Ministerio de Salud

Gobierno de Chile

PS-NC-004

POLÍTICA RESPALDO DE INFORMACIÓN Y SOFTWARE

Sistema de Gestión de Seguridad de la Información – Nivel Central

Versión Oficial Actual v03 – Octubre del 2019

	Responsable	Fecha	Firma
Elaborado	Rodrigo Vidal / Encargado PMG SSI	Octubre 2019	
Revisado	José Villa / Área Seguridad de la Información (Representante Comité de Seguridad)	Octubre 2019	
Aprobado	Gabriel Reveco / Encargado Ciberseguridad (Presidente Comité de Seguridad de la Información)	Octubre 2019	

MINISTERIO DE SALUD
COMITÉ SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE SALUD
ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Contenido

1 PROPOSITO

Establecer las directrices de respaldo de información en la Institución, para proteger los datos y software en la organización, así como los dispositivos de hardware que la soportan, almacenan y distribuyen.

2 ALCANCE O AMBITO DE APLICACIÓN

Esta política se aplica a toda la información electrónica contenida en los servidores centrales, estaciones de trabajo y equipos comunicacionales, que contengan datos, configuraciones, aplicativos y servicios críticos para el MINSAL.

Es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales.

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta política corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Alcance de Dominios y Controles de Seguridad de la Información (Nch-ISO 27001:2013)		
Nombre del Dominio	ID Control ISO 27001	Nombre del Control
Seguridad de las operaciones	A.12.03.01	Respaldo de la información

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- Marco Normativo
  - NCh-ISO27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
  - El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
    - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
    - Leyes relacionadas
  - Circular 28.704, agosto de 1981. Circular sobre disposiciones y recomendaciones referentes a eliminación de Documentos. Contraloría General de la República.

- **Documentos Relacionados**
  - Documento del Sistema de Gestión de Seguridad de la Información, disponibles en isalud.minsal.cl.
  - Procedimiento para la eliminación segura y reutilizaciones de equipos.

4 ROLES Y RESPONSABILIDADES

- **Departamento TIC:**
  - Definir el estándar de respaldo de los servidores centrales y equipos de hardware de la institución, que detalle los respaldos de software básico, de las aplicaciones, configuraciones de servicios y de los datos en ambiente de producción, autorizar las solicitudes de respaldo especiales.

- **Departamento TIC (Operaciones TIC):**
  - Generar los planes de respaldos, coordinar, ejecutar y probar en intervalos de tiempo los respaldos de información, llevar registros de los respaldos y de pruebas.

- **Encargado de Seguridad de la Información / Encargado de Ciberseguridad**
  - Debe definir, en conjunto con el negocio, el tipo y periodicidad de respaldos que se utilizará para cada aplicación o plataforma de servicios.

- **Usuarios**
  - Debe cumplir con lo establecido en esta política.

5 MATERIAS QUE ABORDA.

- Respaldo de la información

6 DIRECTRICES DE LA POLÍTICA

6.1 Cumplimiento de la legislación

Las medidas de control de acceso a la información definidas deben cumplir y ser consistentes con lo dispuesto por las normas y requerimientos legales definidos en el documento “Normativa del Sistema de Gestión de Seguridad de la Información”.

6.2 Consideraciones generales

Minsal mantiene en sus registros información de distintos tipos de importancia (Alta, Media, Baja). El mecanismo, periodicidad y tecnología de respaldo utilizada para resguardar la información en el tiempo dependerá de la importancia que Minsal le asigne.

Cada respaldo que se realice, manual o automático, deberá quedar registrado en los LOGS de los servidores y en un archivo electrónico (Texto, Planilla, etc.) en carpetas de lectura pública de tal forma de habilitarlos a las jefaturas.

Los medios de respaldo removibles deberán ser retirados del recinto donde se realicen los respaldos y llevados a otro que garantice el catálogo, la fiabilidad, seguridad y disponibilidad de estos.

Las claves de usuario NO serán respaldadas.

Información que NO es relevante para el quehacer de la Institución y que resida en los servidores de archivo del MINSAL NO SERÁ respaldada. La utilidad de la información será determinada por el Comité de Seguridad de la Información del Nivel Central.

6.3 Frecuencia y Tipo de respaldo

La periodicidad con que se realizarán los respaldos será de, al menos, 1 respaldo anual para el caso de los computadores críticos definidos por el Comité de Seguridad de la Información. En el caso de los sistemas informáticos y equipos críticos diferentes a los computadores será de, al menos, 1 respaldo mensual.

El área de Operaciones TIC debe definir los tipos de respaldos a utilizar como estándar para la Institución. Cada estándar debe considerar la frecuencia del respaldo, los medios de almacenamiento, tipo de contenido, tiempo de almacenamiento y borrado de esta información.

Las solicitudes especiales de respaldo protegido deberán ser autorizadas por el Jefe del Departamento TIC y los Encargados de Seguridad de la Información / Ciberseguridad.

6.4 Protección a los medios de respaldo

Para prevenir pérdidas accidentales, todos los archivos, bases de datos e información existente en los Sistemas centrales de la institución, se deben respaldar en un Servidor de Respaldo.

El uso y aprovechamiento del Servidor de Respaldo será destinado únicamente para apoyar las funciones que son propias de la Institución.

Queda estrictamente prohibido almacenar, en las carpetas asignadas en el Servidor Institucional de Respaldos, archivos de juegos, música, reproductores de música y/o video, programas de cómputo sin licencia y cualquier otra información ajena a la Institución.

Si el medio magnético u óptico de respaldo se encuentra próximo a su vencimiento, la información contenida en él deberá ser traspasada a otro medio de respaldo de características similares o superiores. Efectuado el traspaso en forma exitosa, se debe proceder a la eliminación del medio original.

Ante un cambio tecnológico que se produzca en los medios de respaldo, que pueda generar obsolescencia tecnológica, deben generarse las acciones necesarias de resguardo de la información en ellos.

6.5 Protección de la información en medios de respaldo

Un nivel mínimo de información crítica de respaldo deberá almacenarse en una ubicación remota, esta instalación deberá ser emplazada a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal. El nivel mínimo de información será definido por el Comité de Seguridad de la Información del Nivel Central. Dicho respaldo debe tener registros exactos y completos de las copias y procedimientos documentados de restablecimiento. En ámbitos críticos para la institución, se deberán almacenar al menos tres generaciones o ciclos de información de respaldo.

El respaldo de datos y software críticos se deben almacenar en un lugar protegido, con acceso controlado.

Toda información crítica grabada en respaldos que son almacenados fuera de la Institución debe ser trasladada con los elementos de seguridad adecuados, ya sea utilizando métodos de encriptación o utilizar métodos apropiados para prevenir intentos de acceso físico no autorizado.

El área de Operaciones TIC debe mantener un inventario actualizado de la información almacenada externamente.

6.6 Vigencia y retención de los respaldos

La retención del respaldo de la información se debe mantener según lo indica la Circular N°051, del 09 de febrero de 2009, sobre disposiciones y recomendaciones referentes a conservación, transferencia y eliminación de documentos, de la Dirección de Bibliotecas, Archivos y Museos.

6.7 Respaldo de estaciones de trabajo

Es responsabilidad del usuario el debido resguardo de la información contenida en el computador asignado. Lo mismo aplica para las personas que utilicen un computador portátil.

Cualquier necesidad de respaldo, debe ser solicitada formalmente por el Jefe del Departamento o Unidad respectiva, justificando la criticidad de la información a respaldar y dirigida al Jefe del Departamento TIC.

6.8 Borrado de la información

La información contenida en los servidores centrales de la Institución que no sea necesaria debe ser borrada.

La información respaldada en medios magnéticos que pierda vigencia o no se necesite, debe ser borrada del medio magnético que lo contiene.

Todo equipo computacional o medio de almacenamiento que sea dado de baja debe ser examinado por el área de Operaciones TIC, para comprobar que la información ha sido borrada.

La destrucción de medios de almacenamiento (como cintas, CD/DVD, etc.) que contienen información, debe ser efectuada de forma que impida el acceso al medio y de acuerdo con lo establecido en el Procedimiento para la eliminación segura y reutilizaciones de equipos.

7 MECANISMO DE DIFUSIÓN.

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Publicación en la intranet de Minsal http://isalud.minsal.cl/
- Correo informativo.

8 PERÍODO DE REVISIÓN.

La revisión del contenido de esta Política se efectuará a lo menos cada dos años por el Comité de Seguridad de la Información, o atendiendo necesidades de cambios para garantizar su idoneidad, adecuación y efectividad.

9 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

Frente a casos de especiales, el Comité de Seguridad de la Información evaluará y podrá establecer condiciones puntuales de excepción en el cumplimiento de las presentes directrices, siempre que no infrinja la legislación vigente. Toda excepción debe ser documentada y generar un proceso de revisión de la política, que determine si se deben agregar directrices en lo particular.

10 HISTORIAL Y CONTROL DE VERSIONES

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio
01	Septiembre 2014	Todas	Creación del documento
02	Octubre 2014	Ninguna	Aprobación por resolución del documento
03	Octubre 2019	Todas	Cambios en la referencia normativa Formato de documento Responsabilidades