RECOVERY LABS®

Security Target for the Secure Data Erasure Software – EraseIT Core

Autor: Daniel SANZ / Jaime HERENCIA
Fecha: 09/07/10
Versión 1.5

Histórico de versiones

VERSION	FECHA	AUTORES	DESCRIPCIÓN
1.0	14/04/10	Daniel SANZ Jaime HERENCIA	Primer documento
1.1	19/05/10	Daniel SANZ Jaime HERENCIA	ERACO-OR-001
1.2	21/05/10	Daniel SANZ Jaime HERENCIA	Nueva versión del TOE
1.3	01/06/10	Daniel SANZ Jaime HERENCIA	Modificaciones sobre la denominación del TOE. Modificado el physical scope.
1.4	22/06/10	Daniel SANZ Jaime HERENCIA	Añadido requisito seguridad FTP_ITC.1
1.5	09/07/10	Daniel SANZ Jaime HERENCIA	Cambio versión del TOE

Tabla de contenidos

1.ST Introduction

1.1. ST reference and TOE reference

The information to identify this document and the TOE is shown below.

ST title:
Security Target for the Secure Data Erasure Software – EraseIT Core
ST version:
1.5
Date:
2010-07-09
Author:
Daniel SANZ / Jaime HERENCIA - RECOVERYLABS S.A.
TOE Identification:
EraseIT Core V1.0.3
CC version:
Common Criteria for Information Technology Security Evaluation, Version 3.1 R3
Keywords:
Residual Information Protection, Disk Erasure, Media Security

1.2. TOE Overview

Software para el borrado seguro de datos almacenados en dispositivos de almacenamiento. Es una aplicación utilizada como **núcleo de borrado** en **aplicaciones clientes de borrado seguro**. Se trata de software destinado al borrado seguro de datos almacenados en dispositivos de almacenamiento. El borrado seguro de los datos se realiza mediante la sobreescritura de la información. La aplicación base se ejecuta sobre una plataforma PC-compatible y utiliza las controladoras de discos IDE, SATA, SCSI, USB para el acceso a la información y la sobreescritura de los discos seleccionados por el usuario. Sobre las unidades de lectura asociadas a los dispositivos de almacenamiento, como en el caso de las unidades USB tipo U3, NO se realiza la operación de borrado seguro. El **método de borrado es configurable** por la aplicación cliente autorizada, posibilitando al **usuario** la realización del mismo según lo especificado en las normas DoD5220.22-M, HMG Infosec Standard No:5, NATO standard, US Navy, NAVSO P-5239-26 – RLL, US Air Force, AFSSI5020, Peter Gutmann patterns, etc.

El proceso de operación de borrado queda registrado mediante una **auditoría** que al finalizar la operación será almacenada en el mismo dispositivo de almacenamiento y podrá ser exportado a la aplicación cliente autorizada.

1.2.1. TOE type

El TOE entra en la categoría de software de borrado seguro.

El TOE se carga durante el arranque del sistema desde diversos medios de distribución (CD/DVD, USB, red, etc). Integra su propio sistema operativo, por lo que elimina cualquier dependencia con éste y aumenta la compatibilidad del producto.

1.2.2. Required non-TOE hardware/software/firmware

Requerimientos del TOE:

- PC compatible x86
- 128 Mb RAM
- BIOS configurada para ejecución desde medios externos.

Especificación equipo:

- Procesador: Intel Celeron D 336, 2800 MHz (21 x 133)
- Placa Base: ASRock 775i65G
- Chipset de la placa base: Intel Springdale-G i865G
- RAM: 1024 MB
- BIOS: AMI P.300 (20/03/07)

Controladoras:

- Controladora SCSI: PCS SCSI Adaptec AHA-2940UW
- Controladora IDE: Intel(R) 82801EB - 24D1
- Controladora USB: Intel 82801EB ICH5 - USB Controller [A-2/A-3]

Discos:

- Disco SCSI: SEAGATE ST39103LW SCSI Disk Device (9 GB, 10000 RPM, Ultra2 SCSI) - LS568113000010161ZJX
- Disco SATA: SEAGATE ST96812AS (60 GB, 5400 RPM, SATA) - 5PJ01493
- Disco USB: SEAGATE ST3802110A USB Device (80 GB, 7200 RPM, Ultra-ATA/100)
- Disco IDE: SEAGATE ST380215A (80 GB, 7200 RPM, Ultra-ATA/100) - 6QZ6XX52
- Disco USB Extraible: USB Flash Memory USB Device (486 MB, USB)

Software:

- Aplicación cliente autorizada de borrado compatible con las TSFIs del TOE

	Scope
Procesador: Intel Celeron D 336, 2800 MHz (21 x 133)	×
Placa Base: ASRock 775i65G	×
Chipset de la placa base: Intel Springdale-G i865G	×
RAM: 1024 MB	×
BIOS: AMI P.300 (20/03/07)	×
Controladora SCSI: PCS SCSI Adaptec AHA-2940UW	×
Controladora IDE: Intel(R) 82801EB - 24D1	×
Controladora USB: Intel 82801EB ICH5 - USB Controller [A-2/A-3]	×
Disco SCSI: SEAGATE ST39103LW SCSI Disk Device (9 GB, 10000 RPM, Ultra2 SCSI) - LS568113000010161ZJX	×
Disco SATA: SEAGATE ST96812AS (60 GB, 5400 RPM, SATA) - 5PJ01493	×
Disco USB: SEAGATE ST3802110A USB Device (80 GB, 7200 RPM, Ultra-ATA/100)	×
Disco IDE: SEAGATE ST380215A (80 GB, 7200 RPM, Ultra-ATA/100) - 6QZ6XX52	×
Disco USB Extraible: USB Flash Memory USB Device (486 MB, USB)	×
Aplicación cliente autorizada de borrado compatible con las TSFIs del TOE	×

✓ En el TOE
× Excluido del TOE

No se realizará la operación de borrado sobre las unidades de sólo lectura.

1.3. TOE Description

EraseIT Core es un programa de borrado seguro de datos, diseñado para garantizar la confidencialidad de la información en la retirada de parques informáticos.

El TOE permite realizar el **borrado seguro** y definitivo de los datos de equipos que van a ser retirados. De esta forma EraseIT Core:

- Evita las situaciones de riesgo:
    - Permitiendo cumplir con las medidas que establece la **LOPD** dirigidas a evitar el acceso a la información contenida en un soporte o su recuperación posterior.
    - Sin riesgo de **fuga de información** confidencial.
    - Sin romper la cadena de **custodia de los datos.**

- Simplifica la gestión de la renovación o retirada de equipos optimizando la logística de traslado de los mismos.

El TOE ofrece las máximas prestaciones a la aplicación cliente autorizada:

- Realiza el borrado en todas las interfaces: IDE, SATA, SCSI, USB, etc.

Parametrizable para cumplir con cualquiera de los estándares internacionales de borrado: **American DoD 5220-22.M Standard Wipe, HMG Infosec Standard No: 5, NATO Standard, Canadian RCMP TSSIT OPS-II Standard Wipe**, **BSI (German overwrite standard by Federal Office for Information Security)**, etc.

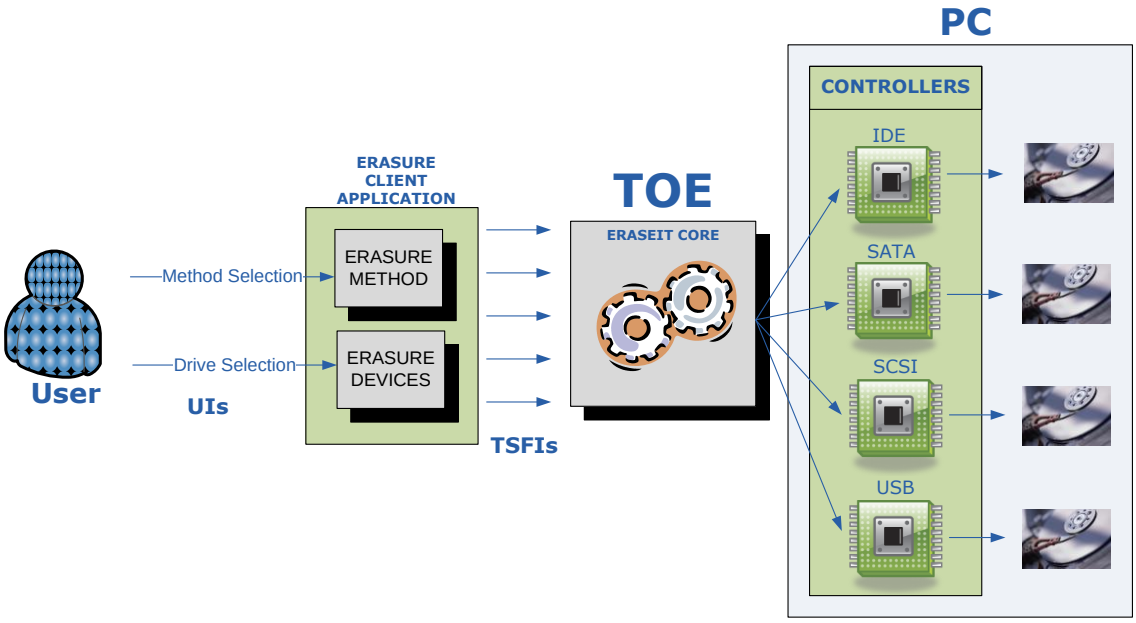

Gráfico 1

1.3.1. Logical Scope

El TOE permite a la aplicación cliente autorizada seleccionar los dispositivos que serán borrados de forma segura y el método que será utilizado para ello. Tras ser introducidos los parámetros, comienza el proceso de borrado durante el cual se realiza un registro de la operación. Al finalizar la operación la aplicación base facilitará al usuario un informe cifrado con toda la información del proceso realizado (dispositivos borrados, método utilizado y los eventos de errores que se hayan producido). En el informe se incluye información horario extraída de un servidor externo, para así confirmar el momento en el que se ha llevado a cabo la operación.

Functionalities	*Scope*	*Coms.*

Borrado seguro de datos	✓	
Selección de dispositivos a borrar	✓	
Selección de método de borrado (DoD5220.22-M, HMG Infosec Standard No:5,…)	✓	
Auditoría de proceso	✓	
Cifrado del informe de borrado	×	
Verificación horaria a través del servidor NIST	×	
Gestión de licencias de uso	×	
Panel de control web para la gestión de borrados	×	Add-on

✓ En el TOE
× Excluido del TOE

La funcionalidad excluida del TOE la proporciona la aplicación base que utiliza el TOE como núcleo de borrado, y no forma parte del alcance del TOE.

1.3.2. Physical scope

El TOE es una aplicación software y por lo tanto todo el hardware/firmware queda excluido desde el punto de vista de componentes externos (ver Gráfico 1). El TOE está formador por la distribución del sistema operativo y los ejecutables correspondientes al EraseIT Core.

2. Conformance claims

Este TOE está conforme a las siguientes especificaciones de la norma Common Criteria:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 R3
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1 R3
- EAL 1 + ALC_FLR.1 + ASE_SPD.1 + ASE_OBJ.2 + ASE_REQ.2

3. Terminology

borrado seguro	Proceso de sobreescritura de un dispositivo de almacenamiento que garantiza la confidencialidad de la información que guarda.
dispositivo de almacenamiento	Dispositivos de almacenamiento masivo de datos. Ej. Disco duro, memoria USB, etc.

operación de borrado seguro	Proceso de borrado seguro de datos de un dispositivo de almacenamiento en todos los sectores del mismo.
método de borrado seguro	Conjunto de operaciones de borrado que componen un proceso de borrado seguro de datos.
aplicación cliente autorizada	Aplicación cliente que se conecta con EraseIT Core utilizando un canal de comunicación seguro.
funciones de selección de método de borrado seguro	Conjunto de funciones que permiten a la aplicación cliente autorizada la elección de un método de borrado seguro.
funciones de selección de dispositivos de almacenamiento	Conjunto de funciones que permiten a la aplicación cliente autorizada la elección de un conjunto de dispositivos de almacenamiento masivo de datos.
todas las funciones del TOE	Conjunto de funciones definidas en la interfaz de conexión entre el TOE y la aplicación cliente autorizada (TSFIs).

4.Security problem definition

4.1. Introduction

El problema de seguridad que se quiere resolver es la confidencialidad de los datos almacenados en los dispositivos.

4.2. Threats

Nombre	*Descripción*
T.DATA_RECOVERY	Un usuario con acceso al disco tras la realización del proceso de borrado pueda realizar una recuperación de los datos originales.
T.NOT_AUTHORIZED	Una aplicación cliente no autorizada pueda comunicarse con el TOE.
T.NOT_PRIVACY	Una aplicación cliente no autorizada pueda conocer los datos transmitidos en la

	comunicación entre el TOE y una aplicación cliente autorizada.

4.3. Organisational security policies

Nombre	*Descripción*
P.AUDIT	El TOE implementará una funcionalidad de auditoría que posibilitará la explotación posterior de las operaciones realizadas para su análisis en grandes flotas.
P.METHOD_SELECTION	El TOE implementará la posibilidad de seleccionar el método de borrado por parte de la aplicación cliente autorizada, para que así pueda realizar el proceso según lo especificado en la norma deseada (Ej. DoD5220.22-M, HMG Infosec Standard No:5, …).
P.DEVICE_SELECTION	El TOE implementará la posibilidad de seleccionar por parte de la aplicación cliente autorizada los dispositivos sobre los que se realizará la operación de borrado seguro de datos.

4.4. Assumptions

Nombre	*Descripción*
A.CODE	Se asume que no se ha ejecutado código por un atacante de manera previa al arranque del TOE.

5.Security objectives

5.1. Security objectives for the TOE

Nombre	*Descripción*
O.DATA_ERASURE	El TOE eliminará la información almacenada en los dispositivos de almacenamiento sobre los que se realiza el proceso de borrado

	seguro.
O.AUDIT	El TOE generará un log que almacenará información sobre el proceso de borrado seguro.
O.METHOD_SELECTION	El TOE dará a la aplicación cliente autorizada la posibilidad de seleccionar el método que se utilizará para la realización del proceso de borrado seguro.
O.DEVICE_SELECTION	El TOE dará a la aplicación cliente autorizada la posibilidad de seleccionar los dispositivos sobre los que se realizará la operación de borrado seguro de datos.
O.TRUSTED_CHANNEL	El TOE provee a la aplicación cliente autorizada un canal de comunicación seguro garantizando que el TOE se está comunicando con una aplicación cliente autorizada y la confidencialidad de la información que se transmite.

5.2. Security objectives for the operational environment

Nombre	*Descripción*
OE.CODE	El entorno debe garantizar que ningún atacante pueda ejecutar código de manera previa al arranque del TOE.

5.3. Relation between security objectives and the security problem definition

5.3.1. Tracing between security objectives and the security problem definition

OBJETIVOS	***AMENAZAS***			***POLÍTICAS***			***HIPÓTESIS***
	T.DATA_ RECOVERY	*T.NOT_ AUTHORIZED*	*T.NOT_ PRIVACY*	*P.AUDIT*	*P.METHOD_ SELECTION*	*P.DEVICE_ SELECTION*	*A.CODE*
O.DATA_ ERASURE	☑						

O.AUDIT				☑			
O.METHOD_ SELECTION					☑		
O.DEVICE_ SELECTION						☑	
O.TRUSTED_CHANNEL		☑	☑				
OE.CODE							☑

5.3.2. Providing a justification for the tracing

O.DATA_ERASURE - T.DATA_RECOVERY

Si se elimina la amenaza de que un usuario pueda recuperar los datos almacenados en un disco, se garantizará la confidencialidad de los mismos.

O.AUDIT – P.AUDIT

Si se realiza un log de las operaciones de borrado seguro de datos utilizando una política de seguridad adecuada, se conseguirá el objetivo de auditar el proceso de borrado.

O.METHOD_SELECTION - P.METHOD_SELECTION

Si se aplica una política de seguridad adecuada, la aplicación base posibilitará a la aplicación cliente autorizada la elección del método de borrado seguro de sus datos.

O.DEVICE_SELECTION - P.DEVICE_SELECTION

Si se aplica una política de seguridad adecuada, la aplicación base posibilitará a la aplicación cliente autorizada la elección de la lista de dispositivos que serán borrados de forma segura.

O.TRUSTED_CHANNEL - T.NOT_AUTHORIZED

Si se elimina la amenaza de que una aplicación cliente no autorizada pueda conectarse con el TOE, se proveerá de un canal de comunicación seguro para aplicaciones cliente autorizadas.

O.TRUSTED_CHANNEL - T.NOT_PRIVACY

Si se elimina la amenaza de que una aplicación cliente no autorizada pueda conocer los datos transmitidos en la comunicación entre el TOE y una aplicación cliente autorizada, se proveerá de una canal de comunicación seguro para aplicaciones cliente autorizadas que garantice la privacidad de la información transmitida.

A.CODE- OE.CODE

Si se asume que ningún usuario puede ejecutar código de forma previa al arranque del TOE se consigue el objetivo de garantizar que ningún atacante pueda ejecutar código de manera previa al arranque del mismo.

5.4. Security objectives: conclusion

Si se consigue prevenir las amenazas e implementar las políticas de seguridad establecidas en este apartado, quedará resuelto el problema de seguridad de este producto.

6. Extended Components Definition

No es necesaria la definición de ningún componente extendido.

7. Security requirements

7.1. Security functional requirements

Class FDP		
FDP_RIP.1 Residual information protection		
	FDP_RIP.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: deallocation of the resource from] the following objects: [assignment: dispositivos de almacenamiento].
Class FAU		
FAU_GEN.1 Security audit data generation		
	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:

		not specified] level of audit; and c) [assignment: en cada operación de borrado seguro].
	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, 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: método de borrado seguro utilizado, dispositivo borrado]. NOTA: el método de borrado y el dispositivo han sido seleccionados por el usuario tal y como se indica en FMT_SMF.1
	Se elimina la dependencia de *FMT_STM.1 – Time stamps* debido a que el TOE no proporciona una fuente de tiempo, se utiliza una fuente externa al TOE.	
Class FMT		
FMT_SMF.1 - Specification of Management Functions		
	FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [assignment: seleccionar método de borrado seguro, seleccionar dispositivos sobre los que realizar la operación de borrado seguro].
Class FTP		
FTP_ITC.1 – Inter-TSF trusted channel		
	FTP_ITC.1.1	º identification of its end points and protection of the channel data from modification or disclosure.
	FTP_ITC.1.2	The TSF shall permit [selection: aplicación cliente autorizada] to initiate communication via the trusted channel.

	FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment: todas las funciones del TOE].

7.2. Relation between SFRs and security objectives

Security Objectives	SFRs			
	FDP_RIP.1	FAU_GEN.1	FMT_SMF.1	FTP_ITC.1
O.DATA_ ERASURE	☑			
O.AUDIT		☑		
O.METHOD_ SELECTION			☑	
O.DEVICE_ SELECTION			☑	
O.TRUSTED_ CHANNEL				☑

7.3. Tracing between SFRs and the security objectives for the TOE

O.DATA_ERASURE – FDP_RIP.1

Si la TSF del producto garantiza que cualquier información almacenada en un dispositivo de almacenamiento será borrado de forma segura se conseguirá el objetivo de mantener la confidencialidad de dicha información.

O.AUDIT – FAU_GEN.1

Si la TSF registra los eventos del proceso de borrado seguro de datos se conseguirá el objetivo de auditoría del mismo.

O.METHOD_SELECTION - FMT_SMF.1

Si la TSF ofrece la posibilidad de ejecución de las funciones de elección del método de borrado a cualquier aplicación cliente autorizada con un único rol definido, se conseguirá el objetivo de que la aplicación cliente autorizada seleccione un método de

borrado acorde a lo especificado en diferentes normas (Ej. DoD5220.22-M, HMG Infosec Standard No:5, etc.).

O.DEVICE_SELECTION - FMT_SMF.1

Si la TSF ofrece la posibilidad de ejecución de las funciones de elección de los dispositivos a borrar de forma segura aplicación cliente autorizada con único rol definido, se conseguirá el objetivo de que la aplicación cliente autorizada seleccione cualquier abanico de dispositivos de almacenamiento a borrar de forma segura.

O.TRUSTED_CHANNEL – FTP_ITC.1

Si la TSF provee un canal de comunicación seguro entre el TOE y una aplicación remota autorizada, se conseguirá el objetivo de proveer a la aplicación cliente autorizada de un canal seguro de comunicación y la confidencialidad de la información que se transmite.

7.4. Security assurance requirements (SARs)

Class ADV: Development		
ADV_FSP.1 Basic functional specification		
	ADV_FSP.1.1D	The developer shall provide a functional specification.
	ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
	ADV_FSP.1.1C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
	ADV_FSP.1.2C	The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.
	ADV_FSP.1.3C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
	ADV_FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and

		presentation of evidence.
	ADV_FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.
Class AGD: Guidance documents		
AGD_OPE.1 Operational user guidance		
	AGD_OPE.1.1D	The developer shall provide operational user guidance.
	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 fulfill 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.
	AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1 Preparative procedures		
	AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.
	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.
	AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.
ALC_CMC.1 Labeling of the TOE		
	ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
	ALC_CMC.1.1C	The TOE shall be labeled with its unique reference.

	ALC_CMC.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_CMS.1 TOE CM coverage		
	ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
	ALC_CMS.1.1C	The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs
	ALC_CMS.1.2C	The configuration list shall uniquely identify the configuration items.
	ALC_CMS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_FLR.1 Basic flaw remediation		
	ALC_FLR.1.1D	The developer shall document flaw remediation procedures addressed to TOE developers.
	ALC_FLR.1.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
	ALC_FLR.1.2C	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
	ALC_FLR.1.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
	ALC_FLR.1.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

	ALC_FLR.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
Class ASE: Security Target evaluation		
ASE_CCL.1 Conformance claims		
	ASE_CCL.1.1D	The developer shall provide a conformance claim.
	ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
	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.
	ASE_CCL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1 Extended components definition		
	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.
	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.1.2C5	The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.
	ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly expressed using existing components.
ASE_INT.1 ST introduction		
	ASE_INT.1.1D	The developer shall provide an ST introduction.
	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 summarize 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.
	ASE_INT.1.1E	The evaluator shall confirm that the information provided meets all

		requirements for content and presentation of evidence.
	ASE_INT.1.2E	The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.
ASE_OBJ.2 Security objectives		
	ASE_OBJ.2.2D	The developer shall provide a statement of security objectives.
	ASE_OBJ.2.1D	The developer shall provide a security objectives rationale.
	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.
	ASE_OBJ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and

		presentation of evidence.
ASE_REQ.2 Derived security requirements		
	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.
	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.
	ASE_REQ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification		
	ASE_TSS.1.1D	The developer shall provide a TOE summary specification.
	ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.
	ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.
ASE_SPD.1 Security problem definition		
	ASE_SPD.1.1D	The developer shall provide a security problem definition.
	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.
	ASE_SPD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
Class ATE: Tests		
ATE_IND.1 Independent testing – conformance		
	ATE_IND.1.1D	The developer shall provide the TOE for testing.
	ATE_IND.1.1C	The TOE shall be suitable for testing.

	ATE_IND.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	ATE_IND.1.2E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.
Class AVA: Vulnerability assessment A		
AVA_VAN.1 Vulnerability survey		
	AVA_VAN.1.1D	The developer shall provide the TOE for testing.
	AVA_VAN.1.1C	The TOE shall be suitable for testing.
	AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
	AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

7.5. SARs and the security requirement rationale

Los SARs especificados han sido elegidos por demanda del mercado.

8.TOE summary specification

SF.OVERWRITE

La TSF se encarga del borrado seguro de los dispositivos de almacenamiento mediante la sobreescritura de los mismos determinada por un conjunto de pasadas fijas o aleatorias que componen el método de borrado.

SF.AUDIT

La TSF genera un informe de borrado que almacena la información relativa al proceso de borrado seguro. Almacena el comienzo y el fin de las operaciones, información de los dispositivos que se han borrado de forma segura y el método de borrado utilizado en el proceso.

SF.METHOD_SELECTION

La TSF permite a la aplicación base la elección por parte del usuario del método de borrado a utilizar en el proceso de borrado seguro. El método de borrado consta de al menos una pasada de sobreescritura del dispositivo con valor fijo o aleatorio y con posibilidad de verificación de la misma.

SF.DEVICE_SELECTION

La TSF permite a la aplicación base la elección de los dispositivos que serán borrados durante el proceso de borrado.

SF.TRUSTED_CHANNEL

La TSF proveerá a la aplicación cliente autorizada un canal seguro de comunicación que garantice la confidencialidad de la información transmitida.

SF.OVERWRITE asegura que toda la información de los dispositivos ha sido borrada de forma segura. Por lo tanto FDP_RIP.1 se cumple.

SF.AUDIT asegura que se audita el proceso de borrado con la información de los dispositivos y el método de borrado utilizado, además de los tiempos en que se han realizado. Por lo tanto FAU_GEN.1 se cumple.

SF.METHOD_SELECTION y SF.DEVICE_SELECTION aseguran que la aplicación base puede elegir los dispositivos y el método de borrado a utilizar durante el proceso de borrado. Por lo tanto FMT_SMF.1 se cumple.

SF.TRUSTED_CHANNEL asegura que el TOE provee a la aplicación cliente de un canal seguro de comunicación. Por lo tanto FTP_ITC.1 se cumple.

SFRs	Security functionalities				
	SF.OVERWRITE	SF.AUDIT	SF.METHOD_ SELECTION	SF.DEVICE_ SELECTION	SF.TRUSTED_ CHANNEL
FDP_RIP.1	☑				
FAU_GEN.1		☑			
FMT_SMF.1			☑	☑	
FTP_ITC.1					☑