SERVICIO DE SALUD TALCAHUANO
SUBDIRECCIÓN ADMINISTRATIVA
ÁREA DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN
HOSPITAL DE TOMÉ

TOMÉ, 28 OCTUBRE 2025

VISTOS:

Considerando el Decreto Fuerza Ley N° 01/24.04.2006 del MINSAL; el D.F.L. N° 29/2004 sobre Estatuto Administrativo; la Ley N° 19.880 sobre Bases de los Procedimientos Administrativos; la Resolución N° 6/2019 de Contraloría sobre exención de toma de razón en materias de personal; los Decretos Supremos de Salud N° 140/2005 y N° 38/2005 que aprueban los Reglamentos Orgánicos de los Servicios de Salud y de los Establecimientos de Salud de Menor Complejidad; la Resolución Exenta N° 2778/2023 del SSThno; la Resolución Exenta N° 1251/2023 que aprueba la Política General de Seguridad de la Información del Hospital de Tomé; el COMGES 2025; y el Ordinario N° 943/2025 del Subsecretario de Redes Asistenciales sobre implementación de controles críticos de seguridad de la información según ISO/IEC 27001:2022; que, conforme al D.S. N° 285/2022 y la Ley N° 21.663 de Ciberseguridad, el Hospital de Tomé se encuentra incluido en la lista preliminar de **Operadores de Importancia Vital (OIV)**; y que, mediante la Providencia N° DHT-6553 y el oficio N° 0106 clasificado como secreto, se instruye evacuar un Informe Técnico Fundado respecto del cumplimiento de los criterios del artículo 4° del D.S. N° 285/2022, se da curso a la presente comunicación.

CONSIDERANDO:

1. Que la adecuada gestión de respaldo de la información es fundamental para garantizar la disponibilidad, integridad y confidencialidad de los datos institucionales, asegurando la continuidad operativa del Hospital de Tomé.
2. Que el Sistema de Gestión de Seguridad de la Información (SGSI) y la Política de Seguridad de la Información Institucional establecen lineamientos para la protección de los activos de información y la implementación de controles críticos, en concordancia con la ISO/IEC 27001:2022 y las orientaciones del Ordinario N° 943/2025 del Subsecretario de Redes Asistenciales.
3. Que el COMGES 2025 define lineamientos estratégicos institucionales para la gestión segura de la información y la continuidad operacional.
4. Que la implementación de procedimientos de respaldo y recuperación de información permite mitigar riesgos asociados a pérdidas de datos, incidentes de seguridad y eventualidades tecnológicas, cumpliendo con la normativa vigente, incluyendo el Decreto Fuerza Ley N° 01/2006 y el D.F.L. N° 29/2004.
5. Que resulta necesario establecer una política institucional de respaldo de información, que asegure la ejecución sistemática, periódica y segura de copias de respaldo, protegiendo la operación institucional y cumpliendo con los estándares de seguridad de la información.

RESOLUCIÓN EXENTA N° 2118

1. **APRUEBASE** la Política de Respaldo de Información del Hospital de Tomé, en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) y de la Política de Seguridad de la Información Institucional, estableciendo lineamientos, responsabilidades y procedimientos para la ejecución sistemática y segura de copias de respaldo de la información institucional.

SERVICIO DE SALUD TALCAHUANO
SUBDIRECCIÓN ADMINISTRATIVA
ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
HOSPITAL DE TOMÉ

2. **DISPONGASE** que la presente política sea implementada, difundida y cumplida por todos los servicios, unidades y funcionarios del Hospital de Tomé, asegurando la continuidad operacional y la protección de los activos de información.
3. **ENCARGUESE** a la Unidad de Tecnologías de la Información y Comunicaciones (TIC) la supervisión, control y actualización periódica de los procedimientos de respaldo y recuperación de información, reportando cualquier incidencia significativa a la Dirección del establecimiento y al comité de Seguridad de la Información
4. **DEJASE CONSTANCIA** de que la presente resolución entra en vigor a partir de su publicación y que cualquier modificación futura deberá efectuarse mediante resolución exenta de la autoridad competente.

"ANÓTESE Y COMUNÍQUESE"

LEC/CCU/ccu
N° INT. 01/21.10.2025
DISTRIBUCIÓN:

- Subdirección Administrativa H. Tomé
- Oficina de Partes Hospital de Tomé
- CR. Apoyo Diagnóstico
- Área Recursos Físicos

FIRMA DIRECTOR HOSPITAL DE TOMÉ ELECTRONICA

Firmado por Aníbal Antonio Cea Henríquez
Fecha 28/10/2025 15:10:10 CLST

PUEDE VALIDAR ESTE DOCUMENTO CON EL SIGUIENTE CODIGO:309237-51704
EN LA SIGUIENTE URL: https://sstalcahuano.cl/validador_panel

POL03-25-0001

POLÍTICA PARA LA GESTIÓN DE COPIAS DE SEGURIDAD

Sistema de Gestión de Seguridad de la Información – Hospital de Tomé

Versión Oficial Actual 1 – Julio 2025

Contenido

1 PROPOSITO.

Definir reglas que aseguren una adecuada generación, resguardo, mantenimiento y recuperación de la información y software de la Organización, sus unidades, áreas y servicios dependientes, almacenada en unidades de respaldo, con el objeto de proveer continuidad a la operación en caso de contingencias y/o interrupciones del servicio de procesamiento de información y datos.

2 ALCANCE O AMBITO DE APLICACIÓN.

Esta política aplica a toda la información electrónica contenida en los servidores, estaciones de trabajo y equipos computacionales, que contengan datos, configuraciones, aplicativos y servicios críticos para el Hospital de Tomé.
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 el Hospital de Tomé.
Esta política abarca los siguientes controles definidos en la norma NCh-ISO 27002:2022, denominada "Tecnologías de la Información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información" y, en específico:

ALCANCE DE DOMINIOS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN NCH-ISO 27002:2022		
NOMBRE DEL DOMINIO	**ID CONTROL**	**NOMBRE DE CONTROL**
Controles tecnológicos	A.08.13	Respaldo de información

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- ISO 27001:2022: Seguridad de la información, ciberseguridad y protección de la privacidad – 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.
    - Ley N° 21.663 sobre Marco de Ciberseguridad, esta ley proporciona un marco para asegurar la ciberseguridad de infraestructuras críticas, que indirectamente impacta en la protección de datos.
    - Ley N° 20.285, sobre acceso a la información pública.
    - Ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
    - Decreto N° 181, aprueba reglamento de la ley N° 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.
    - Ley N° 19.628, sobre protección de la vida privada1.

- Ley N° 19.880, establece las bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado.
- Decreto N° 83, 2004, Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
- El Decreto Supremo N° 7 establece una Norma Técnica de Seguridad de la Información y Ciberseguridad, en concordancia con la Ley Nº21.180 sobre Transformación Digital del Estado

4 ROLES Y RESPONSABILIDADES [Revisar roles de acuerdo con la Institución].

- **Usuarios**
  - Adherirse a las disposiciones de la política, incluyendo el manejo seguro de datos y la notificación de incidentes relacionados con la pérdida o corrupción de información.
- **Jefe de Área de Tecnologías de la Información**
  - Aprobar, en conjunto con la autoridad y el negocio, los planes de respaldo y restauración.
- **Unidades de TI Encargadas (Operaciones TI / Tecnologías Digitales)**
  - Definir el estándar de respaldo de los servidores y equipos computacionales de la institución, que detalle los respaldos de software básicos, de las aplicaciones, configuraciones de servicio y de los datos en los distintos ambientes de producción, QA y Desarrollo, autorizar las solicitudes de respaldo especiales.
  - Generar los planes de respaldo y restauración (Internos o con Terceros)
  - Coordinar, ejecutar y/o supervisar y documentar cada proceso de respaldos, según corresponda cuando se trate de terceros
  - Realizar pruebas regulares de calidad de los respaldos en intervalos de tiempo definidos en la frecuencia y tipos de respaldo en este documento.
  - Llevar registros de los respaldos y de pruebas
  - Notificar al negocio y al encargado de Seguridad de la Información sobre los problemas de calidad de los respaldos que se adviertan
- **Encargado de Seguridad de la Información**
  - Debe definir, en conjunto con el negocio, el tipo y periodicidad de respaldos que se utilizará para cada aplicación o plataforma de servicios.
- **Terceros (Proveedor)**
  - Cumplir con la presente política y los acuerdos administrativos generados, respetando las Políticas de Seguridad de la Información de la Institución.

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 en el SGSI Institucional se deben cumplir y ser consistentes con lo dispuesto por las normas y requerimientos legales definidos y que son parte del Sistema de Gestión de Seguridad de la Información Institucional.

6.2 Consideraciones generales.

El Área de Tecnologías de la Información y Comunicaciones (TIC), será responsable del respaldo de la información contenida en los servidores centrales, mientras que las demás áreas, serán responsables del respaldo de sus datos cuando éstos no se encuentren en un servidor centralizado.

En el caso de que los servidores centrales se encuentren externalizados con un proveedor de servicio, el Área TIC será responsable de verificar que los respaldos sean realizados. (Aplica para contratos con terceros) Para estos casos el proveedor del servicio deberá enviar según acuerdos los "jobs" de respaldos generados y el resultado de estos, de acuerdo con el procedimiento definido en conjunto con el proveedor y de acuerdo con los servidores respaldados.

El Hospital de Tomé 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 el Hospital de Tomé le asigne.

Cada respaldo que se realice, manual o automático, deberá quedar registrado en los LOGS de los servidores, en los informes de reporte diario de la plataforma de respaldo o a través de archivos electrónicos (texto, planilla, etc) que se disponga para tales efectos. Si existe un servicio externo contratado para el resguardo de las cintas magnéticas, se llevará un registro de retiro de las cintas.

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 los datos.

Las claves de usuario NO serán respaldadas.

La información que NO es relevante para el quehacer de la institución y que resida en los servidores de archivo del Hospital de Tomé NO SERÁ respaldada. La utilidad de la información será determinada por el Comité de Seguridad de la Información del Establecimiento.
No se debe ejecutar ningún proceso de resguardo que no se encuentre materializado en la bitácora predefinida y aprobada.

Se debe efectuar las copias de respaldo en horarios adecuados, de forma tal que no afecten el rendimiento de los servidores, preferentemente en horarios no laborales o de baja carga. Se debe realizar la depuración y/o restauración de información a los equipos de procesamiento, teniendo en cuenta las necesidades de contar con la información operativa en línea de acuerdo con los requerimientos específicos y el rendimiento del equipo.

Toda solicitud de respaldo adicional a las habituales debe ser formalizada a través de la mesa de servicio TI por la Jefatura del área solicitante, y dependiendo de la naturaleza del respaldo solicitado, también deberá ser autorizada por el Encargado de Seguridad. (Todos los activos Críticos)

Se debe rotular las copias de respaldo, a fin de facilitar su identificación, identificando entre otras cosas el tipo de respaldo (archivo de datos, aplicación, etc.), el ciclo de respaldo (diario, mensual, etc.) y la fecha de generación del respaldo; cuando sea requerido.

Se deberán efectuar respaldo de la Información de los servidores, previo a una modificación significativa en los Sistemas Operativos.

Se debe realizar un respaldo incremental diario de los servidores que alojan bases de datos, aplicaciones y el sitio web institucional. Para las máquinas virtuales, se emplearán snapshots que permitan una recuperación rápida ante fallos.

En el caso de los recursos de archivos compartidos, se realizarán instantáneas diarias con el fin de optimizar los tiempos de restauración y reducir el uso de cintas magnéticas.
Cuando se realicen respaldos en cinta magnética, estas deberán ser retiradas de la unidad una vez finalizado el proceso, conforme a los procedimientos establecidos de resguardo externo.

6.3 Protección y mantención de 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 Dedicado.

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, lo anterior se extrapola a los computadores institucionales.

Si el medio magnético y 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.

El sitio en el que se mantengan las copias de respaldo deberá cumplir con todas las reglas de control de acceso y seguridad ambiental definidas en el procedimiento de Seguridad Física. En caso de no contar con una bóveda de almacenamiento electrónico y utilizar almacenamiento físico, se deberán considerar los siguientes aspectos:

- Al momento de ingresar el medio de almacenamiento (Disco, CD, DVD u otro) a custodia, debe registrase en la planilla la fecha, hora, rótulo del medio, persona que es responsable de transportar el medio a la custodia, igualmente cuando alguien autorizado solicite unidades para prueba o recuperación.
- Se debe eliminar información cuando el espacio ocupado de los discos esté al límite del nivel de ocupación aceptable (previamente definido), llevando un control de lo borrado y estableciendo los mecanismos para recuperarla en caso de ser necesario.
- Se debe llevar en forma permanente un inventario de los medios magnéticos de almacenamiento existentes, su contenido y el lugar donde están almacenados. Además, se debe realizar un inventario anual de los medios magnéticos, de preferencia en los meses de verano.
- Se deben fijar ubicaciones externas, alejadas de las instalaciones que den origen al respaldo, para conservar las copias de respaldo de la información definidas como críticas. Las mismas se deben adecuar a las condiciones establecidas en la Política de Seguridad Física y Ambiental.
- Se debe establecer la frecuencia y forma de envío de las copias de respaldo a la ubicación externa, el que debe efectuarse por un medio de transporte seguro que garantice la protección física de las mismas.
- Se debe llevar un control de la vida útil de los medios de almacenamiento, con el objeto de no utilizar medio susceptibles de daño para el respaldo de información.

- Anualmente se debe emitir un informe que describa la antigüedad que poseen los distintos dispositivos físicos (CD, Cintas, Catridges, discos u otros) ubicados tanto en el centro de almacenamiento interno como externo de la entidad, con un especial énfasis en aquellos que según especificaciones del fabricante están a punto de expirar su vida útil. Dicho informe deberá ser analizado por el jefe del área de Tecnologías de la Información y Comunicación.

- También se deben emitir un informe que señale la antigüedad de la información almacenada y en especial la que según los entes reguladores que aplique, ya no es necesario conservar. Dicho informe deberá ser analizado en conjunto con las áreas involucradas.

6.4 Respaldo de servicios en nube (si aplica).

Cuando el Hospital de Tomé utilice los servicios en la nube, debe garantizar la creación de copias de seguridad de la información, aplicaciones y sistemas alojados en el entorno del proveedor.

Estas copias de seguridad deben realizarse con la frecuencia establecida en la presente política, asegurando su alineación con los requisitos operativos, legales y de seguridad.

Además, debe evaluar la efectividad del servicio de respaldo proporcionado por el proveedor de la nube, verificando que cumple con los están estándares de protección de los acuerdos de nivel de servicio (SLA). Como parte de este proceso, se deben realizar pruebas periódicas de restauración para confirmar que la información respaldada puede recuperarse de manera confiable en caso de contingencias.

6.5 Recuperación de la Información.

Esta actividad es ejecutada por el Área de Tecnologías de la Información y Comunicación, que administra los servicios tecnológicos.

Se debe documentar el proceso y procedimientos de recuperación de la información almacenada en los medios definidos. Para estos efectos es necesario mantener documentación adecuada de los procedimientos utilizados para la constitución de los respaldos, consignando especialmente cambios al entorno que pudiesen incidir en la recuperación de la información, como son modificaciones al software o procedimientos de administración de bases de datos o sistemas, que pudiesen hacer que información guardada no pudiese ser restablecida.
Se debe duplicar el respaldo en forma previa a llevar a cabo el proceso de restauración de la información. De manera que, si surge algún problema durante la recuperación, los originales no sean dañados.

Se deben realizar pruebas periódicas en aquellos respaldos que por su naturaleza no son requeridos frecuentemente (idealmente en forma trimestral para los datos de los sistemas de aplicación) con el fin de asegurarse la disponibilidad de la información y además se deben realizar pruebas muestrales a la información respaldada por los usuarios en la red. Se deben documentar las pruebas.

En caso de que la función de respaldo y recuperación de la información esté tercerizada, las unidades de TI deberán prever en los contratos suscritos, que dichas funciones se realicen en conformidad a los procedimientos definidos y a esta política.

6.6 Comprobación de integridad de la información.

El Área TIC deberá comprobar la integridad y confiabilidad del sistema utilizado para realizar los respaldos de información. En el caso de que los servidores centrales se encuentren externalizados con un proveedor de servicios, deberá verificar que esto ocurra.

Se realizarán de manera periódica restauraciones de información en un escenario adecuado, a manera de verificar la integridad de la información respaldada.

Se deberá configurar el software de respaldo para que almacene bitácoras en las cuales se registre cada evento al momento de realizar un respaldo de información.

6.7 Restauración de la información.

Los dueños de los activos son los únicos autorizados para solicitar la recuperación de información ante un incidente asociado a la pérdida total, parcial de información o para realizar pruebas controladas de restauración de respaldos.

Para llevar a cabo las pruebas de restauración de información se deberán tener en cuenta los siguientes aspectos:

- El Área TIC elaborará anualmente el plan de pruebas de restauración de información, incluyendo actividades, estimación de fechas, responsables, relevancia de la información (dependencias, aplicaciones) entre otros.
- Se debe conservar el log del registro de la tarea de restauración, con el fin de validar que se ejecutó la tarea satisfactoriamente. En caso de que no se realice la restauración correctamente, se deberán analizar las causas y ejecutar la tarea nuevamente.
- El tiempo de duración de la restauración dependerá del tipo de conexión y tamaño de la data a restaurar.
- La información respaldada debe quedar encriptada en el momento de la generación del backup (respaldo).
- Las pruebas de restauraciones deben ser periódicas, de acuerdo a lo que se defina en el plan de pruebas de restauración de la información, las carpetas y/o archivos a restaurar se seleccionarán aleatoriamente, se seleccionará la ubicación donde se realizará la restauración, esta puede ser en su ubicación original para el caso de información eliminada por un usuario o en una carpeta creada para tal fin (por seguridad se recomienda esta última opción, para evitar que se sobrescriban archivos existentes ya modificados por un usuario).

- Se deberán realizar pruebas aleatorias de la integridad de los respaldos y hacer pruebas de restauración sobre ambientes de pruebas controlados para validar la efectividad de los respaldos.

6.8 Frecuencia y Tipo de respaldo.

Equipos asignados a los funcionarios: 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.

Sistemas y Bases de Datos: Con el fin de mantener los resguardos mínimos requeridos, se establece como estándar para cada unidad el procedimiento de respaldo que deberá contemplar como mínimo cumplir en especial a lo referido a las retenciones requeridas. La Institución podrá definir la retención de los respaldos de acuerdo con criterios previamente definidos y establecidos formalmente.

El período establecido para la ejecución de las copias de seguridad se define de acuerdo con las políticas, tipo, frecuencia y tiempo de retención que se describen:

- Política ambiente producción
    - Respaldos incrementales diarios con retención de 60 días.
    - Respaldos full semanal con retención de 365 días
    - Respaldos full mensual con retención de 2.190 días
    - Respaldo full anual con retención 2.190
- Política ambiente de pruebas (QA)
    - 1 respaldo semanal incremental con retención de 60 días.
    - Respaldo full mensual con retención de 365 días.
- Política ambiente desarrollo
    - 1 respaldo semanal incremental con retención de 60 días.
    - Respaldo full mensual con retención de 365 días.

El área de Tecnologías de la Información 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 Área de TI y el Encargado de Seguridad de la Información / Ciberseguridad.

6.9 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 establecimiento. 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.

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 TI debe mantener un inventario actualizado de la información almacenada externamente, proporcionado por el proveedor que mantiene el servicio de resguardo del respaldo.

6.10 Protección de la información en medios magnéticos (cintas).

Se deberán garantizar la custodia y almacenamiento de los medios magnéticos (cintas) a través de un servicio especializado, que considere el resguardo del respaldo, será responsabilidad del proveedor que preste el servicio:

Las cintas de respaldo deben tener un lugar de protección física y ambiental adecuada para mantener la confidencialidad, la integridad y la disponibilidad de la información digital, de software y sistemas informáticos.

Se debe velar por la custodia física de todos los medios magnéticos, tanto históricos como vigentes almacenados en dependencias del proveedor del servicio de respaldo. El acceso al lugar de almacenamiento de las cintas de respaldo debe ser restringido y sólo podrán acceder a aquellas personas autorizadas.

El respaldo de datos y software críticos se deben almacenar en un lugar protegido, con acceso controlado y de la misma forma el servicio de resguardo del respaldo.
Se deberá mantener un catálogo actualizado del software de respaldo el que debe ser entregado periódicamente en copia al Área de TI, así como el registro de altas y bajas de cintas por el proveedor del servicio.

Se deberá asegurar que no existan intervenciones foráneas en los respaldos afectados durante los traslados por el proveedor.
Se deben asegurar la recuperación de información a un estado consistente y conocido en caso de falla del sistema, así como mantener la consistencia de los inventarios de los medios magnéticos onsite.

Se debe verificar el estado de los soportes físicos que contienen las copias de seguridad, comprobando que los respaldos son capaces de recuperar la información respaldada.
Se debe disponer mecanismos de cifrado sobre los medios portables.
Será responsabilidad del referente técnico del contrato, velar por el cumplimiento de los puntos señalados.

6.11 Vigencia, revisión y retención de los respaldos.

La obligación de la administración de realizar respaldos de la información que consta en los sistemas de información se rige por lo previsto en el Decreto 83 de Minsegpres, de 2004, sobre seguridad de la información y la de conservar la información relativa a sus procesos y documentos se regirá por lo previsto en la Ley y normas reglamentarias para cada caso concreto. Lo anterior además debe estar acorde a la Ley Marco de Ciberseguridad.

Se deben asegurar la recuperación de información a un estado consistente y conocido en caso de falla del sistema, así como mantener la consistencia de los inventarios de los medios magnéticos onsite.

Se debe verificar el estado de los soportes físicos que contienen las copias de seguridad, comprobando que los respaldos son capaces de recuperar la información respaldada.
Se debe disponer mecanismos de cifrado sobre los medios portables.

6.12 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 Área o unidad respectiva (excluyente), justificando la criticidad de la información a respaldar, este proceso se realizará a través de la Mesa de Servicio TI, Solicitud de Servicio, Categoría "Gestión de Recursos en la Nube" y Respaldo de Información.

Recuerde que para acceder a la Mesa de Servicio debe realizarlo a través de: https://tic.hospitaldetome.cl

6.13 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. Para el caso del servicio de respaldo externo deberá certificar la correcta eliminación y borrado de medios de respaldo.

Todo equipo computacional o medio de almacenamiento que sea dado de baja debe ser examinado por la Unidad de Operaciones TI, 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 reutilización 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:

- Correo Informativo.
- Mesa de Servicio TI, Sección "Soluciones"
- Carpeta de Seguridad de la Información en la Nube Institucional, disponible en todos los Computadores Institucionales.

8 PERÍODO DE REVISIÓN.

La presente política deberá ser revisada cada dos años o cuando ocurran cambios significativos para garantizar que:

- Sigue siendo adecuada para su propósito.
- Refleja los cambios en las tecnologías.
- Está alineado con la legislación vigente, los estándares internacionales y las mejores prácticas.

9 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

Frente a casos especiales, el Comité de Seguridad de la Información evaluará y podría 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

11 TERMINOLOGÍA

- Jobs: un job es una tarea programada o ejecutada que realiza una acción específica relacionada con la gestión de datos, como hacer una copia de seguridad, restaurar archivos, verificar integridad o replicar datos.