SERVICIO DE SALUD TALCAHUANO
SUBDIRECCIÓN ADMINISTRATIVA
ÁREA DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN
HOSPITAL DE TOMÉ

TOMÉ, 28 OCTUBRE 2025

VISTOS:

Considerando el Decreto Fuerza Ley N° 01/24.04.2006 del MINSAL; el D.F.L. N° 29/2004 sobre Estatuto Administrativo; la Ley N° 19.880 sobre Bases de los Procedimientos Administrativos; la Resolución N° 6/2019 de Contraloría sobre exención de toma de razón en materias de personal; los Decretos Supremos de Salud N° 140/2005 y N° 38/2005 que aprueban los Reglamentos Orgánicos de los Servicios de Salud y de los Establecimientos de Salud de Menor Complejidad; la Resolución Exenta N° 2778/2023 del SSThno; la Resolución Exenta N° 1251/2023 que aprueba la Política General de Seguridad de la Información del Hospital de Tomé; el COMGES 2025; y el Ordinario N° 943/2025 del Subsecretario de Redes Asistenciales sobre implementación de controles críticos de seguridad de la información según ISO/IEC 27001:2022; que, conforme al D.S. N° 285/2022 y la Ley N° 21.663 de Ciberseguridad, el Hospital de Tomé se encuentra incluido en la lista preliminar de **Operadores de Importancia Vital (OIV)**; y que, mediante la Providencia N° DHT-6553 y el oficio N° 0106 clasificado como secreto, se instruye evacuar un Informe Técnico Fundado respecto del cumplimiento de los criterios del artículo 4° del D.S. N° 285/2022, se da curso a la presente comunicación.

CONSIDERANDO:

1. Que la adecuada gestión de los derechos de acceso a los sistemas, aplicaciones, datos e instalaciones del Hospital de Tomé es fundamental para garantizar la confidencialidad, integridad y disponibilidad de la información institucional.
2. Que el Sistema de Gestión de Seguridad de la Información (SGSI) y la Política de Seguridad de la Información Institucional establecen lineamientos para la protección de los activos de información y la implementación de controles críticos, en concordancia con la ISO/IEC 27001:2022 y las orientaciones del Ordinario N° 943/2025 del Subsecretario de Redes Asistenciales.
3. Que el COMGES 2025 define lineamientos estratégicos institucionales para la gestión segura de la información y la continuidad operacional.
4. Que la implementación de procedimientos de gestión de derechos de acceso permite mitigar riesgos asociados a accesos no autorizados, uso indebido de información y posibles incidentes de seguridad informática, cumpliendo con la normativa vigente, incluyendo el Decreto Fuerza Ley N° 01/2006, el D.F.L. N° 29/2004 y la Ley N° 21.663 de Ciberseguridad.
5. Que resulta necesario establecer una política institucional de derechos de acceso que asegure la asignación, control, modificación y revocación segura de los accesos, de acuerdo con los principios de mínimo privilegio y segregación de funciones, resguardando la operación institucional y los datos sensibles del Hospital de Tomé.

RESOLUCIÓN EXENTA N° 2124

1. **APRUEBASE** la Política de Gestión de Derechos de Acceso del Hospital de Tomé, en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) y de la Política de Seguridad de la Información Institucional, estableciendo lineamientos, responsabilidades y procedimientos para la asignación, control, modificación y revocación de accesos a sistemas, aplicaciones, datos e instalaciones.

SERVICIO DE SALUD TALCAHUANO
SUBDIRECCIÓN ADMINISTRATIVA
ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
HOSPITAL DE TOMÉ

2. **DISPONGASE** que la presente política sea implementada, difundida y cumplida por todos los servicios, unidades y funcionarios del Hospital de Tomé, incluyendo personal a honorarios y terceros que presten servicios, asegurando la protección de los activos de información y la continuidad operacional.
3. **ENCARGUESE** a la Unidad de Tecnologías de la Información y Comunicaciones (TIC) y al Responsable de Ciberseguridad la supervisión, control y actualización periódica de los procedimientos de gestión de derechos de acceso, asegurando la trazabilidad de todas las acciones y reportando cualquier incidencia significativa a la Dirección del establecimiento y al Comité de Seguridad de la Información.
4. **DEJASE CONSTANCIA** que la presente resolución entra en vigor a partir de su publicación y que cualquier modificación futura deberá efectuarse mediante resolución exenta de la autoridad competente.

"ANÓTESE Y COMUNÍQUESE"

LEC/CCU/ccu
N° INT. 02/28.10.2025
DISTRIBUCIÓN:

- Subdirección Administrativa H. Tomé
- Oficina de Partes Hospital de Tomé
- CR. Apoyo Diagnóstico
- Área Recursos Físicos
- Área Gestión y Desarrollo de las Personas
- CR. Atención Cerrada
- CR. Atención Abierta
- CR. Emergencia

FIRMA DIRECTOR HOSPITAL DE TOMÉ ELECTRONICA

Firmado por Aníbal Antonio Cea Henríquez
Fecha 28/10/2025 15:09:48 CLST

PUEDE VALIDAR ESTE DOCUMENTO CON EL SIGUIENTE CODIGO:309248-51708
EN LA SIGUIENTE URL: https://sstalcahuano.cl/validador_panel

POL03-25-0002

POLITICA DE SEGURIDAD PARA LA GESTION DE DERECHOS DE ACCESO

Sistema de Gestión de Seguridad de la Información – Hospital de Tomé

Versión Oficial Actual 1 – Julio 2025

Contenido

1 PRÓPOSITO 3
2 ALCANCE O AMBITO DE APLICACIÓN 3
3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS 3
4 ROLES Y RESPONSABILIDADES 4
5 DIRECTRICES 4
5.1 Derechos de Accesos 4
5.2 Accesos a las redes y a los servicios de la red 5
5.3 Control de acceso a la Información 5
5.4 Administración del acceso 5
5.5 Provisionamiento de Acceso (Alta de Usuarios): 6
5.6 Gestión de Cambios de Acceso: 6
5.7 Revocación de Acceso (Baja de Usuarios): 6
5.8 Gestión de Cuentas Privilegiadas 7
5.9 Segregación de funciones 7
5.10 Revisión de los derechos de acceso 7
6 MECANISMO DE DIFUSIÓN. 8
7 PERÍODO DE REVISIÓN. 8
8 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA 8
9 HISTORIAL Y CONTROL DE VERSIONES 8

1 PRÓPOSITO

Este procedimiento establece los lineamientos y controles para la gestión segura de los derechos de acceso a los sistemas, aplicaciones, datos e instalaciones del Hospital de Tomé. El objetivo es asegurar que solo los usuarios autorizados tengan acceso a los recursos necesarios para desempeñar sus funciones, minimizando el riesgo de acceso no autorizado, uso indebido o divulgación de información sensible.

2 ALCANCE O AMBITO DE APLICACIÓN

Es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), así como al personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para el Hospital de Tomé.

Esta política abarca los siguientes controles definidos en la norma NCh-ISO 27002:2013, denominada "Tecnologías de la información-Técnicas de seguridad-Códigos de prácticas para los controles de seguridad de la información" y, en específico:

- A.09.01.01 Política de control de acceso
- A.09.01.02 Accesos a las redes y a los servicios de la red
- A.09.02.02 Asignación de acceso de usuario
- A.09.04.01 Restricción del acceso a la información
- A.09.04.02 Procedimientos de inicio de sesión seguro
- A.09.04.04 Uso de programas utilitarios privilegiados
- A.09.04.05 Control de acceso al código fuente de los programas

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- Marco Normativo
  - NCh-ISO27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
  - Ley N° 19.628, de Protección de vida privada y datos personales.
  - Ley N° 19.799, de firmas y documentos electrónicos.
  - Ley N° 19.927, de Delitos de Pornografía Infantil.
  - Ley N° 20.285 regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado.
  - Ley N° 21.180, de Transformación Digital del Estado.
  - Ley N° 21.459, que 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.
  - Decreto N° 83, 2004, Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
  - El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
    - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
    - Leyes relacionadas

- **Documentos Relacionados**
  - Procedimiento gestión derechos de acceso y devolución de activos [1].

- Política Seguridad de la Red [2].

4 ROLES Y RESPONSABILIDADES

- **Responsable de Ciberseguridad:** Responsable general de la gestión de derechos de acceso, incluyendo la definición de políticas, la supervisión del proceso y la comunicación con la alta dirección.
- **Administradores de Sistemas/Aplicaciones:** Responsables de la implementación técnica de los derechos de acceso en los sistemas y aplicaciones.
- **Propietarios de Datos/Aplicaciones:** Responsables de definir los niveles de acceso requeridos para sus respectivos datos y aplicaciones.
- **Responsables de Recursos Humanos:** Responsables de la gestión del ciclo de vida de los usuarios (alta, baja, cambios de rol) y la comunicación con el área de TI sobre las necesidades de acceso.

5 DIRECTRICES

5.1 Derechos de Accesos

- Los derechos de acceso se otorgarán únicamente cuando exista una necesidad legítima y justificada para el desempeño de las funciones del usuario.
- Se otorgará el nivel mínimo de acceso necesario para que el usuario pueda realizar sus tareas. Se evitarán los accesos amplios o genéricos.
- Se implementará la segregación de funciones para prevenir que una sola persona tenga control sobre procesos críticos que pudieran permitir actividades fraudulentas o no autorizadas.
- Cada usuario es responsable del uso adecuado y seguro de sus credenciales de acceso. No se deben compartir contraseñas ni permitir el acceso a cuentas propias por parte de terceros.
- Todos los usuarios deben conocer y cumplir con las políticas de seguridad del Hospital de Tomé relacionadas con la gestión de derechos de acceso.
- El modelo de roles y los derechos de acceso asignados se revisarán y actualizarán periódicamente para reflejar los cambios en las funciones, responsabilidades y necesidades del negocio.
- Todas las acciones relacionadas con la gestión de derechos de acceso (solicitudes, aprobaciones, asignaciones, modificaciones, revocaciones) deben ser registradas y trazables.
- Se buscará la automatización de los procesos de gestión de derechos de acceso siempre que sea posible para mejorar la eficiencia y reducir el riesgo de errores humanos.
- Se proporcionará formación y concientización regular a los usuarios sobre la importancia de la seguridad de los accesos y sus responsabilidades.
- La gestión de derechos de acceso se realizará en cumplimiento con la normativa legal vigente y los estándares de la industria aplicable
- Se establecerán procesos que eviten redundancias o demoras administrativas injustificadas, permitiendo una gestión dinámica y control constante durante toda la etapa del proceso de Gestión de Derechos de Acceso.

5.2 Accesos a las redes y a los servicios de la red

Los usuarios solo deben tener acceso a la red y a los servicios de red en los que cuentan con autorización específica.

5.3 Control de acceso a la Información

Todos los funcionarios del Hospital de Tomé, incluso terceros, deberán tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la organización. La asignación de privilegios y acceso a los activos de información deben estar basados en las necesidades de las áreas y aprobados por el propietario de los activos. (Propietario de módulos / Funcionalidades cuando aplique)

Estas necesidades de acceso deben ser determinadas por las respectivas jefaturas, en función de las tareas asignadas al cargo del funcionario.

Para todo medio de procesamiento de información al que se necesite conceder accesos (por ejemplo: servidores, aplicaciones, carpetas compartidas, etc.), el dueño de la Información(cuando aplique) en conjunto con el Área TIC debe designar un responsable del medio, quién será encargado de autorizar los permisos de acceso y solicitar los espacios necesarios.

Sólo se deben conceder accesos a terceros previa solicitud del dueño del medio de procesamiento de información y el dueño de la información (cuando aplique), y nunca antes de haberse firmado un acuerdo de confidencialidad. Las cuentas de acceso a terceros deben tener especificado un tiempo de expiración el que debe ser controlado por el Administrador del sistema.

El Comité de Seguridad de la Información tiene las facultades de suspender o eliminar los accesos a cualquier persona que represente riesgo en la confidencialidad, integridad o disponibilidad de la información.

Cualquier intento de acceso no autorizado a los equipos, carpetas compartidas, sistemas e información será considerado un incidente grave, por lo que debe reportarse de inmediato según lo descrito en el procedimiento de Gestión de Incidentes de Seguridad de la Información.

Ante cualquier daño a un activo de información se procederá de acuerdo con lo descrito en la Política General de Seguridad de la Información (Sanciones) y el Procedimiento Acuerdos de Confidencialidad en contratos con terceros.

5.4 Administración del acceso

La administración de perfiles de usuario en las aplicaciones radica en los usuarios administradores de cada aplicación y las jefaturas de área correspondiente. No obstante, la responsabilidad de asignar un determinado perfil a un usuario puede ser delegada por la Jefatura de la Área solicitante o por aquellos a quienes se les haya autorizado. (Jefes de Unidad)

No se podrá otorgar acceso a los sistemas a ningún usuario hasta que se haya completado el proceso de autorización y registro de acuerdo con el Procedimiento de gestión de derechos de accesos y devolución de activos.

Para facilitar la administración de los accesos, se deben definir perfiles de acceso asignables a grupos de usuarios que, por sus responsabilidades en la organización, presenten necesidades de acceso equivalentes.

El área de Operaciones TIC debe implementar las reglas de control de acceso solicitadas por los Administradores de Aplicación y las Jefaturas de Área correspondiente.

Generalmente esto se realizará a través de la Mesa de Servicio como "Solicitud de Servicio", esto para mantener el registro y las trazas correspondientes.

5.5 Provisionamiento de Acceso (Alta de Usuarios):

- Solicitud de Acceso: El proceso de alta de un nuevo usuario o la necesidad de acceso a nuevos recursos debe iniciarse mediante un formulario de solicitud de acceso formal (Portal de Mesa de Servicio TI). La solicitud debe ser completada por la Jefatura de Área o Unidad y aprobada por el Administrador del Sistema.
- Verificación de la Identidad: Antes de la creación de una cuenta, se debe verificar la identidad del solicitante según las políticas del Hospital de Tomé y específicamente del procedimiento de Vinculación funcionaria de la Unidad de Personal del establecimiento.
- Asignación de Roles y Derechos: Los derechos de acceso deben asignarse basándose en el principio de mínimo privilegio y las responsabilidades del rol del usuario. Se deben utilizar roles predefinidos siempre que sea posible.
- Creación de Cuentas: Las cuentas de usuario se crearán por el Área de Tecnologías por aquellos agentes que tengan los privilegios para ello en los sistemas y aplicaciones necesarios, siguiendo las políticas de seguridad de contraseñas, procedimientos y otras configuraciones de seguridad.
- Documentación: Se debe mantener un registro de todos los usuarios, los roles asignados y los derechos de acceso específicos otorgados, para ello el Área de Tecnología deberá tener acceso a las plataformas de control de usuarios (Maestros) de todos los sistemas a los que tenga responsabilidad de administración. Según inventario de Activos.

5.6 Gestión de Cambios de Acceso:

- Solicitud de Modificación: Cualquier cambio en los derechos de acceso de un usuario (cambio de rol, necesidad de acceso a nuevos recursos, revocación de acceso) debe solicitarse mediante un formulario de modificación de acceso formal y aprobado por las partes correspondientes, manteniendo la lógica de autorización del punto 5.5.
- Revisión y Aprobación: Las solicitudes de modificación deben ser revisadas y aprobadas por el supervisor o responsable directo del usuario (Jefatura) y, si es necesario, por el Administrador de Sistema.
- Implementación de Cambios: Los cambios de acceso se implementarán en los sistemas y aplicaciones de manera oportuna y eficiente. En caso de tratarse de proveedores se deben establecer SLA's acorde a las necesidades de la institución.
- Actualización de la Documentación: El registro de los derechos de acceso del usuario debe actualizarse para reflejar los cambios realizados, esto debe mantener una traza y ser accesible para el Área de Tecnologías siempre que sean Administradores del Activo de Información.

5.7 Revocación de Acceso (Baja de Usuarios):

Ante situación de un cambio de cargo de funcionario, se deben revisar sus permisos de acceso lógico asignados y verificar que éstos sigan siendo válidos de acuerdo con su nueva función. Cuando un funcionario termina su relación laboral con el Hospital de Tomé, todos sus permisos de acceso a la información deben ser revocados.

Es responsabilidad de las Jefaturas Directas informar formalmente las desvinculaciones de acuerdo con lo descrito en el procedimiento de gestión de derechos de acceso y devolución de activos.

- Notificación de Baja: Las Jefaturas o Dueños de Procesos deben notificar al área de TI de la baja de un usuario de manera oportuna y trazable, para ello deberá realizarlo a través del Portal de la Mesa de Servicio TI y seleccionar el servicio correspondiente.
- Revocación Inmediata: El acceso del usuario a todos los sistemas, aplicaciones, datos e instalaciones debe ser revocado de forma inmediata al producirse la baja.
- Eliminación de Cuentas: Las cuentas de usuario deben ser desactivadas y, posteriormente, eliminadas de acuerdo con las políticas de retención de cuentas de Hospital de Tomé
- Recuperación de Activos: Se deben tomar las medidas necesarias para asegurar la devolución de cualquier activo de la organización en posesión del usuario que se da de baja.
- Actualización de Registros: Los registros de acceso deben actualizarse para reflejar la baja del usuario, los administradores de sistemas deben revisar que esto se ejecute correctamente.

5.8 Gestión de Cuentas Privilegiadas

Las cuentas de administración tienen el poder de realizar cualquier acción sobre los sistemas que se administran, por lo que deben ser gestionadas con la máxima precaución. Debiendo cumplir, a lo menos, con lo siguiente:

- Identificación de Cuentas Privilegiadas: Se deben identificar claramente las cuentas con privilegios administrativos o de alto nivel en los sistemas y aplicaciones.
- Restricción de Uso: El uso de cuentas privilegiadas debe estar estrictamente limitado a las tareas administrativas necesarias y autorizado por personal específico.
- Cuentas Dedicadas: Siempre que sea posible, se deben utilizar cuentas dedicadas para tareas administrativas, separadas de las cuentas de usuario estándar.
- Gestión de Contraseñas: Las contraseñas de cuentas privilegiadas deben ser robustas, únicas y gestionadas de forma segura (ej. mediante bóvedas de contraseñas).
- Auditoría: El uso de cuentas privilegiadas debe ser auditado y monitoreado de forma regular por el ESI.

5.9 Segregación de funciones

Los derechos de acceso deben ser asignados a perfiles individuales, de forma tal que las acciones realizadas con los accesos otorgados sean de responsabilidad directa del funcionario.

El otorgamiento de accesos respecto a recursos de información del Hospital de Tomé debe considerar una adecuada segregación de funciones, de modo que un mismo funcionario no pueda disponer, por su voluntad, del control de un proceso de negocios completo.

Las excepciones a la regla anterior deben ser aprobadas por la Jefatura de Área correspondiente y autorizadas por el Jefe de Área TIC.

5.10 Revisión de los derechos de acceso

La unidad de Tecnologías Digitales es responsable de los accesos de los administradores de aplicaciones, de tal forma que se establezca un control efectivo desde el registro inicial de la cuenta hasta el momento en que requiera ser modificada, revocada o eliminada. Para ello la Unidad de Tecnologías Digitales deberá gestionar los Maestros de usuarios internos o de terceros (Proveedores)

Los derechos de accesos deben ser revisados:

A intervalos regulares no mayores a 6 meses.

- Después de cualquier cambio mayor en la organización.
- Los accesos de cuentas con mayores privilegios deben ser revisados al menos 2 veces al año.

6 MECANISMO DE DIFUSIÓN.

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Portal Mesa de Servicio TI, Sección Ayuda, Seguridad
- Correo Informativo.

7 PERÍODO DE REVISIÓN.

La presente política deberá ser revisada cada dos años o cuando ocurran cambios significativos para garantizar que:

- Sigue siendo adecuado para su propósito y preciso.
- Refleja los cambios en las tecnologías.
- Está alineado con legislación vigente, los estándares internacionales y mejores prácticas.

8 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

En situaciones excepcionales, el Jefe de TIC, el CISO o el Comité de Seguridad de la Información tendrán la facultad de evaluar y establecer condiciones específicas para la excepción al cumplimiento de las directrices establecidas en esta política, siempre que tales excepciones no infrinjan la legislación vigente ni comprometan la seguridad de la información.
Cada excepción deberá ser debidamente documentada, y se deberá iniciar un proceso de revisión de la política en el que se determinará si es necesario incorporar directrices adicionales o realizar modificaciones específicas.

9 HISTORIAL Y CONTROL DE VERSIONES

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio