

Guía para el proceso de Borrado Seguro

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	5
2. OBJETIVO.....	7
3. ALCANCE Y APLICABILIDAD DEL DOCUMENTO	7
4. RESPONSABILIDADES.....	8
5. TÉRMINOS Y DEFINICIONES	8
6. MARCO NORMATIVO O REGULATORIO	10
7. PROCESOS PARA EL BORRADO SEGURO.....	11
Objetivo:.....	11
7.1 Desmagnetización:.....	11
7.2.1 Desintegración, pulverización, fusión e incineración:.....	12
7.2.2 Trituración:.....	12
7.2.3 Sobre-escritura:	12
7.3 MANEJO DE MEDIOS FÍSICOS.....	13
7.3.1 FLUJO DE SOLICITUD DE PROCESO DE ELIMINACIÓN DOCUMENTOS....	15
7.4 PROCESO DE SOLICITUD DE BORRADO SEGURO.....	16
7.4.1 FLUJO DE TRABAJO	16
8. TECNOLOGÍA DE BORRADO SEGURO (SANITIZACIÓN).....	18
10. CUMPLIMIENTO Y SANCIONES.....	20
10.1 Principio:	20
10.1.2 Políticas de seguridad de la información:.....	20
Referencias	21

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

Tabla de Anexos

Anexo 1 Borrado seguro en Equipos activos de red	22
Anexo 2 Formateo Seguro de medios Físicos.....	24



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

Tabla Ilustraciones

Ilustración 1	Ciclo de vida de la información	5
---------------	---------------------------------------	---

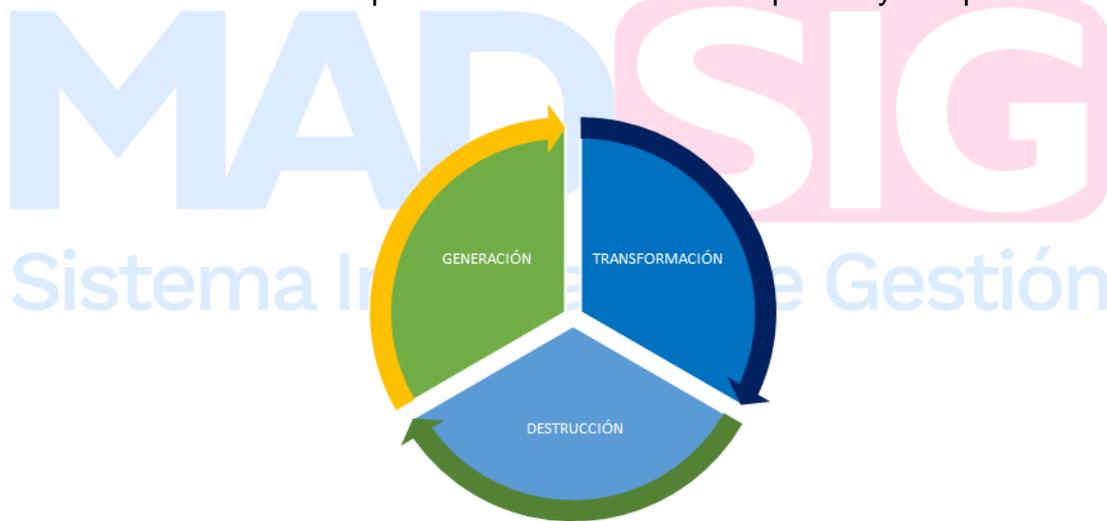


MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

1. INTRODUCCIÓN

Hoy en día las Organizaciones basan su actividad en la información como bases de datos, documentos de texto, archivos, etc. Toda esta información tiene un ciclo de vida la cual, está compuesto por tres fases: generación, transformación y destrucción.

Cuando dicha información cumple su ciclo, se deben emplear herramientas de destrucción y borrado que garanticen la efectividad y confiabilidad del proceso. Evitando de esta forma que la información sea manipulada y comprometida por



terceros.

Ilustración 1 Ciclo de vida de la información

Debido a los grandes volúmenes de datos que se manipulan a diario, junto a los usuarios y medios tecnológicos para hacerlo están siendo objeto de múltiples riesgos, tales como los ataques informáticos externos e internos; Son

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

estos últimos, los que mediante esta guía se pretende controlar en las actividades de baja de equipos de cómputo de la Entidad ya que pueden contener información confidencial o reservada la cual no debe ser accedida por personas no autorizadas, pues su uso indebido generaría impactos catastróficos en cuanto a Seguridad de la Información se refiere.

De acuerdo a “**La Ley 1581 del 2012 “Protección de Datos Personales”** la cual reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada”.

Uno de los lineamientos que esta ley tiene en cuenta es que la entidad que regula el cumplimiento al derecho a la protección de datos personales garantice que se debe dar el debido proceso de borrado, eliminación o destrucción de la información.

Así mismo el **Artículo 15 de la Constitución Política de Colombia**, donde se contempla “el derecho de todo ciudadano colombiano a tener intimidad”, convirtiéndose esta es prioridad por ser parte de unos de los pilares de la seguridad de la información

También se tomará como base la Norma **ISO 27001** y la Norma **ISO 27002**, la primera proporciona una guía sobre cómo deshacerse de los medios de comunicación y los activos de forma que se reduzcan al mínimo los riesgos de la exposición de información comprometedor; la segunda ofrece recomendaciones sobre los procedimientos de desechos, clasificación, mezcla de procedimientos, trazabilidad de la eliminación y borrado de la información; al igual que el **Anexo A 8.3.2** control de la información y los medios de comunicación en la que se

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

almacena, **A 11.2.7** control dirigido al manejar de forma adecuada los equipos que hace uso de los medios de comunicación.

Toda organización ya sea pública o privada tiene el deber de garantizar la confiabilidad, integridad y disponibilidad de la información por lo tanto se deben tener en cuenta estas normas para desarrollar políticas de borrado seguro.

2. OBJETIVO

Definir e identificar las políticas o los lineamientos que permitan establecer de manera eficiente la eliminación; reutilización y borrado de archivos confidenciales contenidos en medios magnéticos, ópticos o eléctricos destinados para baja, donación, cambio o reasignación de equipo, mediante un procedimiento de borrado seguro (sanitización) y la utilización de una herramienta de software de uso libre para evitar la recuperación de información en los activos de almacenamiento de datos.

3. ALCANCE Y APLICABILIDAD DEL DOCUMENTO

Proveer al Ministerio de Ambiente y Desarrollo Sostenible (MADS) de un mecanismo que evite la recuperación de datos confidenciales o sensibles de los dispositivos de almacenamiento masivo como discos duros de estaciones de trabajo, portátiles, discos externos según aplique.

Esta herramienta tendrá aplicabilidad autorizada y restringida exclusivamente al grupo de infraestructura de la oficina TIC, quienes mediante servidores públicos autorizados o servicios de outsourcing de Mesa de Ayuda, Infraestructura, o Seguridad Informática ejecutarán los pasos contenidos en el objetivo y alcance de esta guía.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

Este documento aplica a toda la información digital de los funcionarios, contratistas o terceros que tengan vínculo con la entidad y que posean acceso a la información de la misma en su poder, por lo que es importante dar cumplimiento a la normatividad vigente con el fin de garantizar la seguridad y privacidad de los datos custodiados por la Entidad, asegurando que la información sea eliminada de forma segura y que no pueda ser recuperable posteriormente.

4. RESPONSABILIDADES

- **Equipo de Seguridad de la Información:** debe asegurar que el área encargada realice el procedimiento adecuado y utilice las herramientas asignadas para el proceso de borrado de acuerdo a la normativa vigente; así como emitir normas que permitan garantizar la confiabilidad e integridad del proceso realizado a la información.
- **Jefe de la Oficina de Tecnologías de la Información:** el responsable de revisar, verificar que el proceso a realizar este acorde a la normatividad vigente y adecuado a las buenas prácticas de borrado de la información.
- **Mesa de Ayuda:** Controla, verifica y valida que se esté llevando a cabo la ejecución del proceso que se ejecuta; así como de consolidar los resultados y reportarle al área encargada el éxito del proceso.
- **Responsable de la Información:** Esta área o persona encargada es la responsable de generar las copias de seguridad garantizando el respaldo de la información a la cual se le va a realizar el proceso de borrado.

5. TÉRMINOS Y DEFINICIONES

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

- **Activo:** Recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.
- **Amenazas:** Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Confidencialidad:** Según la norma ISO/IEC 27001, es la propiedad de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Control:** Medida preventiva o correctiva ante la presencia de diferentes riesgos.
- **Disponibilidad:** Según la norma ISO/IEC 27001, es la propiedad de salvaguardar la exactitud y estado completo de los activos de información.
- **Integridad:** Según la norma ISO/IEC 27001, es la propiedad de que la información sea accesible y utilizable por solicitud de un individuo o entidad autorizada cuando se requiera.
- **Riesgo:** Toda posibilidad de ocurrencia de aquella situación que pueda entorpecer el desarrollo normal de las funciones de la empresa e impidan el logro de sus objetivos.
- **Almacenamiento de información:** hace referencia al uso de medios de grabación para conservar los datos utilizando PC y otros dispositivos.
- **Disco Duro:** El Disco Duro es un dispositivo magnético que almacena todos los programas y datos de la computadora. Su capacidad de almacenamiento se mide en gigabytes (GB) y es mayor que la de un disquete (disco flexible).
- **Impresos:** Hace referencia a los documentos físicos impresos.
- **Información Confidencial o sensible:** se consideran documentos clasificados su divulgación solo es permitida a personas autorizadas.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

- **Información Pública:** Información que puede ser distribuida abiertamente al público, puede estar alojada en una página web o esta puede ser solicitada y ofrecida sin ningún tipo de reserva o limitante.

- **Información Reservada:** Aquella que reúne las siguientes condiciones: está en poder o custodia de un sujeto obligado, el acceso a ella puede ocasionar un daño a intereses públicos y se encuentra expresamente prohibida para la ciudadanía en la Ley. Esta prohibición es legítima cuando atiende las circunstancias previstas en el Artículo 19 de la Ley 1712 de 2014¹

- **GEMA:** plataforma de gestión y mesa de asistencia del Ministerio de Desarrollo y Medio Ambiente

6. MARCO NORMATIVO O REGULATORIO

El Ministerio de Ambiente y Desarrollo Sostenible se basa en la siguiente normativa:

- ACUERDO 46 DE 2000 (Mayo 5) "Por el cual se establece el procedimiento para la eliminación documental".²
- “Manual 3.1 para la Implementación de la **Estrategia de Gobierno en Línea** para entidades del Orden Nacional”, **Decreto 2573 de 2014**³ Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea
- **Ley 1273 de 2009**⁴ denominada “**Protección de la información y los datos**”,

¹ REPUBLICA, C. D. (03 de 2014). *Ley 1712 de 2014*. Obtenido de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882>

² NACIÓN, E. C. (02 de 07 de 2021). *gov.co*. Obtenido de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6279>

³ <http://programa.gobiernoenlinea.gov.co/apc-aa-files/e5203d1f18ecfc98d25cb0816b455615/decreto2573-del-12-de-diciembre-de-2014.pdf>

⁴ <http://www.mintic.gov.co/portal/604/w3-article-3705.html>

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	MADSIG <small>Sistema Integrado de Gestión</small>
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

- normas **NTC-ISO 27001⁵** Sistema de Gestión de Seguridad de la Información, **NTC-ISO 27002** Guía de buenas prácticas de seguridad de la información
- RESOLUCIÓN ORGANIZACIONAL OGZ-0070 DE 2014 (agosto 29) Diario Oficial No. 49.264 de 4 de septiembre de 2014 CONTRALORÍA GENERAL DE LA REPÚBLICA.
- **NTC-ISO 27005**, Guía para la Gestión de los riesgos de la seguridad de la información

7. PROCESOS PARA EL BORRADO SEGURO

Objetivo: Utilizar medios eficaces que eviten la recuperación de la información almacenada en los dispositivos.

En esta guía se pretenden dar lineamientos que permitan que el área encargada o las persona asignadas para realizar el procedimiento de borrado o baja de equipos determine cual de estos es el mejor a aplicar.

7.1 Desmagnetización: Este método consiste realizar un proceso de exposición al medio de almacenamiento a un potente campo magnético, el cual elimina los datos, almacenados en el dispositivo. Eso significa que un disco duro que ha sido borrado por este método no se puede utilizar de nuevo.

7.2 Destrucción Física: la finalidad de este proceso es la inutilización física del dispositivo en donde se almacena la información. Este método se puede realizar

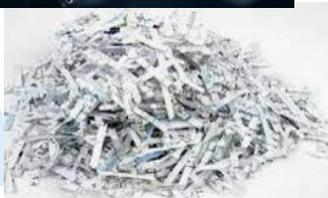


de diferentes formas:

⁵ http://www.iso.org/iso/catalogue_detail?csnumber=54534

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

7.2.1 Desintegración, pulverización, fusión e incineración: estos métodos fueron diseñados con el fin de implementarse para la destrucción de la información definitiva garantizando de esta forma su total eliminación, entre los más utilizados está la incineración, con una máquina destructora.



7.2.2 Trituración: con este proceso se busca destruir información o contenido en almacenamientos flexibles. Entre más pequeño sea el fragmento más seguridad hay de que la información sea irrecuperable, entre los que se pueden encontrar medios de almacenamiento tales como; CD, DVD, USB, discos Extraíbles magneto-ópticos), se recomienda que sean destruidos por pulverización, trituración de corte transversal o incineración.

7.2.3 Sobre-escritura: Consiste en la escritura de datos aleatorios sobre la información contenida en el dispositivo. Es más efectivo cuantas más veces se repita el proceso. Su gran ventaja es que permite seguir utilizando el dispositivo.



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

7.3 MANEJO DE MEDIOS FÍSICOS

Para el manejo de medios físicos se deberá tener presente los siguientes lineamientos, teniendo como guía la norma **27001** y **27002** al igual que el **Anexo A 8.3.2** control de la información y los medios de comunicación en la que se almacena, **A 11.2.7** control dirigido al manejar de forma adecuada los equipos que hace uso de los medios de comunicación.

Por la cual establece requisitos y lineamientos para el manejo y gestión de información:

- Todo funcionario, contratista o cualquier tercero que tenga acceso a la información deberá seguir el debido proceso de solicitud de borrado por medio de la plataforma **GEMA** donde deberá realizar una solicitud formal especificando el objeto de la misma.
- El proceso de borrado seguro o baja de equipos se aplicara a todo tipo de activos destinados al almacenamiento de la información.
- En caso de que estos activos vayan a ser reutilizados o liberados a otra área departamento u organización deben ser objeto de borrado seguro en dado caso que este activo no se le pueda ejecutar este tipo de proceso será el área encargada quien definirá si debe ser destruido y que tipo de metodología va a aplicar.
- El área responsable deberá evaluar si es viable la destrucción de la información tomando como guía los decretos, leyes y otra normativa vigente.
- Para eliminación de medios lógicos este proceso se realizará únicamente cuando la solicitud haya sido autorizada dejando la documentación de constancia.
- La persona encargada de realizar dicho proceso deberá generar un reporte donde se evidencie quien estuvo a cargo del procedimiento y la metodología a utilizar y se deberán dejar anotaciones que evidencien que este se realizó de acuerdo a la normatividad.
- En caso de que en la ejecución del procedimiento se presente algún tipo de falla y no se pueda realizar correctamente este deberá ser documentado e informar al área encargada.

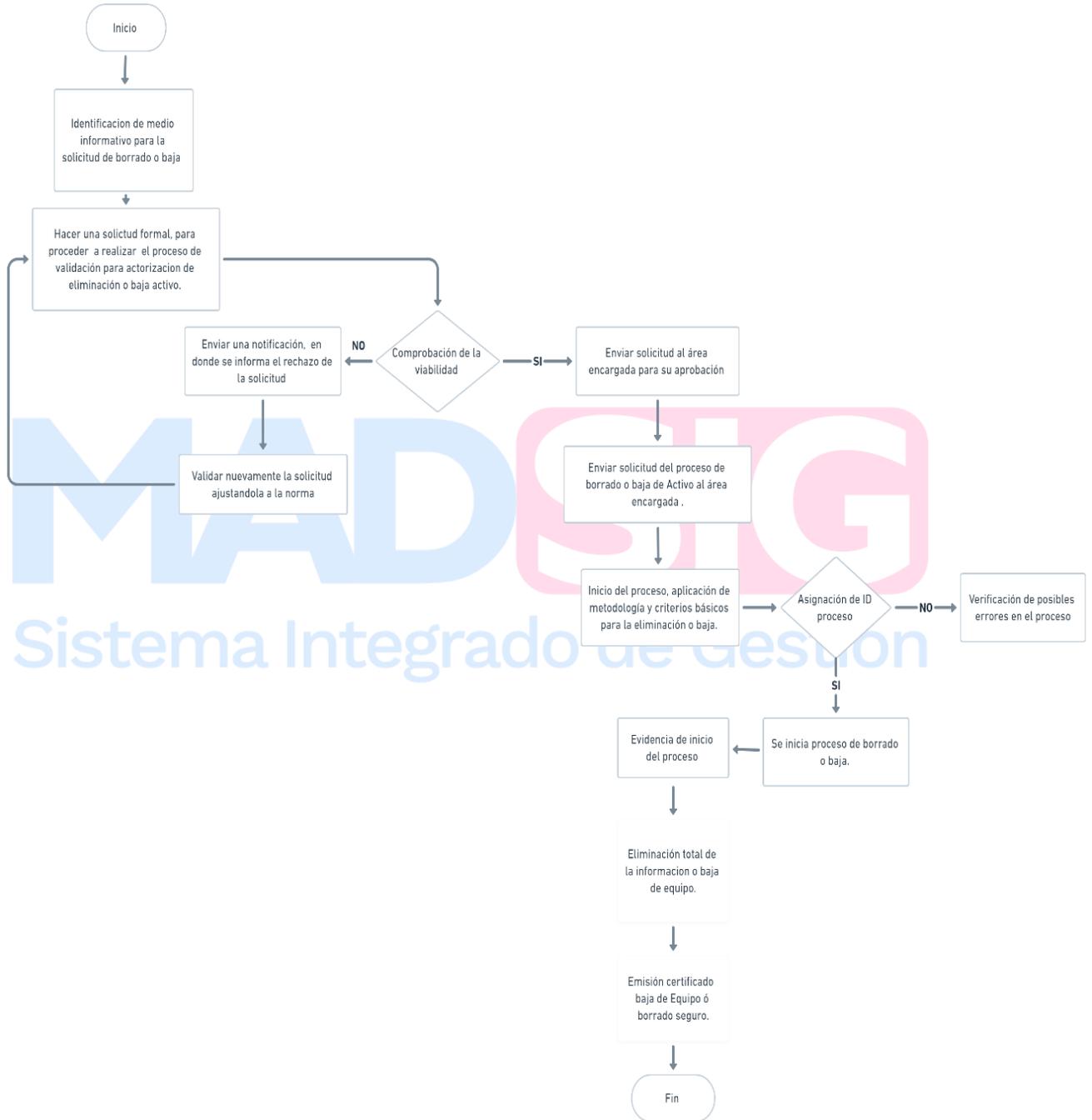
MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

- El área encargada de realizar este proceso deberá garantizar que todos los documentos serán eliminados y no se cuentan con copias en archivos u otros equipos.
- El área encargada de realizar el procedimiento deberá garantizar que la información a eliminar mantendrá la misma seguridad e integridad que ha mantenido durante su ciclo de vida útil hasta el momento del proceso de eliminación o borrado de la misma.
- También se deberá tener en cuenta que dicho método de borrado será amigable con el Medio Ambiente por lo que deberá producir el mínimo de emisiones y desperdicios que lo afecten.
- El área encargada de realizar el proceso de sanitización de equipos deberá enviar trimestralmente un informe donde se evidencie si se han realizado o no los procedimientos de borrado seguro en los activos a su cargo.



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

7.3.1 FLUJO DE SOLICITUD DE PROCESO DE ELIMINACIÓN DOCUMENTOS



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

7.4 PROCESO DE SOLICITUD DE BORRADO SEGURO

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
Reutilización del equipo	Verificar que el dispositivo de almacenamiento a reutilizar o dar de baja no contenga información de la Entidad.	Personal Mesa de ayuda
Realizar el Backup de la información	Si se encuentra información en el dispositivo de almacenamiento, El funcionario de la Mesa de Ayuda realiza el backup de la información.	Personal Mesa de ayuda
Realizar el borrado del disco duro	El funcionario de la Mesa de Ayuda, realiza el borrado seguro, mediante la herramienta seleccionada	Personal Mesa de ayuda
Eliminar todas las particiones del disco	El funcionario de Mesa de Ayuda realiza la eliminación de las particiones del disco duro.	Personal Mesa de ayuda
Alistamiento del disco duro	Si el equipo es reasignado, el funcionario de Mesa de ayuda, realiza el procedimiento de formateo, instalación o restauración del sistema operativo y aplicativos	Personal Mesa de ayuda
Validar la ejecución del borrado seguro	El funcionario de Mesa de Ayuda, valida que el procedimiento sea exitoso y toma los registros generados por la herramienta utilizada y las evidencias del procedimiento realizado.	Personal Mesa de ayuda

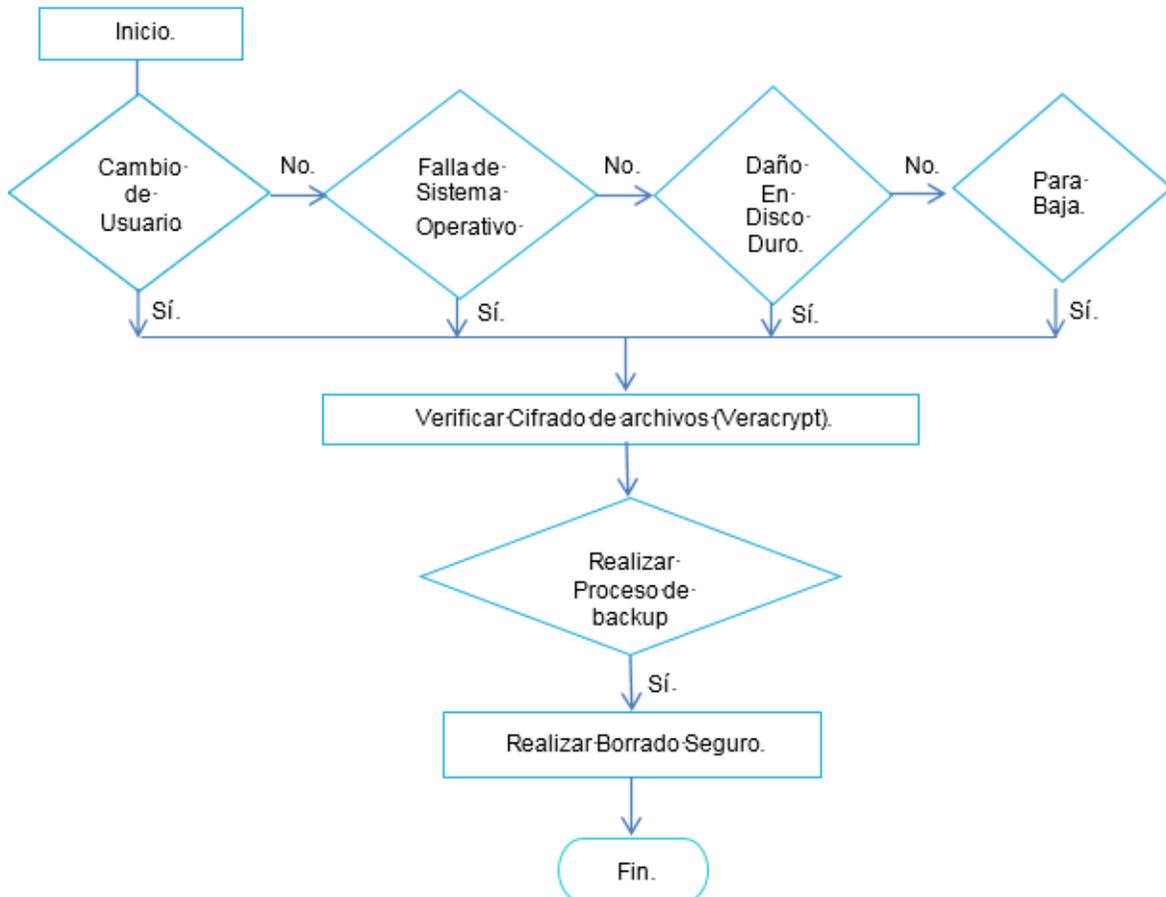
7.4.1 FLUJO DE TRABAJO

Para alcanzar el objetivo de Seguridad de la Información de esta Guía, el personal autorizado de ejecutar el procedimiento de borrado seguro, deberá tener en

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

cuenta los siguientes aspectos antes, durante y después de recibir el equipo de cómputo o el dispositivo de almacenamiento:

Etapas previas: es deber de los integrantes de la Mesa de Ayuda cumplir con todo requerimiento que se realice mediante el procedimiento de solicitudes de soporte.



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

8. TECNOLOGÍA DE BORRADO SEGURO (SANITIZACIÓN)

Existen varios mecanismos y herramientas, así como metodologías avaladas por normas bajo estrictos criterios técnicos de laboratorios especializados para realizar borrado seguro de datos en los dispositivos de almacenamiento internos y externos.

Para el proceso de borrado seguro; el área encargada aplicara la metodología y seleccionara la herramienta de borrado, que permita garantizar la efectividad del proceso de igual forma se dejara como evidencia un documento que identifique claramente que el proceso de borrado que se ha realizado, detallando cuándo y cómo ha sido realizado.

Si el equipo se da de baja por cualquier motivo se debe diligenciar completo el formato de baja de activos fijos y será el área encargada quien determinara si aplica para este proceso emitiendo un documento de constancia de dicho proceso.

En el caso de que la responsabilidad sea transferida a un tercero este proporcionara un certificado de destrucción del equipo.

Todo activo o proceso gestionado en la entidad para el almacenamiento o procesamiento de datos deberá seguir las normas y procedimientos seleccionados; que estos consideren sea la mejor selección para realizar el proceso de Borrado, validando el procedimiento y verificando que cumpla con los solicitado y dejando como evidencia el paso a paso del proceso (ver anexo I & II)

9. ALMACENAMIENTO EN LA NUBE

Con el fin de optimizar procesos y reducir costos es importante establecer lineamientos que permitan establecer reglas y criterios que definan que tipo de información se puede almacenar en la nube.

Al igual que políticas que aseguren que la contratación y el servicio brindado por el prestador de este servicio pueda garantizar la confiabilidad, integridad y disponibilidad de la información

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

El área encargada de realizar dicha contratación del servicio deberá validar las políticas de seguridad de la información; también se le exigirá al proveedor una póliza de respaldo en caso de que exista incumplimiento.

El proveedor deberá disponer de suficiente espacio para realizar las copias de seguridad y garantizar que en caso de que se presente algún imprevisto la información no se verá afectada y se puede recuperar.

Se le exigirá al proveedor del servicio documentación que respalde el proceso de borrado que realiza para garantizar que en ninguno de los dispositivos donde se tuvo acceso a la información quede rastro de ella.

Por parte de la entidad las personas designadas también validaran que dicho proceso haya sido exitoso.

Todo colaborador de la entidad ya sea funcionario, contratista o tercero tendrá la opción de subir información a la nube, pero solo el área encargada podrá realizar copias de seguridad y tener acceso a ellas, así como el único quien podrá realizar el borrado de la información de la nube es el administrador de la plataforma, para este proceso el área encargada debe realizar una solicitud formal ante el proveedor de este servicio.

Se llevará a cabo un registro como evidencia de los dispositivos y personal que han tenido acceso a la información con el fin de validar que en el momento de necesitar eliminar la información no quede rastro de ella.

Es importante que en el documento se evidencien:

- Las características del dispositivo
- Fabricante
- Modelo
- Número de la serie
- Funcionario o área a la que estaba asignado el dispositivo
- Tipo de metodología que se utilizó para realizar el proceso de borrado, que herramienta se utilizó.
- Funcionarios que validaron el proceso
- Fecha de validación
- Finalmente se debe dejar evidencia de que el proceso de eliminación fue exitoso.

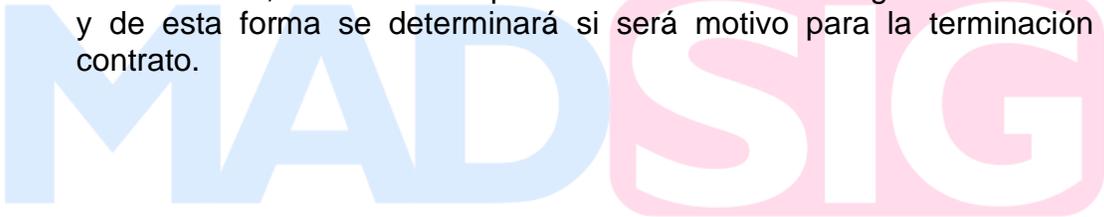
MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

10. CUMPLIMIENTO Y SANCIONES

10.1 Principio: Todos los colaboradores, directivos, proveedores y usuarios que se benefician de los servicios se comprometen a cumplir y respetar el debido proceso para la solicitud de borrado seguro

10.1.2 Lineamientos por Incumplimiento de las actividades relacionadas con el borrado Seguro

- Los colaboradores, proveedores, clientes o contratistas dan por entendido que todo incumplimiento de las normas contenidas en esta guía será considerado como causal para la aplicación de las diferentes medidas correctivas dentro de las que se encuentran sanciones disciplinarias o contractuales, dentro de las que se tendrá en cuenta la gravedad de la falta y de esta forma se determinará si será motivo para la terminación del contrato.


Sistema Integrado de Gestión

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

Referencias

NACIÓN, E. C. (02 de 07 de 2021). *gov.co*. Obtenido de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6279>

REPUBLICA, C. D. (03 de 2014). *Ley 1712 de 2014*. Obtenido de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882>

<https://www.genbeta.com/herramientas/siete-herramientas-gratis-para-borrar-de-forma-segura-tus-discos-duros-hdd-o-ssd>

<https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0044792>

<https://www.pmg-ssi.com/2015/12/eliminacion-segura-documentos-segun-norma-iso-27001/>

<https://www.genbeta.com/herramientas/siete-herramientas-gratis-para-borrar-de-forma-segura-tus-discos-duros-hdd-o-ssd>

https://sc.inegi.org.mx/repositorioNormateca/Oci_13Mzo17.pdf

<https://soporte.athento.com/hc/es/articles/360024036093--C%C3%B3mo-realiza-Athento-el-borrado-seguro-y-permanente-de-los-documentos->

https://www.mineducacion.gov.co/1759/articles-322548_Manuales2020_00.pdf

<http://e->

[asura.unlp.edu.ar/uploads/docs/tutorial para el borrado por software v3.pdf](http://e-basura.unlp.edu.ar/uploads/docs/tutorial_para_el_borrado_por_software_v3.pdf)

[https://e-basura.unlp.edu.ar/uploads/docs/tutorial para el borrado por software v3.pdf](https://e-basura.unlp.edu.ar/uploads/docs/tutorial_para_el_borrado_por_software_v3.pdf)

<http://adecuarse.com/adecuaciones/politicas-seguridad/politica-de-destruccion-de-la-informacion/>

<http://polux.unipiloto.edu.co:8080/00002653.pdf>

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

Borrado seguro de equipos activos de red

Anexo 1 Borrado seguro en Equipos activos de red

PASO 1: Toma de información general del equipo:

- Ubicación: Lugar en que operaba el equipo.
- Equipo: Tipo de equipo y referencia.
- Serial: Código alfanumérico único asignado para identificación
- Placa de inventario: Código asignado por Almacén (MADS).

PASO 2: Backup de configuración:

Se accede al equipo y se toma un backup de configuración previo.

Este archivo se caracteriza por tener una extensión de archivo .cfg, txt ó .dat de forma general. Sin embargo, se debe tener presente que esta puede variar según la referencia y modelo del equipo.

(nombre representativo).txt

PASO 3: Revisión de memoria flash y archivos de configuración (.text, .dat y. ext).

Se debe ingresar a la memoria flash del equipo mediante línea de comando CLI e identificando los archivos correspondientes según la extensión indicada. Desde allí, se puede evidenciar de manera detallada la capacidad en memoria, así como su disponibilidad de espacio. Ver figura 1.

Nota: La unidad de almacenamiento de los equipos activos es tipo flash, por lo que su capacidad es limitada dependiendo del equipo en referencia.

```

Directory of flash:/

 2  -rwx   11135872   Jan 1 1970 01:03:52 +00:00  c37                               .bin
 3  -rwx     2119    Mar 1 1993 00:01:04 +00:00  private-contig.text
 5  -rwx     796    Jul 8 2021 10:16:36 +00:00  vlan.dat
 6  -rwx     6293    Mar 1 1993 00:01:04 +00:00  config.text
 7  drwx     192    Mar 1 1993 00:00:12 +00:00  crashinfo_ext
 9  drwx     192    Mar 1 1993 00:00:03 +00:00  crashinfo
15  -rwx     5144    Mar 1 1993 00:01:04 +00:00  multiple-fs

15998976 bytes total (4073984 bytes free)
```

Figura 1. Ejemplo directorio flash equipo de red.

PASO 4: Eliminación y borrado de archivos de configuración (.text, .dat y. ext).

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

Se efectúa el proceso de borrado que aplica de acuerdo a las indicaciones del fabricante.

Nota: Tener precaución al borrar los archivos de la memoria flash pues de lo contrario puede generar falla en el sistema operativo del mismo y dejarlo inoperable.

```

_ #write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
#
*Mar 1 00:02:33.704: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
_ #delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
_ #delete flash:config.text
Delete filename [config.text]?
Delete flash:config.text? [confirm]

```

Figura 2. Ejemplo borrado mediante línea de comando.

PASO 5: Reinicio del equipo (reload, boot, reboot, etc.).

Seguidamente, se debe efectuar reinicio del equipo para completar el proceso de borrado.

```

_ #reload
Proceed with reload? [confirm]

```

Figura 3. Ejemplo reinicio del equipo mediante línea de comando.

PASO 6: Validación de ocupación de memoria y archivos de configuración.

Posteriormente, se hace verificación sobre la memoria flash que el/los archivo(s) de configuración no exista(n), corroborando igualmente el espacio total indicado de la unidad de almacenamiento.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

```

Directory of flash:/

  2  -rwx   11135872  Jan 1 1970 01:03:52 +00:00  c37                               .bin
  3  -rwx     5144   Mar 1 1993 00:02:33 +00:00  multiple_fs
  9  drwx     192   Mar 1 1993 00:00:03 +00:00  crashinfo

15998976 bytes total (4084224 bytes free)

```

Figura 4. Estado final de la memoria flash.

PASO 7: Verificación de la operación de los componentes de hardware.

Finalmente, se solicita mediante línea de comando CLI el estado operacional del equipo.

```

Switch#show env all
FAN is OK
TEMPERATURE is OK
SW  PID                Serial#      Status      Sys Pwr  PoE Pwr  Watts
---  ---                ---          ---          ---      ---      ---
  1  Built-in                Good
SW  Status              RPS Name      RPS Serial#  RPS Port#
---  ---                ---          ---          ---
  1  Not Present          <>

```

Figura 5. Estado final de la memoria flash.

PASO 8: Concepto técnico sobre la operación y funcionamiento de los equipos.

El personal especialista genera el concepto técnico del equipo sujeto al proceso de borrado seguro

- *Equipo obsoleto, no cumple las características técnicas para la prestación del servicio al MADS, su vida útil está agotada.*

PASO 9: Diligenciamiento hoja de vida del equipo.

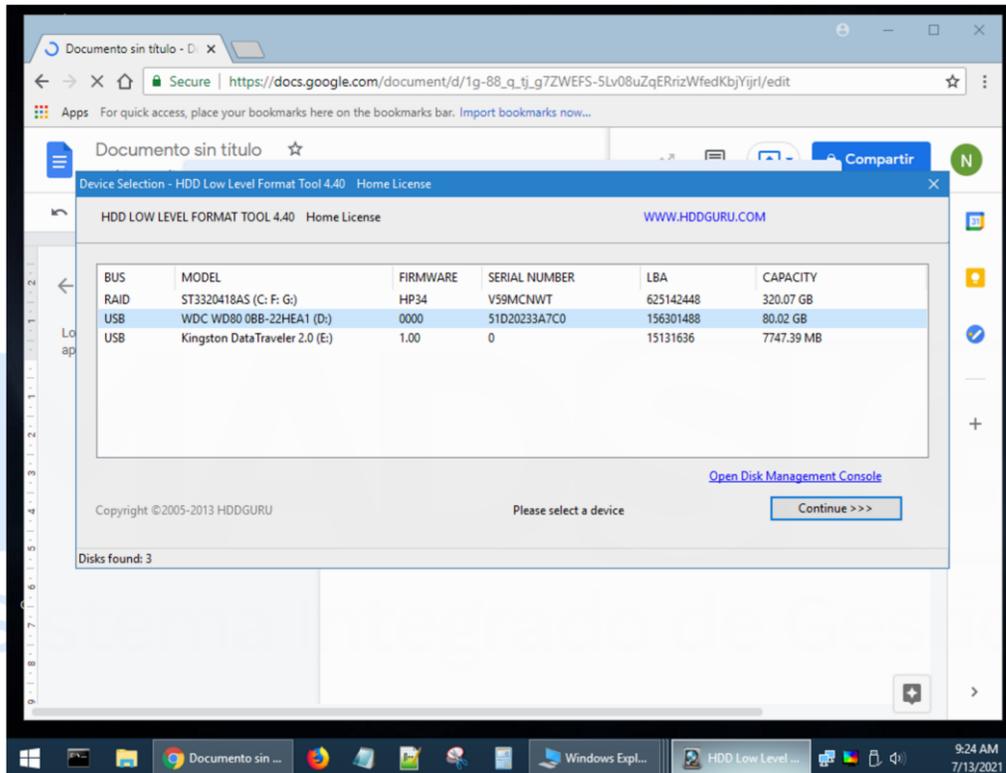
Esta actividad viene acompañada por la hoja de vida del equipo con el formato establecido y aprobado por MADSIG.

Anexo 2 Formateo Seguro de medios Fisicos

Borrado seguro con HDD Low Level Format Tool

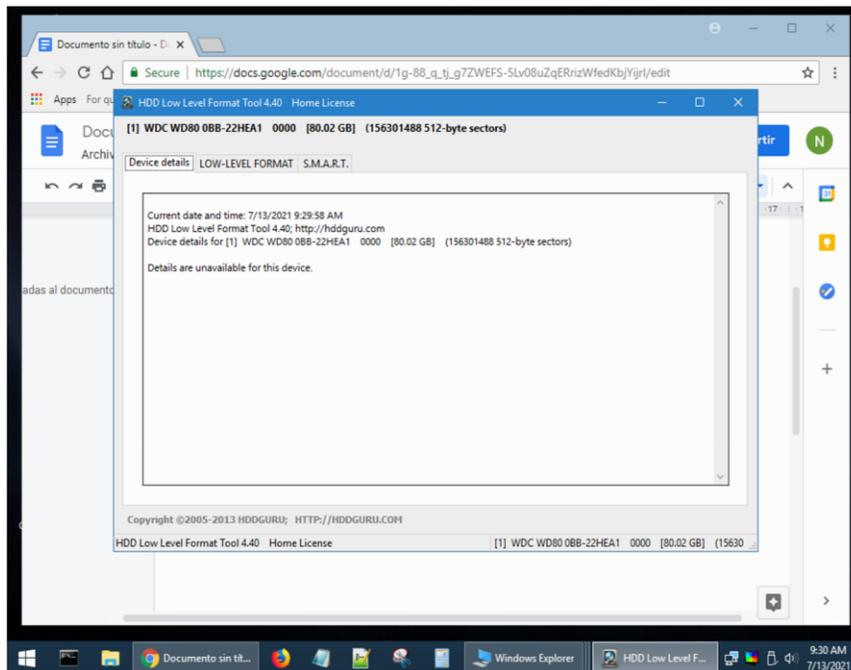
MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

Se ejecuta el programa y nos va aparecer el listado de unidades de almacenamiento que se encuentran en la máquina, en este caso seleccionamos el de USB porque estábamos formateando un disco duro externo.



Ya seleccionado nos aparece la descripción de la unidad de almacenamiento en la primera pestaña, tal como aparece en la imagen,

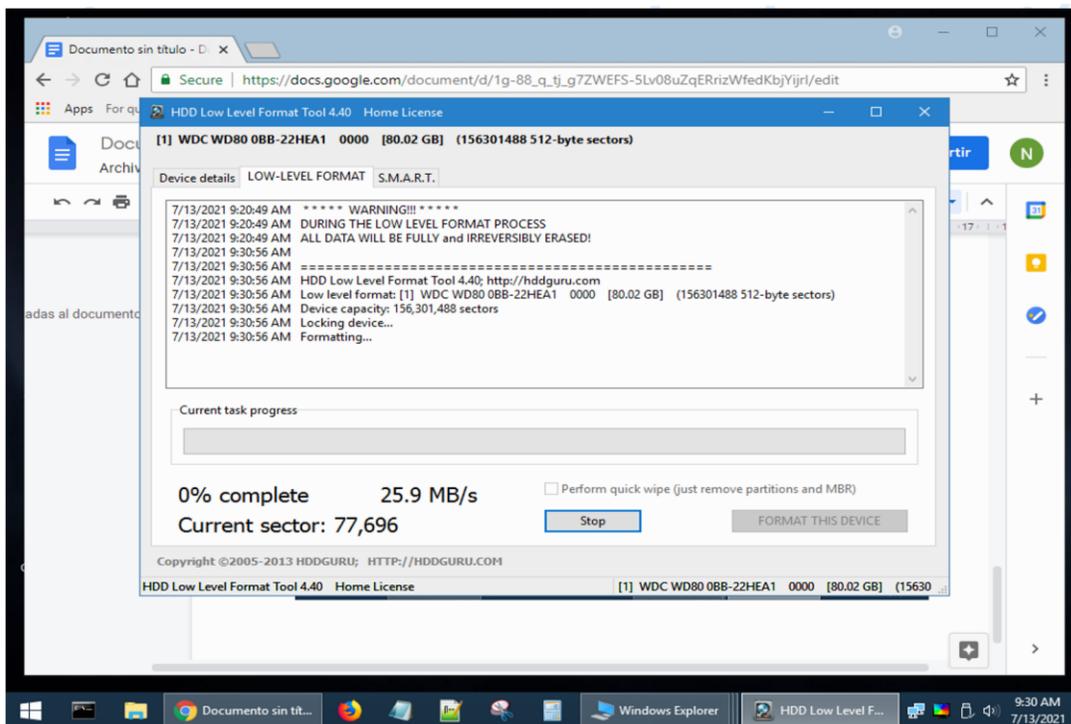
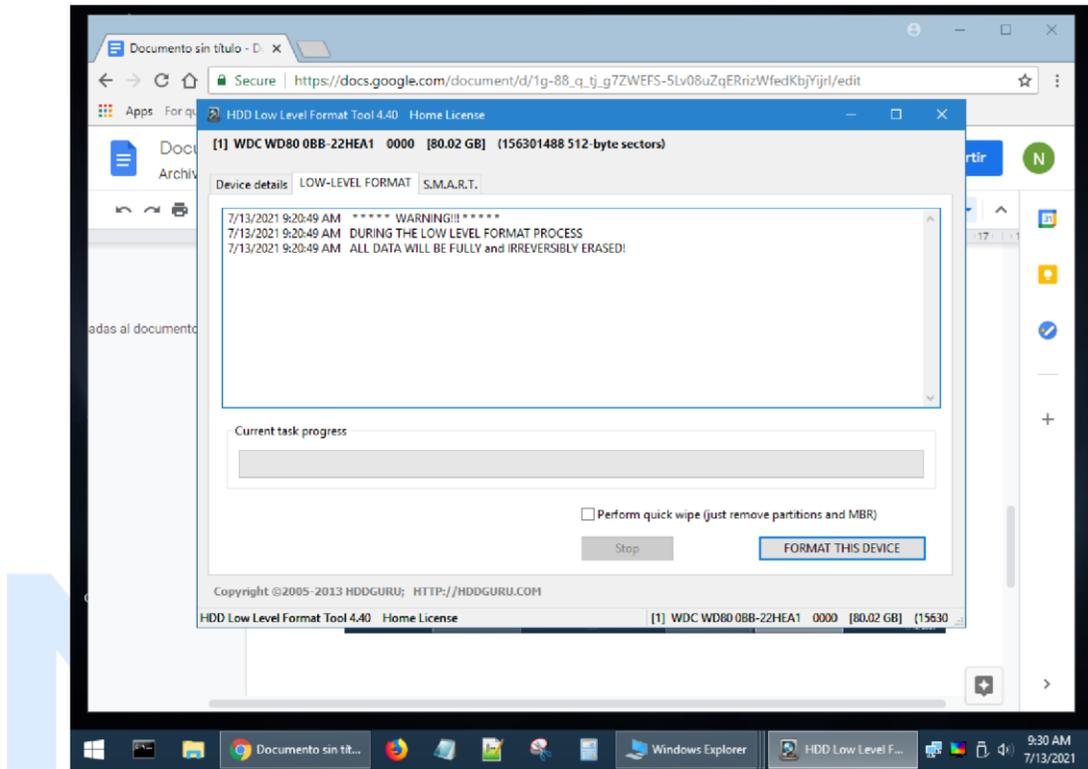
MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04



En la segunda pestaña ya nos deja el programa ejecutar el proceso de formateo lento, para así eliminar toda la información de la unidad de almacenamiento previamente seleccionada,

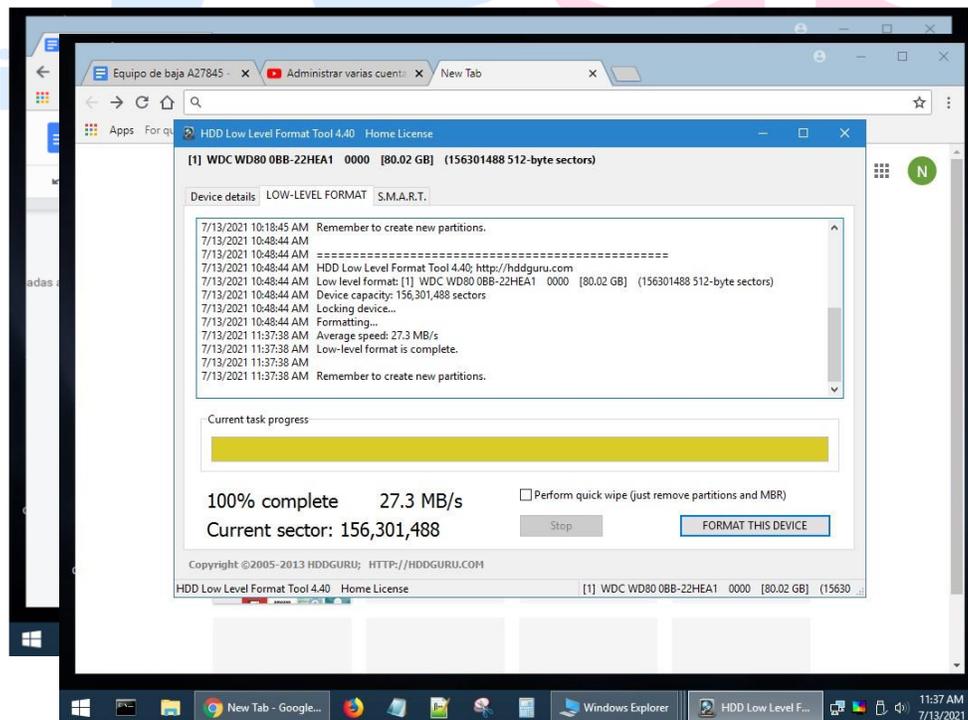
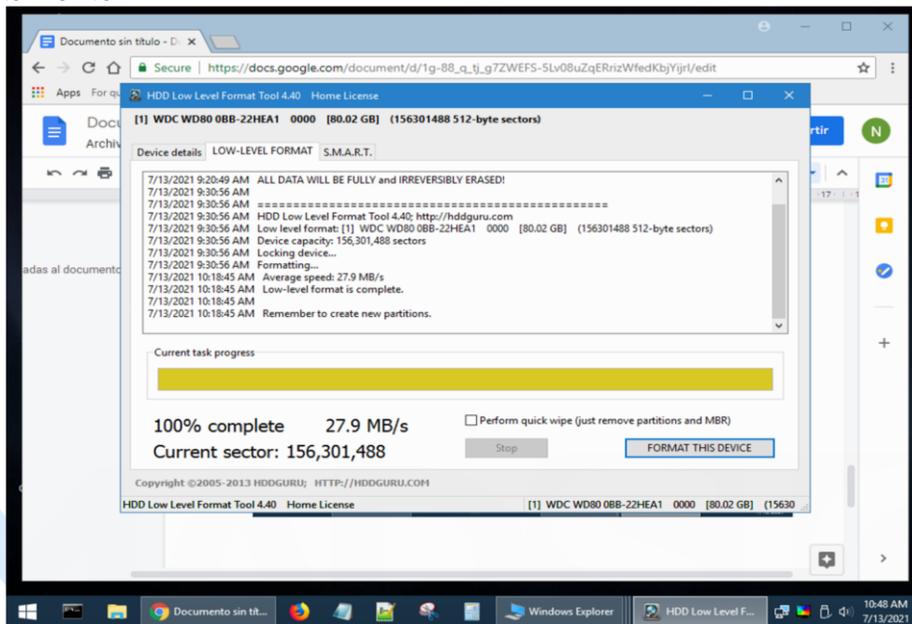
Sistema Integrado de Gestión

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

Proceso el cual se ejecutó tres veces para un formateo seguro, ya llegado al 100% se da cierre al aplicativo y se validó y la unidad estaba vacía completamente.



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	BORRADO SEGURO	 Sistema Integrado de Gestión
	Proceso: Gestión de Servicios de Información y Soporte Tecnológico	
Versión: 02	Vigencia: 20/08/2021	Código: G-E-GTI-04

MAD SIG

Sistema Integrado de Gestión