Asesoría Jurídica

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

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. 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.

XASV

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

CONSIDERANDO

a) Que, el Hospital de Urgencia Asistencia Pública, como establecimiento de alta complejidad y nodo clínico-tecnológico de referencia nacional, debe asegurar la continuidad operativa de sus sistemas críticos y la protección de la información institucional frente a amenazas cibernéticas.

b) Que, el aumento sostenido de vulnerabilidades en infraestructura tecnológica, sistemas clínicos y aplicaciones institucionales representa un riesgo real para la seguridad de la información, la atención oportuna de los pacientes y el cumplimiento de la normativa vigente en materia de protección de datos.

c) Que, el presente Procedimiento de Gestión de Vulnerabilidades establece un marco técnico y operativo para la detección, análisis, clasificación, tratamiento, seguimiento y cierre de vulnerabilidades en activos tecnológicos del HUAP, conforme a estándares internacionales como ISO/IEC 27001, CVSS, CVE y NIST SP 800-40.

d) Que, este instrumento define roles y responsabilidades para el equipo de Ciberseguridad, las jefaturas TIC, los propietarios funcionales de sistemas y el Comité de Ciberseguridad, asegurando trazabilidad documental, control de excepciones, planificación de remediación y mejora continua en la gestión de riesgos tecnológicos.

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;

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

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 vulnerabilidades"*, dicto la siguiente:

RESOLUCIÓN

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

Servicio de Salud Metropolitano Central – Ministerio de Salud	PROCEDIMIENTO GESTIÓN DE VULNERABILIDADES				
	CÓDIGO UTIC	VERSIÓN 01	FECHA 09/2025	VIGENCIA 5 años	N° PÁGINAS 14

HOSPITAL DE URGENCIA ASISTENCIA PUBLICA

Revisado Por:	Aprobado Por:
Firmado por: Ilse Dora del Carmen Silva Robles Jefatura Calidad y Seguridad del Paciente (s) Fecha: 01-10-2025 16:35 CLT Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río	Firmado por: Jorge Arturo Ibáñez Parga Director Huap (s) Fecha: 03-10-2025 17:10 CLT Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

ÍNDICE:

I. INTRODUCCION ..... **¡Error! Marcador no definido.**

II. OBJETIVOS ..... **¡Error! Marcador no definido.**

III. ALCANCE ..... **¡Error! Marcador no definido.**

IV. DEFINICIONES ..... **¡Error! Marcador no definido.**

V. RESPONSABILIDADES: ..... **¡Error! Marcador no definido.**

VI. DESARROLLO DEL PROCESO..... **¡Error! Marcador no definido.**

VII. REGISTROS..... **¡Error! Marcador no definido.**

VIII. DIFUSIÓN..... **¡Error! Marcador no definido.**

IX. REVISIÓN..... **¡Error! Marcador no definido.**

X. EXCEPCIONES AL CUMPLIMIENTO ..... **¡Error! Marcador no definido.**

XI. DISTRIBUCIÓN: ..... **¡Error! Marcador no definido.**

XII. REFERENCIAS BIBLIOGRÁFICAS:..... **¡Error! Marcador no definido.**

XIII. MODIFICACIONES DEL DOCUMENTO: ..... **¡Error! Marcador no definido.**

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.

Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:

https://doc.digital.gob.cl/validador/6RTHG5-654

I. INTRODUCCION

La seguridad de la información constituye un componente esencial para garantizar la continuidad asistencial, la calidad de la atención y la protección de los datos en el Hospital de Urgencia Asistencia Pública (HUAP). Diversos estudios y reportes internacionales (ISO/IEC 27001:2022, NIST SP 800-40) evidencian que la gestión oportuna de vulnerabilidades reduce de manera significativa la probabilidad de incidentes de ciberseguridad, los cuales representan una de las principales amenazas para los sistemas de salud a nivel mundial.

En el contexto nacional, la Ley N° 19.628 sobre protección de la vida privada y las directrices del Ministerio de Salud establecen la obligación de resguardar la confidencialidad, integridad y disponibilidad de la información clínica y administrativa. Asimismo, el aumento sostenido de ciberataques en el sector público sanitario evidencia la magnitud del problema y la necesidad de establecer procedimientos estandarizados de prevención, detección y tratamiento de vulnerabilidades.

El presente protocolo establece lineamientos para la identificación, clasificación, análisis y tratamiento de vulnerabilidades en los activos tecnológicos institucionales, en concordancia con las buenas prácticas de seguridad de la información y la normativa vigente.

La población objetivo corresponde al personal de la Unidad de Tecnologías de la Información, al Comité de Ciberseguridad y a los referentes técnicos de las distintas unidades del HUAP que administren sistemas o servicios críticos. De igual forma, involucra a las jefaturas responsables de aprobar recursos, planes de acción y excepciones asociadas a la gestión de vulnerabilidades.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.

Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:

https://doc.digital.gob.cl/validador/6RTHG5-654

II. OBJETIVOS

General:

Establecer un procedimiento sistemático para la gestión de vulnerabilidades en los activos tecnológicos del Hospital de Urgencia Asistencia Pública (HUAP), con el fin de proteger la información institucional, resguardar la continuidad de los servicios y cumplir con la normativa vigente.

Específicos:

- Identificar y clasificar las vulnerabilidades presentes en los sistemas, redes y aplicaciones institucionales, según su nivel de criticidad y riesgo asociado.

- Coordinar y verificar la implementación de acciones de tratamiento que permitan mitigar, remediar o gestionar los riesgos detectados.

III. ALCANCE

Este protocolo está dirigido a las y los profesionales de la Unidad de Tecnologías de la Información y a las y los integrantes del Comité de Ciberseguridad del Hospital de Urgencia Asistencia Pública (HUAP), quienes son responsables de aplicar, supervisar y dar cumplimiento a las acciones establecidas en materia de gestión de vulnerabilidades.

IV. DEFINICIONES

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

- **SGSI:** Sistema de Gestión de Seguridad de la Información. Conjunto de políticas, procedimientos, controles y recursos implementados para proteger la confidencialidad, integridad y disponibilidad de los activos de información.

- **CVE (Common Vulnerabilities and Exposures):** Diccionario público que asigna identificadores únicos a vulnerabilidades de seguridad conocidas.

- **CVSS (Common Vulnerability Scoring System):** Estándar internacional para asignar una puntuación de severidad a las vulnerabilidades.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

- **Amenaza:** Evento o acción con potencial de comprometer la seguridad de un sistema (ejemplo: ataque malicioso, error humano, desastre natural).
- **Vulnerabilidad:** Debilidad en un sistema o componente que puede ser explotada por una amenaza para afectar su seguridad.
- **Riesgo de Seguridad:** Probabilidad de que una amenaza explote una vulnerabilidad y cause impacto en la confidencialidad, integridad o disponibilidad de la información.
- **Análisis de Riesgos:** Proceso de identificar, evaluar y priorizar riesgos de seguridad en sistemas y procesos.
- **Análisis de Vulnerabilidades**: Identificación y evaluación de debilidades en sistemas, redes o aplicaciones con el fin de tratarlas antes de ser explotadas.
- **Escáner de Vulnerabilidades:** Herramienta automatizada que examina sistemas, aplicaciones o redes en busca de debilidades conocidas o configuraciones inseguras.
- **Prueba de Penetración (Pentest):** Evaluación activa de seguridad que simula ataques reales para identificar vulnerabilidades y verificar la efectividad de los controles.
- **Controles de Seguridad:** Medidas técnicas, administrativas o físicas implementadas para reducir riesgos y proteger los activos de información (ejemplo: firewall, cifrado, autenticación).
- **Política de Seguridad:** Conjunto de reglas y directrices que establecen cómo se deben proteger y administrar los activos de información.
- **Tratamiento de la Vulnerabilidad:** Acción tomada para gestionar un riesgo asociado a una vulnerabilidad (remediación, mitigación, aceptación o transferencia).
- **Remediación:** Corrección de una vulnerabilidad mediante parches, actualizaciones o cambios de configuración.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

- **Incidente de Seguridad:** Evento que compromete o amenaza la confidencialidad, integridad o disponibilidad de la información (ejemplo: acceso no autorizado, fuga de datos, interrupción de servicio).

V. RESPONSABILIDADES:

- **Encargado/a de Ciberseguridad:** Responsable de la ejecución del procedimiento, incluyendo:
    - Coordinación de escaneos automatizados internos y solicitud de escaneos oficiales a MINSAL o ANCI cuando corresponda.
    - Clasificación de la criticidad de las vulnerabilidades.
    - Coordinación del tratamiento con los responsables técnicos.
    - Registro, seguimiento y reporte de hallazgos.
    - Comunicación de incidentes y vulnerabilidades a la Jefatura TIC y al Comité de Ciberseguridad.
- **Equipo de Desarrollo interno o proveedores externos designados:** Responsable de corregir vulnerabilidades detectadas en los sistemas y sitios web desarrollados internamente. Aplica remediaciones, refactoriza código inseguro y colabora en la validación de pruebas.
- **Encargado/a de Infraestructura:** Aplica parches de seguridad, actualiza configuraciones de red y de servicios relacionados (servidores web, bases de datos, entre otros) cuando la vulnerabilidad afecta componentes de infraestructura.
- **Jefatura de Tecnologías de la Información:** Aprueba el presente procedimiento, prioriza recursos para la aplicación de correcciones críticas y gestiona excepciones formales. Supervisa el cumplimiento del plan de remediación.
- **Referentes Técnicos de Sistemas / Propietarios Funcionales:** Personas designadas por cada unidad o área responsable del sistema. Evalúan el impacto de aplicar parches o cambios y, cuando no sea posible corregir de inmediato una vulnerabilidad, validan su registro como riesgo aceptado.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

- **Comité de Ciberseguridad:** Recibe reportes periódicos de avance en gestión de vulnerabilidades y puede aprobar excepciones formales o planes de acción diferidos.

VI. DESARROLLO DEL PROCESO

Inicio del Protocolo:

El procedimiento de gestión de vulnerabilidades del Hospital de Urgencia Asistencia Pública (HUAP) comienza con la detección de debilidades en los sistemas de información.

Estas debilidades pueden identificarse mediante:

- **Escaneos automatizados** (similares a un antivirus que revisa si hay problemas en los sistemas).
- **Solicitudes de escaneo oficial** al Ministerio de Salud (MINSAL) o la Agencia Nacional de Ciberseguridad (ANCI).
- **Auditorías internas o externas** (revisiones programadas para verificar seguridad).
- **Pruebas de penetración** (simulación de un ataque controlado para ver qué tan fácil sería ingresar a un sistema).
- **Reportes internos** entregados por funcionarios o usuarios.

Desarrollo del Proceso:

1.Identificación de Vulnerabilidades

- Se realizan escaneos periódicos (una vez al mes o después de cambios importantes en los sistemas, por ejemplo: cuando se instalan nuevas versiones de programas, se actualizan aplicaciones internas del hospital o se hacen modificaciones grandes en los servidores o la red).

- Para la implementación de nuevos sistemas críticos en el hospital, se deberá solicitar revisión oficial al MINSAL o ANCI.

- Se revisan avisos de seguridad de los fabricantes de software y reportes de incidentes de otras instituciones.

2.Clasificación y Puntuación de Vulnerabilidades

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

- Cada hallazgo se evalúa según su nivel de riesgo.
- Para esto se usa una escala internacional llamada CVSS (Common Vulnerability Scoring System), que mide de 0 a 10 qué tan grave es el problema:

Rango de Puntuación CVSS	Nivel de Riesgo
9.0 – 10.0	**Critico**
7.0 – 8.9	**Alto**
4.0 – 6.9	**Medio**
0.1 – 3.9	**Bajo**
0.0	**Informativo**

- Además de la puntuación, se consideran aspectos como:
  - Qué tan fácil es aprovechar la vulnerabilidad (explotabilidad).
  - El impacto en confidencialidad, integridad y disponibilidad (ejemplo: acceso a datos de pacientes, modificación de información, caída del sistema).
  - La importancia del sistema afectado (ej: sistemas clínicos críticos).

3.Análisis de Vulnerabilidades

- Confirmar que la vulnerabilidad existe realmente en los sistemas del HUAP.
- Identificar qué servidores, aplicaciones o redes están comprometidos.
- Priorizar el orden de tratamiento según riesgo y recursos disponibles.

4.Tratamiento de Vulnerabilidades

Dependiendo de la gravedad y del impacto, se aplican las siguientes acciones:

- Remediación: corregir el problema (ejemplo: instalar una actualización o parche).

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

- Mitigación: aplicar controles temporales (ejemplo: bloquear accesos con un firewall).
- Aceptación: registrar el riesgo y aceptarlo formalmente si no es posible corregirlo de inmediato.
- Transferencia: delegar el riesgo mediante seguros o servicios de terceros.

5.Verificación de la Remediación

- Se vuelven a realizar escaneos o pruebas para confirmar que la vulnerabilidad fue eliminada.

- El Encargado/a de Ciberseguridad valida los resultados y los registra en el repositorio oficial definido por la Unidad de Tecnología de la Información, conforme a los lineamientos de gestión de seguridad de la información.

6.Seguimiento y Monitoreo

- Mantener un registro actualizado de vulnerabilidades abiertas, en tratamiento y cerradas.

- Revisar continuamente nuevas alertas de seguridad.

- Evaluar el protocolo al menos una vez al año o cuando haya cambios tecnológicos relevantes.

- Generar informes periódicos para la Jefatura TIC y el Comité de Ciberseguridad.

Término del Protocolo:

El proceso finaliza con la entrega de reportes oficiales de gestión de vulnerabilidades a las unidades involucradas (TIC, Comité de Ciberseguridad, responsables de sistemas), los cuales se enviarán mediante comunicación oficial por correo electrónico institucional y quedarán disponibles en el repositorio definido por la Unidad de Tecnología de la Información. Estos reportes deberán emitirse dentro de un plazo máximo de 10 días hábiles posteriores a la validación de la remediación o cierre del hallazgo.

VII. REGISTROS

Los registros generados durante la ejecución del presente protocolo deberán conservarse en repositorios seguros definidos por la Unidad de Tecnología de la

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.

Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:

https://doc.digital.gob.cl/validador/6RTHG5-654

Información, en conformidad con los lineamientos de gestión de seguridad de la información del HUAP.

El período mínimo de conservación será de 2 años, garantizando su trazabilidad y cumplimiento normativo.

Se consideran registros:

- Formularios de solicitud de escaneo de seguridad enviados a MINSAL o ANCI, junto con la evidencia de respuesta y resultados.
- Informes de análisis de vulnerabilidades emitidos por herramientas automatizadas o por pruebas manuales.
- Reportes oficiales generados por entidades externas (MINSAL, ANCI).
- Actas y reportes internos de validación elaborados por el Encargado/a de Ciberseguridad.

VIII. DIFUSIÓN

La versión controlada de este documento se almacenará en el repositorio institucional definido por la Unidad de Tecnología de la Información del HUAP.

El/la Encargado/a de Ciberseguridad será responsable de su difusión a las unidades correspondientes mediante:

- Comunicación oficial por correo electrónico al personal de la Unidad de Tecnologías de la Información.
- Envío al Comité de Ciberseguridad para conocimiento y validación.

IX. REVISIÓN

El presente protocolo deberá ser revisado al menos una vez al año, o cuando se produzcan cambios significativos derivados de:

- Incorporación de nueva tecnología.
- Actualización de normativa vigente.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

- Ocurrencia de incidentes críticos de ciberseguridad.

Responsables de la revisión: Encargado/a de Ciberseguridad y Jefatura de Tecnologías de la Información.

El resultado de la revisión se documentará en el apartado 'Modificaciones del Documento' de la presente versión.

X. EXCEPCIONES AL CUMPLIMIENTO

Podrán solicitarse excepciones a este protocolo en casos debidamente justificados, mediante el Formulario institucional de "Solicitud de Excepción" o correo electrónico formal dirigido a la Jefatura TIC, con copia al Comité de Ciberseguridad.

Toda solicitud debe contener:

- Vulnerabilidad o requisito afectado.
- Justificación técnica o clínica.
- Controles compensatorios propuestos.
- Plazo solicitado (máximo 6 meses).

La aprobación de la excepción corresponde a la Jefatura TIC, con visto bueno del Comité de Ciberseguridad.

Las excepciones deberán registrarse en el repositorio oficial definido por la Unidad de Tecnología de la Información y ser revisadas antes de su vencimiento. En caso de persistir la causa, podrán renovarse formalmente o cerrarse mediante la remediación definitiva.

El/la Encargado/a de Ciberseguridad será responsable de mantener actualizado el registro de excepciones y su estado.

XI. DISTRIBUCIÓN:

- Dirección.
- Subdirección de Gestión Clínica.
- Subdirección de Gestión del Cuidado.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

- 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

XII. REFERENCIAS BIBLIOGRÁFICAS:

- International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.
- Biblioteca del Congreso Nacional de Chile. (1999). *Ley N° 19.628 sobre protección de la vida privada*. Gobierno de Chile. https://www.bcn.cl/leychile/navegar?idNorma=141599.
- MITRE Corporation. (s. f.). *Common vulnerabilities and exposures (CVE)*.
- Forum of Incident Response and Security Teams. (s. f.). *Common vulnerability scoring system (CVSS)*. https://www.first.org/cvss/
- National Institute of Standards and Technology. (2019). *NIST Special Publication 800-40 Revision 4: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-40r4.

XIII. MODIFICACIONES DEL DOCUMENTO:

SÍNTESIS DE MODIFICACIONES			RESPONSABLE MODIFICACIÓN	APROBADO POR DIRECTOR
VERSIÓN	FECHA	CAUSA DE MODIFICACIÓN		
01	09/2025	Creación del Documento	Enzo Mayo G. Encargado Ciberseguridad	Dr. Patricio Barría

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

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 Andrea Benítez Ugarte, Profesional Unidad de Calidad y Seguridad del Paciente
3. Christian Echeverría A., Subdirector Administrativo y Financiero

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

Firmado por:
Camila Andrea Benítez Ugarte
Profesional Unidad Calidad y Seguridad del Paciente
Fecha: 26-09-2025 13:53 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Firmado por:
Christian Irving Echeverría Aburto
Subdirector Gestión Administrativa y Financiera
Fecha: 26-09-2025 15:11 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Firmado por:
Susana Ximena Avendaño Durán
Jefatura Tic
Fecha: 30-09-2025 17:08 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654

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 vulnerabilidades"*, 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: 06-11-2025 16:44 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 de Gestión y Desarrollo de las Personas.
5. Departamento de Planificación y Desarrollo.
6. Unidad de Calidad y Seguridad del Paciente.
7. Unidad de Auditoría.
8. Asesoría Jurídica.
9. Oficina de Partes.

XASV

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/6RTHG5-654