Complejo Asistencial Barros Luco
Servicio de Salud Metropolitano Sur
Ministerio de Salud

DIRECCION
SSG/CGS/CMM

CALIDAD EN LOS PROCESOS DE ATENCION EN SALUD
ACREDITADO
Acreditación certificada por SUPERINTENDENCIA DE SALUD

RESOLUCION EXENTA Nº 4876

SANTIAGO 18 DIC 2025

VISTOS:

Las facultades concedidas por los artículos 35 y 36 del DFL N° 1, de 2005, del Ministerio de Salud, que fijó el texto refundido, coordinado y sistematizado del Decreto Ley N° 2.763, de 1979 y de las leyes N°18.933 y N° 18.469; el Decreto de Salud N°38, de 2005, Reglamento Orgánico de los Establecimientos de Salud de Menor complejidad y de los Establecimientos de Autogestión en Red; la ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; en el Decreto Supremo Nº 83, del Ministerio Secretaría General de la Presidencia, de 2004, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; en el Decreto Nº 14 de 2014 del Ministerio de Economía, Fomento y Turismo que modifica Decreto Nº 181, de 2002, que aprueba reglamento de la ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica; ley 21.459 Establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest; en el Decreto Nº 83 de 28 de agosto de 2017, del Ministerio de Relaciones Exteriores que promulga Convenio sobre la Ciberdelincuencia; en la norma chilena NCh-ISO 27001: 2022; en el Instructivo Presidencial N°8 de 2018 que imparte instrucciones urgentes en materia de ciberseguridad; El Decreto N° 7, del 19 de mayo de 2023, del Ministerio Secretaría General de la Presidencia, que establece Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N° 21.180; El Decreto N° 164, del 16 de junio de 2023, del Ministerio del Interior y Seguridad Pública, que aprueba la Política Nacional de Ciberseguridad 2023 – 2028; La Ley N° 21.663, Marco de Ciberseguridad ; Resolución Exenta Numero RA 446/9/2024 de 09 de febrero de 2024 del Servicio de Salud Metropolitano Sur sobre nombramiento en el cargo de director del Hospital Barros Luco Trudeau; La Resolución N°36 de 19 de diciembre de 2024, de Contraloría General de la República, sobre exención del trámite de toma de razón;

CONSIDERANDO

Que, conforme dispone el artículo 11° del decreto 7, establece norma técnica de seguridad de la información y ciberseguridad conforme la ley nº 21.180, 2023, del Ministerio Secretaría General de la Presidencia, los órganos de la Administración del Estado deberán desarrollar e implementar los procesos y acciones necesarios para mantener los planes de recuperación; Que, en mérito de lo antes mencionado, y en cumplimiento a los principios de escrituración, transparencia, eficiencia y eficacia en la administración pública, dicto la siguiente:

RESOLUCION

1.- DÉJESE SIN EFECTO la resolución N°861 del 5 de abril 2021, de la dirección del Hospital que aprueba el documento "Política de seguridad: continuidad operacional";

2.- APRUÉBESE el documento denominado "Política de seguridad continuidad operacional", Código DGTI 09, Versión 03, que rige desde la fecha de la presente resolución exenta, cuyo texto es del siguiente tenor:

POLÍTICA DE SEGURIDAD: CONTINUIDAD OPERACIONAL

	Nombre	Cargo	Firma
Realizado por:	Mijail Muñoz Valenzuela	Encargado de Seguridad de la Información y Ciberseguridad	
Revisado por:	Carolina Muñoz Valenzuela	Jefa de Unidad de Calidad y Seguridad del Paciente	
	Osvaldo Augusto De La Barra Ugalde	Jefe Departamento Control de Gestión	
	Francisco Epul Huilipan	Jefe Departamento Gestión Financiera y Contable	
	Diego Nuñez Apablaza	Jefe de Comunicaciones y Relaciones Públicas	
Aprobado por:	Walter Keupuchur Meza	Director Hospital Barros Luco Trudeau	

INDICE

OBJETIVO

Establecer los lineamientos estratégicos, operativos y de seguridad para garantizar la continuidad de los procesos clínicos, administrativos y tecnológicos del Hospital Barros Luco Trudeau durante eventos disruptivos, incluyendo la protección de la información y preparación de las TIC.

ALCANCE

Aplica a todos los sistemas de información, infraestructura TIC, servicios informáticos críticos, información confidencial.

RESPONSABLES

Departamento de Gestión de Tecnologías de la Información: Es responsable de elaborar, mantener y ejecutar el Plan de Recuperación ante Desastres (DRP), gestionar respaldos, restauraciones, redundancias y coordinar acciones con proveedores tecnológicos críticos.

Encargado de Seguridad de la Información: Es responsable de supervisar el cumplimiento de los controles de seguridad definidos en el DRP, gestionar incidentes de seguridad durante eventos disruptivos y mantener actualizada la documentación de incidentes y mitigaciones.

Proveedores Tecnológicos Críticos: Son responsables de cumplir los acuerdos de nivel de servicio (SLA) establecidos, asegurar la continuidad de sus servicios tecnológicos clave y colaborar activamente en la recuperación ante incidentes o simulacros cuando se requiera.

Jefes de servicios/departamentos/unidades: Son responsables de elaborar, aplicar y mantener procedimientos específicos de continuidad, para asegurar que la interrupción de los sistemas no afecte procesos críticos, y se implementen rutas o mecanismos manuales.

DEFINICIONES

BIA (Análisis de Impacto en el Negocio): Proceso sistemático para identificar y evaluar los efectos potenciales de una interrupción en las operaciones críticas de un negocio.

Eventos Disruptivos: Situaciones imprevistas como fallas técnicas graves, ataques cibernéticos, incendios, cortes de energía o desastres naturales que interrumpen el funcionamiento normal de la infraestructura tecnológica.

Infraestructura Crítica TI: Equipos, redes, sistemas y aplicaciones indispensables para la operación tecnológica.

Plan de Recuperación ante Desastres (DRP): Documento con medidas técnicas que permiten restaurar rápidamente los sistemas y servicios tecnológicos críticos después de una interrupción grave.

Proveedores Tecnológicos Críticos: Empresas externas que suministran o administran servicios tecnológicos clave para la operación (por ejemplo, conectividad, soporte de sistemas, almacenamiento en la nube).

Redundancia Tecnológica: Disponibilidad de sistemas, equipos o enlaces de respaldo que aseguran la continuidad de servicios si ocurre una falla.

Resiliencia Tecnológica: Capacidad de la infraestructura TI (servidores, redes, almacenamiento) para resistir, adaptarse y recuperarse ante fallas, ataques o eventos disruptivos.

Respaldo de Información (Backup): Copia de seguridad programada de datos críticos, almacenada en medios físicos o virtuales para garantizar su recuperación.

Restauración de Datos: Proceso de recuperar y poner en funcionamiento información respaldada para devolverla a su estado operativo después de una pérdida o daño.

RPO (Punto Objetivo de Recuperación): Cantidad máxima de datos que se pueden perder sin causar un impacto crítico, determinada por la frecuencia de los respaldos.

RTO (Tiempo Objetivo de Recuperación): Tiempo máximo permitido para restablecer un sistema o servicio tecnológico después de una interrupción.

Servicios tecnológicos: Hace referencia a servidores, redes de datos y comunicaciones, almacenamientos.

Simulacro DRP: Prueba planificada para verificar la efectividad de los procedimientos de recuperación de sistemas y servicios tecnológicos.

DESARROLLO

1. Principios generales

1.1. Disponibilidad de sistemas críticos

Garantizar que la interrupción de los servicios tecnológicos tenga el menor impacto posible en los procesos esenciales, manteniendo acceso a los sistemas prioritarios mediante mecanismos de respaldo, redundancia y recuperación.

1.2. Protección de la información

Asegurar la confidencialidad, integridad y disponibilidad de la información institucional durante eventos disruptivos, mediante controles temporales, respaldos actualizados y medidas de acceso de emergencia.

1.3. Resiliencia de la infraestructura tecnológica

Diseñar y mantener plataformas, redes, servidores y aplicaciones preparados para resistir, soportar y recuperarse ante incidentes, ataques o fallas graves.

1.4. Obligación conjunta

Cada unidad organizacional es responsable de elaborar, aplicar y mantener procedimientos de continuidad, alineados con el marco institucional. La coordinación y compromiso deben abarcar todos los niveles, desde operativos hasta directivos.

Asegurar que la interrupción de servicios no comprometa la atención clínica esencial. Para ello, se deberán establecer rutas clínicas y administrativas alternativas, priorizar los procesos críticos y habilitar mecanismos manuales o de contingencia validados ante caídas tecnológicas.

2. Lineamientos Generales

- Restaurar los sistemas y servicios tecnológicos críticos dentro de los tiempos definidos para minimizar el impacto operativo.
- Proteger los datos institucionales durante interrupciones, evitando pérdida, alteración o filtración de información.

- Reducir la pérdida de datos no respaldados (RPO) mediante políticas de respaldo y verificación de restauración.
- Asegurar redundancia de infraestructuras clave como servidores, redes y almacenamiento.
- Coordinar acciones con proveedores externos para que sus servicios tecnológicos críticos contemplen planes de recuperación compatibles con el DRP del hospital.

3. Lineamientos específicos

3.1. Plan de Recuperación ante Desastres (DRP)

El hospital deberá documentar, mantener y actualizar su DRP, definiendo sistemas prioritarios, tiempos de recuperación (RTO), puntos de recuperación de datos (RPO) y responsables asignados.

3.2. Respaldo y restauración de datos

Se deberán establecer mecanismos de respaldo, almacenamiento seguro de copias de seguridad y pruebas periódicas de restauración para garantizar su disponibilidad.

3.3. Infraestructura tecnológica resiliente

Los sistemas críticos deberán contar con componentes redundantes (servidores, enlaces de red, almacenamiento) para asegurar la continuidad tecnológica ante fallas o ataques.

3.4. Simulacros y pruebas del DRP

Se deberá realizar al menos una prueba anual del Plan de Recuperación ante Desastres (DRP), simulando interrupciones tecnológicas para comprobar su efectividad. Estas pruebas se ejecutarán de forma parcializada, evitando realizar una interrupción general de todos los sistemas al mismo tiempo. Para su ejecución, se deberá coordinar con la Dirección del HBLT y contar con la autorización del Director, considerando que los tiempos de recuperación (RTO) y los puntos de recuperación (RPO) podrían afectar el funcionamiento normal del hospital.

3.5. Evaluación de riesgos tecnológicos

Anualmente se deberá actualizar el análisis de impacto a los sistemas (BIA tecnológico) y la matriz de riesgos, priorizando plataformas críticas y definiendo tolerancia a interrupciones. Con esto se actualiza el documento del DRP.

3.6. Gestión de incidentes y excepciones

Si ocurre una falla o se necesita aplicar un control de forma diferente a lo establecido, esta situación debe anotarse, revisarse y resolverse con medidas de apoyo, las cuales deberán subsanar el incidente y/o las excepciones, en base a los criterios de expertos (personal técnico y profesional) del DGTI, y debe contar con la revisión del encargado de seguridad de la información y de Ciberseguridad, y aprobación del jefe del Departamento de Gestión en Tecnologías de la Información (DGTI).

SANCIONES

El incumplimiento de las disposiciones establecidas en esta Política de Seguridad de Respaldo de la Información se considerará una infracción a las obligaciones de las funcionarias y funcionarios del Hospital Barros Luco Trudeau.

Las acciones u omisiones que contravengan esta política podrán dar lugar a responsabilidad administrativa, de acuerdo con lo dispuesto en la Ley N°18.834, sobre Estatuto Administrativo o la normativa de personal que resulte aplicable al infractor.

Dependiendo de la gravedad de la infracción, la afectación a la seguridad de la información, la reincidencia y el dolo o culpa con que se haya actuado, las medidas disciplinarias aplicables serán aquellas establecidas en el Estatuto Administrativo, que incluyen, entre otras:

- **Censura:** Reprensión por escrito que se anota en la hoja de vida del funcionario.
- **Multa:** Descuento de un porcentaje de la remuneración mensual.
- **Suspensión del empleo:** Privación temporal del ejercicio del cargo, con goce de parcial de remuneraciones.
- **Destitución:** Término de la relación laboral, por faltas graves a la probidad.

Adicionalmente, sin perjuicio de las responsabilidades administrativas, el incumplimiento grave de esta política, especialmente si involucra el acceso, divulgación o uso no autorizado de datos sensibles (como la ficha clínica), podría acarrear responsabilidad civil o penal, según lo establecido en la Ley N°19.628 sobre Protección de la Vida Privada y el Código Penal, así como otras leyes especiales que sancionen delitos informáticos o la vulneración de la confidencialidad de la información de salud.

Para el personal externo (proveedores y terceros autorizados), el incumplimiento de esta política dará lugar a las sanciones contractuales estipuladas en los contratos o convenios respectivos, sin perjuicio de las acciones legales que el Hospital pueda ejercer por los daños y perjuicios ocasionados.

DIRECCION

3.- DÉJESE ESTABLECIDO que, el documento antes aprobado, por razones de continuidad y buen servicio, inicio su vigencia desde la fecha de la presente resolución exenta.

4.- DÉJESE ESTABLECIDO que, cualquier modificación a la presente Resolución Exenta, deberá ser ratificada por el correspondiente acto administrativo.

ANÓTESE, REGISTRESE Y PUBLIQUESE

SERVICIO DE SALUD M. SUR * DIRECTOR * HOSPITAL BARROS LUCO TRUDEAU

WALTER KEUPUCHUR MEZA
DIRECTOR
HOSPITAL BARROS LUCO TRUDEAU

JENNY CANCINO QUIROZ
MINISTRA DE FE - HBLT

Distribución:
Dirección HBLT
Subdirección Administrativa
Subdirección Gestión Clínica
Subdirección Gestión y Desarrollo de las Personas
Subdirección Médica Atención Cerrada
Subdirección Médica Área Quirúrgica
Subdirección Médica Atención Abierta
Subdirección Gestión de Usuarios
Subdirección Unidades de Apoyo
Enfermera Coordinadora de Atención Cerrada
Enfermera Coordinadora de Atención Abierta
Depto. De Atención a las Personas
DGTI
Oficina de Partes

MINISTRO DE FE