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 gestión adecuada de identidades y derechos de acceso es esencial para garantizar la confidencialidad, integridad y disponibilidad de los activos de información del Hospital de Tomé.
2. Que el Hospital de Tomé requiere establecer procedimientos claros para la creación, modificación, suspensión y eliminación de cuentas de usuario, roles, permisos y credenciales de acceso a los sistemas de información y recursos tecnológicos, asegurando autenticación, autorización y auditoría adecuadas.
3. Que la correcta implementación de este procedimiento asegura el cumplimiento de normativas nacionales, estándares internacionales ISO/IEC 27001:2013 e ISO/IEC 27002:2013, y demás requerimientos legales, incluyendo la Ley N° 19.628, Ley N° 19.799, Ley N° 19.927, Ley N° 20.285, Ley N° 21.180, Ley N° 21.459 y Ley N° 21.663.
4. Que este procedimiento aplica a todos los funcionarios, personal a honorarios y terceros que interactúen con los sistemas de información del Hospital de Tomé, asegurando que cada usuario mantenga sus accesos, credenciales y permisos bajo control, y que los activos de información sean protegidos ante accesos indebidos.
5. Que la implementación de este procedimiento contribuye a formalizar roles y responsabilidades, gestionar el ciclo de vida de los usuarios, coordinar revisiones periódicas de accesos, capacitación y control de credenciales, así como a garantizar la correcta terminación de accesos ante cambios de funciones o desvinculaciones.

RESUELVE EXENTA N° 2119

1. **APRÚEBASE** el Procedimiento de Gestión de Identidad y Derechos de Acceso del Hospital de Tomé, que establece lineamientos, responsabilidades, flujos de trabajo y mecanismos de control para la creación, modificación, suspensión y eliminación de cuentas de usuario, roles, permisos y credenciales de acceso, en concordancia con

normas nacionales, estándares internacionales y buenas prácticas de seguridad de la información**.**

2. **DISPÓNGASE** que todos los funcionarios, colaboradores, personal a honorarios y proveedores externos que operen en el Hospital de Tomé cumplan estrictamente con los lineamientos establecidos en este procedimiento, incluyendo:
   a) Solicitud y aprobación de creación, modificación y pasivamiento de accesos.
   b) Gestión del ciclo de vida de usuarios y permisos de acceso según requerimientos de jefaturas o Área de Gestión de Personas.
   c) Cumplimiento de los controles de seguridad de la información definidos en NCh-ISO 27001:2013 y 27002:2013.
   d) Confidencialidad y protección de credenciales personales.
   e) Revisión periódica de derechos de acceso y reporte a dueños de proceso.
   f) Recuperación y devolución de activos e información al término de funciones o relación contractual.
   g) Capacitación en políticas de gestión de accesos y seguridad de la información.
   h) Cumplimiento con la Política General de Seguridad de la Información del Hospital de Tomé.
3. **ENCÁRQUESE** a los Administradores de Sistemas, Centro de Servicio TI, Gestores de Acceso, Grupo de Seguridad TI y Dueños de Procesos la supervisión, aplicación, monitoreo y control del cumplimiento de este procedimiento, así como la gestión de incidentes, auditorías y medidas correctivas en caso de incumplimiento.
4. **DEJASE CONSTANCIA** que todo funcionario, colaborador o proveedor que tenga credenciales en los sistemas de información del Hospital de Tomé está afecto a este procedimiento y cumplir con todos los lineamientos, directrices y procedimientos establecidos, asegurando la correcta gestión de accesos y protección de los activos de información.
5. **ESTABLÉCESE** que la presente resolución entra en vigor a partir de su publicación, y cualquier modificación futura deberá efectuarse mediante resolución exenta de la autoridad competente, asegurando la coherencia con las normativas legales y estándares internacionales aplicables.

"ANÓTESE Y COMUNÍQUESE"

LEC/CCU/ccu
N° INT. 05/28.10.2025
DISTRIBUCIÓN:

- Subdirección Administrativa H. Tomé
- Subdirección Médica 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

Firmado por Aníbal Antonio Cea Henríquez
Fecha 28/10/2025 15:09:06 CLST

PROC03-25-0002

PROCEDIMIENTO DE GESTIÓN DE IDENTIDAD Y DERECHOS DE ACCESO

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

Versión Oficial Actual 1 – Julio 2025

Contenido

1 PRÓPOSITO

Establecer las actividades necesarias para la gestión de identidades y derechos de acceso a la información, asegurando una adecuada administración de las autorizaciones y claves de acceso de los usuarios a los activos tecnológicos de la organización.

Administrar el ciclo de vida de los usuarios, desde la creación de las cuentas, roles y permisos necesarios hasta su inoperancia; a partir de los requerimientos reportadoS por el Área de Gestión de Personas y/o directamente de su jefatura directa; lo anterior para que el funcionario tenga acceso adecuado a los sistemas de información y recursos tecnológicos validando su autenticación, autorización y auditoría.

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:

Alcance de Dominios y Controles de Seguridad de la Información (NCh-ISO 27001:2013)		
Nombre del Dominio	**ID Control ISO**	**Nombre del Control**
Seguridad relativa a los recursos humanos	A.07.03.01	Responsabilidades ante la finalización o cambio
Gestión de Activos	A.08.01.04	Devolución de Activos
Control de Acceso	A.09.01.02	Accesos a las redes y a los activos de la red
	A.09.02.01	Registro y cancelación de registro de usuario
	A.09.02.03	Gestión de derechos de acceso privilegiados
	A.09.02.04	Gestión de información secreta de autenticación de usuarios
	A.09.02.05	Revisión de los derechos de acceso de usuario
	A.09.02.06	Eliminación o ajuste de los derechos de acceso
	A.09.04.03	Sistema de gestión de contraseñas

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**
  - Política de Gestión de Acceso.
  - Política Seguridad de la Red.

4 ROLES Y RESPONSABILIDADES

- **Administradores de Sistemas**
  - Gestionar los permisos de acceso a los sistemas de información.
  - Revisar la integridad, disponibilidad y coherencia de los accesos otorgados cada 6 meses y reportar a dueños de proceso.
- **Centro de Servicio TI**
  - Recuperar los activos de información de los funcionarios que se desvinculan
- **Gestores de Acceso (Grupo de TI)**
  - Gestionar los requerimientos de acceso en sistemas propios o con terceros
- **Dueños de Procesos**
  - Responsables de generar las solicitudes de creación, modificación y pasivamiento de accesos a los administradores de sistemas y a la Unidad de Personal
  - Aprobar cuando sea necesario la gestión de un acceso
- **Grupo de Seguridad TI**
  - Coordinar la revisión de gestión de identidad y derechos de acceso de usuarios y, la eliminación de cuentas gestionadas por Administradores de Sistemas.
  - Brindar capacitación a los funcionarios en la Política de Gestión de Acceso.
- **Funcionarios y/o Terceros (usuarios)**
  - Mantener confidenciales las credenciales personales e intransferibles.
  - Cumplir con lo establecido en las Políticas y Procedimientos del Sistema de Gestión Seguridad de la Información (SGSI), en todo lo que sea de su competencia.
  - No divulgar información pertinente al Hospital de Tomé o información que tome en conocimiento producto de acceso y la naturaleza de sus funciones.
  - Comprender la responsabilidad funcionaria, aún fuera de las dependencias de trabajo y fuera del horario normal de trabajo.
  - Hacer traspaso de la información perteneciente al Hospital toda vez cese sus funciones o estas cambien.

- Todos los funcionarios o terceros que tengan credenciales en cualquier plataforma tecnológica del Hospital de Tomé, deberá conocer y cumplir con lo establecido en las Políticas de Seguridad de la Información del Hospital de Tomé

5 DIRECTRICES

5.1 Registro de Usuario

En cualquier registro de usuario se debe utilizar registros únicos para permitir a los usuarios vincularse y ser responsables de sus acciones. No se permitirá procesos alternativos que enmascaren, escondan o limiten procesos de trazabilidad digital de las acciones realizadas en sistemas de información del Hospital de Tomé, lo anterior incluye el uso correcto de la red de datos RCE (Red de Comunicación del Estado), dejando prohibido el uso de redes "personales o móviles" para realizar acciones laborales.

5.1.1 Creación de Accesos para Funcionarios

La solicitud de acceso debe ser realizada por la Jefatura de unidad o área (Dueño de Proceso) con al menos 1 día hábil de anticipación, utilizando los servicios del Portal de Mesa de Servicio TI, Solicitudes de Servicio, Categoría "Gestión de Accesos y Registros" que puede ser accedido desde los códigos QR de los fondos de pantalla o desde el siguiente enlace: https://tic.hospitaldetome.cl. Las solicitudes deben realizarse de manera individualizada y deberán completarse todos los datos solicitados.

Este proceso no incluye el equipamiento o licenciamiento requerido por lo que si el usuario no cuenta con esto la creación de cuenta será cerrada.

Las jefaturas deben asegurar que el usuario (funcionario de ahora en adelante) tenga los recursos necesarios para ejecutar sus funciones según estrategia institucional, presupuesto y prioridades, destacando el acceso:

- A la red de Comunicaciones del Estado
- Al equipo de procesamiento (Computador)
- A la o las bases de datos que requiere
- A los servicios complementarios como Impresora, telefonía, entre otros.
- A funcionalidades específicas de plataformas
- A las carpetas compartidas
- A los objetos, grupos y dominios
- A otros recursos que deben identificarse puntualmente al momento de solicitar el servicio de "Evaluación de nuevo puesto de Trabajo" el cual se realiza en el Portal de la Mesa de Servicio TI.

Se debe tener en cuenta que debe existir una adecuada segregación de funciones, desde un punto de vista de control interno, de acuerdo con la función del funcionario, la criticidad de los datos y la oposición de intereses.

Además, los accesos deben tener el principio de mínimo acceso para asegurar la segregación de funciones y el control total de procesos lo cual se puede convertir en una vulnerabilidad y por consiguiente en un riesgo. Las solicitudes realizadas por las jefaturas deben estar correctamente justificadas bajo un concepto de necesidad legitima, lo cual se fundamenta principalmente en las funciones y perfiles del cargo expresadas en los manuales de unidad o área.

5.1.2 Solicitud de Acceso para Funcionarios Activos

En el caso de los traspasos de cargos, se debe evaluar si los permisos otorgados con anterioridad deben o no continuar vigentes. Si se deben habilitar más permisos de los que actualmente tienen, se deberá contar con el requerimiento por parte de la Jefatura de área o unidad (Dueño de Proceso). Item 5.1.1.

Es importante señalar que los sistemas deben mantener trazas exactas de acciones, es por esta razón que es fundamental solicitar a los Administradores de Sistemas la actualización de datos cuando corresponda, por ejemplo, la dependencia de este funcionario ahora será "Hospital de Tomé".

5.1.3 Solicitud de Acceso para Funcionarios con Conectividad Remota

En el caso de funcionarios que se desempeñan bajo modalidad de trabajo remoto (teletrabajo), se debe evaluar de acuerdo con los accesos solicitados, los permisos y herramientas requeridas las cuales deberán ser configuradas en el equipo asignado para esta función. Estos permisos una vez definido deberán ser autorizados por parte de la Jefatura de Unidad o Área respectiva (Dueño de Proceso).

La solicitud de evaluación se debe realizar a través del Item 5.1.1 y todo trabajo remoto debe ser evaluado técnicamente por el Área de Tecnologías de la Información, específicamente:

- **Unidad de Operaciones TI**: Revisión de equipamiento necesario para dar cumplimiento a funciones, tales como notebook, vpn, configuraciones de red, antivirus, software de ofimática, Habilitación de Software especializado, entre otros. Entrega y firma de actas.
- **Unidad Tecnologías Digitales**: Siempre y cuando sea Administrador de Sistema se podrá realizar la modificación de acceso o habilitaciones según corresponda.
- **Unidad de Seguridad de la Información**: Evaluará pertinencia del cumplimiento de las políticas de seguridad en relación a los escenarios de teletrabajo propuestos, autorizará la VPN y capacitará al funcionario en temas de seguridad que sean específicos de esta modalidad.

5.1.4 Acceso a los Recursos de cada uno de los Equipos

El acceso a los recursos de los equipos debe ser solicitado por el Jefe de Unidad o Área a través de lo indicado en el punto 5.1.1 para los cuales se está solicitando acceso.

Como principio general, el usuario sólo debe tener acceso a los recursos mínimos indispensables para realizar su tarea. Sin perjuicio de lo anterior, se establece que "todo funcionario" debe tener acceso a un correo electrónico institucional y al Portal de la Mesa de Servicio TI los cuales se solicitarán por funcionarios de la Unidad de Personal al momento de la inducción a través del Portal de Mesa de Servicio TI.

Queda totalmente prohibido el uso de correos no institucionales dado que vulnera la seguridad del estado y por consiguiente de la Institución, además, en caso que el funcionario "Redireccione" o "Configure" el correo institucional para que envíe todo a una casilla pública a lo que se denomina "Forwarding" dejará de percibir servicios de acceso y será notificado a la Unidad de Seguridad de la Información para Auditoría Interna por incumplimiento de políticas institucionales ligadas a la Seguridad de la Información.

5.2 Administración de Cuentas Especiales

Si un funcionario requiere de una cuenta especial (de altos previlegios), es decir con acceso a sistemas de información, sistemas operativos, sistemas de administración de bases de datos, entre otros; será controlado por un Administrador de Sistema del Área de Tecnologías de la Información la cual deberá ser aprobada por el Dueño del

Activo (Encargado de Operaciones TI o Encargada de Tecnologías Digitales) y Encargado de Seguridad de la Información, resguardando el principio de segregación de funciones.

Estos permisos serán asignados a los usuarios en base a su necesidad de uso y en base a la Política de Control de Acceso, es decir, en base al requisito mínimo para sus roles o funciones.

Se debe identificar las cuentas de usuarios de mayor riesgo de cada uno de los sistemas y mantener una traza de sus estados y permisos.

Los encargados de Activos de TI serán responsables de definir las cuentas con máximos privilegios en las aplicaciones para acceder en situaciones de emergencia, identificando a las personas que pueden acceder a las mismas. Quien en coordinación con los Administradores de Sistemas (en caso de que aplique) gestionará los accesos de usuarios de las aplicaciones Institucionales y el control periódico de accesos autorizados para estos usuarios.

En el caso que los servidores estén bajo modalidad internalizada y no bajo contrato de externalización de servicio (SaaS), las contraseñas de administrador para estos servidores deben permanecer en un sobre cerrado, en un lugar de acceso restringido y cada vez que se cambien deberán ser actualizadas y enviar copia en sobre cerrado al Encargado de Seguridad de la Información.

La responsabilidad por la administración de las contraseñas de mayor riesgo recae en el Jefe de Área de Tecnologías de la Información.

5.3 Creación, Eliminación o Ajustes de Derechos de Acceso

Para solicitar acceso, modificación o baja a un sistema declarado como Activo de Información, será la Jefatura respectiva quien deberá a través de lo indicado en el Item 5.1.1 realizar la gestión.

El sistema de solicitud de creación, eliminación o ajustes de derechos de acceso que establezca la Institución deberá poseer mecanismos de protección de accesos, de identificación del funcionario (jefatura) que genera el requerimiento, manteniendo traza de todo el evento. Los gestores de TI (grupos de gestión de TI) deberán mantener para su registro, copia digital del requerimiento a razón de evidencia de la modificación realizada.

5.4 Creación de Usuarios

La unidad de Personal del Establecimiento deberá generar una Solicitud de Servicio a través de la Mesa de Servicio TI, en el apartado especifico de "Solicitudes de Incorporación", este proceso solo podrá ser ejecutado por personal habilitado lo que incluye las jefaturas.

El proceso tiene un flujo definido en donde se tendrá que completar los campos solicitados y los servicios Básicos como:

- Cuenta de Computador (Opcional)
- Cuenta de Correo Institucional (Obligatorio)
- Perfil de Jefatura en Mesa de Servicio (Opcional)
    - Este Item es importante para que las jefaturas puedan ver todo el catálogo de servicio TI.

Una vez seleccionados y completados los datos solicitados en los servicios se generará una Solicitud de Servicio al grupo de Gestión de Acceso de TI quienes procesarán lo indicado gestionando directamente con el nuevo funcionario/a.

El procedimiento anterior será clave para asegurar un correcto flujo de revisión de antecedentes que aseguren procesos complementarios.

La entrega de contraseñas temporales de ingreso se realiza mediante correo electrónico Institucional, en donde se entregarán las credenciales y un enunciado con las responsabilidades implicadas en el uso de los sistemas de información del Hospital de Tomé.

Las condiciones de uso incluyen:

- Cambiar clave inicialmente programada por TI, se incluye recomendaciones de Seguridad.
- Mantener confidenciales las credenciales secretas
- Cumplir con lo establecido en las Políticas y Procedimientos del Sistema de Seguridad de la Información, en todo lo que sea de su competencia.
- No divulgar información pertinente al Hospital de Tomé o sus funcionarios que tome en conocimiento por la naturaleza de sus funciones.
- Entender la responsabilidad funcionaria, aún fuera de las dependencias de trabajo y fuera del horario normal de trabajo.

Toda creación de acceso debe quedar reflejada en el Sistema de gestión de las Tecnologías de la Información, asegurando toda la traza, responsables y resoluciones.

5.4.1 Registros de usuarios en los sistemas de información

El encargado de la Unidad o Jefatura de Área que sea responsable de los activos de información de su dependencia es responsable de solicitar mediante la Mesa de Servicio TI la creación, modificación o pasivación de accesos en los sistemas de información.

El Administrador de Sistema o el grupo asignado en quien delega parte de la responsabilidad serán responsables de revisar y registrar el nivel de acceso solicitado el cual deberá ser apropiado para el propósito institucional y que sea consistente con la Política (s) de Seguridad de la Institución.

En caso de ser necesario se debe solicitar la autorización de acceso del usuario a los sistemas, al propietario (Dueño de Proceso o Jefatura a cargo del Activo) para su uso y acceso.

5.5 Ajuste de derechos de acceso

Para estos casos el encargado de Unidad o Jefe de Área deberá acceder a la Mesa de Servicio TI y seleccionar del catálogo los servicios correctos para realizar estos ajustes completando los campos requeridos.

5.6 Eliminación derechos de acceso

Para estos casos el encargado de Unidad o jefe de Área deberá acceder a la Mesa de Servicio TI y en el apartado de "Desvincular funcionarios" (solo accesible por Jefaturas) en donde tendrá que completar los campos requeridos siendo algunos datos claves para la gestión como:

- Tipo de Separación
- Última Fecha de trabajo

El campo Última Fecha de Trabajo permitirá conocer a los Gestores de Acceso desde el día que el funcionario ya no podrá realizar más acciones en los sistemas quedando automáticamente pasivado de los siguientes sistemas:

- Cuenta de Computador
- Correo Electrónico Institucional
- Sistemas Críticos
    - Registro Clínico Electrónico
    - Sistema de Imagenología
    - Sistema de Laboratorio
- Mesa de Servicio TI

La información contenida en los sistemas ejecutada por el usuario seguirá existiendo y en el caso del Correo Electrónico y Perfile de Computador se Almacenaran por 1 año calendario.

5.6.1 Devolución de activos

Todo funcionario es responsable de devolver todos los activos pertenecientes a la Institución que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo.

Equipos Personales: en los casos en que un funcionario utilice equipos propios, tiene la obligación de transferir toda la información pertinente al Hospital de Tomé y eliminarlo de cualquier soporte que posea, de ser necesario el Área TIC podrá tener acceso a los equipos para asegurar la transferencia de información.

Si un funcionario posee conocimiento perteneciente al Hospital de Tomé, por haber sido desarrollado dentro del marco de las labores para las que fue contratado, que es importante para las operaciones en curso, es su responsabilidad documentar dicha información y transferirla al Servicio.

Todo funcionario que mantenga información personal en los equipos proporcionados por el Hospital de Tomé deberá consignarla en una carpeta denominada “Información Personal”. Toda la información no incluida en esta carpeta se considera laboral y por tanto podrá ser revisada y respaldada por el Hospital del Tomé.

Es importante aclarar que el uso de equipamiento personal en líneas generales está prohibido y solo se autorizará bajo condicionales demostrables y evaluadas por el Comité de Seguridad de la Información.

Equipos Institucionales: En Chile, el uso de computadores institucionales en el ámbito público esta regulado por principios de probidad administrativa, protección de datos personales y uso eficiente de los recursos públicos. Es por esta razón que su uso esta limitado al cumplimiento de funciones asociadas al cargo o puesto de trabajo. Sin embargo, si de manera excepcional y transitoriamente se debe guardar información “Personal” en el computador esta tendrá que estar claramente identificada y visible desde el Escritorio del equipo.

Sin importar la situación en caso de Devolución, movilización o Desvinculación de un funcionario el equipo debe ser retirado por la Unidad de Operaciones TI en donde la información relacionada con funciones del cargo debe se respaldada antes de formatear o reasignar el equipo.

La información en caso de ser necesaria se podrá traspasar a la Jefatura de la Unidad o Área o en el equipo (Perfil) a reasignar lo cual se realizará a través de acta de entrega, especificando la incorporación del respaldo.

En caso de que en el Equipo existiesen datos personales (fotos, cv's, documentos privados, entre otros) y estos se encontrasen en la carpeta definida por nombre como "Personal" el usuario podrá solicitar eliminar o retirarlos. En caso de que los archivos mencionados no estén en la carpeta "Personal" entonces se entenderá que son Institucionales y serán considerados como respaldo.

Para tales efectos se entenderá como personal:

- Datos de contacto personal (run, dirección, teléfono personal, entre otros)
- Fotografías o Imágenes
- Documentos personales (currículum, cartas, certificados médicos, otros)
- Información Financiera Personal

El Área de TI no divulgará la información que contenga esta carpeta a menos que afecte a la imagen institucional o vulnere alguna Política Pública o Interna en cuyo caso la unidad de Operaciones TI, entregará el equipo a la Unidad de Seguridad de la Información para Auditoría Forense y presentará informe al Comité de Seguridad de la Información.

Los activos recuperados deben ser registrados en el Sistema de Inventario.

En caso de que no se devuelvan todos los activos asignados o sean devueltos con desperfectos, se debe informar a la Subdirección Administrativa para que se tomen las medidas correspondientes, esto último se realizará por escrito y con un informe técnico que acompañe.

5.7 Eliminación de Acceso a funcionarios con accesos críticos o privilegiados

Para el caso de funcionarios con accesos críticos o privilegiados, se debe tener especial cuidado en la gestión de la suspensión de accesos, para estos casos, posterior a la notificación de desvinculación y/o renuncia del funcionario, se deberá proceder con el bloqueo de todas las cuentas del usuario y activos de acuerdo con lo siguiente:

- Bloquear los accesos a los sistemas de información
- Bloqueo de casilla (s) de correo y configuración de mensaje automático de aviso para los correos entrantes.
- Bloqueo de cuentas como VPN, Videconferencia, Almacenamiento en la Nube entre otros.
- Avisar a los proveedores relacionados con la Desvinculación del funcionario.
- Identificación y respaldo de la información laboral contenida en los dispositivos (computadores de escritorio, notebook, tablets, celular, entre otros Institucionales)
- Eliminar de los grupos de mensajería instantánea institucionales relacionados sus funciones de la institución

Lo anterior deberá solicitarse según lo establecido en el punto 5.6 del presente procedimiento.

Al funcionario se le debe otorgar la oportunidad de respaldar su información personal, respetando lo anteriormente indicado, en caso de que esto pueda comprometer la integridad de la información entonces será la Unidad de Operaciones TI quienes respaldaran la carpeta denominada "Personal".

5.8 Revisión de los derechos de acceso de usuario

El o los Administradores de Sistemas serán responsables de gestionar que se efectúe la revisión de los derechos de acceso de acuerdo con los siguientes lineamientos:

- Se debe revisar los derechos de acceso de los usuarios cada 6 meses, el o los administradores de sistemas deberán acceder a sus plataformas de control ya sea centralizada o por cada activo y realizar idealmente de manera automatizada esta revisión considerando:
    - Inactividad Prolongada: Si no ha usado el sistema en 30, 60 o 90 días
        - Revisión con Unidad de Personal si
            - Devinculado
            - Licencia Prolongada
            - Comisión de servicio
    - Accesos fuera de Horario o desde ubicaciones inusuales (si está disponible)
    - Frecuencia vs Rol: Si el rol exige acceso regular o no hay actividad
    - Buscar cuentas duplicadas o temporales que no se han dado de baja
    - Verificar cuentas "genéricas" o compartidas, estas deben estar especialmente justificadas y auditadas.

El encargado de Seguridad de la Información realizará un randomizer de usuarios en los sistemas críticos cada 6 meses, especialmente en el Registro Clínico Electrónico y se ejecutará una auditoría de al menos 7 usuarios con la finalidad de detectar anomalías de accesos.

Sin perjuicio de lo anterior serán los dueños de proceso (Jefaturas de Unidad) los responsables de realizar una revisión de los derechos de acceso de su personal a cargo de acuerdo con los siguientes lineamientos:

- Cambio de Rol, Unidad o Jefatura
- Revisar si amerita realmente el acceso al sistema
- Revisión si los permisos otorgados son acordes a su cargo o son excesivos
    - Aplicar el principio de mínimo privilegio.

5.9 Perfiles de acceso de los usuarios

Los perfiles de acceso son el conjunto de atribuciones y privilegios a los cuales tiene acceso una cuenta de usuario o grupo de usuarios.

El encargado de Unidad o Jefatura de Área responsable de la custodia de los datos de sus procesos debe revisar en forma periódica los perfiles de usuario del personal vigente y realizar una actualización de estos cada vez que ocurra un cambio en la definición de funciones. (Revisar Anexo A de Perfiles de Acceso de Sistemas Críticos)

La administración de los perfiles radica en los Encargados de TI (Unidad de Operaciones y/o Tecnologías Digitales según corresponda) y opcionalmente en Administradores de Sistemas que no son parte de TI. Para este último se debe utilizar el principio de mínimo privilegio y segregación de funciones lo que significará que un Administrador de Sistema no podrá ser a todo evento un Dueño de Proceso y tampoco se permitirá que un Administrador de Sistema cumpla funciones en la misma jerarquía, dado que afecta al principio de segregación de funciones y probidad administrativa.

5.10 Administración de claves de acceso

El Hospital de Tomé considera que todos los sistemas computacionales que permitan acceder a la información que éste administra, debe contar con un sistema de

identificación y autentificación de usuarios que permita garantizar que sólo personal debidamente autorizado tenga acceso a la información, considerando, además, sólo acceso a través de claves seguras, únicas e intransferibles. Para una adecuada administración de las claves de acceso a los recursos informáticos los Administradores de Sistemas deberán tener acceso a un sistema que permita la administración y gestión local con el objetivo de que las gestiones sean oportunas, eficientes y de resolución local.

Cuando el establecimiento entre a una etapa de transformación digital según lo establecido por las leyes nacionales se deberá contar con herramientas y/o estrategia que permita la gestión de acceso de manera eficiente y centralizada como por ejemplo a través de Maestros de Usuarios integrados a nivel de capa de acceso a los sistemas, integración de clave única, protocolos de autenticación como LDAP entre otros. Lo anterior es clave para mantener la seguridad y no se generen efectos colaterales producto de vicios por el aumento de credenciales en cada sistema.

Para una adecuada administración de las claves de acceso a los activos de información, debe tenerse en cuenta las siguientes consideraciones:

5.10.1 Cuentas de Usuario

Las cuentas de usuario deben cumplir con los requerimientos que se detallan a continuación:

- Cada persona debe tener una única identificación de su cuenta personal de usuario en todos los sistemas/equipos de la unidad.
- La identificación de la cuenta personal debe corresponder a una nomenclatura estándar predefinida compuesta por (8) caracteres como mínimo. Contener letras mayúsculas, minúsculas y números.
- La identificación de cuentas especiales también debe corresponder a una nomenclatura estándar predefinida compuesta por (8) caracteres como mínimo, asignando los primeros dos caracteres al código correspondiente al sistema / aplicación, y los restantes deberán ser una serie de caracteres que identifiquen el tipo de permiso otorgado a la cuenta. (Mapeable)
- Se deja establecido que para aquellas aplicaciones donde el control de acceso a la aplicación es realizado fuera de los sistemas institucionales (servidores internos) y estas sean tercerizadas, será de acuerdo con lo estipulado por las bases técnicas, manteniendo en todo momento las recomendaciones de mejores prácticas nacionales e internacionales.

5.10.2 Utilización de las cuentas de usuario

En los entornos hospitalarios, donde la información sensible y la continuidad operativa son críticas, el uso adecuado de las cuentas de usuario es esencial para garantizar la seguridad de los sistemas y la confidencialidad de los datos clínicos. A continuación, se establecen las principales buenas prácticas recomendadas para el uso responsable y seguro de las cuentas de usuario en plataformas institucionales.

Todas las cuentas de usuario deben ser personales, únicas e intransferibles. En ninguna circunstancia se permite compartir credenciales, ya que esto compromete la trazabilidad y pone en riesgo la integridad de la información.

Cada acción realizada en los sistemas debe poder ser atribuida claramente a una persona identificable.

Es fundamental aplicar el principio de mínimo privilegio: los usuarios deben contar exclusivamente con los permisos necesarios para cumplir sus funciones. El otorgamiento de accesos debe estar basado en el perfil del cargo y su ubicación dentro de la organización, evitando así accesos innecesarios a sistemas clínicos o administrativos sensibles.

La creación, modificación y eliminación de cuentas debe ser gestionada de forma centralizada, preferentemente a través de un directorio institucional como Active Directory o similar. Este proceso debe estar coordinado con las áreas de Recursos Humanos y Jefaturas, para garantizar la activación o desactivación inmediata de cuentas frente a ingresos, traslados, licencias prolongadas o desvinculaciones.

Respecto a la seguridad de acceso, las contraseñas deben cumplir con políticas de complejidad definidas institucionalmente y cambiarse de forma periódica. Además, se recomienda la implementación de autenticación multifactor (2FA) para todos los accesos a sistemas críticos, especialmente si se permite el acceso remoto. Lo anterior De acuerdo con las directrices del NIST (SP 800-63B).

Es obligatorio registrar y auditar todos los accesos realizados a los sistemas institucionales. Los registros deben incluir el usuario, fecha, hora y tipo de acción realizada y origen (IP), y deben mantenerse disponibles para auditorías internas o externas. Esta trazabilidad es clave para prevenir y responder a incidentes de seguridad.

Las cuentas que permanezcan inactivas por más de 30 días deben ser revisadas, y si no hay justificación para su mantenimiento, deben ser desactivadas de forma automática o manual según el procedimiento establecido. El monitoreo continuo permite detectar accesos innecesarios o cuentas olvidadas que podrían ser explotadas.

Por normativa interna, las cuentas institucionales deben ser utilizadas exclusivamente para fines laborales. No está permitido acceder a redes sociales, correos personales u otros servicios no autorizados desde estas cuentas, particularmente en equipos compartidos o ubicados en áreas clínicas.

Los funcionarios deben recibir capacitación periódica respecto al uso seguro de sus credenciales, la detección de intentos de fraude informático (como el phishing), y las buenas prácticas relacionadas con el cierre de sesiones, bloqueo de pantalla y resguardo de su identidad digital.

En el caso de las cuentas privilegiadas, tales como las utilizadas para administración de sistemas, se debe establecer un control más estricto. Estas cuentas deben estar separadas de las cuentas de uso diario y contar con medidas adicionales de seguridad y auditoría. Asimismo, las cuentas técnicas o de servicio, utilizadas por aplicaciones o integraciones, deben documentarse, mantenerse bajo control, y contar con contraseñas almacenadas en bóvedas seguras y rotadas periódicamente.

Por último, se recomienda que todas las estaciones de trabajo cuenten con políticas de bloqueo automático tras un período breve de inactividad, idealmente no superior a los 5 o 10 minutos. Además, los accesos de los funcionarios a los sistemas críticos deben ser revisados de forma periódica, al menos dos veces al año, para validar su vigencia y pertinencia según sus funciones actuales.

5.10.3 Administración de contraseñas de cada usuario

Toda cuenta de usuario debe tener asociada obligatoriamente una contraseña.
Cada vez que un usuario sea creado en un recurso de la Institución, se deberá definir una contraseña única y robusta. Esta contraseña de carácter personal deberá ser cambiada obligatoriamente en el primer acceso realizado por el usuario.
Todas las contraseñas deben cumplir con los siguientes requisitos:

- Deben permanecer encriptadas y residir en archivos ocultos y protegidos
- No deben ser visibles por pantalla al momento de ser ingresadas
- Deben ser definidas con una longitud mínima de ocho (8) posiciones.
- Deben contener letras y números (ser alfanumérica)
- No deben ser en blanco
- No deben ser genéricas o de fácil detección.

Para la generación de contraseñas se debe seguir la siguiente metodología de combinación de datos:

- La contraseña no debe ser igual a la identificación personal (ej: Francisco321) ni tampoco ser demasiado obvias.
- Los encargados TI o personal a cargo deben comunicar al usuario la contraseña (cuando se le otorgue por primera vez) o en su defecto una automatización enviará al correo institucional instrucciones para la generación de contraseña.
- En caso de que el encargado de TI o personal lo crea conveniente debe utilizar adicionalmente procedimientos de llamado y re-llamado para asegurarse la identidad del usuario al que le transfiere la contraseña.

Para el cambio de contraseña deben considerarse los siguientes requisitos:

- Exigir el cambio automático, la primera vez que el usuario ingresa al sistema
- Ser distinta a la última contraseña utilizada
- Permitir ser cambiadas toda vez que el usuario lo requiera

5.10.4 Bloqueo de cuentas

De cumplirse el número de intentos fallidos establecido, la cuenta debe quedar bloqueada, siendo los únicos autorizados para su desbloqueo el Área de TI. La misma sólo debe ser reconectada, con la autorización de Encargados de TI o por un tiempo de espera predefinido por este. En ausencia de éste, podrá ser habilitada por el Centro de Servicio TI a través de la autorización de la encargada del Centro de Servicio TI, quien deberá informar de este evento al Encargado TI correspondiente como observador o inspector en el requerimiento en cuestión. Para las cuentas especiales de mayor riesgo, la reconexión debe ser documentada y comunicada al Encargado de Seguridad.

De ser solicitado se podrá bloquear la cuenta de usuario durante los permisos u ausencias prolongadas. Para ello el jefe directo deberá informar, a través de la Mesa de Servicio TI las fechas durante las cuales se producirá la ausencia, esto se puede realizar en el servicio de Cuentas en la acción de “Modificación”.

El bloqueo deberá permanecer hasta la efectiva comunicación con el usuario responsable de la misma.

5.10.5 Otras claves de sistemas

Existen servicios críticos gestionados directamente por determinadas unidades funcionales, cuyo acceso es de carácter altamente sensible y estratégico. En estos casos, la administración y custodia de las credenciales de acceso recae exclusivamente en la unidad responsable, excluyéndose expresamente al Área de Tecnologías de la Información, salvo que se acuerde lo contrario bajo un esquema formal de control.

Entre estos servicios se encuentran, por ejemplo:

- Cuentas de acceso a plataformas bancarias institucionales.
- Cuentas asociadas al sistema de Facturación Electrónica.
- Cuentas asociadas a Sistemas de Recursos Humanos
- Otros servicios críticos definidos por la jefatura del área correspondiente.

La gestión de estas credenciales deberá realizarse en conformidad con las buenas prácticas internacionales, tales como la protección mediante almacenamiento seguro (por ejemplo, bóvedas de contraseñas), uso de autenticación multifactor cuando esté disponible, rotación periódica bajo procedimientos controlados, y acceso restringido exclusivamente a personal autorizado. Toda manipulación de estas credenciales deberá quedar registrada y resguardada de forma que garantice la trazabilidad, confidencialidad y disponibilidad del servicio, además, deberá aplicarse todo lo contenido en el presente procedimiento de Gestión de Identidad y Derechos de Acceso.

Sin perjuicio de lo anterior en Encargado de Seguridad de la Información Institucional podrá auditar estas cuentas cuando estime necesario o cuando exista algún evento de seguridad.

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

10 ANEXO A: PERFILES DE ACCESO

Los perfiles de accesos presentes en el Procedimiento de Gestión de Identidad y Derechos de Acceso corresponden a los Activos Críticos que se encuentran definidos en el SGSI de la Institución.

10.1 Perfiles de acceso registro clínico electrónico Trakcare

AMBULATORIO		
GS (Grupo Seguridad)	**PA (Perfil de Acceso)**	**Tipo Profesional**
CLXX Médico Ambulatorio	CLTL Médico Ambulatorio HT	Médico
CLXX Médico Ambulatorio GO	CLTL Médico Ambulatorio GO HT	Ginecólogo
CLXX Médico Ambulatorio SM	CLXX Médico Ambulatorio SM HT	Psiquiatra
CLXX Odontología	CLTL Odontología	Odontólogos
CLXX Enfermería ambulatorio SM	CLTL Enfermería ambulatorio SM	Enfermera Salud Mental
CLXX Enfermería Ambulatorio	CLTL Enfermería Ambulatorio	Enfermera
CLXX Matrona Ambulatorio	CLTL Matrona Ambulatorio ITS HT	Matrona ITS
CLXX Matrona Ambulatorio	CLTL Matrona Ambulatorio	Matrona
CLXX Nutricionista Ambulatorio	CLTL Nutricionista Ambulatorio	Nutricionista
CLXX Psicología Ambulatorio SM	CLTL Psicología Ambulatorio SM	Psicólogo Salud Mental
CLXX Psicología Ambulatorio	CLTL Psicología Ambulatorio	Psicólogo
CLXX Terapeuta ocupacional ambulatorio SM	CLTL Terapeuta ocupacional ambulatorio SM	Terapeuta Ocupacional Salud mental
CLXX Terapeuta ocupacional ambulatorio	CLTL Terapeuta ocupacional ambulatorio	Terapeuta Ocupacional
CLXX Asistente social Ambulatorio SM	CLTL Asistente social Ambulatorio SM	Trabajador Social Salud Mental
CLXX Asistente social Ambulatorio	CLTL Asistente social Ambulatorio	Trabajador Social
CLXX TP Ambulatorio	CLTL TP Ambulatorio	TENS
CLXX Mantenedor de Agenda	CLTL Mantenedor de Agenda	Mantenedor
CLXX Admisión Ambulatoria	CLTL Admisión Ambulatoria	Admisión Ambulatoria
CLXX Inscripción de Paciente	CLTL Inscripción de Paciente	Admisión Ambulatoria
CLXX Gestión	CLTL Gestión	Administrativos
CLXX Fallecimiento de Paciente	CLXX Fallecimiento de Paciente	Archivo/Admisión
CLXX Gestión de Documentos	CLTL Gestión de Documentos	Archivo
CLXX Historia Clínica Paciente	CLXX Historia Clínica Pacientes	Archivo
CLXX GES Administrativo	CLTL GES Admin	GES
CLXX GES Administrador	CLXX GES Administrador	GES
CLXX TP Ambulatorio	CLTL TP Ambulatorio	TENS
CLXX Gestión de Interconsultas	CLTL Gestión de Interconsultas	Gestión de LE
CLXX Médico Contralor	CLTL Médico Contralor	Médico Contralor
CLXX Kinesiólogo ambulatorio	CLXX Kinesiólogo ambulatorio	Kinesiólogo
CLXX fonoaudiólogo	CLXX fonoaudiólogo	Fonoaudiólogo
CLXX Analizador de Datos	CLTL Analizador de Datos	Gestión
CLXX Tecnólogo Médico Ambulatorio	CLTL Tecnólogo Médico Ambulatorio	Tecnólogo Médico

APOYO DIAGNOSTICO		
GS (Grupo Seguridad)	**PA (Perfil de Acceso)**	**Tipo Profesional**
CLXX Técnico Farmacéutico	CLTL Técnico Farmacéutico	Técnico
CLXX Químico Farmacéutico	CLTL Químico Farmacéutico	Químico Farmacéutico
CLXX Stock	CLTL Stock	Químico Farmacéutico
CLXX Transcripción Recetas	CLTL Transcripción Recetas	Químico Farmacéutico
CLXX Gestión	CLTL Gestión	Químico Farmacéutico
CLXX Admisión Imagenología 2	CLTL Admisión Imagenología 2	Admisión
CLXX Tecnólogo Médico Imagenología	CLTL Tecnólogo Médico Imagenología	Tecnólogo Médico
CLXX Técnico Paramédico Imagenología 2	CLTL Técnico Paramédico Imagenología 2	Técnico
CLXX Gestión	CLTL Gestión	Administrativo
CLXX Admisión Laboratorio	CLTL Admisión Laboratorio	Admisión Laboratorio
TCE Toma de Muestras	TCE Toma de Muestras	Enfermera Laboratorio
CLXX Recepción Laboratorio	CLTL Recepción Laboratorio	Tecnólogo Médico
CLXX Gestión	CLTL Gestión	Administrativo

SERVICIO PABELLON QUIRURGICO		
GS (Grupo Seguridad)	**PA (Perfil Acceso)**	Tipo Profesional
CLXX Anestesiólogo	CLTL Anestesiólogo	Anestesista
CLXX Cirujano	CLTL Cirujano	Cirujano
CLXX Enf/Mat Pabellón/Recuperación	CLTL Enf/Mat Pabellón/Recuperación	Enfermera /Matrona
CLXX TP Pabellón/Recuperación	CLTL TP Pabellón/Recuperación	TENS recuperación
CLXX Admisión Hospitalizado	CLTL Admisión Hospitalizado	Admisión Pabellon
CLXX Técnico Anestesia	CLTL Técnico Anestesia	Técnico Anestesia
CLXX Gestor Agendamiento Quirúrgico	CLTL Gestor Agendamiento Quirúrgico	Gestor Agendamiento Quirúrgico
CLXX Admisión Hospitalizado	CLTL Admisión Pabellón Ambulatorio	Admisión Pabellón Ambulatorio
CLXX Mantenedor Agenda Pabellón	CLTL Mantenedor Agenda Pabellón	Mantenedor Agenda Pabellón
CLXX Analizador de Datos	CLTL Analizador de Datos	Gestión

GS Administrativo		
Grupo Seguridad	**Perfil Acceso**	**Tipo Profesional**
CLXX Admisión Hospitalizado	CLTL Admisión Hospitalizado	Admisión Hospitalizados
CLXX Gestión Camas	CLTL Gestión Camas	EU gestor de Camas
CLXX Analizador de Datos	CLTL Analizador de Datos	Gestión

HOSPITALIZADOS		
GS (Grupo Seguridad)	**PA (Perfil Acceso)**	**Tipo Profesional**
CLXX Médico Hospitalización Adulto	CLTL Médico Hospitalización Adulto HT	Médico Hospitalizados
CLXX Enfermería Hospitalizado Adulto	CLTL Enfermería Hospitalizado Adulto	Enfermera Hospitalizados
CLXX TP Hospitalización Adulto	CLTL TP Hospitalización Adulto	TENS Hospitalizados
CLXX Nutricionista Hospitalizado	CLTL Nutricionista Hospitalizado	Nutricionista Hospitalizados
CLXX Profesionales Clínicos Hospitalizado	CLTL Profesionales Clínicos Hospitalizado	Hospitalizados
CLXX Kinesiólogo Hospitalizado	CLTL Kinesiólogo Hospitalizado	Kinesiólogo Hospitalizados
CLXX Fonoaudiólogo Hospitalizado	CLTL Fonoaudiólogo Hospitalizado	Fonoaudiólogo Hospitalizado
CLXX Médico Hospitalización Pediatria	CLTL Médico Hospitalización Pediatría HT	Pediatra Hospitalizados
CLXX TP Hospitalización Pediatría	CLTL TP Hospitalización Pediatría	TENS Pediatría Hospitalizado
CLXX Enfermería Hospitalizado Pediatría	CLTL Enfermería Hospitalizado Pediatría	Enfermera Pediatría Hospitalizados
CLXX Médico Hospitalización Cirugía	CLTL Médico Hospitalización Cirugía HT	Cirujano Hospitalizados
CLXX Médico Hospitalización GO HT	CLTL Médico Hospitalización GO HT	Médico
CLXX Enf/Mat hospitalizado Neonatología	CLTL Enf/Mat hospitalizado Neonatología	Enfermera (EU) / Matrona
CLXX Matrona Hosp	CLTL Matrona Hosp	Matrona
CLXX TP Hospitalizado Maternidad	CLTL TP Hospitalizado Maternidad	TENS Maternidad

HOSPITALIZACION DOMICILIARIA (HODOM)		
GS (Grupo Seguridad)	**PA (Perfil de Acceso)**	**Tipo Profesional**
CLXX Admision Hospitalizado	CLTL Admisión Hospitalizado	Admisión HODOM
CLXX.IP.Enfermeria Hospitalización Domiciliaria	CLTL.IP.Enfermeria Hospitalización Domiciliaria Adultos HT	Enfermera/a
CLXX.IP.Enfermeria Hospitalización Domiciliaria	CLTL.IP.Enfermeria Hospitalización Domiciliaria Pediatria HT	Enfermera/a
CLXX.IP.Medico Hospitalización Domiciliaria	CLTL.IP.Medico Hospitalización Domiciliaria Adulto HT	Medico
CLXX.IP.Medico Hospitalización Domiciliaria	CLTL.IP.Medico Hospitalización Domiciliaria Pediatría HT	Medico
CLXX.TP Hospitalización Domiciliaria	CLTL.IP.TP Hospitalización Domiciliaria Adulto HT	TENS
CLXX.TP Hospitalización Domiciliaria	CLTL.IP.TP Hospitalización Domiciliaria Pediatria HT	TENS
CLXX.IP.Profesionales Clínicos Hospitalización Domiciliaria	CLTL.IP.Nutricion Hospitalización Domiciliaria HT	Nutricionista
CLXX.IP.Profesionales Clínicos Hospitalización Domiciliaria	CLTL.IP.Terapeuta Ocupacional Hospitalización Domiciliaria HT	Terapeuta Ocupacional
CLXX.IP.Profesionales Clínicos Hospitalización Domiciliaria	CLTL.IP.Fonoaudiologia Hospitalización Domiciliaria HT	Fonoaudiólogo/a
CLXX.IP.Profesionales Clínicos Hospitalización Domiciliaria	CLTL.IP.Kinesiologia Hospitalización Domiciliaria HT	Kinesiólogo/a
CLXX.IP.Profesionales Clínicos Hospitalización Domiciliaria	CLTL.IP.Trabajador Social Hospitalización Domiciliaria HT	Trabajador Social

URGENCIA		
GS (Grupo Seguridad)	**PA (Perfil de Acceso)**	**Tipo Profesional**
CLXX.EM.Médico Urgencia	CLTL Médico Urgencia Adulto 2 HT	Médico Adulto
CLXX.EM.Enfermería Urgencia	CLTL Enfermería Urgencia	Enfermera
CLXX.EM.Enfermería Urgencia/Revertir Alta	CLTL Enfermería Urgencia/Revertir Alta	Enfermera
CLXX.EM.Matrona Urgencia	CLTL Matrona de Urgencia HT	Matrona
CLXX.EM.TP Urgencia	CLTL TP Urgencia	TENS
CLXX.EM.TP Urgencia G-O ESI	CLTL TP Urgencia Maternidad	TENS GO
CLXX Admisión de Urgencia	CLTL Admisión de urgencia	Admisión
CLXX Admisión de Urgencia + Revertir Alta	CLTL Admisión de urgencia	Admisión
CLXX Digitador de Urgencia	CLXX Digitador de Urgencia	Digitador de Urgencia
CLXX.EM.Profesional Clínico Urgencia	CLTL Profesional Clínico Urgencia	Profesional Clínico Urgencia
CLXX.EM.Profesional Clínico Urgencia	CLTL Kinesiología Urgencia	Kinesiologo
CLXX.EM.Profesional Clínico Urgencia	CLTL Asistente Social Urgencia	Asistente Social
CLXX.EM.Profesional Clínico Urgencia	CLTL Nutricionista Urgencia	Nutricionionista
CLXX.EM.Profesional Clínico Urgencia	CLTL Fonoaudiologia Urgencia	Fonoaudiologo
CLXX.EM.Profesional Clínico Urgencia	CLTL Psicologia Urgencia	Psicologo
CLXX.EM.Profesional Clínico Urgencia	CLTL Terapia Ocupacional Urgencia	Terapeuta ocupacional

10.1.1 Terminología

- **Perfiles de Acceso**: El perfil de acceso es un conjunto de componentes funcionales que permiten al usuario realizar diferentes acciones en un sistema dado y es lo que el funcionario podrá identificar visualmente para el trabajo diario.
- **Grupo de Seguridad**: Corresponde al conjunto de roles permitidos segmentados en grupos los cuales son asociados a perfiles de acceso para una visualización completa de acciones y funcionalidades para el usuario final.

10.2 Perfiles de acceso sistema de imagenología (RIS/PACS) - Medicap

Perfil	Tipo Profesional
Administrador HT	Administrador de Sistema
Recepcionista HT	Admisionista
Informante HT	Médico Radiólogo
Tecnólogo HT	Tecnólogo
Enfermería HT	Enfermera
Tens HT	Técnico Paramédico Profesional
BUSCADOR DE ESTUDIOS	Usuario General
TM Asignación HT	Tecnólogo Médico
Tens Endoscopía HT	Tecnico Paramédico Profesional
Enfermería Endoscopía HT	Enfermera
Informante Endoscopía HT	Medico Radiólogo
Informante CardioHT	Médico Radiólogo
Administrador CardioHT	Administrador
Recepcionista CardioHT	Admisionista

10.3 Perfiles de acceso a sistema de Directorio Activo

Perfil	Tipo Profesional
Administrador de Dominio	Ingeniero
Administrador	Administrador

10.4 Perfiles de acceso a sistema de Laboratorio - Syslab

Perfil	Tipo Profesional
Administrador	Administrador de Sistema
Tecnólogo médico laboratorio	Tecnólogo
Técnico paramédico Laboratorio	Técnico Paramédico