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

DIRECCIÓN
STG/CGS/CMM

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

RESOLUCION EXENTA Nº 3391

SANTIAGO 03 SEP 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 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 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 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 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 artículo 1° de la ley 21663, ley marco de ciberseguridad, 2024, del Ministerio del Interior y Seguridad Publica, establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; 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° 860 del 5 de abril 2021, de la dirección del Hospital que aprueba el documento "Política de seguridad respuesta ante incidentes";

2.- APRUÉBESE el documento denominado "Política de seguridad respuesta ante incidentes de Ciberseguridad", Código DGTI 08, Versión 03, que rige desde la fecha de la presente resolución exenta, cuyo texto es del siguiente tenor:

POLÍTICA DE SEGURIDAD: RESPUESTA ANTE INCIDENTES DE CIBERSEGURIDAD

	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 Gomez Silva	Asesor Jurídico	
	Diego Nuñez Apablaza	Jefe de Comunicaciones y Relaciones Públicas	
	Osvaldo Augusto De La Barra Ugalde	Jefe Departamento Control de Gestión	
	Francisco Epul Huilipan	Jefe Departamento Gestión Financiera y Contable	
Aprobado por:	Walter Fabian Keupuchur Meza	Director Hospital Barros Luco Trudeau	

INDICE

OBJETIVO

Establecer la Política de Seguridad Respuesta ante Incidentes, para asegurar el proceso de manejo de acciones correctivas y acciones preventivas para la gestión de Seguridad de la Información.

ALCANCE

Toda la institución de modo que cualquiera pueda notificar un incidente de seguridad al DGTI, para que éste tome las medidas correctivas y preventivas.

RESPONSABLES

Departamento de Gestión de Tecnologías de la Información: Es el responsable de solucionar incidentes de seguridad y normalizar la entrega de los servicios.

Jefe de Departamento de gestión de Tecnologías de la Información: Es el responsable de Gestionar los procedimientos necesarios para que el departamento de gestión de Tecnologías de la información pueda solucionar los incidentes de seguridad, aprobar manuales y procedimientos de atención de mesa de ayuda.

Encargado de seguridad de la Información: Velar por la creación y cumplimiento de las políticas de seguridad de la institución atendiendo la normativa vigente.

Funcionarios del Hospital Barros Luco Trudeau: Es el personal de la institución al cual está sujeto al cumplimiento de las políticas descritas en este documento.

Personal Externo al Hospital Barros Luco Trudeau: Es el personal, que realiza funciones en el Hospital Barros Luco Trudeau, perteneciente a empresas externas o sin vinculación a éste.

PROCEDIMIENTO

- Procedimiento de Respuesta ante Incidentes de Ciberseguridad para usuarias/os.
- Procedimiento de Respuesta técnica ante Incidentes de Ciberseguridad (DGTI).

DEFINICIONES

Confidencialidad: Solo las personas autorizadas pueden acceder a la información.

Integridad: Los datos deben ser precisos y no alterados sin autorización.

Disponibilidad: La información debe estar accesible cuando se necesite.

Resiliencia: Es la capacidad de resistir, responder y recuperarse de ataques o fallos, asegurando la continuidad de las operaciones con el menor impacto posible.

Incidente de ciberseguridad: Todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.

Medidas/acciones:

- **Acciones correctivas:** Esta acción se realiza, como resultado a la detección de un incidente de seguridad, cuya categorización es de importancia significativa.
- **Acciones preventivas:** Esta acción se realiza, como resultado a la detección de una situación que podría llegar a ser un problema de seguridad.

Contención: Acciones inmediatas para detener la propagación de un incidente y limitar su impacto, como bloquear accesos o aislar dispositivos (desconexión de la red de datos).

Erradicación / Aislar: Eliminar o aislar la causa del incidente para evitar nuevos daños, aplicando parches, bloqueos o separación de equipos.

Recuperación: Restaurar sistemas, servicios o datos afectados para reanudar la operación normal de forma segura y con mínimo impacto.

DESARROLLO

Principios Generales

- **Preparación:** Es importante contar con una planificación básica, definir procedimientos claros y capacitar al personal clave para responder de manera efectiva ante incidentes.
- **Detección y análisis:** Se deben implementar mecanismos que permitan identificar incidentes de manera temprana. A través de herramientas automatizadas, reportes de usuarios o monitoreo. El análisis debe centrarse en comprender el impacto y definir la prioridad de la respuesta.
- **Contención, erradicación/aislar y recuperación:** Ante la detección de un incidente, se deben aplicar medidas de contención inmediatas para evitar su

propagación. Es imperativo eliminar o aislar la amenaza, esto puede incluir bloquear accesos, aislar dispositivos afectados o aplicar parches de seguridad, y restaurar los sistemas y servicios afectados, garantizando su operatividad con el menor impacto posible.

- **Documentación y registro:** Todas las acciones y decisiones tomadas durante la gestión del incidente deben ser registradas de manera detallada. Es obligatorio mantener un registro completo para facilitar análisis futuros, auditorías y el cumplimiento de normativas de seguridad.
- **Comunicación:** Se debe informar a todas las partes interesadas, internas y externas, según corresponda. La comunicación debe realizarse de manera estructurada, clara y oportuna, asegurando que la información se maneje de forma segura y responsable, por las vías formales y definidas.
- **Mejora continua:** Después de cada incidente, se deben evaluar las causas y las respuestas implementadas. Es obligatorio actualizar procedimientos, políticas y controles con base en las lecciones aprendidas, con el fin de fortalecer la seguridad y reducir la probabilidad de incidentes futuros.
- **Coordinación:** Se debe colaborar con entidades externas, como autoridades reguladoras y organismos especializados en ciberseguridad, según establezca la ley.

Responsabilidades y Roles

Para garantizar una gestión eficaz de incidentes, se definen los siguientes roles y sus responsabilidades:

- **Usuarios de sistemas, funcionarias/os, personal externo y proveedores:**
  - Reportar cualquier actividad sospechosa o incidente de ciberseguridad.
  - No intentar resolver incidentes por cuenta propia.
  - Seguir los procedimientos de seguridad establecidos.
- **Equipo de Respuesta ante Incidentes:**
  - Analizar y clasificar los incidentes según su impacto y urgencia.
  - Implementar medidas de contención y mitigación de daños.
  - Coordinar con otras áreas para la recuperación y restauración de los sistemas afectados.
  - Dependiendo del nivel del impacto, informar a las autoridades y organismos especializados en ciberseguridad.

- Documentar el incidente y generar informes detallados.

- **Administradores de Sistemas y Seguridad:**
  - Aplicar controles de seguridad y monitorear la infraestructura informática.
  - Implementar medidas correctivas y preventivas en los sistemas afectados.
  - Mantener copias de seguridad de los sistemas críticos y garantizar su disponibilidad en caso de incidentes.
- **Equipo de Comunicaciones:**
  - Es responsable de gestionar la comunicación oficial del incidente, asegurando que la información sea clara, precisa y alineada con la estrategia de la organización.
  - Debe informar a las partes interesadas internas y externas según corresponda.
- **Autoridades:**
  - Garantizar que el "Equipo de Respuesta ante Incidentes de Seguridad" cuente con el apoyo necesario para gestionar el incidente de manera eficiente.
  - Asegurar el cumplimiento de los procedimientos.
  - Comunicar la situación a instancias superiores si es necesario.

Notificación y Comunicación

Se debe realizar una correcta gestión de la comunicación durante y después de un incidente, es fundamental para minimizar riesgos adicionales.

- **Internamente:**
  Se debe informar a las partes involucradas según el nivel de gravedad del incidente y por las vías formales y establecidas por la Dirección.
- **Externamente:**
  - Si el incidente afecta datos de terceros (pacientes, proveedores, etc.), se debe evaluar la forma de notificación conforme a normativas legales.
  - En caso de incidentes críticos, se debe notificar a las autoridades regulatorias y organismos especializados en ciberseguridad.
- **Manejo de crisis y reputación:**
  - La comunicación con los medios será gestionada por el equipo designado y no se podrá divulgar información sin autorización.

- Se deben preparar comunicados oficiales en caso de incidentes de alto impacto.

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.

ANEXOS

CLASIFICACIÓN E IMPACTO DE INCIDENTES DE CIBERSEGURIDAD

CLASIFICACIÓN DE INCIDENTES DE CIBERSEGURIDAD

Los incidentes de ciberseguridad, se pueden clasificar según sus efectos que generan. Estos pueden ser:

- **Uso no autorizado de redes y sistemas informáticos**: Acceso indebido a la infraestructura y sistemas internos, ya sea por robo de credenciales, explotación de vulnerabilidades o cualquier otro método que permita ingresar sin autorización.

- **Phishing o fraude**:

  - **En infraestructura propia:** Envío de correos no deseados, intentos de estafa o la creación de sitios fraudulentos utilizando los propios sistemas de la institución.

  - **Relacionadas con la institución:** Ataques externos que usan la imagen de la institución para engañar a usuarios y obtener información confidencial.

- **Ejecución no autorizada de código**: Instalación o ejecución de software malicioso sin permiso, como inyecciones de código o malware dentro de los sistemas.

- **Robo o filtración de datos:** Exposición o pérdida de información sensible debido a ataques como la interceptación de datos en tránsito o el acceso indebido a bases de datos expuestas.

- **Interrupción o denegación de servicio:** Ataques que bloquean o ralentizan sistemas y servicios esenciales, como aquellos que saturan redes o servidores para dejarlos fuera de funcionamiento.

- **Modificación no autorizada de configuraciones:** Cambios no autorizados en la configuración de sistemas que pueden afectar su rendimiento, seguridad o disponibilidad.

ÁREAS DE IMPACTO DE LOS INCIDENTES DE CIBERSEGURIDAD

Los incidentes pueden agruparse en cuatro grandes áreas según su efecto en la organización:

- **Impacto en el uso legítimo de recursos:** Incidentes que afectan el acceso y correcto uso de redes y sistemas, como accesos no autorizados o ataques de phishing.
- **Impacto en la confidencialidad de la información:** Casos donde datos sensibles quedan expuestos o son robados, afectando la privacidad y seguridad de la información.
- **Impacto en la disponibilidad de servicios:** Situaciones donde los sistemas o servicios dejan de estar operativos total o parcialmente, afectando su correcto funcionamiento.
- **Impacto en la integridad de la información:** Alteraciones no autorizadas en datos, sistemas o configuraciones que pueden comprometer su fiabilidad y precisión.

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 METROPOLITANO SUR ORIENTE
DIRECTOR

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