Supersalud	**GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN**	**CÓDIGO**	DIMN14
	MANUAL PARA LAS COPIAS DE SEGURIDAD DE LA INFORMACIÓN	**VERSIÓN**	1
		FECHA	17/05/2023

Manual para las copias de seguridad de la Información

Superintendencia Nacional de Salud

Fecha del documento (17 – 05– 2023)

Contenido

Objetivo

Generar lineamientos que respalden la información mediante la utilización de elementos tecnológicos de almacenamientos externos o diferentes a los utilizados en la operación rutinaria de la entidad para garantizar la confidencialidad, integridad y disponibilidad como alternativa de respaldo eficiente ante la posibilidad de pérdida de los datos e información.

Alcance

Este documento aplica para todos los procesos del Sistema Integrado de Gestión. Inicia con la operación de respaldo de la información en el datacenter o centro de almacenamiento de la información y termina con la identificación, rotulación y almacenamiento de la copia de seguridad en los lugares establecidos de acuerdo con los requisitos de retención establecidos en las Tablas de Retención Documental de la entidad.

Políticas de operación

Generalidades

La Subdirección de Tecnologías de la Información debe proveer el respaldo de los activos de información mediante la utilización de elementos tecnológicos de almacenamiento externo o diferente a los utilizados en la operación normal de manera segura.

Los mecanismos para brindar controles de seguridad a la red de la Superintendencia Nacional de Salud, al igual que los funcionarios y terceros deben acogerse a los controles de seguridad establecidos:

1. Se debe garantizar la salvaguarda de la información que esté alojada en los equipos que requieran servicio de mantenimiento donde se deba reinstalar el sistema operativo, formatear el o los disco(s) duro(s) de que disponga, mediante una copia de respaldo que deberá dejar en Sistemas de Almacenamiento durante el tiempo que dure el mantenimiento y puesta a punto del equipo.

2. Antes de adelantar un mantenimiento correctivo para el caso de daño de un disco duro, el responsable del mantenimiento debe contar con las herramientas y mecanismos técnicos y tecnológicos para buscar salvar la información almacenada en el dispositivo averiado.

3. Para los Despachos, Oficinas, Direcciones, Subdirecciones y la Secretaría General, la Entidad ha dispuesto un recurso de almacenamiento en la red, donde debe reposar la información propia de su gestión. El tipo de información que debe ser resguardada en el servidor de archivos de acuerdo con la Ley 1712 de 2014 es Pública Clasificada Artículo 18 y Pública Reservada. Artículo 19.

4. La información que de acuerdo con la Ley 1712 de 2014 en su artículo 11 se considera pública debe ser guardada en el almacenamiento en la nube, donde se cuenta con las medidas de aseguramiento y respaldo de la información que cada funcionario allí deposita.

- En el Servidor de Archivos donde se almacena la información de cada una de las dependencias se tiene control de Modificación/cambios /eliminación: La información que se almacena a través de las carpetas compartidas en la red cuentan con logs (registros de auditoria).

- Los activos de información deben ser gestionados conforme está estipulado en el **Manual para la Clasificación y Etiquetado de Activos** de Información de la entidad.

5. Es deber de los responsables de la información de cada sistema de información verificar la integridad de la información, una vez sea restaurada.

6. Se debe hacer *backup* de la información contenida en las estaciones de trabajo cuando hay retiro de un funcionario de la Entidad.

7. La Subdirección de Tecnologías de la Información debe realizar el resguardo y almacenamiento adecuado de las copias de seguridad para conservación de la información.

Identificación de información crítica.

La Subdirección de Tecnologías de la Información debe identificar:

- El sistema al cual se le realiza la copia de seguridad cuando sea necesario realizar el bloqueo de entrada de usuarios al sistema.

- Si se efectúa una copia completa o parcial a partir del último backup realizado.

- El tipo de sistema de almacenamiento, o si la copia se realiza de manera automática o manual.

Frecuencia Y Tipo De Respaldo

Con el apoyo de sus encargados, la Subdirección de Tecnologías de la Información debe definir los tipos de copias a ejecutar para cada sistema de información.

Para cada copia de respaldo, se debe considerar la frecuencia, los medios de almacenamiento, tipo de contenido, tiempo de almacenamiento y borrado de esta información.

La frecuencia establecida debe ser probada para establecer su practicidad y si es necesario replantear o mejorarla sobre la marcha, verificando que la copia de seguridad se puede hacer correctamente en los tiempos previstos.

Protección de la información en medios de respaldo.

- Los funcionarios asignados deben realizar el registro documentado de las copias de respaldo y del restablecimiento de estas.
- El respaldo de datos y software críticos se deben almacenar en un lugar protegido, con acceso controlado.
- Todo medio o sistema de almacenamiento debe ser rotulado con la siguiente información: Servidor o Base de datos - año - mes – día - hora - consecutivo generado por el sistema.
- En caso de que algún funcionario necesite copias de sus archivos almacenados en el servidor de backup o en los medios de almacenamiento esta solicitud debe ser solicitada a través de la Mesa de Servicios.

- Los centros de cableado y de cómputo deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Pruebas de restauración de las copias de respaldo.

La ejecución de las pruebas de restauración de las copias de respaldo debe asegurar la recuperación de copias de datos, y garantizar la integridad de los datos que contienen.

Se deben realizar pruebas de respaldo programadas trimestralmente y se restaura una copia de seguridad aleatoriamente de las aplicaciones Core de la Entidad para verificar la integridad y disponibilidad de la información, esta tarea deja un registro en la herramienta de gestión de Tecnología de la Información (TI)

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.

- **Centros de cableado:** Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables.

- **Centro de cómputo:** Zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos.

- **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.

- **Equipo de cómputo:** Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

- **Integridad:** Es la protección de la exactitud y estado completo de los activos.

- **Propietario de la información:** Es la unidad organizacional o proceso donde se crean los activos de información.

- **Recursos tecnológicos:** Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Superintendencia Nacional de Salud.

- **Responsable por el activo de información:** 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.

- **SSI:** Subsistema de Seguridad de la Información**.**

- **Sistema de información:** Conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Superintendencia Nacional de Salud o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.