Borrado Seguro Anova

Declaración de Seguridad

Nombre y Versión Producto: Borrado Seguro Anova - V1.2.0
Versión Documento: V0.8
Fabricante: Anova IT Consulting, S.L.
Fecha Edición: Diciembre 2009

1. Contenido

1. Tabla de versiones

Versión	Fecha	Autor	Descripción
0.1	28/07/2009	Miguel Ruiz – Anova	Primer borrador
0.2	05/10/2009	Miguel Ruiz - Anova	Segundo borrador
0.3	26/10/2009	Ángel Arias - Anova	Versión Certificación
0.4	28/10/2009	Ángel Arias – Anova	Versión Certificación
0.5	03/11/2009	Ángel Arias – Anova	Cambios post evaluación ASE
0.6	11/11/2009	Ángel Arias – Anova	Cambios
0.7	16/11/2009	Ángel Arias – Anova	Cambios post evaluación ATE
0.8	11/12/2009	Ángel Arias – Anova	Cambios AVA, corrección Errores, Versión TOE V1.2.0

2. Introducción

Esta declaración de seguridad establece las bases para la evaluación Common Criteria del Producto "Borrado Seguro Anova".

2.1 Identificación

2.1.1. Identificación de la Declaración de Seguridad (DS):

Título: Declaración de seguridad Borrado Seguro Anova

Versión: V0.8

Autor: Anova IT Consulting, S.L.

Fecha de publicación: 16 de Noviembre de 2009

2.1.2. Identificación del Objeto a evaluar (TOE):

Fabricante: Anova IT Consulting, S.L.

Nombre del Producto: Borrado Seguro Anova

Versión: V1.2.0

2.2 TOE overview

El producto Borrado Seguro Anova (**BSA**) es un sistema que permite realizar el borrado seguro de los datos contenidos en los dispositivos de almacenamiento conectado a un equipo.

BSA se presenta como un CD autoarrancable acompañado de una memoria extraíble USB donde está almacenado el paquete de licencias necesario para el funcionamiento de la aplicación.

BSA permite elegir de entre una serie de métodos predefinidos y métodos definidos por el usuario.

Se puede seleccionar un método predefinido de entre los métodos más utilizados en cuanto a número de pasadas y caracteres empleados

Si se elige el método personalizado, el usuario puede definir tantas pasadas de borrado como precise. En cada una de las pasadas se definirá: el carácter empleado (fijo o aleatorio) y si se realiza la verificación tras el borrado.

Siguiendo unas sencillas indicaciones permite iniciar el proceso de borrado de los dispositivos.

Después del proceso de borrado y verificación (si existe) se generará auditoria referente al resultado del proceso de borrado.

Finalizado el proceso se presenta en pantalla el resultado del mismo y almacena dicho resultado en un archivo de texto para su comprobación posterior.

El conjunto de elementos Hardware, Software and firmware no pertenecientes al TOE son los siguientes:

- Máquina X86 con lector de dispositivo óptico disponible
- RAM minima: 128 Mb
- Discos Duros tipo IDE y SATA.

A continuación se detallan los discos duros de la máquina entregada al laboratorio para proceder con su prueba.

TIPO	FABRICANTE	MODELO	INTERFACE	CAPACIDAD
Disco Duro	WESTERN DIGITAL	WD400BB	IDE	40 GB
Disco Duro	WESTERN DIGITAL	WD400BD	SATA	40 GB
Disco Duro	MAXTOR	31024H1	IDE	10 GB
Disco Duro	SEAGATE	ST3802110A	IDE	80 GB
Disco Duro	SEAGATE	ST380013AS	SATA	80 GB
Controladora	Intel® 82801E	Communications I/O	SATA/IDE	

2.3 TOE description

Descripción

BSA realiza el borrado seguro de datos por método de sobreescritura sobre los dispositivos de almacenamiento seleccionados.

La aplicación genera, al final del proceso, un informe en el que se detallan las operaciones realizadas.

Una vez finalizado el proceso de borrado seguro sobre un dispositivo de almacenamiento, los datos que éste contuviera no podrán ser recuperados con ningún método conocido.

El proceso de borrado es muy sencillo:

- Se inicia la aplicación.
- Se muestran los dispositivos detectados en el equipo y se permite seleccionar los dispositivos sobre los que realizar el borrado.
- Se selecciona el método de borrado
- Al aceptar el borrado se inicia el mismo mostrando la pantalla de seguimiento del proceso.
- Una vez finalizado se muestra un resumen del resultado permitiendo almacenar el informe de borrado en un dispositivo extraíble.

Presentación y alcance

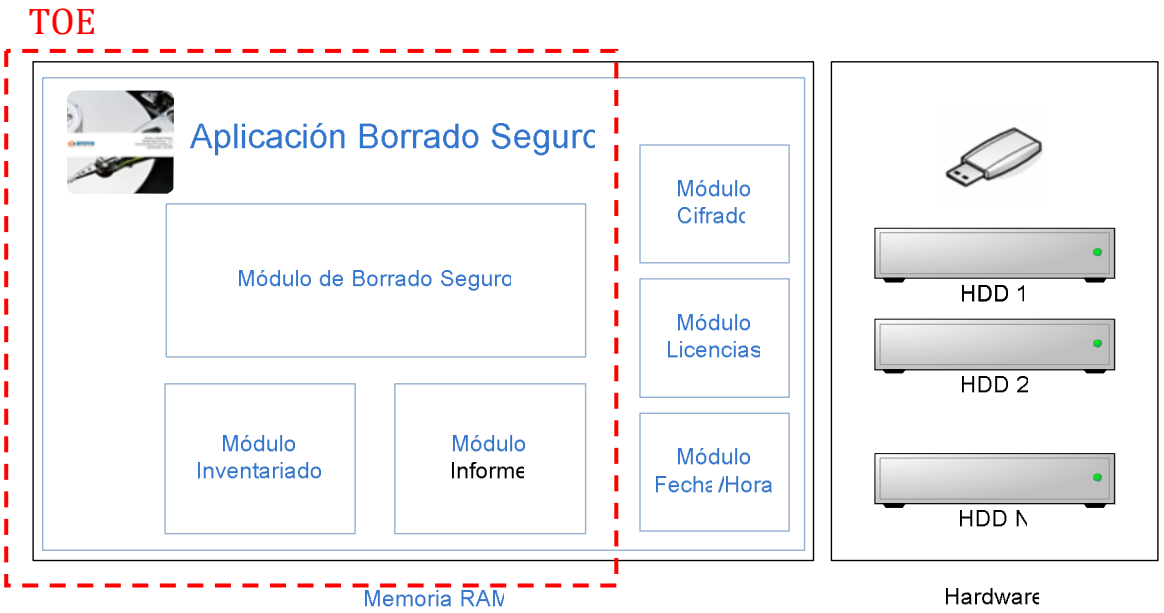
La aplicación se entrega como un Cd-Autoarrancable acompañado de una memoria extraíble USB en donde está almacenada el paquete de licencias necesario para el funcionamiento de la aplicación.

El CD arranca un S.O. Linux y lanza la aplicación de borrado en modo exclusivo.

El CD autoarrancable se puede utilizar en todos aquellos equipos con arquitectura x86.

Ámbito físico y lógico

El TOE es una aplicación SW, por lo que todo el Hardware y Firmware queda excluido del mismo formando parte del entorno. Al ser una aplicación autoejecutable que se carga durante el arranque del sistema desde CD, no existe ningún SW externo con el que interactúe. A continuación se incluye un grafico de contexto del TOE.



Modulo de borrado

Tras seleccionar los dispositivos de almacenamiento y el método de borrado a utilizar. BSA realiza el borrado seguro de datos por método de sobreescritura sobre los dispositivos de almacenamiento seleccionados.

La aplicación puede realizar el borrado seguro en los dispositivos más comunes como son: IDE, SATA y memorias externas USB

Existe un matiz, en el caso de memorias externas USB tipo U3, solo se realiza el borrado seguro sobre la parte correspondiente al disco, dejando la unidad de CD intacta.

Módulo de inventario

Antes de la realización del borrado, el módulo de inventario recopila toda la información del HW del equipo y la incluye dentro del informe de operación.

Fecha en que se ha realizado la operación de borrado

En un equipo informático la fecha actual es un parámetro almacenado y mantenido "en hora" por la BIOS del propio equipo. Si esta hora es alterada, por fallos en la pila que mantiene en funcionamiento la BIOS o porque es modificada por el propio usuario, la fecha anotada en el informe de operación puede no ser correcta.

Para evitar esto, si el equipo se encuentra conectado a Internet, la aplicación realiza una consulta a un servidor de hora en internet (ITS) del NIST, en el informe se almacena tanto la hora presente en la BIOS como la recibida desde el servidor de Internet.

Con este método podemos conocer y certificar, en cierta medida, que la hora en la que se ha realizado la operación es la correcta.

Informe de borrado

Al final de la operación de borrado se genera un informe que recoge todos los datos de la operación realizada pudiendo distinguir la siguiente información:

- Información de Inventario
  - CPU, Memoria, Tarjetas de red,…
- Información de borrado
  - Método de borrado utilizado
  - Marca, modelo, S/N y tamaño en Sectores de cada uno de los dispositivos.
  - Resultado del proceso de borrado, que puede tomar uno de los dos valores siguientes:
    - Borrado Terminado Correctamente
    - Borrado Fallido

Para evitar que el informe pudiera ser alterado y poder asegurar la integridad del mismo tras enviarse por algún medio, se procede a cifrar todo los bloques con una clave simétrica (AES).

Para poder visualizar el informe de borrado se dispone de una aplicación externa de visualización de informes.

El informe generado, con todos sus módulos, se almacenará en el primer sector del dispositivo borrado para poder ser recuperado con posterioridad.

Módulo de Licencias

Para poder realizar la operación de borrado es necesario disponer de una memoria externa USB que contenga un paquete de licencias.

Se consume una licencia por cada disco borrado.

Se deberá presentar al USB el principio y al final de la operación de borrado para dar por concluida la operación.

Funcionalidad	Proporcionada por el TOE
Módulo de Borrado y verificación	Si
Módulo de Inventariado	Si
Módulo de generación de Informes de borrado	Si
Módulo de Fecha y Hora	No
Módulo de Cifrado	No
Módulo de Licencias	No

2.4 Platform Requirements

Requisitos BSA:

- Máquina X86 con lector de dispositivo óptico disponible
- RAM minima: 128 Mb
- Discos Duros tipo IDE y SATA.

3. Conformidades

Esta declaración de seguridad cumple con los requisitos de las siguientes normas:

- Norma CC v.3.1, partes 2 y 3 revisión 3
- ISO/IEC 15408:2009, partes 2 y 3

Define un nivel de garantía de evaluación EAL1 + ASE_SPD.1+ ASE_OBJ.2 ASE_REQ.2; ALC_FLR.1

4. Definición del problema de seguridad

El activo principal protegido por la aplicación Borrado seguro Anova (BSA) es:

“La confidencialidad de los datos”

Se entiende por atacante a cualquier usuario de la aplicación.

4.1 Amenazas

AM1: Después de ejecutar el proceso de borrado satisfactoriamente, cualquier atacante consigue comprometer la confidencialidad de los datos de usuario, accediendo a los datos almacenados previamente en los dispositivos borrados.

4.2 Políticas de seguridad

OSP1: Al finalizar el proceso de borrado se genera un informe en el que se recoge el log de actividades realizadas. Este informe se almacena en el primer sector del dispositivo borrado y puede salvarse en un dispositivo externo. Para su visualización en un equipo externo al sistema.

4.3 Hipótesis

HIP1: La hora que utiliza el TOE para indicar el momento en el que se ha realizado cada actividad es aportada por el entorno con suficiente fiabilidad.

HIP2: No se permite tomar el control del equipo con anterioridad a la ejecución del TOE, impidiendo así la posibilidad de ejecutar código malicioso que interfiera en la ejecución satisfactoria del TOE.

5. Objetivos de seguridad

5.1 Objetivos de seguridad para el TOE

OT1: El producto realiza el borrado de los datos de los dispositivos seleccionados siguiendo el método preconfigurado y/o configurado por el usuario.

OT2: El producto generará un informe de la actividad realizada que incluirá: el inventario HW del equipo, los dispositivos, el método y el resultado de la operación de borrado sobre los dispositivos y permite su revisión por el usuario.

	AM1	OSP1
OT1	X	
OT2		X

El Objetivo de seguridad 1 (OT1) mitiga la amenaza 1 (AM1) por cuanto la realización del borrado seguro inhabilita la posterior recuperación de los datos almacenados previamente.

El Objetivo de seguridad 1 (OT2) cumple la política de seguridad (OSP1) implementándola en su totalidad.

5.2 Objetivos de seguridad para el entorno

OE1: El entorno facilitará una fuente de tiempo suficientemente fiable en sus dos modos de obtención:

- Hora aportada por la BIOS del sistema
- Hora de un servidor externo de hora NTP

En el caso que la conexión a internet no se encuentre habilitada en el informe se indicará como "No Disponible" en el apartado de Hora de Internet.

El objetivo de entorno 1 (OE1) cumple la hipótesis 1(HIP1).

OE2: El entorno debe garantizar que no se ejecuta código malicioso que interfiera en la práctica satisfactoria del TOE.

El objetivo de entorno 2 (OE2) cumple la hipótesis 1(HIP2).

	HIP1	HIP2
OE1	X	
OE2		X

6. Requisitos de seguridad

6.1 Requisitos funcionales de seguridad referente al TOE

6.1.1. Residual information protection (FDP_RIP)

This family addresses the need to ensure that any data contained in a resource is not available when the resource is de-allocated from one object and reallocated to a different object. This family requires protection for any data contained in a resource that has been logically deleted or released, but may still be present within the TSF-controlled resource which in turn may be re-allocated to another object.

FDP_RIP.1 Subset residual information protection, requires that the TSF ensure that any residual information content of any resources is unavailable to a defined subset of the objects controlled by the TSF upon the resource's allocation or deallocation.

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [al finalizar la operación de borrado satisfactoriamente] the following objects: [dispositivos de almacenamiento dentro de los tipos:

- Discos IDE
- Discos SATA

- Discos Externos USB].

6.1.2. Specification of Management Functions (FMT_SMF)

This family allows the specification of the management functions to be provided by the TOE. Management functions provide TSFI that allow administrators to define the parameters that control the operation of security-related aspects of the TOE, such as data protection attributes, TOE protection attributes, audit attributes, and identification and authentication attributes. Management functions also include those functions performed by an operator to ensure continued operation of the TOE, such as backup and recovery. This family works in conjunction with the other components in the FMT: Security management class: the component in this family calls out the management functions, and other families in FMT: Security management restrict the ability to use these management functions.

FMT_SMF.1 Specification of Management Functions requires that the TSF provide specific management functions.

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [Modificar el método de borrado y los dispositivos sobre los que se realiza el borrado. Esta acción se podrá realizar por el usuario antes de la operación de borrado].

6.1.3. Security audit data generation (FAU_GEN)

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

FAU_GEN.1 Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.

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 *not specified* level of audit; and

c) [El resultado del proceso de borrado y verificación.].

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, [El informe contiene información de la actividad realizada incluyendo: el inventario HW del equipo, los dispositivos, el método y el resultado de la operación de borrado sobre los dispositivos].

	OT1	OT2
FDP_RIP.1	X	
FMT_SMF.1	X	
FAU_GEN.1		X

Con estos requisitos de seguridad seleccionados dejamos resueltos los objetivos de seguridad planteados ya que:

- El requisito de seguridad FDP_RIP.1 alcanza el OT1 por cuanto se realiza el borrado seguro de los datos almacenados de un modo que asegura que no queda ninguna información residual al finalizar el proceso de borrado satisfactoriamente.

- A su vez el modo en que se realiza ese borrado puede ser modificado en el modo especificado en el requisito FMT_SMF.1 en el que se especifica que es posible modificar el método y los dispositivos a borrar.
- El OT2 queda cubierto en su totalidad en el requisito FAU_GEN.1 en el que queda especificado como es el informe generado por el TOE y que cubre todos los objetivos expresados en el OT2.

La dependencia de FPT_STM.1 en FAU_GEN.1 no se satisface debido a que el tiempo se obtiene de fuentes externas.

6.2 Requisitos de garantía de seguridad

La evaluación se realizará conforme al nivel de garantía definido por:

EAL1 + ASE_SPD.1+ ASE_OBJ.2 + ASE_REQ.2 + ALC_FLR.1.

6.2.1. Evaluation assurance level 1 (EAL1) - functionally tested

La selección del nivel de evaluación, EAL1, se justifica por razones de mercado.

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage ALC_FLR.1 Basic Flaw Remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

ADV_FSP.1 Basic functional specification

Dependencies: No dependencies.

Developer action elements:

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.

Content and presentation elements:

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

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.

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.

Evaluator action elements:

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

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.

Evaluator action elements:

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 Labelling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Objectives

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labelling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMC.1.1C The TOE shall be labelled with its unique reference.

Evaluator action elements:

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

Dependencies: No dependencies.

Objectives

A CM system can control changes only to those items that have been placed under CM (i.e., the configuration items identified in the configuration list). Placing the TOE itself and the evaluation evidence required by the other SARs in the ST under CM provides assurance that they have been modified in a controlled manner with proper authorisations.

Application notes

ALC_CMS.1.1C introduces the requirement that the TOE itself and the evaluation evidence required by the other SARs in the ST be included in the configuration list and hence be subject to the CM requirements of CM capabilities (ALC_CMC).

Developer action elements:

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

ALC_FLR.1 Basic flaw remediation

Dependencies: No dependencies.

Developer action elements:

ALC_FLR.1.1D The developer shall document and provide flaw remediation procedures addressed to TOE developers.

Content and presentation elements:

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.

Evaluator action elements:

ALC_FLR.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

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.

Evaluator action elements:

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

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.

Evaluator action elements:

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

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.

Evaluator action elements:

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

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_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.

Evaluator action elements:

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

APE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

APE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

APE_SPD.1.1C The security problem definition shall describe the threats.

APE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

APE_SPD.1.3C The security problem definition shall describe the OSPs.

APE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

APE_SPD.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

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.

Evaluator action elements:

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.

ATE_IND.1 Independent testing - conformance

Dependencies: ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Objectives

In this component, the objective is to demonstrate that the TOE operates in accordance with its design representations and guidance documents.

Application notes

This component does not address the use of developer test results. It is applicable where such results are not available, and also in cases where the developer's testing is accepted without validation. The evaluator is required to devise and conduct tests with the objective of confirming that the TOE operates in accordance with its design representations, including but not limited to the functional specification. The approach is to gain confidence in correct operation through representative testing, rather than to conduct every possible test. The extent of testing to be planned for this purpose is a methodology issue, and needs to be considered in the context of a particular TOE and the balance of other evaluation activities.

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

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.

AVA_VAN.1 Vulnerability survey

Dependencies: ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Objectives

A vulnerability survey of information available in the public domain is performed by the evaluator to ascertain potential vulnerabilities that may be easily found by an attacker.

The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Basic.

Developer action elements:

AVA_VAN.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7. Resumen de la especificación del TOE

En el presente documento se han dado respuesta a todas las cuestiones relativas a cual es la funcionalidad ofrecida por el producto Borrado Seguro Anova, identificando claramente qué soluciones aporta, en ante su principal función que es la de eliminar de modo, que no pueda ser recuperada, la información almacenada en un dispositivo de almacenamiento tras realizar el proceso de borrado seguro.

7.2 IT Security Functions

Esta sección muestra las funciones de seguridad realizadas por el TOE, además de la relación entre estos y los requisitos funcionales de seguridad.

IT SECURITY FUNCTION LABEL	**IT Security Function Description**
Borrado	*FDP_RIP.1* El TOE utiliza funciones de bajo nivel para escribir el carácter hexadecimal seleccionado en todas las posiciones de memoria del disco duro seleccionado. Si se produce un fallo en la escritura es detectado y abortado el proceso.
Gestión	FMT_SMF.1 El TOE permite al usuario seleccionar los discos duros en los que realizar el borrado. A su vez permite elegir tanto entre una lista de métodos de borrado predefinidos como crear un método personalizado. Los datos característicos de un método son los siguientes: pasada, carácter de borrado y si realiza verificación o no.
Auditoría	FAU_GEN.1 El TOE proporcionará un informe final de borrado en el que se especifica el borrado utilizado, resultado de operación, la fecha y información la licencia utilizada.