Perfil de Protección Appliance Realia Technologies S.L.

11-04-2011

Versión 2.1

Hoja de Información General

CONTROL DOCUMENTAL

PROYECTO:	
TÍTULO:	Perfil de Protección Appliance Realia Technologies S.L.
VERSIÓN	2.1
FECHA DE EDICIÓN:	11-04-2011
FICHERO:	Perfil de Protección Appliance REALSEC
HERRAMIENTAS DE EDICIÓN:	MICROSOFT WORD 2003
AUTORES:	REALSEC
COMPAÑÍA:	REALSEC

Control de Versiones

Versión	Fecha	Afecta	Breve descripción del cambio
1.0	13/12/2010	Todo	Versión inicial
2.0	24/12/2010	Todo	Solución de ORs, refinamiento del SPD
2.1	11/04/2011	Todo	Tipográfico Se elimina la hipótesis H.ADMINISTRADORES

Índice

1 Introducción

1 Este documento es el Perfil de Protección que describe los requisitos de seguridad de un sistema operativo personalizado y configurado de manera segura; de modo que las aplicaciones que son ejecutadas en el appliance pueden confiar en él.

1.1 Identificación del PP

Título	Perfil de Protección Appliance Realia Technologies S.L.
Versión	Versión 2.1
Autor	Realia Technologies S.L.
Fecha de publicación	11-04-2011

1.2 Resumen del TOE

1.2.1 Tipo de TOE

2 El TOE es un sistema operativo personalizado y configurado de manera segura, cuyo objetivo es la protección de la confidencialidad y la integridad de la información procesada, almacenada y trasmitida.

3 El TOE es un sistema operativo multiusuario y multitarea basado en Linux. El TOE puede proveer servicios a varios usuarios a la vez. Después de realizar la autenticación, los usuarios tienen acceso a un entorno que permite arrancar aplicaciones, ejecutar comandos o crear y acceder a ficheros.

4 El TOE proporciona mecanismos adecuados para separar a los usuarios y proteger sus datos.

5 Los comandos con privilegios están restringidos a los usuarios con rol superusuario.

6 El acceso al TOE se realizará de manera local, puesto que la personalización y configuración del TOE cierra los accesos remotos al mismo.

7 El TOE está compuesto únicamente por software, por lo tanto sólo se tendrá en cuenta el TOE desde el punto de vista lógico.

1.2.1.1 Características de seguridad lógicas

1.2.1.1.1 Funciones de gestión

8 El TOE permite la configuración de los parámetros de seguridad. Mediante este mecanismo, se obtiene un sistema operativo personalizado y configurado de manera segura que se puede considerar una plataforma segura para que se ejecuten diferentes aplicaciones.

1.2.1.1.2 Interfaces del TOE

9 El TOE proporciona un interfaz a través de la consola local, que permite la configuración y personalización del sistema operativo.

10 Existe otro interfaz entre el sistema operativo y el HSM, a través de un driver que se encarga de abstraer el hardware del HSM a las aplicaciones que harán uso de él.

1.2.1.1.3 Roles, servicios y autenticación

11 El TOE soportará los siguientes roles: usuario y superusuario. Los usuarios tendrán acceso a la información almacenada en el TOE dependiendo del rol que posean.

12 El TOE implementará un mecanismo de autenticación basado en la identidad de los usuarios que garantizará la confidencialidad e integridad de la información almacenada en el TOE.

1.2.1.1.4 Auditoría

13 El TOE proporciona la capacidad de detectar y registrar los eventos relevantes a la seguridad.

14 El entorno en el que opera el TOE deberá revisar los registros generados por el TOE con el objeto de detectar posibles violaciones de seguridad o negligencias.

1.2.2 Uso del TOE

15 El TOE se usa como una plataforma segura para ejecutar aplicaciones.

16 El sistema usará el TOE para proteger los datos almacenados en el mismo (Ej.- configuración de las aplicaciones, datos de autenticación en el TOE, configuración del TOE).

17 Además el TOE proporciona a las aplicaciones un interfaz al HSM a través de un driver que se encarga de abstraer el hardware del HSM a las aplicaciones que harán uso de él.

18 Por lo tanto, se puede concluir que el TOE proporciona una plataforma segura para la ejecución de aplicaciones y que además provee un interfaz sencillo a un módulo criptográfico.

1.2.3 Hardware y software no incluido en el TOE

19 El Hardware no estará incluido en el TOE.

20 El software correspondiente a las aplicaciones que se ejecutan en el TOE, no será considerado TOE. Por tanto, todas las aplicaciones que no formen parte del CORE del TOE, no estarán incluidas en el TOE.

21 El HSM con el que se comunica el TOE tampoco está incluido en el TOE.

2 Declaración de conformidad

2.1 Conformidad con respecto a la norma CC

22 Este perfil de protección se desarrolla conforme a la norma Common Criteria versión 3.1 R3 de Julio de 2009:

- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1 R3, Julio 2009, [CC31p2].
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1 R3, Julio 2009, [CC31p3].

según lo siguiente:

- [CC31p2] Parte 2;
- [CC31p3] Parte 3;
- Conforme al paquete de garantía EAL2 según [CC31p3].

23 Este Perfil de Protección, y las declaraciones de seguridad que declaren su cumplimiento, se deberán evaluar utilizando la metodología de evaluación definida en:

- Common Criteria for Information Technology Security Evaluation. Evaluation Methodology. Version 3.1 R3, Julio 2009, [CEM31].

2.2 Conformidad con otros perfiles de protección

24 Este PP no declara el cumplimiento de ningún otro PP.

2.3 Declaraciones de conformidad con respecto a este PP

25 Este PP requiere que la conformidad al mismo se declare de manera estricta, tal como se define en la norma Common Criteria versión 3.1 R3 de Julio de 2009.

3 Definición del problema de seguridad (SPD)

26 Esta sección define el problema de seguridad que se quiere resolver. En lo que respecta a la norma CC, el problema de seguridad es axiomático en el sentido de que el proceso seguido para la derivación final del mismo, está fuera del alcance de la norma, es decir, no se valora.

3.1 Activos del TOE

27 Se tienen en cuenta los siguientes activos:

Id	Descripción del Activo	Valor del activo
A.INFORMATION	La información almacenada, procesada o transmitida por el TOE. En definitiva, la información que se encuentra en el TOE.	Confidencialidad Integridad

28 El TOE contrarresta la amenaza general de acceso no autorizado a la información, donde acceso incluye la revelación, modificación y destrucción de la información por una entidad no autorizada.

3.2 Amenazas

29 Se consideran las siguientes amenazas y valores del los activos afectados (C - Confidencialidad, I-integridad):

Id	Descripción	Activos afectados
T.ACCESS	Un atacante (no usuario del TOE) puede ganar acceso a recursos o realizar operaciones para las cuales no tiene los permisos necesarios. El agente es un **atacante no autorizado** a la organización con recursos y experiencia limitada. El potencial de ataque asociado al atacante es "**Basic**".	A.INFORMATION (C) A.INFORMATION (I)
T.PERMISOS	Un usuario del TOE puede ganar acceso a recursos o realizar operaciones para las cuales no tiene los permisos necesarios. El agente es un **usuario autorizado** en el	A.INFORMATION (C) A.INFORMATION (I)

	TOE **con el rol de usuario**. El potencial de ataque asociado al atacante es "**Basic**".	
T.BAD_ADMIN	Los activos del TOE pueden comprometerse debido a una administración incorrecta del TOE. El agente es un **usuario autorizado** en el TOE **con el rol de superusuario**. El potencial de ataque asociado al atacante es "**Basic**".	A.INFORMATION (C) A.INFORMATION (I)
T. ASSIGN_ROLES	La asignación no coherente de los roles a los usuarios puede provocar un acceso incorrecto a los recursos del TOE. El agente es un **usuario autorizado** en el TOE **con el rol de superusuario** que actúa de manera negligente en la asignación de los roles. El potencial de ataque asociado al atacante es "**Basic**".	A.INFORMATION (C) A.INFORMATION (I)

3.3 Políticas de seguridad organizativas (OSPs)

30 Esta sección detalla las políticas de seguridad organizativas en forma de reglas, prácticas o guías que se siguen en la empresa.

Id	Descripción
P.ROLES	Se separará y se distinguirá entre los siguientes roles: usuario y superusuario.
P.AUDIT	Se registrarán los eventos de seguridad del sistema. El entorno en el que opera el TOE deberá revisar los registros generados por el TOE con el objeto de detectar posibles violaciones de seguridad o negligencias.

3.4 Hipótesis

31 Esta sección detalla hipótesis que se hacen sobre el entorno operacional en el que opera el TOE. Si el TOE opera en un entorno que no cumple estas

hipótesis, éste no será capaz de proporcionar su funcionalidad de seguridad.

Id	Descripción
H.ACCESO_FISICO	Los atacantes no disponen de acceso físico al TOE, es decir el entorno operacional será lo suficientemente seguro para que el atacante no pueda realizar ataques al hardware donde se está ejecutando el TOE.
H.APLICACIONES_SEGURAS	Las aplicaciones que se ejecutarán en el appliance serán seguras y no comprometerán la seguridad del TOE.
H.STM	El entorno proporciona una medida fiable de tiempo.

4 Objetivos de seguridad

32 Esta sección define los objetivos de seguridad que permiten resolver el problema de seguridad expuesto en la anterior sección. Se exponen los objetivos de seguridad para el TOE y los objetivos de seguridad para el entorno operacional.

4.1 Objetivos de seguridad para el TOE

Id	Descripción
O.IDENTIFI_AUTENTICA	El TOE no permitirá al acceso a los usuarios que no se hayan autenticado con anterioridad.
O.CONTROL_PERMISOS	El TOE deberá restringir el acceso a sus servicios dependiendo del role del usuario.
O.AUDITORÍA	El TOE debe proporcionar la capacidad de detectar y registrar los eventos relevantes a la seguridad.
O.ROLES	El TOE soportará los siguientes roles: usuario y superusuario.

4.2 Objetivos de seguridad para el entorno operacional

Id	Descripción
OE.ACCESO_FISICO	Los atacantes no disponen de acceso físico al TOE, es decir el entorno operacional será lo suficientemente seguro para que el atacante no pueda realizar ataques al hardware donde se está ejecutando el TOE.
OE.ASSIGN_ROLES	Los administradores del TOE asignarán los roles a los usuarios de manera coherente permitiéndole realizar únicamente las operaciones para las que fueron autorizado.
OE.ADMINISTRADORES	Los administradores del TOE recibirán la formación necesaria para evitar que los activos del TOE se puedan ver comprometidos. Además, los administradores del TOE serán confiables y cuidarán de la seguridad y correcto funcionamiento del TOE.
OE.APLICACIONES_SEGURAS	Las aplicaciones que se ejecutarán en el appliance serán seguras y no comprometerán la seguridad del TOE.
OE.AUDITORÍA	El entorno del TOE deberá revisar los registros de

	auditoría generados por el TOE para detectar posibles violaciones.
OE.STM	El entorno proporcionará una medida de tiempo que se utilizará en la generación de la información de la auditoría.

4.3 Justificación de los objetivos de seguridad

	T.ACCESS	T.PERMISOS	T.BAD_ADMIN	T.ASSIGN_ROLES	P.ROLES	P.AUDIT	H.ACCESO_FISICO	H.APLICACIONES_SEGURAS	H.STM
O.IDENTIFI_AUTENTICA	X								
O.CONTROL_PERMISOS		X							
O.AUDITORIA						X			
O.ROLES	X	X			X				
OE.ACCESO_FISICO	X	X					X		
OE.APLICACIONES_SEGURAS								X	
OE.ADMINISTRADORES			X						
OE.ASSIGN_ROLES				X					
OE.AUDITORIA						X			
OE.STM									X

Correspondencia de los objetivos de seguridad

33 A continuación se justifica la necesidad y suficiencia de cada objetivo de seguridad para contrarrestar las amenazas, cumplir las políticas organizativas y soportar las suposiciones de entorno.

34 La amenaza T.ACCESS, compromete la confidencialidad e integridad de la información almacenada en el TOE pudiendo el atacante acceder al TOE sin ser usuario autorizado. El objetivo de seguridad del TOE O.IDENTIFI_AUTENTICA, requiere que el TOE verifique y autentique a todos los usuarios antes de permitirse cualquier acción. El objetivo de

seguridad del TOE O.ROLES, requiere que el TOE mantenga los roles de usuario y superusuario. Además el objetivo del entorno OE.ACCESO_FISICO impide los ataques físicos al TOE.

35 La amenaza T.PERMISOS indica que un usuario del TOE puede ganar acceso a recursos o realizar operaciones para las cuales no tiene los permisos necesarios. El objetivo de seguridad del TOE O.CONTROL_PERMISOS, requiere que el TOE restringa el acceso a sus servicios dependiendo del role del usuario. El objetivo de seguridad del TOE O.ROLES, requiere que el TOE mantenga los roles de usuario y superusuario. Además el objetivo del entorno OE.ACCESO_FISICO impide los ataques físicos al TOE.

36 La amenaza T.BAD_ADMIN indica que los activos del TOE pueden comprometerse debido a una administración incorrecta del TOE. El objetivo de seguridad del entorno OE.ADMINISTRADORES especifica que los administradores del TOE recibirán la formación necesaria para evitar que los activos del TOE se puedan ver comprometidos. Además, los administradores del TOE serán confiables y cuidarán de la seguridad y correcto funcionamiento del TOE.

37 La amenaza T.ASSIGN_ROLES indica que los administradores del TOE asignarán los roles a los usuarios de manera coherente permitiéndole realizar únicamente las operaciones para las que fueron autorizado. El objetivo de seguridad del entorno OE.ASSIGN_ROLES especifica que los administradores del TOE asignarán los roles a los usuarios de manera coherente permitiéndole realizar únicamente las operaciones para las que fueron autorizado.

38 La política P.ROLES específica que se separará y se distinguirá entre los siguientes roles: usuario y superusuario. La política se cumple directamente por el objetivo de seguridad del TOE O.ROLES.

39 La política P.AUDIT específica lo siguiente:

- Se registrarán los eventos de seguridad del sistema.
- El entorno en el que opera el TOE deberá revisar los registros generados por el TOE con el objeto de detectar posibles violaciones de seguridad o negligencias.

40 La política se cumple directamente por el objetivo de seguridad del TOE O.AUDITORIA y con el objetivo de seguridad del entorno OE.AUDITORIA.

41 La hipótesis H.ACCESO_FISICO supone que los atacantes no disponen de acceso físico al TOE, es decir el entorno operacional será lo suficientemente seguro para que el atacante no pueda realizar ataques al

hardware donde se está ejecutando el TOE. Esta suposición es directamente cubierta por el objetivo del entorno OE. ACCESO_FISICO.

42 La hipótesis H.APLICACIONES_SEGURAS supone que las aplicaciones que se ejecutarán en el appliance serán seguras y no comprometerán la seguridad del TOE. Esta suposición es directamente cubierta por el objetivo del entorno OE.APLICACIONES_SEGURAS.

43 La hipótesis H.STM supone que el entorno proporciona una fuente de tiempo confiable. Esta suposición es directamente cubierta por el objetivo del entorno OE.STM.

5 Requisitos de seguridad del TOE

5.1 Requisitos funcionales de seguridad

5.1.1 Identificación y Autenticación

44 **FIA_UID.2 User identification before any action**

Hierarchical to: FIA_UID.1 Timing of identification.
Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user**.**

45 **FIA_UAU.2 User authentication before any action**

Hierarchical to: FIA_UAU.1 Timing of authentication.
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.2 Políticas de control de acceso

46 **FDP_ACC.2 Complete access control**

Hierarchical to: FDP_ACC.1 Subset access control
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the ***Política de control de acceso al TOE*** on

(A) Objetos: información almacenada en el TOE (ficheros);

(B) Sujetos: usuarios;

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

47 **FDP_ACF.1 Security attribute based access control**

Hierarchical to: No other components.
Dependencies:
FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the ***Política de control de acceso al TOE*** to objects based on the following:

(A) Objetos:

a. información almacenada en el TOE (ficheros); Atributos: el propietario, los permisos asociados (lectura, escritura y/o ejecución).

(B) Sujetos: usuarios; Atributos: la identidad del usuario, el rol del usuario;

[*assignment: otros atributos de seguridad de los objetos y sujetos***]**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(A) El usuario tendrá acceso a la información almacenada (ficheros) si posee el permiso requerido.

(B) [*assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects*]**.**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*assignment: rules, based on security attributes, that explicitly deny access of subjects to objects*].

48 **FMT_MSA.1 Management of security attributes**

Hierarchical to: No other components.
Dependencies:
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the ***Política de control de acceso al TOE*** to restrict the ability to [*selection: change_default, query, modify, delete, [assignment: other operations*]] the security attributes [*assignment: list of security attributes*] to ***usuario y superusuario***.

Nota de Aplicación:

El autor de la declaración de seguridad deberá definir las operaciones que se pueden hacer sobre los atributos de los objetos declarados en dicha política:

(A) Información almacenada en el TOE (ficheros): identidad, tipo y permisos;

49 **FMT_MSA.3 Static attribute initialisation**

Hierarchical to: No other components.
Dependencies:
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the ***Política de control de acceso al TOE*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the ***usuario y superusuario*** to specify alternative initial values to override the default values when an object or information is created.

50 **FMT_SMF.1 Specification of Management Functions**

Hierarchical to: No other components.
Dependencies: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

(A) Usuarios con rol de superusuario

a. Gestión de usuarios (Creación de nuevos usuarios, Borrado de usuarios y modificación permisos del usuario)

(B) Usuarios con rol de usuario

a. Cambio de contraseña por parte del usuario;

(C) [*assignment: otras funciones de gestión*].

5.1.3 Roles de seguridad

51 **FMT_SMR.1 Security roles**

Hierarchical to: No other components.
Dependencies:
FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [**usuario y superusuario**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.4 Auditoría de seguridad

52 **FAU_GEN.1 Audit data generation**

Hierarchical to: No other components.
Dependencies:
FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*selection, choose one of: minimum, basic, detailed, not specified*] level of audit; and

c)

i. Dispositivos montados;
ii. Inicio y fin de sesión del usuario;
iii. [*assignment: other specifically defined auditable events*]**.**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*assignment: other audit relevant information*].

5.2 Requisitos de garantía de seguridad

53 Los requisitos de garantía que se incluyen a continuación se corresponden con el nivel de garantía definido EAL2, conforme a [CC31p3].

5.2.1 Declaración de seguridad (ASE)

54 ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:
ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:
ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.
ASE_INT.1.2C The ST reference shall uniquely identify the ST.
ASE_INT.1.3C The TOE reference shall identify the TOE.
ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.
ASE_INT.1.5C The TOE overview shall identify the TOE type.
ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.
ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.
ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

55 ASE_CCL.1 Conformance claims

Dependencies:
ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements:
ASE_CCL.1.1D The developer shall provide a conformance claim.
ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:
ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

56 **ASE_SPD.1 Security problem definition**

Dependencies: No dependencies.

Developer action elements:
ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:
ASE_SPD.1.1C The security problem definition shall describe the threats.
ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.
ASE_SPD.1.3C The security problem definition shall describe the OSPs.
ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

57 **ASE_OBJ.2 Security objectives**

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:
ASE_OBJ.2.1D The developer shall provide a statement of security objectives.
ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:
ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.
ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.
ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.
ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.
ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.
ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

58 **ASE_ECD.1 Extended components definition**

Dependencies: No dependencies.

Developer action elements:
ASE_ECD.1.1D The developer shall provide a statement of security requirements.
ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:
ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

59 **ASE_REQ.2 Derived security requirements**

Dependencies:

ASE_OBJ.2 Security objectives
ASE_ECD.1 Extended components definition

Developer action elements:
ASE_REQ.2.1D The developer shall provide a statement of security requirements.
ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:
ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.2.4C All operations shall be performed correctly.
ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.
ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.
ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.
ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

60 **ASE_TSS.1 TOE summary specification**

Dependencies:

ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements:
ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements:
ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

5.2.2 Desarrollo (ADV)

61 **ADV_FSP.2 Security-enforcing functional specification**

Dependencies: ADV_TDS.1 Basic design

Developer action elements:
ADV_FSP.2.1D The developer shall provide a functional specification.
ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:
ADV_FSP.2.1C The functional specification shall completely represent the TSF.
ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.
ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.
ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

62 **ADV_TDS.1 Basic design**

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:
ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:
ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.1.2C The design shall identify all subsystems of the TSF.
ADV_TDS.1.3C The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.
ADV_TDS.1.4C The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.
ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.
ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

63 **ADV_ARC.1 Security architecture description**

Dependencies:
ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:
ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.
ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.
ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:
ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.
ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.
ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.
ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.
ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

5.2.3 Guías de usuario (AGD)

64 **AGD_PRE.1 Preparative procedures**

Dependencies: No dependencies.

Developer action elements:
AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:
AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

65 **AGD_OPE.1 Operational user guidance**

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:
AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:
AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

5.2.4 Soporte al ciclo de vida (ALC)

66 **ALC_CMC.2 Use of a CM system**

Dependencies:
ALC_CMS.1 TOE CM coverage

Developer action elements:
ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.2.2D The developer shall provide the CM documentation.
ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:
ALC_CMC.2.1C The TOE shall be labelled with its unique reference.
ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

67 **ALC_CMS.2 Parts of the TOE CM coverage**

Dependencies: No dependencies.

Developer action elements:
ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:
ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.
ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

68 **ALC_DEL.1 Delivery procedures**

Dependencies: No dependencies.

Developer action elements:
ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:
ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

5.2.5 Pruebas (ATE)

69 **ATE_COV.1 Evidence of coverage**

Dependencies:
ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:
ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:
ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

70 **ATE_FUN.1 Functional testing**

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:
ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:
ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

71 **ATE_IND.2 Independent testing - sample**

Dependencies:
ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:
ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:
ATE_IND.2.1C The TOE shall be suitable for testing.
ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.2.6 Análisis de vulnerabilidades (AVA)

72 **AVA_VAN.2 Vulnerability analysis**

Dependencies:
ADV_ARC.1 Security architecture description
ADV_FSP.2 Security-enforcing functional specification
ADV_TDS.1 Basic design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:
AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

5.3 Justificación de los requisitos de garantía de seguridad

5.3.1 Justificación de los requisitos de funcionalidad de seguridad

73 A continuación se incluye una tabla en la que se muestran los requisitos funcionales que dan cumplimiento a los objetivos de seguridad definidos.

74 Así mismo se incluye la justificación de necesidad y suficiencia de cada uno de los requisitos funcionales de forma que se garantice el cumplimiento de los objetivos de seguridad.

	FAU_GEN.1 Audit data generation	FMT_SMR.1 Security roles	FMT_SMF.1 Specification of Management Functions	FMT_MSA.3 Static attribute initialisation	FMT_MSA.1 Management of security attributes	FDP_ACF.1 Security attribute based access control	FDP_ACC.2 Complete access control	FIA_UAU.2 User authentication before any action	FIA_UID.2 User identification before any action
O.IDENTIFI_AUTENTICA								X	X
O.CONTROL_PERMISOS		X	X	X	X	X	X	X	X
O.AUDITORIA	X								
O.ROLES		X							

75 El objetivo de seguridad O.IDENTIFI_AUTENTICA requiere que el TOE no permita el acceso a los usuarios que no se hayan autenticado con anterioridad. Este objetivo de seguridad se cumple mediante los requisitos FIA_UAU.2 y FIA_UID.2 que requieren de identificación y autenticación por parte del usuario antes de realizar cualquier operación.

76 El objetivo de seguridad O.CONTROL_PERMISOS requiere que el TOE restringa el acceso a sus servicios dependiendo del role del usuario. Este objetivo de seguridad se cumple mediante los requisitos FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1 y FMT_SMR.1 que implementan la política de control de acceso al TOE.

77 El objetivo de seguridad O.AUDITORIA requiere que el TOE restringa el acceso a sus servicios dependiendo del role del usuario. Este objetivo de seguridad se cumple mediante el requisito FAU_GEN.1 que requiere la generación de auditoría.

78 El objetivo de seguridad O.ROLES requiere que el TOE soporte los siguientes roles: usuario y superusuario. Este objetivo de seguridad se cumple mediante el requisito FMT_SMR.1 que define los roles en el sistema.

5.3.2 Dependencias de los requisitos funcionales de seguridad

79 Este perfil de protección satisface todos los requisitos de dependencias de [CC31p2] excepto FPT_STM.1, que es dependencia de FAU_GEN.1, que se deriva al entorno.

5.3.3 Justificación de los requisitos de garantía de seguridad

80 La garantía de seguridad deseada para este tipo de TOE es la proporcionada por el nivel de evaluación EAL2.

6 Acrónimos y definiciones

6.1 Acrónimos

81 Son de aplicación todos los acrónimos y definiciones incluidos en [CC31p1].

CC	Common Criteria
CCN	Centro Criptológico Nacional
CSP	Critical Security Parameter
FW	FirmWare
HW	HardWare
HSM	Hardware Security Module
OSPs	Organisational Security Policies
SPD	Security Problem Definition
SW	Software
PC	Personal Computer
TOE	Target of Evaluation
TSF	TOE Security Functionality

6.2 Definiciones

82 Ninguna.

7 Referencias

83 Common Criteria

[CC31p2] Common Criteria for Information Technology Security Evaluation.
Part 2: Security Functional Components
Version 3.1 R3

[CC31p3] Common Criteria for Information Technology Security Evaluation.
Part 3: Security Assurance Components
Version 3.1 R3

[CEM31] Common Criteria for Information Technology Security Evaluation.
Evaluation Methodology
Version 3.1 R3