Universitat d'Alacant
Universidad de Alicante

Servicio de Informática

# PROCEDIMIENTO PARA EL BORRADO Y LA DESTRUCCIÓN DE SOPORTES DE ALMACENAMIENTO DE INFORMACIÓN.

**Versión 1**

## 1.- Objeto

El objeto del presente documento es la definición del procedimiento el borrado y la destrucción para de soportes de almacenamiento de información.

## 2.- Ámbito de aplicación

Este Procedimiento es de aplicación a todo el ámbito de actuación de la Universidad de Alicante, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información y en las Normas de Seguridad de la misma.

El presente Procedimiento es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Universidad de Alicante, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de la misma.

En el ámbito de la presente normativa, se entiende por usuario cualquier empleado público perteneciente o ajeno a la Universidad de Alicante, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la Universidad y que utilice o posea acceso a los Sistemas de Información de la misma.

## 3.- Vigencia

El presente Procedimiento ha sido aprobado por la Comisión TI de la Universidad de Alicante, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la misma pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la Universidad de Alicante.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de este procedimiento.

## 4.- Revisión y evaluación

La gestión de este Procedimiento corresponde al Responsable de Seguridad, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.

-Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.

- Verificar su efectividad.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Responsable de Seguridad revisará el presente Procedimiento, que se someterá, de haber modificaciones, a la aprobación de la Comisión TI de la Universidad de Alicante.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento

## 5.- Procedimiento de borrado y destrucción

### 5.1- Definiciones

A efectos de este procedimiento, se emplea el término borrado como el procedimiento de eliminación de los datos de un soporte permitiendo la reutilización de dichos soportes, y el término destrucción como el proceso de inutilización física de soportes de almacenamiento que contengan datos electrónicos.

Se pueden distinguir tres tipos genéricos de soportes de almacenamiento ligados a tres tecnologías distintas:

- Soportes magnéticos.
- Soportes ópticos, por ejemplo, CD / DVD.
- Soportes basados en memorias de estado sólido, SSD.

Las técnicas específicas de borrado seguro son:

- La sobreescritura: Consiste en reemplazar los datos almacenados por un patrón binario de información sin sentido. La eficacia de este método depende del número de ciclos de sobreescritura. Existen procedimientos avanzados que permiten saber, con bastante precisión, la información que existía originalmente, por eso la información que se debe sobrescribir debe generar tal desorden en el soporte magnético que la recuperación de los datos originales sea prácticamente imposible. No se puede utilizar en soportes dañados ni en aquellos que no sean regrabables.

- El borrado criptográfico: Consiste en el cifrado de la información almacenada en el soporte utilizando un algoritmo de cifrado de clave privada, con una longitud de clave suficiente para que el descifrado de la información sea técnicamente inviable con las herramientas informáticas disponibles en ese momento. Seguidamente, la clave de cifrado se elimina con alguna de las técnicas de borrado seguro anteriores. Esta técnica se puede utilizar en cualquier tipo de soporte, aunque está especialmente recomendada para las memorias de estado sólido.
- La destrucción física.

### 5.2- Métodos de borrado o destrucción aplicables en cada tipo de soporte

El cuadro siguiente resume los métodos de borrado o destrucción aplicables en cada tipo de soporte:

| | Magnético | Óptico | SSD |
|---|---|---|---|
| Sobreescritura | √ | | √ |
| Borrado criptográfico | √ | | √ |
| Destrucción física | √ | √ | √ |

### 5.3- Borrado seguro

Se utilizará un software que realice la sobreescritura de la información con protocolos que hagan imposible su reconstrucción (mediante una serie consecutiva de sobreescrituras).

Se recomienda utilizar como mínimo tres pasadas de escritura (DOD 5220.22-M(e).

### 5.4- Borrado criptográfico

Se procederá al cifrado de la información con criptografía fuerte y posterior destrucción de la clave de encriptación utilizada. La clave de encriptación será lo suficientemente fuerte para impedir una desencriptación mediante un ataque de fuerza bruta.

### 5.5- Destrucción física

Se procederá a realizar tres taladros que perforen las superficies donde se almacena la información.

En caso de dispositivos ópticos se destruirá por desintegración utilizando una destructora de documentos apropiada para la destrucción de estos soportes.

### 5.6- Medios para el borrado o destrucción

El software para el borrado seguro y borrado criptográfico está disponible en la página web del Servicio de Informática.

Para la destrucción física de soportes magnéticos es necesario seguir el procedimiento de medio ambiente PM-10 gestión /retirada de equipos informáticos ya utilizados.

## 6.- Referencias

Recomendaciones para el borrado lógico de documentación electrónica y destrucción física de soportes informáticos de la Administración General del Estado. Subgrupo de trabajo de documentos electrónicos grupo de trabajo de valoración de series y funciones comunes de la AGE. Comisión superior calificadora de documentos administrativos. Documento aprobado por el Pleno de la Comisión Superior Calificadora de Documentos Administrativos de 13 de diciembre de 2017.

NIST Special Publication 800-88 Revision 1. Guidelines for Media Sanitizacion. Richard Kissel, Andrew Regenscheis, Matthew Scholl, Kevin Stine.