

 Supersalud 	GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIMN10
	MANUAL PARA EL BORRADO SEGURO DE INFORMACIÓN	VERSIÓN	1
		FECHA	15/05/2023

Manual para el borrado seguro de información

Superintendencia Nacional de Salud

Fecha del documento (15 – 05– 2023)

	GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIMN10
	MANUAL PARA EL BORRADO SEGURO DE INFORMACIÓN	VERSIÓN	1
		FECHA	15/05/2023

Contenido

Objetivo	2
Alcance	2
Políticas de operación	3
Generalidades	3
Actividades que ejecutar para solicitar el borrado seguro de la información	4
Definiciones.....	7

	GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIMN10
	MANUAL PARA EL BORRADO SEGURO DE INFORMACIÓN	VERSIÓN	1
		FECHA	15/05/2023

Objetivo

Establecer lineamientos para eliminar de forma segura la información de la Superintendencia Nacional de Salud (SNS) con el fin de salvaguardar la confidencialidad de la información existente en medios de almacenamiento y garantizar que esta no se pueda recuperar.

Alcance

Este documento aplica a toda la información que los funcionarios, contratistas o terceros de la Superintendencia Nacional de Salud tengan en su poder y se encuentre en cualquiera de los siguientes medios de almacenamiento: discos duros internos y externos, memorias USB, documentación impresa o cualquier otro medio de almacenamiento y que se vayan a dar de baja de inventarios, incinerar, vender, entregarlos como parte de otras compras, que se vayan a donar, o que sean reubicados dentro de las áreas de la entidad.

 Supersalud	GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIMN10
	MANUAL PARA EL BORRADO SEGURO DE INFORMACIÓN	VERSIÓN	1
		FECHA	15/05/2023

Políticas de operación

Cuando la información ha sido tratada en la Entidad y llega al final de su vida útil, debe ser eliminada de forma segura, para evitar que pueda caer en manos de terceros y sea recuperada, es por ello por lo que se deberá cumplir con cada uno de los siguientes criterios:

Generalidades

- ✓ El Oficial de Seguridad de la Información o quien haga sus veces debe vigilar que se cumplan las directrices emitidas en este manual para conservar el nivel de confidencialidad de la información y debe actualizar este documento de acuerdo con las necesidades de la entidad.
- ✓ El coordinador de mesa de servicios (tercero) debe verificar que los técnicos de mesa de servicios, ejecuten las actividades establecidas en este manual y deberá consolidar los resultados y reportarle al administrador de plataforma tecnológica local.
- ✓ El responsable de la información de cada dependencia debe solicitar el respaldo de la información a la cual se le va a realizar borrado seguro, de acuerdo con las políticas establecidas en el Manual para las copias de seguridad de la información.
- ✓ El responsable de la información de cada dependencia debe revisar que se hayan realizado las copias de seguridad, las pruebas y el borrado seguro de la información.

	GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIMN10
	MANUAL PARA EL BORRADO SEGURO DE INFORMACIÓN	VERSIÓN	1
		FECHA	15/05/2023

- ✓ El responsable de la información es quien autoriza el borrador de la información digital, para lo cual debe informar a la mesa de servicio a través de una comunicación enviada al correo soporte.oti@supersalud.gov.co. En el caso de disponer de documentos físicos se debe seguir los lineamientos del Archivo General de la Nación.

Actividades que ejecutar para solicitar el borrado seguro de la información

- ✓ El responsable del activo de Información que requiera el borrado de información deberá solicitarlo a través del correo electrónico: soporte.oti@supersalud.gov.co
- ✓ El técnico de mesa de servicios debe efectuar el registro de la solicitud a través de la herramienta de gestión vigente en la entidad, con el fin de llevar un control de las solicitudes de borrado seguro.
- ✓ Antes de comenzar a efectuar el borrado seguro, el analista o técnico de mesa de servicio designado debe verificar el estado de los medios de almacenamiento o activo de tecnología de información, a través de herramientas tecnológicas establecidas para este fin.
- ✓ Realizar una validación de las licencias de software asignado al usuario del equipo a realizar el borrado seguro
- ✓ El analista de mesa de servicio designado para esta actividad deberá ejecutar borrado seguro sobre dispositivos electrónicos. Para cumplir con este requerimiento se debe utilizar uno de los siguientes métodos según sea conveniente:

	GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIMN10
	MANUAL PARA EL BORRADO SEGURO DE INFORMACIÓN	VERSIÓN	1
		FECHA	15/05/2023

1. **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.

2. **Destrucción Física:** El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena y se puede realizar mediante los siguientes métodos:
 - a) **Desintegración, pulverización, fusión e incineración:** métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora 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. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya una seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos. Los medios ópticos de almacenamiento (CD, DVD, magnetoópticos), deben ser destruidos por pulverización, trituración de corte transversal o incineración.

3. **Sobreescritura:** 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, para dispositivos electrónicos se debe utilizar un software

	GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIMN10
	MANUAL PARA EL BORRADO SEGURO DE INFORMACIÓN	VERSIÓN	1
		FECHA	15/05/2023

que efectué borrado a bajo nivel, guardando los registros como evidencia de la destrucción de la información.

- ✓ Una vez realizado el borrado seguro de la información, el profesional designado de la Subdirección de Tecnologías de la Información deberá establecer cuál será la disposición final del activo de T.I., a saber:

1. **Reúso:** Efectuada la valoración técnica del activo de T.I. se entrega a recursos físicos para la reubicación dentro de las áreas de la Superintendencia Nacional de Salud o para ser donados a terceros.

2. **Baja:** Efectuada la valoración técnica del activo de T.I. y se procederá con la destrucción física o se podrá donar a terceros si se ve la necesidad.

- ✓ El funcionario asignado de la Subdirección de Tecnología de Información debe documentar las actividades de borrado seguro en la base de conocimiento de la herramienta.

	GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIMN10
	MANUAL PARA EL BORRADO SEGURO DE INFORMACIÓN	VERSIÓN	1
		FECHA	15/05/2023

Definiciones

- **Activo de información:** Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Entidad y, en consecuencia, debe ser protegido.
- **Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- **Disponibilidad:** es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
- **Integridad:** es la protección de la exactitud y estado completo de los activos.
- **Responsable por el activo de información:** es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.