MAN04-25-0001

MANUAL ORGANIZACIONAL AREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Sistema de Gobernanza TI - Hospital de Tomé

Versión Oficial Actual 2 – Agosto 2026

Contenido

1 PROPOSITO

El Manual Organizacional del Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé es una guía integral diseñada para estructurar, gestionar y alinear las operaciones del área TIC con la misión institucional de brindar atención de salud de calidad, eficiente y segura.

2 ALCANCE O AMBITO DE APLICACIÓN

El presente Manual Organizacional del Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé es aplicable a todas las actividades, procesos y servicios que conforman la gestión tecnológica de la institución.
Su alcance abarca a todos los funcionarios del hospital, incluyendo personal de planta, a contrata, en reemplazo, suplencia y a honorarios, así como a proveedores externos, empresas contratistas y terceros que participen en la provisión, mantenimiento o soporte de soluciones tecnológicas, sistemas de información y equipamiento asociado.

Este manual recopila y consolida las políticas, procedimientos, normas, instructivos y lineamientos técnicos que rigen el funcionamiento del área TIC, asegurando la coherencia y estandarización de las prácticas internas, la adecuada gestión de los recursos tecnológicos y el cumplimiento de los requerimientos normativos, de seguridad de la información y de calidad establecidos por el Ministerio de Salud y por el propio Hospital de Tomé.

Asimismo, este documento establece los roles, responsabilidades y relaciones funcionales del área TIC con las demás unidades del hospital, definiendo los límites de su competencia y su interacción con los procesos clínicos, administrativos y de apoyo.
Su aplicación es de carácter obligatorio para todo el personal que utilice, gestione o administre recursos tecnológicos institucionales.

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

El presente Manual Organizacional del Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé se enmarca dentro de las disposiciones legales, normativas y técnicas que regulan la gestión tecnológica, la seguridad de la información y la transformación digital en los organismos públicos de salud.

A continuación, se presentan las principales referencias normativas y documentales que orientan su aplicación:

3.1 Normativa Legal Nacional

- **Ley N° 21.663 – Marco de Ciberseguridad de la Información de la República de Chile**: Establece los principios, estructuras institucionales y obligaciones del Estado para resguardar la ciberseguridad en los organismos públicos y privados críticos, definiendo responsabilidades de gobernanza, gestión de riesgos y respuesta ante incidentes.
- **Ley N° 21.180 – Transformación Digital del Estado**: Regula la modernización de los procedimientos administrativos del sector público mediante el uso de medios digitales, firma electrónica, interoperabilidad y gestión documental electrónica.
- **Ley N° 19.628 – Sobre Protección de la Vida Privada**: Regula el tratamiento de datos personales y la obligación de resguardar la confidencialidad, integridad y disponibilidad de la información de las personas.
- **Ley N° 18.575 – Orgánica Constitucional de Bases Generales de la Administración del Estado**: Establece los principios de eficiencia, eficacia, responsabilidad y

transparencia que rigen la gestión pública, aplicables también a la administración tecnológica institucional.

- **Ley N° 19.799 – Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación**: Regula el uso de la firma electrónica y otorga validez jurídica a los documentos digitales.
- **Ley N° 20.584 – Derechos y Deberes de los Pacientes**: Define el marco de confidencialidad y protección de los datos clínicos, aspecto directamente relacionado con la gestión segura de los sistemas de información en salud.
- **Ley N° 20.285 – Sobre Acceso a la Información Pública**: Promueve la transparencia activa y pasiva en los organismos públicos, resguardando el equilibrio entre acceso a la información y protección de datos sensibles.
- **Decreto N° 83/2005 del Ministerio de Salud**: Aprueba el Reglamento de los Establecimientos de Autogestión en Red, que establece responsabilidades de gestión y rendición de cuentas en el uso de recursos tecnológicos.

3.2 Normas, Marcos y Estándares Técnicos de Referencia

- **ISO/IEC 27001 y 27002:2013 – Seguridad de la Información**: Estándares internacionales que establecen los requisitos y controles para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).
- **COBIT 2019 – Control Objectives for Information and Related Technology**: Marco de referencia para la gobernanza y gestión de las TI corporativas, utilizado como guía para la alineación estratégica, control y mejora continua de los procesos TIC institucionales.
- **SFIA – Skills Framework for the Information Age**: Marco internacional para la definición de competencias profesionales en tecnología, utilizado como referencia para la gestión del talento y las capacidades del equipo TIC.
- **NIST SP 800-61 y SP 800-53 (referenciales)**: Buenas prácticas en gestión de incidentes y controles de seguridad, adoptadas como referencia para los procedimientos internos del área.
- **SCF – Secure Controls Framework**: Marco integral de controles de seguridad que consolida y armoniza requisitos provenientes de múltiples estándares internacionales (como ISO 27001, NIST, COBIT, CIS, entre otros), permitiendo establecer una estructura unificada y trazable para la gestión de la ciberseguridad y el cumplimiento normativo.
- **ITIL – Information Technology Infrastructure Library:** Conjunto de buenas prácticas internacionales para la gestión de servicios de tecnologías de la información (IT Service Management, ITSM), orientado a alinear los servicios TIC con las necesidades del negocio y los usuarios.

3.3 Documentos Institucionales Internos

- **Plan Desarrollo Estratégico (PDE)**: Define los lineamientos estratégicos globales del Hospital de Tomé y orienta la contribución del área TIC al cumplimiento de la misión institucional.
- **Marco de Gestión de Tecnologías de la Información y Comunicación (APO01)**: Documento que garantiza que las TIC se gestionen de manera alineada con la estrategia institucional, las normativas nacionales vigentes y las buenas prácticas internacionales.

- **Plan Estratégico de Tecnologías de la Información (AP002)**: Documento rector de planificación tecnológica que establece los objetivos, metas y prioridades en materia de transformación digital, infraestructura y servicios informáticos.
- **Manual de Gobernanza TI**: Define la estructura de decisión, roles y responsabilidades de las instancias de dirección y control de las tecnologías de información.
- **Política General de Seguridad de la Información**: Marco superior que define los principios, objetivos y responsabilidades de la seguridad de la información institucional.

3.4 Políticas y Procedimientos Específicos del Área TIC

- Política de Respaldo y Recuperación de la Información.
- Política de Derechos de Acceso.
- Política de Clasificación y Manejo de la Información.
- Política de Gestión de Cambios.
- Política para las Relaciones con Proveedores y Terceros.
- Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- Procedimiento de Gestión de Identidad y Derechos de Acceso.
- Procedimiento de Gestión de Vulnerabilidades.
- Procedimiento de Recuperación ante Desastres.

Estos documentos constituyen los controles críticos del Sistema de Gestión de Seguridad de la Información (SGSI) del Hospital de Tomé y son de cumplimiento obligatorio para todo el personal del área TIC y los terceros que operen sistemas o infraestructura tecnológica institucional.

3.5 Otros Documentos

- Gestión de Incidentes y Solicitudes de Servicios (DSS02)
- Modelo de Madurez C2M2
- Modelo Priorización Objetivos Cobit 2019
- Modelo de Madurez Digital
- Procedimiento de Evaluación de Proyectos de TI

4 ROLES Y RESPONSABILIDADES

El Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé tiene como propósito planificar, administrar y supervisar los recursos tecnológicos institucionales, asegurando la continuidad operativa, la seguridad de la información y el soporte a los procesos clínicos, administrativos y de apoyo.

A continuación, se describen los principales roles y sus responsabilidades dentro de la estructura organizacional del área:

4.1 Subdirección Administrativa

- Establecer los lineamientos estratégicos y aprobar las políticas y planes institucionales en materia de tecnologías de la información.
- Designar formalmente al Jefe del Área TIC y a los responsables de seguridad, modernización digital e Infraestructura TI

- Garantizar la disponibilidad de los recursos humanos, financieros y tecnológicos necesarios para el cumplimiento de los objetivos del área.
- Supervisar el cumplimiento de las normativas legales y regulatorias vigentes relacionadas con la gestión de la información y las tecnologías.

4.2 Jefatura del Área de Tecnologías de la Información y Comunicación

- Liderar la gestión integral del área TIC, asegurando la alineación de las estrategias tecnológicas con los objetivos institucionales definidos en el Plan Estratégico del Hospital.
- Representar al área ante las instancias de dirección, comités y organismos externos vinculados a la modernización y seguridad digital.
- Aprobar los planes, políticas, procedimientos y proyectos tecnológicos desarrollados por las distintas unidades del área.
- Coordinar la planificación presupuestaria, la priorización de iniciativas tecnológicas y la evaluación de desempeño del personal TIC.
- Promover la adopción de marcos de referencia como COBIT, ITIL, ISO 27001 y el SCF, velando por la mejora continua de los procesos.

4.3 Unidad de Operaciones TI

- Administrar la infraestructura tecnológica institucional (servidores, redes, telecomunicaciones, respaldo, almacenamiento y conectividad).
- Asegurar la continuidad operativa de los servicios informáticos y la disponibilidad de los sistemas críticos.
- Monitorear el rendimiento y la capacidad de los sistemas, proponiendo mejoras técnicas o de arquitectura.
- Gestionar las actividades de soporte técnico de segundo nivel y los mantenimientos preventivos o correctivos.
- Implementar y mantener controles técnicos de seguridad definidos por el área de Seguridad de la Información.

4.4 Unidad de Tecnologías Digitales

- Implementar y mantener las soluciones de software, integraciones y plataformas digitales del hospital.
- Asegurar la interoperabilidad con sistemas institucionales del MINSAL, FONASA y otros organismos del Estado.
- Gestionar los ambientes de desarrollo, pruebas y producción, aplicando controles de cambio y versiones.
- Evaluar requerimientos de usuarios y proponer mejoras tecnológicas alineadas con la estrategia de transformación digital.
- Apoyar la implementación de iniciativas de automatización, inteligencia de datos y gobierno digital.

4.5 Unidad de Seguridad de la Información

- Coordinar la implementación, monitoreo y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) del hospital.
- Elaborar y mantener actualizadas las políticas y procedimientos de seguridad, en concordancia con la normativa institucional y legal vigente.
- Coordinar la gestión de incidentes de seguridad, la evaluación de riesgos y la continuidad operativa de los sistemas.
- Asesorar a las unidades TIC y al resto del hospital en materias de seguridad y protección de datos personales.

- Reportar periódicamente a la Jefatura del Área TIC y al Comité de Seguridad de la Información sobre el estado de cumplimiento y los riesgos identificados.

4.6 Personal Técnico y Profesional del Área TIC

- Cumplir con las políticas, procedimientos y normas internas del área TIC y del hospital.
- Ejecutar las tareas asignadas en los ámbitos de soporte, desarrollo, infraestructura, comunicaciones o seguridad, según corresponda.
- Documentar las actividades realizadas, mantener actualizado el inventario de activos tecnológicos y reportar incidentes o anomalías detectadas.
- Participar en las capacitaciones, auditorías y procesos de mejora continua promovidos por la jefatura.
- Contribuir activamente a la mejora de los servicios tecnológicos y a la satisfacción de los usuarios internos.

4.7 Usuarios Internos

- Utilizar los recursos tecnológicos institucionales de forma responsable, cumpliendo con las políticas y normativas establecidas.
- Notificar oportunamente al área TIC sobre fallas, incidentes o necesidades de soporte.
- Respetar las políticas de uso aceptable, confidencialidad y seguridad de la información.
- Participar en las instancias de capacitación o inducción tecnológica dispuestas por el hospital.

4.8 Terceros y Proveedores

- Cumplir con las políticas institucionales y las cláusulas contractuales relativas a seguridad, confidencialidad, continuidad y calidad de servicio.
- Garantizar que los servicios prestados se ajusten a los niveles de servicio (SLA) y estándares técnicos definidos por el área TIC.
- Colaborar en auditorías, revisiones o evaluaciones cuando sea requerido por el hospital.
- Reportar de forma inmediata cualquier incidente que afecte la integridad, disponibilidad o confidencialidad de los sistemas o datos institucionales.

5 RESUMEN EJECUTIVO DEL MANUAL ORGANIZACIONAL

El Manual Organizacional del Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé es un instrumento rector que formaliza la estructura, funciones, procesos y políticas que sustentan la gestión tecnológica institucional. Su propósito es consolidar el rol de las TIC como un habilitador estratégico, articulando la continuidad operativa, la seguridad de la información y la innovación digital en función de los objetivos sanitarios y administrativos del hospital.

El documento se alinea con los principios del Modelo de Gobernanza de TI basado en COBIT 2019, particularmente en los procesos APO01 (Marco de Gestión de TI) y APO02 (Gestión de la Estrategia), que orientan la definición de la visión tecnológica, la planificación estratégica, la asignación de recursos y la medición del desempeño. Su aplicación permite a la institución fortalecer la trazabilidad, el control y la sostenibilidad de las inversiones y servicios digitales.

Asimismo, el manual incorpora los lineamientos establecidos por la Ley N° 21.180 de Transformación Digital del Estado y la Ley N° 21.663 Marco de Ciberseguridad, asegurando el cumplimiento normativo y la coherencia con las políticas públicas del sector salud.

5.1 Objetivo y Contexto

El manual tiene por objetivo dotar al área TIC de un marco organizacional y de gestión integral, que facilite la planificación, ejecución y evaluación de sus funciones en un entorno sanitario altamente dependiente de la tecnología.

Su enfoque se sustenta en tres pilares estratégicos:

- **Seguridad de la Información**: Protección de los datos clínicos y administrativos bajo un enfoque de riesgo, asegurando confidencialidad, integridad y disponibilidad.
- **Infraestructura y Continuidad Operacional**: Estabilidad y resiliencia de los servicios tecnológicos críticos, garantizando la continuidad asistencial.
- **Transformación y Tecnologías Digitales**: Innovación, interoperabilidad y automatización de procesos clínico-administrativos que fortalecen la eficiencia institucional.

Estos pilares se integran en un Marco de Gestión de TI (APO01) que define la arquitectura organizativa, los roles y la gobernanza del área, y en una Gestión de Estrategia (APO02) que asegura la alineación entre las capacidades tecnológicas y los objetivos institucionales.

5.2 Estructura Organizacional

El Área de TIC depende jerárquicamente de la Subdirección Administrativa y se estructura en tres unidades funcionales interdependientes:

- **Unidad de Operaciones TI**: Responsable de la infraestructura tecnológica, soporte operativo y continuidad de servicios. Administra el Centro de Servicio TI, punto único de contacto para incidentes, solicitudes y gestión de activos tecnológicos.
- **Unidad de Tecnologías Digitales**: Lidera la modernización tecnológica, interoperabilidad de sistemas y desarrollo de soluciones digitales orientadas a la eficiencia institucional.
- **Unidad de Integridad y Seguridad de la Información**: Administra el Sistema de Gestión de Seguridad de la Información (SGSI), coordina auditorías y supervisa los controles críticos, riesgos y cumplimiento regulatorio.

La Jefatura TIC ejerce la gobernanza estratégica del área, dirigiendo la ejecución del Plan Estratégico de Tecnologías de la Información (PETI), el Marco de Gestión de TI y la supervisión de la madurez digital institucional.

A pesar de una dotación operativa limitada (70% del mínimo viable, 57% bajo régimen de compra de servicios), el área mantiene una orientación clara hacia la mejora continua y la madurez tecnológica sostenible.

5.3 Procesos y Servicios

El modelo de gestión se estructura en torno a los dominios de COBIT 2019 (EDM, APO, BAI y DSS), priorizando 19 objetivos clave enfocados en gobernanza, seguridad y calidad de los servicios tecnológicos.
La madurez promedio de los procesos se sitúa en 1.1 sobre 5, frente a una meta institucional de 2.6, lo que refleja una brecha del 53,85% y define una hoja de ruta clara hacia la optimización.

Para su seguimiento y evaluación, se utilizan modelos complementarios de madurez como C2M2 (Cybersecurity Capability Maturity Model) y MMGD (Modelo de Madurez de la Gestión Digital), que permiten medir la evolución institucional en resiliencia, gobernanza y capacidades digitales.

Los servicios operativos se encuentran formalizados en el Catálogo de Servicios TI, disponible en el portal de la Mesa de Servicio TI, donde se agrupan las prestaciones de soporte técnico, gestión de usuarios, mantenimiento, administración de infraestructura y asesoría tecnológica.

Catálogo de Servicios TI: https://hospitaldetome.freshservice.com/support/catalog/items
Portal TIC: https://tic.hospitaldetome.cl

5.4 Políticas y Seguridad

El Hospital de Tomé ha consolidado un Marco de Seguridad de la Información basado en ISO/IEC 27001:2022, el Secure Controls Framework (SCF) y las directrices del Comité de Seguridad de la Información, en cumplimiento con la Ley Marco de Ciberseguridad.

Entre las políticas y procedimientos vigentes se destacan:

- Política de Respaldo y Recuperación de la Información.
- Política de Derechos de Acceso.
- Política de Clasificación y Manejo de la Información.
- Política de Gestión de Cambios.
- Política para las Relaciones con Proveedores y Terceros.
- Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- Procedimiento de Gestión de Identidad y Derechos de Acceso.
- Procedimiento de Gestión de Vulnerabilidades.
- Procedimiento de Recuperación ante Desastres.
- Procedimiento de Continuidad y Recuperación ante Desastres

Estas políticas constituyen los controles críticos del SGSI, y su cumplimiento es obligatorio para funcionarios, contratistas y proveedores.

La supervisión de la aplicación de estas políticas recae en el Comité de Seguridad de la Información (Res. Ex. N° 848/2024) y el Comité de Modernización Digital (Res. Ex. N° 2255/2024), los cuales actúan como órganos de decisión, seguimiento y priorización estratégica.

5.5 Estrategia y Madurez Tecnológica

La Estrategia de Tecnologías de la Información (TI) constituye el núcleo articulador entre la transformación digital, la gestión clínica-administrativa y la gobernanza institucional.
Su objetivo es posicionar a las TI como un motor de crecimiento, sostenibilidad y modernización del Hospital de Tomé, habilitando capacidades analíticas, interoperables y seguras que fortalezcan la gestión basada en evidencia y el valor público en salud.

El enfoque estratégico integra metodologías y marcos internacionales (COBIT, ITIL, TOGAF, C2M2 y MMGD), permitiendo una gestión sistémica del desempeño, los riesgos, los recursos y los resultados.

Con ello, el área proyecta alcanzar una madurez tecnológica intermedia-avanzada hacia 2027, fortaleciendo su papel como socio estratégico de la dirección hospitalaria y pilar clave en la ejecución del Plan de Desarrollo Estratégico (PDE) 2024–2026.

6 MANUAL ORGANIZACIONAL

6.1 Estructura Organizacional y Funciones

6.1.1 Dependencia Jerárquica y Relación Funcional

El Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé depende jerárquicamente de la Subdirección Administrativa, la cual a su vez reporta a la Dirección del Establecimiento. La Jefatura del Área TIC ejerce la representación técnica y la conducción operativa del área frente a la Subdirección Administrativa y la Dirección, siendo responsable de la ejecución del Plan Estratégico de Tecnologías de la Información (PETI) y del cumplimiento de las políticas institucionales relacionadas con TIC.

Líneas jerárquicas clave:

- Dirección del Hospital ← Subdirección Administrativa ← Jefatura Área TIC ← Unidades funcionales (Operaciones TI, Tecnologías Digitales, Integridad y Seguridad de la Información).

6.1.2 Dependencia Funciona y coordinación transversal

Más allá de la relación jerárquica, el Área TIC mantiene dependencias funcionales con múltiples unidades del hospital para asegurar la entrega de valor clínico y administrativo. Estas relaciones funcionales se regulan mediante protocolos, convenios internos y las responsabilidades definidas en los procesos (p. ej. proyectos, gestión de cambios, continuidad y soporte).

Ejemplos de relaciones funcionales:

- Unidades clínicas (Medicina, Enfermería, Laboratorio, Imagenología): coordinación para implementación, interoperabilidad y soporte del Registro Clínico Electrónico y plataformas asociadas, como también de infraestructura y servicios.
- Subdirección Médica / Jefaturas Clínicas: revisión y aprobación de requerimientos clínicos, pruebas de aceptación y gestión de adopción.
- Gestión y Desarrollo de las Personas: coordinación para capacitación, gestión de ausentismo y gestión del cambio.
- Unidad de Finanzas y Abastecimiento: gestión de contratos, compras, licencias y presupuesto TIC.
- Gestión de Riesgos / Calidad / Prevención de Riesgos: alineamiento en continuidad operativa, seguridad física y eventos que afecten la operación asistencial.
- Oficina de Proyectos TI: coordinación operativa y metodológica de proyectos de modernización y despliegue.

6.1.3 Mecanismos de gobernanza y toma de decisiones

Para asegurar transparencia, segregación de funciones y decisión, el Área TIC articula instancias formales de gobernanza:

- Comité de Seguridad de la Información (Res. Ex. N° 848/2024)
  Función: Validar políticas, aprobar controles críticos del SGSI, priorizar iniciativas de seguridad, supervisar la gestión de incidentes y revisar resultados de auditorías.
- Comité de Modernización Digital (Res. Ex. N° 2255/2024)
  Función: Priorizar y supervisar iniciativas de transformación digital, evaluar propuestas de inversión tecnológica, articular proyectos con el PDE y COMGES, y validar impactos en procesos clínicos y administrativos.

Estas instancias definen aprobaciones, criterios de priorización y mecanismos de escalamiento; su actuación mitiga conflictos de interés y evita concentración de decisiones en una sola persona.

6.1.4 Autoridad y límites de decisión

Se establecen los siguientes niveles de autoridad para decisiones TIC, correlacionados con la materia y el impacto:

- Decisiones estratégicas y de inversión (ej.: incorporación de plataformas institucionales, presupuesto): Dirección del Hospital y Subdirección Administrativa, con recomendación técnica del Comité de Modernización Digital y Jefatura TIC.
- Decisiones de seguridad y controles críticos (ej.: aceptación de riesgos residuales, cambios en el SGSI): Comité de Seguridad de la Información con asesoría del Encargado de Seguridad de la Información.
- Aprobaciones operativas y cambios de arquitectura (ej.: cambios en configuración de red con posible impacto en producción): Jefatura TIC en conjunto con Encargado de Operaciones TI y, según el caso, con notificación al Comité de Seguridad.
- Aprobaciones de cambios rutinarios o solicitudes de usuario: gestionadas por el Centro de Servicio TI bajo procesos de gestión de cambios y procedimientos aprobados.

6.1.5 Segregación de funciones y control de conflictos

Con el objetivo de proteger la integridad de los procesos y evitar la concentración de poder o conflicto de interés, el Área TIC aplica principios de segregación de funciones en ámbitos críticos:

- Separación entre desarrollo/implementación y aprobación/recepción de cambios (p. ej. quien desarrolla no es quien aprueba la puesta en producción).
- Separación entre operaciones (soporte y mantenimiento) y auditoría/seguimiento (seguridad y cumplimiento).

Los controles de segregación se materializan mediante roles definidos, procesos formales (gestión de cambios, control de acceso, gestión de proveedores) y revisiones periódicas por el Comité de Seguridad de la Información.

6.1.6 Escalamiento y continuidad operativa

Se define la ruta de escalamiento ante incidentes operativos o de seguridad:

1. Centro de Servicio TI — recepción y primer nivel de diagnóstico.
2. Encargado de Operaciones TI / Especialistas — segundo nivel de soporte y resolución técnica.
3. Jefatura TIC / Encargado de Seguridad — escalamiento en incidentes con impacto institucional. (Puede incluir a Subdirección Administrativa)
4. Comité de Seguridad / Dirección — activación de Comité y decisiones estratégicas en incidentes mayores o crisis (p. ej. incidentes de ciberseguridad, interrupción crítica de servicios clínicos).

Los procedimientos de escalamiento están descritos en los Procedimientos de Gestión de Incidentes y en el Plan de Continuidad de Negocio / Recuperación ante Desastres.

6.1.7 Subrogancias y continuidad de mando

La subrogancia del Área TIC se establece para mantener continuidad operativa y priorizar la estabilidad del servicio. El orden de subrogancias es el siguiente (resumen):

Rol	1era Subrogancia	2da Subrogancia	3era Subrogancia
Jefe de Área TI	Operaciones TI	Tecnologías Digitales	Subdirección Administrativa
Encargado Operaciones TI	Jefe de Área TI	—	—
Encargado de Seguridad	Jefe de Área TI	—	—
Encargada Tecnologías Digitales	Jefe de Área TI	—	—
Encargada Centro de Servicio	Operaciones TI	Jefe de Área TI	—

Reglas de subrogancia: durante el período de subrogancia no se permiten cambios de procesos ni aprobaciones que impliquen modificaciones estratégicas sin la venia expresa de la Jefatura (o de la Subdirección Administrativa para decisiones de mayor impacto).

6.1.8 Relación con proveedores y terceros

La interacción con proveedores se gestiona a través de contratos, convenios y pólizas que definen responsabilidades, niveles de servicio (SLA), controles de seguridad y cláusulas de confidencialidad. La Unidad de Tecnologías Digitales y la Jefatura TIC coordinan requisitos técnicos; la Subdirección Administrativa formaliza los contratos y controla el cumplimiento financiero.

Los proveedores que gestionan datos o servicios críticos deben cumplir con los requerimientos del SGSI y someterse a evaluaciones de seguridad y auditorías periódicas.

6.2 Antecedentes y Fundamentos del Área TIC

6.2.1 Formación del Área

El Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé, dependiente de la Subdirección Administrativa, fue oficialmente constituida mediante la Resolución Exenta N°1711 del 6 de marzo de 2016.

Previamente, la gestión tecnológica operaba como un centro de costo enfocado principalmente en la administración y soporte de infraestructura TI.

La formalización del área respondió a la necesidad de incorporar las Tecnologías de la Información a la estrategia institucional, impulsada inicialmente por la implementación del Registro Clínico Electrónico (RCE).

En el año 2017, mediante Resolución Exenta N°597 del 16 de enero de 2017, se redefinieron sus funciones, incorporando unidades como Información en Salud, Archivo, Gestión Documental y la Subrogancia de la Unidad de Admisión.

A partir de esta expansión funcional, el área comenzó a participar en diversos comités institucionales, entre ellos:

- Comité de Epidemiología (Rex. N°2538/06.06.2016)
- Comité de Lobby (Rex. N°2390/02.05.2017)
- Comité Comunicacional (Rex. N°847/18.05.2015)
- Comité de Gestión de Riesgos Críticos (Rex. N°1088/25.06.2015)

Adicionalmente, el Jefe de Tecnologías de la Información fue designado como Referente del Proyecto SIDRA mediante Resolución Exenta N°736/04.05.2015, consolidando la participación del área en proyectos estratégicos del Servicio de Salud.

Incluso, entre el 22 de noviembre de 2018 y el 28 de enero de 2019, la jefatura del área asumió la subrogancia de la Subdirección Administrativa, reflejando el reconocimiento institucional de su madurez operativa y capacidad de gestión.

Actualmente, el área mantiene una estructura actualizada y orientada a la Transformación Digital, fortaleciendo la Continuidad Operacional y la Seguridad de la Información, según lo establecido en la Resolución Exenta N°108/31.01.2023.

El Área de Tecnologías de la Información y Comunicación depende jerárquicamente de la Subdirección Administrativa del Hospital, formando parte de la estructura estratégica que sustenta la gestión operativa, financiera y de soporte institucional.
Su función transversal la posiciona como un actor clave en la implementación de políticas de modernización, la gobernanza tecnológica y la provisión de servicios digitales que habilitan la gestión clínica y administrativa del establecimiento.

El área articula sus acciones con otras subdirecciones, unidades y comités institucionales, en particular con el Comité de Seguridad de la Información y el Comité de Modernización Digital, los cuales aseguran la segregación de funciones y la toma de decisiones colegiadas en materias críticas relacionadas con la seguridad, la innovación y la priorización de proyectos tecnológicos.

6.2.2 Misión

El Área de Tecnologías de la Información y Comunicación, dependiente de la Subdirección Administrativa, tiene como misión brindar servicios tecnológicos profesionales, de calidad y oportunos, basados en estándares de mejora continua, alineamiento estratégico y eficiencia.

Su propósito es apoyar y generar valor al cumplimiento de los objetivos institucionales del Hospital de Tomé mediante el uso ético, seguro y eficiente de las Tecnologías de la Información.

6.2.3 Visión

El Área TIC busca posicionarse como un pilar estratégico de alto valor institucional, a través de una infraestructura robusta, una gestión digital moderna y una cultura de seguridad de la información madura.

Su visión es consolidar procesos tecnológicos con niveles avanzados de madurez y gobernanza, impulsando soluciones innovadoras, accesibles y sostenibles que fortalezcan la atención de salud y la gestión administrativa del hospital.

6.2.4 Valores Institucionales

Los valores del Área TIC constituyen la base ética y cultural que guía sus decisiones y comportamientos, garantizando la coherencia entre los principios institucionales y la acción tecnológica diaria.

Valor	Principio orientador	Evidencia en la práctica
Ética	Actuamos con integridad, justicia y respeto por la confidencialidad.	- Protección de datos personales y sensibles. - Selección de proveedores sin conflictos de interés. - Procesos con segregación y probidad.
Confiabilidad	Fomentamos la credibilidad mediante resultados consistentes.	- Cumplimiento de plazos y calidad en entregables. - Comunicación transparente con los usuarios. - Garantía de disponibilidad de sistemas críticos.
Compromiso	Nos involucramos plenamente con los objetivos del hospital.	- Participación en la planificación estratégica. - Capacitación continua. - Respuesta oportuna a incidencias críticas.
Eficiencia	Optimizamos recursos humanos, técnicos y financieros.	- Reutilización de infraestructura. - Uso de tecnologías abiertas. - Implementación de metodologías ágiles (Kanban, Scrum).
Empatía	Entendemos las necesidades de los usuarios internos.	- Escucha activa y soporte humano. - Comunicación clara en momentos críticos. - Diseño de soluciones orientadas al usuario.

6.2.5 Organigrama

El Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé cuenta con una estructura organizacional diseñada como respuesta directa a las necesidades institucionales, los estándares técnicos y normativos del sector salud, y los principios establecidos en su misión y visión.

Esta estructura busca alinear la gestión tecnológica con los objetivos estratégicos del hospital, asegurando la continuidad operativa, la seguridad de la información, la modernización digital y la gobernanza efectiva de los recursos tecnológicos.

Su configuración obedece a tres criterios fundamentales:

- **Alineamiento estratégico e institucional**: La organización del área se articula con la planificación institucional y los lineamientos del Ministerio de Salud, garantizando que las decisiones tecnológicas respondan a las prioridades asistenciales, administrativas y de desarrollo organizacional del establecimiento.

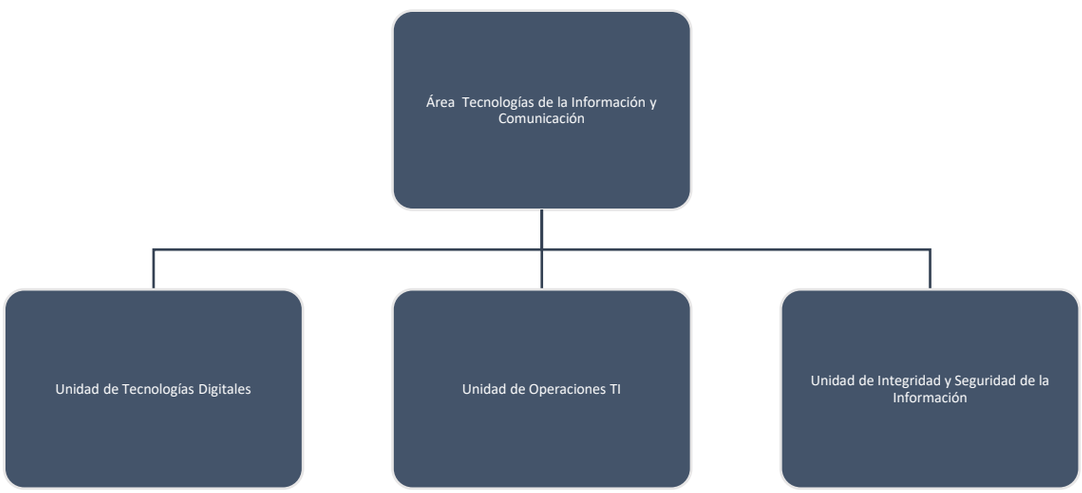
- **Cumplimiento de estándares y buenas prácticas**: La estructura se basa en los marcos COBIT 2019 (APO01, APO02), ITIL v4, ISO/IEC 27001 y ISO/IEC 20000, que promueven la trazabilidad, la gestión por procesos y la mejora continua de los servicios tecnológicos. Su diseño favorece la segregación de funciones, la transparencia en la toma de decisiones y la delimitación clara de responsabilidades.
- **Adaptabilidad y madurez tecnológica**: La estructura organizacional evoluciona conforme a las necesidades del hospital, buscando fortalecer las capacidades institucionales en transformación digital, ciberseguridad y continuidad operacional. Los roles especializados permiten abordar integralmente la operación, la gestión de la información y el soporte a los usuarios, garantizando un servicio TI eficiente, seguro y orientado al usuario final.

El organigrama refleja esta visión integrada, mostrando la dependencia jerárquica del Área TIC respecto de la Subdirección Administrativa y la distribución interna en tres unidades funcionales:

- Unidad de Operaciones TI
- Unidad de Tecnologías Digitales
- Unidad de Integridad y Seguridad de la Información

Además, los ámbitos de gestión del Sistema de Gestión de Seguridad de la Información (SGSI) y de Transformación Digital se desarrollan con el apoyo de comités institucionales especializados, garantizando la segregación de funciones y la gobernanza colaborativa, tales como el:

- Comité de Seguridad de la Información (Res. Ex. N° 848/2024)
- Comité de Modernización Digital (Res. Ex. N° 2255/2024)



El presente organigrama corresponde a la estructura funcional vigente del Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé. En los anexos del presente manual se detalla tanto la estructura actual, con sus dependencias y roles operativos definidos por resolución, como la estructura proyectada, orientada al fortalecimiento institucional y al cumplimiento de los objetivos estratégicos establecidos en el Plan Estratégico de Tecnologías de la Información (PETI).

6.3 Funciones del Área TIC y de sus Unidades

El Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé tiene como función general planificar, desarrollar, implementar y mantener los sistemas, servicios e infraestructuras tecnológicas que soportan la gestión clínica, administrativa y estratégica del establecimiento.

Sus funciones se orientan a garantizar la continuidad operativa, la seguridad de la información, la eficiencia institucional y la modernización digital, conforme a los principios de gobernanza establecidos en los marcos COBIT 2019, ITIL v4, ISO/IEC 27001 y ISO/IEC 20000-1.

Entre sus funciones generales se destacan:

Ámbito de Función	Descripción / Actividades Principales
Planificación y Gobernanza Tecnológica	• Elaborar y mantener actualizado el *Plan Estratégico de Tecnologías de la Información (PETI)* y los planes operativos asociados. • Alinear las inversiones y proyectos tecnológicos con los objetivos estratégicos institucionales y del Servicio de Salud. • Participar en la formulación y seguimiento del presupuesto TIC, asegurando el uso eficiente de los recursos.
Gestión de Infraestructura y Servicios TI	• Administrar los activos tecnológicos del hospital, asegurando su operación continua, disponibilidad y mantenimiento. • Proveer servicios de soporte técnico y gestión de incidentes conforme a los niveles de servicio establecidos (SLA). • Supervisar la capacidad, rendimiento y obsolescencia de la infraestructura tecnológica.
Seguridad y Continuidad Operativa	• Implementar y mantener el *Sistema de Gestión de Seguridad de la Información (SGSI)* bajo los lineamientos de la ISO/IEC 27001. • Coordinar las acciones del *Plan de Continuidad Operativa* y *Recuperación ante Desastres (BCP/DRP)*. • Monitorear y gestionar riesgos tecnológicos y de ciberseguridad.
Transformación Digital y Gestión de Proyectos	• Impulsar iniciativas de modernización digital, interoperabilidad e innovación tecnológica que fortalezcan los procesos clínicos y administrativos. • Gestionar el portafolio de proyectos tecnológicos institucionales en coordinación con los comités de modernización digital. • Promover la adopción de tecnologías emergentes y buenas prácticas digitales.
Gestión de Datos y Aplicaciones Institucionales	• Administrar los sistemas de información institucionales, incluyendo el *Registro Clínico Electrónico (RCE)* y las plataformas administrativas. • Velar por la integridad, confidencialidad y disponibilidad de la información institucional. • Supervisar el ciclo de vida de las aplicaciones, desde su desarrollo hasta su retiro.
Cumplimiento Normativo y Control Interno	• Asegurar la conformidad con la normativa vigente en materia de ciberseguridad, transparencia, protección de datos y gestión documental. • Promover la segregación de funciones, la trazabilidad y la auditoría de procesos tecnológicos. • Participar en revisiones y auditorías internas y externas.

Relaciones Institucionales y Soporte a la Gestión	• Asesorar a la Dirección y Subdirecciones en materia tecnológica, participando en los comités institucionales definidos. • Coordinar con proveedores y terceros la prestación de servicios tecnológicos bajo criterios de calidad, seguridad y eficiencia. • Mantener relaciones de colaboración con el Servicio de Salud y organismos ministeriales en temas de interoperabilidad y estándares.
Gestión de Innovación y Mejora Continua	• Fomentar la innovación tecnológica orientada a la mejora de procesos clínicos y administrativos. • Evaluar tendencias y soluciones tecnológicas que contribuyan a la eficiencia institucional. • Medir y mejorar el desempeño de los servicios mediante indicadores (KPI) y revisiones periódicas.

6.3.1 Funciones Unidad de Tecnologías Digitales

Responsable de la planificación estratégica, la gestión de proyectos, el control de inversiones tecnológicas y la alineación de las iniciativas TIC con los objetivos institucionales y ministeriales. Esta unidad actúa como vínculo entre la Dirección del Hospital y la operación tecnológica, velando por la trazabilidad, la priorización y la eficiencia del gasto TIC (Digitalización) como retorno a la generación de valor.

Función Específica	Descripción / Actividades Principales
Planificación Estratégica y Presupuestaria	Elaborar, actualizar y monitorear el *Plan Estratégico de Tecnologías de la Información (PETI)* y los planes operativos anuales.
Gestión de Proyectos y Portafolio TIC	Coordinar, priorizar y supervisar los proyectos tecnológicos en curso, en alineación con los comités de modernización digital.
Control y Evaluación de Inversiones	Evaluar técnicamente las adquisiciones y contratos TIC, asegurando el cumplimiento normativo y la pertinencia funcional.
Gestión de Indicadores y Reportabilidad	Definir y monitorear indicadores de desempeño (KPI) y generar reportes de avance para la toma de decisiones.
Coordinación Institucional y Ministerial	Representar al Hospital ante instancias regionales o ministeriales en materia de digitalización y de interoperabilidad.

6.3.2 Funciones Unidad Operaciones TI

Encargada de administrar y mantener la infraestructura tecnológica, los sistemas de información, los activos digitales y los servicios de soporte técnico, asegurando la continuidad operativa y la satisfacción de los usuarios internos.

Función Específica	Descripción / Actividades Principales
Administración de Infraestructura	Gestionar servidores, redes, almacenamiento, comunicaciones y equipamiento computacional del hospital.
Gestión de Sistemas y Aplicaciones	Mantener operativos los sistemas de información institucionales (clínicos, administrativos, financieros y de gestión).

Soporte Técnico y Atención de Incidentes	Brindar asistencia técnica presencial y remota a los usuarios, conforme a los niveles de servicio (SLA).
Gestión de Activos y Licencias	Controlar inventario, licenciamiento y renovación de equipos, software y contratos asociados.
Monitoreo y Rendimiento Operacional	Supervisar la capacidad, disponibilidad y desempeño de la infraestructura tecnológica.

6.3.2.1 Centro de Servicio TI

El Centro de Servicio TI constituye la subunidad operativa encargada de gestionar de manera centralizada todas las solicitudes, incidencias y requerimientos tecnológicos del Hospital de Tomé.

Depende funcional y jerárquicamente de la Unidad de Operaciones TI, y actúa como punto único de contacto (Single Point of Contact – SPOC) entre los usuarios internos y el Área TIC.

Su operación se basa en las buenas prácticas de ITIL v4 y en el proceso DSS02 de COBIT 2019 – "Gestionar las peticiones y los incidentes de servicio", garantizando la trazabilidad, priorización y resolución oportuna de los requerimientos tecnológicos institucionales.

Ámbito de Gestión	Funciones Específicas
Gestión de solicitudes e incidentes	Recepción, categorización, priorización y asignación de tickets según criticidad, tipo de servicio y nivel de impacto.
Cumplimiento de SLA y seguimiento	Monitorear los niveles de servicio (SLA), escalar los casos conforme a los procedimientos definidos y asegurar la trazabilidad de las soluciones.
Comunicación con el usuario	Mantener informados a los usuarios sobre el estado de sus requerimientos y tiempos estimados de resolución, garantizando transparencia en la gestión.
Documentación y trazabilidad	Registrar todas las incidencias y solicitudes en el sistema de gestión de servicios (mesa de ayuda), generando reportes e indicadores de desempeño.
Mejora continua y análisis de recurrencias	Identificar problemas recurrentes y proponer medidas preventivas o correctivas en conjunto con la Unidad de Operaciones TI y la Unidad de Seguridad.
Soporte de primer nivel	Ejecutar diagnósticos básicos, resolver incidencias menores y derivar los casos de segundo nivel a especialistas de infraestructura o aplicaciones. (Unidad de Operaciones TI / Unidad de Tecnologías Digitales / Unidad de Seguridad de la Información)

Nota: El *Centro de Servicio TI* consolida la gestión operativa de la demanda tecnológica y representa el punto de medición principal de la percepción de valor del servicio TIC en el hospital.
Su modelo de atención, catálogo de servicios, flujos de escalamiento y métricas asociadas se detallan en el **Anexo: Catálogo de Servicios TIC y Procedimientos de Atención**.

6.3.3 Funciones Unidad de Seguridad de la Información

Responsable de implementar, mantener y fortalecer el *Sistema de Gestión de Seguridad de la Información (SGSI)*, así como los planes de continuidad operativa y recuperación ante desastres. Esta unidad asegura el cumplimiento normativo y la gestión de riesgos tecnológicos, como también de gestión de incidentes de seguridad de la Información.

Función Específica	Descripción / Actividades Principales
Gestión de Seguridad de la Información (SGSI)	Implementar políticas, controles y procedimientos conforme a la ISO/IEC 27001 y la normativa del MINSAL.
Gestión de Riesgos Tecnológicos	Identificar, evaluar y tratar riesgos asociados a la operación tecnológica e infraestructura crítica.
Continuidad Operativa y Recuperación ante Desastres (BCP/DRP)	Mantener actualizados y operativos los planes de continuidad y recuperación de servicios críticos.
Cumplimiento Normativo y Auditorías	Coordinar auditorías internas y externas relacionadas con seguridad, transparencia y protección de datos personales.
Concientización y Cultura de Seguridad	Promover capacitaciones, campañas y buenas prácticas en ciberseguridad dirigidas al personal institucional.

En los anexos se incluye el organigrama detallado del Área TIC, tanto en su estructura actual como en su versión proyectada, junto con la distribución funcional y los perfiles asociados a cada unidad.

6.4 Procesos Clave del Área TIC

6.4.1 Enfoque de Gestión por Procesos

El Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé estructura su funcionamiento bajo un enfoque de gestión por procesos, en conformidad con los principios de COBIT 2019, ITIL v4 e ISO/IEC 20000-1.
Este enfoque permite que las actividades del área se desarrollen de forma planificada, medible y alineada con los objetivos institucionales, garantizando trazabilidad, eficiencia y mejora continua.

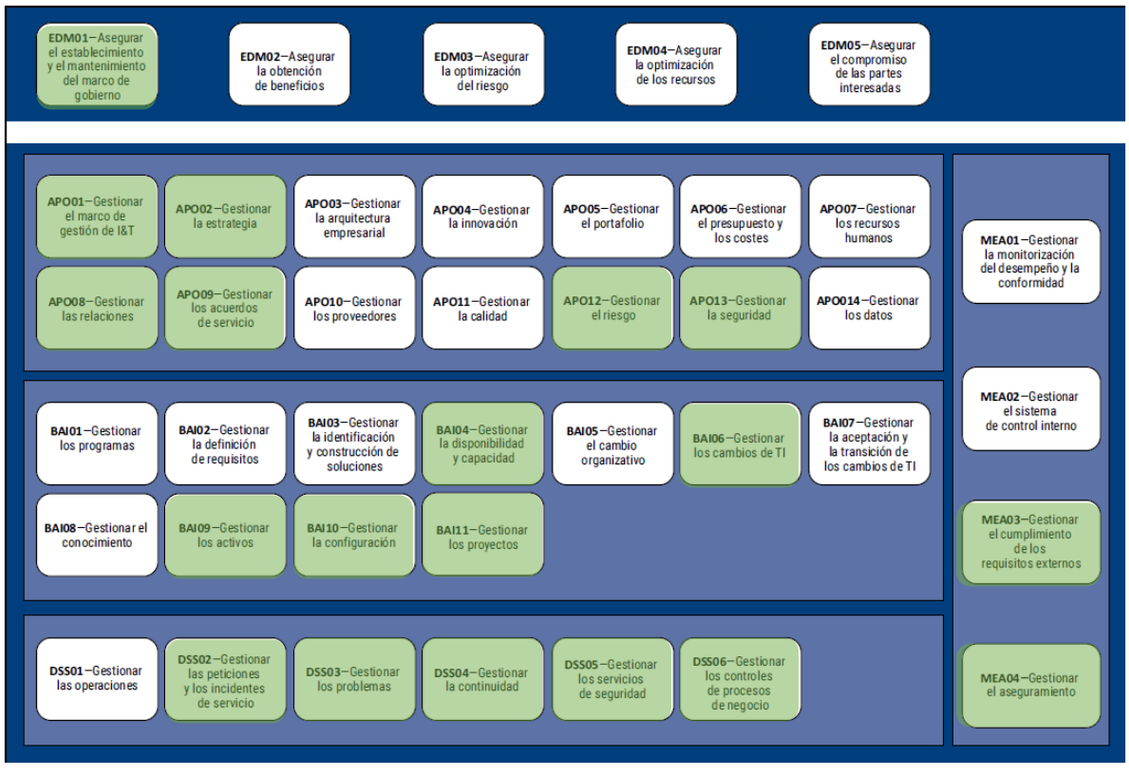
En el contexto hospitalario, donde conviven procesos clínicos, administrativos y de apoyo, esta metodología facilita una interacción transparente entre las unidades usuarias y el área TIC, asegurando que los requerimientos tecnológicos sean gestionados bajo criterios de prioridad, criticidad y seguridad.

6.4.2 Marco de Referencia: COBIT 2019

COBIT 2019 constituye el marco de referencia principal para la estructuración de los procesos del área TIC, permitiendo una visión integral de gobierno y gestión.
Actualmente, el Hospital de Tomé ha identificado 19 procesos clave, distribuidos en los dominios de Gobierno (EDM), Alineación, Planificación y Organización (APO), Construcción, Adquisición e Implementación (BAI), Entrega, Servicio y Soporte (DSS) y Monitoreo, Evaluación y Valoración (MEA).

Estos procesos constituyen la columna vertebral operativa del área, orientando las acciones, políticas y procedimientos que se implementan.

A continuación, se presenta un gráfico de los procesos asumidos por el área TIC por priorización de necesidades respecto al Plan de Desarrollo Estratégico Institucional.



Cabe destacar que los procesos indicados tienen distinto nivel de madurez y el fortalecimiento de estos es parte de la estrategia de gobernanza del Área.

6.4.3 Integración con Políticas, Procedimientos y Catalogo de Servicios

Cada proceso COBIT se vincula con políticas institucionales, procedimientos operativos y registros técnicos, que permiten su ejecución práctica.

Por ejemplo:

- El proceso DSS02 "Gestionar incidentes y solicitudes de servicio" se implementa mediante el Procedimiento de Gestión de Incidentes de Seguridad, complementado por el Catálogo de Servicios TIC.
- El proceso APO12 "Gestionar riesgos" se apoya en la Política de Gestión de Riesgos de Seguridad de la Información.
- El proceso DSS04 "Gestionar la continuidad" se articula con los Planes de Continuidad Operativa y Recuperación ante Desastres.
- El proceso BAI06 "Gestionar cambios de TI" se regula por la Política de Gestión de Cambios y su flujo de aprobación definido en el Comité de Modernización Digital.

El Catálogo de Servicios TIC, que se presenta en el Anexo correspondiente, agrupa los servicios ofrecidos a las distintas unidades del hospital, clasificándolos según su criticidad, nivel de servicio (SLA) y responsable del proceso asociado.

6.4.4 Lógica de Operación del Área TIC

El funcionamiento operativo del área se basa en una cadena de valor que conecta:

- Estrategia y planificación tecnológica (APO01–APO02)
- Desarrollo e implementación de soluciones (BAI09–BAI11)
- Entrega y soporte continuo de servicios (DSS02–DSS06)

- Monitoreo, aseguramiento y mejora (MEA03–MEA04)

De esta manera, el área asegura una gestión integral, que no solo atiende incidentes o proyectos, sino que administra el ciclo de vida completo de los servicios tecnológicos del Hospital.

6.4.5 Armonización Procedimental ante Directrices Externas

El presente procedimiento regula la gestión, análisis y respuesta técnica ante la recepción de directrices, instrucciones u operativos normativos de carácter operativo emitidos por el Servicio de Salud Talcahuano (SST) que incidan en los procesos internos, la arquitectura tecnológica, la seguridad de la información y la continuidad operacional del Hospital de Tomé. Su objetivo es resguardar la autonomía de gestión del establecimiento y garantizar que toda bajada operativa externa se adapte armónicamente a la realidad de alta complejidad y al sistema de compliance local.

En el proceso de revisión, objeción y contrapropuesta de procedimientos externos participarán formalmente los siguientes roles:

1. **Jefatura del Área de Tecnologías de la Información y Comunicación (TIC):** Encargado de realizar el análisis técnico de impacto operacional, ciberseguridad, interoperabilidad y compatibilidad de infraestructura de las directrices emitidas.
2. **Subdirección Administrativa:** Encargada de evaluar la viabilidad administrativa, presupuestaria y estratégica de la instrucción, velando por la coherencia con los objetivos institucionales del hospital.
3. **Dirección del Hospital:** Máxima autoridad ejecutiva del establecimiento, competente para validar formalmente el análisis, suscribir las observaciones técnicas y presentar la propuesta alternativa ante la autoridad superior del Servicio de Salud.

Ante la recepción formal de un procedimiento operativo proveniente del Servicio de Salud, el flujo de gestión institucional se ejecutará bajo las siguientes etapas obligatorias:

- **Fase 1: Análisis Técnico Preliminar (Plazo máximo: 5 días hábiles desde la recepción).** El Área TIC, en conjunto con las unidades involucradas, efectuará una revisión detallada del instructivo externo para identificar posibles anomalías operacionales, brechas de seguridad, riesgos de continuidad de servicio o colisiones con los procedimientos locales vigentes.
- **Fase 2: Elaboración de Informe de Observaciones y Contrapropuesta (Plazo máximo: 10 días hábiles).** Si el análisis detecta perjuicios operacionales o de *compliance* local, la Jefatura TIC elaborará un informe técnico fundamentado. Este informe deberá incluir obligatoriamente una propuesta técnica alternativa válida que cumpla con el estándar de control o la finalidad buscada por el Servicio de Salud, pero adaptada a la arquitectura y los procedimientos vigentes del Hospital de Tomé.
- **Fase 3: Validación y Emisión Institucional.** El informe técnico y la contrapropuesta serán visados por la Subdirección Administrativa y sometidos a la aprobación formal de la Dirección del Hospital.
- **Fase 4: Presentación y Registro Formal.** Mediante Oficio conductor firmado por la Dirección del Hospital, se remitirán al Servicio de Salud Talcahuano las observaciones técnicas junto con la propuesta alternativa validada localmente, solicitando su ponderación y autorización formal. Copia de este antecedente quedará archivada en el control normativo del Área TIC.

En caso de que el Servicio de Salud ratifique su instrucción inicial sin acoger la contrapropuesta local, el Hospital de Tomé adoptará el lineamiento superior para dar cumplimiento al principio de jerarquía administrativa, pero **se eximirá de la responsabilidad directa por los incidentes de continuidad operacional o brechas técnicas** que la aplicación de dicho procedimiento genere, siempre y cuando estas anomalías hubiesen sido advertidas documentadamente y de forma oportuna en el informe técnico original elevado por la Jefatura TIC y la Dirección del Establecimiento.

6.4.6 Nivel de Madurez y Mejora continua de Procesos

La evaluación de madurez de los procesos (basada en COBIT 2019) permite identificar brechas y definir un Plan de Mejoramiento Progresivo orientado a alcanzar los niveles requeridos.

Este plan se articula con el Plan Estratégico de Tecnologías de la Información (PETI), priorizando aquellos procesos que fortalecen la seguridad de la información, la continuidad de los servicios críticos y la transformación digital, integrando todo simultáneamente con el Plan de Desarrollo Estratégico, generando valor directo a la misión institucional y asegurando de esta manera alineación integral y transparente.

7 COMITÉS Y GOBERNANZA

7.1 Propósito y Alcance

Los Comités del Área TIC son instancias colegiadas de gobernanza que aseguran la toma de decisiones transparente, la priorización de inversiones y proyectos, la supervisión de la ejecución de políticas críticas y el control de riesgos tecnológicos. Estas instancias materializan la aplicación de los principios de gobernanza definidos en COBIT 2019 (particularmente los objetivos EDM y APO) y permiten la adecuada segregación de funciones entre la Jefatura TIC, la Subdirección Administrativa y la Dirección del Hospital.

El presente apartado describe la estructura, funciones, autoridades y reglas de operación de los comités institucionales vinculados a TIC.

7.2 Comités y Equipos institucionales relevantes

7.2.1 Comité de Seguridad de la Información (Res. Ex. N° 848/2024)

Objetivo: Validar políticas y controles críticos del SGSI, priorizar iniciativas de seguridad, supervisar la gestión de incidentes y revisar hallazgos de auditoría relacionados con seguridad de la información.
Alcance: Todas las decisiones relativas a la política de seguridad, aceptación de riesgos residuales, ejercicios de recuperación y pruebas BCP/DRP, y autorizaciones de excepciones temporales a controles.

7.2.2 Comité de Modernización Digital (Res. Ex. N° 2255/2024)

Objetivo: Priorizar y supervisar iniciativas de transformación digital y modernización, evaluar propuestas de inversión tecnológica, articular proyectos con el PDE y COMGES y validar impactos en procesos clínicos y administrativos.
Alcance: Portafolio de proyectos TIC, criterios de priorización de inversiones, planes de adopción digital y análisis de impacto en procesos del hospital.

7.2.3 Oficina de Proyectos TI

Objetivo: constituye una unidad operativa dependiente del Área de Tecnologías de la Información y Comunicación, creada con el objetivo de liderar, coordinar y supervisar los proyectos tecnológicos institucionales, tanto clínicos como administrativos.
Su misión es asegurar que las iniciativas digitales se gestionen de forma estructurada, alineadas con los objetivos estratégicos del Hospital, fomentando la eficiencia, la calidad de los procesos y la mejora continua de los servicios institucionales.
Alcance: Implementaciones y/o mejora continua de sistemas que puedan tener un alto impacto de nivel institucional y que necesiten una adecuada articulación. Generalmente estará asociado a sistemas considerado como Críticos.

Cargo / Rol	Función Principal	Dependencia / Rol Asociado

Jefe de Oficina de Proyectos	Supervisar estratégicamente la cartera de proyectos, asegurar la alineación con los objetivos institucionales y validar el cumplimiento de los hitos técnicos y financieros.	Jefe del Área de Tecnologías de la Información y Comunicación
Jefa de Proyecto	Coordinar la ejecución operativa de los proyectos, realizar seguimiento a los avances, gestionar riesgos y asegurar la entrega de resultados conforme al plan aprobado.	Encargado/a de Tecnologías Digitales
Gestor/a del Cambio	Liderar el componente de gestión del cambio, comunicación y capacitación, asegurando la adopción efectiva de nuevas soluciones por parte del personal.	Encargado/a de Desarrollo de Personas
Gestor/a Clínico/a	Representar los intereses y requerimientos de las áreas asistenciales, validando que las soluciones tecnológicas respondan a los flujos y necesidades clínicas.	Jefe/a del Servicio de Medicina

Nota: La composición de la Oficina de Proyectos podrá adaptarse de acuerdo con la naturaleza y complejidad de cada iniciativa, incorporando temporalmente otros especialistas técnicos, clínicos o administrativos.

La Oficina de Proyectos TI actúa como vínculo operativo entre la Jefatura TIC, los Comités de Modernización Digital y las Unidades usuarias.

Todas las iniciativas deben estar registradas en el Portafolio de Proyectos Institucional, y su priorización se realiza conforme a los criterios definidos por el Comité de Modernización Digital y la Subdirección Administrativa.

La documentación técnica, actas de reunión, cronogramas y entregables se almacenan en la Nube Institucional → Documentación TI → Oficina de Proyectos, garantizando trazabilidad, auditoría y transparencia.

7.2.4 Coordinación de Alta Dirección de TI

Se establece formalmente la Coordinación de Alta Dirección de TI como la instancia oficial de encuentro, análisis estratégico y toma de decisiones conjunta entre la Jefatura del Área de Tecnologías de la Información y Comunicación (TIC) y la Subdirección Administrativa del Hospital de Tomé. Su propósito central es formalizar la gestión del área, asegurar el alineamiento de los proyectos tecnológicos con los objetivos institucionales, coordinar la priorización de recursos, y gestionar de manera compartida los riesgos tecnológicos y operativos, evitando la toma de decisiones aisladas y garantizando la participación de la Subdirección en el gobierno de las tecnologías del establecimiento.

La instancia estará constituida formalmente por:

1. **Subdirección Administrativa:** Quien presidirá la instancia y velará por la coherencia presupuestaria, administrativa y estratégica.
2. **Jefatura del Área de Tecnologías de la Información y Comunicación (TIC):** Quien actuará como secretario técnico, presentando la cuenta de gestión, los mapas de riesgo y las propuestas de priorización. *Nota:* Podrán ser convocados en calidad de invitados permanentes u ocasionales otros referentes de unidades clínicas o administrativas cuando los temas de infraestructura o sistemas así lo requieran.

Frecuencia: Las sesiones se realizarán con carácter ordinario y obligatorio de forma bimensual. Adicionalmente, podrán convocarse sesiones extraordinarias a solicitud de cualquiera de sus integrantes ante situaciones críticas de ciberseguridad, fallas graves de continuidad operacional o contingencias normativas.

Formalidad: Cada sesión deberá quedar registrada formalmente mediante una Acta de Acuerdos y Seguimiento, la cual contendrá los temas tratados, las decisiones adoptadas, los niveles de prioridad asignados a los proyectos y los responsables de su ejecución. Dicho registro formará parte integral del sistema de gestión del Área TIC.

Serán competencias exclusivas de esta instancia de gobernanza:

- **Cuenta de Gestión y Avances:** Revisión del estado de cumplimiento de los planes de trabajo, proyectos de infraestructura y modernización tecnológica ejecutados por el Área TIC.
- **Alineamiento y Priorización:** Evaluar y aprobar la estrategia institucional en materia de sistemas, determinando las prioridades de desarrollo e implementación ante recursos limitados.
- **Gestión de Riesgos y Ciberseguridad:** Evaluar los riesgos operacionales, vulnerabilidades detectadas, planes de contingencia y el impacto de normativas externas (provenientes del Servicio de Salud o del MINSAL) sobre la plataforma tecnológica del hospital.
- **Resguardo de la Toma de Decisiones:** Consolidar una instancia de validación jerárquica donde la Subdirección Administrativa se interiorice y avale las decisiones técnicas complejas tomadas por el Área TIC, asumiendo una gobernanza compartida y reduciendo la discrecionalidad operativa aislada.

8 GESTIÓN OPERATIVA ÁREA TIC

8.1 Horarios de Atención del Área TIC

El Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé establece sus horarios de atención y operación con el objetivo de garantizar la continuidad de los servicios tecnológicos institucionales y la atención oportuna a los usuarios internos.

Horario de funcionamiento general:

- Lunes a Jueves: de 08:00 a 17:00 horas (jornada hábil administrativa).
- Viernes: de 8:00 a 16:00 horas

Horario de colación: se realiza por turnos para mantener continuidad operacional para el soporte nivel 1, en caso excepcional de no tener esta rotación disponible, se indicará en modalidad de aviso en el Centro de Servicio (web)

Cobertura extendida y contingencias:

Fuera del horario hábil, no es disponible el soporte institucional, destinado a la atención de incidentes que afecten la continuidad de los servicios clínicos o administrativos esenciales, sin embargo, para situaciones de prioridad Alta a Urgente los funcionarios principalmente de Registro Clínico Electrónico y/o Sistema de Imagenología, podrán utilizar los siguientes contactos:

- **Sistema de Imagenología (Medicap)**
  - Contacto Telefónico Soporte +569 8775 0109
  - Jefatura de Soporte (Solo caso justificado) +569 7518 4536
- **Registro Clínico Electrónico (TrakCare)**
  - Contacto Telefónico Soporte +80038700

Estos accesos a reporte de incidentes solo deben utilizarse en horario inhábil y siempre que sea una situación que no pueda esperar.

Es importante mencionar que existen protocolos de calidad y seguridad del paciente relativos a la continuidad de la atención en modalidad de contingencia, los cuales deberán aplicarse para estos casos.

Canales oficiales de atención:

- Sitio Web Área de Tecnologías: https://tic.hospitaldetome.cl/
- Sitio Web Centro de Servicio TI: https://mda.hospitaldetome.cl/
- Portal Mesa de Ayuda: https://hospitaldetome.freshservice.com/support/home
- Teléfono interno de soporte: 415016
- Aplicación Móvil: Descargar desde una Store (Apple o Android) App Freshservice
    - Entrar con credenciales (correo institucional y clave de sistema)
    - URL de sistema: https://hospitaldetome.freshservice.com/
- Presencial, ubicada en Mariano Egaña 1685:
    - Oficina TIC, Tercer Piso.
    - Oficina Jefe TIC, Primer Piso

Compromiso de atención:
El área garantiza una respuesta inicial dentro de los plazos definidos en los SLA del Catálogo de Servicios TI, priorizando las incidencias críticas que impacten directamente en la atención al paciente o en los procesos institucionales esenciales.

Prioridad	Primera Respuesta	Solución
Urgente	20 Minutos	30 Minutos
Alta	20 Minutos	45 Minutos
Medio	20 Minutos	1 Día
Bajo	30 Minutos	5 Días

El Área TIC mantiene compromisos de respuesta y resolución definidos según la criticidad de la incidencia y la disponibilidad de recursos internos y de proveedores.
Estos tiempos de atención reflejan la capacidad actual de gestión del área, considerando su dotación, infraestructura, herramientas y soporte externo contratado.
Los tiempos establecidos representan el estándar operativo actual del Área TIC.
Cualquier modificación o ajuste a estos plazos implica impactos directos en la inversión institucional, la contratación de servicios externos, la capacidad de respuesta del personal TIC y la infraestructura tecnológica de soporte.
Los SLA son revisados anualmente en función de los resultados del Catálogo de Servicios y del Plan de Continuidad Operativa.

8.2 Dependencias Físicas y Recursos del Área TIC

El Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé cuenta con distintas dependencias distribuidas en los recintos institucionales, las cuales permiten desarrollar las funciones operativas, administrativas y técnicas necesarias para la continuidad y soporte de los servicios digitales.

Cada espacio cumple un rol específico dentro de la estructura del área y posee medidas de acceso y resguardo acordes a su nivel de criticidad.

Dependencia	Ubicación	Descripción y función principal
Oficina de Jefatura del Área TIC	Mariano Egaña 1685, Primer Piso SDA	Espacio destinado a la gestión estratégica, planificación, coordinación y supervisión general de las actividades del área. Se realizan reuniones de coordinación y control de avance.

Oficina TIC	Mariano Egaña 1685, Tercer Piso SDA	Dependencia operativa donde se desempeña el equipo técnico y administrativo de soporte. Alberga el **Centro de Servicio TI**, desde donde se gestionan los incidentes, requerimientos y servicios del catálogo institucional.
Centro de Datos y Comunicaciones A	Mariano Egaña 1640, Hall Hospital	Sala técnica principal que aloja infraestructura crítica: servidores, equipos de comunicaciones, sistemas de respaldo y monitoreo. Posee control de acceso restringido, sistemas de climatización, energía redundante y UPS.
Centro de Datos y Comunicaciones B	Mariano Egaña 1640, Hall Hospital	Sala técnica secundaria que actúa extensión del Centro de Datos A.
Bodega de Activos TIC	Mariano Egaña 1640, Quinto Piso Hospital	Espacio destinado al almacenamiento, rotulación, retiro y control de equipamiento tecnológico en tránsito, reparación o baja. Gestionado por la Unidad de Operaciones TI.
Shaft Comunicaciones – Primer Piso Hospital	Mariano Egaña 1640	Ducto técnico que concentra el cableado estructurado y equipamiento de red del primer nivel, asegurando conectividad física y orden de la infraestructura.
Shaft Comunicaciones – Segundo Piso Hospital	Mariano Egaña 1640	Ducto técnico que concentra el cableado estructurado y equipamiento de red del segundo nivel, asegurando conectividad física y orden de la infraestructura.
Shaft Comunicaciones – Tercer Piso Hospital	Mariano Egaña 1640	Ducto técnico que concentra el cableado estructurado y equipamiento de red del tercer nivel, asegurando conectividad física y orden de la infraestructura.

Consideraciones generales

- Todas las dependencias TIC poseen acceso controlado y supervisión periódica, conforme a los lineamientos del área de Seguridad.
- Las zonas críticas (centros de datos) cuentan con control de temperatura, sistemas de respaldo energético, y restricción de acceso físico solo a personal autorizado.
- El inventario y las condiciones de operación de cada dependencia son revisados semestralmente por el Encargado de Operaciones TI.

8.3 Reuniones de Área y Coordinación Interna

El Área de Tecnologías de la Información y Comunicación (TIC) mantiene una estructura de reuniones periódicas orientadas a asegurar la alineación estratégica, el control operativo y la mejora continua de sus procesos. Estas instancias permiten coordinar esfuerzos entre las distintas unidades técnicas y promover la comunicación interna, el seguimiento de compromisos y la toma de decisiones basadas en datos.

Tipo de reunión	Periodicidad	Participantes	Objetivo principal
Reunión de Coordinación General TIC	Diaria (8am)	Jefatura TIC, Encargados de unidades	Revisar el estado general de los servicios, incidentes críticos, avances de proyectos y tareas pendientes. Identificar bloqueos y priorizar acciones.
Reunión de Área	Mensual	Jefatura TI, Jefes de	Instancia formal para

TIC		Unidades y Centro de Servicio	informar y comunicar a toda el Área actualización de proyectos, comunicados, actividades.
Reunión de Mesa de Servicio / Centro de Servicio TI	Quincenal	Encargado de Operaciones, Equipo Centro de Servicio	Analizar métricas del sistema de tickets, cumplimiento de SLA, incidentes repetitivos y solicitudes en curso. Definir acciones preventivas y de mejora.
Reunión de Oficina de Proyectos	Según Gantt	Oficina de Proyectos Digitales, Jefatura TIC, Gestores Clínicos y Administrativos	Evaluar el avance de proyectos, hitos, entregables y riesgos. Ajustar cronogramas y revisar requerimientos con las unidades clínicas y administrativas.
Reuniones extraordinarias	Según contingencia	Personal involucrado según tema	Activadas ante eventos críticos, incidentes mayores o interrupciones de servicio. Su objetivo es restablecer la continuidad operativa y definir medidas correctivas.

8.3.1 Reuniones de Confianza y Canales de Denuncia

El área de Tecnología de la Información y Comunicación del Hospital de Tomé asume el compromiso de garantizar un entorno laboral seguro, libre de acoso laboral, violencia en el trabajo y hostigamiento, conforme a lo establecido en la Ley Karin. Esta normativa modifica el Código del Trabajo y otros cuerpos legales para reforzar la prevención, investigación y sanción del acoso laboral, sexual y violencia en los espacios de trabajo.

En ese contexto, esta instancia de "Reunión de Confianza" o canal interno ofrece un espacio confidencial para que los funcionarios del área puedan expresar inquietudes, denuncias o problemas relacionados al clima laboral, con protección y resguardo ante posibles represalias.

Tipo de reunión / Canal	Periodicidad	Participantes	Objetivo principal
Reunión de Confianza	Según necesidad	Personal del Área TIC, Jefatura del Área TIC y Monitor Vals (a solicitud)	Proporcionar un espacio seguro y confidencial para que el personal del área TIC comunique situaciones de acoso laboral, violencia en el trabajo o hostigamiento, garantizando protección al/los denunciante(s) y seguimiento institucional.

8.3.2 Gestión de acuerdos y seguimiento

- Todas las reuniones generan **actas digitales** que registran acuerdos, responsables, plazos y compromisos.
- Las actas se almacenan en el repositorio **SharePoint del Área TIC**.
- El cumplimiento de acuerdos es revisado en la siguiente reunión correspondiente.

8.4 Gestión Documental del Área TIC

La gestión documental en el Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé tiene como propósito asegurar la trazabilidad, integridad, disponibilidad y confidencialidad de los documentos técnicos, administrativos y operativos que sustentan la función del área.

Este proceso se enmarca en lo establecido por la Ley N° 21.180 sobre Transformación Digital del Estado, la Ley N° 19.880 sobre Bases de los Procedimientos Administrativos, y los principios de transparencia y probidad administrativa contenidos en la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

En coherencia con dichos cuerpos normativos, el Área TIC fomenta activamente el uso de plataformas digitales institucionales para la creación, gestión, almacenamiento y difusión controlada de la información, reduciendo el uso de soportes físicos y promoviendo la sostenibilidad operativa y medioambiental.

La documentación generada por el área se clasifica en 4 niveles de acceso pública, interna, Reservada y Confidencial y se almacena en medios institucionales aprobados, garantizando el cumplimiento de las Políticas de Seguridad de la Información, el SGSI y la política de clasificación de la información basada en TLP (Traffic Light Protocol 2.0).

A continuación, se describen los principales medios de gestión documental utilizados por el área:

Plataforma / Medio	Propósito Principal	Tipo de Documentos	Nivel de Acceso	Unidad Responsable
SharePoint Institucional (Repositorio TIC)	Repositorio central de documentación estratégica, técnica y de comité.	Políticas, procedimientos, actas, reportes técnicos, respaldos SGSI.	Reservada / Confidencial	Área TIC – Comité de Seguridad de la Información
Nube Institucional – Carpeta "Guías Rápidas HT"	Espacio compartido orientado a la difusión interna de documentación de apoyo.	Guías rápidas, instructivos, documentos de apoyo operativo.	Público interno	Área TIC
Centro de Soluciones – Mesa de Servicio (Freshservice)	Portal público de acceso a documentación formalizada y vigente.	Manuales, catálogos de servicio, instructivos de usuario, material formativo.	Público / Interno por categoría	Área TIC – Centro de Servicio

El Área TIC mantiene mecanismos de **control de versiones y actualización periódica** de la documentación, asegurando que toda información publicada sea **vigente, aprobada y trazable**.

8.5 Herramientas y Plataformas de Uso Interno

El Área de Tecnologías de la Información y Comunicación (TIC) del Hospital de Tomé dispone de un conjunto de herramientas digitales que permiten gestionar de manera eficiente los procesos técnicos, administrativos y de soporte, garantizando la trazabilidad, la colaboración y el cumplimiento de los estándares institucionales.

El uso de estas herramientas se enmarca en los principios de la Ley N° 21.180 sobre Transformación Digital del Estado, que promueve la gestión electrónica de los actos administrativos y el uso seguro de plataformas tecnológicas, así como en las buenas prácticas de gobernanza TI (COBIT, ITIL e ISO/IEC 20000) adoptadas por el área.

Las plataformas institucionales utilizadas por el Área TIC tienen como objetivos principales:

- Optimizar la gestión de incidentes, requerimientos y activos tecnológicos.
- Facilitar la comunicación y coordinación interna del equipo TIC.
- Estandarizar la gestión documental, la planificación y el seguimiento de actividades.
- Mejorar la trazabilidad, seguridad y eficiencia en la ejecución de los servicios tecnológicos.

A continuación, se detallan las principales herramientas y sus propósitos:

Herramienta / Plataforma	Propósito Principal	Descripción Operativa	Unidad Responsable
Freshservice (Centro de Servicio)	Gestión de solicitudes, incidentes y catálogo de servicios TI.	Plataforma central de gestión operativa basada en ITIL; permite trazabilidad de solicitudes, SLAs, reportes y base de conocimiento.	Tecnologías Digitales
SharePoint Institucional	Repositorio documental y coordinación de procesos internos.	Espacio de trabajo colaborativo que aloja documentos de gestión, actas de comité, políticas, proyectos y tableros Kanban.	Área TIC
Freshservice Proyect	Planificación y seguimiento de tareas y proyectos.	Utilizado para coordinar actividades internas, definir responsables y controlar avances de iniciativas.	Área TIC
Slack	Comunicación, colaboración.	Canal principal de comunicación interna; soporta coordinación sincrónica.	Área TIC
Freshservice Panel de Monitoreo de Infraestructura	Supervisión de servicios críticos e infraestructura.	Permite detectar fallas, medir rendimiento y asegurar continuidad operativa.	Unidad de Operaciones TI
Sistema de Virtualización de Ambientes	Sistema virtual de ambientes.	Permite la creación de entornos virtuales para generar servicios y realizar pruebas	Seguridad de la Información / Ingeniería de Sistemas
Monitoreo de Consumibles de Impresión	Control de insumos y funcionamiento de impresoras.	Permite el seguimiento del consumo de tóner, estado de dispositivos y solicitudes de mantenimiento.	Unidad de Operaciones TI
Sistema de	Administración de	Controla cuentas de	Unidad de

Gestión de Políticas de Grupo (Active Directory)	identidades y configuraciones institucionales.	usuario, políticas de seguridad y configuraciones de red a nivel de dominio.	Operaciones TI
Sistema de cuaderno digital (OneNote)	Registro y trazabilidad de actividades y reuniones.	Espacio estructurado para registrar decisiones, acuerdos técnicos y bitácoras operativas del área.	Jefatura TIC
Sistema de Generación de ID Documental	Control de numeración y trazabilidad de documentos.	Asigna identificadores únicos a políticas, procedimientos y registros oficiales del área TIC.	Jefatura TIC
Freshservice Gestión de Activos	Control y trazabilidad del inventario tecnológico.	Módulo de Freshservice que administra el ciclo de vida de los activos TI (hardware, software y licencias), asociando cada elemento a usuarios, contratos y servicios.	Unidad de Operaciones TI
Fortigate Web Monitor	Monitoreo de tráfico y seguridad perimetral.	Supervisa el tráfico de red, accesos web y amenazas en tiempo real mediante firewall institucional.	Unidad de Seguridad de la Información
SimpleRisk (SGSI)	Gestión del Sistema de Seguridad de la Información.	Plataforma utilizada para la administración de riesgos, controles y cumplimiento de la norma ISO/IEC 27001.	Unidad de Seguridad de la Información
Uptime Kuma	Monitoreo de disponibilidad de servicios.	Sistema interno que supervisa la operatividad de plataformas y sistemas críticos del hospital.	Unidad de Operaciones TI

8.6 Gestión de Riesgos TI

La gestión de riesgos tecnológicos constituye un proceso esencial dentro de la gobernanza de las Tecnologías de la Información y Comunicación del Hospital de Tomé. Este proceso se enmarca en el dominio APO12 (“Gestionar los Riesgos”) del marco de referencia COBIT 2019, el cual establece la necesidad de identificar, evaluar, priorizar y tratar los riesgos asociados a los servicios, activos y procesos tecnológicos, asegurando la continuidad operativa y la protección de la información institucional.

En concordancia con lo dispuesto en la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, artículo 5°, y el Decreto N° 77/2004 de la Contraloría General de la República, que instruyen sobre el deber de las instituciones públicas de implementar mecanismos de control interno y gestión de riesgos, el Área TIC incorpora de manera formal y documentada este proceso en su modelo de gobernanza.

8.6.1 Procedimiento

La identificación y declaración de riesgos TI se canaliza mediante un servicio disponible en el Catálogo de Servicios TI, denominado "Gestión de Riesgos Tecnológicos", accesible a todos los funcionarios del área TIC.

- Cualquier integrante del área puede declarar un riesgo detectado mediante el sistema de mesa de servicio institucional (Freshservice).
- La Unidad de Seguridad de la Información recibe y analiza cada declaración, determinando su criticidad, probabilidad e impacto.
- Los riesgos validados son incorporados y gestionados dentro de la plataforma SimpleRisk, que forma parte del Sistema de Gestión de Seguridad de la Información (SGSI) institucional.
- La trazabilidad del ciclo de vida del riesgo —desde su identificación hasta su mitigación o aceptación— queda registrada electrónicamente en dicha plataforma.

8.6.2 Integración y Priorización

El proceso de gestión de riesgos TI es considerado uno de los procesos priorizados dentro de la gobernabilidad tecnológica del hospital, dado que:

- Permite anticipar vulnerabilidades y reducir el impacto de incidentes sobre los servicios críticos.
- Facilita la toma de decisiones basada en evidencia, aportando insumos a la planificación estratégica, continuidad operacional y seguridad.
- Asegura el cumplimiento de las obligaciones institucionales en materia de ciberseguridad, protección de datos personales (Ley N° 19.628) y transformación digital del Estado (Ley N° 21.180).

En consecuencia, la gestión de riesgos TI se constituye como un componente estructural de la mejora continua del área TIC, asegurando que la función tecnológica contribuya de manera sostenible, segura y eficiente al cumplimiento de la misión institucional.

8.7 Plan de Continuidad Operacional y Recuperación Ante Desastres

Este procedimiento del Área de Tecnologías de la Información y Comunicación del Hospital de Tomé tiene como propósito garantizar la continuidad y recuperación oportuna de los servicios tecnológicos críticos ante incidentes que afecten la disponibilidad, integridad o confidencialidad de la información institucional.

Este plan se sustenta en el marco COBIT 2019, específicamente en el proceso DSS04: "Gestionar la Continuidad", y en los lineamientos de las normas ISO/IEC 22301:2019 (Gestión de Continuidad del Negocio) e ISO/IEC 27001:2022 (Seguridad de la Información).
Asimismo, responde a las obligaciones de control interno establecidas en la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado a través de Procedimiento de Seguridad denominado "Procedimiento de Recuperación ante Desastres PROC03-25-0005, y las directrices del Ministerio de Salud sobre la protección y disponibilidad de los sistemas de información clínicos y administrativos.

El documento interno es de carácter reservado, sin embargo, si se necesita conocer detalles del mismo se puede solicitar una reunión a través del Catalogo de Servicio "Asesoría TI – Seguridad" y solicitar este apoyo.

8.8 Evaluación de Proyectos de Tecnologías de la Información

La evaluación de proyectos de Tecnologías de la Información (TI) constituye un proceso esencial dentro de la gobernanza tecnológica del Hospital de Tomé, orientado a asegurar que toda iniciativa de carácter tecnológico sea viable, estratégica y cumpla con la normativa vigente. Este procedimiento responde a los principios de eficiencia, transparencia y uso racional de los recursos públicos establecidos en la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, y se encuentra alineado con las directrices ministeriales y normativas de transformación digital impulsadas por el Estado de Chile (Ley N° 21.180).

El proceso tiene como finalidad evaluar las propuestas tecnológicas en función de su madurez, alineamiento estratégico, factibilidad financiera, cumplimiento normativo y nivel de seguridad de la información, asegurando que su ejecución contribuya efectivamente al fortalecimiento institucional y a la continuidad operativa de los servicios críticos.

La Unidad de Tecnologías Digitales, dependiente del Área TIC, es la responsable de aplicar este proceso de evaluación, utilizando una metodología estructurada basada en niveles de madurez (CMM), la cual permite medir de forma objetiva el grado de preparación y sustentabilidad del proyecto.

Para iniciar este proceso, toda unidad o área del hospital que requiera implementar o adquirir una solución tecnológica deberá ingresar una solicitud a través del Catálogo de Servicios de la Mesa de Servicio, seleccionando el servicio denominado "Evaluación de Proyectos TI".
Dicha solicitud activará el proceso formal de revisión por parte del evaluador de proyectos, quien analizará la propuesta y elaborará un informe técnico con recomendaciones.

El resultado de la evaluación podrá clasificarse en niveles de madurez Bajo, Medio o Alto, determinando la viabilidad del proyecto y las condiciones necesarias para su ejecución, según lo establecido en el procedimiento institucional vigente.

Este mecanismo permite estandarizar la toma de decisiones, reducir riesgos operacionales, y priorizar aquellas iniciativas que generen mayor valor institucional y contribuyan al proceso de Transformación Digital del Hospital de Tomé.

8.9 Solicitudes de Infraestructura y Brechas Habilitantes

Las solicitudes de infraestructura tecnológica del área TIC, incluyendo aquellas que corresponden a brechas habilitantes (por ejemplo: nuevos enlaces, gabinetes, climatización de data-center, red, UPS, etc.), están sujetas al procedimiento general de evaluación de proyectos TI, pero con especial atención al marco presupuestario y de inversión pública establecido por el proceso EvalTIC.

Procedimiento:

a) Toda solicitud de infraestructura debe inicialmente ingresarse a través del servicio del catálogo denominado "Evaluación de Proyecto TI"
b) La Unidad de Operaciones TI realiza una evaluación técnica preliminar para determinar:
   I. si el valor estimado del requerimiento excede los montos o umbrales definidos para el proceso EvalTIC.
   II. la pertinencia respecto de los lineamientos institucionales, continuidad operacional, interoperabilidad y seguridad de la información.
c) Si el monto estimado es inferior al umbral que obliga a evaluación-EvalTIC, el proyecto puede enfocarse como iniciativa interna de adquisición, licitación o mejora,

dependiendo de la disponibilidad presupuestaria, priorización institucional y compatibilidad operativa.

d) En cambio, si el monto estimado excede el umbral establecido para EvalTIC, la solicitud debe formularse como un proyecto completo conforme a los lineamientos de EvalTIC (Guía para formuladores 2025).
    I. En ese caso, el proyecto debe ingresar al ciclo de formulación y evaluación EvalTIC, presentándose en los plazos definidos (generalmente de mayo a julio para la formulación, evaluación en Julio–Septiembre del año siguiente) para su priorización por la Dirección de Presupuestos (DIPRES) y la División de Gobierno Digital (DGD).
e) La aprobación Técnica y/o presupuestaria de estos proyectos depende de su inclusión en la cartera EvalTIC, lo que implica que la institución no podrá ejecutar ni comprometer gasto significativo fuera del proceso sin riesgo de no financiamiento o cuestionamiento legal.
f) En todos los casos, las solicitudes de infraestructura deberán considerar:
    I. el ciclo de vida completo del activo (instalación, operación, mantenimiento, obsolescencia).
    II. su vinculación con los servicios críticos del hospital.
    III. el impacto en continuidad operacional, compatibilidad e integración con sistemas existentes.
    IV. la evaluación de riesgos de seguridad de la información asociada.
g) Los resultados de la evaluación, la decisión de aprobación o rechazo, los plazos de ejecución, los responsables y el mecanismo de financiamiento quedan documentados en la herramienta de gestión de proyectos y deben quedar registrados en la mesa de servicio TIC como parte del expediente de trazabilidad.

La incorporación de este procedimiento interno se apoya en el marco regulatorio chileno que exige autorización previa de la Dirección de Presupuestos para inversiones en Tecnologías de la Información cuando no han sido evaluadas en el proceso EvalTIC.

Asimismo, fortalece la gobernanza de TI del Hospital de Tomé al asegurar que las decisiones de inversión en infraestructura se realicen de forma transparente, alineada con la estrategia institucional, y con los controles necesarios para evitar riesgos operativos, de seguridad o gastos públicos ineficientes. Esta práctica contribuye directamente al proceso APO05: Gestión de la Cartera de Inversiones y al proceso BAI11: Gestión de Proyectos del marco COBIT 2019.

8.10 Uso Responsable del los Activos Tecnológicos y Cuentas Institucionales

El uso responsable de los recursos tecnológicos del Hospital de Tomé constituye una obligación funcional y un pilar esencial para la seguridad de la información y la continuidad de los servicios institucionales.

8.10.1 Principios Generales

Todo funcionario o colaborador que acceda a los sistemas, equipos o redes institucionales deberá:

a) Firmar el Certificado de Confidencialidad disponible en la Unidad de Gestión y Desarrollo de las Personas, conforme a las disposiciones del Sistema de Seguridad de la Información del hospital.

b) Conocer y respetar las Políticas y Procedimientos vigentes del Sistema de Gestión de Seguridad de la Información (SGSI), en especial los relacionados con confidencialidad, integridad, disponibilidad y trazabilidad de los activos, disponibles en https://hospitaldetome.freshservice.com/support/solutions/37000014175
c) Usar exclusivamente el correo institucional para comunicaciones laborales, garantizando la autenticidad y trazabilidad de las interacciones.
d) Mantener la confidencialidad de las credenciales, evitando su divulgación, préstamo o almacenamiento inseguro.
e) Utilizar los activos de información y equipos institucionales solo para fines relacionados con las funciones propias del cargo.
f) Informar inmediatamente a la Mesa de Servicio cualquier sospecha de incidente de seguridad, acceso indebido o pérdida de información.

8.10.2 Responsabilidad del Área TI

El Área de Tecnologías de la Información y Comunicaciones (TIC) es responsable de:

a) Habilitar, administrar y auditar las cuentas institucionales y accesos a sistemas.
b) Garantizar que cada usuario cuente con las credenciales necesarias conforme a su perfil y cargo.
c) Coordinar con la Unidad de Gestión de Personas y/o jefaturas la revocación o suspensión de accesos cuando proceda (término de contrato, suspensión, traslado, etc.) para ello las jefaturas tienen disponible el servicio:
    I. Para incorporaciones: https://hospitaldetome.freshservice.com/support/employee_onboarding/new
    II. Para desvinculaciones: https://hospitaldetome.freshservice.com/support/employee_offboarding/new
d) Promover el uso seguro y eficiente de los activos tecnológicos mediante capacitaciones, guías rápidas y difusión de buenas prácticas.

8.10.3 Fundamento Normativo

Esta disposición se apoya en:

a) Ley N°19.628 sobre Protección de la Vida Privada.
b) Ley N°21.180 sobre Transformación Digital del Estado.
c) Decreto Supremo N°83/2005 del Ministerio de Salud (Reglamento sobre Requisitos de Seguridad de la Información en Sistemas de Salud).
d) Política Institucional de Seguridad de la Información del Hospital de Tomé, basada en el estándar ISO/IEC 27001:2022.

El incumplimiento de estas obligaciones puede constituir una falta administrativa, sin perjuicio de las sanciones establecidas en la normativa vigente y los reglamentos internos.

9 PERÍODO DE REVISIÓN.

El presente manual deberá ser revisado anualmente o cuando ocurran cambios significativos para garantizar que:

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

10 HISTORIAL Y CONTROL DE VERSIONES.

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio
1.0	28-03-2025		Confección de Manual
1.1	13-05-2025		Ajuste de Formato
1.2	19-05-2025	Anexo 11.10	Incorporación de Perfiles SFIA 9 (Actualización de la versión SFIA 8), Incorporación de Equipo de Proyecto, incorporación de Reuniones de Área.
1.3	06-11-2025	Item 8	Incorporación y depuración del Item 8, Desarrollo de Anexos.
1.4	30-07-2026	Item 6.4.5	Incorporación Item 6.4.5 Armonización Procedimental ante Directrices Externas
1.4	30-07-2026	Anexo 11.10.11	Se incorpora perfil de Delegado de Protección de Datos
1.4	30-7-2026	Anexo 11.10.8	Se incorpora perfil de Coordinador de Transformación Digital
1.4	30-7-2026	Item 7.2.4	Se incorpora la Coordinación de Alta Dirección de TI, con el propósito de transparentar y compartir las decisiones estrategias de TI con la Subdirección Administrativa de manera Bimensual.

11 ANEXOS

11.1 índice de Anexos – Manual Organizacional TIC

N°	TÍTULO DEL ANEXO	DESCRIPCIÓN / CONTENIDO	ORIGEN / RESPONSABLE
Anexo 1	Organigrama del Área TIC (Versión Actual y Proyectada)	Representación visual de la estructura organizacional vigente y la proyectada en el plan de desarrollo TIC.	Jefatura TIC
Anexo 2	Mapa de Procesos TIC (Basado en COBIT 2019)	Diagrama y descripción resumida de los 19 procesos priorizados según COBIT, con su nivel actual y nivel objetivo.	Jefatura TIC
Anexo 3	Catálogo de Servicios TIC	Listado formal de servicios ofrecidos por el Área TIC, con sus descripciones, responsables, canales de atención y SLA.	Centro de Servicio TIC
Anexo 4	Procedimiento de Gestión de Incidentes y Solicitudes	Flujo y documentación del proceso DSS02 e ITIL, con formularios o enlaces a Freshservice.	Centro de Servicio TIC
Anexo 5	Procedimiento de Evaluación de Proyectos TI	Matriz de evaluación, metodología y criterios de madurez del proceso de evaluación institucional.	Unidad de Tecnologías Digitales
Anexo 6	Procedimiento de Continuidad Operacional y Recuperación ante Desastres	Lineamientos de activación, roles, priorización de activos críticos y tiempos de recuperación.	Unidad Seguridad de la Información
Anexo 7	Políticas y Procedimientos de Seguridad de la Información	Políticas aprobadas (uso aceptable, contraseñas, correo, respaldo, TLP, etc.).	Comité de Seguridad de la Información
Anexo 8	Plan de Desarrollo Digital Institucional (Extracto TIC)	Vinculación con el plan estratégico institucional y lineamientos de modernización digital.	Subdirección Administrativa / TIC
Anexo 9	Perfiles del Área TI en formato SFIA Versión 8	Estandarización de perfiles profesionales para el área de Tecnologías de la Información	Jefatura TIC

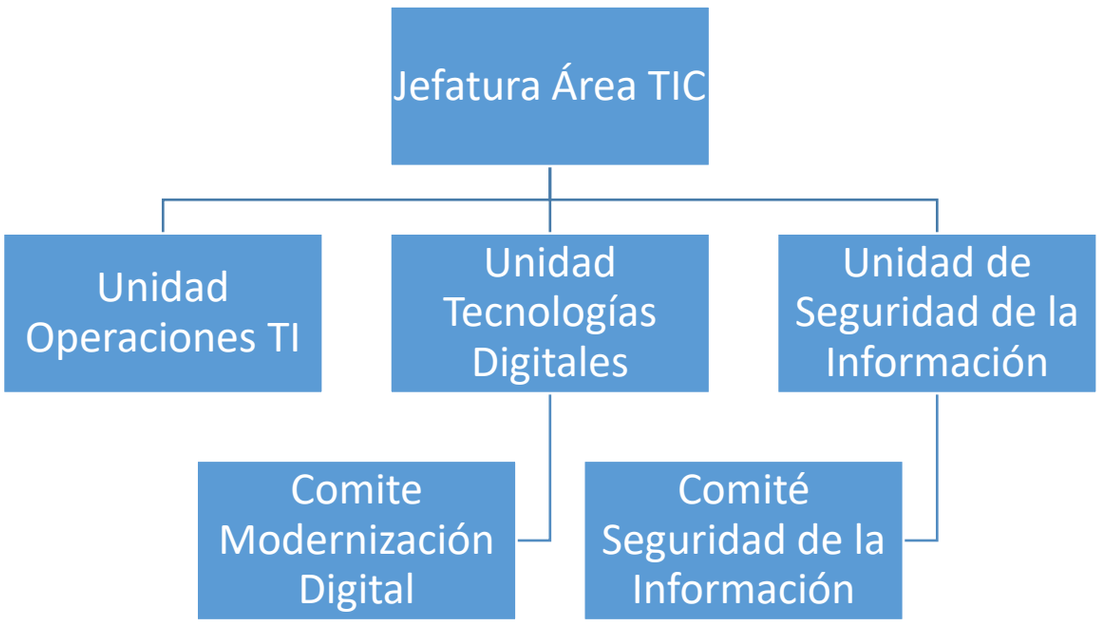
11.2 Organigrama del Área TIC

El Área de Tecnologías de la Información (TIC) del Hospital de Tomé se encuentra estructurada de acuerdo con las directrices institucionales.

El organigrama vigente refleja una estructura funcional, orientada a la entrega, segura y oportuna de los servicios tecnológicos que sustentan la operación clínica, administrativa y de apoyo del hospital.
Actualmente, el área depende jerárquicamente de la Subdirección Administrativa, y se organiza en torno a las siguientes unidades operativas:

- **Unidad de Operaciones TI**: responsable de la administración de infraestructura tecnológica, redes, respaldo, servidores, impresoras y soporte técnico.
- **Unidad de Seguridad de la Información**: encargada de la implementación y seguimiento del Sistema de Gestión de Seguridad de la Información (SGSI), la gestión de riesgos y el cumplimiento normativo.
- **Unidad de Tecnologías Digitales**: enfocada en la gestión de sistemas, desarrollo de soluciones, administración de usuarios y evaluación de proyectos TI.
- **Centro de Servicio TIC (Mesa de Ayuda)**: punto único de contacto para la atención de requerimientos e incidentes, a través de la plataforma institucional Freshservice. (Subunidad Informar compuesta 100% por Compras de Servicio)

Esta estructura busca alinear la gestión tecnológica con los objetivos estratégicos institucionales, promoviendo la gobernanza TI, la continuidad operativa, la seguridad de la información y la mejora continua de los servicios.



En el marco del proceso de fortalecimiento institucional y modernización tecnológica del Hospital de Tomé, el Área de Tecnologías de la Información proyecta una evolución estructural orientada a la especialización funcional, la optimización de procesos operativos y el fortalecimiento de la gobernanza tecnológica.

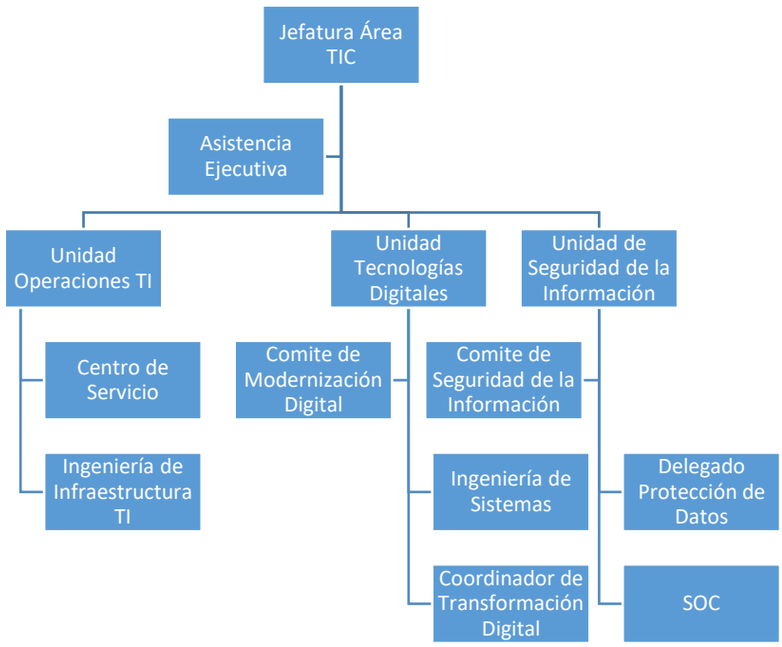
La estructura actual, compuesta por la Jefatura del Área TIC y tres unidades operativas (Operaciones TI, Tecnologías Digitales y Seguridad de la Información), ha permitido sostener la continuidad de los servicios y responder a las necesidades institucionales. No obstante, el crecimiento en la demanda de servicios tecnológicos, la incorporación de nuevos sistemas clínicos y administrativos, y la adopción de estándares de seguridad más exigentes hacen necesario un rediseño organizacional.

La estructura proyectada contempla una mayor segmentación de funciones y responsabilidades, promoviendo la creación de subunidades especializadas que permitan una gestión más eficaz, un control más granular y una participación estratégica en los procesos institucionales.

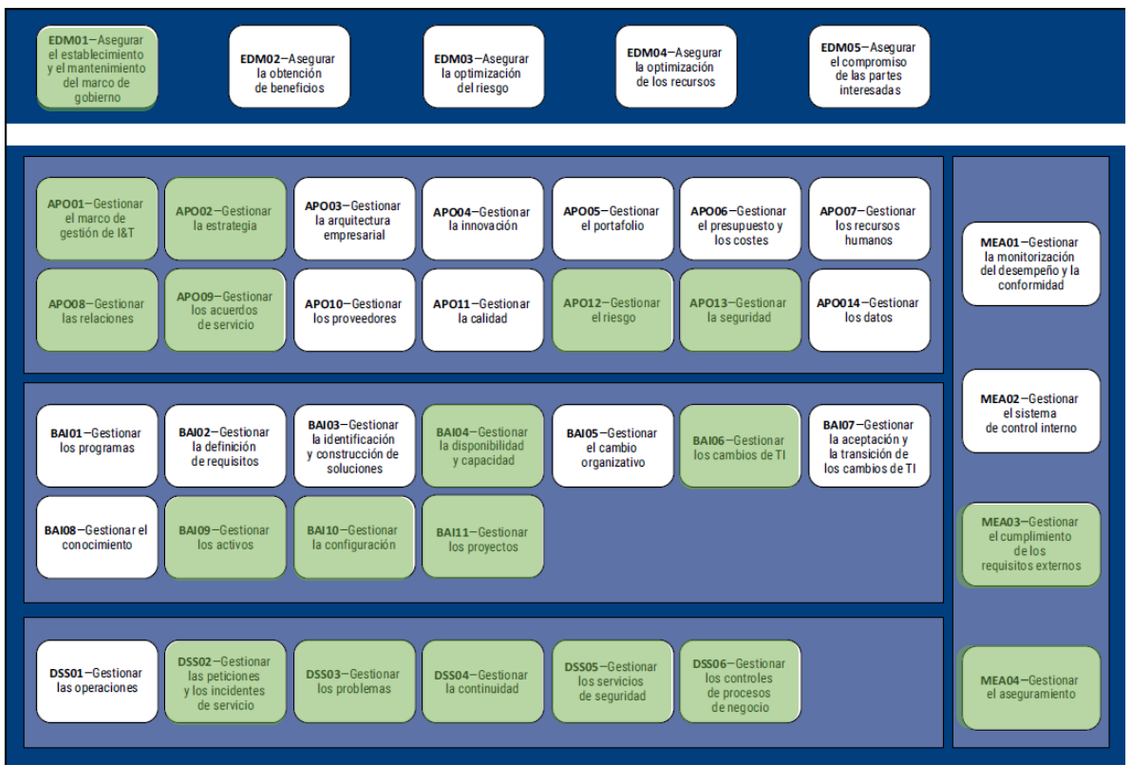
La nueva propuesta considera la siguiente configuración:

- Jefatura del Área TIC: Mantiene la dirección estratégica, coordinación transversal y alineación con los objetivos institucionales, incorporando una Asistencia Ejecutiva para reforzar la gestión administrativa, seguimiento de compromisos y control documental.
- Unidad de Operaciones TI: Se fortalece mediante dos subcomponentes:
    - Centro de Servicio: como punto único de contacto con los usuarios internos, encargado de la atención, seguimiento y resolución de incidentes y requerimientos.
    - Ingeniería de Infraestructura TI: enfocada en la gestión de servidores, redes, telecomunicaciones, respaldo, disponibilidad y continuidad operativa.
- Unidad de Tecnologías Digitales: Evoluciona hacia un rol estratégico en la Transformación Digital, incorporando equipos dedicados a:
    - Coordinador Transformación Digital: impulso de proyectos innovadores, automatización de procesos y adopción de soluciones que potencien la eficiencia institucional.
    - Ingeniería de Sistemas: administración técnica, integración y desarrollo de sistemas hospitalarios y administrativos.
    - Comité de Modernización Digital: instancia asesora para la priorización y evaluación de iniciativas tecnológicas.
- Unidad de Seguridad de la Información: Se consolida como un eje transversal, estructurada en torno a tres componentes:
    - SGSI: administración del Sistema de Gestión de Seguridad de la Información, políticas y controles normativos en cumplimiento a la Ley 21.663.
    - Delegado Protección de Datos: Ente gestor transversal de la gestión de la protección de datos en cumplimiento a la Ley 21.719.
    - SOC (Security Operations Center): monitoreo proactivo, detección de incidentes y respuesta ante amenazas de ciberseguridad.
    - Comité de Seguridad de la Información: instancia de gobernanza para la toma de decisiones y seguimiento de la estrategia de seguridad.

Este nuevo modelo busca una simbiosis entre la operación, la seguridad y la innovación, permitiendo que el Área TIC no solo actúe como soporte, sino como actor estratégico en la gestión hospitalaria, potenciando la transformación digital, la continuidad de los servicios críticos y la protección integral de la información.



11.3 MAPA DE PROCESOS TIC (BASADO EN COBIT 2019)



Con el objetivo de fortalecer la gobernanza y gestión de las Tecnologías de la Información en el Hospital de Tomé, el Área TIC ha adoptado el marco de referencia COBIT 2019, priorizando 19 procesos clave alineados con los objetivos estratégicos institucionales y ministeriales.

La priorización de los procesos se realizó conforme al modelo de diseño de COBIT 2019, el cual considera diez factores de diseño que permiten adaptar el sistema de gobierno y gestión a la realidad y necesidades de la organización. Estos factores fueron analizados y contrastados con el Plan de Desarrollo Estratégico Institucional (PDE) y otros instrumentos de planificación interna, permitiendo establecer un modelo de gobernanza TI coherente y proporcional a la criticidad de los servicios hospitalarios.

Los factores de diseño considerados fueron:

1. Estrategia empresarial.
2. Metas empresariales.
3. Perfil de riesgo.
4. Problemas y oportunidades de TI.
5. Requerimientos de cumplimiento.
6. Rol de TI (soporte, estratégico o transformador).
7. Modelo de aprovisionamiento de TI.
8. Métodos de adopción de tecnología.
9. Tamaño de la empresa.
10. Amenazas del entorno.

A partir de esta evaluación, se determinó un conjunto de procesos priorizados que representan los dominios de Gobernanza, Planificación, Ejecución, Soporte y Monitoreo, con foco en la sostenibilidad, continuidad y madurez institucional del Área TIC.

A continuación, se detallan los 19 procesos priorizados, junto con su descripción, capacidad actual y capacidad proyectada:

Objetivo de Gestión COBIT 2019	Descripción	Capacidad Actual	Capacidad Proyectada
APO01 – Gestionar el Marco de Gestión de TI	Define y mantiene el marco integral para la gestión de TI, alineado con la estrategia institucional.	**Nivel 2 – Gestionado:** Existe estructura básica y control parcial.	**Nivel 4 – Cuantitativamente Gestionado:** Marco institucionalizado, con métricas de desempeño.
APO02 – Gestionar la Estrategia	Alinea la estrategia tecnológica con los objetivos institucionales y ministeriales.	**Nivel 2 – Gestionado:** Estrategia alineada parcialmente al PETI.	**Nivel 4 – Cuantitativamente Gestionado:** Estrategia integrada y evaluada con indicadores.
APO03 – Gestionar la Arquitectura Empresarial	Desarrolla y mantiene la arquitectura de procesos, datos, aplicaciones e infraestructura.	**Nivel 1 – Inicial:** En desarrollo, documentación limitada.	**Nivel 3 – Definido:** Arquitectura formalizada y actualizada.
APO04 – Gestionar la Innovación	Promueve la adopción de tecnologías emergentes y prácticas innovadoras.	**Nivel 2 – Gestionado:** Innovaciones puntuales sin marco formal.	**Nivel 4 – Cuantitativamente Gestionado:** Innovación sistematizada y medible.
APO07 – Gestionar Recursos Humanos	Garantiza la disponibilidad de personal competente en TI.	**Nivel 2 – Gestionado:** Capacitación reactiva, no planificada.	**Nivel 3 – Definido:** Plan anual de desarrollo de competencias en TI.
APO08 – Gestionar Relaciones	Administra las relaciones con usuarios, proveedores y partes interesadas.	**Nivel 2 – Gestionado:** Relación funcional, pero no monitoreada.	**Nivel 4 – Cuantitativamente Gestionado:** Relaciones evaluadas con métricas de satisfacción.
APO10 – Gestionar Proveedores	Supervisa y controla los contratos y servicios externos de TI.	**Nivel 2 – Gestionado:** Contratos operativos sin gestión de desempeño.	**Nivel 3 – Definido:** Gestión basada en indicadores y SLAs.
APO12 – Gestionar Riesgos	Identifica, evalúa y mitiga los riesgos relacionados con TI.	**Nivel 2 – Gestionado:** Registro de riesgos inicial, no integrado.	**Nivel 4 – Cuantitativamente Gestionado:** Riesgos integrados a la gestión institucional (SimpleRisk).
APO13 – Gestionar la Seguridad	Implementa y mantiene un sistema de gestión de seguridad de la información.	**Nivel 3 – Definido:** SGSI activo con controles y políticas.	**Nivel 5 – Optimizado:** Seguridad proactiva con mejora continua y monitoreo continuo.
BAI01 – Gestionar Programas y Proyectos	Gestiona los proyectos de TI mediante metodologías estandarizadas.	**Nivel 2 – Gestionado:** Uso de metodologías híbridas básicas.	**Nivel 4 – Cuantitativamente Gestionado:** Oficina de Proyectos TI institucionalizada.
BAI02 – Gestionar la Definición de Requisitos	Define y valida los requisitos funcionales y técnicos de los sistemas.	**Nivel 2 – Gestionado:** Documentación parcial de requerimientos.	**Nivel 3 – Definido:** Requisitos estandarizados y validados con usuarios.
BAI03 – Gestionar Soluciones	Supervisa el desarrollo, integración y	**Nivel 2 – Gestionado:** Control parcial, sin	**Nivel 3 – Definido:** Ciclo de vida de soluciones

Identificadas	mantenimiento de soluciones tecnológicas.	métricas.	formalizado.
BAI04 – Gestionar la Disponibilidad y Capacidad	Asegura que los recursos tecnológicos estén disponibles según los niveles requeridos.	**Nivel 2 – Gestionado:** Monitoreo parcial.	**Nivel 4 – Cuantitativamente Gestionado:** Gestión proactiva y predictiva.
BAI06 – Gestionar Cambios	Controla los cambios en infraestructura y aplicaciones minimizando riesgos.	**Nivel 3 – Definido:** Proceso estructurado con aprobación formal.	**Nivel 4 – Cuantitativamente Gestionado:** Evaluación de impacto y trazabilidad completa.
DSS01 – Gestionar Operaciones	Administra las operaciones diarias de TI garantizando continuidad y soporte.	**Nivel 3 – Definido:** Operación gestionada con Mesa de Servicio.	**Nivel 5 – Optimizado:** Operaciones automatizadas y monitoreadas 24/7.
DSS02 – Gestionar Solicitudes e Incidentes	Gestiona la atención de solicitudes y resolución de incidentes.	**Nivel 3 – Definido:** Centro de Servicio TI operativo con SLA definidos.	**Nivel 4 – Cuantitativamente Gestionado:** Gestión predictiva y basada en analítica.
DSS04 – Gestionar Continuidad	Mantiene la disponibilidad de los servicios ante fallas o desastres.	**Nivel 2 – Gestionado:** Procedimientos básicos (BCP/DRP).	**Nivel 4 – Cuantitativamente Gestionado:** Planes probados y monitoreados periódicamente.
DSS05 – Gestionar Servicios de Seguridad	Proporciona servicios de seguridad operativa (SOC).	**Nivel 2 – Gestionado:** Actividades reactivas.	**Nivel 4 – Cuantitativamente Gestionado:** SOC activo con alertamiento y respuesta automatizada.
MEA01 – Monitorear, Evaluar y Valorar el Desempeño y Conformidad	Evalúa la efectividad del sistema de gestión de TI y el cumplimiento normativo.	**Nivel 2 – Gestionado:** Seguimiento parcial mediante indicadores operativos.	**Nivel 4 – Cuantitativamente Gestionado:** Evaluación integral con auditorías internas y externas.

El nivel promedio de madurez actual de los procesos priorizados del marco COBIT 2019 en el Área TIC se estima en 2,4 (Gestionado), lo que indica que existen procedimientos definidos y aplicados de manera consistente, aunque aún con oportunidades de estandarización, automatización y trazabilidad.

El nivel de madurez proyectado es de 3,8 (Establecido y Medido), reflejando la necesidad institucional de transitar hacia una gestión basada en evidencia, controlada y con mejora continua, en coherencia con los principios de gobernanza definidos por el Modelo de Gestión Hospitalario y el Plan de Desarrollo Estratégico Institucional (PDE).
Este avance responde directamente a los factores de diseño del sistema de gobernanza de TI, definidos por COBIT, los cuales incluyen el alineamiento estratégico, la entrega de valor, la gestión del riesgo, la optimización de recursos y el cumplimiento normativo, entre otros. En particular, los factores analizados permiten que las iniciativas TIC se articulen con los objetivos estratégicos de salud pública, la continuidad operacional, la modernización digital y la seguridad de la información.

El incremento proyectado de madurez busca:

- Consolidar la gobernabilidad TI, asegurando la trazabilidad entre decisiones, riesgos y beneficios tecnológicos.
- Fortalecer la gestión del riesgo y la seguridad de la información, en el marco del SGSI institucional y las políticas públicas digitales.
- Optimizar la toma de decisiones, mediante métricas objetivas, control de desempeño y priorización basada en valor.
- Aumentar la eficiencia operativa, a través de procesos estandarizados y automatizados, con roles y responsabilidades claramente definidos.

En suma, este proceso de maduración permitirá a la organización alinear su gestión tecnológica con las mejores prácticas internacionales, garantizando sostenibilidad, control y valor agregado para la institución y su entorno asistencial.

11.4 CATALOGO DE SERVICIOS

El Catálogo de Servicios TI constituye el instrumento formal que describe los servicios tecnológicos disponibles para los usuarios internos del establecimiento, gestionados a través de la Mesa de Ayuda del Centro de Servicio TI. Su objetivo es garantizar una atención oportuna, trazable y estandarizada de los requerimientos, incidentes y solicitudes de soporte relacionadas con los activos y recursos tecnológicos institucionales.

Este catálogo permite visibilizar el alcance, niveles de servicio y responsabilidades asociadas a cada prestación, fortaleciendo la transparencia y la gestión basada en buenas prácticas de ITIL y COBIT. Asimismo, contribuye a alinear la operación TI con los procesos clínicos y administrativos del hospital, asegurando la continuidad operativa y la satisfacción de los usuarios finales.

Los servicios se agrupan por categorías operacionales y estratégicas, tales como Gestión de Accesos y Registros, Gestión de Activos, Conectividad y Redes, Comunicación y Colaboración, Seguridad de la Información, entre otras.

Nombre del Servicio	Descripción Breve	Categoría
Accesos Otros Sistemas	Creación o ajuste de credenciales de acceso a plataformas institucionales.	Gestión de Accesos y Registros
Activación de Office	Habilitación o activación de licencias de Microsoft Office.	Gestión de Accesos y Registros
Anexo Telefónico	Creación, modificación o traslado de anexos telefónicos institucionales.	Conectividad y Redes
Asesorías TI	Asistencia técnica y consultiva para temas tecnológicos o normativos TI.	Gestión de Accesos y Registros
Asignación de Impresoras	Configuración y vinculación de equipos de impresión a usuarios o unidades.	Gestión de Recursos en la Nube
Auditoría de Acceso RCE	Revisión de trazabilidad y accesos al Registro Clínico Electrónico.	Seguridad de la Información
Auditoría Transparencia	Análisis de cumplimiento normativo y publicación de información pública.	Transparencia
Cierre de Agenda	Soporte en la configuración y cierre de agendas clínicas.	Configuración de Sistemas
Correo Masivo Institucional	Envío de comunicaciones oficiales a la comunidad hospitalaria.	Comunicación y Colaboración
Cuenta Apoyo Diagnóstico	Creación o administración de cuentas de apoyo en sistemas clínicos.	Gestión de Accesos y Registros
Cuenta RCE	Habilitación o bloqueo de cuentas del Registro Clínico Electrónico.	Gestión de Accesos y Registros
Entrega de Equipamiento TI	Registro y entrega de dispositivos tecnológicos institucionales.	Gestión de Activos
Evaluación de Correos	Análisis de posibles correos maliciosos o sospechosos.	Seguridad de la Información
Evaluación de Proyectos TI	Análisis técnico y estratégico de iniciativas tecnológicas.	Planificación y Adquisición Tecnológica
Evaluación de Seguridad	Revisión de cumplimiento de políticas y controles de seguridad.	Seguridad de la Información
Exámenes Laboratorio	Soporte en la configuración de módulos de laboratorio clínico.	Configuración de Sistemas
Firma Electrónica	Creación o renovación de certificados de firma electrónica.	Gestión de Accesos y Registros
Firma Panel Documental	Activación de firmas digitales en paneles documentales internos.	Gestión de Accesos y Registros
Gestión Cuenta Correo	Creación, modificación o cierre de cuentas de correo institucional.	Gestión de Accesos y Registros
Gestión Cuenta PC	Creación o eliminación de usuarios en equipos institucionales.	Gestión de Accesos y Registros
Gestión de Fármaco	Soporte a módulos de prescripción y stock farmacéutico.	Configuración de Sistemas

Gestión de Locales	Configuración de locales en sistemas clínicos y administrativos.	Configuración de Sistemas
Gestión Mapas de Piso	Mantenimiento de la cartografía institucional y sus ubicaciones.	Configuración de Sistemas
Instalación de Software	Instalación y configuración de aplicaciones corporativas.	Gestión de Activos
Licencia Médica	Creación o gestión de accesos para licencias médicas electrónicas.	Gestión de Accesos y Registros
Mod. Lista de Espera RCE	Ajuste de parámetros en módulos de lista de espera.	Configuración de Sistemas
Modificación Sitio Web	Actualización o mejora de contenido institucional web.	Comunicación y Colaboración
Modificar Especialidad RCE	Ajuste de especialidades médicas en el RCE.	Configuración de Sistemas
Nube Institucional	Gestión de carpetas y permisos en el entorno de almacenamiento colaborativo.	Gestión de Recursos en la Nube
Nuevo Puesto de Trabajo	Preparación integral de equipamiento para nuevos funcionarios.	Gestión de Activos
Permisos Jefatura MDS TI	Autorizaciones avanzadas de acceso a plataformas institucionales.	Gestión de Accesos y Registros
Plataformas Ministeriales	Configuración y soporte de plataformas dependientes del MINSAL.	Gestión

Los 47 servicios actualmente gestionados por el Centro de Servicio TI se encuentran estructurados bajo el proceso DSS02 – Gestionar Solicitudes y Servicios, definido en el marco de COBIT 2019, el cual regula la administración eficiente, controlada y trazable de todos los servicios tecnológicos institucionales.

Este proceso se articula con las mejores prácticas de ITIL (Information Technology Infrastructure Library), que permiten garantizar una operación alineada a estándares internacionales de gestión de servicios, asegurando continuidad, mejora continua y valor para los usuarios internos.

En este contexto, los servicios del catálogo se gestionan conforme a los siguientes subprocesos principales:

- **Gestión de Problemas**: orientada a identificar y eliminar causas raíz de incidencias recurrentes, reduciendo el impacto operativo y mejorando la disponibilidad de los servicios.
- **Gestión de Cambios**: regula la evaluación, aprobación y ejecución controlada de modificaciones en los servicios o infraestructuras TI, minimizando riesgos y asegurando trazabilidad.
- **Gestión de Liberaciones**: coordina la entrega, implementación y validación de nuevas versiones o funcionalidades, garantizando que los cambios aprobados se integren correctamente al entorno operativo.

El Área de Tecnologías de la Información del Hospital de Tomé ha fortalecido sus capacidades mediante procesos de capacitación y alineamiento en ITIL, con el propósito de ofrecer servicios de calidad, eficientes y sostenibles, dentro del marco presupuestario y de recursos humanos actualmente disponibles.

Este enfoque permite consolidar una cultura de servicio orientada a la mejora continua, la gestión proactiva y la gobernabilidad tecnológica, contribuyendo directamente a los objetivos estratégicos institucionales y a la modernización digital del hospital.

11.5 PROCEDIMIENTO DE GESTIÓN DE INCIDENTES Y SOLICITUDES

El presente procedimiento forma parte del sistema de gestión de servicios del Área de Tecnologías de la Información y Comunicaciones (TIC) del Hospital de Tomé y se encuentra disponible en el Portal de Soluciones Institucional:

https://hospitaldetome.freshservice.com/a/solutions/articles/37000024597?language=es-LA

Este procedimiento se encuentra alineado con el proceso DSS02 de COBIT 2019 ("Gestionar las peticiones y los incidentes de servicio") y adopta las mejores prácticas de ITIL 4, garantizando una atención sistemática, eficiente y trazable frente a las interrupciones de los servicios TI o solicitudes de los usuarios internos del hospital.

Su propósito es asegurar la continuidad operativa, la satisfacción de los usuarios y la optimización de recursos técnicos y humanos, contribuyendo directamente a los objetivos estratégicos institucionales y al cumplimiento de los Acuerdos de Niveles de Servicio (SLA).

11.5.1 Alcance

El procedimiento aplica a todas las unidades y servicios clínico-administrativos del Hospital de Tomé que utilicen servicios o activos tecnológicos gestionados por el Área TIC. Comprende la gestión de:

- **Incidentes**: interrupciones o degradaciones no planificadas en los servicios tecnológicos institucionales.
- **Solicitudes de servicio**: requerimientos de carácter estándar, como accesos, instalaciones, configuraciones o asesorías.

11.5.2 Flujo general de gestión

El ciclo de atención de incidentes y solicitudes se estructura en siete etapas principales:

Etapa	Descripción
1. Registro y Clasificación	El usuario registra su solicitud o incidente en el Portal de la Mesa de Servicio o mediante los canales oficiales definidos. El ticket se clasifica y prioriza.
2. Priorización	Se determina el nivel de impacto y urgencia para asignar una prioridad (Urgente, Alta, Media, Baja), en base a los SLA establecidos.
3. Asignación	El ticket se deriva al técnico o grupo de resolución correspondiente según la naturaleza del incidente o solicitud (Infraestructura, Software, Comunicaciones, Seguridad, etc.).
4. Diagnóstico y Resolución	El agente realiza acciones correctivas o de análisis, apoyándose en la Base de Conocimiento (Centro de Soluciones) y, si corresponde, se coordina con proveedores externos.
5. Escalamiento	Si el incidente no puede resolverse dentro de los tiempos definidos o requiere competencias de un nivel superior, se escala al segundo nivel de soporte o al Comité de Seguridad / Infraestructura según corresponda.
6. Cierre y Validación	Una vez resuelto, el agente documenta la solución y el usuario valida la conformidad del servicio. El sistema registra automáticamente el tiempo de resolución.
7. Evaluación y Mejora Continua	Los tickets cerrados alimentan los indicadores de gestión y el análisis de tendencias para la identificación de problemas recurrentes, riesgos tecnológicos y oportunidades de mejora.

11.5.3 Niveles de Prioridad y Compromisos de Atención (SLA)

Prioridad	Primera Respuesta	Tiempo Máximo de Resolución	Ejemplo
Urgente	15 minutos	3 horas	Falla total en sistema crítico.
Alta	15 minutos	4 horas	Degradación importante en sistemas o servicios esenciales.
Media	20 minutos	6 horas	Problemas menores o solicitudes operativas estándar.
Baja	20 minutos	8 horas	Requerimientos administrativos, cambios planificados o consultas.

Estos valores representan la capacidad operativa actual, considerando los recursos humanos y técnicos disponibles.
Cualquier ajuste a estos tiempos implica un impacto directo en inversión, contratación de servicios y ampliación de cobertura técnica.

11.5.4 Integración con Procesos de Gobernanza TI

El proceso DSS02 se articula directamente con otros procesos críticos de gestión TI, asegurando un flujo coherente dentro del marco COBIT e ITIL:

- Gestión de Problemas (DSS03): análisis y tratamiento de causas raíz de incidentes recurrentes.
- Gestión de Cambios (BAI06): planificación y control de modificaciones necesarias para resolver o prevenir incidentes.
- Gestión de Activos (BAI09): control del ciclo de vida de hardware y software intervenidos.
- Gestión de Seguridad de la Información (DSS05): coordinación frente a incidentes de confidencialidad, integridad o disponibilidad.

Esta integración permite mantener la trazabilidad, asegurar la continuidad operativa y fomentar la mejora continua dentro del modelo de madurez institucional.

11.5.5 Indicadores de Desempeño

Dado que el compromiso del área TI es ofrecer servicios de calidad y que el centro de servicio TI es el punto único de contacto, es que se establecen indicadores claves de gestión (KPI), para asegurar el cumplimiento y satisfacción.

Indicador	Descripción	Meta
% de Cumplimiento Primera Respuesta		>=80%
% de Cumplimiento tiempo de Resolución		>=80%
Satisfacción del Solicitante		> 3

11.6 PROCEDIMIENTO DE EVALUACIÓN DE PROYECTOS TI

Este procedimiento establece un marco estructurado para la evaluación de proyectos de TI en el Hospital de Tomé, asegurando su viabilidad técnica, financiera y estratégica, y su alineamiento con los objetivos institucionales, la normativa vigente y las buenas prácticas de seguridad de la información.

Aplica a todas las iniciativas tecnológicas que involucren adquisición, desarrollo, mejora o incorporación de soluciones TI.
Toda solicitud extraordinaria de unidades o servicios deberá contar con evaluación y recomendación del Evaluador de Proyectos TI antes de su ejecución o tramitación presupuestaria.

11.6.1 Objetivos Específicos

- Alinear los proyectos con la estrategia institucional y de transformación digital.
- Evaluar viabilidad presupuestaria y sostenibilidad.
- Asegurar el cumplimiento normativo y regulatorio.
- Determinar la madurez y el impacto organizacional del proceso objetivo.
- Evaluar la gobernanza y gestión del cambio asociada.
- Garantizar la incorporación de medidas de ciberseguridad y protección de datos.
- Emitir un informe de evaluación que facilite la toma de decisiones por parte de la Dirección y Subdirección Administrativa.

11.6.2 Metodología de Evaluación

La evaluación se basa en un modelo de madurez de 5 niveles (1–5) inspirado en CMMI.
Cada proyecto es evaluado en 6 dimensiones con ponderaciones específicas; se obtiene un puntaje final ponderado que determina el nivel de madurez global del proyecto.

Dimensión	Peso	Descripción del Nivel 1 (Inicial)	Descripción del Nivel 5 (Optimizado)
Alineamiento Estratégico	20%	Sin relación con objetivos institucionales.	Totalmente alineado, con indicadores y métricas de impacto.
Presupuesto y Viabilidad	15%	Sin respaldo financiero definido.	Plan completo con control y sostenibilidad presupuestaria.
Cumplimiento Normativo	20%	No se consideran regulaciones.	Cumplimiento validado mediante auditorías y revisiones periódicas.
Madurez del Proceso Objetivo	15%	Sin documentación ni métricas.	Automatizado, medido y en mejora continua.
Gobernanza del Proyecto	15%	Sin estructura ni roles claros.	Gobernanza adaptable, con seguimiento y aprendizaje organizacional.
Seguridad de la Información	15%	Sin medidas de seguridad.	Controles avanzados, monitoreo y cumplimiento ISO 27002.

La tabla anterior es una representación general del nivel mínimo y máximo por cada dimensión.

11.6.3 Clasificación de Madurez Global

Nivel	Rango Ponderado	Interpretación	Condición de Ejecución
Bajo	1.0 – 2.5	Alto riesgo, baja madurez.	Requiere rediseño antes de aprobación. Solo ejecutable por **excepción** institucional.
Medio	2.6 – 3.5	Viable con ajustes y mitigaciones.	Puede avanzar con plan de mejoras.
Alto	3.6 – 5.0	Bien definido, bajo riesgo.	Aprobado para ejecución.

11.6.4 Recomendaciones para Proyectos de Nivel Bajo o Medio

Dimensión	Acciones Correctivas Clave
Alineamiento Estratégico	Revisar vínculo con el Plan Estratégico Institucional y definir KPI de impacto.
Presupuesto y Viabilidad	Asegurar financiamiento completo, ciclo de vida ≥ 24 meses, y considerar Plan de Compras TI.
Cumplimiento Normativo	Verificar normativas técnicas, sectoriales y de seguridad; consultar a ANCI o CISO si hay dudas.
Madurez del Proceso Objetivo	Documentar procesos, roles e indicadores; asegurar capacitación funcional.
Gobernanza del Proyecto	Definir comité, roles y actas de seguimiento; incluir gestión del cambio.
Seguridad de la Información	Incorporar análisis de riesgo por el CISO y controles de seguridad básicos (ISO 27002).

11.6.5 Evaluador de Proyecto TI

La Unidad de Tecnologías Digitales y/o Unidad de Operaciones TI es responsable de aplicar el presente procedimiento, analizar cada iniciativa, asignar puntajes, emitir recomendaciones y elevar el Informe de Evaluación a la Jefatura de TI, CISO y Subdirección Administrativa.

Responsabilidades principales:

- Aplicar la matriz de evaluación y justificar cada puntaje.
- Emitir recomendaciones para mejorar la madurez del proyecto.
- Gestionar excepciones y coordinaciones con la Alta Dirección.
- Supervisar la implementación de medidas correctivas.

11.6.6 Resultado y Seguimiento

Una vez finalizada la evaluación:

- Se elabora un Informe Técnico de Evaluación con los resultados y recomendaciones.
- El Comité de Modernización en primera instancia decide su ejecución, postergación o rechazo, en caso de aceptarse el Comité de Abastecimiento aprobará, postergará o rechazará su ejecución según prioridad presupuestaria.
- Los proyectos con observaciones deberán implementar mejoras antes de su reingreso a evaluación.

11.7 PROCEDIMIENTO RECUPERACIÓN ANTE DESASTRES

11.7.1 Propósito

El presente procedimiento tiene por objetivo garantizar la continuidad operativa y la restauración eficiente de los sistemas críticos del Hospital de Tomé ante incidentes o desastres que afecten la disponibilidad, integridad o confidencialidad de la información.

Se encuentra alineado con la norma ISO/IEC 27001:2022 y con las Políticas de Seguridad de la Información y Continuidad Operativa institucionales, integrándose al marco de gestión de riesgos y resiliencia tecnológica del hospital.

11.7.2 Alcance

Este procedimiento aplica a todos los servicios y plataformas tecnológicas críticas que sustentan procesos clínicos, administrativos y de soporte.
Comprende las fases de detección, evaluación, activación, recuperación, validación, retorno y post-análisis ante un incidente de desastre.

11.7.3 Sistemas Críticos

Sistema / Servicio	Descripción	Proveedor / Gestión	Responsabilidad Operativa
Registro Clínico Electrónico (TrakCare)	Sistema central de registro de atención de pacientes.	InterSystems (Modalidad SaaS)	Tecnologías Digitales / Proveedor
Sistema de Imagenología (RIS/PACS – Medicap)	Gestión de imágenes diagnósticas y exámenes.	Lebox	Operaciones TI / Imagenología
Sistema de Laboratorio (Syslab)	Gestión de muestras, resultados y trazabilidad.	Syslab S.A.	Operaciones TI / Laboratorio
Active Directory (AD)	Autenticación y control de acceso institucional.	Gestión Interna	Operaciones TI / Seguridad de la Información

11.7.4 Objetivos de Recuperación

Sistema / Servicio	RPO (Recovery Point Objective)	RTO (Recovery Time Objective)	Observaciones
TrakCare (SaaS)	0	< 5 minutos	Respaldado y gestionado por proveedor InterSystems.
RIS/PACS – Medicap	≤ 2 horas	≤ 2 horas	Sincronización local y respaldo externo.
Syslab	≤ 2 horas	≤ 2 horas	Consultar Información al Área de TI
Active Directory (AD)	≤ 2 horas	≤ 2 horas	Consultar Información al Área de TI

Nota: RPO define el punto máximo aceptable de pérdida de datos y RTO el tiempo máximo permitido para restaurar el servicio.

11.7.5 Contactos Clave y Roles

Rol	Nombre	Teléfono / Anexo	Correo Electrónico	Responsabilidad
Activación DRP / Coordinador General	César Cáceres Urrutia	415016 / +56 9 8471 4155	cesar.caceres@redsalud.gob.cl	Activación del plan, coordinación general y comunicación
Seguridad de la Información (CISO)	César Cáceres Urrutia	415016 / +56 9 8471 4155	cesar.caceres@redsalud.gob.cl	Evaluación de riesgos, comunicación de incidentes y resguardo de evidencias.
Operaciones TI	Leandro Cuadra Vera	415065 / +56 9 6176 3608	leandro.cuadra@redsalud.gob.cl	Recuperación de infraestructura, redes y servidores.
Tecnologías Digitales	Jeniffer Parra Millán	414777 / +56 9 9493 1575	jeniffer.parra@redsalud.gob.cl	Coordinación de aplicaciones, proveedores y pruebas de validación.

11.7.6 Procedimiento General de Recuperación

- **Detección y Notificación**
  - Identificar el incidente disruptivo (fallo técnico, corte eléctrico, ataque cibernético, desastre natural, etc.).
  - Notificar de inmediato al CISO y al Coordinador DRP.
  - Registrar la incidencia en el sistema de gestión de seguridad o mesa técnica.
    - **https://hospitaldetome.freshservice.com/support/tickets/new** Categoría Seguridad
- **Evaluación del Impacto**
  - Analizar el alcance y severidad del incidente.
  - Determinar afectación en sistemas críticos y dependencias.
  - Decidir activación del DRP según el impacto detectado.
- **Activación del DRP**
  - La **Jefatura de TI** autoriza formalmente la activación.
  - Comunicar a todos los equipos internos y proveedores asociados.
  - Establecer canal de comunicación centralizado.
- **Ejecución de Estrategias de Recuperación**
  - Aplicar procedimientos técnicos de restauración según sistema.
  - Implementar respaldos y restauración de datos conforme a los objetivos RTO/RPO.
  - Redirigir operaciones a sistemas recuperados o entornos alternos.
- **Monitoreo y Validación**
  - Verificar la funcionalidad completa del servicio.
  - Validar la integridad de la información y cumplimiento de tiempos.
  - Registrar incidencias secundarias o lecciones aprendidas.
- **Restauración del Entorno Primario**
  - Retornar al entorno principal una vez validada la estabilidad.
  - Coordinar validaciones cruzadas entre TI y usuarios clave.
- **Informe Post-Incidente**

- Elaborar informe técnico con descripción del evento, tiempos, acciones y resultados.
- Incorporar oportunidades de mejora en el plan DRP.
- Capacitar a los equipos involucrados según resultados.

11.7.7 Comunicación durante el incidente

Tipo de Comunicación	Plazo Máximo	Responsable	Medio / Observación
Interna (Dirección / Unidades Críticas)	Aviso inmediato + actualización cada 1 hora	Coordinador DRP	Mensajería y Sitio Web Estado Infraestructura TI
Externa (Usuarios / Comunidad Hospitalaria)	Aviso en 1 hora, estimación de recuperación en 2 horas	CISO / Comunicaciones	Correo o comunicado interno.
Proveedores Críticos	Aviso inmediato tras activación DRP	Tecnologías Digitales	Contacto directo vía correo y soporte técnico.

El área TIC mantiene un servicio dedicado para la revisión del estado de toda la infraestructura TI y sus servicios asociados, para acceder a el se debe visitar el siguiente enlace: https://tic.status.freshservice.com/ los usuarios podrás suscribirse para recibir notificaciones en tiempo real.

11.8 POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

El Hospital ha desarrollado e implementado un conjunto de políticas y procedimientos formales que conforman el marco del Sistema de Gestión de Seguridad de la Información (SGSI), alineado con la norma ISO/IEC 27001:2022, la legislación nacional vigente y los lineamientos de Gobernanza TI establecidos por COBIT 2019.

Estas políticas permiten asegurar la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional, estableciendo controles y responsabilidades claras para todo el ciclo de vida de los activos de información.

A continuación, se presenta un resumen de las políticas y procedimientos vigentes, con su propósito, ámbito de aplicación y las principales referencias normativas asociadas:

Código	Nombre	Descripción	Referencias Normativas
POL03-25-0001	**Política de Respaldo**	Define los lineamientos para garantizar la integridad, disponibilidad y recuperación de la información mediante respaldos periódicos y seguros.	ISO/IEC 27001:2022 – A.8.13; Ley 19.628; Dto. N°83
POL03-25-0002	**Política de Derechos de Acceso**	Establece principios para la gestión segura de accesos, aplicando autenticación, autorización y trazabilidad.	ISO/IEC 27001:2022 – A.9.1; Ley 21.459; NCh-ISO 27002:2013
POL03-25-0003	**Política para la Clasificación y Manejo de la Información**	Define niveles de clasificación (Pública, Interna, Reservada, Confidencial) y los controles aplicables según su criticidad.	ISO/IEC 27001:2022 – A.5.12; Ley 19.628; Ley 20.285
POL03-25-0004	**Política de Gestión de Cambio**	Regula el proceso formal para implementar cambios en sistemas, infraestructura y aplicaciones, evitando riesgos operativos.	ISO/IEC 27001:2022 – A.8.32; COBIT 2019; Ley 21.180
POL03-25-0005	**Política para las Relaciones con los Proveedores**	Establece requisitos de seguridad y continuidad en contratos con proveedores, incluyendo cláusulas de SLA y auditoría.	ISO/IEC 27001:2022 – A.5.19; Ley 21.459; ISO 22301
PROC03-25-0001	**Procedimiento de Gestión de Incidentes de Seguridad**	Define los pasos para la detección, análisis, contención, notificación y reporte de incidentes de seguridad.	ISO/IEC 27001:2022 – A.5.24; Ley 21.459; NIST SP 800-61
PROC03-25-0002	**Procedimiento de Gestión de Identidad y Derechos de Acceso**	Regula el ciclo de vida de usuarios: creación, modificación, eliminación y control de cuentas privilegiadas.	ISO/IEC 27001:2022 – A.9.2; Ley 19.628; NCh-ISO 27002:2013
PROC03-25-0003	**Procedimiento de Gestión de Vulnerabilidades**	Establece el proceso para identificar, evaluar, priorizar y tratar vulnerabilidades en sistemas y aplicaciones.	ISO/IEC 27001:2022 – A.8.8; CVSS v3.1; Ley 21.459
PROC03-25-0005	**Plan de Recuperación ante Desastres (DRP)**	Define estrategias y procedimientos para restaurar sistemas críticos ante desastres, con RTO y RPO definidos.	ISO/IEC 27001:2022 – A.5.17; ISO 22301; Ley 21.180

El cumplimiento de estas políticas y procedimientos es obligatorio para todo el personal del Hospital que interactúe con sistemas de información o maneje datos institucionales.
Su aplicación práctica permite fortalecer la cultura de seguridad, mantener la confianza digital y asegurar la continuidad operativa ante incidentes o amenazas que comprometan la información o los servicios tecnológicos.

Para revisar el detalle documental se debe acceder al siguiente link: https://hospitaldetome.freshservice.com/support/solutions/37000014175

11.9 PLAN DE DESARROLLO DIGITAL INSTITUCIONAL (EXTRACTO TIC)

11.9.1 Objetivo General

Avanzar hacia un modelo de madurez digital intermedio-avanzado al año 2027, consolidando las Tecnologías de la Información como habilitador estratégico del Plan de Desarrollo Estratégico (PDE 2024–2026) y de la Ley 21.180 de Transformación Digital del Estado.

11.9.2 Madurez Digital Institucional

Modelo	Línea Base	Meta 2027	Prioridades
MMGD	1,75 / 4	≥2 / 4	Alineamiento Plan Informático con Estrategia, Gestión de Proyectos TI, Integración de información, Publicación de datos abiertos
C2M2	1,5 / 3	≥1,7 / 3	Conciencia Situacional, Gestión de Vulnerabilidades, Gestión de Riesgos, Respuesta a Incidentes, Gestión de Activos y Cadena de Suministro
COBIT 2019	17%	26%	APO02 (Estrategia), APO14 (Datos), BAI11 (Proyectos), APO13 (Seguridad), DSS02 (Incidentes)
TOGAF + ITIL	Operacional: 90,15%	Operacional: 100%Infraestructura: 70%	Arquitectura tecnológica planificada, SLA consolidados, operación proactiva

11.9.3 Capacidades Prioritarias y Acciones Claves

Gestión de Datos Clínicos y Acceso Digital de Pacientes

- Integración RCE con BI/Analítica avanzada y telemedicina.
- Portales de paciente y sistemas de contactabilidad multicanal.
- Tableros quirúrgicos en tiempo real.
- **Impacto PDE:** Calidad, continuidad operativa, innovación.

Gestión Digital de Activos y Mantenimiento

- ERP modular integrado con inventario, bodega y finanzas.
- Monitoreo en tiempo real de equipos críticos.
- Capacitación en gestión de servicios bajo ITIL/ISO.
- **Impacto PDE:** Optimización de recursos y continuidad operativa.

Gestión Integral de Personas y Capacitación Digital

- Sistema de ausentismo con alertas y reportes automáticos.
- Plataforma e-learning con trazabilidad completa.
- Portal de autoservicio para funcionarios.
- **Impacto PDE:** Optimización de recursos y modernización.

Gestión Proactiva de Pacientes Crónicos

- Telemonitoreo integrado con RCE y alertas automáticas.
- Analítica avanzada para microgestión y priorización de intervenciones.
- Plataforma de comunicación paciente-hospital.
- **Impacto PDE:** Calidad y seguridad, innovación.

11.9.4 Hoja de Ruta de Implementación

Área	Acción Clave	Responsable	Prioridad	Impacto PDE	Resultado Esperado
Gestión Ambulatoria	Integrar RCE-BI y telemedicina	TI + UCGIS	Alta	Calidad	Tableros de datos en tiempo real
Gestión Ambulatoria	Portal de paciente	TI + Gestión Cuidado	Alta	Calidad + Innovación	Mayor acceso y empoderamiento del paciente
Mantenimiento Preventivo	ERP integrado y monitoreo	TI + RRFF	Alta/Media	Optimización y Continuidad	Control de activos y alertas tempranas
Gestión Personas	Ausentismo con alertas y e-learning	TI + RRHH	Alta/Media	Optimización + Innovación	Planificación de dotación y capacitación digital
Enfermedades Crónicas	Telemonitoreo y analítica avanzada	TI + Clínicos	Alta/Media	Calidad + Innovación	Seguimiento continuo y reducción de descompensaciones

11.9.5 Brechas Críticas Identificadas

- **Mantenimiento y Activos:** Inventario único ausente, procesos no estandarizados, baja madurez en contratos y SLA.
- **Gestión de Personas:** Procesos manuales, falta de indicadores, ausencia de políticas de capacitación digital, limitada alfabetización digital.
- **Control de Enfermedades Crónicas:** Gobernanza de datos insuficiente, escasa interoperabilidad, procesos poco homogéneos, carencias en capacitación clínica digital.
- **Analítica y Toma de Decisiones:** Falta de modelo de datos, calidad de datos heterogénea, roles de datos no formalizados, limitada experiencia en BI, ausencia de políticas éticas de datos.

11.9.6 Fases de implementación

Fase	Materia	Acciones Clave
Fase 1: Bases Organizacionales	Mantenimiento, RRHH, Datos	Inventario de activos, capacitación ITIL/ISO, catálogo de servicios, gobernanza de datos, políticas de seguridad y confidencialidad
Fase 2: Digitalización y Estandarización	Procesos críticos	Digitalización de procesos, catálogos de servicios RRFF/RRHH, protocolos de telemonitoreo, reconversión de fuerza laboral, rol de Ingeniero de Datos
Fase 3: Integración y Analítica	Sistemas y datos	Integración de sistemas y tableros BI, SLA de proveedores, ampliación plataforma de autoservicio, formalización de roles de datos, capacitación mandos medios en BI
Fase 4: Optimización e Innovación	Mantenimiento, RRHH, Enfermedades Crónicas, Analítica	Monitoreo predictivo, analítica predictiva, IA para estratificación de riesgo, consolidación de unidad de analítica institucional, cultura de decisiones basadas en datos

11.9.7 Conclusión

La estrategia de TI del Hospital de Tomé permite:

- Fortalecer la continuidad operativa y la seguridad en la atención.
- Optimizar recursos mediante gestión digital de activos y RRHH.
- Impulsar la innovación con analítica avanzada, telemonitoreo y portales digitales.

- Mejorar la toma de decisiones mediante datos confiables y gobernanza sólida.

El resultado esperado es alcanzar una madurez digital avanzada, sostenible y escalable, integrando personas, procesos y tecnología, con impacto directo en la misión y objetivos estratégicos del hospital.

Para revisar detalles de la estrategia se puede acceder al Portal de Soluciones del Área de TI en el siguiente link:
https://hospitaldetome.freshservice.com/support/solutions/articles/37000024685-Estrategia-de-Tecnolog-as-de-la-Informaci-n

11.10 PERFILES DEL ÁREA TI EN FORMATO SFIA VERSIÓN 8

11.10.1 JEFATURA ÁREA DE TECNOLOGÍAS

11.10.1.1 ROL JEFATURA

El Jefe de Tecnologías de la Información y Comunicación (TIC) es el responsable de liderar la estrategia, planificación y ejecución de las iniciativas tecnológicas de la organización, asegurando la alineación con los objetivos institucionales y el impulso de la transformación digital sostenible. Este rol abarca la gestión integral de los recursos tecnológicos, promoviendo la innovación, la eficiencia operativa y la seguridad en un entorno digital dinámico.

a) **Garantía de la Seguridad de la Información**: Desarrollar e implementar políticas, procedimientos y herramientas para proteger los datos y sistemas de la organización, asegurando la confidencialidad, integridad y disponibilidad frente a amenazas internas y externas.
b) **Promoción de Tecnologías y Procesos Digitales**: Liderar la adopción de soluciones tecnológicas innovadoras y la automatización de procesos digitales, optimizando flujos de trabajo y mejorando la experiencia de usuarios internos y externos.
c) **Alineación Estratégica**: Colaborar con la alta dirección para integrar las TIC en la estrategia organizacional, identificando oportunidades de innovación que impulsen la competitividad y el cumplimiento de metas institucionales.
d) **Gestión de Equipos y Proveedores**: Dirigir equipos multidisciplinarios de TI, fomentar el desarrollo profesional y coordinar con proveedores externos para garantizar la calidad y eficiencia de los servicios tecnológicos.
e) **Sostenibilidad y Cumplimiento**: Asegurar que las iniciativas tecnológicas sean ambientalmente responsables y cumplan con normativas locales e internacionales, contribuyendo a una transformación digital ética y sostenible.

11.10.1.2 PROCESOS ASOCIADOS

Proceso	Nivel Requerido	Nivel Actual
Gestionar el cumplimiento de los requisitos externos	4	1
Gestionar el aseguramiento	3	1
Asegurar el establecimiento y el mantenimiento del marco de gobierno	2	2
Asegurar el compromiso de las partes interesadas	2	1
Gestionar el macro de gestión de TI*	2	2

La Jefatura de Tecnologías de la Información y Comunicación debe alcanzar una madurez mínima de sus procesos de **2,8** para poder brindar total cumplimiento a las metas institucionales, actualmente (2025) se logra un **1,4.** La metodología de mejora continua se logra a través del Manual de Gobernanza de TI y la implementación gradual de procesos a través de la estrategia de Gestión de Riesgos Críticos del Establecimiento.
*Nota: Los items marcados con (*) representan a los procesos implementados en el 2024-2025.
Si bien la Jefatura de TI puede utilizar otros procesos establecidos en la Gobernanza de TI, en este manual se declaran los específicos para una mejor comprensión.

11.10.1.3 PERFIL DEL CARGO

El perfil del Cargo de jefe de Tecnologías de la Información y Comunicación del Hospital de Tomé está asociado a Liderar estratégicamente supervisando todas las operaciones tecnológicas del Establecimiento. Su principal objetivo es alinear la tecnología con los

objetivos del Plan Estratégico, asegurando que la infraestructura tecnológica sea eficiente, segura y soporte el crecimiento de la institución.
Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Ingeniero Civil en Informática y Computación (Preferible)
- Ingeniero en Informática
- Ingeniero Civil Industrial, Especialización en TI

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.
Planificación estratégica (ITSP)	Crear y mantener estrategias a nivel organizacional para alinear los planes, acciones y recursos de negocio generales con los objetivos de negocio de alto nivel.	7
Análisis de la Situación Institucional (BUSA)	Investigar las situaciones del negocio para definir recomendaciones a fin de tomar medidas que permitan mejorar.	6
Mejora de procesos de negocio (BPRE)	Crear enfoques nuevos y potencialmente disruptivos para llevar a cabo actividades comerciales.	7
Gobernanza (GOVN)	Definir y operar marcos para el apoyo de la toma de decisiones, gestión de riesgos, relaciones con las partes interesadas y el cumplimiento de las obligaciones organizativas y regulatorias.	7
Arquitectura empresarial y de negocios (STPL)	Alinear la estrategia tecnológica de la organización con su misión, estrategia y procesos comerciales, y documentarlo mediante modelos arquitectónicos.	7
Adquisición (SORC)	Gestionar la adquisición o el encargo de productos y servicios, o brindar asesoramiento sobre ellos.	6
Dirección de Proyectos (PRMG)	Lograr los resultados acordados del proyecto alineando las técnicas de gestión, colaboración, liderazgo y gobernanza adecuadas con los contextos específicos del proyecto y la organización.	5
Aseguramiento de la Información (INAS)	Proteger y gestionar los riesgos relacionados con el uso, el almacenamiento y la transmisión de datos y sistemas de información.	7
Gestión de servicios tecnológicos (ITMG)	Gestionar la prestación de servicios basados en la tecnología para cumplir necesidades organizacionales definidas.	7
Presupuesto y previsión (BUDF)	Elaboración y gestión del presupuesto, así como de las previsiones financieras que permitan tanto la eficaz toma de decisiones y la asignación de recursos.	5

El nivel de responsabilidad de las habilidades expuestas pondera un **6.4/7** lo que significa que este rol tiene una influencia organizativa considerable, toma decisiones de alto nivel, moldea políticas, demuestra liderazgo, promueve la colaboración organizacional y acepta la rendición de cuentas en áreas clave.

Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Orienta las decisiones y estrategias de alto nivel dentro de las políticas y objetivos generales de la organización. Tiene autoridad y rendición de cuentas definidas por las acciones y decisiones dentro de un área significativa de trabajo, incluso aspectos técnicos, financieros y de calidad. Delega la responsabilidad de los objetivos operativos.
INFLUENCIA	Influye en la formación de la estrategia y en la ejecución de los planes de negocio. Tiene un nivel gerencial significativo de contacto con colegas internos y contactos externos. Tiene liderazgo organizacional e influencia sobre el nombramiento y manejo de recursos relacionados con la implementación de iniciativas estratégicas.
COMPLEJIDAD	Realiza actividades laborales de alta complejidad que abarcan aspectos técnicos, financieros y de calidad.
CONOCIMIENTO	Aplica amplios conocimientos empresariales para permitir el liderazgo estratégico y la toma de decisiones en diversos ámbitos.

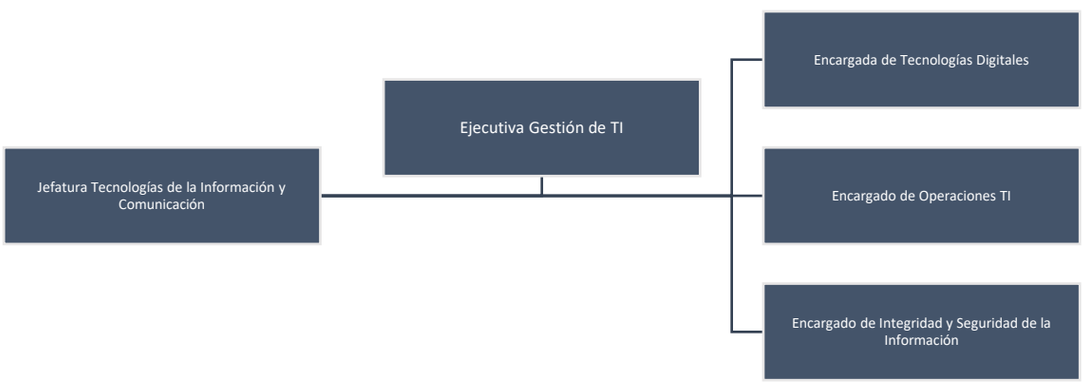
Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza su criterio para tomar decisiones que inician el logro de los objetivos estratégicos acordados, incluido el rendimiento financiero. • Escala cuando se ve afectada una dirección estratégica más amplia
PLANIFICACIÓN	• Inicia e influye en los objetivos estratégicos y asigna responsabilidades.
COLABORACIÓN	• Lidera la colaboración con una amplia gama de partes interesadas a través de objetivos contrapuestos dentro de la organización. • Establece conexiones sólidas e influyentes con contactos internos y externos fundamentales a nivel de dirección superior/líder técnico.
RESOLUCIÓN DE PROBLEMAS	• Anticipa y lidera la resolución de problemas y oportunidades que puedan afectar los objetivos de la organización, estableciendo un enfoque estratégico y asignando recursos.
MENTALIDAD DE MEJORA	• Impulsa iniciativas de mejora que tienen un impacto significativo en la organización. • Alinea las estrategias de mejora con los objetivos organizacionales. • Involucra a las partes interesadas en los procesos de mejora.
CREATIVIDAD	• Aplica creativamente una amplia gama de nuevas ideas y técnicas de gestión eficaces para lograr resultados que se alinean con la estrategia de la organización.
COMUNICACIÓN	• Comunica con credibilidad a todos los niveles y en toda la organización a audiencias amplias con objetivos divergentes. • Explica claramente información e ideas complejas, influyendo en la dirección estratégica. • Promueve el intercambio de información en toda la

	organización.
LIDERAZGO	• Proporciona liderazgo a nivel organizacional. • Contribuye al desarrollo e implementación de políticas y estrategias. • Entiende y comunica la evolución de la industria, y el rol y el impacto de la tecnología. • Gestiona y mitiga los riesgos organizacionales. • Equilibra los requisitos de las propuestas con las necesidades más generales de la organización.
ADAPTABILIDAD	• Impulsa la adaptabilidad organizacional iniciando y liderando cambios significativos. Influye en las estrategias de gestión del cambio a nivel organizacional.
MENTALIDAD DIGITAL	• Lidera la mejora de las capacidades digitales de la organización. • Identifica y respalda oportunidades para adoptar nuevas tecnologías y servicios digitales. • Lidera la gobernanza digital y el cumplimiento de la legislación pertinente, y la necesidad de productos y servicios.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Desempeña un papel de liderazgo en la promoción y garantía de una cultura y prácticas de trabajo adecuadas, incluida la igualdad de acceso y oportunidades para las personas con capacidades diversas.

11.10.1.4 PERSONAL A CARGO DIRECTO

El rol de Jefe de Área de Tecnologías de la información tiene bajo su cargo a los siguientes roles:



11.10.2 ENCARGADO OPERACIONES TI

11.10.2.1 ROL ENCARGADO

El Encargado de Operaciones TI lidera el desarrollo, construcción, seguimiento y mejora de la Línea Estratégica de Infraestructura de TI, garantizando una infraestructura robusta y su soporte operacional. Coordina con el Centro de Servicios TI para brindar soporte operativo, gestionar activos y monitorear continuamente los activos críticos, implementando acciones preventivas para asegurar la continuidad operativa. Además, asume la responsabilidad de subrogar al Jefe de Área de Tecnologías de la Información cuando sea necesario.

a) **Desarrollar infraestructura TI: Diseñar, construir y mejorar la línea estratégica de la Infraestructura de TI para garantizar robustez**
b) **Asegurar Soporte Operacional**: Mantener la operatividad mediante soporte continuo, en sus respectivas especialidades de Infraestructura y Sistemas gestionados por el Centro de Servicio TI.
c) **Monitorear activos Críticos**: Supervisar activos TI críticos, implementando acciones preventivas para la continuidad operativa.

11.10.2.2 PROCESOS ASOCIADOS

Proceso	Nivel Requerido	Nivel Actual
Gestión de Riesgos	4	1
Gestionar la Continuidad*	3	1
Gestionar las peticiones y los incidentes de servicio*	2	2
Gestionar las relaciones con proveedores*	2	1
Gestionar la disponibilidad y la capacidad	2	1
Gestionar los proyectos	2	1
Gestionar los problemas*	2	1
Gestionar los Activos*	2	2
Gestionar la configuración*	2	2
Gestión de Cambio*	2	1

El encargado de Operaciones TI debe alcanzar una madurez mínima de sus procesos de **2.3** para poder brindar total cumplimiento a las metas institucionales, actualmente (2025) se logra un **1,3.**
La metodología de mejora continua se logra a través del Manual de Gobernanza de TI y la implementación gradual de procesos a través de la estrategia de Gestión de Riesgos Críticos del Establecimiento y el SGSI.
*Nota: Los items marcados con (*) representan a los procesos implementados en el 2024-2025.
Con los procesos a implementar en el 2025 se espera que para inicios del 2026 se logre una madurez de 2.1 lo que es un gran avance propiciado por el COMGES 2025 asociado a la implementación de controles críticos relacionados a la Seguridad de la Información contenidos en la ISO/IEC 27002:2013.

11.10.2.3 PERFIL DEL CARGO

El perfil del Cargo de Encargado de Operaciones TI es responsable de garantizar que la infraestructura tecnológica del Hospital funcione de manera eficiente, segura y confiable. Su rol es crucial para mantener los sistemas operativos, las redes, el hardware y el software en óptimas condiciones, asegurando así la continuidad de las operaciones del establecimiento.
Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Ingeniero en Informática (Preferible)
- Ingeniero Civil en Informática
- Ingeniero en Telecomunicaciones

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.
MÉTODOS Y HERRAMIENTAS (METL)	Asegurarse de que se adopten y utilicen de manera efectiva los métodos y las herramientas en toda la organización.	6
GESTIÓN DE NIVEL DE SERVICIO (SLMO)	Acordar objetivos para los niveles de servicio y evaluar, supervisar y gestionar la prestación de servicios en relación con los objetivos.	5
GESTIÓN DEL CATÁLOGO DE SERVICIOS (SCMG)	Brindar una fuente de información coherente sobre los servicios y productos disponibles para clientes y usuarios.	4
GESTIÓN DE INCIDENTES (USUP)	Coordinar las respuestas a los informes de incidentes, minimizar los impactos negativos y restaurar el servicio lo más rápidamente posible.	5
GESTIÓN DE PROBLEMAS (PBMG)	Gestionar el ciclo de vida de todos los problemas que han ocurrido o que podrían ocurrir durante la prestación de un servicio.	5
CONTROL DE CAMBIOS (CHMG)	Evaluar los riesgos asociados con los cambios propuestos y garantizar el control y la coordinación de los cambios en los productos, servicios o sistemas.	5
GESTIÓN DE ACTIVOS (ASMG)	Gestionar el ciclo de vida completo de los activos desde la adquisición, operación y mantenimiento hasta su retiro del ambiente productivo.	5
ADQUISICIÓN (SORC)	Gestionar la adquisición o el encargo de productos y servicios, o brindar asesoramiento sobre ellos.	4
GESTION DE LA CONTINUIDAD (COPL)	Desarrollar, implementar y probar un marco de la continuidad del negocio	5
GESTIÓN DE RIESGOS (BURM)	Planificar e implementar procesos y procedimientos en toda la organización para la gestión de riesgos hacia el éxito o la integridad de la empresa.	3
INFRAESTRUCTURA DE TI (ITOP)	Implementar, configurar y operar infraestructura de TI.	5
GESTIÓN DE INSTALACIONES (DCMA)	Planificar, diseñar y gestionar los edificios, el espacio y las instalaciones que, en conjunto, componen el parque informático de TI.	5
GESTIÓN DE LA DISPONIBILIDAD (AVMT)	Garantizar que los servicios ofrezcan los niveles acordados de disponibilidad para satisfacer las necesidades actuales y futuras del negocio.	5
GESTIÓN DE LA CAPACIDAD (CPMG)	Garantizar que los componentes del servicio tengan la capacidad y el rendimiento necesarios para satisfacer las necesidades actuales y planificadas del negocio.	3
GESTIÓN DE OFERTAS / PROPUESTAS (BIDM)	Gestionar la preparación y presentación de ofertas y propuestas de contratos, adjudicaciones, proyectos o servicios.	5
GESTIÓN DE PROVEEDORES (SUPP)	Alinear los objetivos y las actividades de los proveedores de una organización con las estrategias y los planes de abastecimiento, el equilibrio de los costos, la eficiencia y la calidad del servicio.	5
GESTIÓN DE IDENTIDAD Y	Gestiona la verificación de identidad y los	3

ACCESO (IAMT)	permisos de acceso dentro de los sistemas y entornos organizativos.	

El nivel de responsabilidad de las habilidades expuestas pondera un **4.7 (5)/7** lo que significa que este rol proporciona orientación autorizada en su campo y trabaja bajo una dirección amplia. Responsable de entregar resultados de trabajo significativos, desde el análisis hasta la ejecución y evaluación.

Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Trabaja bajo una dirección amplia. El trabajo es de iniciativa propia, coherente con los requisitos operativos y presupuestarios acordados para cumplir los objetivos técnicos y/o grupales asignados. Define tareas y delega el trabajo en equipos e individuos dentro de su área de responsabilidad.
INFLUENCIA	Influye en las decisiones críticas bajo su dominio. Mantiene contacto a nivel operativo que impacta en la ejecución e implementación con colegas internos y contactos externos. Tiene influencia considerable en la asignación y gestión de los recursos requeridos para entregar los proyectos.
COMPLEJIDAD	Realiza una amplia gama de actividades complejas de trabajo técnico y/o profesional, que requieren la aplicación de principios fundamentales en una gama de contextos impredecibles.
CONOCIMIENTO	Aplica conocimientos para interpretar situaciones complejas y ofrecer asesoramiento autorizado. Aplica una experiencia profunda en campos específicos, con una comprensión más amplia en toda la industria o negocio.

Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza el buen juicio para tomar decisiones informadas sobre las acciones para lograr resultados organizacionales, como el cumplimiento de metas, plazos y presupuestos. • Plantea cuestionamientos cuando los objetivos están en riesgo.
PLANIFICACIÓN	• Analiza, diseña, planifica, establece hitos y ejecuta y evalúa el trabajo según los objetivos de tiempo, costo y calidad.
COLABORACIÓN	• Facilita la colaboración entre las partes interesadas que tienen diversos objetivos. • Garantiza formas de trabajo colaborativas en todas las etapas del trabajo para satisfacer las necesidades del usuario/cliente. • Construye relaciones efectivas en toda la organización y con clientes, proveedores y socios.
RESOLUCIÓN DE PROBLEMAS	• Investiga cuestiones complejas para identificar las causas fundamentales y los impactos, evalúa una variedad de soluciones y toma decisiones informadas sobre el mejor curso de acción, a menudo en colaboración con otros expertos.
MENTALIDAD DE MEJORA	• Identifica y evalúa mejoras potenciales de productos, prácticas o servicios. • Dirige la aplicación de mejoras dentro de su propia área de responsabilidades.

	• Evalúa la efectividad de los cambios implementados.
CREATIVIDAD	• Aplica de manera creativa el pensamiento innovador y prácticas de diseño para identificar soluciones que le den valor en beneficio de clientes y partes interesadas.
COMUNICACIÓN	• Comunica claramente y con impacto, articulando información e ideas complejas para audiencias amplias con diferentes puntos de vista. • Lidera y fomenta conversaciones para compartir ideas y generar consenso sobre las medidas a tomar.
LIDERAZGO	• Proporciona liderazgo a nivel operativo. • Implementa y ejecuta políticas alineadas con los planes estratégicos. • Estima y evalúa riesgos. • Al examinar propuestas toma en cuenta todos los requisitos.
ADAPTABILIDAD	• Lidera adaptaciones a entornos empresariales cambiantes. • Guía a los equipos a través de las transiciones, manteniendo el enfoque en los objetivos organizacionales.
MENTALIDAD DIGITAL	• Reconoce y evalúa el impacto organizacional de las nuevas tecnologías y servicios digitales. • Implementa prácticas nuevas y efectivas. • Asesora sobre los estándares, métodos, herramientas, aplicaciones y procesos disponibles y relevantes para especialidades grupales, y puede tomar decisiones apropiadas a partir de las alternativas.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Contribuye de manera proactiva a la implementación de prácticas de trabajo profesionales y ayuda a promover una cultura organizacional de apoyo.

11.10.2.4 PERSONAL A CARGO DIRECTO

El rol de Encargado de Operaciones TI tiene bajo su cargo a los siguientes roles:

11.10.3 ENCARGADA CENTRO DE SERVICIO TI

11.10.3.1 ROL ENCARGADA

La Encargada del Centro de Servicios TI lidera la mesa de ayuda tecnológica, actuando como el punto central de contacto para todas las solicitudes de soporte técnico de los usuarios. Su rol implica dirigir y coordinar un equipo dedicado a gestionar, priorizar y resolver eficientemente incidentes y solicitudes, asegurando una experiencia de usuario fluida. Además, colabora estrechamente con otras áreas de TI para garantizar soluciones integrales y oportunas, optimizando la operatividad y la satisfacción del usuario.

a) **Dirigir la Mesa de Ayuda TI: Supervisar y coordinar las operaciones del equipo de soporte, asegurando un servicio eficiente y de calidad como punto único de contacto.**
b) **Gestionar incidentes y solicitudes**: Priorizar, asignar y resolver incidentes y solicitudes de soporte técnico de manera oportuna, minimizando interrupciones.
c) **Coordinar con unidades de TI**: Colaborar con otros equipos de TI para escalar y resolver eventos complejos, garantizando soluciones integrales.
d) **Optimizar la experiencia del usuario**: Monitorear la calidad del servicio e implementar mejoras continuas para aumentar la satisfacción y eficiencia del soporte.

11.10.3.2 PROCESOS ASOCIADOS

Proceso	Nivel Requerido	Nivel Actual
Gestionar las peticiones y los incidentes de servicio*	2	2
Gestionar los problemas*	2	1
Gestionar los Activos*	2	2
Gestionar la configuración*	2	2
Gestión de Cambio*	2	1

La Encargada del Centro de Servicio TI debe alcanzar una madurez mínima de sus procesos de **2** para poder brindar total cumplimiento a las metas institucionales, actualmente (2025) se logra un **1,6.**
La metodología de mejora continua se logra a través del Manual de Gobernanza de TI y la implementación gradual de procesos a través de la estrategia de Gestión de Riesgos Críticos del Establecimiento y el SGSI.
*Nota: Los items marcados con (*) representan a los procesos implementados en el 2024-2025.
Con los procesos a implementar en el 2025 se espera que para inicios del 2026 se logre una madurez de 2 lo que es un gran avance propiciado por el COMGES 2025 asociado a la implementación de controles críticos relacionados a la Seguridad de la Información contenidos en la ISO/IEC 27002:2013 y a requerimientos derivadas de Auditoría Interna indicada por el CAIGG en el 2024.

11.10.3.3 PERFIL DEL CARGO

El perfil del Cargo de Encargada del Centro de Servicio TI es responsable de dirigir y coordinar servicio de atención al usuario que actúa como punto único de contacto para todas las solicitudes de soporte técnico. Su equipo se encarga de gestionar, priorizar y resolver de manera eficiente los incidentes y solicitudes de los usuarios, coordinándose internamente con otras áreas de TI para garantizar una solución integral.
Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Ingeniero en Informática (Preferible)
- Ingeniero en Telecomunicaciones
- Ingeniero Industrial, Especialización TI

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.
MÉTODOS Y HERRAMIENTAS (METL)	Asegurarse de que se adopten y utilicen de manera efectiva los métodos y las herramientas en toda la organización.	3
GESTIÓN DE NIVEL DE SERVICIO (SLMO)	Acordar objetivos para los niveles de servicio y evaluar, supervisar y gestionar la prestación de servicios en relación con los objetivos.	3
GESTIÓN DEL CATÁLOGO DE SERVICIOS (SCMG)	Brindar una fuente de información coherente sobre los servicios y productos disponibles para clientes y usuarios.	3
GESTIÓN DE INCIDENTES (USUP)	Coordinar las respuestas a los informes de incidentes, minimizar los impactos negativos y restaurar el servicio lo más rápidamente posible.	2
GESTIÓN DE PROBLEMAS (PBMG)	Gestionar el ciclo de vida de todos los problemas que han ocurrido o que podrían ocurrir durante la prestación de un servicio.	3
CONTROL DE CAMBIOS (CHMG)	Evaluar los riesgos asociados con los cambios propuestos y garantizar el control y la coordinación de los cambios en los productos, servicios o sistemas.	3
SOPORTE DE SERVICIO AL CLIENTE (CSMG)	Gestionar y operar las funciones del servicio de atención al cliente o del servicio técnico.	5
GESTIÓN DE ACTIVOS (ASMG)	Gestionar el ciclo de vida completo de los activos desde la adquisición, operación y mantenimiento hasta su retiro del ambiente productivo.	4
GESTIÓN DE LA CONFIGURACIÓN (CFMG)	Planificar, identificar, controlar, contabilizar y auditar elementos de configuración (CI) y sus interrelaciones.	2

El nivel de responsabilidad de las habilidades expuestas pondera un **3.1 (3)/7** lo que significa que este rol realiza tareas variadas, a veces complejas y no rutinarias, utilizando métodos y procedimientos estándar. Trabaja bajo dirección general, ejerce discreción y gestiona el propio trabajo dentro de los plazos. Potencia proactivamente las habilidades y el impacto en el lugar de trabajo. Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Trabaja bajo dirección general para completar las tareas asignadas. Recibe orientación y hace revisar el trabajo en hitos acordados. Cuando es necesario, delega tareas rutinarias a otros dentro de su propio equipo.
INFLUENCIA	Trabaja e influye en las decisiones del equipo. Tiene un nivel transaccional de contacto con personas ajenas a su equipo, incluso colegas internos y contactos externos.
COMPLEJIDAD	Realiza una variedad de trabajos, a veces complejos y no rutinarios, en ambientes variados.
CONOCIMIENTO	Aplica el conocimiento de una serie de prácticas específicas de roles para completar tareas dentro de límites definidos y tiene una apreciación de cómo este conocimiento se aplica al contexto empresarial más amplio.

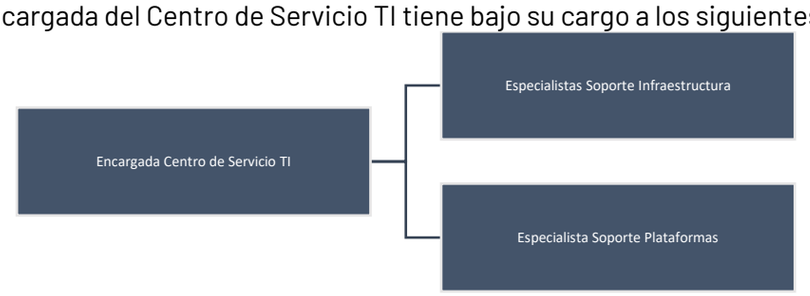
Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza discreción para identificar y responder a problemas complejos relacionados con sus propias asignaciones.

	• Determina cuándo los problemas deben escalarse a un nivel superior.
PLANIFICACIÓN	• Organiza y realiza un seguimiento de su propio trabajo (y de otros, cuando sea necesario) para cumplir los plazos acordados.
COLABORACIÓN	• Comprende y colabora en el análisis de las necesidades del usuario/cliente y así lo representa en su trabajo.
RESOLUCIÓN DE PROBLEMAS	• Aplica un enfoque metódico para investigar y evaluar opciones para resolver problemas rutinarios y moderadamente complejos.
MENTALIDAD DE MEJORA	• Identifica e implementa mejoras en su propia área de trabajo. • Contribuye a las mejoras de procesos a nivel de equipo.
CREATIVIDAD	• Aplica y contribuye a las técnicas de pensamiento creativo para aportar nuevas ideas para su propio trabajo y para actividades en equipo.
COMUNICACIÓN	• Se comunica con el equipo y las partes interesadas dentro y fuera de la organización, explicando y presentando información de forma clara. • Contribuye a una variedad de conversaciones relacionadas con el trabajo y escucha a los demás para comprender y hace preguntas de sondeo relevantes para su función.
LIDERAZGO	• Proporciona orientación básica y apoyo a los miembros menos experimentados del equipo según sea necesario.
ADAPTABILIDAD	• Se adapta y responde al cambio y muestra iniciativa en la adopción de nuevos métodos o tecnologías.
MENTALIDAD DIGITAL	• Explora y aplica herramientas y habilidades digitales relevantes para su función. • Comprende y aplica de manera efectiva métodos, herramientas, aplicaciones y procesos adecuados.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Aplica el profesionalismo adecuado y las prácticas y conocimientos prácticos para trabajar.

11.10.3.4 PERSONAL A CARGO DIRECTO

El rol de Encargada del Centro de Servicio TI tiene bajo su cargo a los siguientes roles:



11.10.4 ESPECIALISTAS SOPORTE INFRAESTRUCTURA

11.10.4.1 ROL ESPECIALISTA INFRAESTRUCTURA

El Especialista de Soporte de Infraestructura TI es responsable de garantizar el correcto funcionamiento y la disponibilidad de la infraestructura tecnológica de la organización. Su labor es esencial para mantener la continuidad operativa de los servicios de TI, mediante la gestión, mantenimiento y optimización de los sistemas y recursos tecnológicos. Colabora con otros equipos de TI para resolver problemas técnicos y prevenir interrupciones, asegurando un entorno tecnológico estable y eficiente.

a) **Mantener la infraestructura TI: Realiza el mantenimiento preventivo y correctivo de servidores, redes y otros componentes tecnológicos para garantizar su operatividad.**
b) **Resolver incidencias técnicas/solicitudes**: Diagnosticar y solucionar fallos en la infraestructura, colaborando con otros equipos de TI para garantizar una respuesta rápida.

11.10.4.2 PROCESOS ASOCIADOS

Proceso	Nivel Requerido	Nivel Actual
Gestionar las peticiones y los incidentes de servicio*	2	2
Gestionar los problemas*	2	1
Gestionar los Activos*	2	2
Gestionar la configuración*	2	2
Gestión de Cambio*	2	1

El Especialista de Soporte Infraestructura tiene el mismo modelo de madurez que el Rol de Encargada del Centro de Servicio TI, dado que se abordan los mismos procesos.

11.10.4.3 PERFIL DEL CARGO

El perfil del Cargo de Encargada del Centro de Servicio TI es responsable de dirigir y coordinar servicio de atención al usuario que actúa como punto único de contacto para todas las solicitudes de soporte técnico. Su equipo se encarga de gestionar, priorizar y resolver de manera eficiente los incidentes y solicitudes de los usuarios, coordinándose internamente con otras áreas de TI para garantizar una solución integral.
Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Técnico Superior en Informática o Redes (Preferible)
- Técnico Superior Administrador de Sistemas
- Ingeniero en Informática (Sin experiencia)

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.
ASESORAMIENTO ESPECIALIADO (TECH)	Proporcionar asesoramiento y orientación autorizados en un área especializada.	4
SOPORTE DE RED (NTAS)	Prestación de servicios de mantenimiento y soporte para redes de comunicaciones.	2
SOPORTE DE APLICACIONES (ASUP)	Prestar servicios de gestión, técnicos y administrativos para apoyar y mantener aplicaciones en vivo.	2
ADMINISTRACIÓN DEL SOFTWARE DE SISTEMAS (SYSP)	Instalación, gestión y mantenimiento de sistemas operativos, gestión de datos, ofimática y software utilitario en diversos entornos de infraestructura.	2
GESTIÓN DE INCIDENTES (USUP)	Coordinar las respuestas a los informes de incidentes, minimizar los impactos negativos y	2

	restaurar el servicio lo más rápidamente posible.	
GESTIÓN DE PROBLEMAS (PBMG)	Gestionar el ciclo de vida de todos los problemas que han ocurrido o que podrían ocurrir durante la prestación de un servicio.	2
CONTROL DE CAMBIOS (CHMG)	Evaluar los riesgos asociados con los cambios propuestos y garantizar el control y la coordinación de los cambios en los productos, servicios o sistemas.	2
SOPORTE DE SERVICIO AL CLIENTE (CSMG)	Gestionar y operar las funciones del servicio de atención al cliente o del servicio técnico.	2
GESTIÓN DE ACTIVOS (ASMG)	Gestionar el ciclo de vida completo de los activos desde la adquisición, operación y mantenimiento hasta su retiro del ambiente productivo.	2
GESTIÓN DE LA CONFIGURACIÓN (CFMG)	Planificar, identificar, controlar, contabilizar y auditar elementos de configuración (CI) y sus interrelaciones.	2
GESTIÓN DE IDENTIDAD Y ACCESO (IAMT)	Gestiona la verificación de identidad y los permisos de acceso dentro de los sistemas y entornos organizativos.	1

El nivel de responsabilidad de las habilidades expuestas pondera un **2.2 (2)/7** lo que significa que este rol proporciona asistencia a otros, trabaja bajo supervisión de rutina y usa su discreción para abordar problemas rutinarios. Aprende activamente a través de entrenamiento y experiencias en el trabajo. Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Trabaja bajo dirección rutinaria. Recibe instrucciones y orientación, su trabajo es revisado regularmente.
INFLUENCIA	Se espera que contribuya a las discusiones del equipo con los miembros inmediatos del equipo. Trabaja junto a los miembros del equipo, contribuyendo a las decisiones del equipo. Cuando el rol lo requiere, interactúa con personas fuera de su equipo, incluyendo colegas internos y contactos externos.
COMPLEJIDAD	Realiza una variedad de actividades laborales en diversos entornos.
CONOCIMIENTO	Aplica el conocimiento de las tareas y prácticas comunes del lugar de trabajo para apoyar las actividades del equipo bajo orientación.

Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza discreción limitada para resolver problemas o consultas. • Decide cuándo buscar orientación en situaciones inesperadas.
PLANIFICACIÓN	• Planifica su propio trabajo en cortos horizontes temporales de forma organizada.
COLABORACIÓN	• Comprende la necesidad de colaborar con su equipo y considera las necesidades del usuario/cliente.
RESOLUCIÓN DE PROBLEMAS	• Investiga y resuelve problemas rutinarios.
MENTALIDAD DE MEJORA	• Propone ideas para mejorar el área de trabajo propia. • Implementa cambios acordados en las tareas de trabajo asignadas.
CREATIVIDAD	• Aplica el pensamiento creativo para sugerir nuevas formas de abordar una tarea y resolver problemas.
COMUNICACIÓN	• Comunica información familiar con el equipo inmediato y las partes interesadas directamente

	relacionadas con su función. • Escucha para obtener comprensión y hace preguntas relevantes para aclarar o buscar más información.
LIDERAZGO	• Se hace cargo de desarrollar su experiencia laboral.
ADAPTABILIDAD	• Se ajusta a diferentes dinámicas de equipo y requisitos de trabajo. • Participa en procesos de adaptación de equipos.
MENTALIDAD DIGITAL	• Tiene habilidades digitales suficientes para su rol; comprende y utiliza métodos, herramientas, aplicaciones y procesos apropiados.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Tiene una buena comprensión de su papel y de las reglas y expectativas de la organización.

11.10.4.4 PERSONAL A CARGO DIRECTO

El rol no presenta personal a cargo directo por una definición de estructura organizativa.

11.10.5 ESPECIALISTAS SOPORTE PLATAFORMAS

11.10.5.1 ROL ESPECIALISTA PLATAFORMAS

El Especialista de Soporte de Plataformas es responsable de garantizar el funcionamiento óptimo y la continuidad de las plataformas y sistemas institucionales, incluyendo el Registro Clínico Electrónico, RIS/PACS, sistemas de laboratorio, recursos humanos, finanzas y abastecimiento, entre otros. Su rol es crucial para mantener la operatividad de estos sistemas, implementar mejoras continuas y capacitar a los usuarios, asegurando una integración eficiente y un soporte técnico de calidad que respalde los procesos institucionales.

a) **Mantener plataformas y sistemas:** Gestionar y realizar mantenimiento preventivo y correctivo de las plataformas institucionales para garantizar su disponibilidad y correcto funcionamiento.
b) **Capacitar Usuarios**: Diseñar y ejecutar programas de capacitación continua para usuarios, asegurando un uso adecuado y eficiente de los sistemas.
c) **Coordinar soporte técnico**: Colaborar con equipos de TI y proveedores externos para resolver problemas complejos y garantizar la integración de las plataformas con otros sistemas.

11.10.5.2 PROCESOS ASOCIADOS

Proceso	Nivel Requerido	Nivel Actual
Gestionar las peticiones y los incidentes de servicio*	2	2
Gestionar los problemas*	2	1
Gestionar los Activos*	2	2
Gestionar la configuración*	2	2
Gestión de Cambio*	2	1

El Especialista de Soporte de Plataformas tiene el mismo modelo de madurez que el Rol de Encargada del Centro de Servicio TI, dado que se abordan los mismos procesos.
Sin embargo, este rol no está activo en la institución y es realizado en parte por la Encargada de Tecnologías Digitales.

11.10.5.3 PERFIL DEL CARGO

El perfil del Cargo de Encargada del Centro de Servicio TI es responsable de garantizar el funcionamiento óptimo y la continuidad de las plataformas y sistemas institucionales.
Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Tecnólogo en Informática Biomédica (Preferible)
- Ingeniero en Informática
- Ingeniero Industrial, Especialización en TI

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.
ASESORAMIENTO ESPECIALIADO (TECH)	Proporcionar asesoramiento y orientación autorizados en un área especializada.	4
PRUEBAS (TEST)	Investigar productos, sistemas y servicios para evaluar el comportamiento y si este cumple requisitos y características especificados o no especificados.	3
SOPORTE DE APLICACIONES (ASUP)	Prestar servicios de gestión, técnicos y administrativos para apoyar y mantener aplicaciones en vivo.	3
CONSULTORÍA (CNSL)	Proporciona consejos y recomendaciones, basados en conocimientos y experiencia, para abordar las necesidades del cliente.	4

GESTIÓN DE INCIDENTES (USUP)	Coordinar las respuestas a los informes de incidentes, minimizar los impactos negativos y restaurar el servicio lo más rápidamente posible.	2
GESTIÓN DE PROBLEMAS (PBMG)	Gestionar el ciclo de vida de todos los problemas que han ocurrido o que podrían ocurrir durante la prestación de un servicio.	2
CONTROL DE CAMBIOS (CHMG)	Evaluar los riesgos asociados con los cambios propuestos y garantizar el control y la coordinación de los cambios en los productos, servicios o sistemas.	2
SOPORTE DE SERVICIO AL CLIENTE (CSMG)	Gestionar y operar las funciones del servicio de atención al cliente o del servicio técnico.	2
GESTIÓN DE ACTIVOS (ASMG)	Gestionar el ciclo de vida completo de los activos desde la adquisición, operación y mantenimiento hasta su retiro del ambiente productivo.	2
ENTREGA DE APREDIZAJE (ETDL)	Transferir conocimientos, desarrollar habilidades y cambiar comportamientos utilizando una variedad de técnicas, recursos y medios.	4
GESTIÓN DE IDENTIDAD Y ACCESO (IAMT)	Gestiona la verificación de identidad y los permisos de acceso dentro de los sistemas y entornos organizativos.	2

El nivel de responsabilidad de las habilidades expuestas pondera un **2.8 (3)/7** lo que significa que este rol realiza tareas variadas, a veces complejas y no rutinarias, utilizando métodos y procedimientos estándar. Trabaja bajo dirección general, ejerce discreción y gestiona el propio trabajo dentro de los plazos. Potencia proactivamente las habilidades y el impacto en el lugar de trabajo.
Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Trabaja bajo dirección general para completar las tareas asignadas. Recibe orientación y hace revisar el trabajo en hitos acordados. Cuando es necesario, delega tareas rutinarias a otros dentro de su propio equipo.
INFLUENCIA	Trabaja e influye en las decisiones del equipo. Tiene un nivel transaccional de contacto con personas ajenas a su equipo, incluso colegas internos y contactos externos.
COMPLEJIDAD	Realiza una variedad de trabajos, a veces complejos y no rutinarios, en ambientes variados.
CONOCIMIENTO	Aplica el conocimiento de una serie de prácticas específicas de roles para completar tareas dentro de límites definidos y tiene una apreciación de cómo este conocimiento se aplica al contexto empresarial más amplio.

Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza discreción para identificar y responder a problemas complejos relacionados con sus propias asignaciones. • Determina cuándo los problemas deben escalarse a un nivel superior.
PLANIFICACIÓN	• Organiza y realiza un seguimiento de su propio trabajo (y de otros, cuando sea necesario) para cumplir los plazos acordados.
COLABORACIÓN	• Comprende y colabora en el análisis de las necesidades del usuario/cliente y así lo representa en su trabajo.

RESOLUCIÓN DE PROBLEMAS	• Aplica un enfoque metódico para investigar y evaluar opciones para resolver problemas rutinarios y moderadamente complejos.
MENTALIDAD DE MEJORA	• Identifica e implementa mejoras en su propia área de trabajo. • Contribuye a las mejoras de procesos a nivel de equipo.
CREATIVIDAD	• Aplica y contribuye a las técnicas de pensamiento creativo para aportar nuevas ideas para su propio trabajo y para actividades en equipo.
COMUNICACIÓN	• Se comunica con el equipo y las partes interesadas dentro y fuera de la organización, explicando y presentando información de forma clara. • Contribuye a una variedad de conversaciones relacionadas con el trabajo y escucha a los demás para comprender y hace preguntas de sondeo relevantes para su función.
LIDERAZGO	• Proporciona orientación básica y apoyo a los miembros menos experimentados del equipo según sea necesario.
ADAPTABILIDAD	• Se adapta y responde al cambio y muestra iniciativa en la adopción de nuevos métodos o tecnologías.
MENTALIDAD DIGITAL	• Explora y aplica herramientas y habilidades digitales relevantes para su función. • Comprende y aplica de manera efectiva métodos, herramientas, aplicaciones y procesos adecuados.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Aplica el profesionalismo adecuado y las prácticas y conocimientos prácticos para trabajar.

11.10.5.4 PERSONAL A CARGO DIRECTO

El rol no presenta personal a cargo directo por una definición de estructura organizativa.

11.10.6 ENCARGADA TECNOLOGÍAS DIGITALES

11.10.6.1 ROL ENCARGADA

La Encargada de Tecnologías Digitales actúa como líder táctico en la transformación digital del hospital, promoviendo la adopción estratégica de tecnologías innovadoras. Su rol es esencial para evaluar las capacidades tecnológicas actuales, diseñar e implementar soluciones digitales que optimicen los procesos institucionales y guiar a la organización hacia un futuro digitalmente avanzado. Colabora con diversas áreas para alinear las iniciativas tecnológicas con los objetivos estratégicos, asegurando una integración efectiva y sostenible.

a) **Diseñar soluciones innovadoras:** Desarrollar e implementar estrategias y herramientas digitales que optimicen procesos clínicos, administrativos y operativos del hospital.
b) **Impulsar la transformación digital**: Liderar proyectos de adopción tecnológica, promoviendo una cultura de innovación y alineación con los objetivos institucionales.
c) **Coordinar con áreas clave**: Colaborar con equipos de TI, clínicos y administrativos para garantizar la integración y aceptación de las soluciones digitales.
d)

11.10.6.2 PROCESOS ASOCIADOS

Proceso	Nivel Requerido	Nivel Actual
Gestión de Riesgos	4	1
Gestionar la Continuidad*	3	1
Gestionar las peticiones y los incidentes de servicio*	2	2
Gestionar las relaciones con proveedores*	2	1
Gestionar la disponibilidad y la capacidad	2	1
Gestionar los proyectos	2	1
Gestionar los problemas*	2	1
Gestionar los Activos*	2	2
Gestionar la configuración*	2	2
Gestión de Cambio*	2	1

La encargada de Tecnologías Digitales debe alcanzar una madurez mínima de sus procesos de **2.3** para poder brindar total cumplimiento a las metas institucionales, actualmente (2025) se logra un **1,3.**
La metodología de mejora continua se logra a través del Manual de Gobernanza de TI y la implementación gradual de procesos a través de la estrategia de Gestión de Riesgos Críticos del Establecimiento y el SGSI.
*Nota: Los items marcados con (*) representan a los procesos implementados en el 2024-2025.
Con los procesos a implementar en el 2025 se espera que para inicios del 2026 se logre una madurez de 2.1 lo que es un gran avance propiciado por el COMGES 2025 asociado a la implementación de controles críticos relacionados a la Seguridad de la Información contenidos en la ISO/IEC 27002:2013.

11.10.6.3 PERFIL DEL CARGO

El perfil de la Encargada de Tecnologías actúa como líder táctico en la transformación digital del hospital, promoviendo la adopción estratégica de tecnologías innovadoras.
Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Ingeniero Civil en Informática (Preferible)
- Ingeniero en Informática
- Ingeniero Civil Industrial, Especialización en TI
- Ingeniería Comercial, Especialización TI
- Tecnólogo en Informática Biomédica

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.
MÉTODOS Y HERRAMIENTAS (METL)	Asegurarse de que se adopten y utilicen de manera efectiva los métodos y las herramientas en toda la organización.	6
GESTIÓN DE NIVEL DE SERVICIO (SLMO)	Acordar objetivos para los niveles de servicio y evaluar, supervisar y gestionar la prestación de servicios en relación con los objetivos.	5
GESTIÓN DEL CATÁLOGO DE SERVICIOS (SCMG)	Brindar una fuente de información coherente sobre los servicios y productos disponibles para clientes y usuarios.	4
GESTIÓN DE INCIDENTES (USUP)	Coordinar las respuestas a los informes de incidentes, minimizar los impactos negativos y restaurar el servicio lo más rápidamente posible.	5
GESTIÓN DE PROBLEMAS (PBMG)	Gestionar el ciclo de vida de todos los problemas que han ocurrido o que podrían ocurrir durante la prestación de un servicio.	5
CONTROL DE CAMBIOS (CHMG)	Evaluar los riesgos asociados con los cambios propuestos y garantizar el control y la coordinación de los cambios en los productos, servicios o sistemas.	5
GESTIÓN DE ACTIVOS (ASMG)	Gestionar el ciclo de vida completo de los activos desde la adquisición, operación y mantenimiento hasta su retiro del ambiente productivo.	5
ADQUISICIÓN (SORC)	Gestionar la adquisición o el encargo de productos y servicios, o brindar asesoramiento sobre ellos.	4
GESTION DE LA CONTINUIDAD (COPL)	Desarrollar, implementar y probar un marco de la continuidad del negocio	5
GESTIÓN DE RIESGOS (BURM)	Planificar e implementar procesos y procedimientos en toda la organización para la gestión de riesgos hacia el éxito o la integridad de la empresa.	3
DESARROLLO DE LAS CAPACIDADES ORGANIZATIVAS (OCDV)	Brindar liderazgo, asesoramiento y apoyo para la implementación a fin de evaluar las capacidades organizativas e identificar, priorizar e implementar mejoras.	5
DIRECCION DE PROYECTOS (PRMG)	Entrega los resultados acordados en proyectos que usan técnicas de gestión, colaboración, liderazgo y gobierno adecuadas.	4
GESTIÓN DE OFERTAS / PROPUESTAS (BIDM)	Gestionar la preparación y presentación de ofertas y propuestas de contratos, adjudicaciones, proyectos o servicios.	5
GESTIÓN DE PROVEEDORES (SUPP)	Alinear los objetivos y las actividades de los proveedores de una organización con las estrategias y los planes de abastecimiento, el equilibrio de los costos, la eficiencia y la calidad del servicio.	5
GESTIÓN DE IDENTIDAD Y ACCESO (IAMT)	Gestiona la verificación de identidad y los permisos de acceso dentro de los sistemas y entornos organizativos.	2

El nivel de responsabilidad de las habilidades expuestas pondera un **4.7 (5)/7** lo que significa que este rol proporciona orientación autorizada en su campo y trabaja bajo una dirección

amplia. Responsable de entregar resultados de trabajo significativos, desde el análisis hasta la ejecución y evaluación.
Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Trabaja bajo una dirección amplia. El trabajo es de iniciativa propia, coherente con los requisitos operativos y presupuestarios acordados para cumplir los objetivos técnicos y/o grupales asignados. Define tareas y delega el trabajo en equipos e individuos dentro de su área de responsabilidad.
INFLUENCIA	Influye en las decisiones críticas bajo su dominio. Mantiene contacto a nivel operativo que impacta en la ejecución e implementación con colegas internos y contactos externos. Tiene influencia considerable en la asignación y gestión de los recursos requeridos para entregar los proyectos.
COMPLEJIDAD	Realiza una amplia gama de actividades complejas de trabajo técnico y/o profesional, que requieren la aplicación de principios fundamentales en una gama de contextos impredecibles.
CONOCIMIENTO	Aplica conocimientos para interpretar situaciones complejas y ofrecer asesoramiento autorizado. Aplica una experiencia profunda en campos específicos, con una comprensión más amplia en toda la industria o negocio.

Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza el buen juicio para tomar decisiones informadas sobre las acciones para lograr resultados organizacionales, como el cumplimiento de metas, plazos y presupuestos. • Plantea cuestionamientos cuando los objetivos están en riesgo.
PLANIFICACIÓN	• Analiza, diseña, planifica, establece hitos y ejecuta y evalúa el trabajo según los objetivos de tiempo, costo y calidad.
COLABORACIÓN	• Facilita la colaboración entre las partes interesadas que tienen diversos objetivos. • Garantiza formas de trabajo colaborativas en todas las etapas del trabajo para satisfacer las necesidades del usuario/cliente. • Construye relaciones efectivas en toda la organización y con clientes, proveedores y socios.
RESOLUCIÓN DE PROBLEMAS	• Investiga cuestiones complejas para identificar las causas fundamentales y los impactos, evalúa una variedad de soluciones y toma decisiones informadas sobre el mejor curso de acción, a menudo en colaboración con otros expertos.
MENTALIDAD DE MEJORA	• Identifica y evalúa mejoras potenciales de productos, prácticas o servicios. • Dirige la aplicación de mejoras dentro de su propia área de responsabilidades. • Evalúa la efectividad de los cambios implementados.
CREATIVIDAD	• Aplica de manera creativa el pensamiento innovador y prácticas de diseño para identificar soluciones que le den valor en beneficio de clientes y partes interesadas.
COMUNICACIÓN	• Comunica claramente y con impacto, articulando

	información e ideas complejas para audiencias amplias con diferentes puntos de vista. • Lidera y fomenta conversaciones para compartir ideas y generar consenso sobre las medidas a tomar.
LIDERAZGO	• Proporciona liderazgo a nivel operativo. • Implementa y ejecuta políticas alineadas con los planes estratégicos. • Estima y evalúa riesgos. • Al examinar propuestas toma en cuenta todos los requisitos.
ADAPTABILIDAD	• Lidera adaptaciones a entornos empresariales cambiantes. • Guía a los equipos a través de las transiciones, manteniendo el enfoque en los objetivos organizacionales.
MENTALIDAD DIGITAL	• Reconoce y evalúa el impacto organizacional de las nuevas tecnologías y servicios digitales. • Implementa prácticas nuevas y efectivas. • Asesora sobre los estándares, métodos, herramientas, aplicaciones y procesos disponibles y relevantes para especialidades grupales, y puede tomar decisiones apropiadas a partir de las alternativas.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Contribuye de manera proactiva a la implementación de prácticas de trabajo profesionales y ayuda a promover una cultura organizacional de apoyo.

11.10.6.4 PERSONAL A CARGO DIRECTO

El rol de Encargada de Tecnologías Digitales tiene bajo su cargo el siguiente rol:

11.10.7 INGENIERO DE PROCESOS Y SERVICIOS TI

11.10.7.1 ROL

El Ingeniero de Procesos y Servicios TI, bajo la dirección de la Encargada de Tecnologías Digitales, es responsable de liderar el desarrollo, mejora e integración de sistemas y procesos tecnológicos en el hospital. Su rol es clave para optimizar estructuras de datos, implementar sistemas, coordinar iniciativas de transformación digital alineadas con las políticas del Estado, y garantizar el versionamiento y la calidad de las soluciones tecnológicas. Trabaja en colaboración con equipos internos y externos para impulsar la eficiencia operativa y la innovación digital.

a) **Desarrollar y mejorar sistemas:** Diseñar, programar y optimizar sistemas tecnológicos para satisfacer las necesidades operativas y estratégicas del hospital.
b) **Gestionar estructuras de datos**: Definir y mantener estructuras de datos robustas, asegurando su integridad, seguridad y accesibilidad para los sistemas institucionales.
c) **Coordinar integraciones de sistemas**: Implementar y gestionar integraciones entre plataformas, garantizando interoperabilidad y flujo eficiente de información.
d) **Implementar sistemas tecnológicos**: Liderar la puesta en marcha de nuevos sistemas, asegurando su correcta configuración, prueba y adopción por los usuarios.
e) **Coordinar Transformación Digital**: Apoyar iniciativas de transformación digital, alineándolas con las políticas del Estado y los objetivos institucionales, incluyendo versionamiento y documentación.

11.10.7.2 PROCESOS ASOCIADOS

Proceso	Nivel Requerido	Nivel Actual
Gestión de Riesgos	4	1
Gestionar la Continuidad*	3	1
Gestionar las peticiones y los incidentes de servicio*	2	2
Gestionar las relaciones con proveedores*	2	1
Gestionar la disponibilidad y la capacidad	2	1
Gestionar los proyectos	2	1
Gestionar los problemas*	2	1
Gestionar los Activos*	2	2
Gestionar la configuración*	2	2
Gestión de Cambio*	2	1

El Ingeniero de Procesos y Servicios TI debe alcanzar una madurez mínima de sus procesos de **2.3** para poder brindar total cumplimiento a las metas institucionales, actualmente (2025) se logra un **1,3.**
La metodología de mejora continua se logra a través del Manual de Gobernanza de TI y la implementación gradual de procesos a través de la estrategia de Gestión de Riesgos Críticos del Establecimiento y el SGSI.
*Nota: Los items marcados con (*) representan a los procesos implementados en el 2024-2025.
Con los procesos a implementar en el 2025 se espera que para inicios del 2026 se logre una madurez de 2.1 lo que es un gran avance propiciado por el COMGES 2025 asociado a la implementación de controles críticos relacionados a la Seguridad de la Información contenidos en la ISO/IEC 27002:2013.
Este Rol debería tener otros procesos importantes, sin embargo, por el momento no se encuentran priorizados en el sistema de gobernanza.
Además, este rol no está activo en la institución.

11.10.7.3 PERFIL DEL CARGO

El perfil de Ingeniero de Procesos y Servicios TI está muy ligado a la Ingeniería de Software y todo el ciclo de vida asociado al mismo.

Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Ingeniero en Informática, Senior (Preferible)
- Ingeniero Civil en Informática
- Ingeniero Civil Industrial, Especialidad TI

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.
INGENIERÍA DE DATOS (DENG)	Diseño, construcción, puesta en funcionamiento, seguridad y monitorización de canalizaciones de datos, almacenes y sistemas de procesamiento en tiempo real para una gestión de datos escalable y confiable.	4
INGENIERÍA DEL CICLO DE VIDA DE SISTEMAS Y SOFTWARE (SLEN)	Establecer y desplegar un ambiente para el desarrollo, operación segura y mejora continua de productos y servicios de sistemas y software.	4
INSTALACIÓN Y DESINTALACIÓN DE SISTEMAS (HSIN)	Instalar y probar, o desmantelar y eliminar, sistemas o componentes del sistema.	5
INTELIENCIA ARTIFICIAL (IA) Y ÉTICA DE DATOS (AIDE)	Implementar y promover prácticas éticas en el diseño, desarrollo, despliegue y uso de IA y tecnologías relacionadas con datos.	4
MODELADO Y DISEÑO DE DATOS (DTAN)	Desarrollar modelos y diagramas para representar, comunicar y gestionar los requisitos de los datos y de los activos de datos.	5
PROGRAMACIÓN/DESARROLLO DE SOFTWARE (PROG)	Desarrollar componentes de software para ofrecer valor a las partes interesadas.	5
PRUEBAS DE ACEPTACIÓN DEL USUARIO FINAL (BPTS)	Validar sistemas, productos, procesos de negocio o servicios para determinar si se han cumplido los criterios de aceptación.	3
PRUEBA DE ASPECTOS NO FUNCIONALES (NFTS)	Evaluar los sistemas y servicios para revisar el rendimiento, la seguridad, la escalabilidad y otras características no funcionales con respecto a los requisitos o a los estándares esperados.	3
PRUEBAS (TEST)	Evaluar los requisitos y características funcionales específicas o no especificadas de los productos, sistemas y servicios mediante investigación y pruebas.	3
GESTIÓN DE INCIDENTES (USUP)	Coordinar las respuestas a los informes de incidentes, minimizar los impactos negativos y restaurar el servicio lo más rápidamente posible.	5
GESTIÓN DE PROBLEMAS (PBMG)	Gestionar el ciclo de vida de todos los problemas que han ocurrido o que podrían ocurrir durante la prestación de un servicio.	5
CONTROL DE CAMBIOS (CHMG)	Evaluar los riesgos asociados con los cambios propuestos y garantizar el control y la coordinación de los cambios en los productos, servicios o sistemas.	5
GESTIÓN DE IDENTIDAD Y ACCESO (IAMT)	Gestiona la verificación de identidad y los permisos de acceso dentro de los sistemas y	3

	entornos organizativos.	

El nivel de responsabilidad de las habilidades expuestas pondera un **4.2 (4)/7** lo que significa que este rol Realiza diversas actividades complejas, apoya y guía a otros, delega tareas cuando corresponde, trabaja de forma autónoma bajo dirección general y aporta experiencia para cumplir los objetivos del equipo.
Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Trabaja bajo dirección general dentro de un claro marco de rendición de cuentas. Ejerce una considerable responsabilidad personal y autonomía. Cuando es necesario, planifica, programa y delega el trabajo en otros, normalmente dentro del propio equipo.
INFLUENCIA	Influye en los proyectos y en los objetivos del equipo. Tiene un nivel táctico de contacto con personas ajenas a su equipo, incluidos colegas internos y contactos externos.
COMPLEJIDAD	El trabajo incluye una amplia gama de actividades técnicas o profesionales complejas en diversos contextos.
CONOCIMIENTO	Aplica el conocimiento en diferentes áreas en su campo, integrando este conocimiento para realizar tareas complejas y diversas. Aplica un conocimiento práctico del dominio de la organización.

Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza su criterio y una discreción sustancial para identificar y responder a problemas complejos y tareas relacionadas con proyectos y objetivos del equipo. • Escala cuando el alcance se ve afectado.
PLANIFICACIÓN	• Planifica, programa y supervisa el trabajo para cumplir determinados objetivos y procesos personales y/o de equipo, demostrando un enfoque analítico para cumplir alcanzar los objetivos de tiempo y calidad.
COLABORACIÓN	• Facilita la colaboración entre partes interesadas que comparten objetivos comunes. • Colabora con los equipos interfuncionales y contribuye en ellos para garantizar que se satisfagan las necesidades de los usuarios y clientes en todo el producto a entregar y el alcance de su labor.
RESOLUCIÓN DE PROBLEMAS	• Investiga la causa y el impacto, evalúa las opciones y resuelve una amplia gama de problemas complejos.
MENTALIDAD DE MEJORA	• Alienta y apoya los debates en equipo sobre iniciativas de mejora. • Implementa cambios de procedimiento dentro de un ámbito definido de trabajo.
CREATIVIDAD	• Aplica, facilita y desarrolla conceptos de pensamiento creativo y encuentra formas alternativas de enfocar los resultados del equipo.
COMUNICACIÓN	• Se comunica tanto con audiencias técnicas como no técnicas, incluidos el equipo y las partes interesadas dentro y fuera de la organización. • Según sea necesario, toma la iniciativa en la explicación de conceptos complejos para apoyar la toma de decisiones. • Escucha y hace preguntas perspicaces para identificar diferentes perspectivas a fin de aclarar y confirmar la comprensión.

LIDERAZGO	• Dirige, apoya o guía a los miembros del equipo. • Desarrolla soluciones para actividades laborales complejas relacionadas con asignaciones. • Demuestra una comprensión de los factores de riesgo en su trabajo. • Contribuye con conocimientos especializados a la definición de requisitos para respaldar propuestas.
ADAPTABILIDAD	• Permite a otros adaptarse y cambiar en respuesta a los desafíos y cambios en el entorno de trabajo.
MENTALIDAD DIGITAL	• Maximiza las capacidades de las aplicaciones para su función, y evalúa y soporta el uso de nuevas tecnologías y herramientas digitales. • Selecciona adecuadamente y evalúa el impacto de los cambios en los estándares, métodos, herramientas, aplicaciones y procesos aplicables y relevantes para la propia especialidad.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Adapta y aplica las normas aplicables, reconociendo su importancia en la consecución de resultados en equipo.

11.10.7.4 PERSONAL A CARGO DIRECTO

El rol no presenta personal a cargo directo por una definición de estructura organizativa.

11.10.8 COORDINADOR DE TRANSFORMACIÓN DIGITAL

11.10.8.1 ROL

El Coordinador de Transformación Digital es el responsable de liderar, articular y supervisar la implementación de la estrategia de transformación digital institucional, asegurando el cumplimiento de la Ley N°21.180 sobre Transformación Digital del Estado, sus reglamentos asociados y demás lineamientos técnicos emitidos por la autoridad competente. Este rol tiene como propósito garantizar la digitalización progresiva de los procedimientos administrativos, la interoperabilidad entre organismos, la adecuada gestión documental electrónica y la adopción de capacidades digitales institucionales orientadas a la eficiencia, trazabilidad y calidad de los servicios públicos.

El rol abarca la coordinación transversal entre áreas técnicas, administrativas y directivas para asegurar la correcta implementación de iniciativas digitales alineadas con los objetivos estratégicos institucionales y las exigencias normativas del Estado Digital.

a) **Gestión del Cumplimiento Normativo Digital**: Asegurar el cumplimiento de la Ley N°21.180 y sus normativas complementarias, promoviendo la correcta implementación de procedimientos administrativos electrónicos, expediente electrónico, interoperabilidad y notificaciones digitales.
b) **Coordinación de la Transformación Digital Institucional**: Liderar y coordinar iniciativas de modernización digital, promoviendo la adopción de tecnologías y procesos digitales que permitan optimizar la gestión institucional y la experiencia usuaria.
c) **Gestión de Interoperabilidad y Gobierno Digital**: Coordinar la integración e interoperabilidad de sistemas institucionales con plataformas y servicios digitales del Estado, asegurando estándares técnicos, trazabilidad y continuidad operacional.
d) **Gestión del Cambio Organizacional**: Impulsar estrategias de adopción digital, fortalecimiento de capacidades institucionales y acompañamiento al cambio organizacional derivado de la implementación de tecnologías y procesos digitales.
e) **Gestión de Riesgos y Continuidad Digital**: Identificar y gestionar riesgos asociados a los procesos de transformación digital, asegurando la continuidad operativa, la disponibilidad de servicios digitales y la adecuada gestión documental electrónica.
f) **Articulación Estratégica**: Colaborar con la dirección institucional y las distintas áreas del establecimiento para alinear la transformación digital con los objetivos estratégicos, regulatorios y operacionales de la organización.

11.10.8.2 PROCESOS ASOCIADOS

Proceso	Nivel Requerido	Nivel Actual
BAI02 – Gestionar la Definición de Requisitos	3	1
BAI06 – Gestionar los cambios de TI	3	1
BAI07 – Gestionar la Aceptación y Transición Cambios TI	2	1
EDM05 – Asegurar el compromiso de las partes interesadas	2	1
MEA03 – Gestionar el cumplimiento de los requisitos externos	3	1
BAI11 – Gestionar los Proyectos	3	2
BAI03 – Gestionar la Identificación y Construcción de Soluciones	3	1

La Coordinación de Transformación Digital debe alcanzar una madurez mínima de sus procesos de 2,7 para asegurar el cumplimiento de la Ley N°21.180 y la correcta digitalización de los procedimientos institucionales. Actualmente (2025) se alcanza un nivel de madurez de 1,14. La mejora continua se desarrollará mediante el fortalecimiento del Modelo de Gobernanza Digital institucional, la gestión de riesgos críticos y la implementación gradual de capacidades digitales interoperables.

*Nota: Los ítems marcados con (*) representan procesos implementados entre 2024-2025.
Si bien la Coordinación de Transformación Digital puede utilizar otros procesos establecidos en la Gobernanza de TI institucional, en este manual se declaran los procesos mínimos requeridos para asegurar claridad organizacional y cumplimiento normativo.

11.10.8.3 PERFIL DEL CARGO

El perfil del cargo de Coordinador de Transformación Digital del Hospital de Tomé está asociado a liderar y coordinar estratégicamente la implementación de capacidades digitales institucionales, asegurando el cumplimiento regulatorio asociado a la digitalización del Estado y promoviendo la modernización de los procesos organizacionales mediante tecnologías digitales y modelos de gestión orientados a la eficiencia, trazabilidad y calidad de servicio.

Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Ingeniero Civil en Informática, Senior (Preferible)
- Ingeniero en Informática, Senior Salud
- Ingeniero Civil Industrial, Senior (Experiencia en Salud / Especialización Transformación Digital)
- Administrador Público con especialización en Gobierno Digital (Senior)

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.
Análisis de la Situación Empresarial BUSA	Investigar las situaciones del negocio para definir recomendaciones a fin de tomar medidas que permitan mejorar.	6
Gestión y definición de requerimientos REQM	Gestión de los requerimientos durante todo el ciclo de vida operativo y de entrega.	5
Modelado y diseño de datos DTAN	Desarrollar modelos y diagramas para representar, comunicar y gestionar los requisitos de los datos y de los activos de datos.	3
Mejora de procesos de negocio BPRE	Crear enfoques nuevos y potencialmente disruptivos para llevar a cabo actividades comerciales.	4
Gestión del cambio organizativo CIPM	Planificar, diseñar e implementar actividades para la transición de la organización y las personas al estado futuro requerido.	3
Control de cambios CHMG	Evaluar los riesgos asociados con los cambios propuestos y garantizar el control y la coordinación de los cambios en los productos, servicios o sistemas.	4
Gestión de las relaciones con las partes interesadas RLMT	Analizar, gestionar e influir sistemáticamente en las relaciones con las partes interesadas para lograr resultados mutuamente beneficiosos mediante un compromiso estructurado.	5
Evaluación de inversiones	Evaluar el atractivo de posibles inversiones o	4

INVA	proyectos.	
Dirección de proyectos PRMG	Lograr los resultados acordados del proyecto alineando las técnicas de gestión, colaboración, liderazgo y gobernanza adecuadas con los contextos específicos del proyecto y la organización.	4

El nivel de responsabilidad de las habilidades expuestas pondera un 4.2/7, lo que significa que este rol posee una influencia organizacional relevante, coordina iniciativas estratégicas transversales, promueve el cumplimiento regulatorio y facilita la adopción institucional de capacidades digitales.

Realiza diversas actividades complejas, apoya y guía a otros, delega tareas cuando corresponde, trabaja de forma autónoma bajo dirección general y aporta experiencia para cumplir los objetivos del equipo.

Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Trabaja bajo dirección general dentro de un claro marco de rendición de cuentas. Ejerce una considerable responsabilidad personal y autonomía. Cuando es necesario, planifica, programa y delega el trabajo en otros, normalmente dentro del propio equipo.
INFLUENCIA	Influye en los proyectos y en los objetivos del equipo. Tiene un nivel táctico de contacto con personas ajenas a su equipo, incluidos colegas internos y contactos externos.
COMPLEJIDAD	El trabajo incluye una amplia gama de actividades técnicas o profesionales complejas en diversos contextos.
CONOCIMIENTO	Aplica el conocimiento en diferentes áreas en su campo, integrando este conocimiento para realizar tareas complejas y diversas. Aplica un conocimiento práctico del dominio de la organización.

Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza su criterio y una discreción sustancial para identificar y responder a problemas complejos y tareas relacionadas con proyectos y objetivos del equipo. • Escala cuando el alcance se ve afectado.
PLANIFICACIÓN	• Planifica, programa y supervisa el trabajo para cumplir determinados objetivos y procesos personales y/o de equipo, demostrando un enfoque analítico para cumplir alcanzar los objetivos de tiempo y calidad.
COLABORACIÓN	• Planifica, programa y supervisa el trabajo para cumplir determinados objetivos y procesos personales y/o de equipo, demostrando un enfoque analítico para cumplir alcanzar los objetivos de tiempo y calidad.
RESOLUCIÓN DE PROBLEMAS	• Investiga la causa y el impacto, evalúa las opciones y resuelve una amplia gama de problemas complejos.
MENTALIDAD DE MEJORA	• Alienta y apoya los debates en equipo sobre iniciativas de mejora. • Implementa cambios de procedimiento dentro de un ámbito definido de trabajo.
CREATIVIDAD	• Aplica, facilita y desarrolla conceptos de pensamiento creativo y encuentra formas alternativas de enfocar los resultados del equipo.
COMUNICACIÓN	• Se comunica tanto con audiencias técnicas como no

	técnicas, incluidos el equipo y las partes interesadas dentro y fuera de la organización. • Según sea necesario, toma la iniciativa en la explicación de conceptos complejos para apoyar la toma de decisiones. • Escucha y hace preguntas perspicaces para identificar diferentes perspectivas a fin de aclarar y confirmar la comprensión.
LIDERAZGO	• Dirige, apoya o guía a los miembros del equipo. • Desarrolla soluciones para actividades laborales complejas relacionadas con asignaciones. • Demuestra una comprensión de los factores de riesgo en su trabajo. • Contribuye con conocimientos especializados a la definición de requisitos para respaldar propuestas.
ADAPTABILIDAD	• Permite a otros adaptarse y cambiar en respuesta a los desafíos y cambios en el entorno de trabajo.
MENTALIDAD DIGITAL	• Maximiza las capacidades de las aplicaciones para su función, y evalúa y soporta el uso de nuevas tecnologías y herramientas digitales. • Selecciona adecuadamente y evalúa el impacto de los cambios en los estándares, métodos, herramientas, aplicaciones y procesos aplicables y relevantes para la propia especialidad.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Adapta y aplica las normas aplicables, reconociendo su importancia en la consecución de resultados en equipo.

11.10.8.4 PERSONAL A CARGO DIRECTO

El rol no presenta personal a cargo directo por una definición de estructura organizativa.

11.10.9 ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN

11.10.9.1 ROL

El Encargado de Seguridad de la Información lidera la gestión y protección de los activos digitales del hospital, asegurando la integridad, confidencialidad y disponibilidad de la información institucional y personal. Su rol es crucial para asesorar, implementar y monitorear políticas de ciberseguridad, cumpliendo con normativas como las leyes Nº19.628, Nº20.584 y Nº19.223. Coordina estrategias de prevención, mitigación y respuesta a emergencias, promoviendo un entorno seguro para la continuidad de los servicios tecnológicos.

a) **Asesorar en ciberseguridad:** Proporcionar orientación técnica y estratégica para proteger los sistemas y datos institucionales frente a amenazas digitales.
b) **Gestionar políticas de seguridad**: Implementar y supervisar el cumplimiento de políticas de ciberseguridad, alineadas con normativas legales y estándares institucionales.
c) **Monitorear integridad de redes**: Supervisar el rendimiento y seguridad de las redes, identificando vulnerabilidades y aplicando medidas preventivas.
d) **Coordinar respuesta a incidentes de Seguridad**: Liderar la mitigación y gestión de emergencias de seguridad, minimizando impactos y asegurando la continuidad operativa.
e) **Gestionar mejoras en seguridad**: Evaluar, proponer y coordinar la adquisición de herramientas y soluciones para fortalecer la infraestructura de ciberseguridad.

11.10.9.2 PROCESOS ASOCIADOS

Proceso	Nivel Requerido	Nivel Actual
Gestión de Riesgos	4	1
Gestionar las peticiones y los incidentes de servicio*	2	2
Gestionar los problemas*	2	1
Gestionar la Seguridad	4	4
Gestión de Cambio*	2	1

El Encargado de Seguridad de la Información debe alcanzar una madurez mínima de sus procesos de **2.3** para poder brindar total cumplimiento a las metas institucionales, actualmente (2025) se logra un **1,8.**
La metodología de mejora continua se logra a través del Manual de Gobernanza de TI y la implementación gradual de procesos a través de la estrategia de Gestión de Riesgos Críticos del Establecimiento y el SGSI.
*Nota: Los items marcados con (*) representan a los procesos implementados en el 2024-2025.
Con los procesos a implementar en el 2025 se espera que para inicios del 2026 se logre una madurez de 2.2 lo que es un gran avance propiciado por el COMGES 2025 asociado a la implementación de controles críticos relacionados a la Seguridad de la Información contenidos en la ISO/IEC 27002:2013.

11.10.9.3 PERFIL DEL CARGO

El perfil de Ingeniero de Procesos y Servicios TI está muy ligado a la Ingeniería de Software y todo el ciclo de vida asociado al mismo.
Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Ingeniero Civil en Informática, Especialización en Seguridad (Preferible)
- Ingeniero en Informática, Especialización en Seguridad
- Ingeniero en Telecomunicaciones, Especialización en Seguridad
- Ingeniero en Ciberseguridad (Senior)

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.

ASESORAMIENTO ESPECIALIZADO (TECH)	Proporcionar asesoramiento y orientación autorizados en un área especializada.	6
AUDITAR (AUDT)	Brindar evaluaciones independientes basadas en riesgos de la eficacia de los procesos, los controles y el entorno de cumplimiento de una organización.	5
SEGURIDAD DE LA INFORMACIÓN (SCTY)	Definir y operar un marco de controles de seguridad y estrategias de gestión de seguridad.	6

El nivel de responsabilidad de las habilidades expuestas pondera un **5,6 (5)/7** lo que significa que este rol proporciona orientación autorizada en su campo y trabaja bajo una dirección amplia. Responsable de entregar resultados de trabajo significativos, desde el análisis hasta la ejecución y evaluación.
Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Trabaja bajo una dirección amplia. El trabajo es de iniciativa propia, coherente con los requisitos operativos y presupuestarios acordados para cumplir los objetivos técnicos y/o grupales asignados. Define tareas y delega el trabajo en equipos e individuos dentro de su área de responsabilidad.
INFLUENCIA	Influye en las decisiones críticas bajo su dominio. Mantiene contacto a nivel operativo que impacta en la ejecución e implementación con colegas internos y contactos externos. Tiene influencia considerable en la asignación y gestión de los recursos requeridos para entregar los proyectos.
COMPLEJIDAD	Realiza una amplia gama de actividades complejas de trabajo técnico y/o profesional, que requieren la aplicación de principios fundamentales en una gama de contextos impredecibles.
CONOCIMIENTO	Aplica conocimientos para interpretar situaciones complejas y ofrecer asesoramiento autorizado. Aplica una experiencia profunda en campos específicos, con una comprensión más amplia en toda la industria o negocio.

Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza el buen juicio para tomar decisiones informadas sobre las acciones para lograr resultados organizacionales, como el cumplimiento de metas, plazos y presupuestos. • Plantea cuestionamientos cuando los objetivos están en riesgo.
PLANIFICACIÓN	• Analiza, diseña, planifica, establece hitos y ejecuta y evalúa el trabajo según los objetivos de tiempo, costo y calidad.
COLABORACIÓN	• Facilita la colaboración entre las partes interesadas que tienen diversos objetivos. • Garantiza formas de trabajo colaborativas en todas las etapas del trabajo para satisfacer las necesidades del usuario/cliente. • Construye relaciones efectivas en toda la organización y con clientes, proveedores y socios.
RESOLUCIÓN DE PROBLEMAS	• Investiga cuestiones complejas para identificar las causas fundamentales y los impactos, evalúa una variedad de soluciones y toma decisiones informadas sobre el mejor curso de acción, a menudo en colaboración con otros expertos.

MENTALIDAD DE MEJORA	• Identifica y evalúa mejoras potenciales de productos, prácticas o servicios. • Dirige la aplicación de mejoras dentro de su propia área de responsabilidades. • Evalúa la efectividad de los cambios implementados.
CREATIVIDAD	• Aplica de manera creativa el pensamiento innovador y prácticas de diseño para identificar soluciones que le den valor en beneficio de clientes y partes interesadas.
COMUNICACIÓN	• Comunica claramente y con impacto, articulando información e ideas complejas para audiencias amplias con diferentes puntos de vista. • Lidera y fomenta conversaciones para compartir ideas y generar consenso sobre las medidas a tomar.
LIDERAZGO	• Proporciona liderazgo a nivel operativo. • Implementa y ejecuta políticas alineadas con los planes estratégicos. • Estima y evalúa riesgos. • Al examinar propuestas toma en cuenta todos los requisitos.
ADAPTABILIDAD	• Lidera adaptaciones a entornos empresariales cambiantes. • Guía a los equipos a través de las transiciones, manteniendo el enfoque en los objetivos organizacionales.
MENTALIDAD DIGITAL	• Reconoce y evalúa el impacto organizacional de las nuevas tecnologías y servicios digitales. • Implementa prácticas nuevas y efectivas. • Asesora sobre los estándares, métodos, herramientas, aplicaciones y procesos disponibles y relevantes para especialidades grupales, y puede tomar decisiones apropiadas a partir de las alternativas.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Contribuye de manera proactiva a la implementación de prácticas de trabajo profesionales y ayuda a promover una cultura organizacional de apoyo.

11.10.9.4 PERSONAL A CARGO DIRECTO

El rol no presenta personal a cargo directo por una definición de estructura organizativa.

11.10.10 ENCARGADO DE CIBERSEGURIDAD

11.10.10.1 ROL

El Encargado de Ciberseguridad, orientado a liderar el Centro de Operaciones de Seguridad (SOC), es responsable de monitorear, detectar, responder y prevenir amenazas cibernéticas en tiempo real para proteger los activos digitales del hospital. Su rol es crítico para garantizar la seguridad de la información institucional y personal, cumpliendo con normativas como las leyes Nº19.628, Nº20.584 y Nº19.223. Coordina análisis de incidentes, respuesta rápida y mejora continua de las defensas tecnológicas, asegurando la continuidad operativa en un entorno seguro.

a) **Monitoreo amenazas en tiempo real:** Supervisar continuamente los sistemas y redes mediante herramientas del SOC para detectar actividades sospechosas o ciberataques.
b) **Gestionar respuesta a incidentes**: Coordinar la investigación, contención y mitigación de incidentes de seguridad, minimizando impactos y restaurando la operatividad.
c) **Analizar y prevenir amenazas**: Realizar análisis de inteligencia de amenazas para identificar vulnerabilidades y aplicar medidas preventivas proactivas.
d) **Implementar herramientas de seguridad**: Configurar y mantener tecnologías de ciberseguridad, como SIEM, firewalls y sistemas de detección de intrusos, para fortalecer las defensas.
e) **Liderar el SOC**: Ejecutar técnicas de ciberseguridad y coordinar sus esfuerzos para garantizar una respuesta efectiva y alineada con los objetivos institucionales.

11.10.10.2PROCESOS ASOCIADOS

Proceso	Nivel Requerido	Nivel Actual
Gestión de Riesgos	4	1
Gestionar las peticiones y los incidentes de servicio*	2	2
Gestionar los problemas*	2	1
Gestión de Cambio*	2	1

El Encargado de Ciberseguridad debe alcanzar una madurez mínima de sus procesos de **2.5** para poder brindar total cumplimiento a las metas institucionales, actualmente (2025) se logra un **1,25.**
La metodología de mejora continua se logra a través del Manual de Gobernanza de TI y la implementación gradual de procesos a través de la estrategia de Gestión de Riesgos Críticos del Establecimiento y el SGSI.
*Nota: Los items marcados con (*) representan a los procesos implementados en el 2024-2025.
Con los procesos a implementar en el 2025 se espera que para inicios del 2026 se logre una madurez de 1,75 lo que es un gran avance propiciado por el COMGES 2025 asociado a la implementación de controles críticos relacionados a la Seguridad de la Información contenidos en la ISO/IEC 27002:2013.
Sin embargo, este rol no esta activo en la institución.

11.10.10.3PERFIL DEL CARGO

El perfil de Ingeniero de Procesos y Servicios TI está muy ligado a la Ingeniería de Software y todo el ciclo de vida asociado al mismo.
Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Ingeniero en Informática, Especialización en Ciberseguridad (Preferible)
- Ingeniero en Ciberseguridad (Senior)
- Ingeniero en Telecomunicaciones, Especialización en Seguridad
- Ingeniero Civil en Informática, Especialización en Seguridad

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.
ASESORAMIENTO ESPECIALIZADO (TECH)	Proporcionar asesoramiento y orientación autorizados en un área especializada.	6
AUDITAR (AUDT)	Brindar evaluaciones independientes basadas en riesgos de la eficacia de los procesos, los controles y el entorno de cumplimiento de una organización.	3
EVALUACIÓN DE VULNERABILIDADES (VUAS)	Identificar y clasificar vulnerabilidades de seguridad en redes, sistemas y aplicaciones, y mitigar o eliminar su impacto.	5
INVESTIGACIÓN DE DELITOS CIBERNETICOS (CRIM)	Investiga ciberdelitos, recopila evidencia, determina los impactos de los incidentes y colabora con los equipos legales para proteger los activos digitales.	3
INVESTIGACIÓN DE VULNERABILIDADES (VURE)	Realizar una investigación aplicada para descubrir, evaluar y mitigar vulnerabilidades y debilidades de seguridad nuevas o desconocidas.	3
PRUEBAS DE PENETRACIÓN (PENT)	Probar la efectividad de los controles de seguridad emulando las herramientas y técnicas de probables atacantes.	3
OPERACIONES DE SEGURIDAD (SCAD)	Gestiona y administra las medidas de seguridad, utilizando herramientas e inteligencia para proteger los activos, garantizando el cumplimiento y la integridad operativa.	4
GESTIÓN DE INCIDENTES (USUP)	Coordinar las respuestas a los informes de incidentes, minimizar los impactos negativos y restaurar el servicio lo más rápidamente posible.	5
GESTIÓN DE PROBLEMAS (PBMG)	Gestionar el ciclo de vida de todos los problemas que han ocurrido o que podrían ocurrir durante la prestación de un servicio.	5
CONTROL DE CAMBIOS (CHMG)	Evaluar los riesgos asociados con los cambios propuestos y garantizar el control y la coordinación de los cambios en los productos, servicios o sistemas.	5

El nivel de responsabilidad de las habilidades expuestas pondera un **4,2 (4)/7** lo que significa que este rol Realiza diversas actividades complejas, apoya y guía a otros, delega tareas cuando corresponde, trabaja de forma autónoma bajo dirección general y aporta experiencia para cumplir los objetivos del equipo.
Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Trabaja bajo dirección general dentro de un claro marco de rendición de cuentas. Ejerce una considerable responsabilidad personal y autonomía. Cuando es necesario, planifica, programa y delega el trabajo en otros, normalmente dentro del propio equipo.
INFLUENCIA	Influye en los proyectos y en los objetivos del equipo. Tiene un nivel táctico de contacto con personas ajenas a su equipo, incluidos colegas internos y contactos externos.
COMPLEJIDAD	El trabajo incluye una amplia gama de actividades técnicas o profesionales complejas en diversos contextos.
CONOCIMIENTO	Aplica el conocimiento en diferentes áreas en su campo, integrando este conocimiento para realizar tareas complejas y diversas. Aplica un conocimiento práctico del dominio de la organización.

Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza su criterio y una discreción sustancial para identificar y responder a problemas complejos y tareas relacionadas con proyectos y objetivos del equipo. • Escala cuando el alcance se ve afectado.
PLANIFICACIÓN	• Planifica, programa y supervisa el trabajo para cumplir determinados objetivos y procesos personales y/o de equipo, demostrando un enfoque analítico para cumplir alcanzar los objetivos de tiempo y calidad.
COLABORACIÓN	• Facilita la colaboración entre partes interesadas que comparten objetivos comunes. • Colabora con los equipos interfuncionales y contribuye en ellos para garantizar que se satisfagan las necesidades de los usuarios y clientes en todo el producto a entregar y el alcance de su labor.
RESOLUCIÓN DE PROBLEMAS	• Investiga la causa y el impacto, evalúa las opciones y resuelve una amplia gama de problemas complejos.
MENTALIDAD DE MEJORA	• Alienta y apoya los debates en equipo sobre iniciativas de mejora. • Implementa cambios de procedimiento dentro de un ámbito definido de trabajo.
CREATIVIDAD	• Aplica, facilita y desarrolla conceptos de pensamiento creativo y encuentra formas alternativas de enfocar los resultados del equipo.
COMUNICACIÓN	• Se comunica tanto con audiencias técnicas como no técnicas, incluidos el equipo y las partes interesadas dentro y fuera de la organización. • Según sea necesario, toma la iniciativa en la explicación de conceptos complejos para apoyar la toma de decisiones. • Escucha y hace preguntas perspicaces para identificar diferentes perspectivas a fin de aclarar y confirmar la comprensión.
LIDERAZGO	• Dirige, apoya o guía a los miembros del equipo. • Desarrolla soluciones para actividades laborales complejas relacionadas con asignaciones. • Demuestra una comprensión de los factores de riesgo en su trabajo. • Contribuye con conocimientos especializados a la definición de requisitos para respaldar propuestas.
ADAPTABILIDAD	• Permite a otros adaptarse y cambiar en respuesta a los desafíos y cambios en el entorno de trabajo.
MENTALIDAD DIGITAL	• Maximiza las capacidades de las aplicaciones para su función, y evalúa y soporta el uso de nuevas tecnologías y herramientas digitales. • Selecciona adecuadamente y evalúa el impacto de los cambios en los estándares, métodos, herramientas, aplicaciones y procesos aplicables y relevantes para la propia especialidad.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Adapta y aplica las normas aplicables, reconociendo su importancia en la consecución de resultados en equipo.

11.10.10.4 PERSONAL A CARGO DIRECTO

El rol no presenta personal a cargo directo por una definición de estructura organizativa.

11.10.11 DELEGADO DE PROTECCIÓN DE DATOS PERSONALES

11.10.11.1 ROL

El Delegado de Protección de Datos Personales (DPO) es el responsable de supervisar, asesorar y promover el cumplimiento institucional de la normativa vigente en materia de protección de datos personales, privacidad y tratamiento lícito de información, conforme a la Ley N°21.719 y demás regulaciones aplicables. Su propósito es asegurar que la organización implemente medidas técnicas, organizacionales y de gobernanza que resguarden los derechos y libertades de los titulares de datos personales, especialmente respecto de información sensible y datos de salud.

Este rol actúa con independencia técnica y funcional, asesorando a la dirección institucional, áreas operativas y responsables de tratamiento de datos respecto de riesgos, obligaciones regulatorias y buenas prácticas asociadas al tratamiento de datos personales.

El rol abarca la supervisión del cumplimiento normativo, la promoción de una cultura institucional de privacidad, la gestión de riesgos asociados al tratamiento de datos personales y la coordinación con organismos reguladores y partes interesadas.

a) **Supervisión del Cumplimiento Normativo**: Supervisar el cumplimiento institucional de la Ley N°21.719, reglamentos asociados y demás disposiciones relacionadas con privacidad, protección de datos personales y tratamiento de información sensible.
b) **Asesoría en Protección de Datos**: Asesorar a la dirección y a las distintas áreas institucionales respecto de obligaciones legales, riesgos, principios de privacidad y medidas de cumplimiento relacionadas con el tratamiento de datos personales.
c) **Gestión de Riesgos de Privacidad**: Identificar, evaluar y supervisar riesgos asociados al tratamiento de datos personales, promoviendo medidas preventivas y correctivas para resguardar los derechos de los titulares.
d) **Gestión de Incidentes de Privacidad y Seguridad**: Coordinar la gestión y análisis de incidentes relacionados con vulneraciones de datos personales, apoyando la implementación de medidas de mitigación y cumplimiento regulatorio.
e) **Promoción de Cultura de Privacidad**: Impulsar iniciativas de capacitación, concientización y fortalecimiento institucional en materias de privacidad, confidencialidad y tratamiento responsable de datos personales.
f) **Supervisión de Evaluaciones de Impacto**: Promover y supervisar la realización de evaluaciones de impacto en privacidad cuando corresponda, especialmente respecto de tratamientos de alto riesgo o datos sensibles.
g) **Relación con Autoridades y Titulares**: Actuar como punto de contacto institucional ante autoridades regulatorias y titulares de datos personales en materias relacionadas con privacidad y protección de datos.

11.10.11.2 PROCESOS ASOCIADOS

Proceso	Nivel Requerido	Nivel Actual
MEA03 - Gestionar el cumplimiento de los requisitos externos	3	1
MEA04 - Gestionar el aseguramiento	2	1
APO13 - Gestionar la seguridad de la información	3	3
EDM05 - Asegurar el compromiso de las partes interesadas*	3	2

El Delegado de Protección de Datos Personales debe alcanzar una madurez mínima de sus procesos de 2.75 para asegurar el cumplimiento regulatorio, la adecuada gestión de riesgos de privacidad y la protección efectiva de los datos personales tratados por la institución. Actualmente (2026) se alcanza un nivel de madurez de 1,75. La mejora continua se desarrollará mediante el fortalecimiento del Modelo de Gobernanza de Datos, la implementación progresiva

de controles organizacionales y la integración de la privacidad dentro de la gestión institucional de riesgos.

*Nota: Los ítems marcados con (*) representan procesos implementados entre 2024-2025.
Si bien el Delegado de Protección de Datos Personales puede utilizar otros procesos establecidos en la Gobernanza de TI y Seguridad de la Información institucional, en este manual se declaran los procesos mínimos necesarios para asegurar claridad organizacional y cumplimiento normativo.

11.10.11.3 PERFIL DEL CARGO

El perfil del cargo de Delegado de Protección de Datos Personales del Hospital de Tomé está asociado a supervisar y asesorar estratégicamente a la organización en materias de privacidad, protección de datos personales y cumplimiento regulatorio, promoviendo una cultura institucional orientada al tratamiento responsable, seguro y ético de la información.

Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Abogado con especialización en Protección de Datos y Derecho Digital
- Administrador Público, Senior con Especialidad en Seguridad de la Información o Privacidad de la Información
- Ingeniero Civil Industrial, Especialización en Gestión de Riesgos o Compliance
- Ingeniero Civil en Informática, Especialización en Seguridad o Privacidad
- Ingeniero en Ciberseguridad (Senior)

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.
Gobernanza (GOVN)	Definir y operar marcos para el apoyo de la toma de decisiones, gestión de riesgos, relaciones con las partes interesadas y el cumplimiento de las obligaciones organizativas y regulatorias.	7
Aseguramiento de la Información (INAS)	Proteger y gestionar los riesgos relacionados con el uso, el almacenamiento y la transmisión de datos y sistemas de información.	6
Gestión de Riesgos (BURM)	Planificación e implementación de procesos de gestión de riesgos en toda la empresa, alineados con la estrategia organizativa y los marcos de gobernanza.	5
Información y cumplimiento de datos PEDP	Implementar y promover el cumplimiento de las legislaciones sobre la gestión de la información y los datos.	6
Gestión de Seguridad de la Información (SCTY)	Definir y operar un marco de controles de seguridad y estrategias de gestión de seguridad.	6
Auditoría (AUDT)	Brindar evaluaciones independientes basadas en los riesgos y la efectividad de los procesos, los controles y el entorno de cumplimiento de una organización.	7
Gestión de Relaciones con Partes Interesadas (RLMT)	Analizar, gestionar e influir sistemáticamente en las relaciones con las partes interesadas para lograr resultados mutuamente beneficiosos mediante un compromiso estructurado.	4
Gestión del Cambio	Planificar, diseñar e implementar actividades	3

Organizacional (CIPM)	para la transición de la organización y las personas al estado futuro requerido.	
Análisis de la Situación Institucional (BUSA)	Investigar las situaciones del negocio para definir recomendaciones a fin de tomar medidas que permitan mejorar.	4
Educación y Desarrollo (ETDL)	Transferir conocimientos, desarrollar habilidades y cambiar comportamientos utilizando una variedad de técnicas, recursos y medios.	3

El nivel de responsabilidad de las habilidades expuestas pondera un 5.1/7, lo que significa que este rol posee una influencia organizacional relevante, participa en decisiones regulatorias y estratégicas relacionadas con privacidad y mantiene una función de supervisión y asesoría transversal dentro de la organización.

Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Trabaja bajo una dirección amplia. El trabajo es de iniciativa propia, coherente con los requisitos operativos y presupuestarios acordados para cumplir los objetivos técnicos y/o grupales asignados. Define tareas y delega el trabajo en equipos e individuos dentro de su área de responsabilidad.
INFLUENCIA	Influye en las decisiones críticas bajo su dominio. Mantiene contacto a nivel operativo que impacta en la ejecución e implementación con colegas internos y contactos externos. Tiene influencia considerable en la asignación y gestión de los recursos requeridos para entregar los proyectos.
COMPLEJIDAD	Realiza una amplia gama de actividades complejas de trabajo técnico y/o profesional, que requieren la aplicación de principios fundamentales en una gama de contextos impredecibles.
CONOCIMIENTO	Aplica conocimientos para interpretar situaciones complejas y ofrecer asesoramiento autorizado. Aplica una experiencia profunda en campos específicos, con una comprensión más amplia en toda la industria o negocio.

Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza el buen juicio para tomar decisiones informadas sobre las acciones para lograr resultados organizacionales, como el cumplimiento de metas, plazos y presupuestos. • Plantea cuestionamientos cuando los objetivos están en riesgo.
PLANIFICACIÓN	• Analiza, diseña, planifica, establece hitos y ejecuta y evalúa el trabajo según los objetivos de tiempo, costo y calidad.
COLABORACIÓN	• Facilita la colaboración entre las partes interesadas que tienen diversos objetivos. • Garantiza formas de trabajo colaborativas en todas las etapas del trabajo para satisfacer las necesidades del usuario/cliente. • Construye relaciones efectivas en toda la organización y con clientes, proveedores y socios.
RESOLUCIÓN DE PROBLEMAS	• Investiga cuestiones complejas para identificar las causas fundamentales y los impactos, evalúa una variedad de soluciones y toma decisiones informadas

	sobre el mejor curso de acción, a menudo en colaboración con otros expertos.
MENTALIDAD DE MEJORA	• Identifica y evalúa mejoras potenciales de productos, prácticas o servicios. • Dirige la aplicación de mejoras dentro de su propia área de responsabilidades. • Evalúa la efectividad de los cambios implementados.
CREATIVIDAD	• Aplica de manera creativa el pensamiento innovador y prácticas de diseño para identificar soluciones que le den valor en beneficio de clientes y partes interesadas.
COMUNICACIÓN	• Comunica claramente y con impacto, articulando información e ideas complejas para audiencias amplias con diferentes puntos de vista. • Lidera y fomenta conversaciones para compartir ideas y generar consenso sobre las medidas a tomar.
LIDERAZGO	• Proporciona liderazgo a nivel operativo. • Implementa y ejecuta políticas alineadas con los planes estratégicos. • Estima y evalúa riesgos. • Al examinar propuestas toma en cuenta todos los requisitos.
ADAPTABILIDAD	• Lidera adaptaciones a entornos empresariales cambiantes. • Guía a los equipos a través de las transiciones, manteniendo el enfoque en los objetivos organizacionales.
MENTALIDAD DIGITAL	• Reconoce y evalúa el impacto organizacional de las nuevas tecnologías y servicios digitales. • Implementa prácticas nuevas y efectivas. • Asesora sobre los estándares, métodos, herramientas, aplicaciones y procesos disponibles y relevantes para especialidades grupales, y puede tomar decisiones apropiadas a partir de las alternativas.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Contribuye de manera proactiva a la implementación de prácticas de trabajo profesionales y ayuda a promover una cultura organizacional de apoyo.

11.10.11.4 PERSONAL A CARGO DIRECTO

El rol no presenta personal a cargo directo por una definición de estructura organizativa.

11.10.12 EJECUTIVO/A DE TECNOLOGÍAS

11.10.12.1 ROL

El Ejecutivo de TI desempeña un rol clave como asesor administrativo dentro del área de Tecnologías de la Información, brindando soporte integral a las unidades de TI en la gestión de procesos administrativos y operativos. Su función es esencial para optimizar la coordinación interna, facilitando la gestión documental, los procesos de facturación, la organización de reuniones y la planificación de agendas. Actúa como un enlace estratégico entre las áreas técnicas y administrativas, asegurando la eficiencia, el cumplimiento normativo y la fluidez en las operaciones del área de TI.

a) **Gestionar documentación** Organizar, archivar y mantener actualizada la documentación técnica y administrativa de TI, asegurando su accesibilidad y cumplimiento normativo.
b) **Coordinar procesos de facturación**: Apoyar en la gestión de facturas, contratos y pagos relacionados con proveedores de TI, verificando su correcta ejecución y registro.
c) **Planificar reuniones y agendas**: Organizar y coordinar reuniones internas y externas, gestionando agendas de los equipos de TI para optimizar el tiempo y la productividad.
d) **Apoyar la gestión de proyectos** Colaborar en la planificación y seguimiento de proyectos de TI, asegurando la alineación con los objetivos y plazos establecidos.
e) **Facilitar comunicación interdepartamental**: Actuar como punto de contacto entre las unidades de TI y otras áreas administrativas, promoviendo una comunicación efectiva y resolución de necesidades.

11.10.12.2PROCESOS ASOCIADOS

El Rol de Ejecutivo TI no tiene asociación directa con procesos de Gobernanza, dado que articula como un rol de soporte al mismo.

11.10.12.3PERFIL DEL CARGO

El perfil de Ingeniero de Procesos y Servicios TI está muy ligado a la Ingeniería de Software y todo el ciclo de vida asociado al mismo.
Las profesiones que se enmarcan en este rol de manera más eficiente y con mayor idoneidad son:

- Administrador Público (Preferible)
- Técnico Superior en Administración, Experiencia en TI

Las habilidades específicas que debe tener este rol son:

HABILIDAD	DESCRIPCIÓN	NIVEL RESP.
ADMINISTRACIÓN DE EMPRESAS (ADMN)	Gestionar y realizar tareas y servicios administrativos para permitir que las personas, los equipos y las organizaciones tengan éxito en sus objetivos.	3
GESTIÓN DE LAS RELACIONES CON LAS PARTES INTERESADAS (RLTM)	Analizar, gestionar e influir sistemáticamente en las relaciones con las partes interesadas para lograr resultados mutuamente beneficiosos mediante un compromiso estructurado.	4
MEJORA DE PROCESOS DE NEGOCIO (BPRE)	Crear enfoques nuevos y potencialmente disruptivos para llevar a cabo actividades comerciales.	2
GESTIÓN DE CONTRATOS (ITCM)	Gestionar y operar contratos formales, atendiendo las necesidades de los proveedores y los clientes en la prestación de productos y servicios.	3

El nivel de responsabilidad de las habilidades expuestas pondera un **3/7** lo que significa que este rol realiza tareas variadas, a veces complejas y no rutinarias, utilizando métodos y

procedimientos estándar. Trabaja bajo dirección general, ejerce discreción y gestiona el propio trabajo dentro de los plazos. Potencia proactivamente las habilidades y el impacto en el lugar de trabajo.

Para este rol se espera el siguiente comportamiento:

COMPORTAMIENTO	DESCRIPCIÓN
AUTONOMÍA	Trabaja bajo dirección general para completar las tareas asignadas. Recibe orientación y hace revisar el trabajo en hitos acordados. Cuando es necesario, delega tareas rutinarias a otros dentro de su propio equipo.
INFLUENCIA	Trabaja e influye en las decisiones del equipo. Tiene un nivel transaccional de contacto con personas ajenas a su equipo, incluso colegas internos y contactos externos.
COMPLEJIDAD	Realiza una variedad de trabajos, a veces complejos y no rutinarios, en ambientes variados.
CONOCIMIENTO	Aplica el conocimiento de una serie de prácticas específicas de roles para completar tareas dentro de límites definidos y tiene una apreciación de cómo este conocimiento se aplica al contexto empresarial más amplio.

Lo anterior se relaciona directamente con los Factores Conductuales esperados para este rol:

FACTOR CONDUCTUAL	DESCRIPCIÓN
TOMA DE DECISIONES	• Utiliza discreción para identificar y responder a problemas complejos relacionados con sus propias asignaciones. • Determina cuándo los problemas deben escalarse a un nivel superior.
PLANIFICACIÓN	• Organiza y realiza un seguimiento de su propio trabajo (y de otros, cuando sea necesario) para cumplir los plazos acordados.
COLABORACIÓN	• Comprende y colabora en el análisis de las necesidades del usuario/cliente y así lo representa en su trabajo.
RESOLUCIÓN DE PROBLEMAS	• Aplica un enfoque metódico para investigar y evaluar opciones para resolver problemas rutinarios y moderadamente complejos.
MENTALIDAD DE MEJORA	• Identifica e implementa mejoras en su propia área de trabajo. • Contribuye a las mejoras de procesos a nivel de equipo.
CREATIVIDAD	• Aplica y contribuye a las técnicas de pensamiento creativo para aportar nuevas ideas para su propio trabajo y para actividades en equipo.
COMUNICACIÓN	• Se comunica con el equipo y las partes interesadas dentro y fuera de la organización, explicando y presentando información de forma clara. • Contribuye a una variedad de conversaciones relacionadas con el trabajo y escucha a los demás para comprender y hace preguntas de sondeo relevantes para su función.
LIDERAZGO	• Proporciona orientación básica y apoyo a los miembros menos experimentados del equipo según sea necesario.
ADAPTABILIDAD	• Se adapta y responde al cambio y muestra iniciativa en la adopción de nuevos métodos o tecnologías.
MENTALIDAD DIGITAL	• Explora y aplica herramientas y habilidades digitales relevantes para su función.

	• Comprende y aplica de manera efectiva métodos, herramientas, aplicaciones y procesos adecuados.
SEGURIDAD, PRIVACIDAD Y ÉTICA	• Aplica el profesionalismo adecuado y las prácticas y conocimientos prácticos para trabajar.

11.10.12.4 PERSONAL A CARGO DIRECTO

El rol no presenta personal a cargo directo por una definición de estructura organizativa.