Asesoría jurídica

Mat.: Aprueba *"Procedimiento de Gestión de Derechos de Acceso"*.

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)

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/T4LUP9-602

CONSIDERANDO

a) Que, el Hospital de Urgencia Asistencia Pública, como establecimiento autogestionado de alta complejidad y nodo crítico de la red asistencial, debe garantizar la seguridad, integridad y disponibilidad de la información clínica y administrativa, resguardando los datos personales y sensibles de pacientes y funcionarios conforme a la normativa vigente.

b) Que, el control adecuado de los derechos de acceso a sistemas, redes y recursos tecnológicos constituye un componente esencial de la seguridad de la información, siendo reconocido por estándares internacionales como NCh-ISO/IEC 27001 y 27002, y por la legislación nacional aplicable en materia de protección de datos, firma electrónica y delitos informáticos.

c) Que, el presente Procedimiento de Gestión de Derechos de Acceso establece un marco formal y estandarizado para la creación, modificación, revisión, uso y revocación de credenciales institucionales, asegurando trazabilidad, control de privilegios, asignación basada en funciones y medidas oportunas ante movimientos de personal, incidentes o contingencias operativas.

d) Que, este instrumento define roles y responsabilidades para la Unidad de Tecnologías de la Información, el Encargado de Ciberseguridad, las jefaturas, los propietarios de activos de información, usuarios internos y prestadores externos, incorporando criterios de auditoría, supervisión continua, gestión de riesgos y mecanismos de excepción debidamente regulados.

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/T4LUP9-602

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 de Gestión de Derechos de Acceso"*, dicto la siguiente:

RESOLUCIÓN

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

Servicio de Salud Metropolitano Central – Ministerio de Salud	PROCEDIMIENTO DE GESTION DE DERECHOS DE ACCESO				
	CÓDIGO UTIC	VERSIÓN 01	FECHA 11/2025	VIGENCIA 5 años	N° PÁGINAS 19

HOSPITAL DE URGENCIA ASISTENCIA PUBLICA

Revisado Por:	Aprobado Por:
FIRMA ELECTRONICA AVANZADA – GOBIERNO DE CHILE Firmado por: Karla Andrea Alfaro Flores Jefatura Calidad y Seguridad del Paciente Fecha: 10-12-2025 17:42 CLT Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río	FIRMA ELECTRONICA AVANZADA – GOBIERNO DE CHILE Firmado por: Patricio Raúl Barría Ailef Director Huap Fecha: 10-12-2025 18:20 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/T4LUP9-602

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/T4LUP9-602

ÍNDICE:

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/T4LUP9-602

I.INTRODUCCIÓN:

El control de accesos a los sistemas de información constituye un componente esencial para garantizar la confidencialidad, integridad y disponibilidad de los datos clínicos y administrativos en el Hospital de Urgencia Asistencia Pública. La evidencia internacional demuestra que gran parte de los incidentes de seguridad de la información se producen por accesos indebidos o mal gestionados, lo que puede generar riesgos de filtración de datos sensibles, afectación a la continuidad de la atención de salud y vulneración de la privacidad de los pacientes.

En Chile, la protección de los datos personales y de la información en salud se encuentra regulada por la Ley N° 19.628 sobre protección de la vida privada, la Ley N° 19.799 sobre documentos electrónicos y firma digital, la Ley N° 21.459 sobre delitos informáticos, además de las normas internacionales NCh-ISO/IEC 27001 y 27002, que establecen lineamientos para la gestión segura de accesos.

La población objetivo de este protocolo corresponde a todos los funcionarios del HUAP (planta, contrata, honorarios y suplentes), así como a los prestadores externos y proveedores que requieran acceso a sistemas institucionales

II.OBJETIVOS:

General

Establecer el procedimiento para la gestión de derechos de acceso a los sistemas de información y recursos tecnológicos del Hospital de Urgencia Asistencia Pública (HUAP), con el fin de resguardar la seguridad de la información institucional y dar cumplimiento a la normativa legal vigente.

Específicos

- Implementar controles administrativos y técnicos que aseguren la asignación, modificación y revocación de accesos de forma oportuna y segura.

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/T4LUP9-602

- Garantizar la trazabilidad y revisión periódica de los derechos de acceso otorgados a funcionarios y terceros, minimizando el riesgo de accesos indebidos o no autorizados.

III.ALCANCE:

Este protocolo está dirigido a todas y todos los funcionarios del Hospital de Urgencia Asistencia Pública (HUAP), incluyendo personal de planta, contrata, suplencias, honorarios y reemplazos, así como a prestadores externos y proveedores que, en el marco de sus funciones, requieran acceso a sistemas de información, aplicaciones, redes o recursos tecnológicos institucionales.

IV.DEFINICIONES:

- **HUAP:** Hospital de Urgencia Asistencia Pública.
- **Usuario/a:** Persona autorizada para acceder a un sistema de información o recurso tecnológico institucional.
- **Credencial:** Conjunto de datos (usuario y contraseña, tarjeta, token u otro medio) que permite autenticar la identidad de un/a usuario/a.
- **Autenticación:** Proceso de verificación de la identidad de un/a usuario/a antes de otorgar acceso a un sistema.
- **Autorización:** Proceso mediante el cual se otorgan permisos y privilegios específicos a un/a usuario/a.
- **Privilegio:** Nivel de acceso o conjunto de permisos asignados a un/a usuario/a dentro de un sistema de información.
- **Rol:** Conjunto predefinido de permisos que corresponden a una función laboral determinada (ej.: administrativo/a, clínico/a, jefe/a de servicio).
- **Revocación:** Acción de retirar o deshabilitar los accesos otorgados a un/a usuario/a.
- **Norma ISO/IEC 27001:** Estándar internacional para la gestión de la seguridad de la información.
- **Revocación oportuna:** Acción de deshabilitar accesos en un plazo máximo definido tras una desvinculación o cambio de funciones.
- **Acceso privilegiado:** Cuenta con permisos elevados o de administración sobre sistemas o bases de datos.

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/T4LUP9-602

V.RESPONSABLES:

Responsable de la Ejecución

Unidad de Tecnologías de la Información (TIC):

- Crear, modificar y revocar cuentas en sistemas institucionales, redes, aplicaciones clínicas/administrativas y correos institucionales, conforme a las solicitudes autorizadas.
- Ejecutar la revocación de accesos dentro de 24 horas hábiles tras ser notificada una desvinculación, suspensión o traslado.
- Mantener registros actualizados de accesos otorgados, privilegios habilitados, fechas de creación, modificación y revocación.
- Resguardar y respaldar los registros y logs asociados por un período mínimo de 5 años.
- Habilitar accesos temporales, bloquear credenciales o aplicar medidas contingentes ante incidentes o fallas técnicas.
- Procesar las solicitudes ingresadas por el canal formal (formulario oficial o, en casos excepcionales, correo institucional desde jefatura).

Jefaturas de Unidad o Funcionales:

- Solicitar la creación, modificación o baja de accesos mediante el canal formal definido en este procedimiento.
- Validar el perfil de acceso requerido según las funciones del cargo.
- Informar de manera inmediata desvinculaciones, traslados o licencias prolongadas (mayores a 30 días).
- Solicitar la creación, modificación o eliminación de correos institucionales, cuando aplique.

Unidad de Gestión y Desarrollo de las Personas (RRHH):

- Notificar ingresos, términos de contrata, reemplazos, licencias prolongadas y desvinculaciones a TIC.
- Entregar mensualmente una nómina consolidada de movimientos de personal.

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/T4LUP9-602

- Mantener coordinadamente con TIC un registro actualizado del personal activo.

Propietarios/as de Activos de Información:

Son responsables de los sistemas o datos bajo su administración:

- Definir los niveles de acceso y privilegios requeridos, en su rol de administradores funcionales del sistema, en coordinación con la jefatura de la unidad donde se desempeña el usuario.
- Autorizar expresamente accesos a información crítica o sensible.
- Participar en revisiones semestrales de accesos vigentes.
- En el caso de sistemas gubernamentales o normados (SIGFE, Mercado Público, DPI, Ley Lobby, etc.), informar a los administradores institucionales correspondientes cuando existan altas o bajas de cuentas, dada la obligación de auditoría externa.

Usuarios/as (Funcionarios/as y Terceros):

- Cambiar la contraseña inicial en el primer ingreso.
- Resguardar adecuadamente sus credenciales, quedando estrictamente prohibido compartirlas.
- Informar inmediatamente la pérdida, robo o sospecha de uso indebido de credenciales a su jefatura y a TIC.

Responsable de la Supervisión

Encargado de Ciberseguridad y Seguridad de la Información:

- Supervisar el cumplimiento de las directrices establecidas, incluidos los plazos de creación y revocación de cuentas.
- Revisar periódicamente los accesos privilegiados y coordinar medidas correctivas.
- Establecer lineamientos técnicos para auditoría, control y eliminación de accesos.
- Evaluar los incidentes relacionados con credenciales o uso indebido.
- Reportar hallazgos y desviaciones al Comité de Ciberseguridad del HUAP.

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/T4LUP9-602

Responsable de Evaluación

Auditoría Interna o Externa (cuando aplique):

- Verificar la trazabilidad y documentación de las cuentas creadas, modificadas o revocadas.
- Evaluar el cumplimiento de los plazos definidos para la revocación de accesos.
- Revisar el resguardo del registro histórico de accesos, conforme a la normativa vigente.
- Emitir informes de hallazgos y solicitar planes de mejora.
- Recomendar actualizaciones al procedimiento según la normativa aplicable o brechas detectadas.

VI. DESARROLLO DEL PROCESO

El procedimiento comienza con la **solicitud formal** de creación, modificación o revocación de accesos a sistemas, redes o aplicaciones institucionales.

Todas las solicitudes deben ser realizadas **exclusivamente por la jefatura directa** del funcionario/a o prestador/a externo, mediante el **sistema institucional de solicitudes**.

Solicitud vía plataforma institucional (canal único y oficial)

Las jefaturas autorizadas deberán gestionar todas las solicitudes a través de la plataforma:

http://solicitudes.hhuap.local/

Dentro del sistema:

1. La jefatura accede con sus **credenciales institucionales**.
2. Se despliegan los **formularios disponibles**, según el tipo de acceso requerido (por ejemplo: creación de cuenta de correo, accesos a sistemas clínicos o administrativos, modificación de permisos, revocación de accesos, etc.).

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/T4LUP9-602

3. Cada formulario presenta **sus propios campos obligatorios**, los cuales **varían según el sistema o tipo de acceso solicitado**.
4. La jefatura debe completar toda la información requerida y enviar la solicitud.

El sistema registra automáticamente:

- la solicitud,
- la trazabilidad,
- el usuario que la ingresó,
- y la fecha y hora de envío.

Las solicitudes incompletas o incorrectamente ingresadas podrán ser devueltas para corrección.

Plazos de atención según tipo de sistema:

Sistemas Clínicos (con administración externa)
Incluye sistemas clínicos que no son desarrollados ni administrados por TIC, sino por proveedores externos, tales como SINA, Imagenología, Laboratorio y otros sistemas clínicos contratados**.**

- **Creación o habilitación de accesos en SINA:** hasta **8 horas hábiles**, según los tiempos establecidos por el proveedor externo.

- **Creación o habilitación de accesos en otros sistemas clínicos externos:** hasta **1 día hábil**, cuando no existan validaciones adicionales.
- **Modificación de permisos:** hasta **1 día hábil**, sujeto a la disponibilidad del proveedor externo.

- **Sistemas con validación o administración externa:** El plazo máximo será de hasta **1 día hábil**, siempre que el sistema lo permita. Sin embargo, los plazos pueden variar según los tiempos de respuesta del proveedor o administrador funcional externo.

Sistemas No Clínicos (correo electrónico, red, accesos administrativos)

- **Creación de correo institucional:** hasta **72 horas hábiles**.
- **Otros accesos administrativos o de red:** hasta **24 horas hábiles**.

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/T4LUP9-602

Casos excepcionales

Si la plataforma se encuentra temporalmente fuera de servicio y la situación afecta la continuidad operativa o corresponde a un incidente crítico de seguridad, se permitirá un mecanismo excepcional.
En estos casos:

- La jefatura deberá indicar explícitamente el carácter de **urgencia**,
- Entregar la información mínima necesaria para ejecutar la acción,
- Regularizar la solicitud en la plataforma una vez restablecido el servicio.

Canales informales no se aceptan

No se procesarán solicitudes enviadas por vías no oficiales, tales como:

- WhatsApp
- Mensajes personales
- Llamadas o instrucciones verbales
- Redes sociales

Sólo se consideran válidas las solicitudes ingresadas mediante la **plataforma institucional** o el mecanismo excepcional autorizado en contingencias.

El proceso se desarrolla según el flujo descrito en el **Anexo 1 – Flujograma de Gestión de Accesos**.

Identificación y autorización

- **Recursos Humanos** notificará a la Unidad de Tecnologías de la Información (TIC) sobre ingresos, traslados o desvinculaciones de personal.

- Mensualmente, RRHH entregará a TIC una **nómina consolidada de movimientos** para mantener actualizado el control de accesos vigentes.

- Las desvinculaciones inmediatas o críticas deben ser notificadas a TIC **dentro de las 24 horas hábiles** siguientes.
- La **jefatura directa** es responsable de validar el perfil de acceso requerido y autorizar formalmente la solicitud mediante la plataforma institucional.

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/T4LUP9-602

Creación de cuentas y credenciales

- TIC crea las cuentas correspondientes en **Active Directory**, sistemas clínicos y administrativos, según corresponda.

- TIC gestiona la **habilitación, modificación o eliminación de correos institucionales**, cuando la jefatura lo solicita. Esto incluye:
  - Creación de casillas,
  - Cambios de nombre o unidad,
  - Alias o redirecciones,
  - Eliminación de cuentas por término de funciones,
  - Respaldos conforme a normativa vigente.

- Debido a la disponibilidad limitada de casillas, la creación de un nuevo correo institucional requerirá que la jefatura **solicite la eliminación de una cuenta existente** asociada a su unidad.
- TIC no gestionará nuevas casillas sin la instrucción formal de eliminación previa.
- La contraseña inicial es generada por TIC y debe ser cambiada por el usuario en su primer acceso. La contraseña debe cumplir con los siguientes requisitos mínimos:
  - Longitud mínima de 8 caracteres
  - Debe incluir al menos una letra mayúscula, una minúscula, un número y un carácter especial (por ejemplo: @, #, $, etc.)
  - No puede ser una palabra común o fácilmente adivinable

- Todas las contraseñas tienen una vigencia máxima de **tres (3) meses**; el sistema notificará automáticamente su vencimiento.

Gestión de accesos en sistemas gubernamentales o normados

Para plataformas gubernamentales o sujetas a regulación externa (por ejemplo: SIGFE, Mercado Público, Ley de Lobby, DPI, entre otras), la creación, modificación o revocación de usuarios deberá ser informada al administrador o responsable institucional de cada sistema.

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/T4LUP9-602

- **Los administradores o responsables institucionales de cada sistema** serán los encargados de ejecutar las gestiones de creación, modificación, habilitación, suspensión o cierre de cuentas, conforme a los lineamientos establecidos por el organismo externo correspondiente.

- **TIC no gestiona directamente la habilitación o modificación de usuarios en estas plataformas**, pero deberá apoyar en:
  - La coordinación técnica cuando se requiera acceso a equipos, configuraciones de red o permisos locales.
  - La verificación de que el funcionario cuenta con credenciales institucionales activas (correo corporativo, red, etc.).
  - El registro interno de las solicitudes recibidas desde las jefaturas.

- Algunos sistemas pueden requerir documentación adicional, trazabilidad, firma electrónica o validaciones externas, lo que deberá ser considerado por los administradores institucionales para efectos de cumplimiento de plazos.

- Todas las gestiones relacionadas con sistemas gubernamentales deberán quedar registradas por los administradores institucionales correspondientes, con el fin de mantener trazabilidad para auditorías internas o externas.

Gestión y uso de credenciales

- Se prohíbe estrictamente **compartir credenciales** o almacenarlas en lugares visibles o de acceso público.

- Se prohíbe **guardar credenciales, correos, claves de sistemas o datos de autenticación en los computadores institucionales**, incluyendo navegadores, clientes de correo o aplicaciones que permitan recordar contraseñas

- Cualquier alteración no autorizada de equipos, configuraciones o antivirus constituye incumplimiento del protocolo.

- Los usuarios son responsables del uso seguro de sus credenciales.

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/T4LUP9-602

- Ante sospechas de uso indebido, pérdida o vulneración, el usuario debe informar de inmediato a su jefatura y a TIC.

Revisión y control de accesos

- El **Encargado de Ciberseguridad y Seguridad de la Información** supervisa los accesos privilegiados y coordina acciones correctivas ante incidentes.

- TIC mantiene un registro actualizado de todas las cuentas institucionales, incluyendo:
  - Fechas de creación,
  - Modificación,
  - Revocación,
  - Privilegios especiales.

- Se realizarán revisiones semestrales en conjunto con los propietarios de activos de información para verificar accesos vigentes y detectar repositorios sin protección adecuada.

Revocación de accesos

- La jefatura directa deberá solicitar la baja de accesos de manera inmediata y, en todo caso, dentro de un plazo máximo de 4 horas hábiles desde que se conozca el movimiento de personal (desvinculación, traslado, suspensión de funciones o licencias prolongadas).

- TIC ejecutará la revocación en un plazo máximo de **24 horas hábiles** desde la notificación.
- RRHH, TIC y Seguridad de la Información mantendrán actualizados los registros de personal activo y accesos asociados.
- Toda revocación deberá quedar registrada, indicando fecha, responsable y detalle de la acción.

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/T4LUP9-602

Término del Protocolo

El protocolo finaliza cuando TIC confirma que la creación, modificación o revocación solicitada fue:

- ejecutada correctamente,
- documentada,
- registrada en la base de datos institucional de usuarios.

VII.CONTINGENCIAS

En caso de presentarse situaciones que impidan la gestión normal de los derechos de acceso, se aplicarán las siguientes medidas de contingencia:

Falla del sistema o red:

- Si los sistemas de autenticación, red o correo institucional se encuentran fuera de servicio, la Unidad de Tecnologías de la Información deberá:
- Notificar la situación al Encargado de Ciberseguridad y Seguridad de la Información y a las jefaturas afectadas.
- Habilitar accesos temporales o alternativos según evaluación técnica y el nivel de criticidad definido por la Unidad de Tecnologías de la Información en coordinación con el Encargado de Ciberseguridad y Seguridad de la Información. El tiempo de respuesta dependerá del nivel de criticidad establecido (alta: respuesta inmediata; media: hasta 4 horas hábiles; baja: hasta 24 horas hábiles).
- Registrar las acciones ejecutadas y regularizar los accesos una vez restablecido el sistema.

Imposibilidad de revocar accesos a tiempo:

- Si por causas técnicas no es posible desactivar una cuenta dentro del plazo establecido, la Unidad de Tecnologías de la Información deberá:
- Bloquear temporalmente las credenciales o cambiar la contraseña para evitar su uso.

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/T4LUP9-602

- Informar al Encargado de Ciberseguridad y Seguridad de la Información y dejar constancia en el registro de incidentes.
- Completar la revocación definitiva una vez solucionado el inconveniente.

Pérdida, robo o uso indebido de credenciales:

- El usuario afectado deberá informar de inmediato a su jefatura y a la Unidad de Tecnologías de la Información.
- La Unidad de Tecnologías de la Información procederá al bloqueo preventivo de la cuenta y emitirá nuevas credenciales si corresponde.
- El Encargado de Ciberseguridad y Seguridad de la Información evaluará la necesidad de acciones adicionales o reporte al Comité de Ciberseguridad.

Incidentes de seguridad o accesos no autorizados:

- Se deberá activar el Procedimiento de Gestión de Incidentes de Seguridad de la Información del HUAP.
- Toda acción o resultado será documentado en el registro oficial de incidentes.

VIII. REGISTROS

Los registros asociados a la gestión de accesos deben mantenerse actualizados, seguros y disponibles para auditorías internas o externas.

La Unidad de Tecnologías de la Información (UTIC) será responsable de conservar y respaldar esta información en el repositorio institucional que defina para tales fines, asegurando su disponibilidad, integridad y trazabilidad.

Los registros deberán conservarse por un período mínimo de 5 años, conforme a las políticas institucionales de gestión documental.

IX. DIFUSIÓN

El protocolo se difundirá de manera accesible y comprensible para las áreas involucradas, mediante:

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/T4LUP9-602

- Envío de correo electrónico informativo a todas las unidades del hospital.
- Publicación en el repositorio documental institucional.

X.REVISIÓN

El procedimiento deberá revisarse al menos una vez al año, o antes si ocurre alguna de las siguientes situaciones:

- Cambios relevantes en los sistemas TIC o procesos de acceso.
- Actualización normativa o de políticas institucionales.
- Incidentes que evidencien fallas en la aplicación del procedimiento.

Responsables de la revisión:
Encargado de Ciberseguridad y Seguridad de la Información y Jefatura de la Unidad de Tecnologías de la Información, en coordinación con el Comité de Ciberseguridad del HUAP.

El resultado de la revisión deberá registrarse en el apartado “Modificaciones del Documento”.

XI.EXCEPCIONES AL CUMPLIMIENTO

Podrán solicitarse excepciones a este procedimiento en casos justificados, mediante correo formal dirigido a la Jefatura de TIC, con copia al Comité de Ciberseguridad.

Toda solicitud deberá incluir:

- Descripción del caso y motivo de la excepción.
- Riesgos identificados y medidas de control alternativas.
- Plazo máximo de vigencia (hasta 6 meses).

La aprobación corresponde a la Jefatura de TIC, con visto bueno del Encargado de Ciberseguridad y Seguridad de la Información, mediante respuesta formal por correo electrónico, en la que se indique explícitamente:

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/T4LUP9-602

- La aceptación de la excepción solicitada.
- Las condiciones o controles compensatorios que deberán aplicarse.
- El período autorizado de vigencia.

Las excepciones deberán registrarse y revisarse antes de su vencimiento.

XII.DISTRIBUCIÓN

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

XIII.REFERENCIAS BIBLIOGRÁFICAS

- Instituto Nacional de Normalización. (2013). *NCh-ISO 27001.Of2013: Sistemas de gestión de la seguridad de la información*. Santiago, Chile: INN.
- International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls*. Ginebra, Suiza: ISO/IEC.
- Ministerio de Salud de Chile. (2025). *Orientaciones técnicas sobre ciberseguridad y continuidad operativa (COMGES 2025)*. Santiago, Chile: MINSAL.

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/T4LUP9-602

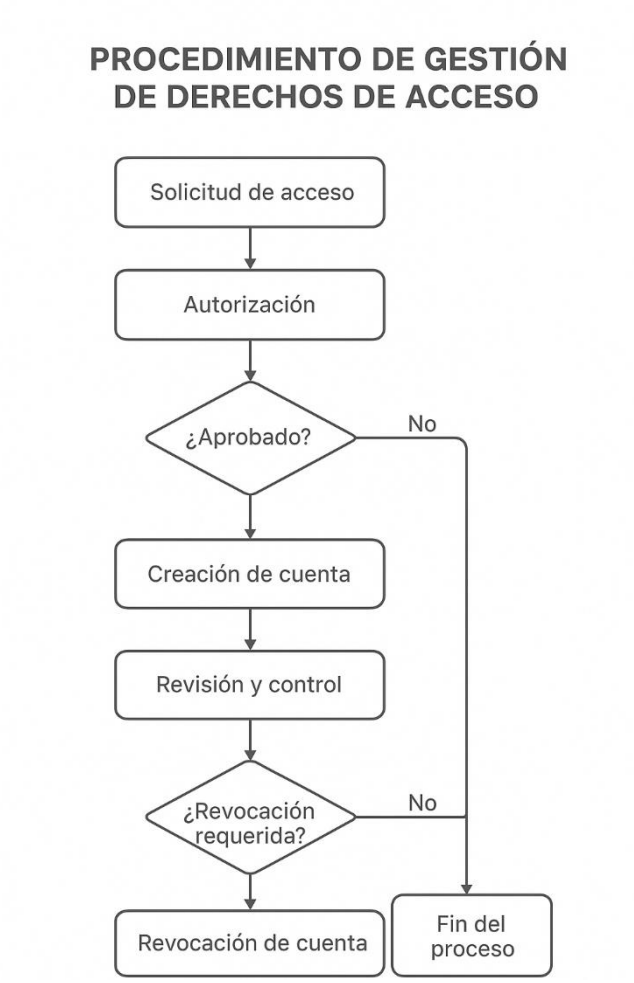
XIV.MODIFICACIONES DEL DOCUMENTO

SÍNTESIS DE MODIFICACIONES			RESPONSABLE MODIFICACIÓN	APROBADO POR DIRECTOR
VERSIÓN	FECHA	CAUSA DE MODIFICACIÓN		
01	11/2025	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/T4LUP9-602

XV.ANEXOS

Anexo 1. Flujograma del Procedimiento de Gestión de Derechos de Acceso



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/T4LUP9-602

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
4. Ps. Jorge Hurtado A., Subdirector (s) de Gestión y Desarrollo de las Personas

FIRMA ELECTRONICA AVANZADA · GOBIERNO DE CHILE

Firmado por:
Camila Andrea Benítez Ugarte
Profesional Unidad Calidad y Seguridad del Paciente
Fecha: 01-12-2025 08:35 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Firmado por:
Susana Ximena Avendaño Durán
Jefatura Tic
Fecha: 01-12-2025 12:29 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Firmado por:
Christian Irving Echeverría Aburto
Subdirector Gestión Administrativa y Financiera
Fecha: 01-12-2025 16:16 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Firmado por:
Jorge Eduardo Hurtado Almonacid
Subdirector de Gestión y Desarrollo de Personas
Fecha: 03-12-2025 13:27 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/T4LUP9-602

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 de Gestión de Derechos de Acceso"*, 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 09:53 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. Subdirección Administrativa y Financiera.
6. Unidad de Calidad y Seguridad del Paciente.
7. Unidad de Tecnologías de la Información.
8. Asesoría Jurídica.
9. Oficina de Partes.

ÍJVE(S)

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/T4LUP9-602