Asesoría jurídica

Mat.: Aprueba *"Procedimiento Gestión de incidentes"*.

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. La 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.

ÍJVE(S)

CONSIDERANDO

a) Que, el Hospital de Urgencia Asistencia Pública, como establecimiento autogestionado de alta complejidad y centro asistencial crítico a nivel nacional, depende de sistemas de información seguros y operativos para garantizar la continuidad del cuidado clínico y la administración eficiente de sus procesos institucionales.

b) Que, la creciente digitalización de los procesos hospitalarios y el aumento de ciberamenazas, tales como accesos no autorizados, ransomware, phishing y pérdida de dispositivos, representan riesgos significativos para la confidencialidad, integridad y disponibilidad de la información institucional, afectando potencialmente la atención de pacientes y la seguridad clínica.

c) Que, el presente Procedimiento de Gestión de Incidentes tiene por objeto establecer un marco formal y estandarizado para la detección, notificación, análisis, contención, erradicación, restauración, cierre y reporte de incidentes de seguridad de la información, incorporando los lineamientos de la Ley N° 21.633, el Decreto N° 295/2024, la Orientación Técnica de Ciberseguridad del Ministerio de Salud (2025) y las normas NCh-ISO/IEC 27001:2022 y 27035:2022.

d) Que, este instrumento define roles y responsabilidades para todo el personal del HUAP, la Mesa de Ayuda TIC, el Área TIC y el Encargado de Seguridad de la Información y Ciberseguridad, asegurando trazabilidad del manejo de incidentes, preservación de evidencias, cumplimiento de tiempos de respuesta (SLA), reporte obligatorio a la Agencia Nacional de Ciberseguridad (ANCI) y articulación con unidades clínicas cuando exista impacto asistencial**.**

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*** del *"Procedimiento Gestión de incidentes"*, dicto la siguiente:

RESOLUCIÓN

I. APRUÉBANSE la ***primera versión*** del *"Procedimiento Gestión de incidentes "*, que es del siguiente tenor:

Servicio de Salud Metropolitano Central – Ministerio de Salud	PROCEDIMIENTO GESTIÓN DE INCIDENTES				
	CÓDIGO UTIC	VERSIÓN 01	FECHA 10/2025	VIGENCIA 5 años	N° PÁGINAS 18

HOSPITAL DE URGENCIA ASISTENCIA PUBLICA

Revisado Por:	Aprobado Por:
FIRMA ELECTRÓNICA AVANZADA – GOBIERNO DE CHILE Firmado por: Karla Andrea Alfaro Flores Jefatura Calidad y Seguridad del Paciente Fecha: 03-11-2025 13:27 CLT Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río	FIRMA ELECTRÓNICA AVANZADA – GOBIERNO DE CHILE Firmado por: Patricio Raúl Barría Ailef Director Huap Fecha: 04-11-2025 14:42 CLT Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

ÍNDICE:

I. INTRODUCCIÓN

La gestión de incidentes de seguridad de la información constituye un componente esencial de la continuidad asistencial en el Hospital de Urgencia Asistencia Pública (HUAP). La creciente digitalización de los procesos clínicos y administrativos ha incrementado la exposición a ciber amenazas tales como accesos no autorizados, malware, ransomware y pérdida de dispositivos, las cuales pueden comprometer la confidencialidad, integridad y disponibilidad de la información institucional.

A nivel nacional, según datos del CSIRT de Gobierno (2024), los incidentes de ciberseguridad en el sector salud se han incrementado en un 35% respecto del año anterior, afectando tanto la atención directa de pacientes como la disponibilidad de sistemas críticos. En el contexto hospitalario, la evidencia internacional indica que los ciberataques pueden generar retrasos en procedimientos clínicos, filtración de datos sensibles y pérdidas financieras significativas.

Este procedimiento se fundamenta en normativas legales y técnicas vigentes, tales como la Ley N° 21.633 sobre reporte de incidentes de ciberseguridad, el Decreto N° 295 del Ministerio del Interior (2024), la Orientación Técnica de Ciberseguridad del Ministerio de Salud (2025), y las normas NCh-ISO/IEC 27001:2022 y NCh-ISO/IEC 27035:2022 sobre gestión de incidentes de seguridad de la información.

II. OBJETIVOS

General:

Establecer el procedimiento institucional para la detección, análisis, contención y resolución de incidentes de seguridad de la información en el Hospital de Urgencia Asistencia Pública (HUAP), a fin de proteger los activos de información y mantener la continuidad asistencial conforme a la normativa vigente.

Específicos:

- Implementar mecanismos claros y accesibles de notificación y registro de incidentes de seguridad de la información por parte de todo el personal y terceros vinculados al Hospital de Urgencia Asistencia Pública (HUAP).

- Garantizar una gestión coordinada y eficiente de los incidentes de seguridad de la información, promoviendo la mejora continua y la aplicación de medidas preventivas en la institución.

III. ALCANCE

Este procedimiento está dirigido a todas y todos los funcionarios del Hospital de Urgencia Asistencia Pública (HUAP), así como al personal externo y proveedores que, de manera directa o indirecta, accedan, utilicen o gestionen los sistemas de información, servicios digitales y activos de información institucionales.

IV. DEFINICIONES

- **HUAP:** Hospital de Urgencia Asistencia Pública.

- **Ministerio de Salud (MINSAL):** Autoridad nacional responsable de normar y supervisar los procesos de salud en Chile.

- **Agencia Nacional de Ciberseguridad (ANCI):** Autoridad Nacional encargada de coordinar, supervisar y fiscalizar la Ciberseguridad en Chile, a la cual deben reportarse incidentes críticos o de alto impacto conforme a la Ley N.º 21.633.

- **CSIRT:** Equipo Nacional de Respuesta a Incidentes de Seguridad Informática perteneciente a la Agencia Nacional de Ciberseguridad.

- **Incidente de seguridad de la información:** Evento no deseado o inesperado que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información institucional.

- **Evento de seguridad:** Situación que puede indicar una posible falla de seguridad, pero que aún no ha sido confirmada como incidente.

- **Vulnerabilidad:** Debilidad en un sistema, proceso o configuración que puede ser explotada y dar origen a un incidente de seguridad.

- **Activo de información:** Datos, sistemas, equipos, aplicaciones o cualquier recurso que tenga valor para la institución y que requiere protección.

- **Ransomware:** Tipo de software malicioso que bloquea o cifra los archivos de un dispositivo o sistema, impidiendo su uso normal, y que generalmente solicita un rescate económico para restablecer el acceso.

- **Phishing:** Técnica utilizada por atacantes para obtener información confidencial de las personas (como contraseñas o datos bancarios) mediante correos electrónicos, mensajes u otros medios que aparentan ser legítimos.

- **Malware:** Software diseñado con fines maliciosos, como dañar, alterar o acceder sin autorización a sistemas, aplicaciones o información del Hospital, incluyendo virus, troyanos, ransomware, spyware y otros programas dañinos.

V. RESPONSABLES DE LA EJECUCIÓN

Responsables de ejecución

- **Todo el personal del HUAP (funcionarias/os y personal externo autorizado)** Notificar oportunamente cualquier evento, debilidad o sospecha de incidente de seguridad a través de los canales oficiales.

- **Mesa de Ayuda TIC / Soporte Técnico:** Recibir y registrar los incidentes reportados en la planilla oficial o sistema de tickets, entregar atención inicial y escalar cuando corresponda.

- **Área TIC:** Ejecutar las acciones técnicas necesarias para contener y resolver los incidentes, en coordinación con el Encargado de Seguridad de la Información y Ciberseguridad.

Responsable de supervisión

- **Encargado de Seguridad de la Información y Ciberseguridad:** Coordinar el ciclo completo de gestión del incidente (detección, análisis, clasificación, contención, resolución y cierre), mantener registro actualizado de incidentes y supervisar la correcta aplicación del procedimiento por parte del personal y las áreas involucradas.

Responsable de evaluación

- **Dirección del HUAP:** Evaluar periódicamente el cumplimiento del protocolo, garantizar la disponibilidad de recursos para su implementación, y aprobar la actualización del documento conforme a la normativa vigente y las orientaciones del Ministerio de Salud y la Agencia Nacional de Ciberseguridad (ANCI).

VI. DESARROLLO DEL PROCESO

Inicio del Protocolo

El proceso se inicia con la detección y notificación de un evento sospechoso de seguridad de la información por parte de cualquier funcionario/a, personal externo o proveedor del Hospital de Urgencia Asistencia Pública (HUAP).

Desarrollo del Proceso

1. **Detección y Notificación**
   - Cualquier funcionario/a o tercero vinculado al HUAP que detecte un incidente de seguridad de la información debe **notificar inmediatamente a la Mesa de Ayuda TIC** mediante **correo institucional o teléfono oficial**, entregando la siguiente información mínima:
     - Nombre y Unidad
     - Fecha y hora del evento
     - Descripción del evento
     - Activo afectado

   - **No se permiten canales informales** como WhatsApp u otros medios no oficiales.
   - Se consideran sospechosos:
     - correos de phishing.
     - pantallas de bloqueo/ransomware.
     - lentitud o caída inusual de sistemas clínicos.
     - accesos no reconocidos.
     - pérdida/robo de dispositivos.

   - Acción inicial del usuario antes de notificar (contención básica):
     - **Phishing:** no abrir enlaces ni adjuntos, no entregar credenciales.
     - **Ransomware / pantalla de bloqueo:** desconectar de inmediato el equipo de la red (cable o WiFi). Si no es posible, apagar el dispositivo.
     - **Pérdida/robo de dispositivo:** notificar sin intentar acceder o manipular remotamente.
     - **Accesos no reconocidos:** cerrar sesión si es posible y no volver a ingresar hasta recibir instrucciones.

2. Registro del Incidente

Responsable: Mesa de Ayuda TIC.

- Se registra en el sistema de tickets o en la **Planilla Oficial de Registro de Incidentes (Anexo 1)**, con los siguientes campos: número correlativo, fecha/hora, reportante, descripción, activo afectado, severidad inicial.
- **Plazo máximo:** 30 minutos desde la notificación.
- **Niveles de servicio (SLA internos):**
  - **Incidentes Críticos (ej. Ransomware activo, caída total de sistema clínico, fuga de datos sensibles):** la Unidad de TIC debe iniciar contacto con el área afectada e instruir acciones de contención en **≤ 5 minutos** desde la notificación.
  - **Incidentes de Alto impacto:** contacto inicial en **≤ 15 minutos**.
  - **Incidentes de impacto Medio o Bajo:** contacto inicial en **≤ 1 hora**.

3. Clasificación y Priorización

- **Responsable:** Encargado/a de Seguridad de la Información y Ciberseguridad.
- **Niveles de impacto:** Bajo, Medio, Alto, Crítico.
- **Tiempos de reporte:**
  - **Incidentes Críticos o Altos:** deben reportarse a la ANCI dentro de un plazo máximo de ≤ 3 horas.
  - **Incidentes Medios:** deben ser gestionados y documentados en un plazo no mayor a ≤ 24 horas desde su notificación.
  - **Incidentes Bajos:** deben quedar registrados y resueltos en un plazo máximo de ≤ 72 horas, sin necesidad de reporte externo, salvo que escalen en impacto.
- **Reporte a la ANCI**:
  La Agencia Nacional de Ciberseguridad de Chile (ANCI) requiere que se reporten incidentes de **Alto o Crítico impacto** que afecten a servicios esenciales.
  Criterios específicos de reportes según la ANCI:

- **Ransomware activo** que interrumpa operaciones críticas
- **Caída completa de sistemas clínicos** que afecte la atención de pacientes
- **Fuga o exposición de datos sensibles** (historial clínico, información personal de pacientes)
- **Acceso no autorizado a sistemas críticos** que pueda comprometer la continuidad asistencial
- **Otros incidentes cibernéticos significativos** que impacten infraestructura crítica

Responsable del reporte a la ANCI: Encargado/a de Seguridad de la Información y Ciberseguridad, utilizando la plataforma disponible 24/7 en portal.anci.gob.cl. La falta de reporte puede acarrear responsabilidades legales según la Ley N° 21.663.

4. Contención Inmediata

- **Responsable:** Área TIC, bajo coordinación del Encargado/a de Seguridad de la Información y Ciberseguridad.
- **Acciones:** aislar equipos, bloquear usuarios, desactivar servicios comprometidos, cortar Internet si hay propagación:
  - Aislar equipos comprometidos.
  - Bloquear usuarios afectados.
  - Desactivar servicios comprometidos.
  - Cortar Internet si se detecta propagación del incidente
- **Preservación de evidencias:**
  - no reiniciar ni formatear
  - guardar logs/capturas
  - registrar hora exacta de las acciones.

5. Erradicación

- Eliminar malware o accesos no autorizados.
- Restablecer contraseñas.
- Aplicar parches de seguridad.
- Dar de baja credenciales de usuarios desvinculados.

6. Restauración y Retorno a la Operación

- Restaurar servicios desde respaldos probados.
- Verificar integridad de la información recuperada.
- Realizar pruebas de validación antes de liberar el servicio.
- Validar con el área clínica/usuaria afectada.

7. Cierre del Incidente y Lecciones Aprendidas

- **Responsable:** Encargado/a de Ciberseguridad.
- **Documentar:** resumen, medidas adoptadas, tiempo de respuesta, impacto real, recomendaciones.
- Definir medidas correctivas y elaborar informe final para Dirección y ANCI (cuando corresponda).

8. Escalamiento y Comunicación

- **Interno:**
  - Incidentes críticos se informan a Dirección en máximo 1 hora.
  - En incidentes con impacto asistencial (ej. caída de sistemas clínicos, pérdida de acceso a historiales, interrupción de resultados de laboratorio o imágenes), se debe notificar de inmediato a Subdirección de Gestión Clínica y Unidad de Calidad y Seguridad del Paciente para la activación de planes de contingencia clínica.

  .
- **Externo:** Incidentes de Alto o Crítico impacto deben reportarse a la ANCI en máximo 3 horas (Ley N° 21.633).

- **Comunicación interna:**
  - Emisión de avisos preventivos cuando corresponda.
  - Las unidades clínicas afectadas deben recibir instrucciones claras sobre las medidas de contingencia a aplicar.

Término del Protocolo

El proceso concluye con el cierre formal del incidente y la emisión del informe final. Este protocolo debe ser distribuido a todas las unidades clínicas y administrativas del HUAP, incluyendo personal interno y externo que interactúe con sistemas de información y activos críticos.

VII. REGISTROS

Los registros generados durante la gestión de incidentes de seguridad de la información deben almacenarse de forma segura y trazable, garantizando su integridad, confidencialidad y disponibilidad, y quedando accesibles para auditorías internas y externas.

1. Planilla Oficial de Registro de Incidentes (Anexo 1)

- **Registro:** incidentes de seguridad de la información reportados, incluyendo campos mínimos:
  - Número de incidente.
  - Fecha y hora de reporte.
  - Persona que reporta.
  - Activo afectado.
  - Descripción breve.
  - Impacto y nivel de criticidad (Bajo, Medio, Alto, Crítico).
  - Acciones de contención y resolución.
  - Estado (Abierto / Cerrado).
  - Fecha de cierre.
  - Lecciones aprendidas.

- **Formato:** Excel institucional almacenado en el repositorio oficial del HUAP.
- **Responsable:** Encargado/a de Seguridad de la Información y Ciberseguridad.
- **Conservación:** mínimo 5 años en el repositorio institucional, conforme al Protocolo de Gestión Documental del HUAP.

2. Sistema de Tickets de Mesa de Ayuda TIC (si aplica)

- **Registro:** incidentes ingresados digitalmente a través del sistema oficial de soporte.
- **Función:** repositorio complementario a la planilla oficial.
- **Responsable:** Unidad de Mesa de Ayuda TIC.
- **Frecuencia:** cada incidente reportado por funcionario/a, proveedor o tercero debe ser registrado en el sistema en un máximo de 30 minutos desde la notificación.

3. Evidencias Técnicas

- **Registro:** documentación técnica básica vinculada al incidente (logs, capturas de pantalla, reportes de herramientas de seguridad, respaldos de comunicaciones internas).
- **Responsable:** Unidad TIC bajo coordinación del Encargado/a de Ciberseguridad.
- **Almacenamiento:** carpeta compartida con control de acceso restringido a personal autorizado.
- **Conservación:** en concordancia con los registros oficiales (mínimo 5 años).

4. Historial de Reportes a la ANCI (cuando corresponda)

- **Registro:** copia de comunicaciones oficiales realizadas a la Agencia Nacional de Ciberseguridad (ANCI), según lo dispuesto por la Ley N.º 21.633.
- **Responsable:** Encargado/a de Seguridad de la Información y Ciberseguridad.
- **Almacenamiento:** repositorio institucional de documentos normativos y legales.

VIII. DIFUSION

El presente Protocolo de Gestión de Incidentes de Seguridad de la Información será difundido de manera accesible y comprensible a todas las unidades del

HUAP, asegurando que el personal interno y externo conozca los procedimientos básicos de notificación, registro y respuesta.
La difusión se realizará a través de los siguientes medios:

Correo electrónico institucional: envío informativo a todas las unidades clínicas y administrativas del HUAP.

Avisos internos preventivos: comunicados breves frente a incidentes frecuentes (ej. phishing, ransomware).

IX. REVISIÓN

El presente protocolo deberá ser revisado al menos una vez al año, o antes si ocurre alguna de las siguientes situaciones:

- Cambios normativos emitidos por el MINSAL, la ANCI u otros organismos competentes.
- Modificaciones relevantes en los sistemas TIC o procesos críticos.
- Incidentes de seguridad que evidencien deficiencias en su aplicación.

Responsables de la revisión: Encargado/a de Seguridad de la Información y Ciberseguridad, en coordinación con la Jefatura de la Unidad de Tecnologías de la Información.

El resultado de la revisión deberá documentarse en la sección “Modificaciones del Documento” de la presente versión

X. DISTRIBUCIÓN

- Dirección
- Subdirección de Gestión Clínica
- Subdirección de Gestión del Cuidado
- Subdirección Administrativa y Financiera
- Subdirección de Gestión y Desarrollo de las Personas
- Unidad de Calidad y Seguridad del Paciente.
- Unidad de Tecnologías de la Información.

XI. REFERENCIAS BIBLIOGRÁFICAS

- Congreso Nacional de Chile. (2023). *Ley N° 21.663: Marco de Ciberseguridad*. Biblioteca del Congreso Nacional de Chile. Disponible en: https://www.bcn.cl
- Instituto Nacional de Normalización. (2022). *NCh-ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos*. Santiago de Chile: INN.
- Instituto Nacional de Normalización. (2022). *NCh-ISO/IEC 27002:2022. Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información*. Santiago de Chile: INN.
- Ministerio de Salud. (2025). *Orientación técnica indicador COMGES de ciberseguridad 2025: Implementación de controles críticos de seguridad de la información y ciberseguridad*. Santiago de Chile: MINSAL.
- Ministerio del Interior y Seguridad Pública. (2024). *Decreto N° 295: Reglamento de reporte de incidentes de ciberseguridad de la Ley N° 21.633*. Santiago de Chile: Gobierno de Chile.
- Hospital de Urgencia Asistencia Pública. (2024). *Protocolo de Gestión Documental*. Unidad de Calidad y Seguridad del Paciente, versión 04.

Santiago de Chile: HUAP. Disponible en: https://doc.digital.gob.cl/validador/2GSJZF-686

- Congreso Nacional de Chile. (2002). *Ley N° 19.799: Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma*. Biblioteca del Congreso Nacional de Chile. Disponible en: https://www.bcn.cl

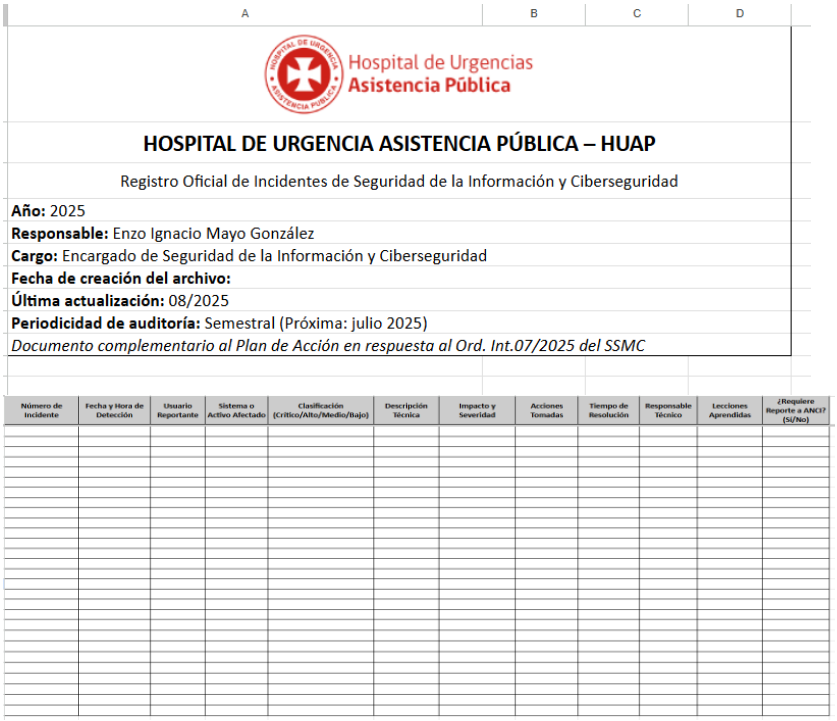
XII. MODIFICACIONES DEL DOCUMENTO

SÍNTESIS DE MODIFICACIONES			RESPONSABLE MODIFICACIÓN	APROBADO POR
VERSIÓN	FECHA	CAUSA DE MODIFICACIÓN		
01	10/2025	Creación del Documento	Enzo Mayo G. Encargado Ciberseguridad	Dr. Patricio Barría

XIII. ANEXOS

ANEXO N° 1: Plantilla Oficial de Registro de Incidentes:

La planilla oficial se mantiene en formato Excel en el repositorio institucional y será administrada por el Encargado de Seguridad de la Información y Ciberseguridad.



Hospital de Urgencias Asistencia Pública

HOSPITAL DE URGENCIA ASISTENCIA PÚBLICA – HUAP

Registro Oficial de Incidentes de Seguridad de la Información y Ciberseguridad

Año: 2025
Responsable: Enzo Ignacio Mayo González
Cargo: Encargado de Seguridad de la Información y Ciberseguridad
Fecha de creación del archivo:
Última actualización: 08/2025
Periodicidad de auditoría: Semestral (Próxima: julio 2025)
Documento complementario al Plan de Acción en respuesta al Ord. Int.07/2025 del SSMC

Número de Incidente	Fecha y Hora de Detección	Usuario Reportante	Sistema o Activo Afectado	Clasificación (Crítico/Alto/Medio/Bajo)	Descripción Técnica	Impacto y Severidad	Acciones Tomadas	Tiempo de Resolución	Responsable Técnico	Lecciones Aprendidas	¿Requiere Reporte a ANCI? (Sí/No)

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: 28-10-2025 15:40 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Firmado por:
Susana Ximena Avendaño Durán
Jefatura Tic
Fecha: 28-10-2025 15:46 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Firmado por:
Christian Irving Echeverría Aburto
Subdirector Gestión Administrativa y Financiera
Fecha: 28-10-2025 17:37 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

II. TÉNGASE PRESENTE la vigencia de este procedimiento a contar de la fecha de la total tramitación de la presente Resolución.

III. ESTABLÉCESE que el señalado *"Procedimiento Gestión de incidentes"*, 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 este procedimiento.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

FIRMA ELECTRÓNICA AVANZADA · GOBIERNO DE CHILE

Firmado por:
Patricio Raúl Barría Ailef
Director Huap
Fecha: 16-12-2025 10:04 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 Administrativa y Financiera.
5. Subdirección de Gestión y Desarrollo de las Personas.
6. Unidad de Tecnologías de la Información.
7. Unidad de Calidad y Seguridad del Paciente.
8. Asesoría Jurídica.
9. Oficina de Partes.

ÍJVE(S)