



DIRECCION

STG/CGS/CMM



RESOLUCION EXENTA N° 4272

SANTIAGO

30 OCT 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 N° 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 N° 14 de 2014 que modifica Decreto N° 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 21459 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 N° 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 que imparte instrucciones urgentes en materia 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

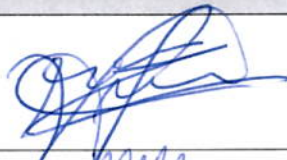







Que, conforme dispone el numeral 8) del decreto 7, establece norma técnica de seguridad de la información y ciberseguridad conforme la ley n° 21.180, 2023, del Ministerio Secretaría General de la Presidencia, es necesario establecer un proceso para resguardar la confidencialidad, integridad y disponibilidad de la información, así como proteger la infraestructura informática de las plataformas electrónicas que sustentan sus procedimientos administrativos, reforzando el cumplimiento de los principios establecidos en el artículo 16 bis nuevo de la ley N° 19.880; 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.- **APRUEBESE** el documento denominado "Procedimiento de Seguridad Control de Cambios", Código DGTI 15, Versión 01, que rige desde la fecha de la presente resolución exenta, cuyo texto es del siguiente tenor:

 <p>Hospital Barros Luco Trudeau</p>	CODIGO: DGTI 15		Vigencia: 5 años
	Procedimiento de Seguridad: Control de Cambios		Fecha de Aprobación: Octubre de 2025
	Versión: 1	1 de 8	Fecha término de Vigencia: Octubre de 2030
			DGTI

PROCEDIMIENTO DE SEGURIDAD: CONTROL DE CAMBIOS


	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	
	Claudio Gómez Silva	Asesor Jurídico	
	Osvaldo Augusto De La Barra Ugalde	Jefe Departamento Control de Gestión	
	Francisco Epul Huilipan	Jefe Departamento Gestión Financiera y Contable	
	Fabiola Fuentes Carreño	Jefa del Depto. de Gestión de las Personas	
	Diego Nuñez Apablaza	Jefe de Comunicaciones y Relaciones Públicas	
Aprobado por:	Walter Keupuchur Meza	Director HBLT	



 Hospital Barros Luco Trudeau	CODIGO: DGTI 15		Vigencia: 5 años
	Procedimiento de Seguridad: Control de Cambios		Fecha de Aprobación: Octubre de 2025 Fecha término de Vigencia: Octubre de 2030
	Versión: 1	2 de 8	DGTI

INDICE

OBJETIVO	3
ALCANCE	3
RESPONSABLES	3
DEFINICIONES	4
DESARROLLO	5
Cambios en Sistemas de Desarrollo propio	5
Cambios en Infraestructura Hardware, software básicos y Comunicaciones	6
Gestión de cambios por parte de proveedores.....	7
Cambios de emergencia	7
SANCIONES	7

 Hospital Barros Luco Trudeau	CODIGO: DGTI 15		Vigencia: 5 años
	Procedimiento de Seguridad: Control de Cambios		Fecha de Aprobación: Octubre de 2025
	Versión: 1		3 de 8
			Fecha término de Vigencia: Octubre de 2030
			DGTI

OBJETIVO

Establecer un procedimiento que permita gestionar de forma segura, eficiente y trazable todos los cambios realizados en los sistemas de información, equipamiento y plataformas tecnológicas del hospital, sin afectar la atención a los pacientes ni la disponibilidad de los recursos informáticos.

ALCANCE

- Sistemas de información internos.
- Sistemas y plataformas provistas por proveedores.
- Equipamiento computacional de usuarios finales.
- Infraestructura tecnológica (servidores, redes, almacenamiento).
- Ambientes de desarrollo, prueba y producción.

RESPONSABLES

- **Departamento de Gestión en Tecnologías de la Información (DGTI)**, es responsable de evaluar, aprobar e implementar los cambios con base en criterios técnicos y de seguridad, garantizando la trazabilidad, integridad y disponibilidad de los sistemas.
- **Encargado de Seguridad de la Información y Ciberseguridad**, participa en la evaluación de riesgos cuando los cambios involucran datos sensibles, sistemas críticos o conectividad con plataformas de terceros, asegurando el cumplimiento de los principios de seguridad de la información.
- **Requirentes**, informan necesidades funcionales o fallas que requieran cambios, y colaboran en la validación funcional posterior a la implementación cuando sea necesario para asegurar que los resultados cumplan con los requerimientos operativos.
- **Proveedores de sistemas y servicios**, deben colaborar con el DGTI en la planificación, ejecución segura y documentación de los cambios que afecten plataformas contratadas o sistemas interoperables, cumpliendo los mismos estándares de trazabilidad, disponibilidad y seguridad exigidos internamente, según Política de seguridad desarrollo, mantención y adquisición de sistemas de información, año 2024, Hospital Barros Luco Trudeau, código DGTI 13, versión 2, resolución exenta 1545. Son responsables de la Gestión de Cambio de sus sistemas y servicios.

RELACIONADO

Política de seguridad Control de Cambios, año 2021, Hospital Barros Luco Trudeau, código 10, versión 1, resolución exenta 862.

 Hospital Barros Luco Trudeau	CODIGO: DGTI 15		Vigencia: 5 años
	Procedimiento de Seguridad: Control de Cambios		Fecha de Aprobación: Octubre de 2025 Fecha término de Vigencia: Octubre de 2030
	Versión: 1	4 de 8	DGTI

DEFINICIONES

- **Criticidad:** Grado de importancia de un cambio o situación que puede afectar la operación.
- **Continuidad operativa:** Capacidad de mantener funcionando los servicios sin interrupciones, incluso frente a fallas o incidentes.
- **Indisponibilidad:** Estado en el que un sistema o servicio no está accesible o no funciona, afectando su uso normal.
- **Levantamiento detallado:** Proceso de recopilar y describir claramente los requerimientos o necesidades que se deben implementar o cambiar en un sistema.
- **Gestión de requerimientos:** Organización y control de las necesidades solicitadas por los usuarios respecto a los sistemas, para asegurar que se comprendan, planifiquen y ejecuten correctamente.
- **Compatibilidad:** Capacidad de un sistema para funcionar correctamente junto con otros sistemas, sin generar errores o conflictos.
- **Entorno de QA (Calidad de software):** Ambiente controlado de pruebas que permite verificar si un sistema, o cambio, funciona bien antes de su uso real en producción.
- **Preproducción:** Entorno o espacio de prueba donde se revisa un sistema antes de usarlo en la operación real. Es como un simulador que se parece lo más posible a la versión final.
- **Producción:** Ambiente o sistema real que utilizan los usuarios en su trabajo diario.
- **Rollback (vuelta atrás):** Acción de restaurar un sistema a un estado anterior cuando un cambio falla o genera problemas, utilizando copias de seguridad o configuraciones previas.
- **Configuraciones:** Conjunto de ajustes o parámetros que determinan cómo funciona un sistema, software o dispositivo.
- **Control de versiones:** Método para registrar, administrar y recuperar cambios realizados en programas, documentos o configuraciones.
- **Trazabilidad:** Capacidad de seguir y verificar el historial, aplicación y modificaciones realizadas a un sistema, documento o proceso.
- **Incidentes:** Eventos, problemas o fallas que afectan la operación normal de los sistemas o servicios, pudiendo comprometer su disponibilidad o seguridad.

 Hospital Barros Luco Trudeau	CODIGO: DGTI 15		Vigencia: 5 años
	Procedimiento de Seguridad: Control de Cambios		Fecha de Aprobación: Octubre de 2025
	Versión: 1	5 de 8	Fecha término de Vigencia: Octubre de 2030
			DGTI

DESARROLLO

Principios Generales

Clasificación del Cambio


La criticidad de un cambio se determina en función de su impacto en la continuidad operativa del HBLT, la cantidad de usuarios o servicios afectados, la dependencia de sistemas internos o de terceros, y la disponibilidad requerida 24/7. La clasificación se define como sigue:

- **Crítico:** Aquel que puede afectar directa o indirectamente la operación de servicios esenciales del hospital, incluyendo áreas clínicas (urgencia, hospitalización, etc.), de apoyo (laboratorio, imagenología, etc.), y administrativas (finanzas, abastecimiento, etc.) cuando estos impactan la atención en salud, continuidad de procesos o la gestión de recursos.
- **No Crítico:** Cambio que afecta sistemas o procesos sin impacto directo en la atención, continuidad o seguridad del servicio. Son programables sin urgencia y se pueden ejecutar en cualquier horario, siempre que no generen indisponibilidad significativa.
- **Emergencia:** Aquel que debe ser ejecutado inmediatamente para prevenir o corregir una falla que afecte la disponibilidad, confidencialidad o integridad de sistemas críticos. Puede ser aplicado sin el proceso formal completo, pero debe ser documentado posteriormente y comunicado si el impacto operativo lo requiere.

Cambios en Sistemas de Desarrollo propio

1. Solicitud de Cambio

- Se recibirá la solicitud de cambio por plataforma de ticket del DGTI, enviado un correo a la mesa de soporte, indicando:
 - La solicitud debe indicar nombre del sistema que requiere el cambio.
 - Módulo del sistema que requiere el cambio.
 - Nombre y contacto de la jefatura.
- El equipo de requerimientos realizará un levantamiento detallado del cambio con la/el dueña/o del sistema.
- Una vez aceptado el documento de requerimientos por la/el dueña/o del sistema, éste será subido a la plataforma de Gestión de requerimientos para el equipo de desarrollo.

 Hospital Barros Luco Trudeau	CODIGO: DGTI 15		Vigencia: 5 años Fecha de Aprobación: Octubre de 2025 Fecha término de Vigencia: Octubre de 2030
	Procedimiento de Seguridad: Control de Cambios		
	Versión: 1	6 de 8	DGTI

2. Evaluación Técnica y de Riesgos

- El DGTI deberá revisar el impacto en la disponibilidad, seguridad, continuidad del servicio y compatibilidad con otros sistemas (internos o de terceros).
- El equipo del DGTI deberá definir prioridades y planificar los tiempos de trabajo.

3. Pruebas y Validación

- Se prueban los cambios en entornos de QA (Calidad de software) y en preproducción antes de su implementación en producción.
- Validación en el ambiente de preproducción, en conjunto con el usuario solicitante o jefatura correspondiente.

4. Ejecución del Cambio

- Teniendo los resultados anteriores, se determinará fecha y hora del paso a producción.
- Se mantendrá un monitoreo en tiempo real, revisando la correcta gestión de los datos en la base de datos, realizado por el Administrador de base de datos y supervisado por el líder de Desarrollo.
- Se implementa el plan de Rollback (vuelta atrás) si es necesario.
- Se comunica a usuarios sólo en caso de que el cambio afecte directamente su operación.

5. Post-implementación y Documentación

- Se validan los resultados entre el área de requerimientos y la/el usuaria/o del sistema.
- Se actualizan procedimientos, configuraciones y documentación técnica, si aplica.

6. Control de Versiones

- Con el fin de asegurar la trazabilidad, integridad y recuperación efectiva ante fallas o incidentes, se debe implementar un control de versiones formal.

Cambios en Infraestructura Hardware, software básicos y Comunicaciones

- El DGTI deberá crear un plan para los cambios que involucren la infraestructura, para lo cual deberá realizar la "Clasificación del Cambio", impacto en la disponibilidad, seguridad, continuidad del servicio y compatibilidad con otros sistemas.

 Hospital Barros Luco Trudeau	CODIGO: DGTI 15		Vigencia: 5 años
	Procedimiento de Seguridad: Control de Cambios		Fecha de Aprobación: Octubre de 2025 Fecha término de Vigencia: Octubre de 2030
	Versión: 1	7 de 8	DGTI

- Cuando en la gestión de un cambio participan terceros, éstos deben ser supervisados y coordinados por el área correspondiente del DGTI, esta puede ser Infraestructura (para servidores y centros de datos), redes (para redes de datos y comunicaciones) o soporte técnico (para computadores), quienes validarán el correcto cambio.
- Deberá mantenerse un registro de los cambios realizados en la plataforma de administración de proyectos. El acceso al registro de cambios lo podrá realizar el personal del área de desarrollo, requerimientos, QA y la jefatura del DGTI.
- Se actualizan procedimientos y documentación técnica, si aplica.

Gestión de cambios por parte de proveedores

El proveedor de servicios y/o sistemas de información, será responsable de realizar la Gestión de Cambios de sus sistemas e infraestructura.

- Según numeral 10. Gestión de Cambios, Anexo de Seguridad de la Información para Sistemas de información, Política de seguridad desarrollo, mantención y adquisición de sistemas de información, año 2024, Hospital Barros Luco Trudeau, código DGTI 13, versión 2, resolución exenta 1545.
- Según numeral 11. Base de Datos de la Gestión de Configuración (CMDB), Anexo de Seguridad de la Información para Sistemas de información, Política de seguridad desarrollo, mantención y adquisición de sistemas de información, año 2024, Hospital Barros Luco Trudeau, código DGTI 13, versión 2, resolución exenta 1545.

Cambios de emergencia

Los cambios de emergencia deben ser gestionados dentro del presente procedimiento, mediante un flujo simplificado que permita su ejecución inmediata cuando sea necesario. Posterior a su aplicación, se debe registrar toda la información asociada al cambio y someterla a revisión y validación por parte del 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

 Hospital Barros Luco Trudeau	CODIGO: DGTI 15		Vigencia: 5 años
	Procedimiento de Seguridad: Control de Cambios		Fecha de Aprobación: Octubre de 2025 Fecha término de Vigencia: Octubre de 2030
	Versión: 1	8 de 8	DGTI

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



2.- 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.

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

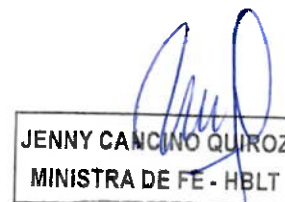
ANÓTESE, REGISTRESE Y PUBLIQUESE



WALTER KEUPUCHUR MEZA
DIRECTOR
HOSPITAL BARROS LUCO TRUDEAU

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