CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Ricardo De Jesús Delgado Montes Cargo: Coordinador Grupo de Trabajo de Servicios Tecnológicos	Nombre: Oscar Javier Asprilla Cruz Cargo: Jefe Oficina de Tecnología e Informática.	Nombre: Giselle Johana Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad. Fecha: 2018-11-27

1 OBJETIVO

Definir las directrices generales para el borrado seguro de la información en la Superintendencia de Industria y Comercio - SIC, a través de la descripción de las actividades de solicitud, preparación, ejecución e informe del resultado del borrado seguro, con el fin de preservar la confidencialidad de la información.

2 DESTINATARIOS

Este procedimiento aplica para la mesa de servicios, servidores públicos, contratistas y terceros de la entidad.

3 GLOSARIO

BORRADO SEGURO: Se refiere al procedimiento necesario para garantizar que la información existente en un medio de almacenamiento, no pueda ser recuperada a través de alguna técnica especializada.

DISPOSITIVO DE ALMACENAMIENTO: Se refiere a cualquier elemento que se utiliza para almacenar información tales como, discos duros, memorias USB, entre otros.

INFORMACIÓN DIGITAL: Cualquier tipo de información contenida en un medio digital, bien sea en forma de base de datos, en forma de archivos digitales o de intercambio.

LISTA DE ARCHIVOS: Es un término genérico que referencia al conjunto de elementos que cada sistema de archivos utiliza para guardar, tanto la información que identifica los archivos (nombre, tipo, fecha de creación, etc.), como un índice que recoge la ubicación física del contenido del archivo.

4 REFERENCIAS

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
NTC-ISO-IEC	27001:2013	Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de seguridad de la Información. Requisitos.	Aplicación total	Aplicación total

5 GENERALIDADES[1]

El ciclo de vida de la información, de forma simplificada, consta de tres fases: generación, transformación y destrucción. Toda información tiene una vida útil tanto si está en formato digital (CD, DVD, Flash USB, discos magnéticos, tarjetas de memoria, etc.) como en formatos tradicionales (papel, carpetas, entre otros). Cuando la vida de la información llega a su fin, se deben emplear mecanismos de destrucción y borrado seguro para evitar que esta quede al alcance de terceros.

Con el borrado seguro y destrucción de soportes de información no solo se busca proteger la difusión de información confidencial de la entidad, sino también proteger la fuga de datos personales de los ciudadanos que puedan contener los soportes.

Son comunes los incidentes de seguridad de la información, presentados en las organizaciones por la falta de diligencia en el borrado de la información que, por ejemplo, son arrojados en lugares públicos (papeleras, contenedores, etc.) o no son debidamente destruidos (triturados, desmagnetizados, sobrescritos, etc.), encontrando información evidentemente llamativa como datos bancarios, médicos, de menores, etc.

5.1 MÉTODOS DE BORRADO SEGURO DE INFORMACIÓN

5.1.1 Desmagnetización

La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo.

Este método es válido para la destrucción de datos de los dispositivos magnéticos, por ejemplo, discos duros, disquetes, cintas magnéticas de backup, etc. Cada dispositivo, según su tamaño, forma y el tipo de soporte magnético, necesita de una potencia específica para asegurar la completa polarización de todas las partículas.

5.1.2 Destrucción física

El objetivo de la destrucción física es la inutilización del soporte que almacena la información para evitar la recuperación posterior de los datos que almacena. Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento:

[1] Información basada en la Guía sobre borrado seguro de la información Instituto Nacional de Ciberseguridad INCIBE de España: https://www.incibe.es/protege-tu-empresa/guias/borrado-seguro-informacion-aproximacion-el-empresario

a) Desintegración, pulverización, fusión e incineración: son métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una trituradora de metal o en una planta de incineración autorizada, con las capacidades específicas para realizar estas actividades de manera eficaz, segura y sin peligro.

b) Trituración: las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles.

Como todo proceso de destrucción física, su correcta realización implica la imposibilidad de recuperación posterior por ningún medio de almacenamiento. Para el caso de los discos duros es importante asegurar que las partes internas del disco han sido destruidas eficazmente, no sólo la cubierta externa.

5.1.3 Sobre-escritura

La sobrescritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento. La sobrescritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados, por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables, como los CD's y DVD's.

5.2 VENTAJAS E INCONVENIENTES DE LOS MÉTODOS DE BORRADO SEGURO

A continuación, se presenta un resumen de las principales características y aplicabilidad de cada uno de estos métodos de borrado de información.

Destrucción física		Desmagnetización		Sobrescritura	
✓	Eliminación de forma segura de la información.	✓	Eliminación de forma segura de la información.	✓	Eliminación de forma segura de la información.
×	Un sistema de destrucción para cada soporte.	×	Una configuración del sistema para cada soporte.	✓	Una única solución para todos los dispositivos.
×	Dificultad de certificación del proceso.	×	Dificultad de certificación del proceso.	✓	Garantía documental de la operación.
×	Necesidad de transportar los equipos a una	×	Necesidad de transportar los equipos a una ubicación externa.	✓	Posibilidad de eliminación en las propias oficinas.

Destrucción física		Desmagnetización		Sobrescritura	
	ubicación externa.				
×	Medidas extraordinarias para garantizar la cadena de custodia.	×	Medidas extraordinarias para garantizar la cadena de custodia.	✓	Garantía de la cadena de custodia.
×	Destrucción de dispositivos, no regrabables, ópticos.	×	Sólo válido para dispositivos de almacenamiento magnético.	×	No válido para dispositivos no regrabables ni ópticos.
×	Destrucción definitiva y dificultad de reciclaje de materiales.	×	Tras el proceso el dispositivo deja de funcionar correctamente.	✓	Reutilización de los dispositivos con garantías de funcionamiento.

5.3 MÉTODOS NO SEGUROS DE BORRADO DE INFORMACIÓN DIGITAL

Un borrado no seguro de información digital se presenta cuando se utilizan los métodos de borrado dispuestos por el propio sistema operativo, por ejemplo, con la opción «eliminar» o la tecla «Supr» o «Delete», se borra exclusivamente de la lista de archivos sin que se elimine realmente el contenido del archivo, que permanece en la zona de almacenamiento hasta que se reutilice ese espacio con un nuevo archivo, lo cual lo hace fácilmente recuperable.

De forma específica, no son métodos de destrucción segura:

- Los comandos de borrado del sistema operativo como la opción «eliminar» o la tecla «Supr» o «Delete».

- Al formatear un dispositivo de almacenamiento, normalmente solo se sobrescribe el área donde se aloja el sistema operativo, mientras que el área de datos, donde se encuentra el contenido de los archivos, no es alterada.

5.4 BORRADO SEGURO DE LA INFORMACION EN LA SIC

Teniendo en cuenta los métodos de borrado y sus ventajas o desventajas, el siguiente cuadro presenta un resumen del tipo de destrucción más adecuado para la información de la SIC, dependiendo del soporte.

Soporte	Tipo	Destrucción física	Sobre escritura
Discos Duros.	Magnético	×	✓
Disquetes.	Magnético	×	✓
Cintas de Backup.	Magnético	×	✓
CD.	Óptico	✓	×
DVD.	Óptico	✓	×
Blu-ray Disc.	Óptico	✓	×
Memorias USB.	Electrónico	×	✓
Discos Duros SSD.	Electrónico	×	✓
Papel	Físico	✓	×

- Para aplicar el borrado seguro de información utilizando el método de destrucción física, los servidores públicos, contratistas y terceros de la entidad pueden utilizar las trituradoras de papel dispuestas en la Entidad. No obstante, antes de aplicar este método se debe tener en cuenta las tablas de retención documental de la SIC.

- Para aplicar el borrado seguro de información utilizando el método de sobrescritura, se debe seguir el presente procedimiento[2]:

6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
1	Solicitar y preparar el borrado seguro.	Solicitud de borrado seguro de información a la mesa de servicios, por medio de alguno de los siguientes canales: 1. Portal web: http://mesadeservicios.sic.gov.co/ 2. Correo electrónico: mesadeservicios@sic.gov.co 3. Llamada telefónica: Extensión 10502.	Se realiza la solicitud de borrado seguro y se prepara la ejecución, llevando a cabo las siguientes actividades: • Solicitar el borrado seguro. • Realizar backup de la información.	Servidor público y/o contratista responsable del almacén. Coordinador del Grupo de Trabajo de Servicios Tecnológicos. Jefe de la Oficina de Tecnología e Informática o quien él delegue. Coordinador, jefe de oficina, director o delegado del	Backup de la información. Correo electrónico de notificación de borrado no exitoso.

[2] El procedimiento no es aplicable para cintas de backup.

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
				área responsable de la información. Mesa de servicios	
2	Ejecutar e informar el resultado del proceso de borrado seguro.	Solicitud de borrado seguro autorizada	Se ejecuta el borrado seguro, verificando la correcta ejecución del proceso y finalmente informando al usuario. Esta etapa comprende las siguientes actividades: • Ejecutar el borrado seguro. • Informar al usuario.	Mesa de servicios.	Correo electrónico de notificación de borrado exitoso.

7 DESCRIPCION DE ETAPAS Y ACTIVIDADES

7.1 ETAPA 1: SOLICITAR Y PREPARAR EL BORRADO SEGURO

A continuación, se presentan las actividades de esta etapa:

7.1.1 Solicitar el borrado seguro.

Se debe realizar una solicitud a la mesa de servicios para el borrado seguro, a través de los canales dispuestos para tal fin, la cual puede presentarse por alguno de los siguientes casos:

a) Cuando se libera y retorna al almacén un equipo de cómputo, portátil o dispositivo de almacenamiento extraíble de propiedad de la entidad, para ser reasignado o darse de baja. En este caso, la solicitud de borrado seguro debe realizarla el servidor público y/o contratista responsable del almacén, como parte de la actividad de reintegro de bienes, a más tardar en tres (3) días hábiles posterior al retiro.

b) Cuando el equipo de cómputo, portátil o dispositivo de almacenamiento alquilado deben ser retornado al proveedor. En este caso, la solicitud debe realizarla el Coordinador del Grupo de Trabajo de Servicios Tecnológicos, jefe de la Oficina de Tecnología e Informática o jefe de área o quien ellos deleguen.

c) Cuando el borrado seguro tiene el propósito de mantener la confidencialidad de la información, por ejemplo, en el evento de finalización del periodo de retención de archivos digitales de acuerdo con las tablas de retención documental de la entidad. En este caso, la solicitud debe realizarla el coordinador, jefe de oficina, director o delegado del área responsable de la información.

Para cualquiera de los casos mencionados, la mesa de servicios será la encargada de recibir la solicitud de borrado seguro y tramitarla en las siguientes diez (10) horas. Esta solicitud deberá incluir el nombre y datos relevantes del equipo de cómputo, portátil o dispositivo de almacenamiento sobre el cual se desea realizar el procedimiento de borrado seguro.

7.1.2 Realizar backup de la información

La mesa de servicios, antes de realizar el borrado seguro debe realizar un backup de toda la información del equipo de cómputo, portátil o dispositivo de almacenamiento, a menos que el usuario solicitante indique expresamente en el requerimiento que no es necesario.

7.2 ETAPA 2: EJECUTAR E INFORMAR EL RESULTADO DEL BORRADO SEGURO

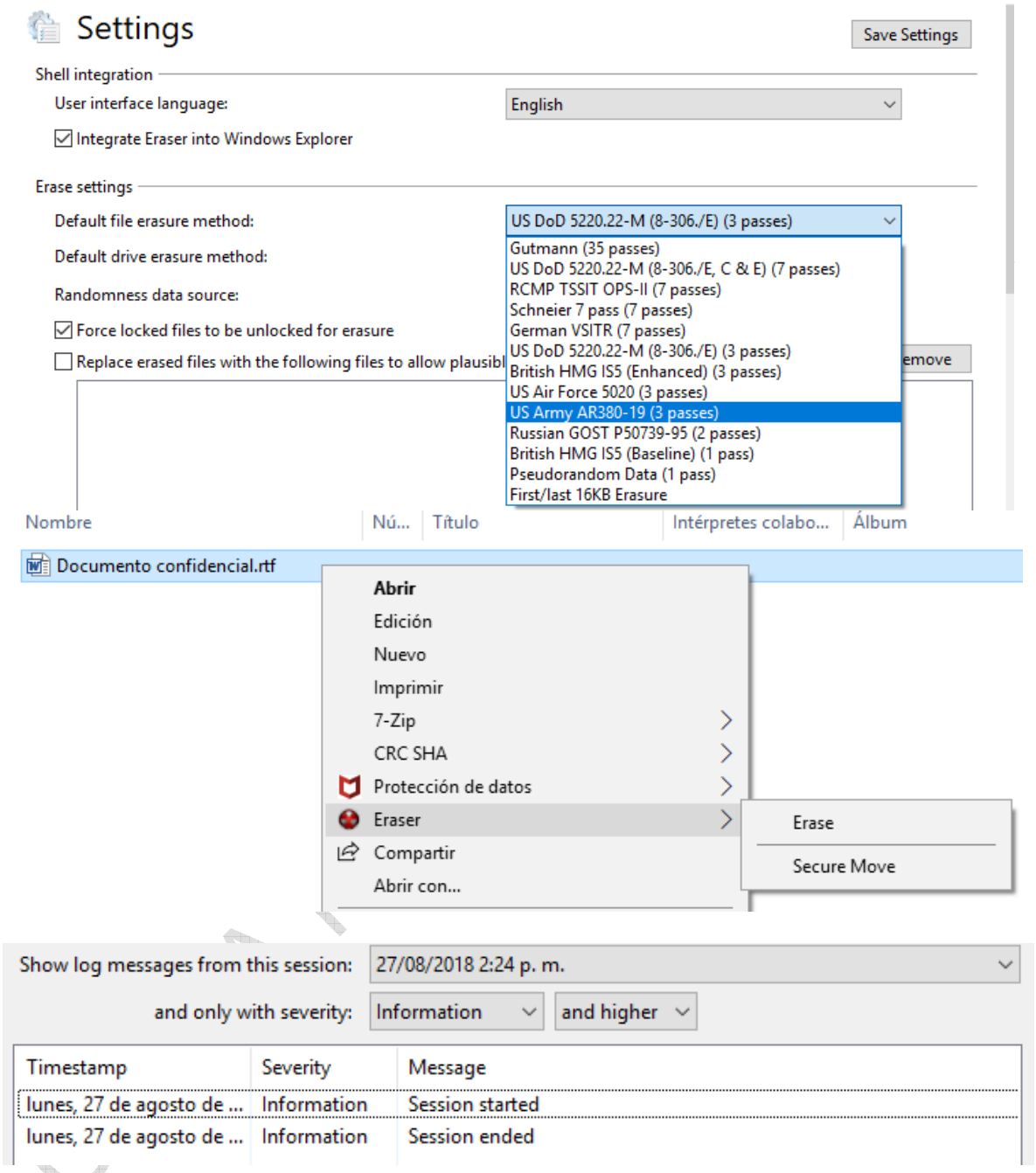
A continuación, se presentan las actividades de esta etapa:

7.2.1 Ejecutar el borrado seguro

Una vez realizado el backup de la información (si aplica), la mesa de servicios configura la herramienta especializada para el borrado seguro, utilizando un método de borrado de al menos tres pasadas. Se recomiendan los siguientes:

- US Army AR380-19.
- US DoD 5220.22-M.
- British HMG IS5.
- US Air forcé 5020.

Para llevar a cabo el borrado, el agente de la mesa de servicios asignado al caso, selecciona las unidades de disco, carpetas o archivos a borrar y ejecuta la herramienta especializada para el borrado seguro, verificando los logs para garantizar la correcta finalización. A continuación, se presentan imágenes que ilustran lo anterior:



7.2.2 Informar al usuario

La mesa de servicios es la encargada de informar al usuario y documentar el resultado de la actividad, aportando las evidencias respectivas (pantallazos y logs de la herramienta especializada para el borrado seguro). Esta actividad se realizará

por medio de correo electrónico y documentación del caso en la herramienta de casos de la mesa de servicios (Aranda).

De resultar fallido el borrado seguro, la mesa de servicios puede sugerir alternativas para que sean implementadas por el usuario solicitante, por ejemplo, la destrucción física del dispositivo de almacenamiento.

8 DOCUMENTOS RELACIONADOS

SC05-I01 Políticas del Sistema de Gestión de Seguridad de la Información - SGSI.

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

1. Se realiza cambio en el código documental debido al cambio de proceso.
2. Se realiza una actualización general sobre las actividades y etapas del procedimiento, incluyendo los códigos de la documentación relacionada en el procedimiento.
3. Cambia del proceso GS02 Gestión de la Seguridad de la Información al GS01 Administración de la Infraestructura Tecnológica. Código anterior GS02-P07

_____

Fin documento