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

DIRECCION
SMG/CGS/CMM

ABOGADO - SSMM

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

RESOLUCION EXENTA Nº 3392

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.- APRUÉBESE el documento denominado "Procedimiento de Seguridad respuesta técnica ante incidentes de ciberseguridad (DGTI)", Código DGTI 08 B, Versión 01, que rige desde la fecha de la presente resolución exenta, cuyo texto es del siguiente tenor:

PROCEDIMIENTO DE SEGURIDAD: RESPUESTA TÉCNICA ANTE INCIDENTES DE CIBERSEGURIDAD (DGTI)

	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 HBLT	

INDICE

OBJETIVO

Establecer un procedimiento técnico con las acciones iniciales necesarias para la detección, contención, análisis, mitigación, reporte y recuperación ante incidentes de ciberseguridad, asegurando la continuidad operativa, la integridad de los sistemas y la protección de la información.

ALCANCE

- Personal técnico/profesional del Depto. de Gestion en Tecnologías de la Información (DGTI).

RESPONSABLES

- **Departamento de Gestión de Tecnologías de la Información:** Es el responsable de solucionar incidentes de ciberseguridad y normalizar 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.

DESARROLLO

CLASIFICACIÓN DE INCIDENTES

Es fundamental identificar y clasificar los incidentes según su tipo y nivel de impacto para determinar la respuesta adecuada.

Tipos de incidentes

- **Malware y Ransomware:** Infecciones de virus, troyanos o cifrado de datos por ransomware.
- **Phishing y Fraudes Electrónicos:** Suplantación de identidad o intentos de engaño para obtener credenciales.

- **Ataques de Denegación de Servicio (DDoS):** Sobrecarga intencional de servidores o redes.
- **Accesos no Autorizados:** Intrusiones o intentos de acceso indebido a sistemas.
- **Fugas de Información:** Pérdida, filtración o exposición de datos sensibles.
- **Vulnerabilidades Críticas:** Fallas de seguridad que pueden ser explotadas si no se corrigen.

Clasificación por nivel de severidad

- **Bajo:** No afecta operaciones ni datos críticos.
- **Medio:** Puede afectar a algunos usuarios o servicios, pero sin comprometer datos críticos.
- **Alto:** Impacto significativo en los servicios del hospital o en la privacidad de datos sensibles.
- **Crítico:** Compromete la integridad de los sistemas, expone información sensible o afecta la continuidad operativa.

Efectos significativos

Los incidentes de ciberseguridad que se **deben reportar al CSIRT Nacional**, según sus efectos significativos:

- Si se interrumpe la continuidad de un servicio esencial. En dicho caso deberá considerarse, tanto los servicios entregados por proveedores, como la cadena de suministro, de una institución que preste servicios esenciales o de un operador de importancia vital.
- Si afecta la integridad física o la salud de las personas.
- Si afecta la integridad o confidencialidad de activos informáticos, o la disponibilidad de alguna red o sistema informático, aun cuando esto no produzca o hubiere producido afectación inmediata en la provisión del servicio.
- Si se utilizan o ingresan sin autorización a redes o sistemas informáticos, aun cuando esto no produzca o hubiere producido afectación inmediata en la provisión del servicio.
- Si afectan sistemas informáticos que contengan datos personales.

Para determinar la importancia de los efectos de un incidente de ciberseguridad se deberán tener especialmente en consideración el número de personas afectadas; la duración del incidente.

EQUIPO DE RESPUESTA ANTE INCIDENTES (ERI)

Es el responsable de la primera respuesta ante un incidente de seguridad de severidad media, alta o crítica.
El Equipo de Respuesta ante Incidentes (ERI), estará integrado por:

- Encargado de infraestructura tecnológica.
- Encargado de Redes de datos y comunicaciones.
- Encargado de continuidad Operativa.
- Encargado de seguridad de la información y ciberseguridad.
- Personal técnico/profesional de informática a quien se le deleguen actividades y/o funciones para estos efectos.

DETECCIÓN Y REGISTRO

- Identificación de un posible incidente mediante herramientas de monitoreo, alertas o reportes de usuarios.
- **Registro inmediato** en una base de datos o sistema de gestión de incidentes, con detalles como:
  - Fecha y hora del incidente.
  - Usuario o sistema afectado.
  - Tipo de incidente detectado.
  - Evidencia inicial.

ANÁLISIS Y CLASIFICACIÓN

El Equipo de Respuesta ante Incidentes (ERI) debe realizar una evaluación preliminar:

- **Confirmar el incidente** y verificar su autenticidad.
- **Determinar el alcance** del impacto en sistemas, redes de datos y usuarias(os).
- **Determinar nivel de severidad** bajo, medio, alto o crítico.
- **Determinar efecto significativo**, que determinará el deber de notificar al CSIRT Nacional.
- **Priorizar la respuesta** según el nivel de severidad.

REPORTE AL CSIRT NACIONAL

En caso que se cumplan uno o más de los **efectos significativos**, el incidente debe ser reportado al CSIRT Nacional.

Revisar el Anexo "***Reporte al CSIRT Nacional***" en este documento.

PLANES DE CONTENCIÓN

La contención busca evitar la propagación del incidente y minimizar daños. Según el tipo de ataque, se pueden aplicar medidas como:

Phishing (correos maliciosos)

- Informar a mds@minsal.cl y solicitar el bloqueo del correo malicioso, indicando la información del correo, cuerpo del mensaje, correo del remitente, en lo posible, adjuntar correo phishing.
- Comunicarse con la/el usuaria/o afectada/o, quien recibió el correo malicioso, y cambiar la contraseña del correo, por una temporal y, que posteriormente, la/el usuaria/o la cambie.

Malware

- **Desconectar de la red** inmediatamente los equipos infectados para evitar la propagación.
- **Finalizar procesos sospechosos** a través del Administrador de Tareas o herramientas de seguridad.
- **Ejecutar un análisis de malware** con un antivirus actualizado en modo seguro.
- **Verificar si hay copias de seguridad recientes** antes de intentar restaurar archivos.

Ransomware

- **Desconectar de la red:** Deshabilitar WiFi y desconectar el cable de red (LAN) del equipo.
- **Evitar propagación lateral:** Si el equipo está en un dominio (Active Directory), deshabilitar la cuenta en el servidor.
- **Identificar si otros equipos están afectados:** Revisar tráfico sospechoso en SIEM, Antivirus o firewalls.

Accesos No Autorizados

- **Bloquear inmediatamente las cuentas comprometidas** y registrar la actividad sospechosa.

- **Forzar el cierre de sesión en todos los dispositivos** de las cuentas afectadas.
- **Cambiar contraseñas de acceso** por contraseñas seguras.
- **Revisar registros de acceso** para identificar el origen y posibles vulnerabilidades explotadas.
- **Fortalecer medidas de seguridad**, como restringir accesos según el principio de menor privilegio.

Ataques DDoS

Solicitar a TELCO en caso de no tener administración del firewall, lo siguiente:

- **Activar reglas de mitigación en firewalls y balanceadores de carga** para filtrar tráfico malicioso.
- **Limitar el tráfico por IP o geolocalización**, según patrones anómalos detectados.
- **Habilitar servicios de mitigación DDoS** si la organización cuenta con ellos.
- **Monitorear continuamente el tráfico** para identificar patrones y mejorar las defensas.

Fugas de Información

- **Revocar accesos inmediatamente** a usuarios o sistemas comprometidos.
- **Identificar qué información fue expuesta** y evaluar el impacto en la organización.
- **Aislar y proteger sistemas afectados**, evitando modificaciones o eliminaciones de registros.
- **Activar protocolos de respuesta** para notificar a las partes involucradas si es necesario.
- **Investigar el origen del incidente** y reforzar controles de acceso y seguridad de datos.

La contención debe aplicarse sin comprometer la evidencia necesaria para la investigación.

ERRADICACIÓN Y RECUPERACIÓN

Erradicación

- Identificar y eliminar la causa raíz del incidente.
- Aplicar parches de seguridad o configuraciones correctivas.
- Desinstalar software malicioso y revisar logs en busca de actividad sospechosa.

Recuperación

- Restaurar sistemas afectados desde copias de seguridad seguras.
- Validar la integridad de los datos antes de reanudar operaciones.
- Supervisar durante un período para detectar posibles ataques recurrentes.

REGISTRO Y DOCUMENTACIÓN

Todo incidente debe ser documentado detalladamente, incluyendo:

- Descripción del incidente y su impacto.
- Indicar si se identificó la causa raíz y el origen.
- Medidas tomadas en cada fase de respuesta.
- Resultados obtenidos y tiempo de resolución.
- Recomendaciones para evitar incidentes similares.

Esta documentación servirá para mejoras futuras.

PRUEBAS Y SIMULACROS

- Se deben realizar **ejercicios periódicos** de respuesta ante incidentes para evaluar la efectividad del protocolo.
- Pruebas como **simulaciones de ataques** o ejercicios de recuperación de datos ayudan a mejorar la preparación del equipo.
- Se deben ajustar los procedimientos según los resultados obtenidos en estos ensayos.

ANEXO

ANEXO N°1: REPORTE AL CSIRT NACIONAL

Si el incidente de ciberseguridad se encuentra entre uno de los **Efectos significativos**, se debe realizar el reporte al CSIRT Nacional, según estipula la ley.

Plataforma de reporte de incidentes

El personal autorizado para reportar al CSIRT Nacional es:

- Encargado de seguridad de la información y ciberseguridad del HBLT
- Encargado (s) de seguridad de la información y ciberseguridad del HBLT

Los informes de ciberataques e incidentes de ciberseguridad deben ser enviados a través de una plataforma tecnológica disponible las 24 horas del día.

- Deben estar inscritos en la plataforma https://portal.anci.gob.cl
- Esta plataforma permitirá también que los reportes se comuniquen simultáneamente a otras autoridades que deban ser notificadas.

Alerta Temprana

- Una vez que se conoce un incidente, la institución obligada a reportar debe enviar una alerta en un plazo máximo de **3 horas**.
- El aviso debe incluir la información mínima requerida, como:
  - La identificación de la institución,
  - Datos de contacto del delegado de ciberseguridad,
  - Fecha y hora del incidente,
  - Evidencias,
  - Repercusiones potenciales y detalles sobre los indicios del incidente.

Segundo reporte

- En un plazo máximo de **72 horas** desde que se tuvo conocimiento del incidente, la institución debe enviar un segundo reporte al CSIRT Nacional.
- Para los operadores de importancia vital, si el servicio esencial se ha visto afectado, la actualización debe ser enviada en un plazo máximo de **24 horas**.

Plan de acción de los operadores de importancia vital

- Estos operadores deben implementar e informar un plan de acción en un plazo no superior a **7 días** desde el conocimiento del incidente.
- El plan incluye un programa de recuperación de información y definición de responsabilidades técnicas y administrativas.

Informe Final

- Dentro de un plazo máximo de **15 días** desde la alerta temprana, la institución debe elaborar un informe final si el incidente ha sido gestionado.

  Este informe debe contener:
  - Descripción detallada del incidente y su impacto.
  - Tipo de amenaza o causa probable.
  - Medidas de mitigación aplicadas.
  - Cualquier impacto significativo observable.
  - Para operadores de importancia vital, deben incluir información adicional sobre vulnerabilidades y controles fallidos.

Informe parcial de incidente de ocurrencia prolongada

- Si el incidente no se gestiona en el tiempo estipulado, se debe enviar un informe parcial cada **15 días** sobre el estado del incidente.

Actualización de los informes

- El CSIRT Nacional puede solicitar información adicional a la institución obligada para gestionar el incidente de manera efectiva.
- Los informes son considerados información secreta y deben manejarse con confidencialidad.

Protección de Datos

En los reportes de incidentes debe omitirse cualquier dato o información personal, en cumplimiento con la legislación sobre protección de datos personales. La dirección IP no se considera un dato personal para estos efectos.

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

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