Asesoría Jurídica

Mat.: Aprueba *"Política de respaldo de información y software"*

Santiago.

VISTOS, Lo dispuesto en:

1. El Decreto con Fuerza de Ley N° 1, de 2005, del Ministerio de Salud, que fija texto refundido, coordinado y sistematizado del Decreto Ley N°2.763, de 1979, y de las leyes N^{os}. 18.933 y 18.469;

2. El Decreto con Fuerza de Ley N° 1/19.653, de 2001, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado;

3. La Ley N°19.880, sobre Bases de los Procedimientos Administrativos de los Órganos del Estado;

4. Los Decretos Supremos N° 140/2004 y N° 38/2005, ambos del Ministerio de Salud, que aprueban los reglamentos orgánicos de los Servicios de Salud y de los Establecimientos de Autogestión en Red;

5. La Resolución N° 36/2024, de la Contraloría General de la República, que establece los actos administrativos exentos del trámite de toma de razón.

6. La Resolución Exenta RA N°116675/92/2024, de 30 de enero de 2024, que modifica la Resolución Exenta RA N°116675/419/2023, del Servicio de Salud Metropolitano Central, que nombra en calidad de titular el cargo de Director del Hospital de Urgencia Asistencia Pública.

7. Resolución Exenta N°3.195, de 2024, del Hospital de Urgencia Asistencia Pública, que establece jefaturas, determina subrogancia para los cargos de Director, Subdirector, Jefes y Encargados de Unidades, del Hospital de Urgencia Asistencia Pública.

XASV

CONSIDERANDO

a) Que, el Hospital de Urgencia Asistencia Pública, como establecimiento autogestionado de alta complejidad, debe garantizar la disponibilidad, integridad y confidencialidad de la información crítica institucional, en cumplimiento de sus funciones clínicas, administrativas y de soporte.

b) Que, la creciente dependencia de sistemas informáticos para la gestión hospitalaria y la amenaza de incidentes tecnológicos, ciberataques o fallas operativas, exigen contar con políticas formales de respaldo y recuperación de información que aseguren la continuidad operativa y la resiliencia institucional.

c) Que, la presente Política de Respaldo de Información y Software establece las directrices técnicas, roles, procedimientos y responsabilidades que regulan la generación, almacenamiento, mantenimiento y restauración de activos digitales esenciales del HUAP, en conformidad con la normativa vigente, los estándares ISO/IEC 27001 y las orientaciones del MINSAL en materia de ciberseguridad.

d) Que, este instrumento incorpora prácticas como el modelo de respaldo 3-2-1, pruebas periódicas de recuperación, clasificación de activos críticos, registro de logs, control de medios físicos y mecanismos de mejora continua, aplicables a todos los funcionarios, terceros o empresas externas que intervienen en la administración de dichos activos

e) Que, de conformidad con lo anterior, en el ejercicio de lo dispuesto en el artículo 23 letra c) del Decreto Supremo N°38. De 2005, del Ministerio de Salud, que contiene el Reglamento Orgánico de los Establecimientos de Salud de Menor Complejidad y de los Establecimientos de Autogestión en Red, según el cual le corresponde al Director organizar internamente el Establecimiento Autogestionado y;

f) asignar las tareas correspondientes, con el fin de atender las necesidades públicas o colectivas de una manera regular, continua y permanente, como lo ordenan los artículos 3° y 28 de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, y con la finalidad de establecer la ***primera versión*** de la *"Política de respaldo de información y software"*, dicto la siguiente:

RESOLUCIÓN

I. APRUÉBANSE la ***primera versión*** de la *"Política de respaldo de información y software"*, que es del siguiente tenor:

Servicio de Salud Metropolitano Central – Ministerio de Salud	POLÍTICA DE RESPALDO DE INFORMACIÓN Y SOFTWARE				
	CÓDIGO UTIC	VERSIÓN 01	FECHA 09/2025	VIGENCIA 5 años	N° PÁGINAS 22

HOSPITAL DE URGENCIA ASISTENCIA PUBLICA

Revisado Por:	Aprobado Por:
FIRMA ELECTRONICA AVANZADA – GOBIERNO DE CHILE Firmado por: Ilse Dora del Carmen Silva Robles Jefatura Calidad y Seguridad del Paciente (s) Fecha: 29-09-2025 08:46 CLT Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río	FIRMA ELECTRONICA AVANZADA – GOBIERNO DE CHILE Firmado por: Jorge Arturo Ibáñez Parga Director Huap (s) Fecha: 29-09-2025 19:14 CLT Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

ÍNDICE:

I. PROPÓSITO Y OBJETIVO:

Definir las directrices institucionales que aseguren la generación, almacenamiento, control, mantenimiento, recuperación y retención de la información y software crítico del Hospital de Urgencia Asistencia Pública (HUAP). Esta política tiene como objetivo garantizar la disponibilidad, integridad y confidencialidad de la información institucional ante pérdida, corrupción, ciber incidentes, fallas técnicas o desastres.

II. ALCANCE O ÁMBITO DE APLICACIÓN:

Esta política aplica a todos los activos de información institucional del Hospital de Urgencia Asistencia Pública (HUAP) que procesen, almacenen o respalden datos clínicos, administrativos o de soporte. Se excluyen los equipos personales asignados a funcionarios, cuya responsabilidad de respaldo recae en el propio usuario, según lo establecido en esta política.

La aplicación de esta política incluye a todos los funcionarios, personal a honorarios, empresas externas o terceros que intervienen en la administración, respaldo, recuperación o supervisión de dichos activos institucionales.

En particular, abarca los siguientes activos críticos:

- Servidores centrales en entornos virtuales (Proxmox)
- Sistemas de almacenamiento NAS, Storage (File Server)
- Estaciones de trabajo de jefaturas con información sensible
- Bases de datos institucionales (Navicat)
- Equipos médicos con software embebido y software clínico.

III. MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- ISO/IEC 27001:2022 – Establece requisitos para sistemas de gestión de seguridad de la información, incluyendo ciberseguridad y protección de la privacidad.
- ISO/IEC 27002:2022 – Proporciona controles de seguridad de la información aplicables a la implementación de la norma ISO/IEC 27001.
- Ley N° 21.663 – Marco de Ciberseguridad para infraestructuras críticas.
- Ley N° 20.285 – Acceso a la información pública.
- Ley N° 19.799 – Firma electrónica y documentos digitales.
- Decreto Supremo N° 181 – Reglamento de la ley N° 19.799 sobre firma electrónica.
- Ley N° 19.628 – Protección de la vida privada.
- Ley N° 19.880 – Procedimientos administrativos en órganos del Estado.
- Decreto Supremo N° 83 (2004) – Norma técnica sobre seguridad y confidencialidad de documentos electrónicos.
- Decreto Supremo N° 7 – Norma técnica de ciberseguridad en el marco de la Ley N° 21.180 sobre Transformación Digital del Estado.
- Orientaciones técnicas del MINSAL sobre respaldo y continuidad operativa.

IV. ROLES Y RESPONSABILIDADES.

- **Dirección:**
  - Aprueba y respalda la presente política en su calidad de máxima autoridad institucional.
  - Supervisa su implementación a través de informes periódicos emitidos por la Unidad TIC y el Encargado/a de Ciberseguridad, pudiendo delegar esta función a la Subdirección Administrativa y Financiera (SDA).

- **Área TIC:**
  - Diseña y mantiene los estándares de respaldo (frecuencia, medios, cifrado).
  - Coordina planes con Dirección y unidades operativas.
  - Garantiza medidas de continuidad operativa y resiliencia tecnológica.

- **Infraestructura TI / Operaciones:**
  - Ejecuta los respaldos automáticos o manuales según política vigente.
  - Documenta logs y estados de respaldo.
  - Realiza pruebas de recuperación trimestrales o según criticidad del activo.
  - Notifica incidentes de respaldo fallido o recuperación incompleta.

- **Encargado/a de Seguridad de la Información / Ciberseguridad:**
  - Define, junto a TIC y unidades usuarias, la frecuencia y tipo de respaldo por sistema.
  - Supervisa el cumplimiento normativo de la política.
  - Apoya la gestión de incidentes relacionados con pérdida o corrupción de datos.

- **Unidad de Auditoría:**
  - Revisa el cumplimiento de esta política en auditorías internas o externas.
  - Controla evidencia de respaldos, bitácoras, almacenamiento seguro y recuperación.

- **Departamentos y Unidades Funcionales:**
  - Son áreas del hospital que gestionan información institucional relevante para la operación clínica, administrativa o de soporte.
  - Deben informar a TIC sobre los sistemas o archivos que requieren respaldo y coordinar su correcta implementación.

- **Funcionarios que utilizan sistemas institucionales:**
  - Cumplen con las buenas prácticas de manejo y almacenamiento de información crítica.
  - Reportan pérdidas, alteraciones o corrupción de datos al área correspondiente.

V. MATERIAS QUE ABORDA.

La presente política regula los aspectos técnicos y administrativos necesarios para asegurar la correcta planificación, ejecución, verificación y mejora de los procesos

de respaldo y recuperación de información crítica del HUAP. En particular, aborda las siguientes materias:

- Definición del modelo de respaldo adaptado al enfoque 3-2-1, con dos copias en diferentes medios y una copia fuera del sitio.
- Inventario y clasificación de activos críticos respaldados, incluyendo máquinas virtuales, NAS, bases de datos y estaciones de trabajo sensibles.
- Determinación de la frecuencia y métodos de respaldo según tipo de activo, utilizando herramientas como rsync, Cobian Backup y Navicat.
- Establecimiento de parámetros de recuperación (RTO y RPO) con tiempos máximos definidos por tipo de sistema.
- Seguridad de la información respaldada, incluyendo cifrado en tránsito, control de accesos y envío de logs automatizados.
- Criterios de retención y eliminación segura de respaldos, conforme a requisitos operativos y capacidad de almacenamiento.
- Gestión de incidentes y registro de fallas, mediante alertas automáticas y bitácoras manuales.
- Asignación clara de roles y responsabilidades para personal técnico y jefaturas.
- Planificación y ejecución de pruebas de restauración documentadas, realizadas dos veces al año para validar integridad y tiempos de recuperación.
- Monitoreo y mejora continua del proceso de respaldo, incluyendo auditorías periódicas de logs y revisión anual de la política.

VI. DIRECTRICES DE LA POLÍTICA.

1. Cumplimiento de la legislación.

a. Las medidas de control de acceso, protección y manejo de la información respaldada deberán cumplir con las normativas y requerimientos legales descritos en el apartado 3 “Marco Normativo y Documentos Relacionados”. Esto incluye, pero no se limita a, la protección de la información clínica, diagnósticos, datos personales de pacientes y demás datos sensibles conforme a la legislación vigente en materia de privacidad y protección de datos personales.

2. Consideraciones generales.

a. Responsabilidad Institucional de Respaldo

i. El Encargado/a de Infraestructura TI es responsable de ejecutar y mantener los respaldos automáticos de los sistemas bajo su administración. Las unidades funcionales deberán coordinar con TIC el respaldo de información crítica que se gestione localmente (por ejemplo, archivos en estaciones de trabajo), especialmente en jefaturas o áreas sensibles.

b. Respaldos en Plataformas o Servicios Externos

i. Cuando se utilicen servicios externos para almacenamiento o respaldo, el Unidad TIC deberá verificar que el proveedor cumpla con los acuerdos de servicio establecidos. Se solicitará evidencia básica de ejecución (logs, informes automáticos o capturas), cuando sea aplicable.

c. Registro de Respaldo y Trazabilidad

i. Todos los respaldos deben dejar evidencia registrada mediante logs automáticos (rsync, cron, Cobian), capturas de pantalla en respaldos manuales, o bitácoras en caso de falla de los mecanismos automatizados. Estos registros se conservarán según la política de retención y estarán disponibles para auditoría.

d. Custodia Segura de Medios Removibles

i. Los discos externos utilizados para respaldos deben estar rotulados y almacenados en un lugar seguro dentro del

hospital, bajo supervisión del equipo TIC. Se evitará el uso de medios sin identificación o bajo custodia no autorizada.

e. Exclusión de Credenciales

i. Está prohibido respaldar contraseñas, claves privadas u otros datos de autenticación sensibles. Esta medida busca proteger la confidencialidad y prevenir accesos indebidos.

f. Procedimientos Autorizados y Documentados

i. Solo se ejecutarán procedimientos de respaldo previamente definidos por el equipo TIC. Toda modificación deberá ser validada técnicamente y registrada en la bitácora institucional.

g. Horarios de Ejecución de Respaldo

i. Los respaldos automáticos se programan fuera del horario hábil (por ejemplo, 05:00 AM) para evitar interferencias con los sistemas productivos. Los respaldos manuales se realizarán según disponibilidad operativa.

h. Mantenimiento y Restauración Periódica

i. Se deben realizar labores de depuración de respaldos antiguos, verificación de integridad y restauración de archivos o sistemas, conforme a las necesidades operativas y a la política de retención. Las restauraciones deben ser controladas, evaluadas y documentadas.

i. Solicitudes Especiales de Respaldo

i. Toda solicitud de respaldo fuera del ciclo habitual (por ejemplo, previo a auditoría o mantenimiento) deberá ser enviada por correo institucional y aprobada por el encargado/a de ciberseguridad o jefatura TIC.

j. Rotulación Estandarizada

i. Los respaldos deben incluir rotulación clara (nombre, fecha, tipo de copia) para facilitar su trazabilidad y gestión en procesos de restauración o eliminación.

k. Respaldo Previo a Cambios Críticos

i. Antes de realizar actualizaciones, migraciones o intervenciones en sistemas críticos, se debe ejecutar un respaldo completo del entorno afectado.

l. Frecuencia Recomendada por Tipo de Activo

i. Bases de datos: respaldo completo diario.

ii. Máquinas virtuales (Proxmox): se realizan respaldos completos (full) una vez a la semana para cada máquina en producción. Además, algunas máquinas se respaldan a diario, dependiendo de su criticidad. No se realizan respaldos diarios de todas las máquinas debido a limitaciones en la infraestructura.

iii. Archivos compartidos (NAS): instantánea o respaldo completo diario.

iv. Archivos locales de jefaturas: respaldo mensual (automático o manual según criticidad).

3. Protección y mantención de los medios de respaldo.

a. Servidor de Respaldo Dedicado

i. La información crítica de los sistemas institucionales se respalda en servidores designados exclusivamente para esta función. Estos servidores no deben utilizarse para almacenamiento personal ni para fines distintos al respaldo institucional.

b. Prohibición de Uso Inadecuado

i. Está prohibido almacenar en los servidores de respaldo archivos no relacionados con funciones institucionales, como contenido personal, multimedia, software sin licencia u otros elementos ajenos a la operación del hospital.

c. Sustitución de Medios Obsoletos

i. Cuando un disco externo o medio físico muestre signos de desgaste o fallas, su contenido será transferido a un nuevo dispositivo. El medio anterior será eliminado conforme a las prácticas de destrucción segura definidas por TIC.

d. Actualización por Obsolescencia Tecnológica

i. Frente a cambios tecnológicos o incompatibilidades, el equipo TIC evaluará la migración de respaldos a medios más actuales, asegurando la integridad y disponibilidad de la información.

e. Seguridad del Sitio de Respaldo

i. Los respaldos se almacenan en ubicaciones físicas dentro del hospital que cuentan con acceso restringido. Se busca mantener condiciones adecuadas de seguridad ambiental (temperatura, humedad) y control de acceso básico.

f. Gestión en Bóvedas o Almacenamiento Físico

i. Cuando se utilicen discos externos, se aplicarán medidas mínimas de control:

1. Rotulación clara del dispositivo.
2. Registro básico del uso (fecha, responsable, tipo de respaldo).
3. Inventario actualizado de medios disponibles.
4. Eliminación de información conforme a la política de retención.

g. Etiqueta y Clasificación

i. Todo medio físico debe estar rotulado con nombre del respaldo, fecha, tipo de copia (diaria, mensual, externa) y nivel de criticidad, si aplica.

h. Evaluación Periódica

i. El estado de los medios físicos será revisado al menos una vez al año por el equipo TIC, junto al encargado/a de ciberseguridad, para verificar su funcionalidad y vigencia.

4. Respaldo de servicios en nube (si aplica).

a. Cuando el Hospital de Urgencia Asistencia Pública (HUAP) utilice servicios en la nube formalmente contratados o gestionados por el equipo TIC, se deberá garantizar la creación de copias de seguridad de la información, aplicaciones y sistemas alojados en dichos entornos.

Estas copias deben realizarse con la frecuencia definida en esta política, cumpliendo los requisitos operativos, legales y de seguridad.

El equipo TIC será responsable de controlar el uso de estos servicios, mantener un inventario actualizado de los entornos en nube utilizados, y verificar que los proveedores cumplan con los acuerdos de nivel de servicio (SLA). Como parte de este control, se deben realizar pruebas periódicas de restauración para asegurar que la información respaldada pueda recuperarse de forma confiable ante contingencias.

5. Recuperación de la Información.

a. Responsabilidad

i. La recuperación de información es responsabilidad exclusiva del equipo de Infraestructura TI del HUAP, encargado de administrar los respaldos y ejecutar procesos de restauración cuando sea necesario.

b. Documentación de Procesos

i. Se mantendrá documentación básica sobre los procedimientos de restauración, incluyendo:

1. Pasos generales para restaurar desde discos externos, NAS o servidores.
2. Registro de cambios relevantes en el entorno tecnológico que puedan afectar la recuperación.
3. Procedimientos simplificados para recuperación ante contingencias operativas.

c. Duplicación de Respaldos para Recuperación

i. Cuando sea posible, se recomienda realizar una copia duplicada del respaldo antes de iniciar la restauración, especialmente en casos críticos, para preservar la integridad de los datos originales.

d. Pruebas Periódicas de Restauración

i. Se realizarán dos pruebas anuales de restauración completa, que incluirán:

1. Validación de la integridad de los datos restaurados.

2. Registro de resultados y observaciones en informe técnico.
3. Evaluación aproximada de los tiempos de recuperación, en función de los objetivos definidos (RTO y RPO), cuando sea posible.

e. Contratación y Tercerización

i. En caso de que se utilicen servicios externos para respaldo o recuperación, los contratos deberán incluir cláusulas que aseguren:
   1. Cumplimiento de esta política.
   2. Entrega de evidencia de restauraciones realizadas.
   3. Posibilidad de auditoría por parte del HUAP.

f. Mejora Continua

i. Todo incidente o falla detectada durante procesos de recuperación será analizado por el equipo TIC, con el fin de implementar mejoras técnicas y operativas que fortalezcan la eficacia del plan de respaldo.
   Las acciones específicas dependerán del tipo de incidente y serán definidas por el equipo TIC en cada caso.

6. Comprobación de integridad de la información.

a. El equipo de Infraestructura TI del HUAP es responsable de verificar la integridad de los respaldos mediante restauraciones periódicas y revisión de logs generados por las herramientas utilizadas.

b. Se realizan dos pruebas anuales de restauración completa, en entornos controlados, para validar que los respaldos pueden recuperarse correctamente.

c. El software de respaldo (rsync, Cobian Backup, Navicat) está configurado para generar logs automáticos que registran cada evento de respaldo.

d. En caso de respaldos manuales, se utilizan capturas de pantalla y bitácoras como evidencia de ejecución.

e. Cuando se utilizan servicios externos, se solicita evidencia básica de respaldo y restauración, si corresponde.

7. Restauración de la información.

a. Revisiones Periódicas del Estado de Respaldos

i. El equipo de Infraestructura TI realiza revisiones periódicas de los respaldos disponibles, verificando que los archivos críticos estén accesibles y recuperables en caso de necesidad.

b. Plan de Restauración de Información

i. Las restauraciones se ejecutan según procedimientos definidos por el equipo TIC. En cada caso se documentan:
   1. Actividades realizadas.
   2. Fecha de ejecución.
   3. Responsable técnico.
   4. Tipo y criticidad de la información restaurada.

   Los procedimientos específicos serán formalizados por el equipo TIC en documentos técnicos complementarios.

c. Registro de la Tarea de Restauración

i. Cada restauración debe contar con evidencia registrada (log del sistema, captura de pantalla o bitácora manual). En caso de fallas:
   1. Se analiza la causa.
   2. Se repite la restauración si es necesario.
   3. Se documentan las acciones correctivas.

d. Duración del Proceso de Restauración

i. El tiempo de restauración depende de:
   1. La velocidad de red disponible.
   2. El tamaño de los datos.
   3. La herramienta utilizada (rsync, Cobian, Navicat).

e. Cifrado de la Información Respaldada

i. Los respaldos se transfieren mediante protocolos cifrados (rsync sobre SSH). En el caso de medios portables, se evalúa el uso de cifrado según criticidad.

f. Pruebas Periódicas de Restauración

i. Se realizan dos pruebas anuales de restauración en entornos controlados. Las pruebas incluyen:
   1. Selección aleatoria de archivos o carpetas.
   2. Restauración en carpeta segura para evitar sobrescritura.
   3. Validación de integridad y trazabilidad.

g. Autorización para Solicitar Recuperación

i. Solo los responsables de los activos de información pueden solicitar:
   1. Restauración ante pérdida total o parcial.
   2. Pruebas de restauración para validar respaldos.

8. Frecuencia y Tipo de respaldo.

a. Equipos asignados a los funcionarios: Cada funcionario es responsable de respaldar la información contenida en su equipo computacional asignado, especialmente cuando se trata de archivos sensibles o institucionales. Este respaldo debe realizarse localmente, utilizando medios disponibles como carpetas organizadas o según sus propias necesidades.

El equipo TIC no interviene en este proceso, pero puede entregar orientación general si se solicita formalmente.

La periodicidad del respaldo dependerá de la organización personal del funcionario, la criticidad de la información que maneja y sus necesidades operativas.

b. Sistemas y bases de datos: El equipo de Infraestructura TI mantiene respaldos automáticos de los sistemas institucionales según el siguiente esquema:

i. Ambiente producción.
   1. Servicios críticos: respaldo incremental y full diario.

2. Máquinas virtuales (Proxmox): respaldo completo diario y se mantienen copias semanales en NAS.
3. Retención: rotación automática según espacio disponible (1 copia semanal). No se aplican retenciones prolongadas.

ii. Ambiente de pruebas (QA).

1. Actualización completa mensual.
2. Retención: solo se conserva el respaldo más reciente.

iii. Ambiente Desarrollo.

1. Respaldo completo diario
2. Retención mínima: solo respaldo más reciente.

c. Definición de estándares: El equipo TIC define los tipos de respaldo institucionales considerando:

i. Frecuencia de ejecución.
ii. Medio de almacenamiento (NAS, disco externo, servidor remoto).
iii. Tipo de contenido.
iv. Tiempo de retención.
v. Procedimiento de eliminación.

Las solicitudes de respaldo fuera del ciclo habitual deben ser coordinadas directamente con el equipo TIC.

9. Protección de la información en medios de respaldo.

a. La información crítica del HUAP se respalda siguiendo un modelo adaptado del enfoque 3-2-1, considerando las capacidades actuales del hospital. Esto implica:

i. Dos copias de seguridad: una local y una en servidor remoto (NAS).
ii. Diversidad de medios: se utilizan discos internos, NAS y discos externos según disponibilidad.
iii. Respaldo fuera del sitio: se mantiene una copia en red remota (nodo distinto al de producción), lo que permite recuperación ante fallos locales.

Cuando sea posible, se evaluará la incorporación de copias inmutables o almacenamiento offline para fortalecer la resiliencia ante ciber incidentes.

Toda información respaldada fuera del hospital debe ser trasladada con medidas de seguridad adecuadas, como cifrado en tránsito (rsync sobre SSH) y control de acceso físico.

El equipo TIC mantiene un inventario actualizado de los respaldos externos, incluyendo ubicación, fecha y tipo de contenido, para facilitar auditorías y recuperación.

10. Protección de la información en discos duros externos.

a. Cuando se utilicen discos duros externos para almacenar respaldos, se deberán aplicar medidas básicas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información institucional.

   i. Los discos deben estar rotulados claramente con nombre del respaldo, fecha y tipo de copia.
   ii. Deben ser almacenados en un lugar seguro dentro del hospital, bajo supervisión del equipo TIC.
   iii. Se recomienda mantener una copia duplicada (clone) para respaldos críticos, especialmente si se trasladan fuera del sitio.
   iv. El traslado de discos debe realizarse por personal autorizado, evitando intervenciones no registradas.
   v. Se debe verificar periódicamente el estado físico de los discos y la capacidad de recuperación de los datos almacenados.
   vi. En caso de falla, se debe restaurar desde la copia duplicada o desde el respaldo remoto disponible.
   vii. Se recomienda aplicar cifrado en medios portables cuando se trate de información sensible o crítica.

   El equipo TIC mantendrá un registro básico de uso y estado de los discos externos, incluyendo altas, bajas y ubicación actual.

11. Vigencia, revisión y retención de los respaldos.

a. Los respaldos serán gestionados conforme a los tiempos de retención definidos por el equipo TIC, considerando la criticidad de la información —definida en conjunto con las unidades responsables de cada sistema—, la capacidad de almacenamiento disponible y los requisitos operativos y normativos aplicables.

b. Una vez cumplido el período de retención, los respaldos serán eliminados de forma segura, asegurando la confidencialidad de los datos mediante procedimientos definidos por el equipo TIC (por ejemplo, sobreescritura, eliminación manual o destrucción física del medio).

c. La política de respaldo será revisada anualmente o cuando ocurran cambios significativos en la infraestructura tecnológica, normativa vigente o procesos institucionales, con el fin de mantener su vigencia y aplicabilidad.

12. Respaldo de estaciones de trabajo.

a. Cada funcionario es responsable de respaldar la información contenida en su equipo computacional asignado, especialmente cuando se trata de archivos sensibles o institucionales. Este respaldo debe realizarse localmente, utilizando medios disponibles según sus propias necesidades. El equipo TIC no interviene en este proceso.

b. En casos excepcionales, como auditorías o cambios de equipo, la jefatura podrá coordinar directamente con TIC la ejecución de un respaldo, dejando evidencia registrada si corresponde.

c. El equipo TIC evaluará la solicitud y, si procede, coordinará la ejecución del respaldo, ya sea mediante herramientas automáticas (como Cobian Backup) o procedimientos manuales, dejando evidencia registrada.

13. Borrado de la información.

a. La información contenida en los servidores centrales del HUAP, que ya no sea necesaria, será eliminada conforme a los criterios

definidos por el equipo TIC, priorizando la liberación de espacio y la protección de datos sensibles.

En el caso de información clínica o datos de pacientes, la eliminación deberá regirse por la normativa vigente en materia de protección de datos, y será responsabilidad del proveedor del sistema correspondiente, según el tipo de sistema utilizado.

b. Los respaldos almacenados en discos externos que hayan cumplido su período de retención o que ya no sean requeridos deberán ser eliminados manualmente por el equipo TIC, asegurando que no queden accesibles ni recuperables por terceros.

c. Todo equipo computacional o medio de almacenamiento que sea dado de baja deberá ser revisado por el equipo TIC para verificar que la información ha sido eliminada. En caso de medios físicos (discos duros, CD/DVD), se aplicarán métodos de sobrescritura o destrucción física, según disponibilidad.

d. La eliminación de información se realizará de forma que impida el acceso no autorizado, siguiendo prácticas básicas de seguridad. En caso de contar con procedimientos formales de eliminación segura, estos serán aplicados.

VII. MECANISMO DE DIFUSIÓN.

La presente política será comunicada de manera que su contenido sea accesible y comprensible para todos los funcionarios, honorarios y terceros que utilizan sistemas institucionales.

Al menos se difundirá mediante correo electrónico informativo a todas las unidades del hospital.

VIII. PERÍODO DE REVISIÓN.

La política será revisada anualmente o cuando ocurran cambios significativos en:

- Infraestructura tecnológica.
- Normativa legal o regulatoria.
- Procesos institucionales relacionados con respaldo y recuperación.

El equipo TIC y el Encargado/a de Ciberseguridad coordinarán la revisión a través de reuniones con las unidades afectadas, recopilación de observaciones y elaboración de un informe con los ajustes propuestos.

El informe con los ajustes propuestos será presentado al Comité de Ciberseguridad para su validación y, de ser necesario, a las instancias correspondientes para su aprobación.

IX. EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

En situaciones excepcionales, el Jefe/a TIC, el Encargado/a de Ciberseguridad o el Comité de Ciberseguridad podrán autorizar excepciones a esta política, siempre que:

I. No se infrinja la legislación vigente.
II. No se comprometa la seguridad de la información institucional.

Toda excepción deberá ser documentada formalmente y podrá dar lugar a una revisión parcial de la política, si se considera necesario.

X. DISTRIBUCIÓN:

- Dirección.
- Subdirección Gestión Clínica.
- Subdirección Administrativa.
- Unidad de Calidad y Seguridad del Paciente.
- Unidad de Tecnología de la Información
- Unidad de Auditoría

XI. REFERENCIAS BIBLIOGRÁFICAS:

- International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022. Sistemas de gestión de seguridad de la información. Ginebra: ISO/IEC.

- International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27002:2022. Controles de seguridad de la información. Ginebra: ISO/IEC.
- Chile. (2024). *Ley N° 21.663*: Marco de Ciberseguridad. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile
- Chile. (1999). *Ley N° 19.628*: Sobre protección de la vida privada. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile
- Chile. (2008). *Ley N° 20.285*: Sobre acceso a la información pública. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile
- Chile. (2002). *Ley N° 19.799*: Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile
- Chile. Ministerio de Economía, Fomento y Reconstrucción. (2002). Decreto Supremo N° 181: Reglamento de la Ley N° 19.799 sobre firma electrónica. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile
- Chile. Ministerio Secretaría General de la Presidencia. (2005). Decreto Supremo N° 83: Norma técnica sobre seguridad de documentos electrónicos. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile
- Chile. Ministerio Secretaría General de la Presidencia. (2020). Decreto Supremo N° 7: Norma técnica de ciberseguridad, en el marco de la Ley N° 21.180. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile
- Ministerio de Salud de Chile. (s. f.). Orientaciones técnicas sobre respaldo y continuidad operativa. Santiago de Chile: MINSAL.

XII. MODIFICACIONES DEL DOCUMENTO:

SÍNTESIS DE MODIFICACIONES			RESPONSABLE MODIFICACIÓN	APROBADO POR DIRECTOR
VERSIÓN	FECHA	CAUSA DE MODIFICACIÓN		
01	09/2025	Creación del Documento	Enzo Mayo Gonzalez Encargado Ciberseguridad	Dr. Patricio Barría A.

Elaborado por:

1. Enzo Mayo G., Encargado de Ciberseguridad y Seguridad de la Información

Revisado por:

1. Susana Avendaño D., Jefa Unidad de Tecnologías de la Información
2. TM. Camila Benítez Ugarte, Profesional Unidad de Calidad y Seguridad del Paciente
3. Christian Echeverría A, Subdirector Administrativo y Financiero

Firmado por:
Camila Andrea Benítez Ugarte
Profesional Unidad Calidad y Seguridad del Paciente
Fecha: 25-09-2025 09:21 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Firmado por:
Susana Ximena Avendaño Durán
Jefatura Tic
Fecha: 26-09-2025 11:41 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Firmado por:
Christian Irving Echeverría Aburto
Subdirector Gestión Administrativa y Financiera
Fecha: 26-09-2025 15:10 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

II. TÉNGASE PRESENTE la vigencia de esta política a contar de la fecha de la total tramitación de la presente Resolución.

III. ESTABLÉCESE que la señalada *"Política de respaldo de información y software"*, debe ser el que se tenga en consideración a contar de la fecha de su entrada en vigencia.

IV. DÉJESE SIN EFECTO toda normativa interna que diga relación con la materia de esta política.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

FIRMA ELECTRÓNICA AVANZADA · GOBIERNO DE CHILE

Firmado por:
Patricio Raúl Barría Ailef
Director Huap
Fecha: 06-11-2025 17:03 CLT
Hospital de Urgencia Asistencia
Pública Dr. Alejandro del Río

CEWSP
Distribución:

1. Dirección.
2. Subdirección de Gestión Clínica.
3. Subdirección de Gestión del Cuidado.
4. Subdirección de Gestión y Desarrollo de las Personas.
5. Departamento de Planificación y Desarrollo.
6. Unidad de Calidad y Seguridad del Paciente.
7. Unidad de Auditoría.
8. Asesoría Jurídica.
9. Oficina de Partes.

XASV