1. OBJETIVO

Esta guía describe la forma en la cual deben manipularse dichos medios (Computadores, CD, DVD, Memoria, Discos Duros, Cintas) toda vez que la información contenida en estos medios debe ser correctamente borrada y/o eliminada y/o destruida antes de que los medios sean reusados o desechados. De igual forma se contempla la información que se encuentra en medio físico.

Describir las actividades que se deben realizar para evitar cualquier traspaso de información no segura por medio de procedimientos de destrucción o reutilización seguro de medios de almacenamiento de información.

2. ALCANCE

Inicia con la gestión del ciclo de vida de la información y termina con la destrucción de los medios.

3. DEFINICIONES:

3.1. Almacenamiento de información: El almacenamiento es una de las actividades o capacidades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada.

3.2. Concientización: Es hacer que alguien se percate, se dé cuenta de algo, a través de los datos que tenga o se le den, y poner en movimiento su razonamiento, para que de lo que se quiere concientizar, lo considere detenidamente, para que reconozca sus atributos, tantos los esenciales como todas las modificaciones en sí mismo de ese "algo".

3.3. Confidencialidad: Propiedad de la información que determina que esté disponible a personas autorizadas).

3.4. Disco Duro: Los discos duros tienen una gran capacidad de almacenamiento de información, pero al estar alojados normalmente dentro de la computadora (discos internos), no son extraíbles fácilmente.

3.5. Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático

3.6. Impresos: Hace referencia a los documentos físicos impresos.

3.7. Información Confidencial: Documentos clasificados como altamente sensitivos. La divulgación solo se permite a terceros bajo autorización del nivel directivo o bajo orden de autoridad competente.

3.8. Información Pública: Información que puede ser distribuida abiertamente al público, que puede ser obtenida y ofrecida sin reserva alguna. Para que la información sea pública debe ser clasificada como como tal por el dueño del proceso.

3.9. Información Reservada: Es aquella Información que:

Por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones.

Cabe mencionar aquí la información genética, y los "datos sensibles" o aquellos relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.

De igual manera, será reservada aquella información clasificada como tal por mandato legal o que esté relacionada con la defensa.

3.10. Información Uso Interno: Información que es propia del ICBF y que no puede ser distribuida al público en general, esta información tiene un destinatario, un macroproceso o proceso especifico y requiere autorización para ser distribuida a terceros diferentes al destinatario definido.

Por regla general toda la información es de uso interno a menos que alguien con autoridad en el ICBF permita su distribución al público o a las partes interesadas en dicha información.

3.11. Rotulado de Información: Todo activo de información tanto físico como digital debe contar con una etiqueta que describe su clasificación a nivel de Confidencialidad de manera correspondiente.

3.12. Sensibilización: La sensibilización de las personas fomenta actitudes positivas y solidarias.

3.13. Medio: dispositivo de almacenamiento de la información.

3.14. Reusó o reutilización: Acción de volver a utilizar o usar los dispositivos tecnológicos, después de un uso específico.

3.15. Desecho: Corresponde a todos aquellos dispositivos eléctricos o electrónicos que han sido desechados o descartados, tales como: computadoras, teléfonos celulares, televisores y electrodomésticos. La chatarra electrónica se caracteriza por su rápido crecimiento debido a la rápida obsolescencia que están adquiriendo los dispositivos electrónicos y por la mayor demanda de estos en todo el mundo, entre otros factores. Su tratamiento inadecuado puede ocasionar graves impactos al medioambiente y poner en riesgo la salud humana.

3.16. Destrucción: Acción de eliminación total de los dispositivos de almacenamiento de información digital.

4. DESARROLLO

4.1. INTRODUCCIÓN

El riesgo de exposición y/o pérdida de la información Confidencial o de Reservada, se ha vuelto cada vez más común en los medios como son: (Computadores, CD, DVD, Memoria, Discos Duros, Cintas), en los cuales el **ICBF** almacena los activos de información. Estos representan un riesgo ya que es muy frecuente que sean reasignados, entregados o manipulados para eliminar de forma segura los contenidos, y realizar previa copia de dicha información.

Es importante tener en cuenta el ciclo de vida de la información desde el enfoque de la seguridad, el cual contempla aspectos de vital importancia en la manipulación de medios y Borrado Seguro de los mismos.

4.2. GESTION DEL CICLO DE VIDA DE LA INFORMACIÓN

Dada la evolución en el volumen de la información con la que trabaja la Entidad en la actualidad, se requiere establecer procedimientos y políticas que se deben seguir para gestionar los datos, desde que estos se crean o generan hasta su eliminación definitiva, teniendo en consideración el valor de la disponibilidad de la información.

La información por su naturaleza cuenta con su propio ciclo de vida, el cual se describe a continuación:

- **Fase 1: Clasificación de datos.**
  Todos los datos que se crean, generan o almacenan se deben identificar y rotular**,** para mejorar la eficiencia en el momento en que se efectúen los procesos de búsqueda, recuperación o auditoría, para esta clasificación se debe utilizar la guía **G10.MP06 Guía de Rotulación**.

  Esta clasificación de datos permite conocer con qué datos se cuenta, qué tratamiento darles, dónde almacenarlos, qué jerarquía tienen, cuál es su volumen, cuáles pueden ser eliminados y cómo recuperarlos de nuevo cuando sea necesario volver a trabajar con ellos.

- **Fase 2: Almacenamiento físico.**
  La información que se encuentra rotulada con: (Confidencial – Reservada) teniendo en cuenta la guía de **G10.MP06 Guía de Rotulación**, se debe almacenar en la NAS, para lo cual se debe solicitar a través de la Mesa de Soluciones Informáticas, que esta información se incluya con las opciones de almacenamiento disponible, teniendo en cuenta el procedimiento **PR11.MPA6 Gestión Copia de Seguridad v1**.

- **Fase 3: Disposición.**
  La información almacenada de manera segura debe estar disponible para los usuarios cuando estos la necesiten. La información también debe ser mantenida y utilizada de tal forma que su Confidencialidad, Integridad y Disponibilidad no se vea comprometida, teniendo en cuenta el procedimiento **PR11.MPA6 Gestión Copia de Seguridad v1**.

- **Fase 4: Utilización de la información almacenada.**

El uso o utilización se lleva a cabo mediante la restauración de las copias de seguridad, teniendo en cuenta el procedimiento **PR12.MPA6 Gestión Restauración de Copias de Seguridad**.

5. NORMAS GENERALES

- Cuando se requiera asignar, trasladar, reasignar, repotenciar, devolver al almacén o dar de baja un equipo de cómputo, a los Funcionarios y/o Contratistas de la Entidad, para la ejecución de sus funciones, se debe realizar solicitud ante la mesa de soluciones informáticas MIS, vía telefónicamente a la extensión 8080 o por correo a mis@icbf.gov.co.

- Para los medios electromagnéticos, digitales donde haya reposado información considerada dentro del nivel de clasificación que contempla la **G10.MP06 Guía de Rotulación** como: (Confidencial o Reservada), deben ser borrados y/o eliminados y/o destruidos de forma segura cuando cambien de propósito o sean devueltos por garantía o cuando termine su vida util.

- Cuando los medios sean descartados totalmente deben ser destruidos.

- Debe tomarse previamente copia de seguridad de la información (Confidencial o Reservada) de manera preventiva antes de proceder con un borrado seguro o eliminación del medio, teniendo en cuenta el procedimiento **PR11.MPA6 Gestión Copia de Seguridad v1**.

- La Dirección de Información y Tecnología es responsable por la configuración y toma de las copias de seguridad, teniendo en cuenta que la solicitud debe venir del dueño del Macroproceso o Proceso donde se requiere hacer la copia de seguridad.

- Las acciones de borrado seguro son responsabilidad de la Dirección de Información y Tecnología o a quien designe en su nombre, teniendo en cuenta la **Guía de Gestion de Bienes G2.MPA1.P5 v4 en el numeral 2.2.5.6 Inventarios Individuales**, para cuando el caso sea de:

    a. Devolución de Bienes al Almacén.
    b. Traslado de Bienes Entre Cuentadantes.

- Las acciones de destrucción para los equipos contenedores de información en los casos que apliquen son responsabilidad del Almacenista de cada Regional, como por ejemplo (donaciones, baja de activos, etc.), y debe ser realizado teniendo en cuenta: **PR4.MPA1.P5 Procedimiento para Definir la Destinación de Bienes Muebles v1**, **PR6.MPA1.P5 Procedimiento Baja Definitiva de Bienes Muebles v1** y **PR32 MPA1 P5 procedimiento para la disposición final de Residuos de aparatos eléctricos y electrónicos – RAEE** y **F1 PR32 MPA1 P5 Listado RAEE's v1.xls**.

6. ALISTAMIENTO DE EQUIPOS

Comprende la preparación completa del equipo de cómputo para garantizar operatividad y las prestaciones requeridas por el usuario final en la red del **ICBF**, una vez se ha efectuado una devolución al Almacén o traslado de Bienes entre Cuentadante.

Nota: Para el alistamiento de máquinas se debe utilizar la lista de chequeo **PPC-ID-170-ICBFOI-003-F1**.

Para llevar a cabo el alistamiento de equipos que estaban en uso, se debe tener en cuenta:

- Contar con el aval mediante ticket solicitada a la Dirección de Información y Tecnología, donde conste que se realizó el proceso de revisión y Backup del equipo objeto del traslado según indica la **Guía de Gestion de Bienes G2.MPA1.P5 v4 en el numeral 2.2.5.6 Inventarios Individuales**.

  Nota importante: La labor de alistamiento de maquina debe ser realizada por personal técnico calificado.

Adicionalmente se surtirán las siguientes acciones:

6.1. Formateo de maquina a bajo nivel.

6.2. Instalación del Sistema Operativo:
Se instala el Sistema Operativo (S.O), autorizado por la Entidad, los medios de instalación deben ser proporcionados por el **ICBF** para garantizar el cumplimiento de las políticas legales de licenciamiento.

6.3. Configuraciones:
- Configuración de la maquina al dominio.
- Configuración del perfil de usuario.

6.4. Instalación de Antivirus
- Se debe instalar el antivirus actualizado y licenciado por la Entidad.

6.5. Instalación de Aplicaciones
- Ofimática licenciada.
- Aplicativos Administrativos y Misionales si se requiere para el ejercicio de su labor, el cual debe estar solicitado mediante ticket y este debe ser avalado por el Supervisor del Contrato.

6.6. Restablecer Respaldo de información usuario:

Para los casos que aplica; Tener en cuenta la copia de seguridad de información elaborada, la información debe ser alojada en las ubicaciones originales desde donde se realizó la copia de seguridad y de esta forma garantizar mínimo impacto. Proceder con la instalación del software que tenía el usuario en la máquina y se había detectado en la maquina antes de realizar el alistamiento. Solicitar a **ICBF** el licenciamiento de este software.

7. MÉTODOS DE DESTRUCCIÓN DE LA INFORMACIÓN

Se debe utilizar el siguiente método para destrucción total de la información contenidos en los dispositivos de almacenamiento son:

a. La des magnetización.

La des magnetización 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, como por ejemplo, los discos duros, disquetes, cintas magnéticas de Backup, DVD, etc.

b. Sobre-escritura.

Este método 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 y DVD.

El método de sobre-escritura para la destrucción segura de la información es el que dispone del mayor número de ventajas entre las que se pueden destacar las siguientes:

- Se puede utilizar para todos los dispositivos regrabables.
- Permite la reutilización de los dispositivos.

8. BORRADO SEGURO DE MEDIOS

La Solicitud de borrado seguro de medios debe ser enviado por el dueño del Macroproceso o Proceso a través de la mesa de Soluciones Informáticas. La solución a esta solicitud debe quedar documentada y evidenciada donde conste que se realizó el proceso de revisión y Backup del equipo objeto del traslado según indica la **Guía de Gestion de Bienes G2.MPA1.P5 v4 en el numeral 2.2.5.6 Inventarios Individuales**.

9. DESTRUCCIÓN SEGURA DE MEDIOS

La información CD y/o DVD, Memorias, Cintas, etc., que corresponda a información clasificada según su rotulación en (Confidencial o Reservada) para el **ICBF**, y que este hayan cumplido su uso, el dueño del Macroproceso o Proceso debe enviar a almacén los medios para que ellos proceda a su destrucción de acuerdo con el procedimiento **PR32 MPA1 P5 Procedimientos Manejo de RAEES v1.pdf** y **F1 PR32 MPA1 P5 Listado RAEE's v1.xls** y **Guía de Gestiona de Bienes G2.MPA1.P5 v4**.

10. NATURALEZA DE LOS CAMBIOS:

Ítem Modif.	Nombre del ítem	Descripción del Cambio
1	Objetivo	Se amplió la descripción de medios y del borrado seguro de los mismos
2	Alcance	Se simplificó el alcance
3	Definiciones	Se incluyó el capítulo de definiciones
4	Desarrollo	Se amplió la introducción y se incluyó la Gestion del ciclo de vida de la información
5	Normas Generales	Se amplió la información incluyendo la normatividad relacionada.
6	Alistamiento de maquinas	Se incluye alistamiento de máquinas dado que es una actividad muy relevante para la manipulación de medios y borrado seguro.
7	Métodos de Destrucción	Se incluye este nuevo capitulo
8	Borrado seguro de medios	Se modificó eliminando la tabla y referenciando la guía de Gestion de Bienes.
9	Destrucción segura de Medios	Se aplique correctamente la guía para la destrucción de los medios.