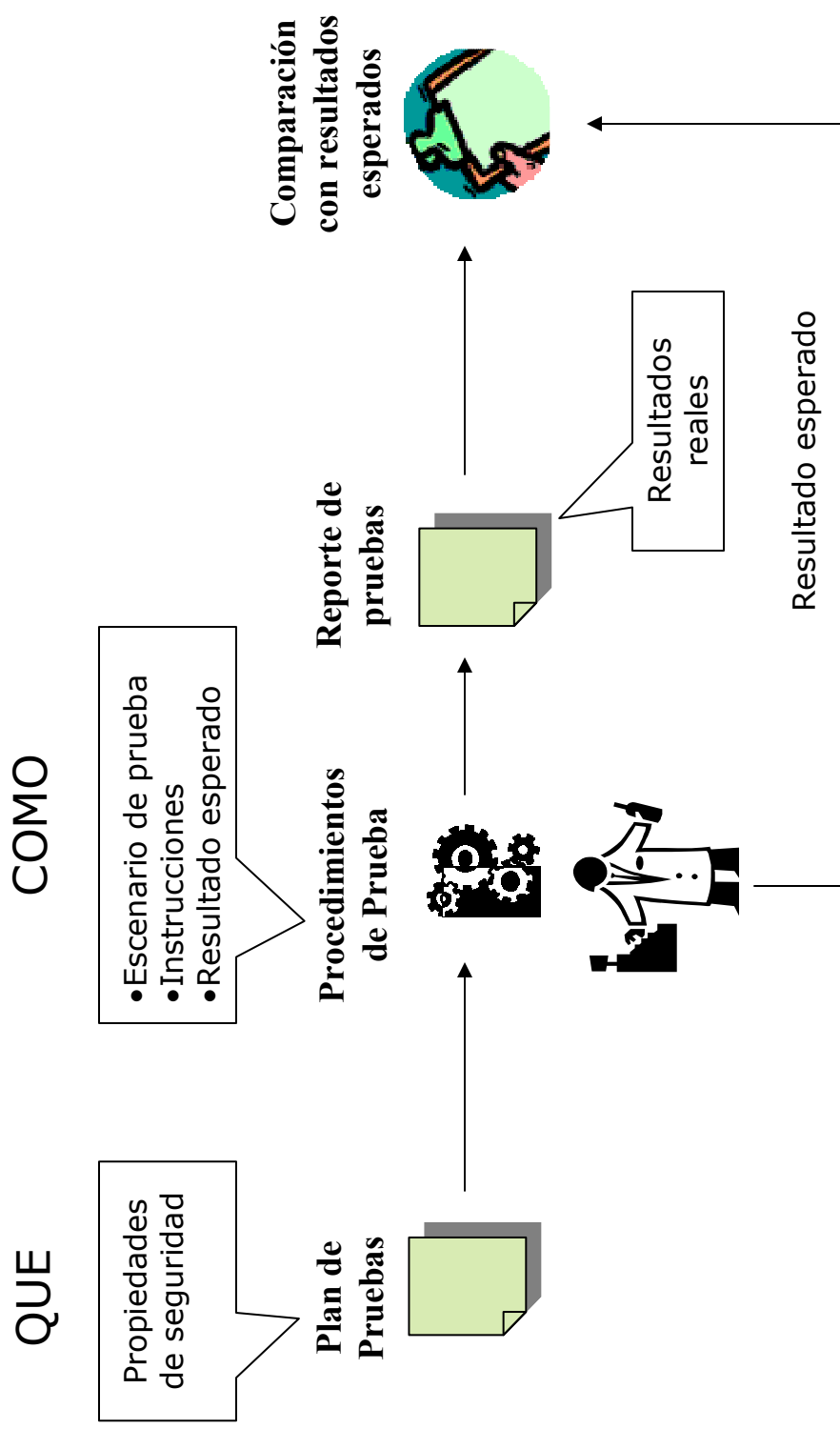
- Análisis de vulnerabilidades desde la perspectiva del Desarrollador.
- Describe los “dominios de seguridad” del TOE.
- Estudia propiedades de seguridad transversales:
 1. El proceso de inicialización del TOE es seguro.
 2. Las contramedidas no puede ser eludidas.
 3. Las contramedidas se protegen contra la manipulación del TOE por agentes hostiles.



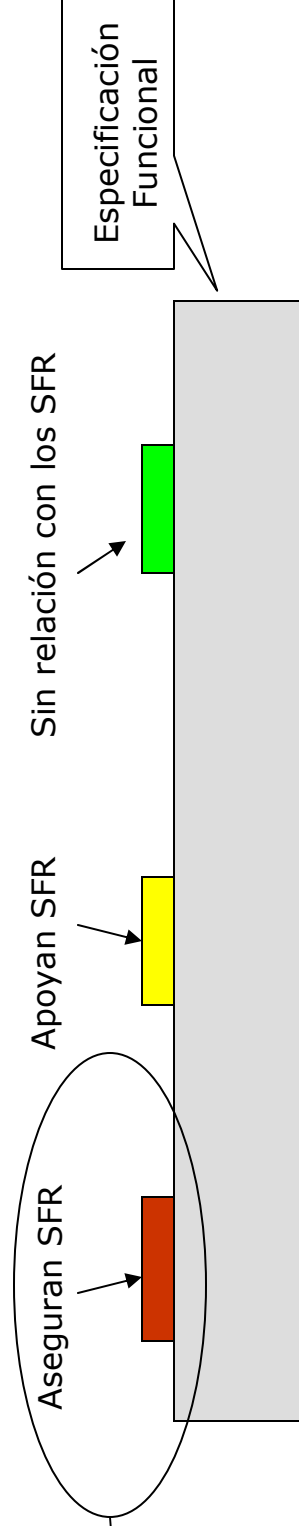
Componente de confianza: Test Funcional (ATE)

- Familias de requerimientos:
 - ATE_FUN: Documentación de Testeo Funcional
 - ATE_COV: Análisis de cobertura del testeo
 - ATE_DPT: Profundidad del testeo
 - ATE_IND: Testeo Independiente
- Objetivos:
 - Las contramedidas son conformes a la especificación.
 - ¡No se trata de tests de penetración!
 - Condiciones de uso esperadas, no se introduce stress.

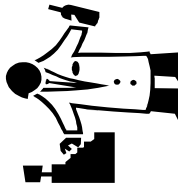
Test Funcional (ATE): Documentación



Test Funcional (ATE): Análisis de Cobertura

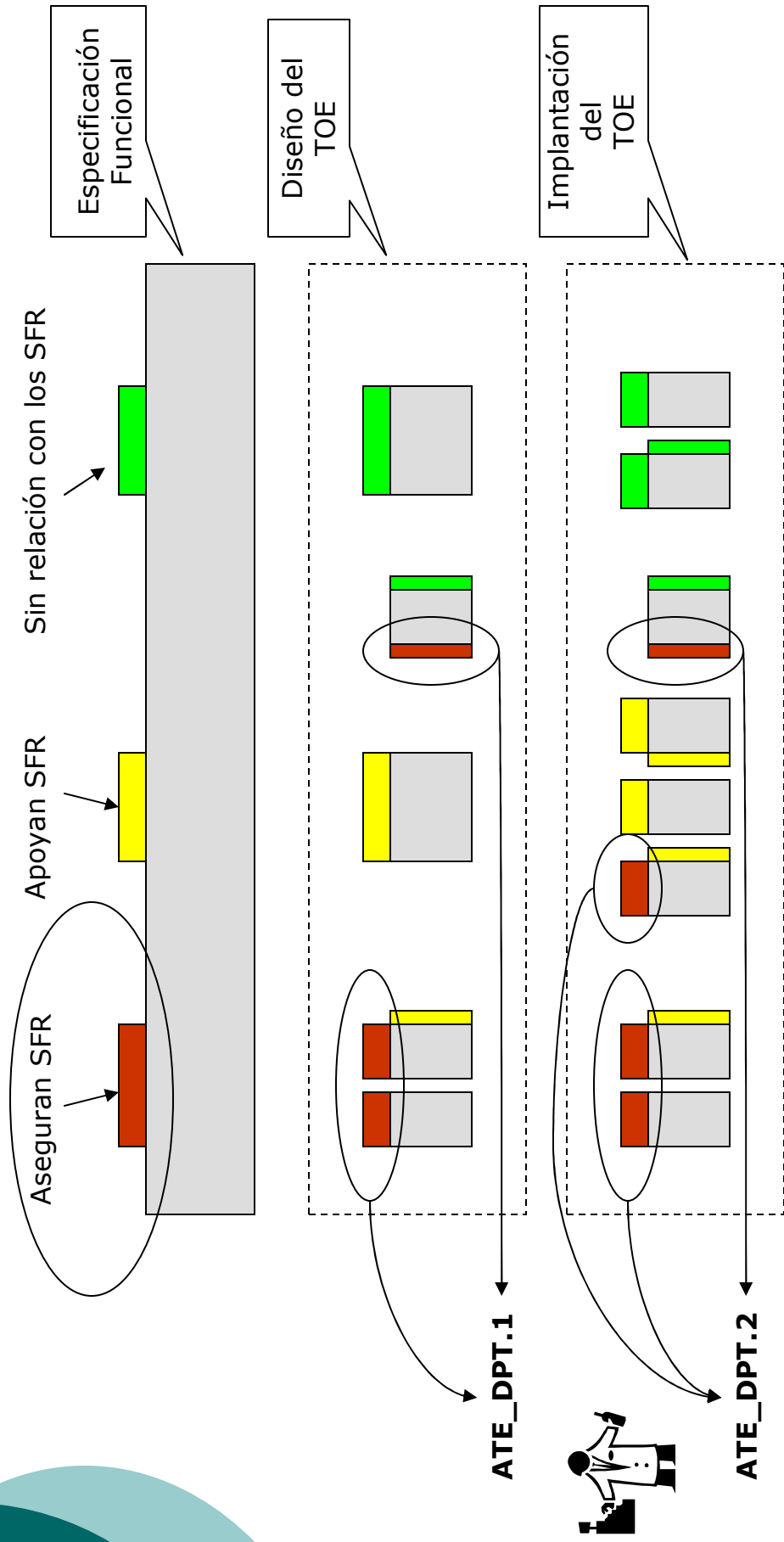


ATE_COV.1



- **Parcial:** solo se provee una descripción del grado de cobertura de las TSFI (ATE_COV.2)
- **Total:** análisis demostrando que las TSFI son ejercitadas completamente (ATE_COV.3)

Test Funcional (ATE): Profundidad de Testeo





Análisis de Vulnerabilidad (AVA)



- Objetivo: buscar y explotar vulnerabilidades experimentando con el TOE.
- Medios:
 - Revisión de código y de la documentación del TOE.
 - Test de penetración: usos no esperados, hipótesis implícitas, estrés del TOE, casos límite...
- Niveles de confianza en función de:
 - Representación del TOE utilizada
 - Ataques conocidos o investigación independiente.
 - Nivel de potencial del atacante (4 niveles).



© Dr. Ing. Eduardo Giménez

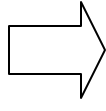
Análisis de Vulnerabilidad (AVA)

Ejemplo de Ataque SPA sobre RSA

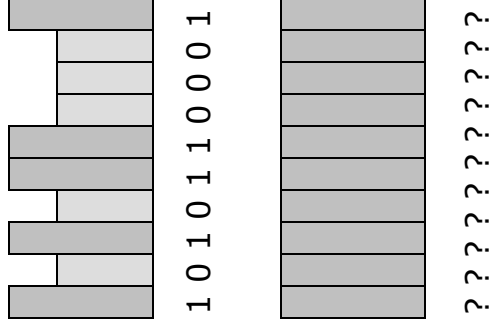
- Cálculo de $Z = X^E \text{ mod } N$, con $E = \sum_{i=0}^{i=n-1} e_i * 2^i$ la clave privada.

Algoritmo
"Square and
Multiply" de
Donald Knuth

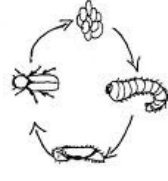
```
Z := 1;
for i = n-1 downto 0 do
  Z := Z * Z mod N;
  if ei = 1 then Z := Z * X mod N
done
```



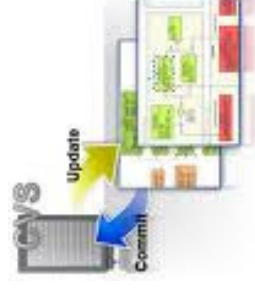
```
Z := 1;
for l = n-1 downto 0 do
  Z := Z * Z mod N;
  T := Z * X mod N;
  if ei = 1 then Z := T else Z := Z;
done
```



Componente de Confianza: Soporte al Ciclo de Vida (ALC)



- Definición del ciclo de vida del TOE:
 - Procedimientos de desarrollo y mantenimiento
 - Uso de métricas de calidad sobre tolerancia a fallas
- Herramientas y técnicas:
 - Lenguajes de programación, ambientes, compiladores.
- Gestión de configuración:
 - Identificar y generar (compilar) el TOE correcto
 - Control y aprobación de cambios en el TOE
 - Alcance de la información bajo control
 - Control de versiones y desarrollo concurrente

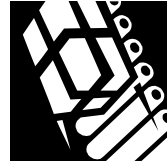


Componente de Confianza: Soporte al Ciclo de Vida (ALC)



- Seguridad del sitio de desarrollo:
 - Protección física del sitio de desarrollo
 - Control y formación del personal
 - Protección de los puestos de trabajo y la intranet
 - Auditorías por parte del evaluador

- Entrega y operación:
 - Evitar que el TOE sea modificado luego de liberado
 - Asegurar que el destinatario recibe un TOE auténtico
 - Evitar que se divulgue la liberación del TOE
 - Evitar que el TOE sea interceptado o demorado.



Componente de Confianza: Manuales y Guías (AGD)



- Manual de operación del TOE:
 - Roles, responsabilidades y privilegios
 - Interfaces que debe utilizar cada rol
 - Parámetros de las interfaces que controlan la seguridad
 - Eventos y acciones a tener en cuenta
 - Modos de operación seguros
 - Medidas organizacionales para mantener la seguridad
- Manual de preparación del TOE:
 - Aceptación, preparación y configuración del TOE
 - Preparación del ambiente operativo del TOE



Los documentos que componen el estándar

- CC Part 1: Introduction and general model
- CC Part 2: Security functional requirements
- CC Part 3: Security Assurance Requirements
- CEM: Common Evaluation Methodology

Disponible gratuitamente: <http://www.commoncriteriaportal.org>

Conclusiones (1/2)

- Criterios Comunes: iuna herramienta muy poderosa!
- ... pero bastante cara
- ... que exige un esfuerzo de documentación importante
- ... e introduce rigideces en el desarrollo.



- Versión v3.1, Rev 3: más simple y modular



Conclusiones (2/2)

- ¡Si exigimos un certificado hay que leer el ST!
- Conviene elegir PP ya evaluados por algún esquema.
- Ser conscientes de lo que cuesta al proveedor.



¡Gracias por su atención!

Es el momento de las preguntas....