PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN MODELO DE GOBIERNO DE TI CON ENFOQUE DE SEGURIDAD DE INFORMACIÓN PARA EMPRESAS PRESTADORAS DE SERVICIOS DE SALUD BAJO LA ÓPTICA DE COBIT 5.0

ANEXOS

Tesis para optar el Título de **Ingeniera Informática** que presenta el bachiller:

Diana Estefanía Lepage Hoces

ASESOR: Moisés Antonio Villena Aguilar

Lima, Abril del 2014

Contenido

Índice de Tablas

Índice de Ilustraciones

ANEXO A: Carta de conformidad de la empresa

1.1 Carta

Miraflores, 05 de noviembre del 2013

Dr. Manuel Tupia Anticona
Coordinador de la especialidad de Ingeniería Informática
Pontificia Universidad Católica del Perú
Pte.

Por medio de la presente carta se informa que la empresa brindó la información respectiva, bajo los criterios de confidencialidad pertinentes, para el desarrollo de la tesis: "Diseño de un gobierno de TI para empresas prestadoras de servicios de salud bajo la óptica de COBIT 5.0" para la obtención del título de Ingeniera de la Srta. Diana Estefanía Lepage Hoces. Los objetivos y sus resultados se detallan a continuación:

Objetivo Específico	Resultado esperado
Elaborar el business case que justifique la implementación del Gobierno de TI en la organización.	Business Case que justifica la implementación del Gobierno de TI.
Mapear las fases del ciclo de vida del Gobierno de TI según COBIT 5.0 para la empresa	Documento que contenga el mapeo de las fases del ciclo de vida de gobierno de TI para la empresa.
Elaborar el balance scorecard de TI de la empresa que refleje las necesidades y expectativas de los stakeholders.	Balance Scorecard de TI.
Elaborar a declaración de aplicabilidad de COBIT 5.0 para el enfoque de Seguridad de Información dentro de la empresa	Matriz de aplicabilidad de procesos habilitadores según COBIT 5.0 en la empresa tomando en cuenta el enfoque de seguridad de información
Modelar los procesos de negocio "AS – IS"	Modelo de los procesos AS-IS de la empresa
Elaborar las políticas de gobierno de TI a aplicarse dentro de la empresa, "TO-BE".	Documento que contenga las políticas de gobierno de TI aplicadas a la empresa. Incluye matriz de responsabilidades.
Evaluar el estado de los procesos habilitadores, correspondientes a los enfoques de gobierno de TI que aplican en la empresa, su evolución y nivel de madurez.	Documento que contenga el estado de los procesos habilitadores y el respectivo nivel de madurez.

Finalmente se señala que se ha participado de reuniones para verificar el desarrollo de los resultados esperados y realizar el trabajo de campo respectivo que complementa a la información brindada.

Esperamos que la presente pueda ser empleada para los fines correspondientes del tesista.
Atentamente.

Claudio del Pozo Gonzales
Sub-Gerente de Servicios de TI
Gerencia de Sistemas y Proyectos de
Transformación – Clínica Internacional

Figura 1.1.1 - Copia de carta de conformidad y evidencia de trabajo de campo

ANEXO B: Marco Teórico y Estado del arte

2.1 COBIT 5.0: Descripción de fases de Gobierno de TI

El ciclo de vida propuesto por COBIT 5.0 comprende de siete fases. El programa de implantación y mejora suele ser continuo e iterativo. Durante la última fase, los nuevos objetivos y requisitos serán identificados y comenzará un nuevo ciclo. [ISACA, 2012c].

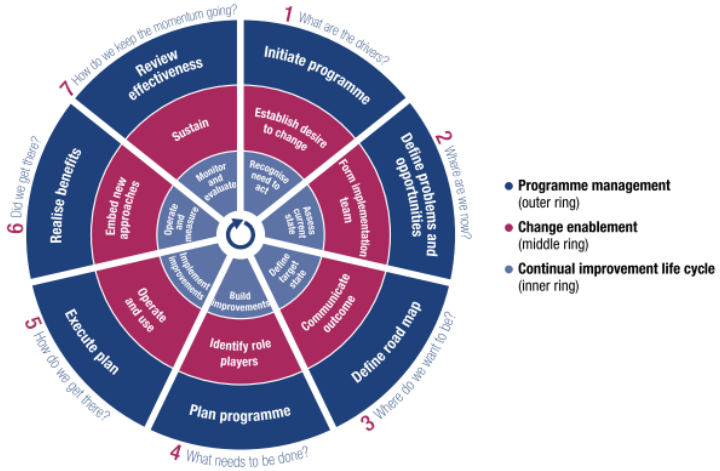


Figura 2.1.1 - Siete fases del ciclo de vida de COBIT 5.0. [ISACA, 2012c].

Estas siete fases se describen a continuación [ISACA, 2012c]:

- **Fase 1 - ¿Cuáles son los drivers?:** Identifica los controles del cambio y crea en el comité estratégico o directivos el deseo del cambio, el cual se expresa en un business case. Los drivers pueden ser eventos, tendencias, déficits de rendimiento, implementaciones de software e incluso objetivos estratégicos de la empresa. Estos pueden actuar como impulsadores del cambio.

- **Fase 2 - ¿Dónde nos encontramos ahora?:** Alinea los objetivos relacionados con las estrategias de la empresa y el riesgo, dando prioridad a los objetivos empresariales más importantes relacionados con las TI, metas y procesos.

- **Fase 3 - ¿Dónde queremos estar?:** Establece un objetivo de mejora seguido de un análisis de brecha para identificar posibles soluciones. Se debe dar prioridad a los proyectos que son más fáciles de lograr y la probabilidad de beneficio es mayor.

- **Fase 4 - ¿Qué necesitamos hacer?:** Planes de soluciones viables y prácticas mediante la definición de los proyectos apoyados por business cases justificables y el desarrollo de un plan de cambios para su implementación.

- **Fase 5 - ¿Qué hacer para llegar ahí?:** En esta fase se prevé la implementación de las soluciones propuestas en la práctica diaria y el establecimiento de medidas y sistemas de control para asegurar el alineamiento con el negocio y que el performance puede ser medido.

- **Fase 6 - ¿Llegamos ahí?:** Esta fase se centra en la transición sostenible de la mejora del gobierno y las prácticas de gestión en las operaciones comunes de negocio y que se logre el monitoreo de las mejoras con las métricas de rendimiento y los beneficios esperados.

- **Fase 7 - ¿Cómo podemos mantener el impulso?:** Comprende la revisión sobre el éxito de la iniciativa, considera la gobernanza adicional o requisitos de gestión y refuerza la necesidad de la mejora continua. Da prioridad a las oportunidades adicionales para mejorar el gobierno de TI.

2.2 COBIT 5.0: Descripción de procesos habilitadores

A continuación se muestra el listado de los procesos habilitadores por cada uno de los dominios que considera el marco.

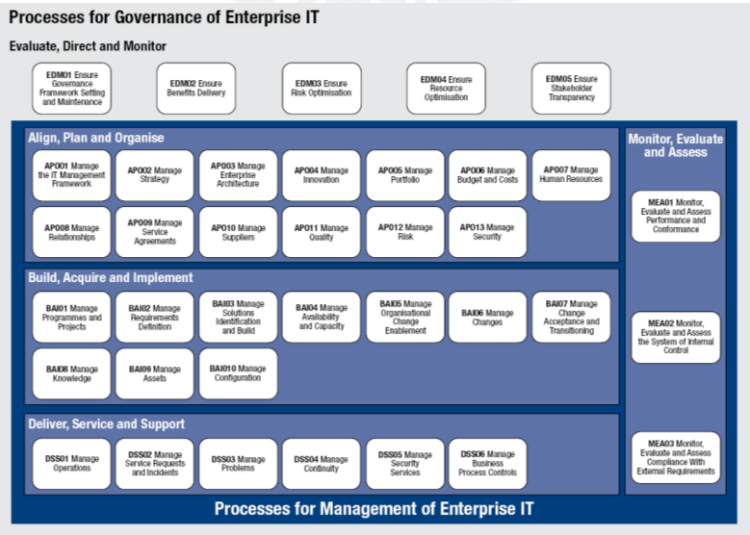


Figura 2.2.1 – COBIT 5.0. Procesos habilitadores. [ISACA, 2012b]

- **Evaluar, Dirigir y Monitorear (EDM)**

  Este dominio en particular está alineado con la norma ISO 38500, la cual se detallará más adelante, pues toma como referencia las tres tareas que recomienda está norma para un buen gobierno de TI.

  Contiene los siguientes procesos habilitadores:

  - Garantizar el mantenimiento y configuración del marco de control de gobierno.
  - Garantizar la entrega de beneficios.
  - Garantizar la optimización de riesgos.
  - Garantizar la optimización de recursos.
  - Garantizar la transparencia de los stakeholders.

- **Alinear, Planear y Organizar (APO)**

  Este dominio se encarga de la administración del planeamiento y organización necesaria para el alineamiento de los objetivos de la empresa y las TI.

  Contiene los siguientes procesos:

  - Gestionar el marco de control de TI.
  - Gestionar la estrategia.
  - Gestionar la arquitectura empresarial.
  - Gestionar la innovación.
  - Gestionar el portafolio.
  - Gestionar el costo y el presupuesto.
  - Gestionar los recursos humanos.
  - Gestionar las relaciones.
  - Gestionar los acuerdos de servicio.
  - Gestionar proveedores.
  - Gestionar la calidad.
  - Gestionar el riesgo.
  - Gestionar la seguridad.

- **Construir, Adquirir e Implementar (BAI)**

  Este dominio abarca el área de construcción de una solución para alinear las TI con la empresa.

  Contiene los siguienteS habilitadores:

  - Gestionar programas y proyectos.
  - Gestionar la definición de requisitos.

- Gestionar la identificación y construcción de soluciones.
- Gestionar la disponibilidad y capacidad.
- Gestionar la habilitación de cambios organizacionales.
- Gestionar los cambios.
- Gestionar la aceptación de cambio y la transición.
- Gestionar el conocimiento.
- Gestionar los activos.
- Gestionar la configuración.

- **Entrega, Servicio y Soporte (DSS)**

  El dominio abarca la operación o ejecución de los planes estratégicos de la empresa y los controles de incidentes a seguir.

  Contiene los siguientes procesos:

  - Gestionar operaciones.
  - Gestionar solicitudes de servicios e incidentes.
  - Gestionar problemas.
  - Gestionar la continuidad.
  - Gestionar los servicios de seguridad.
  - Gestionar los controles de los procesos de negocio.

- **Monitorear, Evaluar y Medir**

  Este dominio abarca lo relacionado al monitoreo de las actividades que garantizarán un buen gobierno de TI y el éxito de esta solución.

  Contiene los siguientes procesos habilitadores:

  - Monitorear, evaluar y medir el rendimiento y la conformidad.
  - Monitorear, evaluar y medir el sistema de control interno.
  - Monitorear, evaluar y medir el cumplimiento de los requerimientos externos.

2.3 COBIT 5.0: Descripción de niveles de madurez

COBIT 5.0 define nuevos modelos de madurez, los cuales se encuentran basados en una norma exigente como lo es la ISO/IEC 15504. Estos son los siguientes [ISACA 2012a]:

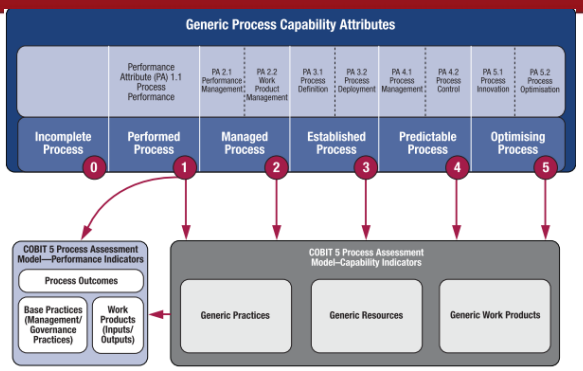


Figura 2.3.1 - Modelos de Madurez según ISO/IEC 15504. [ISACA, 2012a].

Tal como se aprecia en la figura, hay 6 niveles de capacidades para cada proceso. Estos son:

- Proceso incompleto: Este proceso no está implementado o presenta fallas en su propósito.
- Proceso ejecutado: Este proceso implementado logra su propósito.
- Proceso controlado: El proceso ejecutado, previamente descrito es implementado en un modo controlado (planeado, monitoreado y ajustado).
- Proceso estable: El proceso controlado es ahora implementado usando una definición de procesos capaz de lograr los resultados esperados.
- Proceso predecible: El proceso estable descrito ahora opera teniendo en cuenta los límites definidos para lograr los resultados esperados.
- Proceso optimizado: El proceso predecible descrito es continuamente mejorado hasta lograr los objetivos de negocio relevantes actualmente y proyectados.

ANEXO C: Mapeo de Fases de Gobierno de TI

3.1 Caso de Negocio

Contexto Estratégico

Las empresas prestadoras de servicio de salud, en particular con la cual se desarrolla el modelo de gobierno de TI, tiene como meta la ampliación de sus servicios hacia toda la comunidad a través de sus distintas modalidades o canales de atención.

La organización desea llegar a toda la población objetivo y brindar una mejor atención a través de nuevos recursos junto con el apoyo de una buena gestión y manejo de tecnología de vanguardia para satisfacer las necesidades de sus clientes.

La necesidad del negocio es encontrar los recursos y capacidades necesarias para abastecer sus sucursales y poblarlos de la infraestructura tecnológica necesaria para brindar atención y a su vez para soportar sus sistemas organizacionales y cumplir con las regulaciones a las cuales se encuentran sujetas.

Los drivers[1] del cambio identificados son:

- Recursos: Necesidad de integrar servicios que cubran las necesidades y de acuerdo a la expansión deseada y planificada (incremento de sucursales) y que se estén alineados a los objetivos de negocio.
- Regulaciones: Se incorpora la ley 29733 para la protección de datos personales en nuestro país. No se debe dejar de lado las normas previas.
- Tecnología: Contar con tecnología de vanguardia para mejorar su servicio. (Asegurar el retorno del valor).

Entre las necesidades de negocio y entregables deseados se tienen:

Requerimientos clave			
	Core	Deseable	Opcional
Alinear objetivos estratégicos de la organización junto con sus objetivos de TI.	**X**		
Lograr el crecimiento de sucursales de modo de llevar tecnología que beneficien la salud.		**X**	

[1] Drivers: Impulsadores del cambio

Lograr que las tecnologías empleadas sean las mejores del mercado de acuerdo a las necesidades de la empresa.		X	
Reducir los costos en tecnología y procesos de información asegurando la calidad			X
Velar por la información confidencial de todos los pacientes y asegurar su disponibilidad	X		

Tabla 3.1.1- Descripción de Requerimientos.

La inversión deseada para implementar una nueva solución tiene como base lo siguiente:

- Cumplir con la regulación actual y vigente dentro del país: Ley de protección de datos personales, norma técnica peruana de historia clínica y ley de emergencia.
- Brindar responsabilidad a la gerencia y dar una dirección correcta a los recursos técnicos y financieros para logar el cumplimiento de objetivos.

Para llevar a cabo la nueva solución, se requiere según el contexto, desarrollar el proyecto por etapas considerando los cambios que se van a implementar y evaluarlos en el espacio de tiempo necesario utilizando métricas de acuerdo a los drivers del cambio y objetivos deseados.

Análisis y Recomendaciones

Opciones preliminares

Para cubrir las necesidades y según el contexto señalado y colmar las expectativas de la alta dirección y otros stakeholders se listan las siguientes sugerencias que puedan corresponder los requerimientos clave:

Opciones	Descripción
Adquisición de Equipos de vanguardia.	Contar con equipos para detección de enfermedades y tecnologías de información y sistemas que apoyen a la mejora de la experiencia del cliente.
Implementación de sistemas para gestión.	Se desea gestionar los recursos de forma adecuada y medir su desempeño.

Implementar un SGSI[2]	Emplear dicha solución para cumplir con las regulaciones y políticas de seguridad establecidas para velar por la integridad de la información.
Adoptar buenas prácticas de ITIL	Esta opción se recomienda para mejorar la entrega de servicios a los clientes, gestión de proveedores y relaciones de negocio que sean el soporte para cumplir otros objetivos de negocio.
Implementar un SGCN[3]	Se plantea esta solución para evitar la interrupción de los servicios y elaborar su plan de recuperación de servicios de TI.
Implementar un Sistema de Gobierno de TI	Se plantea esta solución para lograr la dirección estratégica y alcance de objetivos, basado en los enfoques y procesos más relevantes, sin dejar de lado los drivers y resultados esperados.
Implementar la mejora continua	Esta opción se toma en cuenta como parte de un trabajo de reingeniería de los procesos y lograr incrementar su eficiencia.

Tabla 3.1.2 - Descripción de Opciones a considerar

Criterios para la elección	1	2	3	4	5	6	7
Cumplir con la regulación	**No**	**No**	**Sí**	**-**	**Sí**	**Sí**	**No**
Cubrir las necesidades de negocio	**Sí**	**No**	**Sí**	**Sí**	**Sí**	**Sí**	**No**
Potenciar y mejorar el servicio entregado	**Sí**	**Sí**	**-**	**Sí**	**No**	**Sí**	**Sí**
Entrega de valor para las partes interesadas	**No**	**No**	**Sí**	**Sí**	**No**	**Sí**	**Sí**
Resultados	Inviable	Inviable	Viable	Viable	Aplica[4]	Viable	Inviable

Tabla 3.1.3 - Evaluación de criterios por propuesta

[2] SGSI: Sistema de Gestión de seguridad de Información
[3] SGCN: Sistema de Gestión de Continuidad de negocios
[4] En este caso particular un SGCN aporta a la solución del problema pero existen mejores opciones.

Opciones viables

Tras la evaluación de los criterios, realizada en base al alcance y definición de este tipo de proyectos, se tiene como opciones viables las siguientes:

- Opción 1: Emplear principios de ITIL para la entrega de servicio.
- Opción 2: Implementar un gobierno de TI.
- Opción 3: Implementar un SGSI.

Análisis de costos e inversión: Resumen

Consideraciones generales:

- Enfoques para gobierno de TI: Seguridad de Información como base proyectándose posteriormente a la gestión de operaciones de TI.
- Costos expresados en dólares.
- Horas laborales: 8 horas.
- Se asume un personal que cuenta con la respectiva certificación en dichos rubros.
- Beneficios Criterios: Preservar vida humana, calidad en procesos, integración con otras soluciones, trabajos futuros y tiempo de vida del proyecto.

	Costo total	Beneficios[5]	Costo efectivo[6]	Costo Beneficio	Costo beneficio Neto
Opción 1: ITIL	90000	40	80000	4000	10000
Opción 2: Gobierno	200000	25	192000	2500	5000
Opción 3: SGSI	121000	35	115000	3500	6000

Tabla 3.1.4 - Resumen de costos de proyectos

Consideraciones y otros datos a asumir:

	ITIL	Gobierno de TI	SGSI
Hora de consultoría	**80**	**100**	**90**
Tiempo de duración [7]	6 meses	10 meses	8 meses
Tiempo destinado a la documentación.	Incluye documentación.	2 meses	Incluye documentación.

Tabla 3.1.5 - Consideraciones y datos

[5] El beneficio se considera como un factor. A mayor beneficio por ahorro de recursos, el factor es menor, por ello el costo total se incrementa a razón.

[6] Costo relacionado al trabajo neto en la consultoría.

[7] En el caso de los tiempos de duración de los proyectos se considera la fase análisis, diseño e implementación con sus respectivas iteraciones. Se toma con base proceso core y un enfoque en particular.

Si bien es cierto, Gobierno de TI es un proyecto de costo más elevado permite trabajos futuros que empleen la propuesta conjunta de implementación de un SGSI y buenas prácticas de ITIL según sea el enfoque.

Justificación y recomendaciones

Se sugieren estas tres opciones viables, pues a nivel general, la organización requiere acciones basadas en procesos clave para poder cumplir con las regulaciones y objetivos estratégicos planteados, lo cual implica realizar un análisis a fondo de los beneficios y cumplimiento con criterios como el alineamiento estratégico, entrega de valor, gestión del riesgo, entre otros que garanticen contrarrestar los efectos de la problemática y adaptarse al contexto descrito.

Criterios	Opción 1	Opción 2	Opción 3
Alineamiento estratégico	**No**	**Sí**	**No**
Entrega de valor	**Sí**	**Sí**	**No**
Gestión de riesgos	**No**	**Sí**	**Sí**
Requerimientos definidos	**Deseable**	**Core**	**Core/Deseable**
Cumplir con la regulación	**No**	**Sí**	**Sí**
Cubrir las necesidades de negocio	**Sí**	**Sí**	**Sí**
Potenciar y mejorar el servicio entregado	**Sí**	**Sí**	**No**
Gestión óptima de recursos	**Sí**	**Sí**	**No**
Costos de implementación	**Costo menor**	**Costo elevado**	**Costo medio**
Costos de retorno (ROI)	**Válido**	**Válido/mayor**	**Válido**
Otros criterios de elección	**Sí**	**Sí**	**Sí**
Resultado		**Seleccionado**	

Tabla 3.1.6 - Análisis de criterios y justificación

Se recomienda que se realice una evaluación exhaustiva a través de cuadros de mando tales como el balance scorecard para la medición de objetivos, con lo cual se podrá tener una situación real.

Considerando la necesidad de llevar a cabo planes estratégicos y se busca una solución integral se plantea optar por un Gobierno de Tecnologías de Información,

pues por medio de esta solución se puede emplear principios para diseñar un SGSI e incluso adoptar buenas prácticas de ITIL por medio de sus procesos habilitadores.

Gestión y Capacidad

Tras la elección de implementar un sistema de gobierno de tecnologías de información, se elabora el plan de supervisión de la inversión. Al ser esta una solución que compromete a la alta dirección, se debe definir el asignar un rol de supervisor y establecer mecanismos de control para velar por la inversión realizada, y a través de métricas e indicadores verificar los resultados. Es posible emplear el balanced scorecard propuesto en COBIT 5.0 y evaluar la perspectiva financiera.

El proyecto debe gestionarse a lo largo de su duración. Se estima que la implementación de gobierno cumple un ciclo de 2 años para lograr resultados visibles, en otras palabras alcanzar un nivel de madurez aceptable en sus procesos. En este caso, se puede emplear el mapeo de fases de un proyecto de gobierno propuesto en COBIT 5.0 en el cual a través de sus ciclos mide los resultados y necesidades incluyendo la inversión.

Para visualizar los resultados, se recomienda la medición de los procesos. COBIT 5.0 brinda los mecanismos e indicadores para identificar el nivel de madurez de estos empleando la norma ISO 15504 como base.

Los riesgos son gestionados dentro de un sistema de gobierno de TI cumpliendo con uno de sus pilares, la gestión del riesgo, lo cual involucra al riesgo técnico, riesgo de inversiones, riesgo operacional, entre otros. COBIT 5.0 propone la gestión de riesgos, al integrarse con el marco de control RISK IT. No obstante se pueden emplear otras normas complementarias como la ISO 31000.

Para la gestión del cambio, se puede gestionar por medio de procesos habilitadores de COBIT o incluso adoptar procesos de la fase de transición de ITIL para aplicar sus buenas prácticas a la gestión y cambios dentro del proyecto y su inversión.

Finalmente, para medir el rendimiento de la inversión realizada y del proyecto en general, se puede complementar la parte de la visualización de resultados junto con el mapeo de fases propuesto por COBIT 5.0 y aplicar métricas e indicadores para la medición y desempeño de los procesos. Se puede optar también por emplear el cuadro de mando (balanced scorecard).

ANEXO D: Mapeo de Fases de Gobierno de TI

4.1 Mapeo de fases de Gobierno de TI

Se realiza la identificación del estado organizacional dentro de cada una de las fases propuestas en COBIT 5.0 durante la iniciativa, ejecución y posterior al programa de gobierno de TI. Junto con el comité estratégico, del cual depende esta iniciativa, se realiza este análisis. Se propone para este fin la siguiente estructura.

4.1.1 Fase 1: ¿Cuáles son los drivers?

Gestión del Programa de gobierno: Inicio
Se establece el comité estratégico responsables de esta iniciativa así como se asignan sus roles y responsabilidades dentro del proyecto. Como se desarrollará un enfoque de seguridad de información se reconoce inicialmente la necesidad del oficial de seguridad de información. Se establecen los objetivos de alto nivel y se prioriza aquellos que van a ser cubiertos por esta iniciativa. Para esto se toma como referencia el plan estratégico de la empresa y el plan de TI vigente (2012 – 2016). El business case antes presentado sustenta la elección del proyecto bajo y sus principales beneficios, de acuerdo a los drivers que han sido identificado y al retorno de la inversión realizada.
Habilitar el cambio: Establecer el deseo de cambio
Entre los principales stakeholders, se reconoce la necesidad de establecer un comité estratégico que se responsabilice de las acciones y dirija de forma idónea la división de TI. Por esta razón y según los drivers identificados, este comité y los involucrados deben comunicar esta iniciativa para motivar al personal para colaborar en esta etapa de cambio producto de los drivers e intenciones para lograr los objetivos estratégicos planteados a corto y largo plazo.

Como organización, se establecen los planes iniciales para lograr este cambio y evaluar el impacto de esta solución frente a los beneficios y resultados esperados.

Mejora continua del ciclo de vida: Reconocer la necesidad de actuar
El comité reconoce que es necesario aplicar medidas y nuevas políticas para la mejora de sus procesos que conlleve a alcanzar los objetivos estratégicos producto de los nuevos impulsos. Recabando la información sobre los las necesidades de los stakeholders, documentos y otros activos que reflejen el estado actual de la organización, se identifican los siguientes drivers y se alinean a guías o principios de organizaciones internacionales: • Recursos: Necesidad de integrar servicios que cubran las necesidades y de acuerdo a la expansión deseada y planificada (incremento de sucursales) y que se estén alineados a los objetivos de negocio. • Regulaciones: Se incorpora la ley 29733 para la protección de datos personales en nuestro país. Se debe mantener lo estipulado por la norma técnica de la historia clínica [Minsa, 2005]. • Tecnología: Contar con tecnología de vanguardia para mejorar su servicio para beneficio de sus clientes. Además de asegurar el retorno de éstas inversiones.

Tabla 4.1.1 - Mapeo Fase 1 del ciclo de vida de gobierno

4.1.2 Fase 2: ¿Dónde estamos?

Gestión del Programa de gobierno: Describir los problemas y oportunidades
Actualmente la empresa atraviesa un proceso de cambio dentro de la alta dirección, por ende existe una nueva visión dentro de la gerencia tanto como de la gerencia de informática. A esto se suma, las regulaciones vigentes dentro de la organización que les exige velar por la seguridad del paciente y mejorar su experiencia empleando sus servicios.

Así mismo, se debe corresponder a las exigencias de sus stakeholders y proveedores, especialmente a los actores y canales a través de los cuales se brindan los servicios, tales como las aseguradoras, institutos con los cuales se trabajan en conjunto y otros programas de salud.

Entre sus oportunidades se identifica la mejora a nivel estratégico de sus tecnologías de información para cumplir con las regulaciones existentes y la oportunidad de crecimiento y acceso a nuevas tecnologías para acceder a la especialización en líneas de negocio que conlleven a competir a nivel local y tener un reconocimiento fuera del país.

Habilitar el cambio: Establecer el equipo de implementación

Para conseguir la implementación del gobierno de TI, se debe de contar con personas con experiencia y conocimiento necesario sobre estos principios y el marco elegido, en este caso COBIT 5.0.

Inicialmente se parte de la iniciativa de comprometer en esta implementación al Jefe de proyectos de la organización y al encargado de establecer gobierno bajo COBIT 4.1.

No obstante, se deberá optar por una capacitación o contar con el apoyo de una consultoría externa, propuesta en el business case, debido a que en el contexto actual, son pocos los certificados en COBIT 5.0 y se va a requerir de una guía o acompañamiento para la implementación y definir la estrategia a seguir.

Adicionalmente a lo largo de la implementación y la asignación de roles se irá incorporando nuevo personal al equipo, sobretodo a un representante de la alta dirección para que se comprometa con esta iniciativa y los cambios que surgirán.

Mejora continua del ciclo de vida: Evaluar el estado actual

Identificados los drivers del cambio, se debe documentar las iniciativas y alinear con los propósitos de COBIT 5.0 e ISACA internacional, reforzando entonces los objetivos de la organización y desarrollando las métricas para su medición.

Se evalúa la situación actual de la organización y se identifica un proceso core de negocio para su mejora bajo el enfoque de seguridad de información.

Bajo el análisis realizado, se refuerzan los objetivos, las estratégicas y métricas a seguir para la medición del proceso a futuro y verificar si se ha alcanzado parte de los objetivos estratégicos y como se refleja dentro de la organización.

Tabla 4.1.2 - Mapeo Fase 2 del ciclo de vida de gobierno

4.1.3 Fase 3: ¿Dónde Queremos Estar?

Gestión del programa de gobierno: Definir la hoja de ruta
Al tener los objetivos de alto nivel definidos, se debe de establecer y formalizar los mecanismos para alcanzarlos. Para esto, el comité estratégico[8] diseña a nivel preliminar un conjunto de pasos a seguir para alcanzar el estado ideal, para que a nivel posterior se materialice o se corrija tomando en cuenta los riesgos producto del cambio y estructura de roles planteada inicialmente. Bajo el business case elaborado, se deberá aterrizar los presupuestos, no obstante dentro de este proyecto académico se deberá asumir de todas formas los gastos reales para formalizar, tal vez a futuro un trabajo de consultoría junto con plazos establecidos y entregables para mostrarlos a la alta gerencia y hacerlos partícipes de la iniciativa de forma escalar. Se asume por tanto, los costos como válidos y que la organización brinda el presupuesto inicial y lo ajusta a los plazos de este proyecto.
Habilitar el cambio: Describir y comunicar los resultados deseados
El comité estratégico debe identificar el rol de comunicador o de lo contrario ser ellos, como dueños de la iniciativa, de comunicar de forma transversal el cambio y lo que se espera a raíz de ello, alineándose siempre al enfoque escogido de seguridad de información.

[8] El comité estratégico forma parte de la organización y la información es confidencial, se propone la estructura para formalizarlo.

Para esto se elabora un plan inicial que debe ser documentado en el cual se muestran todos los beneficios de la iniciativa y a su vez demostrarlos, basándose en todo caso en casos de estudio o en su experiencia empleando COBIT 4.1 como marco de gobierno.

No obstante, se insiste en comunicar también las acciones principales a realizar, tales como la identificación del mapa de procesos y la evaluación a detalle del proceso seleccionado.

Mejora continua del ciclo de vida: Definir el estado ideal y realizar el análisis de brecha

Se evalúa bajo los conceptos de COBIT 5.0 e ISACA y los objetivos de alto nivel. Entre ellos:

- Llegar a ser una de las organizaciones de salud importantes debido a que se trabaja con líneas de negocio innovadoras tales como: Unidad de tórax, oncológica, columna y Stroke[9].

- Así mismo, ser reconocidos como una organización líder en brindar seguridad a todo nivel a nuestros pacientes, como también una excelente experiencia de nuestro servicio. Optando por el alineamiento con estándares no solo a nivel local sino también internacional.

- Ser líderes en tecnología de manera estratégica, continuando con las buenas prácticas a raíz de la implantación de COBIT 4.1.

Se realiza el análisis de brecha para determinar cuánto falta dentro de la organización para llegar a ese estado, empleando estadísticas y gráficos que permita a su vez identificar las oportunidades de mejora dentro de la situación actual.

Tabla 4.1.3 - Mapeo Fase 3 del ciclo de vida de gobierno

[9] Stroke: Accidente cerebrovascular

4.1.4 Fase 4: ¿Qué necesita hacerse?

Gestión del programa de gobierno: Desarrollar un plan de iniciativa
Se desarrolla el plan teniendo como base proyectos para garantizar el éxito del gobierno de TI. Entre ellos: • Dar soporte al repositorio de documentación de la organización y actualizar constantemente así como estandarizar los procesos core de negocio. • Establecer las políticas de seguridad y de TI a nivel macro en conjunto con la propuesta de COBIT 5.0. Se realiza la priorización de los activos y recursos dentro de la organización de acuerdo a la información que gestiona y los procesos seleccionados como base del gobierno. Se tiene los siguientes: • Historias clínicas • Centro de datos dentro del cual están los servidores que almacenan la información de los pacientes y los sistemas core de la organización. • Personal clave y estratégico para dar la continuidad al servicio. Finalmente se establece un plan de proyecto inicial para llevar a cabo la solución y sus entregables, lo cual formaliza la participación de un externo que realizará un trabajo de campo para justificar la iniciativa y desarrollar los planes de mejora y políticas futuras.
Habilitar el cambio: Reforzar el esquema de roles e identificar logros a corto plazo
Dentro de los roles identificados el comité estratégico debe de identificar según el enfoque seleccionado la lista de personas que serán afectadas por dicho cambio, de manera que se hagan responsables de aceptar la calidad del resultado posterior. En este caso, la división o responsables de los proyectos de seguridad de información. Así mismo, dentro de los logros a corto plazo se establecen identificar los siguientes:

- Se identifican las métricas para la evaluación del proceso y los objetivos alcanzados.
- El proceso seleccionado se diseña nuevamente y se establecen las primeras mejoras para lograr un nivel de madurez uno (1).
- Se desprenden las políticas iniciales según los procesos habilitadores que han sido identificados en COBIT 5.0.
- Se formaliza la iniciativa de gobierno contrarrestando los efectos de la resistencia al cambio a nivel organizacional.

No obstante, también se deberá identificar las fortalezas del proceso AS-IS, el cual según la evaluación preliminar bajo la norma ISO 15504 integrada en COBIT 5.0 su nivel de madurez es cero (0), debido a la falta de esquemas y comunicación del proceso de manera transversal a la organización. Entre sus fortalezas se tiene:

- Aceptación de la junta directiva de la organización y revisión de las actividades core.
- Mapeo y asociaciones del proceso a gran nivel permitiendo una futura interacción o integración con otros similares o de soporte.

Mejora continua del ciclo de vida: Diseñar y construir mejoras

Se diseña un mapa con el cual se identifica los principales beneficios de la iniciativa y la viabilidad de su ejecución en conjunto con el comité estratégico. Se reafirma por ende lo siguiente:

- Enfocar el proceso escogido hacia la seguridad de información, bajo los lineamientos de la norma ISO 27001 y respetando la ley de protección de datos personales.
- Validar los lineamientos de Hipaa que es una norma americana que rige la seguridad a nivel del sector salud.

Por esta razón se insiste en identificar a un oficial de seguridad de información dentro de este proceso de mejora para que implemente y haga respetar las políticas que se desprendan a futuro, es decir una vez iniciado el plan de ejecución.

Tabla 4.1.4 - Mapeo Fase 4 del ciclo de vida de gobierno

4.1.5 Fase 5: ¿Cómo llegamos ahí?

Gestión del programa de gobierno: Ejecutar el plan

En esta etapa, se verifican ciertos detalles para la ejecución de todos los planes definidos así como se muestra en el caso de la implementación de los planes d cambio. Dentro de esta, que aún sigue en marcha, se han tomado ciertas consideraciones:

- Verificar que la ejecución del proyecto se encuentre alineada o que tenga como base los planes iniciales, respetando por lo tanto los tiempos establecidos.

- Aprobar junto con el comité estratégico el inicio de cada iteración o etapa importante de los planes. Esto se evidencia con los primeros resultados a corto plazo que han sido obtenidos.

- Brindar informes actualizados a los stakeholders, en este caso, al comité estratégico para garantizar el progreso y realizar la supervisión conjunta. Lo cual, se da a notar con la validación de los entregables y primeros resultados.

- Monitoreo constante del riesgo del proyecto para poder tomar acciones correctivas y, según amerite, aprobar los cambios pertinentes. Este último no se ha presentado hasta el momento, salvo por el ajuste en el alcance y la validación de los plazos de entrega.

Habilitar el cambio: Habilitar el funcionamiento y uso

En esta etapa, se inicia la implementación de los planes de resistencia al cambio que han sido diseñados y formalizados por el comité estratégico lo cual incluye:

- Identificación y reconocimiento del comité estratégico para iniciar las actividades respectivas considerando la aceptación y el compromiso con el cambio. Para esto se puede tomar como ejemplo el cambio que implica la formalización y adaptación de todos los procesos organizacionales a la notación BPMN 2.0.

Así mismo, se inicia la comunicación de funciones y responsabilidades del plan de

cambio, teniendo como fuente, el requerimiento del cambio en la estructura organizacional para permitir nuevos roles o puestos para el mantenimiento del gobierno de TI bajo el enfoque de seguridad de información.
Mejora continua del ciclo de vida: Implementar mejoras
Teniendo como base el input de la fase anterior, en la cual se definen los logros a corto plazo y se diseñan los planes iniciales para la implantación del gobierno de TI, se inicia la implementación de estos planes bajo lo siguiente: - Formalización de los planes de iniciativa ajustándolos a los tiempos pertinentes según la viabilidad y recursos disponibles. En este caso tentativos para la implementación. Para el caso del diseño, se sigue el plan de proyecto inicial. - Elaboración del diseño de la solución y sus documentos complementarios entre los cuales se tiene lo siguiente: • Identificación de métricas para los objetivos organizacionales. • Elaboración de los cuadros de mando para medición de objetivos • Identificación de los procesos habilitadores bajo el enfoque de seguridad de información. • Diseño del mapa de procesos que soporta esta iniciativa

Tabla 4.1.5 - Mapeo Fase 5 del ciclo de vida de gobierno

4.1.6 Fase 6: ¿Hemos llegado?

Gestión del programa de gobierno: Darse cuenta de los beneficios
Para la supervisión e identificación de beneficios del programa de gobierno:: • Teniendo el mapeo de actividades y sub-actividades de gestión para cada habilitador, se realiza la evaluación con el personal indicado de acuerdo a su rol y función para determinar el nivel del logro alcanzado hasta la fecha. • Se compara si lo resultados obtenidos están alineados a los objetivos del proceso

y en consecuencia a los objetivos de negocio de manera que se pueda identificar si la iniciativa y solución es satisfactoria o si falta conciencia para poder aplicar este tipo de proyectos, por lo cual se debe ir más lento y asegurando la materialización de logros positivos y efectivos para cada una de las etapas.

- Frente a los resultados, resaltar las oportunidades de mejora y detallarlas como lecciones aprendidas. En este caso particular, los beneficios del gobierno de TI son evidentes y estratégicos para la organización, pero dentro del diseño no se muestra un alcance total de estos beneficios.

Habilitar el cambio: Insertar nuevos enfoques

Dentro de esta capa media se verifica que dentro de la organización no se han formalizado los roles sugeridos para dirigir la iniciativa de gobierno de TI ni de la función de seguridad de información. No obstante se trabajan en proyectos que puedan justificar los cambios en la estructura organizacional, pero se sugiere justificarlos por casos de negocio.

Como una de las metas a largo plazo es ampliar el alcance del programa de gobierno y fortalecer la toma de decisiones, por medio de planes de cambio se define tiempos clave para poder gobernarse de acuerdo a los nuevos roles y responsabilidades identificada para el enfoque de seguridad de información, es decir velar e insistir para llegar a un acuerdo y reconocimiento formal del comité estratégico y el oficial y gestor de seguridad de información.

Mejora continua del ciclo de vida: Operar y Medir

Junto con la empresa se trazan los periodos para la revisión de cada iteración de gobierno. En principio, como actualmente están todavía bajo el enfoque de COBIT 4.1, se señaló una revisión cada cuatro (4) meses, sin embargo, tomando en cuenta el alcance actual del programa y las brechas del negocio se recomienda la evaluación cada seis (6) meses.

Se identifican las metas y actividades de gestión a aplicar para cada proceso habilitador. Éstas son las métricas base para identificar los beneficios y la realidad de la organización frente a lo que pretende llegar, por esta razón, el escenario base a

analizar es como se encuentran los procesos de negocio a la fecha.

Finalmente se traza como objetivo a largo plazo, revisar el modelo de gobierno de TI y ampliar el alcance de procesos para el mismo enfoque. Sin embargo, otra de las metas es poder optar por otro enfoque adicional, para que, a partir de este programa, se tenga una misma cadena de responsabilidades y decisiones de alto nivel que garantice alcanzar los objetivos de negocio.

Tabla 4.1.6 - Mapeo Fase 6 del ciclo de vida de gobierno

4.1.7 Fase 7: ¿Cómo se mantiene la iniciativa?

Gestión del programa de gobierno: Revisar la efectividad
Se verifica en esta fase que se lleve a cabo la iniciativa, es decir que algunas actividades sean consideradas para el entorno real de la organización. En este caso, la empresa referencia, por medio del marco de gobierno bajo el cual gobiernan, deben de identificar la brecha entre ambos marcos y el enfoque de seguridad, para aplicarlo dentro de los objetivos que tienen definidos. Respecto al modelo de gobierno que ha sido diseñado, se verifica que en efecto, está realizado bajo el entorno de la organización y empleando información real, lo cual se evidencia en el **anexo A.** Finalmente de acuerdo a la efectividad, como la organización no tiene en la actualidad todas las medidas para garantizar la seguridad de información y alineamiento con el marco regulatorio, aunque las actividades identificadas para cada habilitador son adecuadas y aceptadas por la empresa, porque en efecto representan la mejora que desean, los objetivos del programa serán más visibles dentro de las próximas dos (2) iteraciones para poder adecuarse a los cambios y resaltar solo logros y fortalezas a nivel organizacional.
Habilitar el cambio: Sostener
Dentro de las metas futuras se considera que la organización está en el deber de

capacitar y concientizar al personal respecto a estas iniciativas de gobierno, sobre todo orientarlos para adecuarse a cambios organizacionales como el nuevo esquema de roles y responsabilidades propuesto tras la adecuación al marco de gobierno.

No obstante, basándose en los resultados de la evaluación realizada, se debe validar y volver a identificar y definir actividades de los procesos habilitadores de acuerdo a los cambios en el entorno y el nivel de madurez que se pretenda alcanzar.

El comité estratégico tiene la responsabilidad de comunicar los resultados de la evaluación, para que todo el personal este enterado de las debilidades del modelo de gobierno y en conjunto trabajen para alcanzar una meta ideal para beneficio de la organización y logro de objetivos estratégicos

Mejora continua del ciclo de vida: Monitorear y evaluar

Teniendo los resultados de la evaluación de los procesos habilitadores, se debe identificar cuáles son las necesidades de mejora para encaminar esta iniciativa para la siguiente iteración del ciclo de vida. Se considera entonces lo siguiente:

- Formalizar estrategias para la gestión e identificación de riesgos en la organización.
- Establecer una función y estrategias de seguridad de información.
- Lograr un nivel de madurez mayor dentro de los procesos habilitadores para que el este programa de gobierno se encamine y se vuelva sólido en la organización.

Por ello, los nuevos objetivos para el gobierno de TI son:

- Formalizar el programa y el enfoque de seguridad de información.
- Incrementar el nivel de madurez para cada proceso habilitador hacia el nivel superior.
- Complementarse con otros proyectos y regulaciones actuales, considerando incluso incrementar el alcance de este proyecto.

Tabla 4.1.7 - Mapeo Fase 7 del ciclo de vida de gobierno

ANEXO E: Identificación de objetivos e indicadores

5.1 Identificación de objetivos organizacionales y justificación

5.1.1 Resumen de objetivos mapeados

Objetivos Empresa	Objetivos de COBIT 5.0
Ofrecer a los pacientes seguridad y una mejor experiencia dentro de su estancia en la clínica.	Operaciones y personal productivo
Lograr la expansión estratégica de la organización	Portafolio de productos y servicios competitivos.
Lograr ser reconocidos por la excelencia en la atención	Cultura de servicio orientada al cliente.
Lograr la eficiencia en los procesos garantizando la seguridad al paciente.	Optimización de las funcionalidades de los procesos de negocio.
Contar con un equipo de calidad y altamente capacitado	Personal motivado y capacitado
Cumplir con las regulaciones existentes	Cumplimiento con leyes y regulaciones externas.

Tabla 5.1.1 – Mapeo de objetivos organizacionales de la empresa con los objetivos de COBIT 5.0

5.1.2 Justificación del mapeo

Los objetivos son mapeados a los objetivos corporativos de COBIT por lo siguiente:

- Objetivo “A” a Objetivo 14

  La relación es directa debido a que el primer objetivo parte de brindar mejor seguridad y experiencia al paciente por ello se requiere operaciones y personal productivo en capacidad de brindar un servicio de acuerdo a las expectativas.
- Objetivo “B” a Objetivo 2

  Parte de la expansión estratégica no solo consiste en crecimiento a nivel de sucursales sino por medio de programas o nuevos servicios para beneficio del cliente. Por esta razón se mapea con dicho objetivo, pues se deberá mantener un portafolio de servicios competitivo capaz mantener un alto nivel estratégico.

- Objetivo “C” a Objetivo 6

  Se plantea ser reconocidos por “la excelencia de atención brindada a los clientes”, por ello se puede entender que su cultura organizacional busca orientarse a los pacientes y la entrega de mejores servicios. Es así que se realiza el mapeo con el objetivo corporativo 6 de COBIT 5.0.

- Objetivo “D” a Objetivo 11

  Uno de los objetivos críticos es lograr contar con procesos eficientes a nivel financiero y optimización de recursos para satisfacción de los clientes y beneficio de la organización, por ello se justifica el mapeo con el objetivo 11.

- Objetivo “E” a Objetivo 16

  Este objetivo está relacionado directamente al equipo que compone la organización y sus divisiones. Se reconoce la necesidad de contar con personal capacitado para poder cumplir con las necesidades de negocio y brindar una mejor atención al cliente a nivel general. Por esta razón se mapea con el objetivo 16 de COBIT 5.0.

- Objetivo “F” a Objetivo 4

  Finalmente se tiene el objetivo de cumplimiento regulatorio cuyo mapeo es directo al considerar normas como la NTP de historia clínica de los establecimientos del sector salud, Ley de emergencia y la ley de protección de datos personales.

5.2 Mapeo de objetivos organizacionales con objetivos de TI

Se detallan los objetivos y su relación principal (‘P’) o secundaria (‘S’) con los objetivos organizacionales. El resumen de los objetivos de TI a aplicar se encuentra en el documento principal junto con la justificación de su elección.

Objetivo organizacional 2

Perspectiva	Objetivo de TI	Relación Objetivo Organizacional
Financiera	Alineamiento de las tecnologías y estrategia de negocio	P
	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	S
	Materializar beneficios de TI habilitando la inversión	P

	y portafolios de servicio	
Cliente	Entregar servicios de TI alineados con los requerimientos de negocio	P
	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S
Proceso Interno	Agilidad de TI	P
	Optimización de activos, recursos y capacidades de las TI	S
	Capacitación y soporte de procesos de negocio a través de la integración de aplicaciones y tecnología en los procesos empresariales	P
	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	S
	Disponibilidad de información útil y relevante para la toma de decisiones	S
Aprendizaje y Crecimiento	Personal de Negocio y TI competente y motivado	S
	Conocimiento, experiencia e iniciativa para la innovación empresarial	P

Tabla 5.2.1 - Objetivos de TI identificados para objetivo organizacional 2

Objetivo organizacional 4

Perspectiva	Objetivo de TI	Relación Objetivo Organizacional
Financiera	Cumplimiento de TI y soporte para el cumplimiento empresarial de las leyes y regulaciones externas	P
	Riesgos de negocio relacionados con las tecnologías de información gestionadas	S
Cliente	Entregar servicios de TI alineados con los requerimientos de negocio	S
Proceso Interno	Seguridad de Información, infraestructura de procesamiento y aplicaciones	P
	Disponibilidad de información útil y relevante para la toma de decisiones	S

	Cumplimiento de las políticas internas por parte de las TI	S

Tabla 5.2.2 - Objetivos de TI identificados para objetivo organizacional 4

Objetivo organizacional 6

Perspectiva	Objetivo de TI	Relación Objetivo Organizacional
Financiera	Alineamiento de las tecnologías y estrategia de negocio	P
	Materializar beneficios de TI habilitando la inversión y portafolios de servicio	S
Cliente	Entregar servicios de TI alineados con los requerimientos de negocio	P
	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S
Proceso Interno	Agilidad de TI	S
	Capacitación y soporte de procesos de negocio a través de la integración de aplicaciones y tecnología en los procesos empresariales	S
	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	S
Aprendizaje y Crecimiento	Personal de Negocio y TI competente y motivado	S
	Conocimiento, experiencia e iniciativa para la innovación empresarial	S

Tabla 5.2.3 - Objetivos de TI identificados para objetivo organizacional 6

Objetivo organizacional 11

Perspectiva	Objetivo de TI	Relación Objetivo Organizacional
Financiera	Alineamiento de las tecnologías y estrategia de negocio	P

	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	S
	Materializar beneficios de TI habilitando la inversión y portafolios de servicio	S
Cliente	Entregar servicios de TI alineados con los requerimientos de negocio	P
	Uso adecuado de aplicaciones, información y soluciones tecnológicas	P
Proceso Interno	Agilidad de TI	P
	Optimización de activos, recursos y capacidades de las TI	S
	Capacitación y soporte de procesos de negocio a través de la integración de aplicaciones y tecnología en los procesos empresariales	P
	Disponibilidad de información útil y relevante para la toma de decisiones	S
	Conocimiento, experiencia e iniciativa para la innovación empresarial	S

Tabla 5.2.4 - Objetivos de TI identificados para objetivo organizacional 11

Objetivo organizacional 14

Perspectiva	Objetivo de TI	Relación Objetivo Organizacional
Financiera	Materializar beneficios de TI habilitando la inversión y portafolios de servicio	S
Cliente	Uso adecuado de aplicaciones, información y soluciones tecnológicas	P
Proceso Interno	Agilidad de TI	S
	Optimización de activos, recursos y capacidades de las TI	S
	Capacitación y soporte de procesos de negocio a través de la integración de aplicaciones y tecnología en los procesos empresariales	S

Aprendizaje y Crecimiento	Personal de Negocio y TI competente y motivado	P

Tabla 5.2.5 - Objetivos de TI identificados para objetivo organizacional 14

Objetivo organizacional 16

Perspectiva	Objetivo de TI	Relación Objetivo Organizacional
Financiera	Alineamiento de las tecnologías y estrategia de negocio	S
	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	S
	Riesgos de negocio relacionados con las tecnologías de información gestionadas	S
Cliente	Entregar servicios de TI alineados con los requerimientos de negocio	S
	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S
Proceso Interno	Agilidad de TI	S
Aprendizaje y Crecimiento	Personal de Negocio y TI competente y motivado	P
	Conocimiento, experiencia e iniciativa para la innovación empresarial	S

Tabla 5.2.6 - Objetivos de TI identificados para objetivo organizacional 16

5.2.1 Justificación de Objetivos de TI identificados

Para el cumplimiento de los objetivos organizacionales planteados y alineados al marco de gobierno COBIT 5.0 se identifican los siguientes objetivos de TI de acuerdo a las necesidades reales de la empresa para posteriormente identificar las métricas y procesos habilitadores según el enfoque de seguridad de información.

- Alineamiento de las tecnologías y estrategia de negocio

Se considera este objetivo porque al plantear este proyecto se desea alcanzar el alineamiento estratégico entre objetivos de negocio y tecnologías de información, por ello se debe de realizar la evaluación respectiva en la organización para garantizar su cumplimiento.

- Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI

  Otra razón para establecer gobierno de TI es la iniciativa de involucrar a la alta dirección con las decisiones a nivel de tecnologías. Por ello forma parte de los objetivos planteados para la organización.

- Cumplimiento de TI y soporte para el cumplimiento empresarial de las leyes y regulaciones externas

  Se debe garantizar el cumplimiento regulatorio a todo nivel incluyendo normas que competen a las tecnologías o que sean responsabilidad de la división de TI.

- Materializar beneficios de TI habilitando la inversión y portafolios de servicio

  Continuando con las metas e iniciativas del gobierno de TI se debe garantizar el retorno de las inversiones realizando un seguimiento a los beneficios obtenidos por el uso de tecnologías de información.

- Entregar servicios de TI alineados con los requerimientos de negocio

  Según la perspectiva del cliente, se considera como objetivo la entrega de servicios que tengan como base los requerimientos de negocio como parte de los principios de alineamiento estratégico garantizando la satisfacción de los clientes y otros stakeholders.

- Uso adecuado de aplicaciones, información y soluciones tecnológicas

  Se considera el objetivo pues según las normas de la clínica se debe usar adecuadamente la información de los pacientes, datos internos y garantizar la gestión de aplicaciones y soluciones que soporten procesos organizacionales.

- Seguridad de Información, infraestructura de procesamiento y aplicaciones

  Relacionado con el objetivo anterior, se hace hincapié en garantizar la seguridad de información a nivel organizacional y de la infraestructura de procesamiento debido a las regulaciones y la línea de negocio a seguir. La importancia de este objetivo se ve reforzada por la ley de protección de datos personales.

- Optimización de activos, recursos y capacidades de las TI

  Como parte de los objetivos de negocio que señalan apuntar a la excelencia organizacional por medio de la eficiencia, se requiere por lo tanto la optimización a nivel de tecnología en forma estratégica.

- Capacitación y soporte de procesos de negocio a través de la integración de aplicaciones y tecnología en los procesos empresariales

  Se considera este objetivo debido a la importancia de que las tecnologías de información soporten procesos de negocio de forma estratégica contribuyendo a los principios de alineamiento de gobierno de TI.

- Cumplimiento de las políticas internas por parte de las TI

  Se debe garantizar el cumplimiento de las políticas de TI establecidas en la organización y las que se propondrán luego de la aplicación de políticas de gobierno de TI de acuerdo al enfoque de seguridad de información.

- Personal de Negocio y TI competente y motivado

  Se considera parte de los objetivos de Tecnología de información debido a la importancia del personal o equipo dentro de la organización, lo cual se ve reflejado en los objetivos de negocio. Es fundamental por lo tanto garantizar su motivación y contribuir con el crecimiento de sus competencias.

- Conocimiento, experiencia e iniciativa para la innovación empresarial

  Dado que los objetivos organizacionales reflejan la iniciativa de alcanzar la excelencia a través de un crecimiento estratégico, se considera este objetivo que apunta a la innovación por medio de tecnologías y según la experiencia e iniciativas del personal.

5.3 Identificación de métricas para objetivos de negocio y de TI

A continuación se muestran las métricas sugeridas para los objetivos de negocio. Éstas son referenciales y deberán ser ajustadas para cada escenario real de las empresas prestadoras de servicios de salud.

Objetivos organizacionales

En el documento principal se muestran los respectivos cuadros de mando a emplearse dentro de la organización para la medición de las métricas identificadas.

Perspectiva	Objetivo de Negocio	Métricas
Financiera	Portafolio de productos y servicios competitivos.	• Porcentaje de productos y servicios que alcanzan o exceden los objetivos de ingreso y/o cuota de mercado. • Porcentaje de productos y servicios que alcanzan o exceden los objetivos de satisfacción al cliente. • Porcentaje de productos y servicios que proporcionan ventajas competitivas
	Cumplimiento con leyes y regulaciones externas.	• Costo de incumplimientos regulatorios incluyendo acuerdos y sanciones • Número de incumplimientos regulatorios causantes de comentarios públicos o publicidad negativa • Número de incumplimientos regulatorios en relación con acuerdos contractuales con socios de negocios
Cliente	Cultura de servicio orientada al cliente.	• Número de interrupciones del servicio al cliente debidos a incidentes relacionados con el servicio TI (fiabilidad) • Porcentaje de stakeholders que se encuentran satisfechos con que la entrega del servicio de cliente cumpla con los niveles acordados • Número de quejas de clientes
Proceso Interno	Optimización de las funcionalidades de los procesos de negocio.	• Frecuencia de las evaluaciones de madurez de la capacidad de los procesos de negocio • Niveles de satisfacción del Consejo de Administración y la alta dirección con las

		capacidades de los procesos de negocio
	Operaciones y personal productivo	• Número de programas/proyectos en tiempo y presupuesto • Niveles de costo y de personal comparados al benchmarking
Aprendizaje y crecimiento	Personal motivado y capacitado	• Nivel de satisfacción de los stakeholders con la experiencia y capacidades del personal • Porcentaje de personal cuya capacidad es insuficiente para la competencia requerida por su rol • Porcentaje de personal satisfecho

Tabla 5.3.1 - Métricas para los objetivos organizacionales

Objetivos de TI

Perspectiva	Objetivo de TI	Métricas
Financiera	Alineamiento de las tecnologías y estrategia de negocio	• Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas estratégicas de TI • Nivel de satisfacción de los stakeholders con el alcance del portafolio de programas y servicios planificados • Porcentaje de factores de valor de TI mapeados a factores de valor del negocio
	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	• Porcentaje de roles de la dirección ejecutiva con responsabilidad definida en decisiones TI • Frecuencia de reuniones del comité ejecutivo de estrategia de TI • Tasa de ejecución de decisiones TI por parte de la alta dirección.
	Cumplimiento de TI y soporte para el	• Costo de incumplimiento de TI, incluyendo acuerdos, sanciones e impacto en pérdida

	cumplimiento empresarial de las leyes y regulaciones externas	de reputación • Número de incumplimientos de TI reportados al Consejo de Administración o causantes de comentarios o vergüenza pública • Número de incumplimientos relacionados con proveedores de servicios de TI
	Materializar beneficios de TI habilitando la inversión y portafolios de servicio	• Porcentaje de servicios de TI donde se obtienen los beneficios esperados • Porcentaje de inversiones de TI donde se cumplen o exceden los beneficios esperados
Cliente	Entregar servicios de TI alineados con los requerimientos de negocio	• Número de interrupciones de negocio debidas a incidentes de servicios de TI • Porcentaje de stakeholders satisfechos de que la entrega de servicios de TI cumpla los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios de TI
	Uso adecuado de aplicaciones, información y soluciones tecnológicas	• Porcentaje de propietarios de procesos de negocio satisfechos con el apoyo de productos y servicios de TI • Nivel de entendimiento de los usuarios del negocio sobre cómo las soluciones tecnológicas apoyan sus procesos • Valor presente neto (VPN) mostrando el nivel de satisfacción del negocio con la calidad y utilidad de las soluciones tecnológicas
Proceso Interno	Seguridad de Información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública • Tiempo de concesión, cambio y eliminación de privilegios de acceso comparado con los niveles de servicio

		acordados • Frecuencia de las evaluaciones de seguridad en relación a los últimos estándares y guías
	Optimización de activos, recursos y capacidades de las TI	• Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costos • Niveles de satisfacción de la alta dirección y de la división de TI con los costos y capacidades TI
	Capacitación y soporte de procesos de negocio a través de la integración de aplicaciones y tecnología en los procesos empresariales	• Número de incidentes del procesamiento de negocio causados por errores de integración de la tecnología • Número de programas de negocio facilitados por TI retrasados o incurriendo en costos adicionales debido a problemas de integración de la tecnología • Número de aplicaciones o infraestructuras críticas operando aisladamente y no integradas
	Cumplimiento de las políticas internas por parte de las TI	• Número de incidentes relacionados con el incumplimiento de políticas • Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas • Frecuencia de revisión y actualización de políticas
Aprendizaje y crecimiento	Personal de Negocio y TI competente y motivado	• Porcentaje de personal cuyas habilidades de TI son suficientes para la competencia requerida por sus roles • Porcentaje de personal satisfecho con sus roles en TI • Número de horas de aprendizaje/formación por miembro del personal
	Conocimiento, experiencia e	• Nivel de concienciación y comprensión de la alta dirección del negocio sobre las

	iniciativa para la innovación empresarial	posibilidades de Innovación de TI • Nivel de satisfacción de los stakeholders con los niveles de experiencia e ideas de innovación de TI • Número de iniciativas aprobadas resultantes de ideas de TI innovadoras

Tabla 5.3.2 - Métricas para objetivos de TI

ANEXO F: Análisis de procesos de COBIT 5.0 a aplicar a la organización

6.1 Mapeo de objetivos de TI y sus procesos habilitadores

A continuación se presentan los objetivos de TI identificados y su relación con los procesos habilitadores propuestos por COBIT.

Objetivo de TI: Alineamiento de las tecnologías y estrategia de negocio

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno	P
	Garantizar la entrega de beneficios	P
	Garantizar la optimización de riesgos	S
	Garantizar la optimización de recursos	S
	Garantizar la transparencia de los stakeholders	S
Alinear, Planear y Organizar	Gestionar el marco de control de TI	P
	Gestionar la estrategia	P
	Gestionar la arquitectura empresarial	P
	Gestionar el portafolio	P
	Gestionar los recursos humanos	P
	Gestionar las relaciones	P
	Gestionar la innovación	S
	Gestionar el costo y el presupuesto	S
	Gestionar los acuerdos de servicio	S
	Gestionar la calidad	S
Construir, adquirir e implementar	Gestionar programas y proyectos	P
	Gestionar la definición de requisitos	P
	Gestionar la identificación y construcción de soluciones	S
	Gestionar la habilitación de cambios organizacionales	S
	Gestionar el conocimiento	S

Entregar, dar servicio y soporte	Gestionar la continuidad	S
	Gestionar los servicios de seguridad	S
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	S

Tabla 6.1.1 - Procesos habilitadores según Objetivo de TI 1

Objetivo de TI: Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno	P
	Garantizar la entrega de beneficios	S
	Garantizar la optimización de riesgos	S
	Garantizar la optimización de recursos	S
	Garantizar la transparencia de los stakeholders	P
Alinear, Planear y Organizar	Gestionar el marco de control de TI	S
	Gestionar la estrategia	S
	Gestionar la arquitectura empresarial	S
	Gestionar el portafolio	S
	Gestionar el costo y el presupuesto	S
	Gestionar los recursos humanos	S
	Gestionar las relaciones	S
Construir, adquirir e implementar	Gestionar programas y proyectos	S
	Gestionar la definición de requisitos	S
	Gestionar la habilitación de cambios organizacionales	S
	Gestionar el cambio	S
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	S

Tabla 6.1.2 - Procesos habilitadores según Objetivo de TI 2

Objetivo de TI: Cumplimiento de TI y soporte para el cumplimiento empresarial de las leyes y regulaciones externas

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno	S
	Garantizar la optimización de riesgos	S
	Garantizar la transparencia de los stakeholders	S
Alinear, Planear y Organizar	Gestionar el marco de control de TI	P
	Gestionar los recursos humanos	S
	Gestionar proveedores	S
	Gestionar la calidad	S
	Gestionar el riesgo	P
	Gestionar la seguridad	P
Construir, adquirir e implementar	Gestionar la definición de requisitos	S
	Gestionar los activos	S
	Gestionar la configuración	P
Entregar, dar servicio y soporte	Gestionar las operaciones	S
	Gestionar los problemas	S
	Gestionar la continuidad	S
	Gestionar los servicios de seguridad	P
	Gestionar los controles de los procesos de negocio	S
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	S
	Monitorear, evaluar y medir el sistema de control interno	P
	Monitorear, evaluar y medir el cumplimiento de los requerimientos externos	P

Tabla 6.1.3 - Procesos habilitadores según Objetivo de TI 3

Objetivo de TI: Materializar beneficios de TI habilitando la inversión y portafolios de servicio

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno	S
	Garantizar la entrega de beneficios	P
	Garantizar la optimización de recursos	S
Alinear, Planear y Organizar	Gestionar la estrategia	S
	Gestionar la arquitectura empresarial	S
	Gestionar la innovación	P
	Gestionar el portafolio	P
	Gestionar el costo y el presupuesto	P
	Gestionar las relaciones	S
	Gestionar los acuerdos de servicio	S
	Gestionar proveedores	S
	Gestionar la calidad	P
Construir, adquirir e implementar	Gestionar programas y proyectos	P
	Gestionar la definición de requisitos	S
	Gestionar la identificación y construcción de soluciones	S
	Gestionar la disponibilidad y capacidad	S
	Gestionar la habilitación de cambios organizacionales	S
	Gestionar el cambio	S
	Gestionar la aceptación de cambio y la transición	S
	Gestionar el conocimiento	S
Entregar, dar servicio y soporte	Gestionar las operaciones	S
	Gestionar los problemas	S
	Gestionar la continuidad	S
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	S

	Monitorear, evaluar y medir el cumplimiento de los requerimientos externos	S

Tabla 6.1.4 - Procesos habilitadores según Objetivo de TI 4

Objetivo de TI: Entregar servicios de TI alineados con los requerimientos de negocio

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno	P
	Garantizar la entrega de beneficios	P
	Garantizar la optimización de riesgos	S
	Garantizar la optimización de recursos	S
	Garantizar la transparencia de los stakeholders	P
Alinear, Planear y Organizar	Gestionar el marco de control de TI	S
	Gestionar la estrategia	P
	Gestionar la arquitectura empresarial	S
	Gestionar el portafolio	S
	Gestionar el costo y el presupuesto	S
	Gestionar los recursos humanos	S
	Gestionar las relaciones	P
	Gestionar los acuerdos de servicio	P
	Gestionar proveedores	P
	Gestionar la calidad	P
	Gestionar el riesgo	S
	Gestionar la seguridad	S
Construir, adquirir e implementar	Gestionar programas y proyectos	S
	Gestionar la definición de requisitos	P
	Gestionar la identificación y construcción de soluciones	P
	Gestionar la disponibilidad y capacidad	P
	Gestionar la habilitación de cambios organizacionales	S

	Gestionar el cambio	P
	Gestionar la aceptación de cambio y la transición	S
	Gestionar el conocimiento	S
	Gestionar los activos	S
Entregar, dar servicio y soporte	Gestionar las operaciones	P
	Gestionar solicitudes de servicios e incidentes	P
	Gestionar los problemas	P
	Gestionar la continuidad	P
	Gestionar los servicios de seguridad	S
	Gestionar los controles de los procesos de negocio	P
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	P
	Monitorear, evaluar y medir el sistema de control interno	S
	Monitorear, evaluar y medir el cumplimiento de los requerimientos externos	S

Tabla 6.1.5 - Procesos habilitadores según Objetivo de TI 5

Objetivo de TI: Uso adecuado de aplicaciones, información y soluciones tecnológicas

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar la entrega de beneficios	S
	Garantizar la optimización de riesgos	S
	Garantizar la optimización de recursos	S
Alinear, Planear y Organizar	Gestionar la estrategia	S
	Gestionar la arquitectura empresarial	S
	Gestionar la innovación	P
	Gestionar el portafolio	S
	Gestionar el costo y el presupuesto	S
	Gestionar las relaciones	S

	Gestionar los acuerdos de servicio	S
	Gestionar proveedores	S
	Gestionar la calidad	S
	Gestionar el riesgo	S
	Gestionar la seguridad	S
Construir, adquirir e implementar	Gestionar programas y proyectos	S
	Gestionar la definición de requisitos	S
	Gestionar la identificación y construcción de soluciones	S
	Gestionar la disponibilidad y capacidad	S
	Gestionar la habilitación de cambios organizacionales	P
	Gestionar el cambio	S
	Gestionar la aceptación de cambio y la transición	P
	Gestionar el conocimiento	S
	Gestionar la configuración	S
Entregar, dar servicio y soporte	Gestionar las operaciones	S
	Gestionar solicitudes de servicios e incidentes	S
	Gestionar los problemas	S
	Gestionar la continuidad	S
	Gestionar los servicios de seguridad	S
	Gestionar los controles de los procesos de negocio	S
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	S
	Monitorear, evaluar y medir el sistema de control interno	S

Tabla 6.1.6 -Procesos habilitadores según Objetivo de TI 6

Objetivo de TI: Seguridad de Información, infraestructura de procesamiento y aplicaciones

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno	S
	Garantizar la optimización de riesgos	P
Alinear, Planear y Organizar	Gestionar el marco de control de TI	S
	Gestionar la arquitectura empresarial	S
	Gestionar los recursos humanos	S
	Gestionar los acuerdos de servicio	S
	Gestionar proveedores	S
	Gestionar el riesgo	P
	Gestionar la seguridad	P
Construir, adquirir e implementar	Gestionar la definición de requisitos	S
	Gestionar el cambio	P
	Gestionar el conocimiento	S
	Gestionar los activos	S
	Gestionar la configuración	S
Entregar, dar servicio y soporte	Gestionar las operaciones	S
	Gestionar solicitudes de servicios e incidentes	S
	Gestionar la continuidad	S
	Gestionar los controles de los procesos de negocio	S
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	S
	Monitorear, evaluar y medir el sistema de control interno	S
	Monitorear, evaluar y medir el cumplimiento de los requerimientos externos	S

Tabla 6.1.7 - Procesos habilitadores según Objetivo de TI 7

Objetivo de TI: Optimización de activos, recursos y capacidades de las TI

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno	S
	Garantizar la entrega de beneficios	S
	Garantizar la optimización de recursos	P
Alinear, Planear y Organizar	Gestionar el marco de control de TI	P
	Gestionar la estrategia	S
	Gestionar la arquitectura empresarial	P
	Gestionar la innovación	P
	Gestionar el portafolio	S
	Gestionar el costo y el presupuesto	S
	Gestionar los recursos humanos	P
	Gestionar las relaciones	S
	Gestionar los acuerdos de servicio	S
	Gestionar proveedores	S
	Gestionar la calidad	S
Construir, adquirir e implementar	Gestionar programas y proyectos	S
	Gestionar la definición de requisitos	S
	Gestionar la identificación y construcción de soluciones	S
	Gestionar la disponibilidad y capacidad	P
	Gestionar la habilitación de cambios organizacionales	S
	Gestionar el cambio	S
	Gestionar el conocimiento	S
	Gestionar los activos	P
	Gestionar la configuración	P
Entregar, dar servicio y soporte	Gestionar las operaciones	P
	Gestionar los problemas	P
	Gestionar la continuidad	S
	Gestionar los servicios de seguridad	S

	Gestionar los controles de los procesos de negocio	S
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	P

Tabla 6.1.8 - Procesos habilitadores según Objetivo de TI 8

Objetivo de TI: Capacitación y soporte de procesos de negocio a través de la integración de aplicaciones y tecnología en los procesos empresariales

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno	S
	Garantizar la entrega de beneficios	S
Alinear, Planear y Organizar	Gestionar el marco de control de TI	S
	Gestionar la estrategia	S
	Gestionar la arquitectura empresarial	S
	Gestionar la innovación	S
	Gestionar las relaciones	P
Construir, adquirir e implementar	Gestionar la definición de requisitos	P
	Gestionar la identificación y construcción de soluciones	S
	Gestionar la habilitación de cambios organizacionales	S
	Gestionar el cambio	S
	Gestionar la aceptación de cambio y la transición	P
Entregar, dar servicio y soporte	Gestionar los problemas	S
	Gestionar la continuidad	S
	Gestionar los servicios de seguridad	S
	Gestionar los controles de los procesos de negocio	S

Tabla 6.1.9 -Procesos habilitadores según Objetivo de TI 9

Objetivo de TI: Cumplimiento de las políticas internas por parte de las TI

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno	S
	Garantizar la optimización de riesgos	P
	Garantizar la transparencia de los stakeholders	S
Alinear, Planear y Organizar	Gestionar el marco de control de TI	P
	Gestionar la estrategia	S
	Gestionar los recursos humanos	S
	Gestionar las relaciones	S
	Gestionar los acuerdos de servicio	S
	Gestionar proveedores	S
	Gestionar la calidad	S
	Gestionar el riesgo	S
Construir, adquirir e implementar	Gestionar el cambio	S
	Gestionar la aceptación de cambio y la transición	S
	Gestionar los activos	S
	Gestionar la configuración	S
Entregar, dar servicio y soporte	Gestionar las operaciones	S
	Gestionar solicitudes de servicios e incidentes	S
	Gestionar los problemas	S
	Gestionar la continuidad	S
	Gestionar los servicios de seguridad	S
	Gestionar los controles de los procesos de negocio	S
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	P
	Monitorear, evaluar y medir el sistema de control interno	P

	Monitorear, evaluar y medir el cumplimiento de los requerimientos externos	S

Tabla 6.1.10 - Procesos habilitadores según Objetivo de TI 10

Objetivo de TI: Personal de Negocio y TI competente y motivado

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno	S
	Garantizar la entrega de beneficios	S
	Garantizar la optimización de riesgos	S
	Garantizar la optimización de recursos	P
Alinear, Planear y Organizar	Gestionar el marco de control de TI	P
	Gestionar la estrategia	S
	Gestionar los recursos humanos	P
	Gestionar las relaciones	S
	Gestionar la calidad	S
	Gestionar el riesgo	S
Construir, adquirir e implementar	Gestionar programas y proyectos	S
	Gestionar el conocimiento	S
Entregar, dar servicio y soporte	Gestionar las operaciones	S
	Gestionar la continuidad	S
	Gestionar los controles de los procesos de negocio	S
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	S

Tabla 6.1.11 - Procesos habilitadores según Objetivo de TI 11

Objetivo de TI: Conocimiento, experiencia e iniciativa para la innovación empresarial

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno	S
	Garantizar la entrega de beneficios	P
	Garantizar la optimización de riesgos	S
	Garantizar la optimización de recursos	S
	Garantizar la transparencia de los stakeholders	S
Alinear, Planear y Organizar	Gestionar el marco de control de TI	P
	Gestionar la estrategia	P
	Gestionar la arquitectura empresarial	S
	Gestionar la innovación	P
	Gestionar el portafolio	S
	Gestionar los recursos humanos	P
	Gestionar las relaciones	P
	Gestionar proveedores	S
	Gestionar la calidad	S
	Gestionar el riesgo	S
Construir, adquirir e implementar	Gestionar programas y proyectos	S
	Gestionar la definición de requisitos	S
	Gestionar la identificación y construcción de soluciones	S
	Gestionar la disponibilidad y capacidad	S
	Gestionar la habilitación de cambios organizacionales	P
	Gestionar el cambio	S
	Gestionar la aceptación de cambio y la transición	S
	Gestionar el conocimiento	P
Entregar, dar servicio y soporte	Gestionar las operaciones	S
	Gestionar solicitudes de servicios e incidentes	S

	Gestionar los problemas	S
	Gestionar la continuidad	S
	Gestionar los controles de los procesos de negocio	S
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	S
	Monitorear, evaluar y medir el sistema de control interno	S
	Monitorear, evaluar y medir el cumplimiento de los requerimientos externos	S

Tabla 6.1.12 - Procesos habilitadores según Objetivo de TI 12

6.1.1 Justificación de procesos habilitadores

Dentro de la organización se debe tomar en cuenta únicamente aquellos procesos habilitadores que correspondan con la línea de negocio y con su situación, en otras palabras su entorno actual, regulaciones a las cuales están sujetos y hacia dónde se quiera llegar según el plan estratégico vigente y sus planes de TI.

Por esta razón, según la relación principal y secundaria para cada uno de los objetivos de TI y su respectivo proceso habilitador. A nivel general aplican los siguientes procesos habilitadores de COBIT 5.0

Dominio	Proceso Habilitador
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno
	Garantizar la entrega de beneficios
	Garantizar la optimización de riesgos
	Garantizar la optimización de recursos
Alinear, Planear y Organizar	Gestionar el marco de control de TI
	Gestionar la estrategia
	Gestionar la innovación
	Gestionar el portafolio

	Gestionar el costo y el presupuesto
	Gestionar los recursos humanos
	Gestionar los acuerdos de servicio
	Gestionar proveedores
	Gestionar la calidad
	Gestionar el riesgo
	Gestionar la seguridad
Construir, adquirir e implementar	Gestionar programas y proyectos
	Gestionar la definición de requisitos
	Gestionar la disponibilidad y capacidad
	Gestionar la habilitación de cambios organizacionales
	Gestionar el cambio
	Gestionar la aceptación de cambio y la transición
	Gestionar los activos
	Gestionar la configuración
Entregar, dar servicio y soporte	Gestionar las operaciones
	Gestionar solicitudes de servicios e incidentes
	Gestionar la continuidad
	Gestionar los servicios de seguridad
	Gestionar los controles de los procesos de negocio
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad
	Monitorear, evaluar y medir el sistema de control interno
	Monitorear, evaluar y medir el cumplimiento de los requerimientos externos

Tabla 6.1.13 - Aplicación de procesos habilitadores según la organización

- **Dominio Evaluar, Dirigir y Monitorear**

  Este dominio contiene a grandes rasgos los procesos que constituyen los cinco (5) pilares del gobierno. No obstante, dentro de la organización se consideran únicamente cuatro (4) según la priorización. Esto se debe a que la transparencia y relaciones de los stakeholders no es únicamente responsabilidad de la empresa sino también a nivel de la cadena de aseguradoras y otros actores cuyo nivel de impacto sería muy elevado y debería ser tomado en cuenta a largo plazo según la aceptación de esta iniciativa y los resultados iniciales.

- **Dominio Alinear, Planear y Organizar**

  Se consideran dentro de la organización once (11) procesos habilitadores de los trece (13) planteados por COBIT 5.0 según la prioridad. En el caso de la gestión de relaciones no es considerada por un motivo similar al del proceso transparencia de los stakeholders pues primero debe de consolidarse la iniciativa para fortalecerla y comunicarla progresivamente dentro de toda la organización y externos. En el caso de la gestión de la arquitectura empresarial, no es considerada debido a que se plantea realizar el seguimiento a partir del proceso garantizar la optimización del recursos dado que toda la infraestructura técnica ha sido recientemente cambiada y según la organización siguiendo medidas tanto internas como externas.

- **Dominio Construir, Adquirir e Implementar**

  Se consideran en el caso de este dominio ocho (8) de los diez (10) procesos habilitadores contemplados en COBIT 5.0. El proceso de la identificación y construcción de soluciones no se considera debido a que un tema técnico, lo cual actualmente no es uno de los enfoques que la organización desee reforzar. En cuanto a la gestión del conocimiento, no aplica según la prioridad y debido a la resistencia al cambio dentro de estos temas, por lo cual su gestión será a través de otro proceso habilitador y considerado posiblemente en algún trabajo futuro u otra iteración de gobierno según la necesidad de la organización.

- **Dominio Entregar, Dar servicio y soporte**

  En el caso de este dominio, aplican cinco (5) de los seis (6) procesos propuestos en COBIT. Se deja fuera de aplicación la Gestión de problemas debido a que la actual mesa de ayuda no contempla estos conceptos directamente, sino que está incluido dentro de la gestión de incidentes, por lo cual la aplicación de este proceso quedaría pendiente en otra iteración según las políticas y buenas prácticas que requiera adoptar la organización.

- **Dominio Monitorear, Evaluar y Asegurar**

  Para este dominio aplican todos los procesos habilitadores a la cultura de la organización, no obstante, en el caso de Monitorear, evaluar y medir el sistema de control interno se hace la acotación que dentro de la organización se planteó un mecanismo de gobierno y control a partir de COBIT 4.1, por lo cual parte de este proyecto consistiría en realizar el upgrade a COBIT 5.0 según seguridad de

información con un enfoque más corporativo que el planteado en la anterior versión del marco. No obstante, se debe de realizar la evaluación que determine si las políticas de COBIT 4.1 han sido aplicadas o no, pues de lo contrario este modelo sería la primera iniciativa en temas de control interno y gobierno, la cual podría apoyarse en otros marcos y formalizar dentro de la organización dicha división que vele por el cumplimiento de las políticas internas y regulaciones.

6.2 Objetivos de seguridad de información y regulaciones identificados.

Se muestra en las siguientes tablas los objetivos relacionados con la seguridad de información y regulaciones externas e internas debido al enfoque del gobierno de TI. Se muestra la lista de procesos habilitadores de relación principal ('P').

Seguridad de Información, infraestructura de procesamiento y aplicaciones

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar la optimización de riesgos	P
Alinear, Planear y Organizar	Gestionar el riesgo	P
	Gestionar la seguridad	P
Construir, adquirir e implementar	Gestionar el cambio	P

Tabla 6.2.1 - Procesos habilitadores Objetivo de TI 7. Resumen

Cumplimiento de TI y soporte para el cumplimiento empresarial de las leyes y regulaciones externas

Dominio	Proceso	Relación
Alinear, Planear y Organizar	Gestionar el marco de control de TI	P
	Gestionar el riesgo	P
	Gestionar la seguridad	P
Construir, adquirir e implementar	Gestionar la configuración	P
Entregar, dar servicio	Gestionar los servicios de seguridad	P

y soporte		
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el sistema de control interno	P
	Monitorear, evaluar y medir el cumplimiento de los requerimientos externos	P

Tabla 6.2.2 - Procesos habilitadores Objetivo de TI 3. Resumen

Cumplimiento de las políticas internas por parte de las TI

Dominio	Proceso	Relación
Evaluar, Dirigir y Monitorear	Garantizar la optimización de riesgos	P
Alinear, Planear y Organizar	Gestionar el marco de control de TI	P
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad	P
	Monitorear, evaluar y medir el sistema de control interno	P

Tabla 6.2.3 - Procesos habilitadores Objetivo de TI 10. Resumen

6.2.1 Justificación de los procesos habilitadores bajo el enfoque de seguridad de información

Para cada uno de los procesos habilitadores seleccionados se plantea una justificación de su elección tomando en cuenta que se realizará la adaptación para la seguridad de información y a partir del análisis de cada uno de estos y sus respectivas actividades nacerán las políticas y roles a implantar en la organización tomando como base los procesos escogidos para su optimización según el enfoque.

- Garantizar el mantenimiento y configuración del marco de control de gobierno

  Se toma en cuenta este proceso debido a que se debe de gestionar durante todo el ciclo de vida de gobierno el marco que otorga los lineamientos para su implementación dentro de la organización de manera que en caso se tomen otros enfoques para el gobierno o que se modifiquen los procesos o regulaciones en el

ámbito de la seguridad de información se realice la revisión respectiva para ajustar las políticas y actualizarlas según el negocio.

- Garantizar la entrega de beneficios

  A partir del enfoque de seguridad de información se debe garantizar o asegurar que las políticas y proyectos tengan el retorno de inversión esperada tanto para la organización como para los stakeholders.

- Garantizar la optimización de riesgos

  Este proceso es tomado en cuenta debido a que a partir de él se van a identificar los riesgos que puedan dañar a la organización e impedir el logro de sus objetivos y se establecerán las métricas para determinar los riesgos de seguridad principales y como la organización responde ante ellos.

- Gestionar el marco de control de TI

  Este proceso del dominio APO se toma en cuenta debido a que el marco de gobierno que desciende al marco de control de TI, en este caso COBIT 5.0 debe ser constantemente gestionado bajo el enfoque de la organización (seguridad de información) para garantizar el alineamiento de las TI con los objetivos de la empresa y el cumplimiento de las políticas de seguridad.

- Gestionar la estrategia

  Se debe tomar en cuenta el siguiente proceso debido a que se debe de gestionar la estrategia de seguridad planteada y determinar el alineamiento con la organización, la regulación y que las nuevas políticas ayuden al cumplimiento del plan estratégico organizacional y que se materialicen los beneficios y mejoras.

- Gestionar los recursos humanos

  Los recursos humanos son parte importante de la organización, por lo tanto bajo el enfoque de la seguridad de información se debe garantizar la concientización en estos temas y plantear políticas en torno al personal y el trato que deben dar a la información y activos a los que tienen acceso.

- Gestionar el riesgo

  Se debe gestionar a lo largo del ciclo de vida de gobierno los riesgos de seguridad planteados inicialmente de manera que se realicen las correcciones y ajustes oportunos según el negocio y las tendencias dentro del entorno organizacional.

- Gestionar la seguridad

  Se debe garantizar la gestión de la seguridad a nivel organizacional y que se tome en cuenta los riesgos identificados para la elaboración del plan de seguridad de la organización que puede estar alineado a normas vigentes como la ISO/IEC 27001 adoptando los controles de la norma ISO/IEC 27002 adoptando los lineamientos de normas internacionales sin olvidar las regulaciones en cuanto a seguridad.

- Gestionar los programas y proyectos

  Se debe tomar en cuenta le gestión de programas y proyectos organizacionales a nivel de seguridad de información para garantizar que éstos se encuentren alineados con lo que la organización requiere y se encuentra obligada a cumplir desde esta perspectiva, tal como la ley de protección de datos personales, lo cual indica que ningún proyecto futuro y pasado debe dejar escapar estos lineamientos.

- Gestionar el cambio

  El programa de gobierno a implementar trae con él una serie de cambios que deberán ser gestionados. A nivel de la seguridad de información, el marco propone la creación de nuevos roles y adopción de políticas que deberán ser introducidas a la organización en forma progresiva, razón por la cual, los planes del cambio deberán estar actualizados y gestionados de manera de lograr la aceptación y reducir la resistencia al cambio frente a este tipo de proyectos.

- Gestionar los activos

  Se considera la gestión de los activos de la organización bajo el enfoque de seguridad debido a que se deberán de cumplir políticas para mitigar los riesgos producto de las vulnerabilidades en cada uno de éstos activos que brindan soporte a los procesos de negocio y a los procesos tomados como base para la implementación del gobierno de TI.

- Gestionar las solicitudes de servicios e incidentes

  Este proceso, pese a ser parte de la entrega de servicios es considerado debido a que se debe de optimizar la gestión de incidentes de seguridad de información y tener un historial de problemas comunes que puedan dañar activos o que amenacen los datos confidenciales de la organización.

- Gestionar la continuidad

  La gestión de la continuidad forma parte de los procesos habilitadores porque se busca garantizar la disponibilidad de la información, el cual es uno de los pilares de seguridad. Para esto será necesario identificar procesos críticos a proteger de manera de que en caso exista alguna interrupción los tiempos de recuperación sean óptimos para evitar pérdidas económicas y la insatisfacción de los clientes.

- Gestionar los servicios de seguridad

  Se debe garantizar la gestión de los servicios de seguridad y las políticas planteadas según las metas organizacionales y estratégicas, de manera que se asegure una entrega de servicios de seguridad de calidad y que tomen en cuenta las políticas que incluso a lo largo del ciclo de gobierno podrían ir siendo cambiadas dado factores internos o externos.

- Monitorear, evaluar y medir el rendimiento y la conformidad

  Se debe de plantear métricas y documentos que sean input para los procesos relacionados con el control interno y el cumplimiento con requerimientos externos. Estas métricas deberán ser gestionadas y evaluadas para garantizar su conformidad o modificarlas en caso no se vean resultados claros y precisos a través de ellas durante el ciclo de gobierno.

- Monitorear, evaluar y medir el cumplimiento de los requerimientos externos

  Bajo este proceso habilitador, se gestionará y medirá cual es el nivel de cumplimiento con las leyes como la ley de protección de datos personales y otros requerimientos que pueden ser definidos por los stakeholders. A partir de este proceso se darán los inputs y medidas para realizar la evaluación y control del cumplimiento.

ANEXO G: Identificación y diseño de procesos AS - IS

En el presente anexo se muestran los sub-procesos de cada proceso por niveles.

7.1 Proceso: Admisión de pacientes

Sub-proceso nivel 2: Referenciar a otro centro

El siguiente sub-proceso es iniciado según la capacidad resolutiva del paciente o en caso se requiera una transferencia administrativa, lo cual es el trigger para el inicio. Se tiene como actor externo al paciente y al médico del centro de referencia destino.

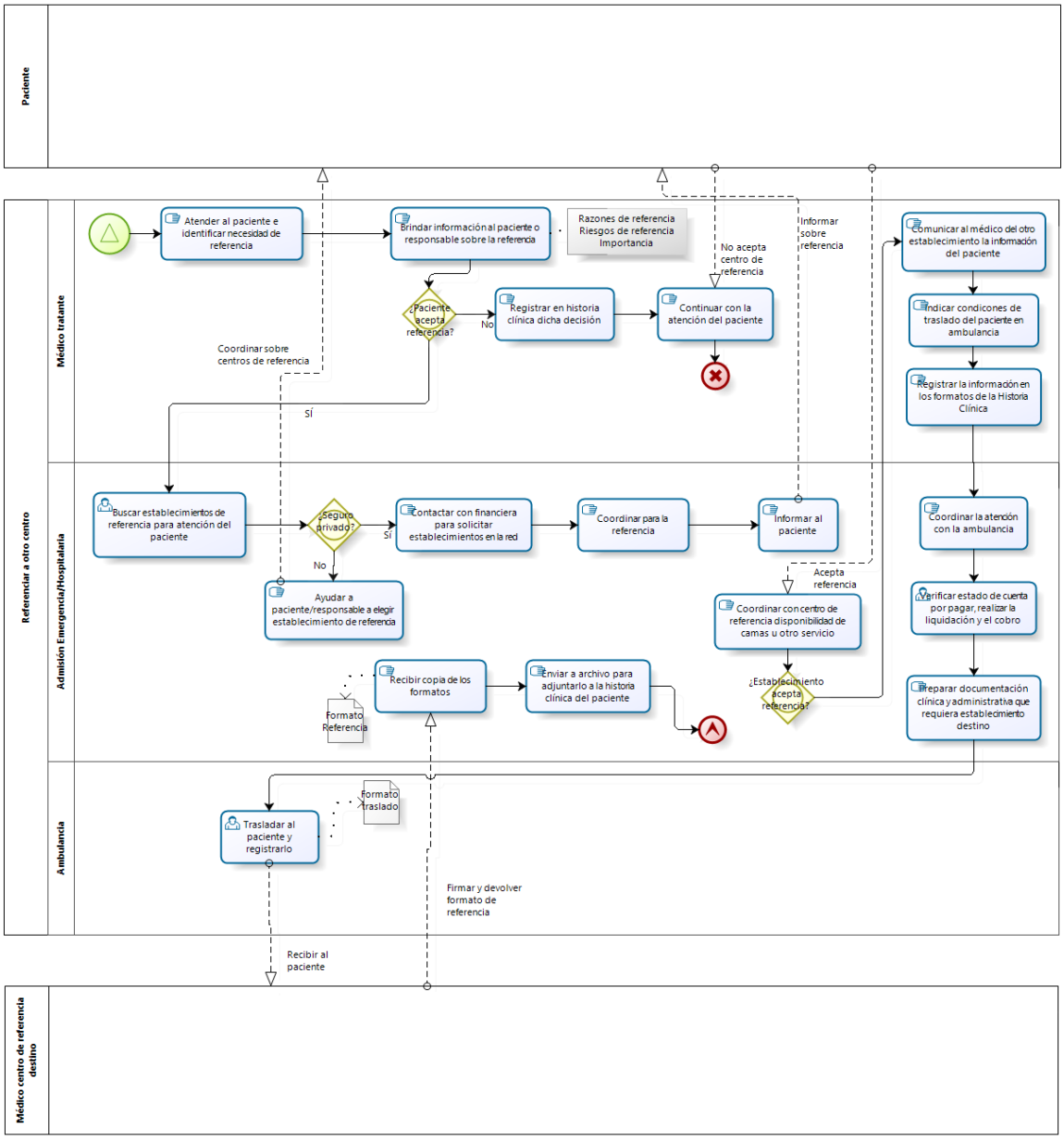


Figura 7.1.1 - Diagrama sub-proceso referenciar a otro centro

Sub-proceso nivel 2: Asignar camas en caso de no disponibilidad

El siguiente sub-proceso es iniciado bajo la condición de que existe una órden previa de hospitalización, por lo tanto se verifica nuevamente la disponibilidad de camas o de lo contrario se deriva a otra sede de la clínica. Así mismo, se observala iteracción con dos actores externos, el paciente y el call center de su aseguradora para validar la cobertura y grupo de opciones con las cuales trabaja para realizar el traslado.

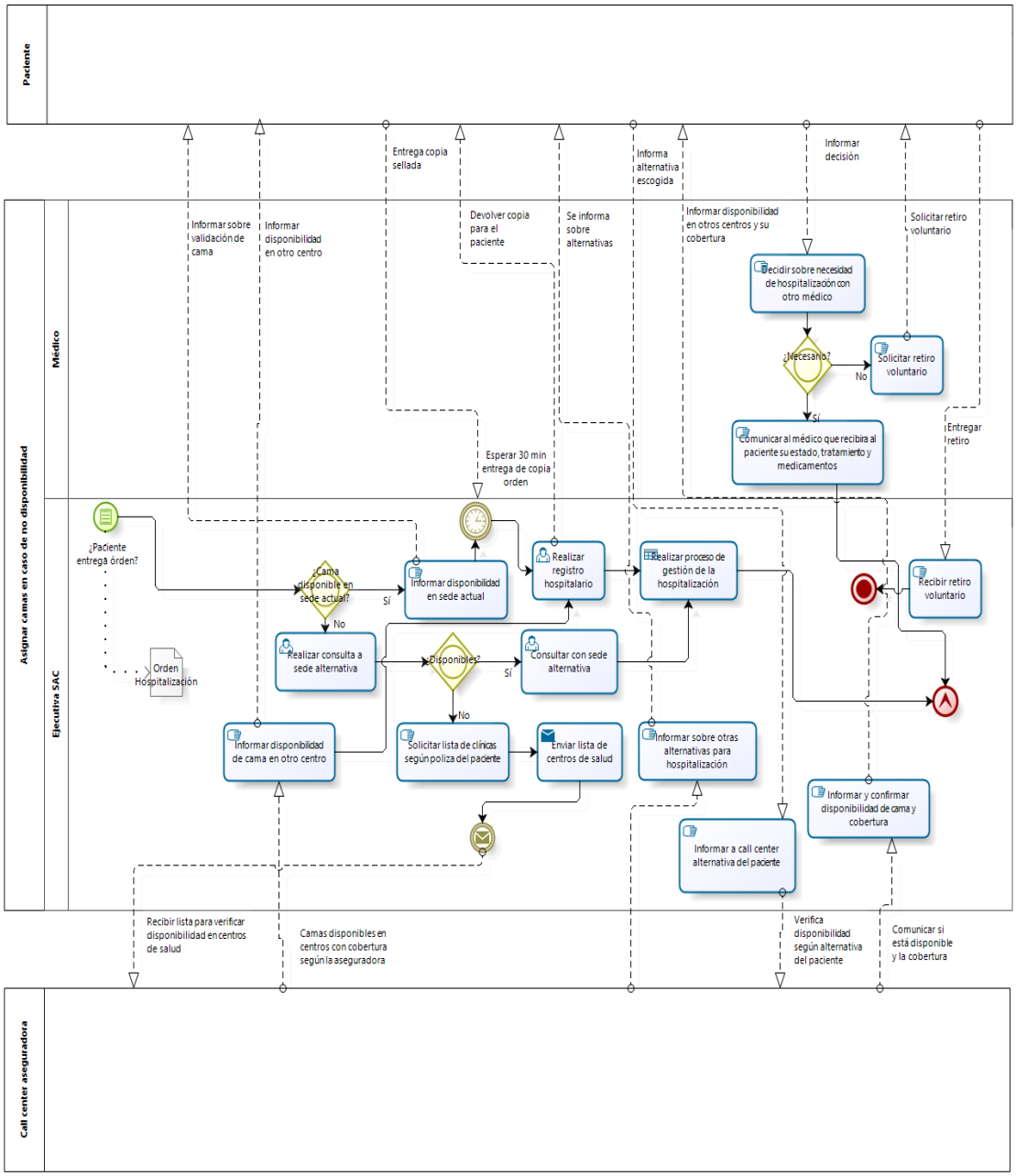


Figura 7.1.2 - Diagrama del sub-proceso asignar camas en caso de no disponibilidad

Sub-proceso nivel 2: Gestionar Cobertura y presupuesto

Este sub-proceso consta de la validación realizada para determinar el presupuesto de la hospitalización del paciente, y en caso esté asegurado proceder a validar la cobertura y la emisión de las cartas de garantía. Se tiene como actores externos al paciente y a la ejecutiva de cartas de garantía de otras aseguradoras distintas a RIMAC.

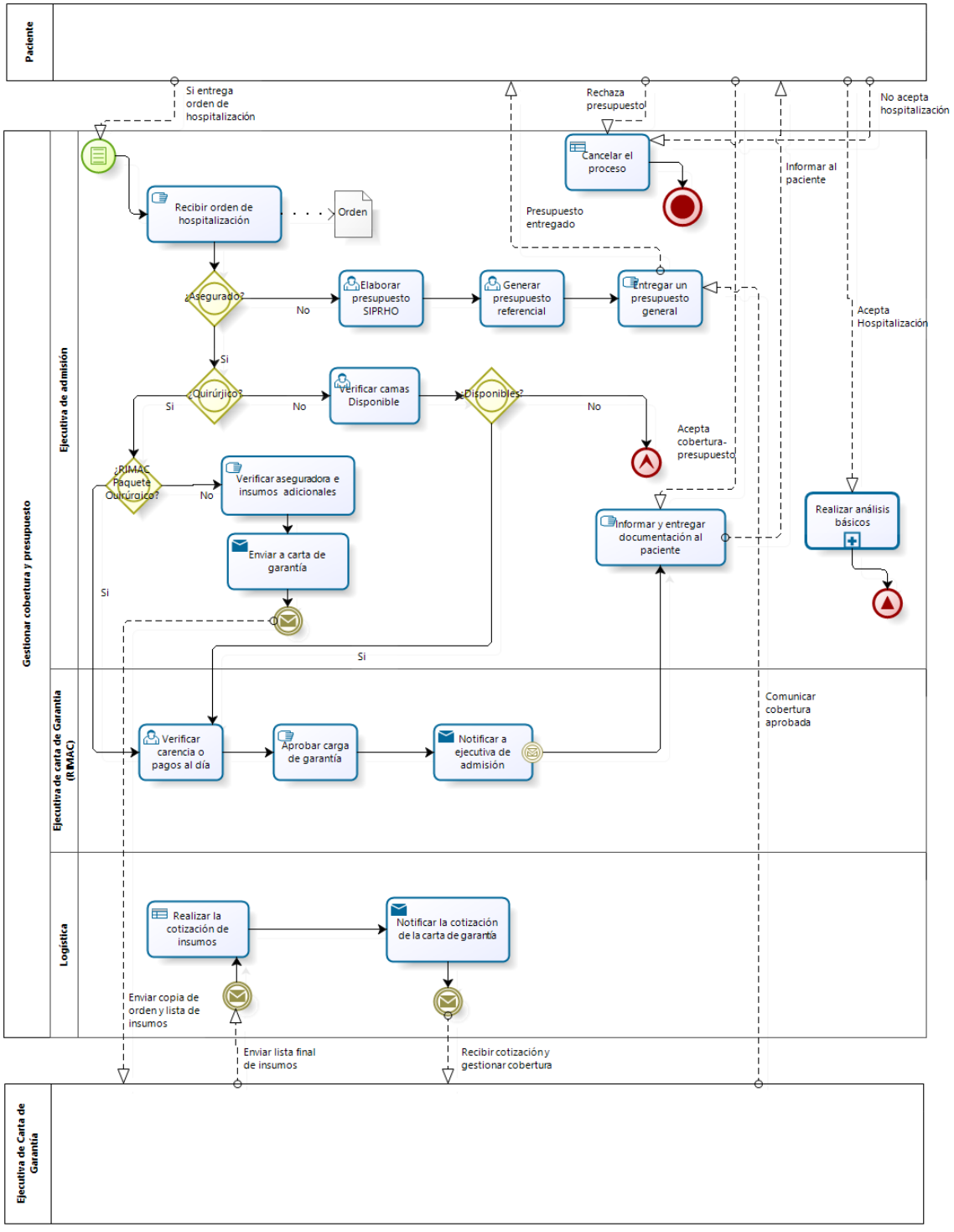


Figura 7.1.3 - Diagrama del sub-proceso gestionar cobertura y presupuesto

Sub-proceso nivel 3: Realizar análisis básicos

Este sub-proceso es iniciado según la derivación a plataforma del paciente luego de la cobertura y presupuesto y proceder con los análisis básicos según el motivo de la hospitalización.

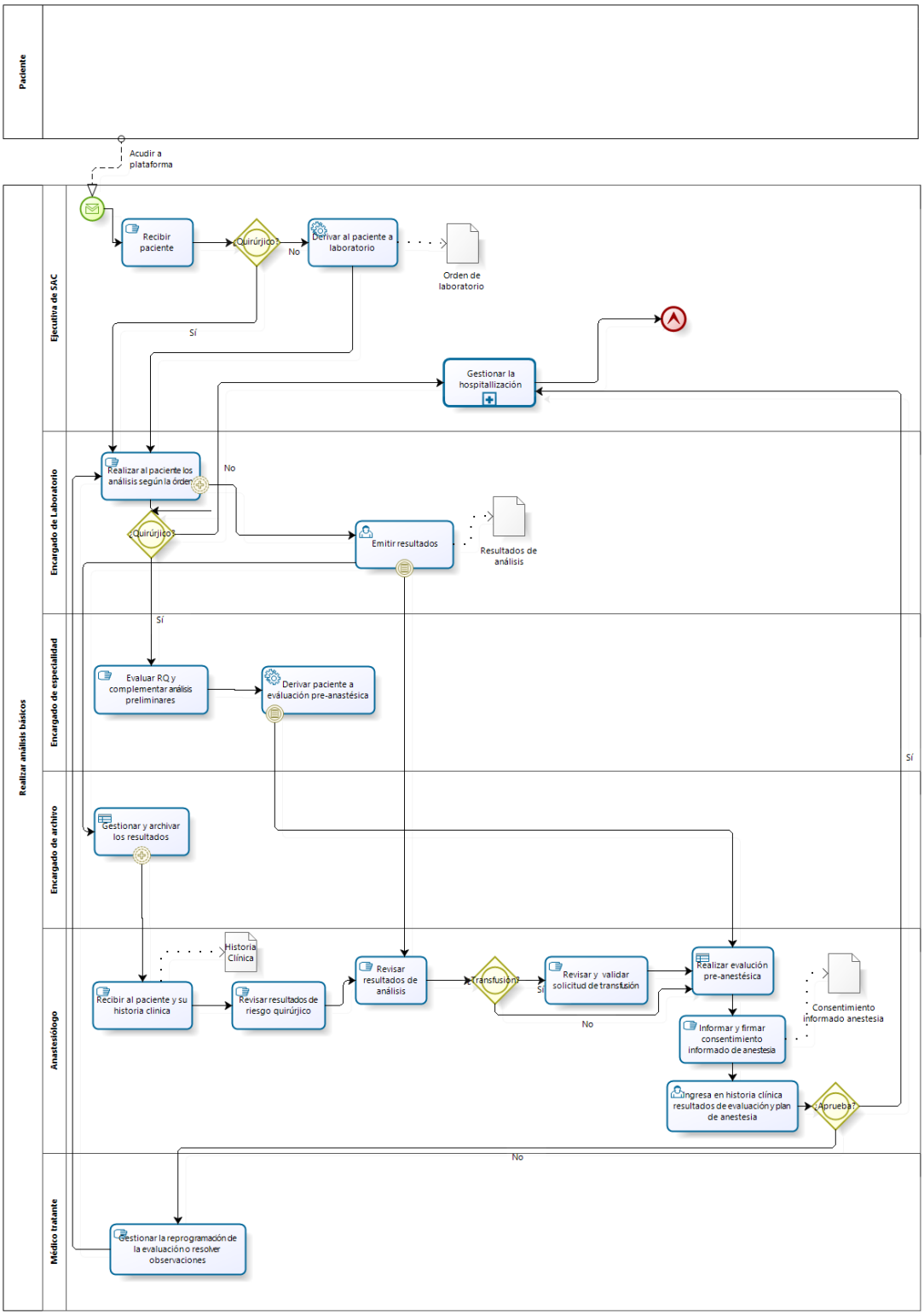


Figura 7.1.4 - Diagrama del sub-proceso realizar análisis básicos

Sub-proceso nivel 4: Gestionar la hospitalización

Finalmente se tiene el sub-proceso de último nivel, gestión de hospitalización en el cual, según los motivos de la hospitalización, confirma los turnos y deriva al paciente a su cuarto y según esta orden se traslada la historia clínica del paciente de recepción al piso al cual se enviará al paciente, escalando, por lo tanto, al proceso "indicar hospitalización" y se tiene como salida la gestión o atención del paciente, lo cual servirá como input para el proceso atención al paciente hospitalizado.

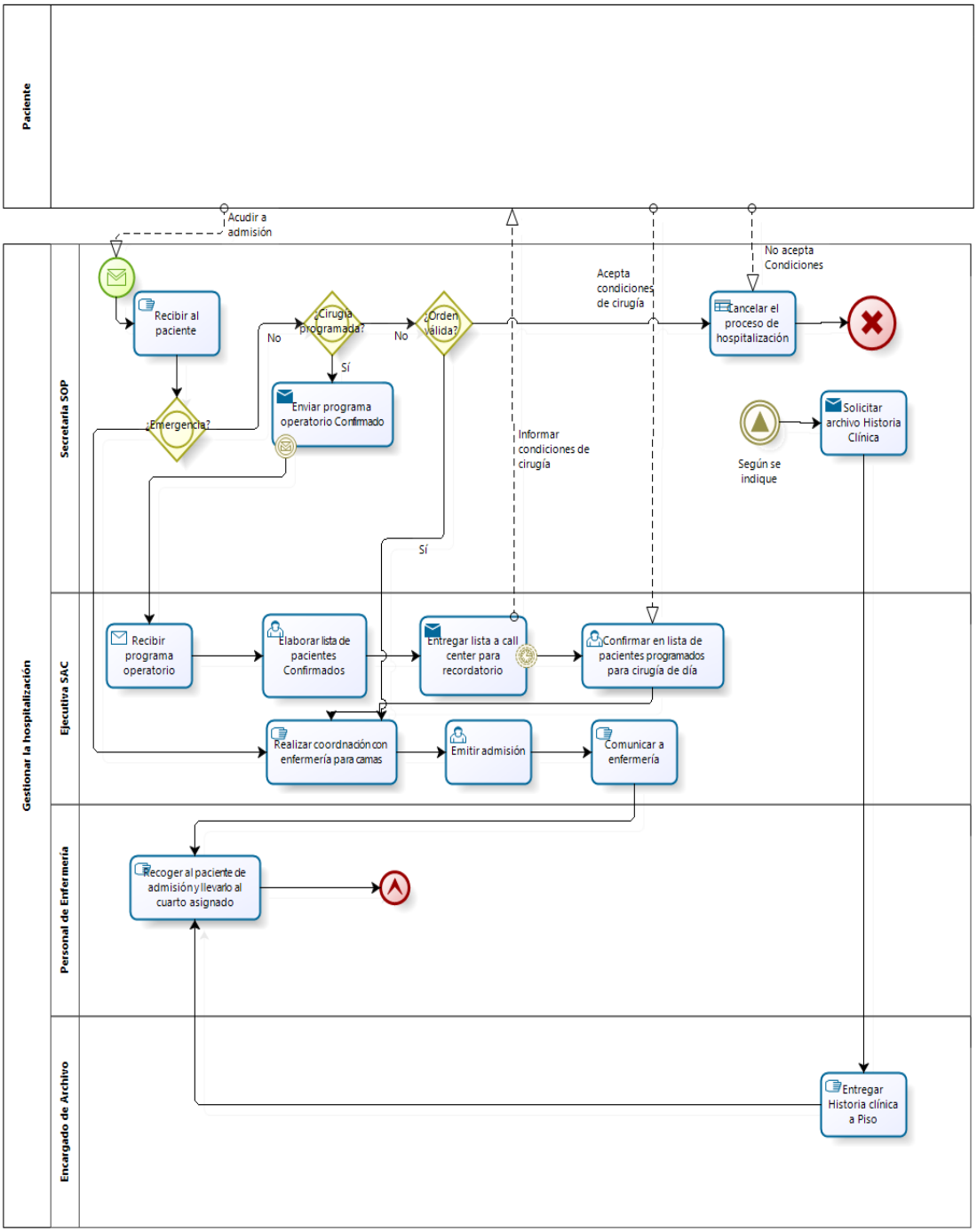


Figura 7.1.5 - Diagrama del sub-proceso gestionar la hospitalización

7.2 Proceso: Atención al paciente hospitalizado

Sub-proceso nivel 2: Atender diariamente al paciente

En el siguiente proceso se muestra como se realiza la atención del paciente hospitalizado, indicando las rondas de seguimiento y la administración del tratamiento indicado por el médico. Adicionalmente dentro del proceso se describen las acciones en caso se requiera que el paciente pase por algún procedimiento, cirugía o algún cambio que genere alguna alerta que deba ser atendida como parte de la atención médica o escalar a otros procesos según las políticas definidas.

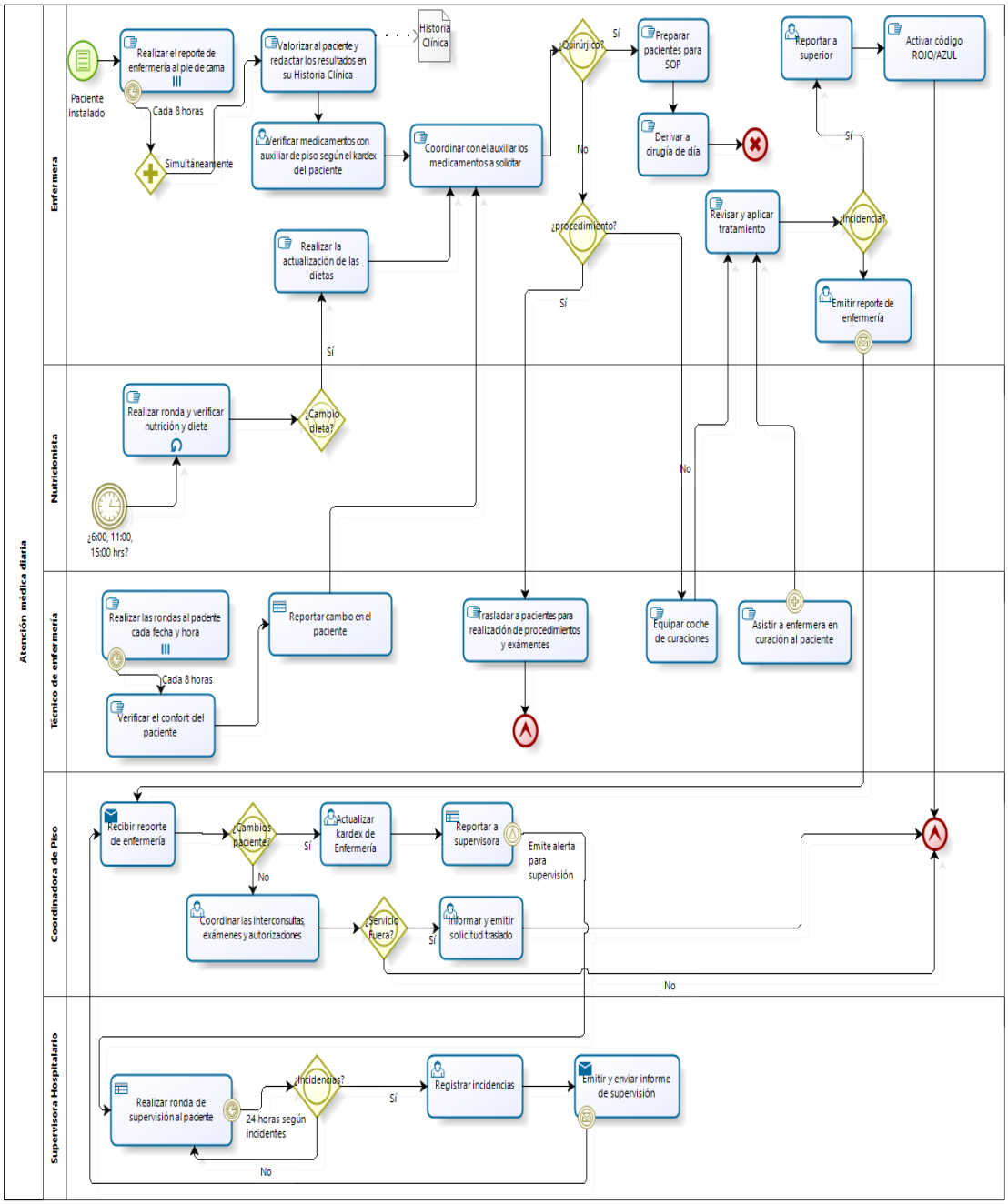


Figura 7.2.1 - Diagrama del sub-proceso atender diariamente al paciente

Sub-proceso nivel 2: Gestionar el equipo médico

En el presente sub-proceso se muestra como se realiza la gestión del equipo médico, la cual es una tarea cíclica debido a que se realiza continuamente según los cambios de turnos o ingresos de nuevos pacientes que requieran alguna atención especializada. Incluye el reporte diario de incidencias a la gerencia médica.

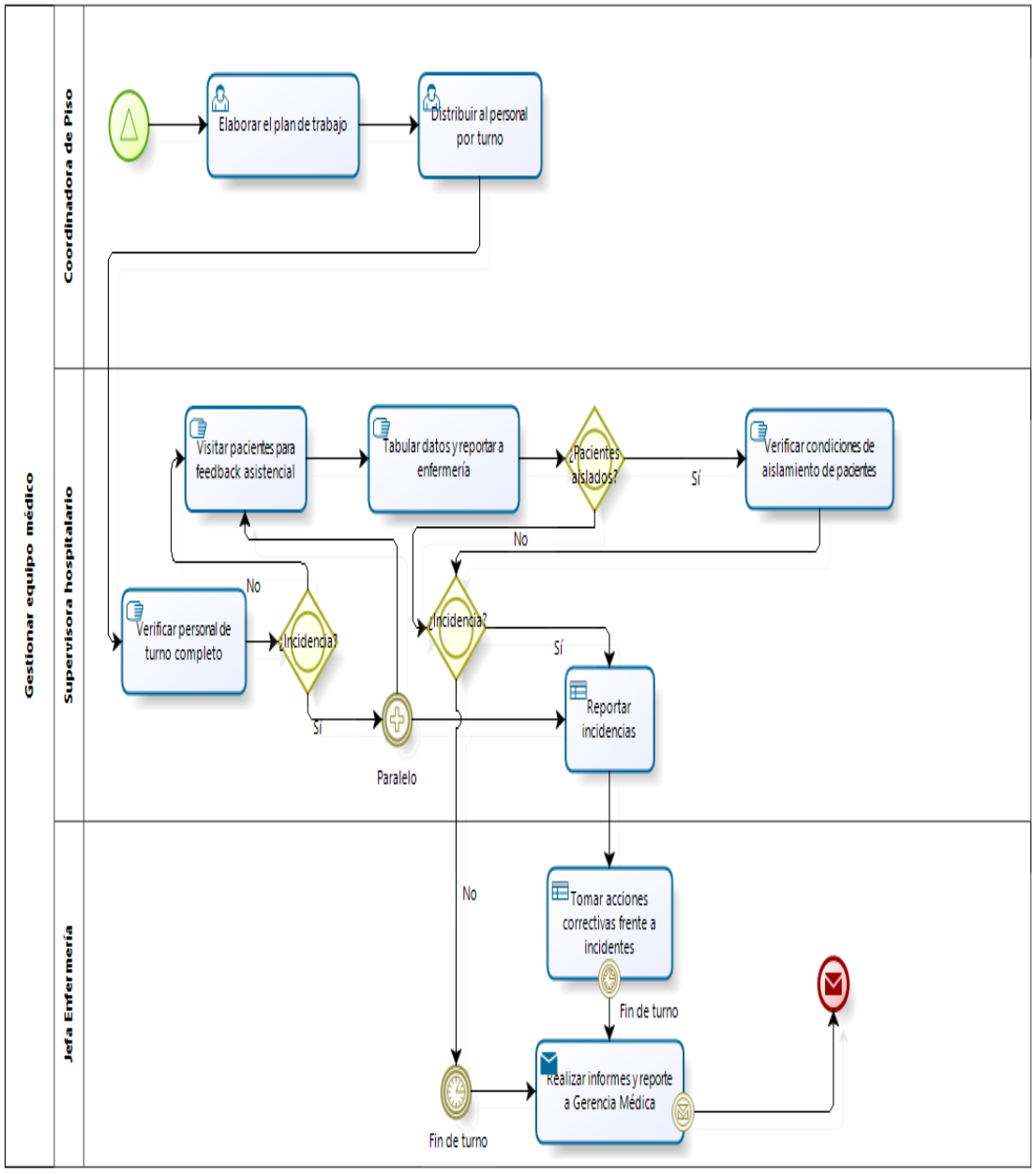


Figura 7.2.2 - Diagrama del sub-proceso gestionar equipo médico

7.3 Proceso: Egreso del paciente

Sub-proceso nivel 2: Realizar la liquidación de cuenta

En este sub-proceso se detalla la liquidación de la cuenta del paciente a través de los sistemas de facturación y control de la clínica. Las entradas y salidas son las notificaciones o mensajes enviados para poder realizar el cobro de la cuenta y finalmente el alta o autorización de la salida del paciente.

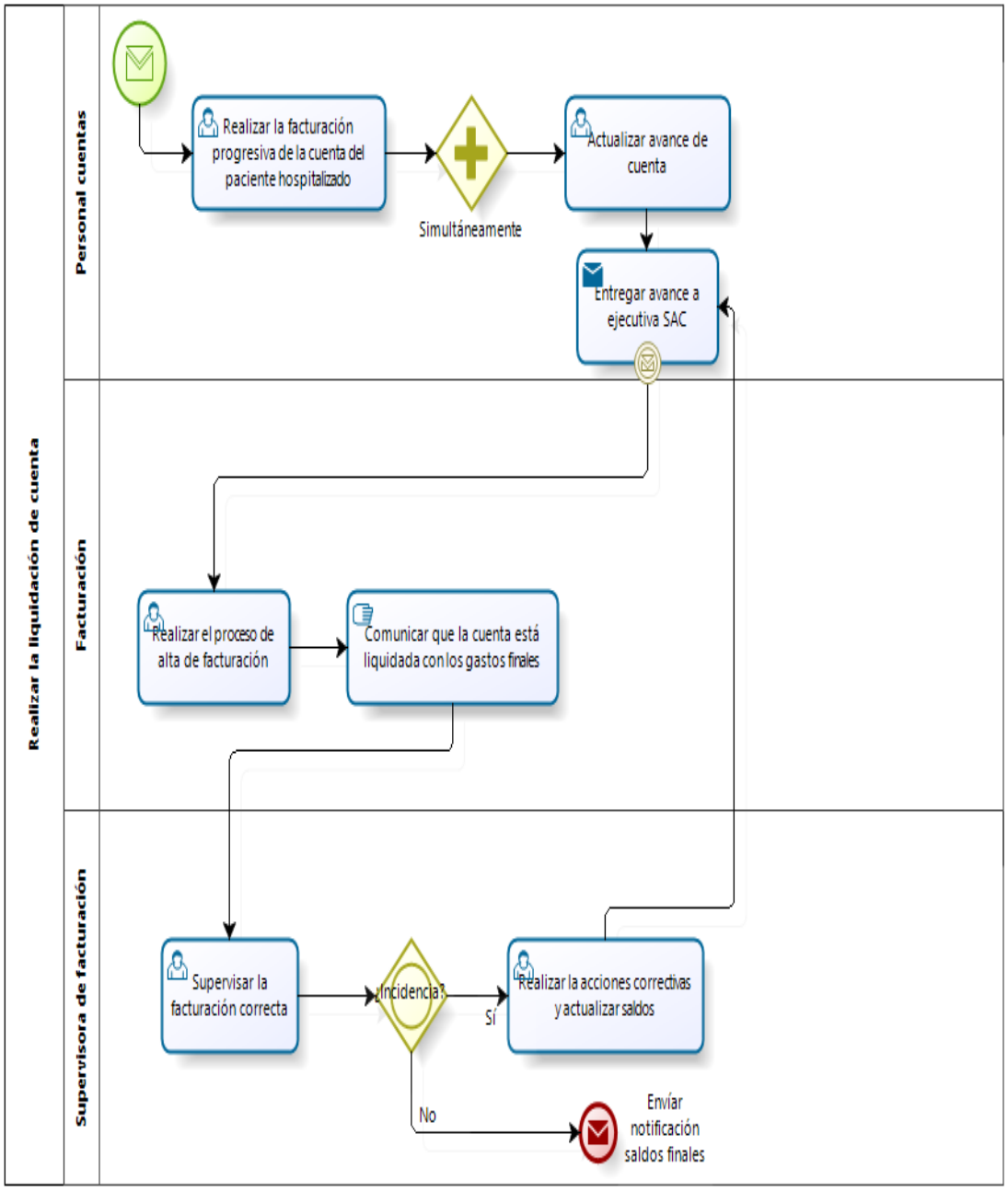
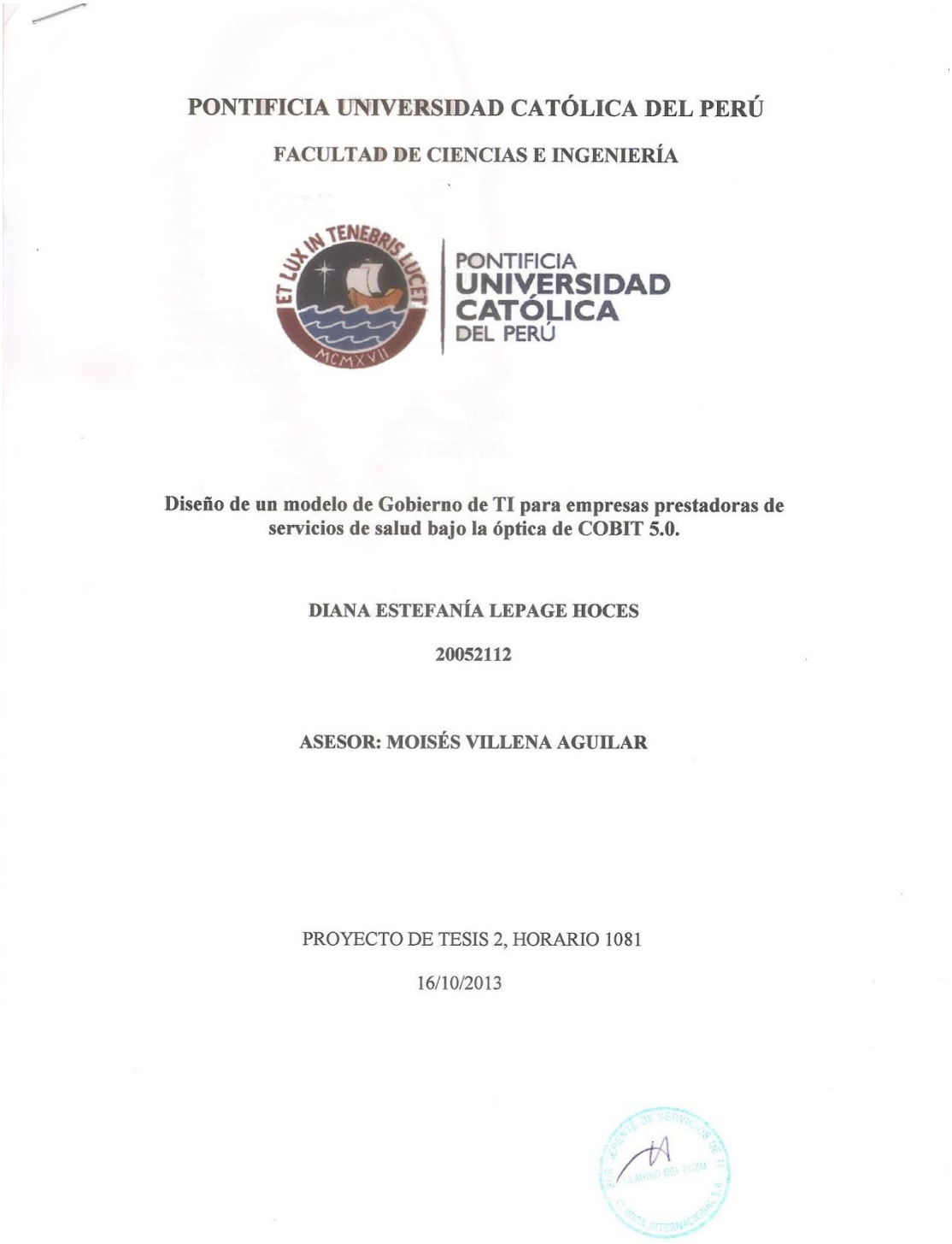


Figura 7.3.1 - Diagrama del sub-proceso realizar la liquidación de la cuenta

ANEXO H: Procesos firmados y aprobados por la empresa

8.1 Documentos aprobados



PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

Diseño de un modelo de Gobierno de TI para empresas prestadoras de servicios de salud bajo la óptica de COBIT 5.0.

DIANA ESTEFANÍA LEPAGE HOCES

20052112

ASESOR: MOISÉS VILLENA AGUILAR

PROYECTO DE TESIS 2, HORARIO 1081

16/10/2013

Figura 8.1.1 - Documentos firmados (1)

Capítulo 7. Identificación y Diseño de procesos AS-IS

En el presente capítulo se muestra el diagrama de los procesos identificados dentro de la empresa prestadora de servicios de salud de referencia, los cuales serán la base de la iniciativa de gobierno de TI y al cual se le aplicarán los procesos habilitadores para determinar roles y políticas de seguridad de información.

Los procesos presentados a continuación se encontraron en un nivel de madurez cero (0) y a través del levantamiento de información serán completados para poder conducirlos a un nivel uno (1) tal como lo indica la norma ISO/IEC 15504 empleada dentro de COBIT 5.0 y que a su vez es lo esperado por la organización según el mapeo de fases de gobierno de TI realizado como parte de los logros a corto plazo.

1.1 Justificación de los procesos empresariales

Para este modelo de gobierno se empleará un proceso organizacional,proceso general o macro-proceso hospitalario del paciente. Este incluye la admisión, atención y egreso del paciente. Adicionalmente se considera el proceso y las políticas de identificación como parte de un proceso transversal a este y otros macro-procesos como el de emergencia, cirugía de día y ambulatorio.

La elección de este juego de procesos se debe a que a lo largo de éstos se manejan documentos reglamentados como historias clínicas y otros relevantes tales como los resultados de análisis realizados al paciente que incluyen datos que deben ser protegidos íntegramente como parte del cumplimiento de la ley 29733 y para conseguir el logro de sus objetivos organizacionales, principalmente, "Ofrecer a los pacientes seguridad y una mejor experiencia dentro de su estancia en la clínica".

Figura 8.1.2 - Documentos firmados (2)

1.2 Proceso: Admisión de pacientes (Indicar hospitalización)

A continuación se presenta el diagrama para el proceso de admisión general, iniciado por un requerimiento externo y por medio del cual, según la necesidad y tipo de atención descenderá a otros sub-procesos hasta admitir al paciente y proceder con el internamiento y el proceso de atención.

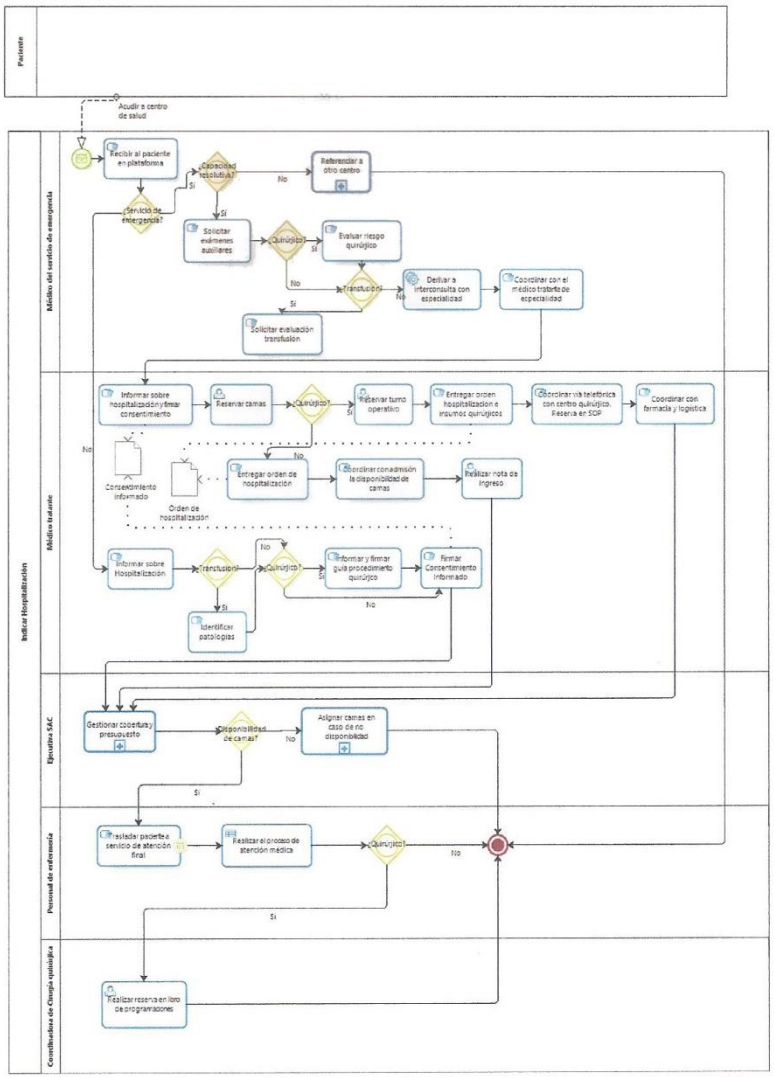


Figura 1.2.1 - Diagrama del proceso de admisión de pacientes

Figura 8.1.3 - Documentos firmados (3)

1.2.1 Sub-proceso nivel 2: Referenciar a otro centro

El siguiente sub proceso es iniciado según la capacidad resolutiva del paciente o en caso se requiera una transferencia administrativa, lo cual es el trigger para el inicio. Se tiene como actor externo al paciente y al médico del centro de referencia destino.

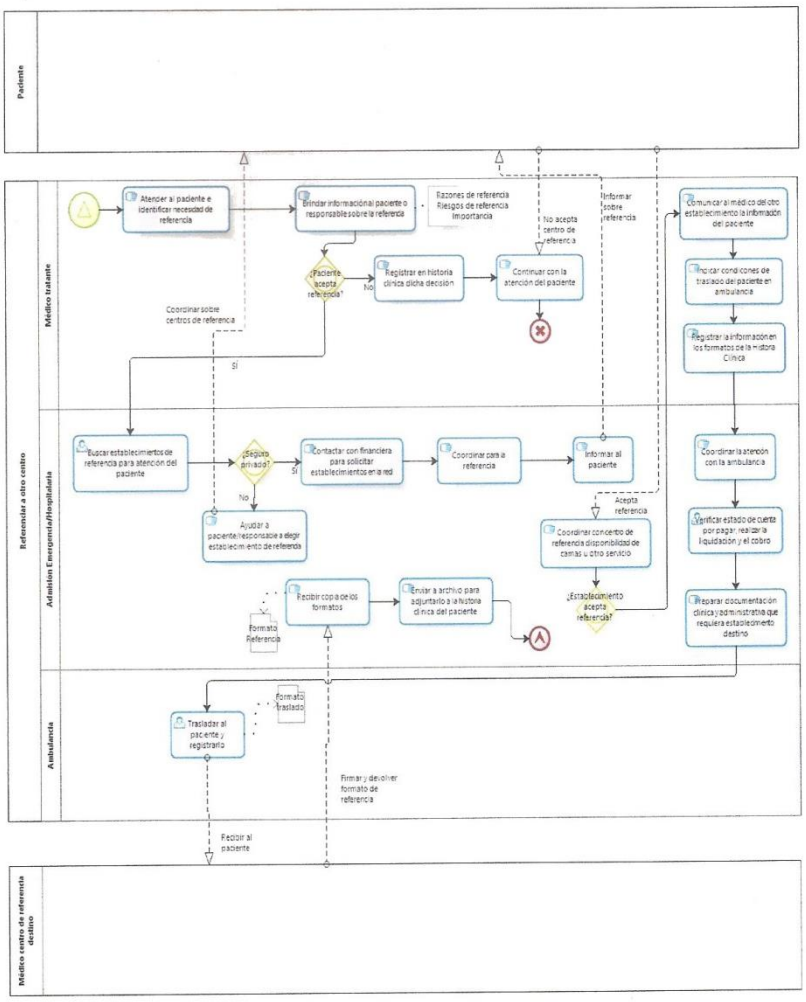


Figura 1.2.2 - Diagrama sub-proceso referenciar a otro centro

Figura 8.1.4 - Documentos firmados (4)

1.2.2 *Sub-proceso nivel 2: Asignar camas en caso de no disponibilidad*

El siguiente sub proceso es iniciado bajo la condición de que existe una órden previa de hospitalización, por lo tanto se verifica nuevamente la disponibilidad de camas o de lo contrario se deriva a otra sede de la clínica. Así mismo, se observala iteracción con dos actores externos, el paciente y el call center de su aseguradora para validar la cobertura y grupo de opciones con las cuales trabaja para realizar el traslado.

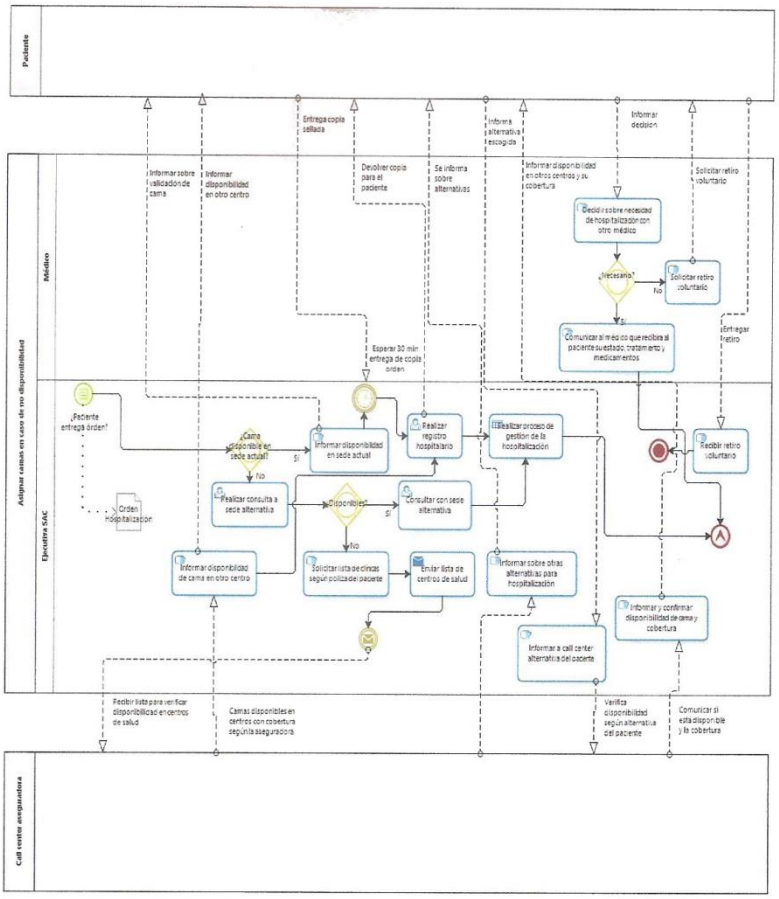


Figura 1.2.3 - Diagrama del sub-proceso asignar camas en caso de no disponibilidad

Figura 8.1.5 - Documentos firmados (5)

1.2.3 Sub-proceso nivel 2: Gestionar Cobertura y presupuesto

Este sub proceso consta de la validación realizada para determinar el presupuesto de la hospitalización del paciente, y en caso esté asegurado proceder a validar la cobertura y la emisión de las cartas de garantía. Se tiene como actores externos al paciente y a la ejecutiva de cartas de garantía de otras aseguradoras distintas a RIMAC.

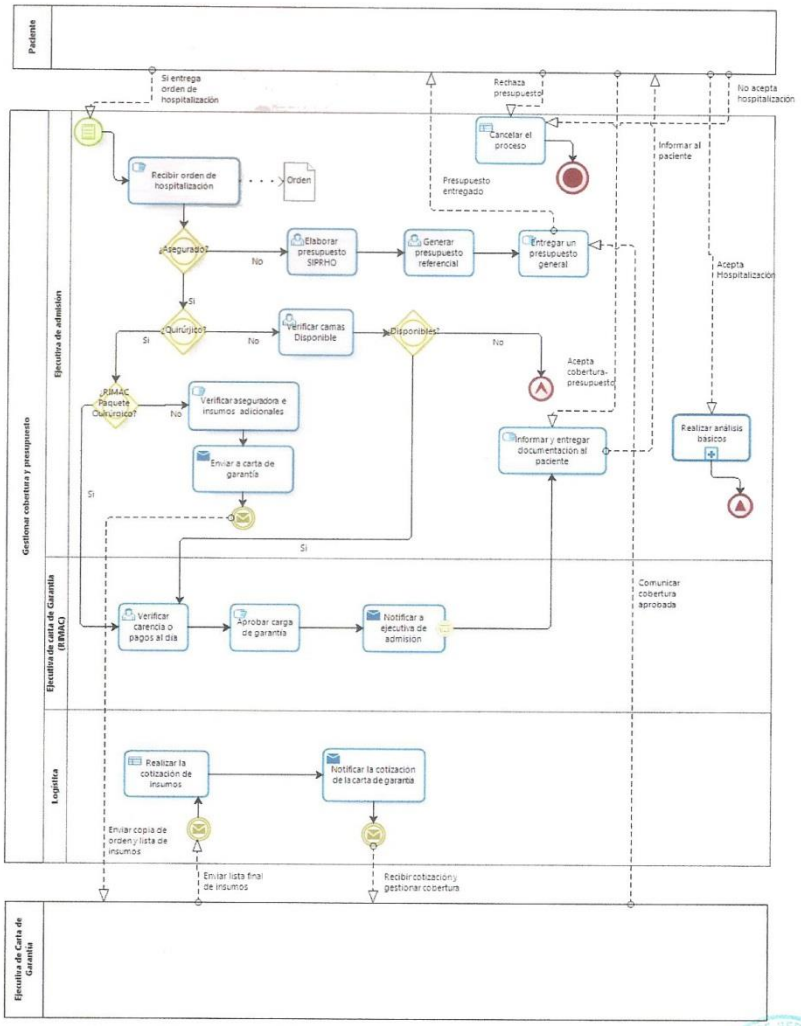


Figura 1.2.4 - Diagrama del sub-proceso gestionar cobertura y presupuesto

Figura 8.1.6 - Documentos firmados (6)

1.2.4 *Sub-proceso nivel 3: Realizar análisis básicos*

Este sub-proceso es iniciado según la derivación a plataforma del paciente luego de la cobertura y presupuesto y proceder con los análisis básicos según el motivo de la hospitalización.

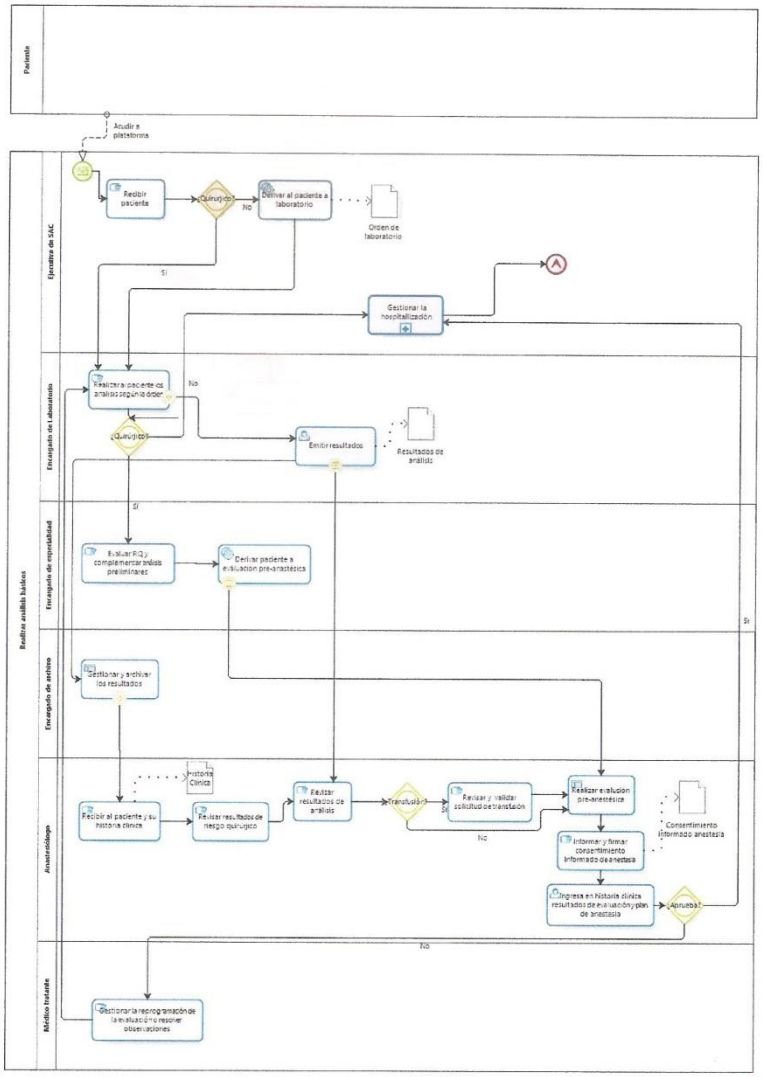


Figura 1.2.5 - Diagrama del sub-proceso realizar análisis básicos

Figura 8.1.7 - Documentos firmados (7)

1.2.5 Sub-proceso nivel 4: Gestionar la hospitalización

Finalmente se tiene el sub-proceso de último nivel, gestión de hospitalización en el cual, según los motivos de la hospitalización, confirma los turnos y deriva al paciente a su cuarto y según esta orden se traslada la historia clínica del paciente de recepción al piso al cual se enviará al paciente, escalando, por lo tanto, al proceso "indicar hospitalización" y se tiene como salida la gestión o atención del paciente, lo cual servirá como input para el proceso atención al paciente hospitalizado.

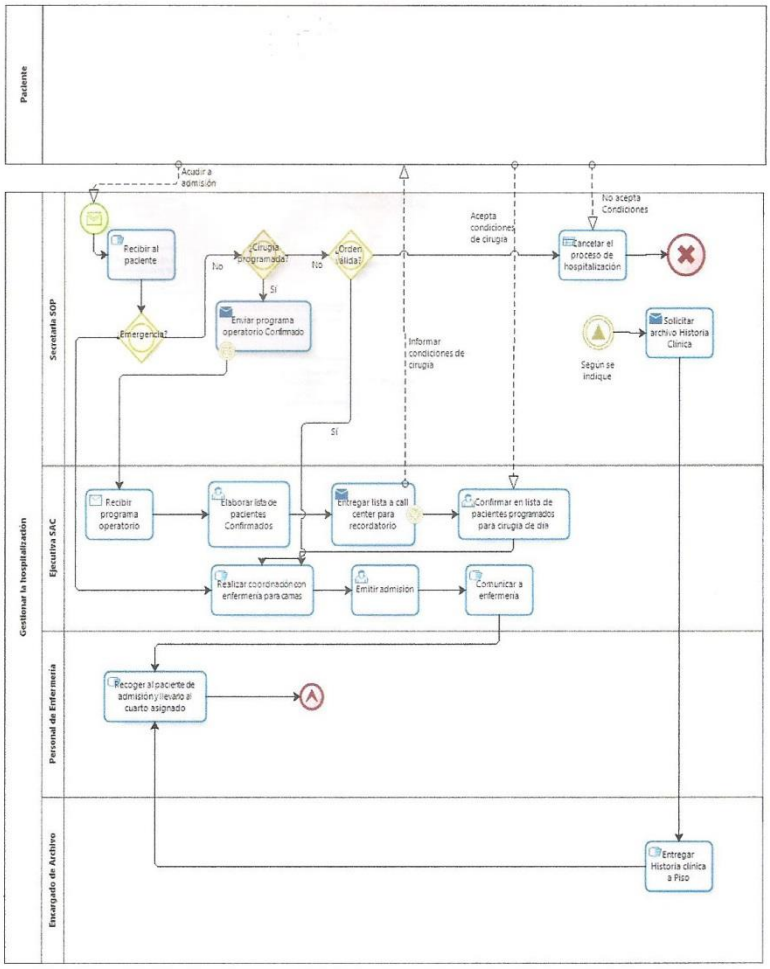


Figura 1.2.6 - Diagrama del sub-proceso gestionar la hospitalización

Figura 8.1.8 - Documentos firmados (8)

1.3 Proceso: Atención del paciente hospitalizado

El presente proceso es parte del macro proceso hospitalario, en este se detalla cómo se brinda la atención al paciente y como planifican los recursos dentro de cada turno. Así mismo, se definen las condiciones de salida que determina si continúa con el proceso de alta del paciente o a otros procesos como transferencia o defunción.

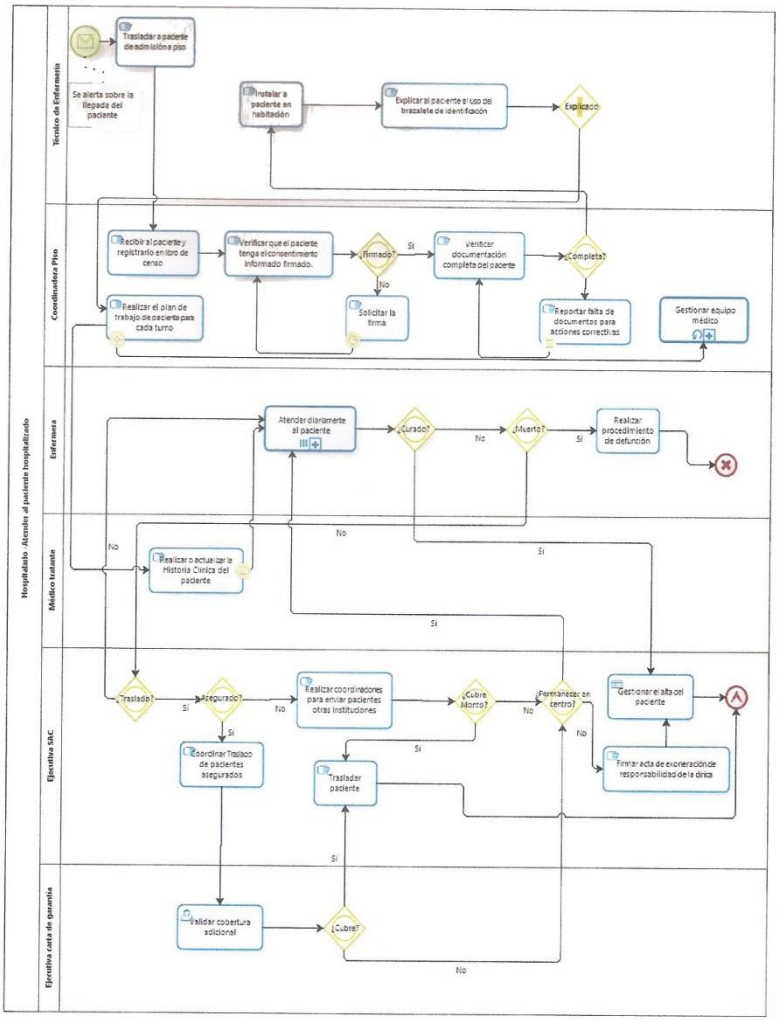


Figura 1.3.1 - Diagrama del proceso atención al paciente hospitalizado

Figura 8.1.9 -Documentos firmados (9)

1.3.1 *Sub-proceso nivel 2: Atender diariamente al paciente*

En el siguiente proceso se muestra como se realiza la atención del paciente hospitalizado, indicando las rondas de seguimiento y la administración del tratamiento indicado por el médico. Adicionalmente dentro del proceso se describen las acciones en caso se requiera que el paciente pase por algún procedimiento, cirugía o algún cambio que genere alguna alerta que deba ser atendida como parte de la atención médica o escalar a otros procesos según las políticas definidas.

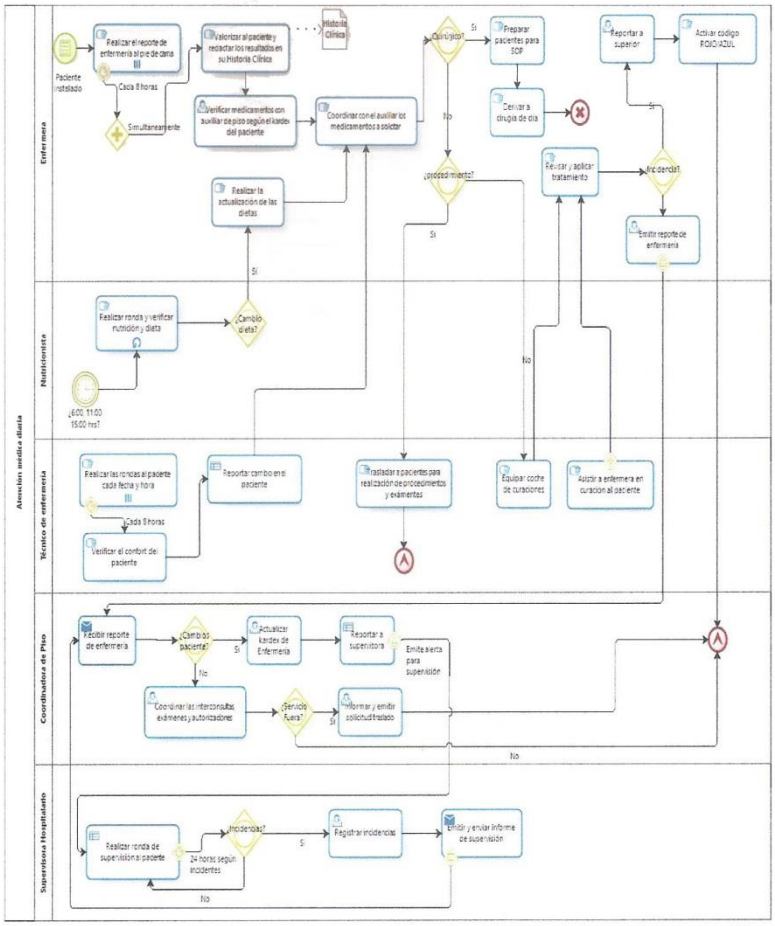


Figura 1.3.2 - Diagrama del sub-proceso atender diariamente al paciente

Figura 8.1.10 - Documentos firmados (10)

1.3.2 *Sub-proceso nivel 2: Gestionar el equipo médico*

En el presente sub-proceso se muestra como se realiza la gestión del equipo médico, la cual es una tarea cíclica debido a que se realiza continuamente según los cambios de turnos o ingresos de nuevos pacientes que requieran alguna atención especializada.

Incluye el reporte diario de incidencias a la gerencia médica.

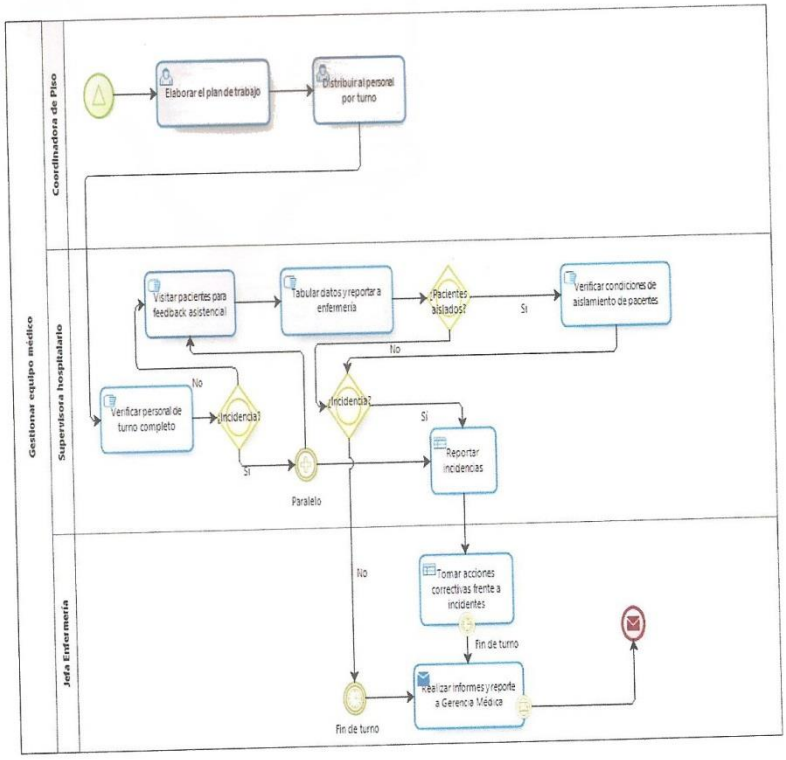


Figura 1.3.3 - Diagrama del sub-proceso gestionar equipo médico

Figura 8.1.11 - Documentos firmados (11)

1.4 Proceso: Egreso del paciente hospitalizado

Este proceso parte del macro proceso hospitalario, detalla el alta del paciente según sus condiciones de salida, es decir, en caso este recuperado o no recuperado, incluso las condiciones bajo las cuales se realiza los trámites para la trasferencia a otro centro de referencia.

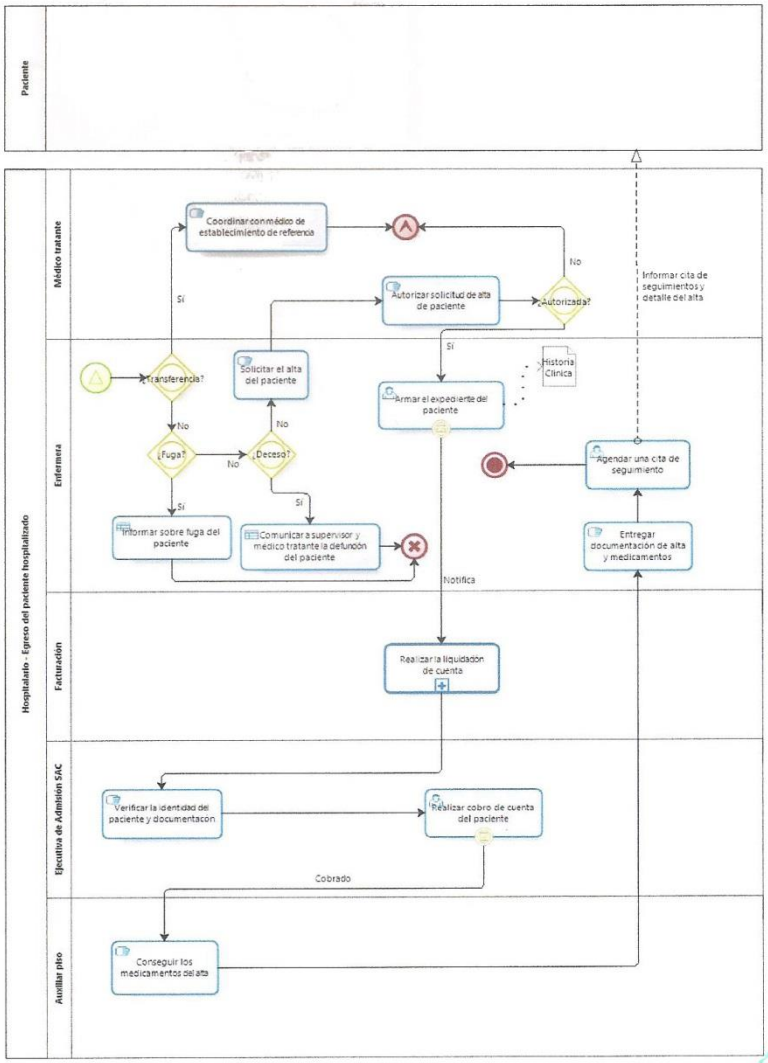


Figura 1.4.1 - Diagrama del proceso Egreso del paciente hospitalizado

Figura 8.1.12 - Documentos firmados (12)

1.4.1 *Sub-proceso nivel 2: Realizar la liquidación de cuenta*

En este sub-proceso se detalla la liquidación de la cuenta del paciente a través de los sistemas de facturación y control de la clínica. Las entradas y salidas son las notificaciones o mensajes enviados para poder realizar el cobro de la cuenta y finalmente el alta o autorización de la salida del paciente.

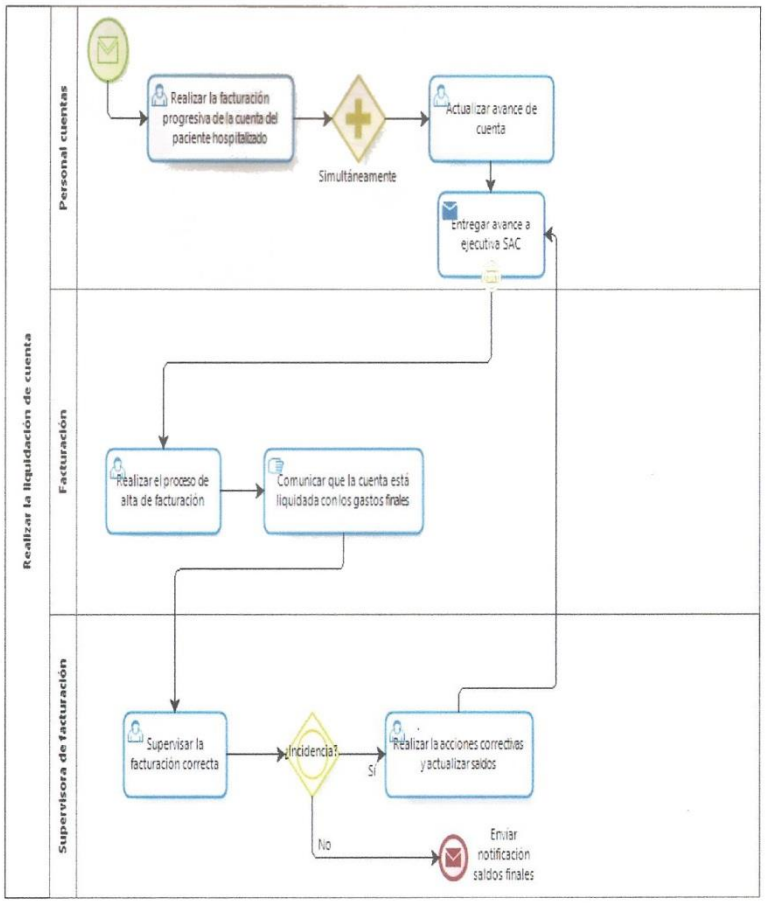


Figura 1.4.2 - Diagrama del sub-proceso realizar la liquidación de la cuenta

Figura 8.1.13 - Documentos firmados (13)

1.5 Proceso: Identificación del paciente hospitalizado

Este proceso se encuentra fuera del macro proceso hospitalario, no obstante se considera debido a que es transversal a los procesos que lo comprenden y detalla las políticas a seguir durante la estancia del paciente para verificar sus datos personales y el detalle de la historia clínica.

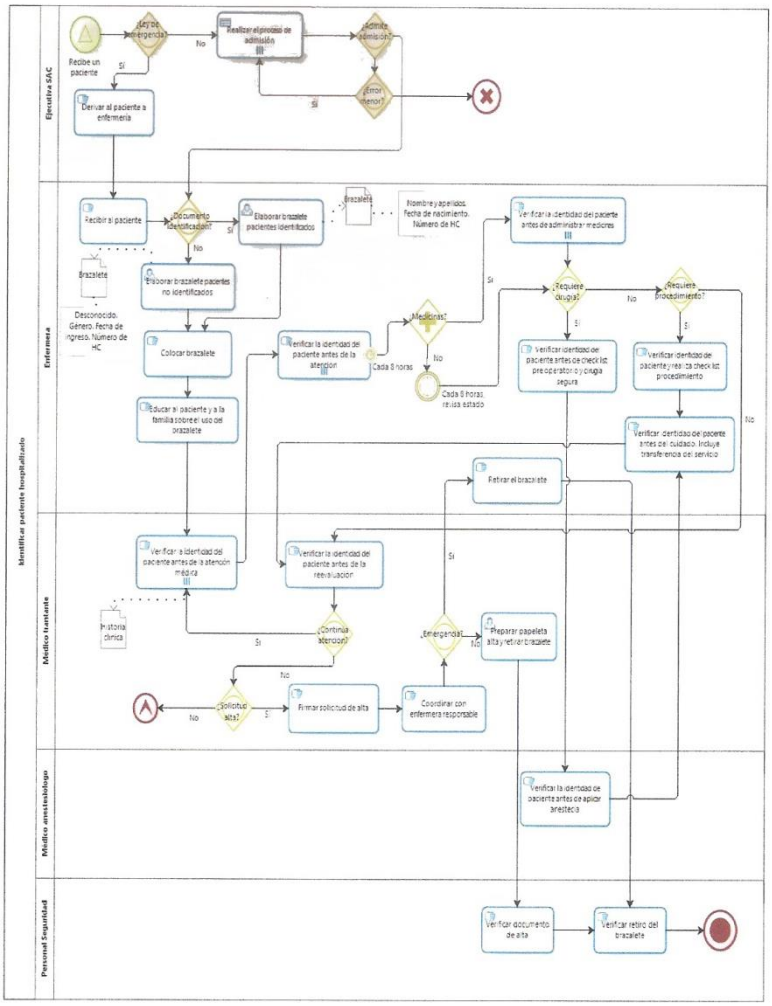


Figura 1.5.1 - Diagrama del proceso Identificación del paciente hospitalizado

Figura 8.1.14 - Documentos firmados (14)

2 Conclusiones del Capítulo

- La selección de los procesos es una de las bases del modelo de gobierno de TI, debido a que permite conocer el estado actual de la organización, para dicho enfoque, y el nivel de madurez del proceso, lo cual valida el alcance real del proyecto y se puede realizar el ajuste para cada una de las iteraciones del ciclo de vida, de manera que se puedan conseguir los logros inmediatos.

- Los procesos seleccionados, tal como se mencionó dentro del mapeo de fases, se encontraban en un nivel de madurez cero (0). No obstante, al haberlos completado se concluye que el nivel de madurez según la norma ISO/IEC 15504 es uno (1).

- Se valida el modelado de procesos en la notación BPMN 2.0 por parte de la empresa modelo para el proyecto, por lo tanto, junto con el comité estratégico, considerando que ahora el nivel de madurez es uno (1), se materializa el primer logro inmediato.

- En caso se decida ampliar el alcance del proyecto, es decir contemplar otros procesos, se deberá tener en cuenta que éstos deben ser mapeados y relacionados con el mapa actual presentado, lo cual implica que los otros procesos deben también ser adaptados a esta notación y ser validados por los dueños del proceso, para posteriormente definir su nivel de madurez.

- Respecto a considerar otros enfoques para este mismo juego de procesos, se deberá realizar el análisis previo para posteriormente realizar la identificación de políticas de TI adicionales a las del enfoque de seguridad de información.

Figura 8.1.15 - Documentos firmados (15)

ANEXO I: Identificación actividades, roles y responsabilidades para los habilitadores

9.1 Actividades de gestión COBIT 5.0 bajo el enfoque de seguridad de Información

A continuación se presenta las actividades de gestión para los cuatro (4) procesos seleccionados y diseñados bajo la notación BPMN 2.0. Para su identificación, tal como se señala, se procede a analizar la viabilidad de aplicación de las actividades propuestas por COBIT 5.0 para cada proceso habilitador que aplican para el enfoque de seguridad de información.

Identificando las sub-actividades para cumplir la actividad de gestión, se elabora la matriz RACI de acuerdo al enfoque del gobierno y las capacidades y roles de la organización para que sean la base para adoptar políticas bajo la norma ISO/IEC 27002:2013.

En la siguiente tabla se muestra la leyenda que será útil para la lectura de la matriz de responsabilidades que se presentarán para cada uno de los procesos habilitadores. La explicación teórica de esta matriz y abreviaturas empleadas se encuentra en el capítulo 2.

Leyenda	Descripción
R	Responsable
A	Accountable
C	Consulted
I	Informated
(*)	Rol no implementado o ejercido dentro de la organización

Tabla 9.1.1 - Leyenda para lectura de matriz RACI

1.1.1 Procesos habilitadores en común para los procesos de la empresa

Para cada uno de los procesos seleccionado se ha realizado un análisis y se determina que pese a los cambios o mejoras futuras a nivel de procesos, las actividades a aplicar para el cumplimiento de los habilitadores no presentan variaciones, por lo cual se puede emplear la misma matriz y adoptar las mismas políticas de TI y seguridad de información.

Se presentan los procesos habilitadores en común:

a. <u>Proceso habilitador: Garantizar el mantenimiento y configuración del marco de control de gobierno</u>

Se verifica la aplicación de todas las actividades de gestión, no obstante se señala que no pueden aplicarse todas las sub-actividades para su cumplimiento debido a la actividad realizada por la empresa y el nivel de madurez al cual se pretenda y sea viable llegar luego de cada iteración.

Luego se procede a elaborar la matriz de responsabilidades para gestionar el habilitador según el enfoque de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Evaluar el sistema de gobierno	Analizar e identificar los factores de entorno interno y externo relacionados a la seguridad de información, los cuales afectan directamente al proceso, junto con las tendencias en el negocio que puedan influir en el diseño del gobierno.
	Evaluar el nivel de la seguridad de información dentro del negocio y el cumplimiento con regulaciones externas[10] dentro del proceso. Entre estas se tiene: Ley de protección de datos personales, Ley de emergencia y la norma técnica peruana de la historia clínica.
	Articular los principios que guiarán el diseño óptimo del modelo de toma de decisiones sobre el gobierno de TI y su enfoque a la seguridad de información.
	Considerar cómo serán aplicadas o enfocadas la ley de protección de datos personales, la ley de emergencia y la norma técnica peruana de la historia clínica en el gobierno de TI de la empresa y en los procesos base.
Dirigir el sistema de gobierno	Exigir la función de seguridad de información para toda la empresa y como esta se aplicará a los procesos.
	Contar con un comité estratégico que esté enfocado a la seguridad de información (ISSC)

[10] Se consideran únicamente las regulaciones para el proceso.

	Alinear la estrategia de seguridad de información con la estrategia empresarial
	Obtener el compromiso de la alta dirección para verificar la seguridad de información y la gestión de riesgos de información.
	Asignar responsabilidad para que se apliquen principios de gobierno, modelos de toma de decisión acordados.
Monitorear el sistema de gobierno	Supervisar mecanismos para asegurar que los sistemas para medir el desempeño de seguridad de información cumplen con la ley de protección de datos personales y la norma técnica peruana de historia clínica.
	Proporcionar supervisión de la efectividad y el cumplimiento con el sistema de control de la empresa.
	Evaluar la efectividad y rendimiento de los stakeholders en los que se ha delegado responsabilidad y autoridad para el gobierno de TI de la empresa.

Tabla 9.1.2 - Actividades de gestión habilitador: Garantizar el mantenimiento y configuración del marco de control de gobierno

Matriz de responsabilidades (RACI)

EDM01: Garantizar el mantenimiento y configuración del marco de control de gobierno																				
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe de proyectos	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas[11]	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Evaluar el sistema de gobierno	A	R	C	C	R	C	R			C	R	C	C	I	R		C		C	
Dirigir el sistema de gobierno	A	R	C	C	R	I	R	I	I	C	C	I	I	C	R	I	I	I	I	I
Monitorear el sistema de gobierno	A	R	C	C	R	I	R	I	I	C	C	I	I	C	R	I	I	I	I	I

Tabla 9.1.3 - Matriz de responsabilidades para el proceso habilitador EDM01

[11] El administrador de plataformas en este caso realiza la gestión de tecnologías a gran nivel incluyendo los sitemas que comprende el proceso. En caso se deba de recurir al desarrollador del sistema, lo reporta y asume la responsabilidad frente a la solución de algún incidente.

b. Proceso habilitador: Garantizar la entrega de beneficios

Se verifica la aplicación de todas las actividades de gestión, no obstante se señala que no pueden aplicarse todas las sub-actividades para su cumplimiento debido a la actividad realizada por la empresa y la gestión de sus inversiones. Adicionalmente se la matriz de responsabilidades destacando las acciones del oficial de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Evaluar la optimización del valor	Identificar y registrar los requisitos de los stakeholders en relación con los procesos base para la protección de sus intereses y la entrega de valor tomando en cuenta los parámetros de seguridad de información. Establecer la dirección respectiva.
	Comprender y discutir periódicamente sobre las oportunidades que pueden surgir a partir de los cambios dentro de los procesos base al emplear tecnologías actuales y optimizar el valor de estas oportunidades.
	Comprender el significado del valor en la empresa y como se ha comunicado, entendido y aplicado a través de los procesos de la organización.
	Evaluar la efectividad de la integración y alineamiento de las estrategias de TI y seguridad de información en la empresa con los objetivos para aportar valor, así como la alineación de estos últimos con el portafolio de inversiones
Dirigir la optimización del valor	Asegurar que se empleen medidas financieras y no financieras para describir el valor añadido de las iniciativas de seguridad de información en los procesos base.
	Establecer un método para demostrar el valor de la seguridad de información para garantizar el uso eficiente (considerando los niveles de seguridad) de los activos dentro de los procesos identificados.

	Dirigir los cambios necesarios en el portafolio de inversiones y servicios para realinearlos con los objetivos actuales, los esperados y/o sus limitaciones.
	Dirigir los cambios necesarios en asignación de imputaciones y responsabilidades del portafolio de inversión y entrega de valor a partir de los servicios y procesos de negocio enfocados a la seguridad de información.
Monitorear la optimización del valor	Monitorear el resultado de las iniciativas de seguridad de información frente a las expectativas para asegurar la entrega de valor de acuerdo a los objetivos de negocio
	Definir objetivos de desempeño, métricas, metas y puntos de referencia. Revisarlos y formalizarlo junto con los stakeholders.
	Tomar medidas de gestión para asegurar la optimización del valor. En caso sean medidas correctivas, asegurarse de que sean iniciadas y controladas.

Tabla 9.1.4 - Actividades de gestión habilitador: Garantizar la entrega de beneficios

Matriz de responsabilidades (RACI)

EDM02: Garantizar la entrega de beneficios	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe de portafolio/proyecto de inversión (*)	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Evaluar optimización del valor	A	R	R	C	R		R		C	C	C	C		C	R		C		C	
Dirigir optimización del valor	A	R	R	C	R	C	R	I	I	I	C	I	I	I	R	I	I	I	I	I
Monitorear optimización valor	A	R	R	C	R		R		R	C	C	C	I	C	R	I	C			

Tabla 9.1.5 - Matriz de responsabilidades para el proceso habilitador EDM02

c. Proceso habilitador: Garantizar la optimización del riesgo

Se verifica la aplicación de todas las actividades de gestión, sin embargo, no pueden aplicarse todas las sub-actividades para su cumplimiento debido a la actividad realizada por la empresa y el tratamiento de riesgos y formalización del comité responsable.

Luego se elabora la matriz de responsabilidades para gestionar el habilitador según el enfoque de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Evaluar la gestión de riesgos	Determinar junto con la directiva de la empresa el nivel de apetito por el riesgo.
	Medir el nivel de integración de la gestión de riesgos de seguridad de información con el modelo general de riesgos de la organización.
	Determinar el grado de alineamiento de la estrategia de riesgos de TI y seguridad de información con la estrategia de riesgos empresariales.
	Determinar si las tecnologías empleadas en los procesos base están sujetas a una evaluación de riesgos adecuada según lo descrito en estándares relevantes que pueda adoptar la organización.
Dirigir la gestión de riesgos	Integrar la gestión de riesgos de seguridad de información dentro del modelo general de riesgos.
	Dirigir la elaboración de planes de comunicación y acción de riesgos promoviendo una cultura consciente sobre estos y su impacto dentro del negocio.
	Dirigir la implantación de mecanismos apropiados para responder a los riesgos cambiantes y notificar a los niveles adecuados según el principio de escalamiento.
	Dirigir para que los riesgos de seguridad de información dentro de los procesos puedan ser identificados por cualquier persona en cualquier momento según las políticas y procedimientos publicados.

Monitorear la gestión del riesgos	Monitorear el perfil frente al riesgo o el apetito del riesgo de la empresa para lograr un equilibro óptimo entre riesgos y oportunidades de negocio
	Incluir las salidas de los procesos de gestión de riesgos de información como entradas las la gestión de riesgos de la organización.
	Comunicar los problemas de la gestión de riesgos al directorio.
	Monitorear las metas y métricas de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos. Iniciar medidas correctivas para casos especiales

Tabla 9.1.6 - Actividades de gestión habilitador: Garantizar la optimización de riesgos

Matriz de responsabilidades (RACI)

EDM03: Garantizar la optimización de riesgos	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Evaluar la gestión de riesgos	A	R	C	C	R	C	R			R	R	I	C	C	R				C	
Dirigir la gestión de riesgos	A	R	C	C	R	C	R	I	I	R	C	I	I	I	R	I	I	I	I	I
Monitorear la gestión de riesgos	A	R	C	C	R	C	R	I	I	R	R	I	C	C	R	I	I	I	I	I

Tabla 9.1.7 - Matriz de responsabilidades para el proceso habilitador EDM03

d. Proceso habilitador: Gestionar el marco de control de TI

Este proceso habilitador realiza la evaluación de la aplicación del marco de gobierno, en este caso se emplea COBIT 5.0. No se toma en cuenta la actividad de gestión APO01.05 debido a que no se cuenta con suficiente madurez dentro de la

organización para poder realizar esta optimización debido a que cuenta con procesos inconclusos y no documentados, por lo cual es recomendable evaluar su aplicación a futuro habiendo logrado mejoras a nivel de proceso y la formalización de roles bajo el enfoque de seguridad de información.

Se muestra seguidamente la matriz de responsabilidades para gestionar el habilitador según el enfoque de seguridad de información, lo cual exige la participación del oficial de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Definir la estructura organizativa	Alinear la seguridad de la información de la organización con la arquitectura de negocio de la empresa.
	Establecer el comité estratégico de TI bajo el enfoque de seguridad de información
	Definir la función de la seguridad de información, capacidades y decisiones necesarias
	Identificar las decisiones necesarias para alcanzar los resultados corporativos y estrategia de TI y seguridad de información para la gestión y ejecución de servicios de TI.
	Establecer un comité estratégico de TI a nivel de consejo administrativo, el cual se asegure que el gobierno de TI está contemplado de forma adecuada y que priorice programas de inversión según la estrategia y objetivos de negocio.
	Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre el negocio y las funciones de TI dentro de la empresa y terceros.
	Verificar la adecuación y eficacia de la estructura organizativa.
Establecer roles y responsabilidades	Establecer, acordar y comunicar los roles de CISO e ISM[12]
	Determinar las funciones de la organización que tienen la obligación de seguridad de información y añadirlas a

[12] ISM: Information Security Manager

	la descripción de puestos.
	Tomar como referencia los requisitos de la empresa y continuidad del servicio de TI para la definición de roles.
	Estructurar los roles y responsabilidades para reducir la posibilidad de que un solo rol pueda comprometer un proceso crítico.
	Implementar prácticas para monitorear que los roles y responsabilidades se pongan en práctica de forma correcta. El nivel de supervisión o monitoreo debe estar en consonancia con este puesto y las responsabilidades asignadas.
Mantener los elementos habilitadores del modelo de gobierno	Considerar el ambiente interno de la empresa incluyendo la gestión de la cultura y filosofía, tolerancia al riesgo, valores éticos, código de conducta, responsabilidad y requisitos de seguridad de información.
	Alinear con estándares nacionales e internacionales de seguridad de información que sean viables. Evaluar buenas prácticas de seguridad de información.
	Desarrollar las políticas de seguridad de información de acuerdo al negocio, procesos y requisitos legales o regulatorio dentro del ambiente interno de la empresa.
	Evaluar y actualizar las políticas como mínimo una vez al año, para ajustarlas de acuerdo a los cambios operativos o a nivel de negocio
	Implantar las políticas de TI y seguridad de información a todo el personal relevante y establecer los métodos y procedimientos de medición de su cumplimiento.
Comunicar los objetivos y la dirección de gestión	Desarrollar un programa de sensibilización sobre seguridad de información
	Establecer indicadores para medir comportamientos con respecto a la seguridad de información
	Proporcionar recursos suficientes y calificados para dar soporte al proceso comunicativo.
	Garantizar que la información comunicada engloba una clara articulación del entorno empresarial y con un nivel

	de detalle adecuado para cada área de la empresa.
Definir la propiedad de la información y del sistema	Definir sistemas y accesos de datos a nivel empresarial dentro de los procesos de gestión de seguridad de información que involucran procesos base.
	Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) en toda la empresa.
	Crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones. Incluir sistemas tercerizados y aquellos cuya propiedad debe permanecer dentro de la empresa.
	Definir e implementar procedimientos para asegurar la integridad y consistencia de la información almacenada en formato electrónico.
Gestionar la mejora continua de los procesos	Examinar informes que detallan el control de la seguridad de información y las debilidades del proceso.
	Contemplar medidas para mejorar la eficiencia y eficacia de la seguridad de información.
	Identificar procesos críticos de negocio basándose en el rendimiento, cumplimiento y los riesgos relacionados. Evaluar la capacidad del proceso e identificar objetivos de mejora.
	Aplicar prácticas de gestión de calidad y en base estas realizar la actualización de los procesos o la implementación de mejoras.
Mantener el cumplimiento de las políticas y procedimientos	Programar y realizar evaluaciones periódicas para determinar el cumplimiento con las políticas y procedimientos de seguridad de información para tomar las acciones correctivas de ser necesario.
	Integrar el rendimiento y el cumplimiento dentro de los objetivos individuales del personal.
	Evaluar el desempeño de los procesos habilitadores del marco de referencia y adoptar las acciones necesarias

Tabla 9.1.8 - Actividades de gestión habilitador: Gestionar el marco de TI

Matriz de responsabilidades (RACI)

APO01: Gestionar el marco de TI																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Definir estructura organizativa		C	C	C	C		C	R	C		C		R	I	A	R	C	C	C	C
Establecer roles y responsabilidades					I	C	I	R	C		C		C	C	A	R	C	C	C	C
Mantener habilitadores del gobierno	C	A	C	C	C	C	I	C		C	C	C			R	C			C	
Comunicar objetivos y dirección de gestión		A	C	R	C	I	R	C	I	R	R	I	I	I	R	I	I	I	I	I
Definir propiedad de la información y sistemas		I	I	C	A	R							C	I	C	C			C	
Gestionar mejora de procesos				A		R			R		C		I	C	R	C	R	R	R	R
Mantener cumplimiento de políticas y procedimientos		A				R		R	R		R		R	I	R	C	R	C	R	R

Tabla 9.1.9 - Matriz de responsabilidades para el proceso habilitador APO01

e. Proceso habilitador: Monitorear, evaluar y medir el rendimiento y la conformidad

Este proceso habilitador dentro de este modelo es compatible para todos los procesos. Aplican todas las actividades de gestión del proceso. Se presentan también las sub-actividades de acuerdo a la realidad de los procesos empleados en el diseño de gobierno y de acuerdo al entorno y realidad de la empresa modelo para la elaboración del proyecto.

Seguidamente se presenta la matriz de responsabilidades para gestionar el proceso habilitador desde un enfoque de seguridad de información a lo largo del ciclo de vida

de gobierno de TI. El oficial de seguridad de información se encarga de evaluar y verificar que los requerimientos definidos se cumplan y que se puedan aplicar las medidas correctivas del caso.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Establecer un enfoque de la supervisión	Identificar las partes interesadas de mantener un enfoque de seguridad de información dentro de la organización y dentro del proceso para cumplimiento de objetivos.
	Alinear y mantener el control de la seguridad de información dentro de los procesos base. Realizar la evaluación del enfoque de gobierno de TI y su alineamiento con la organización.
	Validar el enfoque empleado de seguridad de información para gobierno de TI e identificar nuevos drivers o recursos que permitan alinear otro enfoque de gobierno según sea el caso.
	Solicitar, priorizar y asignar recursos para la supervisión de la función de seguridad de información bajo procedimientos establecidos y dentro de los procesos base.
Establecer los objetivos de cumplimiento y rendimiento	Definir y revisar los objetivos y métricas con los stakeholders respecto a la seguridad de información de acuerdo con los procesos para identificar omisiones y establecer la validez de métricas o tolerancias.
	Comunicar los cambios relacionados con la seguridad de información, su desempeño y el cumplimiento con los stakeholders tomando como base el conjunto de procesos que forman parte del gobierno de TI.
	Evaluar si los objetivos de seguridad de información y las métricas son adecuados para la verificación y medir la performance de los procesos de acuerdo a la ley de protección de datos personales, norma técnica peruana de la historia clínica y la ley de emergencia.
Recopilar y procesar los datos de cumplimiento y	Coleccionar datos y analizar la performance y conformidad relacionada a la seguridad de información

rendimiento	y la gestión de riesgos de información.
	Evaluar la integridad, eficacia e idoneidad de los datos recolectados y consolidarlos.
Analizar e informar sobre el rendimiento	Diseñar informes de rendimiento del proceso desde el enfoque de seguridad de información. Implementar mecanismos para su elaboración de acuerdo a lo esperado por los stakeholders.
	Comparar los valores de rendimiento internos y externos de acuerdo al proceso.
	Distribuir informes a las partes interesadas relevantes, tanto de rendimiento como de las incidencias suscitadas dentro del proceso.
Asegurar la implantación de medidas correctivas	Desarrollar medidas correctivas para tratar los problemas relacionados al proceso y que afecten a la seguridad de información.
	Asegurar la asignación de responsabilidades dentro de las acciones correctivas y emitir los informes respectivos.

Tabla 9.1.10 - Actividades de gestión habilitador: Monitorear, evaluar y medir el rendimiento y la conformidad

Matriz de responsabilidades (RACI)

MEA01: Monitorear, evaluar y medir el rendimiento y la conformidad																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Establecer enfoque de supervisión		A	R	R	C	I	C	I	I	I	R		C	I	R	I	C	C	C	I
Establecer objetivos de cumplimiento y rendimiento		I	I	I	A	R	C		I		R		C		C	I		R	C	I
Recopilar y procesar datos cumplimiento y rendimiento					C	R			I		I		C		A		R	I	R	I

Analizar e informar sobre el rendimiento					A	R	C		C		C		C	C	C		C	C	R	C
Asegurar la implantación de medidas correctivas	I	I	I	I	C	R			C		C		C	I	A		R	C	R	C

Tabla 9.1.11 - Matriz de responsabilidades para el proceso habilitador MEA01

f. Proceso habilitador: Monitorear, evaluar y medir el cumplimiento de requerimientos externos

Este proceso habilitador se encarga de verificar el nivel de cumplimiento con las regulaciones a las que está sujeta la organización de acuerdo a los procesos y actividades que desarrolla. Estas regulaciones son la ley de protección de datos personales, la norma técnica peruana de la historia clínica y la ley de emergencia. Se realizará la verificación y las actualizaciones según sea el caso.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad
Identificar requisitos externos de cumplimiento	Identificar los requerimientos externos de seguridad de información que deben de cumplirse dentro del proceso de acuerdo a la ley de protección de datos personales, norma técnica peruana de la historia clínica y ley de emergencia.
	Establecer mecanismos de monitoreo sobre el cumplimiento de requerimientos externos relacionados a la seguridad de información.
	Identificar posibles cambios en las regulaciones que conlleven a modificaciones dentro del proceso y a la identificación de nuevos requerimientos y exigencias a nivel de seguridad de información.
	Mantener un inventario sobre normas, leyes o requerimientos que debe de cumplir la organización.
Optimizar la respuesta a requisitos externos	Revisar y comunicar los requerimientos externos y regulaciones a todos los stakeholders.
	Revisar periódicamente las políticas y estándares relacionados al proceso para mantener la eficacia y asegurar el cumplimiento y gestión de riesgos.
Confirmar el cumplimiento de requisitos externos	Colectar y analizar datos para garantizar el cumplimiento de la seguridad de información y la gestión de riesgos.

	Evaluar periódicamente las políticas relacionadas al proceso bajo el enfoque de seguridad de información.
Obtener garantía de cumplimiento de requisitos externos	Obtener la conformidad del cumplimiento de políticas que garanticen el alineamiento con requerimientos externos. Determinar el nivel de satisfacción.
	Garantizar que los proveedores de TI cumplan con los requerimientos de seguridad de información.
	Consolidar a nivel empresarial los informes sobre requerimientos externos e internos y difundirlos a todas las unidades de negocio que abarcan el proceso.

Tabla 9.1.12 - Actividades de gestión habilitador: Monitorear, evaluar y medir el cumplimiento de requerimientos externos

Matriz de responsabilidades (RACI)

MEA03: Monitorear, evaluar y medir el cumplimiento de requerimientos externos																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Identificar requisitos externos de cumplimiento					A	R					R			C	R					
Obtener respuesta a requisitos externos		R	R	R	A	R	I	I	R					R	R	C	C	C	R	I
Confirmar cumplimiento de requisitos externos	I	R	R	R	R	R	I	I	C		R			I	R	C	C	C	R	C
Obtener garantía de cumplimiento de requisitos externos	I	I	I	I	C	C	I	I	C		R			A	R	C	I	I	C	C

Tabla 9.1.13- Matriz de responsabilidades para el proceso habilitador MEA03

1.1.2 Proceso de admisión de pacientes

Este proceso admisión de pacientes tiene mayor interacción con actores externos y proveedores, así como mayor gestión a nivel tecnológica debido a los sistemas de atención, reservas e informes. El proceso debe cumplir con la ley de protección de datos personales, ley de emergencia y la norma técnica peruana de la historia clínica.

a. <u>Proceso habilitador: Gestionar la estrategia</u>

El siguiente proceso habilitador se refiere a la estrategia a seguir para llevar a cabo el proceso de admisión y los sub-procesos al interior de este y como se va a gestionar y medir los recursos de acuerdo a los requerimientos de seguridad de información.
Seguidamente se muestra la matriz de responsabilidades para gestionar este proceso habilitador y el cumplimiento de estas sub-actividades y lograr los niveles de madurez esperados.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Comprender la dirección de la empresa	Entender como la seguridad de información debe respaldar los objetivos de la empresa y proteger los intereses de los stakeholders, cumpliendo con la ley de protección de datos personales, norma técnica peruana de la historia clínica y ley de emergencia.
	Entender la arquitectura de negocio y de sistemas de la empresa empleada para dar soporte al proceso e identificar posibles brechas de seguridad de información.
	Identificar los interesados del dentro del proceso y sus requerimientos.
	Determinar las prioridades para desarrollar los cambios estratégicos a nivel de proceso.
Definir el objetivo de las capacidades de TI	Asegurar que los requerimientos de seguridad de información estén incluidos dentro de las capacidades de TI.
	Definir y acordar el impacto de los requerimientos de seguridad de información dentro de la arquitectura de la empresa que soporta el proceso de admisión, según lo que los stakeholders consideren relevante.

	Definir de acuerdo al proceso de admisión, las capacidades y servicios de TI a entregar.
	Definir los objetivos de TI a alto nivel y cómo contribuirán a los objetivos de negocio empresariales y como soporta este proceso al cumplimiento de ambos.
Realizar un análisis de brecha	Identificar dentro del proceso las brechas a cerrar y los cambios requeridos para llegar al nivel deseado.
	Examinar el nivel de cumplimiento del proceso respecto a la ley de protección de datos personales, norma técnica peruana de la historia clínica y la ley de emergencia.
	Mejorar la definición del estado deseado en el proceso y sus objetivos. Sustentarlos demostrando los beneficios a partir de este estado frente al impacto en caso no se llegara a esta meta
Definir el plan estratégico y la hoja de ruta	Definir la estrategia de seguridad de información y alinearla con la de TI y las estrategias de negocio para el cumplimiento de objetivos en el proceso de admisión.
	Crear la hoja de ruta que incluya la planificación e interdependencias de las iniciativas a nivel empresarial de acuerdo al proceso, la cual a su vez señale los riesgos y costos de los cambios.
	Asegurar que el plan estratégico de TI y la hoja de ruta contengan los requerimientos de seguridad de información identificados en el proceso de admisión
	Obtener el apoyo de las partes interesadas y la aprobación del plan.
Comunicar la estrategia y la dirección de TI	Desarrollar el plan estratégico y el plan de seguridad de información que incluya aspectos relacionados al proceso de admisión y comunicarlo a los stakeholders
	Desarrollar el plan de comunicación de acuerdo a público objetivo identificando los canales de comunicación.
	Obtener retroalimentación y actualizar el plan de comunicaciones y la estrategia de seguridad de información y TI según sea necesario para mantener el impulso.

Tabla 9.1.14 - Proceso admisión. Actividades de gestión habilitador: Gestionar la estrategia

Matriz de responsabilidades (RACI)

APO02: Gestionar la estrategia																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Comprender la dirección de la empresa		C	C	C	A	C	C			C	R	C			R	C	I	I	R	C
Definir objetivo de capacidades de TI		A	C	C	C	I	R	C	I	C	C			I	R	C	C	C	C	C
Realizar un análisis de brecha					R	R	C			C	C		C	C	A	C	C	I	R	C
Definir plan estratégico y hoja de ruta		C	I	C	C		C		R	C	C			C	A	C	C	C	C	C
Comunicar estrategia y dirección de TI	I	R	I	I	R	I	A	I	I	I	R	I	I	I	R	I	I	I	I	I

Tabla 9.1.15 - Matriz de responsabilidades para el proceso habilitador APO02 - Proceso Admisión

b. <u>Proceso habilitador: Gestionar los recursos humanos</u>

Se muestra a continuación las actividades que aplican para este proceso de admisión bajo el enfoque de seguridad de información. Posteriormente se muestra la matriz de responsabilidades para su gestión en la organización y a nivel de los actores del proceso.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Mantener la dotación del personal suficiente y adecuado	Evaluar las necesidades de personal periódicamente o frente a cambios organizacionales de forma de asegurar que tanto TI como la empresa cuenta con recursos para soportar el proceso de admisión y la iniciativa de TI
	Dentro de los procesos de contratación, incluir controles de antecedentes de acuerdo a la función a realizar.

	Asegurar que los requisitos de seguridad se incorporan en el proceso de contratación.
	Asegurar la existencia de capacitaciones y que existe personal capaz de cubrir funciones críticas de otro para reducir la dependencia.
Identificar personal clave de TI	Asegurar la segregación de funciones en roles críticos del proceso.
	Minimizar dependencia de una persona en la realización de una función crítica dentro del proceso de admisión a través de captura e intercambio de conocimiento.
	Identificar y ejecutar acciones según cambios laborales relacionados a los actores del proceso de admisión.
Mantener las habilidades y competencias del personal	Definir habilidades y competencias necesarias de los recursos para lograr los objetivos dentro del proceso y poder escalar hacia los objetivos de alto nivel.
	Brindar capacitaciones y programas de seguridad de información al personal que ejecuta los procesos y a nivel transversal para formar conciencia.
	Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. A partir de estas identificar si se requieren habilidades adicionales para cubrir el proceso y ejecutar el plan de acción para desarrollarlas.
	Asegurar conocimientos y habilidades del personal solicitando certificaciones según la función a realizar. En caso de la seguridad de información, si aplicase, se podría solicitar certificaciones como ISO/IEC 27002, CISM, ISO/IEC 27001: Leed Auditor.
Evaluar el desempeño laboral de los empleados	Dentro de la evaluación del desempeño, considerar criterios con respecto a la seguridad de información.
	Establecer objetivos individuales alineados con los objetivos del proceso de admisión. Deben reflejar competencias básicas, valores empresariales y habilidades para las funciones.
	Proporcionar instrucciones para uso y almacenamiento de información personal dentro del proceso de

	evaluación.
	Implementar un proceso de reconocimiento a medida que el personal alcance el compromiso, desarrollo de competencias y logro de objetivos.
Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio	Gestionar la ubicación del personal de seguridad de información de acuerdo a los requerimientos de negocio.
	Comprender la demanda actual y futura de recursos humanos involucrados dentro del proceso de admisión para apoyar el logro de objetivos de TI y necesidades operativas del día a día.
	Mantener información adecuada sobre el tiempo dedicado a diferentes tareas, trabajos, servicios o proyectos
Gestionar el personal contratado	Obtener un acuerdo formal por parte del personal sobre las políticas y requisitos de la seguridad de información a aplicarse en el proceso de admisión.
	Implementar políticas o procedimientos que describan como gestionar el personal para identificar necesidad de tercerizar algún servicio de TI.
	Llevar a cabo revisiones para asegurar que el personal cumple con sus funciones, que el derecho de acceso son adecuados y alineados con los acuerdos pactados al firmar el contrato.

Tabla 9.1.16 - Proceso admisión. Actividades de gestión habilitador: Gestionar los recursos humanos

Matriz de responsabilidades (RACI)

APO07: Gestionar los recursos humanos																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Mantener personal suficiente y adecuado									R	I	C		R		A	R	R	C	R	C
Identificar personal clave de TI								I	R		R		R		A	R	R	R	R	R
Mantener habilidad y competencia del personal									R		C		R		A	R	R	R	R	R
Evaluar desempeño laboral del empleado									R		R		R		A	R	R	R	R	R
Planificar y realizar seguimiento del uso de recusos humanos de TI y negocio					R	C	A	R	R		C		I		R	R	R	C	R	C
Gestionar personal contratado							I	I	R		C		R		A	R	C	C	R	C

Tabla 9.1.17 - Matriz de responsabilidades para el proceso habilitador APO07 - Proceso Admisión

c. Proceso habilitador: Gestionar el riesgo

En el proceso habilitador gestión de riesgo, se toma como alcance los riesgos de seguridad de información que pueden desencadenarse en el proceso de admisión de pacientes y bajar la calidad de su performance.

Se detalla también la matriz de responsabilidades para llevar a cabo la gestión del habilitador y llevarlo al nivel de madurez deseado por la empresa siguiendo el enfoque de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Recopilar datos	Identificar y recolectar datos para la identificación, análisis y comunicación de los riesgos de seguridad de información.

	Medir y analizar datos históricos de riesgo de TI y seguridad de información suscitados dentro del proceso de admisión y de pérdidas experimentadas de acuerdo a las tendencias externas.
	Determinar condiciones específicas que existían o faltaban cuando se materializaron los riesgos dentro de los procesos y como afectaban la frecuencia del evento y la pérdida.
	Ejecutar análisis del entorno para verificar los factores de riesgo asociados al proceso.
Analizar el riesgo	Identificar, analizar y evaluar los riesgos de información dentro del proceso.
	Construir los escenarios de riesgo de TI y seguridad dentro del proceso. Incluir las asociaciones y dependencias entre las amenazas, para detectar medidas de emergencia.
	Identificar los riesgos residuales dentro del proceso e identificar exposiciones que puedan requerir una repuesta al riesgo
	Validar resultados del análisis de riesgos del proceso antes de usarlos para la toma de decisiones. Verificar alineamiento con requerimientos organizacionales.
Mantener un perfil del riesgo	Crear e informar el nivel aceptable y exposición al riesgo que incluya los aspectos de seguridad de acuerdo al proceso.
	Identificar dentro del proceso los servicios esenciales para sostenerlo. Analizar la dependencia e identificar debilidades.
	Definir un conjunto de indicadores que permitan la identificación rápida y supervisión de los riesgos de seguridad del proceso y sus tendencias.
Expresar el riesgo	Definir e implementar evaluaciones y estrategias de respuesta frente a los riesgos del proceso de admisión.
	Informar los resultados del análisis de riesgos a los stakeholders sobre el proceso de admisión en términos adecuados y entendibles para soportar decisiones

	empresariales.
	Informar el perfil del riesgo a los stakeholders junto con la efectividad del proceso de admisión y los controles asociados y a la vez identificar oportunidades de TI para aceptar un mayor riesgo e incrementar la capacidad de gestión.
Definir un portafolio de acciones para la gestión de riesgos	Monitorear continuamente los riesgos de seguridad de información del proceso de admisión y verificar que el riesgo este alineado con el apetito y tolerancia al riesgo definido por la organización.
	Definir conjunto de propuestas para reducir el riesgo o proyectos para incrementar las oportunidades estratégicas de acuerdo a los beneficios y regulaciones.
Responder al riesgo	Aplicar las prácticas y controles para la mitigación de riesgos de seguridad. Se recomienda aplicar en este caso la norma ISO/IEC 27002:2013. Incluir controles preventivos y correctivos.
	Catalogar los incidentes y comunicar los impactos de negocio a los responsables.

Tabla 9.1.18 - Proceso admisión. Actividades de gestión habilitador: Gestionar el riesgo

Matriz de responsabilidades (RACI)

APO12: Gestionar el riesgo																				
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Recopilar datos		I				R		I	R	R	R	I		C	A	C	C	C	R	C
Analizar el riesgo		I				R		I	C	R	C	I		C	A	C	C	C	R	C
Mantener un perfil del riesgo		I				R		I	C	A	C	I		C	R	C	C	C	R	C

Expresar el riesgo		I				R		I	C	R	C	I		C	A	C	C	C	C	C
Definir portafolio de acciones para gestión del riesgo		I				R		I	C	A	R	I		C	R	I	C	I	C	C
Responder al riesgo		I				R		I	R	R	R	I		C	A	R	R	R	R	R

Tabla 9.1.19 - Matriz de responsabilidades para el proceso habilitador APO12 - Proceso Admisión

d. Proceso habilitador: Gestionar la seguridad

El siguiente proceso habilitador indica cómo debe gestionarse la función de seguridad de información. Para este proceso se recomienda la alineación con un sistema de gestión de seguridad de información, por ser un proceso core de negocio, y su alineamiento con la ley de protección de datos personales, norma técnica peruana de la historia clínica y la ley de emergencia. Se muestra también la matriz de responsabilidades, destacando que es el oficial de seguridad de información quien mantiene un SGSI alineado a las necesidades y requerimientos de la organización.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Establecer y mantener un SGSI	Definir el alcance del SGSI de acuerdo a las características de la organización y sus políticas.
	Diseñar un enfoque de gestión de seguridad y alinear el SGSI a este.
	Realizar la declaración de la aplicabilidad del SGSI.
	Comunicar los roles y responsabilidades en la gestión de la seguridad de información y el enfoque del SGSI.
	Comprometer a la alta dirección para iniciar las actividades de implementación del SGSI.
Definir y gestionar un plan de tratamiento del riesgo de la seguridad de información	Diseñar, mantener y aplicar un plan de tratamiento de riesgos de seguridad de información alineados con los objetivos estratégicos de la organización y fines del proceso.
	Desarrollar propuestas de mejora al plan de riesgos basados en casos de negocio de acuerdo a los roles y responsabilidades a necesitar para su aplicación y acorde a los drivers identificados.
	Definir la medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizarlas

	para producir resultados reproducibles y comparables.
	Integrar la planificación, diseño, implementación y supervisión de procedimientos de seguridad y controles para prevención y detección temprana de eventos dentro del proceso de admisión y la respuesta a incidentes.
Supervisar y revisar el SGSI	Realizar revisiones periódicas del SGSI incluyendo las políticas, objetivos definidos en la etapa de concepción del SGSI
	Realizar evaluaciones o auditorías al SGSI de forma periódica para determinar su cumplimiento e identificar mejoras en el proceso.
	Registrar acciones y eventos que podrían tener impacto en la efectividad o desempeño del SGSI.

Tabla 9.1.20 - Proceso admisión. Actividades de gestión habilitador: Gestionar la seguridad

Matriz de responsabilidades (RACI)

APO13: Gestionar la seguridad	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Establecer y mantener un SGSI		C		C	C	C	C	I	I	C	A	C		I	R	I	I	I	R	C
Definir gestionar plan tratamiento de riesgos de seguridad información		C		C	C	C	C	I	I	C	A	C		I	R	C	C	C	R	C
Supervisar y revisar el SGSI					C	R	C	I	R		A			C	R	R	R	R	R	R

Tabla 9.1.21 - Matriz de responsabilidades para el proceso habilitador APO13 - Proceso Admisión

e. Proceso habilitador: Gestionar los programas y proyectos

Para el proceso de admisión se consideran aplicables algunas actividades de gestión de este proceso habilitador debido a que dentro de la organización el conjunto de procesos que integran el macro-proceso hospitalario cubren un único programa. No obstante, no aplican todas las actividades relacionadas a proyecto debido a que como parte de este proceso de negocio es más relevante tratarlos a alto nivel, encaminarlos y alinearlos estratégicamente con la cartera de proyectos y los requerimientos de seguridad de información. Se muestra también la respectiva matriz de responsabilidades de acuerdo al análisis y aplicación del habilitador.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Mantener un enfoque estándar para la gestión de programas y proyectos.	Incorporar los requerimientos de seguridad de información dentro de los proyectos asociados al proceso de admisión.
	Establecer procedimientos para asegurar que todos los proyectos relacionados al proceso e información cuentan con las medidas de seguridad requeridas o exigibles.
	Actualizar el enfoque de gestión de programas y proyectos en base a mejoras a partir del uso de estas estrategias.
Gestionar el compromiso de las partes interesadas.	Identificar como las partes interesadas se asocian a los proyectos relacionados con el proceso y comprometerlos para que se involucren y tomen medidas respecto a estos programas o proyectos.
Desarrollar y mantener el plan del programa.	Desarrollar un plan de seguridad de información que incluya controles a implementar por parte del equipo de proyecto dentro del proceso.
	Incluir recursos dentro del proyecto para identificar e implementar los requerimientos de seguridad de información.
	Asignar la responsabilidad ejecutiva para cada proyecto en forma clara y sin ambigüedades, incluyendo beneficios, control de costos, la gestión de riesgos y la coordinación de las actividades de los proyectos.
	Mantener el plan de programa para asegurar su actualización de acuerdo al proyecto y el proceso al que está asociado, así como la actualización del caso de

	negocio que lo justifica y garantiza el alineamiento estratégico.
Planificar proyectos	Integrar la seguridad de información y las tecnologías con la gestión de proyectos.
	Desarrollar plan de proyecto con información que permita a la dirección controlar el progreso del proyecto. Incluir recursos, responsabilidades e hitos que marcan el cierre de cada una de las etapas.
	Mantener los planes de proyecto y sus dependencias, asegurando la comunicación entre estos y que al realizar un cambio en uno de éstos se refleje en los demás.
	Establecer un marco base para proyectos, el cual es revisado, aprobado e incorporado a los planes de proyecto vigentes.
Gestionar la calidad de los programas y proyectos.	Identificar las actividades y prácticas para garantizar la calidad de los proyectos. Asegurar que las tareas provean garantías del cumplimiento de los requerimientos definidos.
	Definir los requerimientos de validación y verificación de la calidad de entregables de los proyectos asociados al proceso.
Gestionar el riesgo de los programas y proyectos.	Registrar riesgos de seguridad de información y las acciones correctivas frente a estos. Revisar y actualizar la matriz de riesgos de proyecto periódicamente.
	Integrar proyectos de seguridad de información al programa y proceso de admisión de pacientes. Alinearlos a los procesos de gestión de proyectos.
	Asignar la responsabilidad al personal con capacidades adecuadas para ejecutar el proceso de gestión del riesgo de los proyecto.
Supervisar y controlar proyectos.	Determinar evaluaciones periódicas a los proyectos para asegurar que los requerimientos de seguridad de información asociados al proceso son implementados de forma efectiva.
	Supervisar los cambios al programa y revisar requerimientos claves de desempeño para verificar el

	avance.
	Obtener la aprobación y firma de los entregables producidos en cada iteración del proyecto asociado al proceso.

Tabla 9.1.22 - Proceso admisión. Actividades de gestión habilitador: Gestionar programas y proyectos

Matriz de responsabilidades (RACI)

BAI01: Gestionar programas y proyectos	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Mantener enfoque para gestión de programas y proyectos	I	A	C	C	R		R		C	C	C			I	R				C	
Gestionar el compromiso de las partes interesadas		A	C	C	R	C	C	R	I		I				R	I	C	I	C	C
Desarrollar y mantener el plan del programa			C	C	A	C		R	R	C	R			C	C	I	C	I	R	C
Planificar proyectos						C	I	A	R		C				C	C	C	C	R	C
Gestionar la calidad de los programas y proyectos					C	R	I	A	R	C	R			I	C	I	C		C	C
Gestionar el riesgo de los programas y proyectos					R	R	I	A	R	C	R			I	C	C	C	C	R	C
Supervisar y controlar proyectos					I	R	I	A	R	C	C			C	C	I	C	C	R	C

Tabla 9.1.23 - Matriz de responsabilidades para el proceso habilitador BAI01 - Proceso Admisión

f. Proceso habilitador: Gestionar el cambio

El siguiente proceso habilitador pretende contrarrestar los cambios y la resistencia a estos dentro de la organización alineándolos a las estrategias y a los requerimientos de seguridad de información. Para estos se toma en cuenta la alineación y

cumplimiento con la ley de protección de datos personales, norma técnica peruana de la historia clínica y la ley de emergencia.

Se detalla también el esquema de roles a seguir para la aplicación del habilitador en la matriz de responsabilidades ajustada al proceso de admisión y la lista de actividades de aplicación. Se destaca la intervención del oficial de seguridad de información para que supervise que los cambios se alinean a los requerimientos de seguridad de información definidos y el cumplimiento con la regulación.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Evaluar, priorizar y autorizar solicitudes de cambio	Asegurar que los cambios se ajustan a la política de seguridad de información.
	Asegurar que se realice la evaluación del impacto potencial de los cambios en seguridad de información
	Garantizar la aprobación del cambio por parte de los los dueños del proceso de admisión, gestores de servicio y los respectivos stakeholders. Considerar los tipos de cambio para su aprobación.
	Formalizar las solicitudes de cambio y estandarizarlas de manera que todo cambio a nivel del proceso sea a través de un procedimiento definido. Realizar la respectiva clasificación para identificar y mejorar la gestión.
	Evaluar las solicitudes de manera estructurada en base a su priorización y de acuerdo a las funciones del proceso. Realizar el análisis de impacto dentro de los planes y servicios que involucra este proceso considerando a los proveedores y los acuerdos de servicio.
Gestionar cambios de emergencia	Desarrollar medidas para atender cambios de emergencia en el proceso de admisión a nivel de la seguridad de información.
	Mantener un registro de los riesgos de seguridad de información a partir de cambios de emergencia realizados en el proceso.
	Supervisar los cambios de emergencia dentro del proceso de admisión y realizar las revisiones post-implantación involucrando a las partes interesadas.

Hacer seguimiento e informar cambios de estado	Mantener un sistema de seguimiento e informe para todas las solicitudes de cambio enfocados en seguridad de información dentro del proceso de admisión.
	Supervisar los cambios de seguridad de información abiertos para asegurar que sean cerrados en los plazos previstos.
	Elaborar los informes de cambio en seguridad de información dentro del proceso y que incluyan las métricas de rendimiento para facilitar su revisión y seguimiento
Cerrar y documentar los cambios	Realizar la documentación sobre las revisiones de cambios de seguridad de información.
	Definir un periodo válido para preservar la información sobre los cambios realizados dentro del proceso bajo los enfoques de seguridad.

Tabla 9.1.24 - Proceso admisión. Actividades de gestión habilitador: Gestionar el cambio

Matriz de responsabilidades (RACI)

BAI06: Gestionar el cambio	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Evaluar, priorizar y autorizar peticiones de cambio					A	R			C	C	R			C	R	C	C	R	R	
Gestionar cambios de emergencia					A	I				C	R			I	R	C	R	I	R	
Hacer seguimiento e informar cambios de estado					C	R			C		C				A	C	R	C	R	
Cerrar y documentar los cambios					A	R			R	C	C				R	C	R	I	C	

Tabla 9.1.25 - Matriz de responsabilidades para el proceso habilitador BAI06 - Proceso Admisión

g. Proceso habilitador: Gestionar los activos

En este proceso habilitador aplican todas las actividades de gestión a excepción de la optimización del costo de los activos, pues requiere manejo de inversiones frente a tecnologías de información, lo cual se gestiona desde el proceso de gobierno Garantizar la entrega de beneficios. Se muestra también la matriz de responsabilidades.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Identificar y registrar activos actuales	Identificar los activos asociados al proceso, registrarlos indicando su estado actual. Alinearlos con procesos de gestión de cambios y enfocarlos a la función de seguridad de información.
	Identificar requerimientos de seguridad de información de acuerdo a los activos del proceso de admisión. Tener en cuenta sus dependencias entre ellos.
	Identificar requerimientos legales o reglamentarios sobre seguridad de información que deban de considerarse dentro de la gestión de activos del proceso.
	Determinar si el activo proporciona valor dentro del proceso y si continúa en condiciones útiles para soportar dicho proceso.
Gestionar activos críticos	Garantizar el cumplimiento de requisitos de seguridad de información en los activos que comprenden el proceso.
	Definir niveles de criticidad. De acuerdo a esto, identificar activos críticos y registrarlos. Esta evaluación deberá realizarse en torno a los requerimientos de seguridad de información.
	Considerar el riesgo de falla, necesidad de cambio o reemplazo total del activo critico dentro del proceso para cumplir la función de seguridad de información.
	Supervisar el rendimiento de los activos críticos por medio de evaluaciones o planes en los cuales se definan procesos para reparación o reemplazos.
Gestionar el ciclo de vida de los activos	Identificar y comunicar los riesgos de seguridad de información y los incumplimientos respecto a las medidas

	para mitigarlos a lo largo del ciclo de vida de los activos del proceso de admisión.
	Asegurar que las medidas de seguridad de información y los requerimientos estén alineados al ciclo de vida.
	Realizar adquisiciones de activos en base a solicitudes aprobadas de acuerdo a las políticas y prácticas de la empresa bajo los criterios de la seguridad de información y alineados al proceso de admisión de pacientes.
	Eliminar activos de forma segura siguiendo procedimientos que garanticen la protección y destrucción de datos que alguna vez estuvieron almacenados en ellos.
Administrar licencias	Establecer procedimientos de control en base a instalaciones de sistemas o software dentro de los activos de TI.
	Mantener un registro de todas las licencias de software adquiridas para los activos que soportan el proceso base.
	Realizar auditorías para identificar si existe software no autorizado o si se cumplen los mecanismos de control evidenciados en el inventario y registro de activos.

Tabla 9.1.26 - Proceso admisión. Actividades de gestión habilitador: Gestionar los activos

Matriz de responsabilidades (RACI)

BAI09: Gestionar los activos	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Identificar y registrar activos actuales			C			C					C				I	R	A	C	C	
Gestionar activos críticos			C		I	C				C	C			C		R	A	C	C	C

Gestionar el ciclo de vida de los activos						C				I	C					R	A	R	I	
Administrar licencias					I	C					I			C	A	R	R	C		

Tabla 9.1.27 - Matriz de responsabilidades para el proceso habilitador BAI09 - Proceso Admisión

h. Proceso habilitador: Gestionar las solicitudes e incidentes de servicio

Este proceso habilitador indica las actividades a seguir para llevar a cabo la gestión de incidentes y solicitudes de seguridad de información, los cuales pueden ser inmediatos o a través de algún proceso para su solución temporal o total. Se prioriza aquellas solicitudes o incidentes de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Definir esquemas de clasificación de incidentes y solicitudes de servicio	Definir y comunicar las características de los incidentes potenciales de seguridad de información para su reconocimiento y comprender el impacto que podría tener en el proceso.
	Definir modelos de solicitudes de servicio relacionados a la seguridad de información para facilitar la su atención y respuesta dentro del proceso de admisión.
	Definir la clasificación y priorización de incidentes y solicitudes de servicio relacionados al proceso de admisión tomando en cuenta los requerimientos de seguridad de información.
Registrar, clasificar y priorizar solicitudes e incidentes	Investigar los incidentes de seguridad y elaborar, en base a estos, procedimientos de respuesta. Asegurar que las medidas sean definidas y protejan los pilares de seguridad y que sean difundidas.
	Registrar incidentes y solicitudes de servicio relacionados a la seguridad de información dentro del proceso de admisión.
	Realizar la priorización y clasificación de los incidentes de acuerdo al impacto dentro del negocio y al proceso de admisión.
Verificar, aprobar y resolver solicitudes de	Seguir procedimientos y modelos de solicitudes para elementos frecuentes de seguridad de información, para

servicio	así resolver solicitudes de forma estandarizada.
Investigar, diagnosticar y localizar incidentes	Mantener procedimientos para recopilar evidencias sobre incidentes de acuerdo a requisitos externos y el marco legal al cual se encuentra sujeto el proceso. Asegurar que el personal esté al tanto de los requisitos.
	Registrar un nuevo problema en caso no exista dentro de la base de datos y/o si el incidente de seguridad de información es recurrente.
	Identificar posibles soluciones temporales o permanentes para los incidentes de seguridad de información, asignar su tratamiento a los especialistas respectivos.
Resolver y recuperarse de incidentes	Definir un plan de respuesta para los incidentes de seguridad de información en el cual se detalla las soluciones apropiadas.
	Ejecutar las acciones de recuperación para restablecer el proceso de admisión completamente.
	Documentar la solución e identificar si es temporal o permanente para tomarlo en cuenta a futuro.
Cerrar solicitudes de servicio e incidentes	Verificar con los usuarios del proceso si se ha completado la solicitud del servicio o si el incidente ha sido resuelto. En caso afirmativo cerrar la solicitud o incidente.
Seguir el estado y emitir informes	Asegurar que los incidentes de seguridad de información, el análisis y seguimiento de estos, siguen los procedimientos existentes.
	Informar el resultado de las investigaciones sobre los incidentes de seguridad a las partes interesadas y a la gerencia ejecutiva.
	Elaborar informes y distribuirlos periódicamente a los stakeholders como parte de la mejora continua.

Tabla 9.1.28 - Proceso admisión. Actividades de gestión habilitador: Gestionar las solicitudes e incidentes de servicio

Matriz de responsabilidades (RACI)

DSS02: Gestionar solicitudes e incidentes de servicio																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Definir esquema de clasificación de incidentes y solicitud de servicio						C				I	I				A	C	R	R	R	C
Registrar, clasificar y priorizar solicitudes e incidentes						I				I	C						A	R	C	
Verificar, aprobar y resolver solicitudes de servicio						R				C	C				I	C	R	A	C	
Investigar, diagnosticar y localizar incidentes						R				I	C			I	I	C	R	A	C	
Resolver y recuperarse de incidentes						I				I	I			I	I	C	R	A	R	
Cerrar solicitudes de servicio e incidentes						C				I	C			I	I	I	A	C	R	
Seguir el estado y emitir informes						I				I	C	I		I	I	I	A	R	C	

Tabla 9.1.29 - Matriz de responsabilidades para el proceso habilitador DSS02 - Proceso Admisión

i. Proceso habilitador: Gestionar la continuidad

El siguiente proceso habilitador indica cómo crear estrategias que garanticen que el proceso de admisión de pacientes estará disponible ante diversas situaciones y emergencias. En este caso se busca el compromiso del oficial de seguridad de información que señale que los incidentes o riesgos de seguridad de información, en caso se materialicen, afectaran lo menos posible la continuidad de negocio.

Se presenta también la matriz de responsabilidades de acuerdo al proceso de admisión de pacientes y el proceso habilitador, realizando los ajustes que orienten el enfoque de gobierno de TI, seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Definir las políticas de continuidad de negocio, objetivos y alcance	Determinar el nivel de criticidad del proceso de admisión de pacientes a nivel de seguridad de información y de acuerdo a la ley de protección de datos personales, norma técnica peruana de la historia clínica y ley de emergencia, para verificar que su aplicación en el programa de continuidad.
	Asegurar que la seguridad de información forma parte del ciclo de vida de continuidad de negocio.
	Identificar partes interesadas, roles y responsabilidades claves dentro del proceso para alinearlos a los objetivos y políticas del SGCN.
Mantener una estrategia de continuidad	Identificar e incluir escenarios que den pie a eventos que afecten la continuidad del proceso de admisión dentro del enfoque de la seguridad de información.
	Realizar el análisis de impacto de negocio para el proceso de admisión, incluyendo los factores de seguridad de información y el máximo tolerable de interrupción en estos aspectos.
	Analizar las amenazas que afecten la continuidad del proceso bajo el enfoque de la seguridad de información para mejorar métodos preventivos e incrementar la resiliencia.
	Obtener la aprobación de los ejecutivos y dar pie a las estrategias seleccionadas que cubran los requerimientos definidos para el SGCN bajo el enfoque de seguridad de información.
Desarrollar e implementar una respuesta a la continuidad de negocio	Alinear los aspectos de seguridad de información del proceso de admisión a las estrategias de continuidad y el SGCN. Incluirlas en el Plan de continuidad de negocios.
	Asegurar que los proveedores clave del proceso definan estrategias de continuidad de negocio y recuperación. Evaluar cómo afecta que no se cuente con estas para considerarlo dentro de las políticas del SGCN.
	Definir los procedimientos de recuperación para reanudar el proceso de admisión y que este cumpla con los

	requerimientos de seguridad de información definidos.
	Definir y documentar recursos necesarios para recuperar el proceso, incluyendo todos los planes documentados y considerando las necesidades de seguridad y almacenamiento de la información en otro lugar. Distribuir los planes.
Ejecutar, probar y revisar el plan de continuidad	Planificar actividades para probar el plan como está definido en los documentos. Asignar roles y responsabilidades para esta actividad.
	Realizar el análisis y revisión para determinar el logro.
Revisar, mantener y mejorar el plan de continuidad	Considerar que los incidentes de seguridad de información, dentro del proceso de admisión, son fuentes para probar y verificar las repuestas del plan de continuidad de negocios.
	Revisar el plan periódicamente tomando en cuenta los objetivos de negocio, objetivos de TI y los lineamientos del proceso de admisión junto con sus estrategias de seguridad. Considerar posibles cambios producto del entorno.
	Comunicar los cambios en torno al plan de continuidad que puedan afectar los procesos o los requerimientos de seguridad de información
Gestionar acuerdos de respaldo	Asegurar que los requerimientos de seguridad se cumplen en los procesos de backup y restauración de la información dentro del proceso de admisión de pacientes.
	Realizar las copias de seguridad respectivas y establecer políticas para su gestión de acuerdo a las regulaciones y exigencias dentro del proceso de admisión, salvaguardando los datos del paciente.
	Probar y mantener las copias de seguridad recientes y aquellas archivadas de manera periódica para garantizar la disponibilidad de la información y su integridad.
Ejecutar revisiones post-reanudación	Asegurar que los parámetros y niveles de seguridad estén incluidos luego de la reanudación del proceso de admisión.

	Evaluar la efectividad del plan de acuerdo a los tiempos definidos en el análisis de impacto de negocio de acuerdo al proceso de admisión.
	Identificar debilidades u omisiones como parte de la mejora continua para asegurar que el proceso de admisión podrá llevarse a cabo sin inconvenientes ante cualquier evento bajo condiciones seguras.

Tabla 9.1.30 - Proceso admisión. Actividades de gestión habilitador: Gestionar la continuidad

Matriz de responsabilidades (RACI)

DSS04: Gestionar la continuidad	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Definir la política de continuidad de negocio, objetivos y alcance				A	C	R				C	C			C	R	I	C	C	R	R
Mantener una estrategia de continuidad				A	C	R				I	I			C	R	I	R		R	R
Desarrollar e implementar una respuesta a la continuidad de negocio					I	R					C		I	C	R	I	C		R	A
Ejercitar, probar y revisar el plan de continuidad					I	R					I		I	R	R	I	R	I	R	A
Revisar, mantener y mejorar el plan de continuidad				A	I	R				I	C				R		C		C	R
Gestionar acuerdos de respaldo											I					C	I		C	R
Ejecutar revisiones post-reanudación					C	R				I	C				R	I			C	A

Tabla 9.1.31 - Matriz de responsabilidades para el proceso habilitador DSS04 - Proceso Admisión

j. Proceso habilitador: Gestionar los servicios de seguridad

Se muestra la aplicación de las actividades de gestión de acuerdo al proceso que garanticen la seguridad a nivel técnico y lógico para el procesamiento y almacenamiento de datos.

Así mismo, se muestra la matriz de responsabilidades para dar continuidad a lo largo del ciclo de vida de gobierno a este proceso habilitador y su aplicación en el proceso de negocio de admisión de pacientes.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Proteger contra software malicioso	Instalar y activar herramientas de protección frente a software malicioso en todas las estaciones que procesan la información del paciente. Concientizar al usuario de estas sobre las amenazas y forzar la responsabilidad de prevención.
	Revisar y evaluar sobre nuevas amenazas que afecten las fuentes de procesamiento de información de los pacientes.
	Filtrar el tráfico entrante, como los correos electrónicos y descargas para protegerse frente a información no solicitada y sensible.
Gestionar la seguridad de la red y las conexiones	De acuerdo al análisis de riesgo, mantener una política de seguridad para conexiones.
	Cifrar la información en tránsito de acuerdo con su clasificación verificando el cumplimiento con la ley de protección de datos personales y norma técnica peruana de la historia clínica.
	Establecer mecanismos para recepción segura de la información.
	Realizar pruebas sobre la seguridad del sistema para determinar la protección sobre los datos intercambiados dentro del proceso de admisión de pacientes.
Gestionar la seguridad de los puestos de usuario final	Configurar los sistemas operativos de forma correcta y segura en las estaciones que abarcan el proceso de admisión.

	Cifrar la información almacenada y gestionada de acuerdo a su clasificación
	Implementar mecanismos de bloqueo de los dispositivos.
	Implementar el filtrado del tráfico de la red en dispositivos de usuario final dentro del proceso de admisión
	Deshacerse de los dispositivos de usuario final de forma segura.
Gestionar la identidad del usuario y el acceso lógico	Mantener los derechos de acceso de los usuarios de acuerdo a los requerimientos del proceso de admisión.
	Autenticar los accesos a los activos de información de acuerdo al nivel de seguridad y según los lineamientos de los procesos de negocio.
	Segregar y gestionar cuentas de usuario privilegiadas.
	Realizar revisiones periódicas de la gestión de cuentas y privilegios dentro del proceso de admisión. Verificar que la identificación de estas es unequívoca.
Gestionar documentos sensibles y dispositivos de salida	Establecer procedimientos de empleo, eliminación y destrucción de las historias clínicas y actas de conformidad y garantía.
	Asignar privilegios de acceso a información de historias clínicas, actas de conformidad y garantía.
	Realizar un inventario de documentos sensibles y dispositivos de salida críticos para llevar a cabo el proceso de admisión de pacientes.
	Establecer políticas de protección física apropiadas sobre formularios o documentos que contienen información sensible.

Tabla 9.1.32 - Proceso admisión. Actividades de gestión habilitador: Gestionar los servicios de seguridad

Matriz de responsabilidades (RACI)

DSS05: Gestionar los servicios de seguridad																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Proteger contra software malicioso						R				C	A		R		C	I	R	I	C	
Gestionar seguridad de red y conexiones						I				C	A			C	C	I	R	I	C	
Gestionar seguridad de puestos de usuario final						I				C	A		I		C		R	I	R	
Gestionar identidad del usuario y acceso lógico						R				C	A		I	C	C		R	I	R	C
Gestionar documentos sensibles y dispositivos de salida						C	I			I	C				A	I	R		R	

Tabla 9.1.33 - Matriz de responsabilidades para el proceso habilitador DSS05 - Proceso Admisión

1.1.3 Proceso Atención del paciente

Otro de los procesos que forman parte del alcance del proyecto de tesis es el proceso de atención. Este proceso a diferencia del proceso de admisión, contiene más actividades manuales y de gestión debido a que su objetivo es garantizar la seguridad y confort del paciente brindándole la atención y cuidados respectivos. No se deja de lado las actividades técnicas y la gestión de información confidencial como las historias clínicas.

a. Proceso habilitador: Gestionar la estrategia

En este proceso habilitador, de acuerdo al proceso de atención, se determina la estrategia a seguir por parte del personal y según lo determina la alta dirección para cumplir con los requerimientos y la función de seguridad de información.

Se presenta la matriz de responsabilidades para gestionar el habilitador de acuerdo al enfoque de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Comprender la dirección de la empresa	Entender como la seguridad de información debe respaldar los objetivos de la organización dentro del proceso de atención al paciente hospitalizado, cumpliendo con la ley de protección de datos personales y la norma técnica peruana de la historia clínica.
	Identificar los stakeholders e interesados del proceso de atención y sus requerimientos.
	Desarrollar y mantener un entendimiento de las estrategias, objetivos de negocio, entorno y retos operativos actuales dentro del proceso de admisión acorde con la seguridad de información.
	Determinar las prioridades para desarrollar los cambios estratégicos a nivel de proceso.
Evaluar entorno, capacidades y rendimientos actuales	Establecer la línea base de seguridad de información dentro del proceso de atención al paciente.
	Crear criterios de seguridad de información claros y relevantes dentro del proceso de atención de pacientes. Identificar los riesgos.
	Identificar diferencias entre el proceso de negocio actual y las capacidades de TI según estándares de calidad y mejores prácticas.
	Identificar debilidades, fortalezas, oportunidades y amenazas del proceso de atención y las capacidades y servicios para evaluar el desempeño actual de las funciones de seguridad de información.
Realizar un análisis de brecha	Identificar dentro del proceso las brechas a cerrar y los cambios requeridos para llegar al nivel deseado.
	Examinar el nivel de cumplimiento con la ley de protección de datos personales, norma técnica peruana de la historia clínica dentro del proceso de atención al paciente.

	Definir las metas deseadas del proceso y establecer los beneficios que se obtienen al llegar a estas.
Definir el plan estratégico y la hoja de ruta	Definir la estrategia de seguridad de información y alinearla a la estrategia de negocio para cumplir los objetivos del proceso.
	Crear la hoja de ruta que incluya la planificación e interdependencias de las iniciativas a nivel empresarial de acuerdo al proceso, la cual a su vez señale los riesgos y costos de los cambios.
	Asegurar que el plan estratégico de TI y la hoja de ruta contengan los requerimientos de seguridad de información identificados en el proceso de atención.
Comunicar la estrategia y la dirección de TI	Desarrollar el plan estratégico y el plan de seguridad de información que incluya el proceso de atención de pacientes y comunicarlo a los stakeholders.
	Desarrollar el plan de comunicación de la estrategia aplicada dentro del proceso de atención. Identificar canales de comunicación.
	Actualizar el plan de comunicación según la retroalimentación del personal y a la estrategia de seguridad de información dentro del proceso de atención.

Tabla 9.1.34 - Proceso atención. Actividades de gestión habilitador: Gestionar la estrategia

Matriz de responsabilidades (RACI)

APO02: Gestionar la estrategia																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Comprender la dirección de la empresa		C	C	C	A	C	C			C	R	C			R	C	I	I	R	C

Evaluar entorno, capacidades y rendimiento actual		C	C	C	R	C	C			C	C			C	A	I	C	I	R	C
Realizar un análisis de brecha					R	R	C			C	C		C	C	A	I	C	I	R	C
Definir plan estratégico y hoja de ruta		C	I	C	C		C		R	C	C			C	A	C	C	I	C	C
Comunicar estrategia y dirección de TI	I	R	I	I	R	I	A	I	I	I	R	I	I	I	R	I	I	I	I	I

Tabla 9.1.35 - Matriz de responsabilidades para el proceso habilitador APO02 - Proceso Atención

b. Proceso habilitador: Gestionar los recursos humanos

Se detalla la aplicación de actividades de gestión de acuerdo al proceso de atención de pacientes. El objetivo es que los recursos humanos sean capaces de soportar el proceso a nivel de negocio y tecnológico garantizando el cumplimiento de requerimientos de seguridad de información. Se muestra también la matriz de responsabilidades, la cual a diferencia del proceso de admisión, muestra menor requerimiento a nivel técnico, pero siguiendo el enfoque de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Mantener la dotación del personal suficiente y adecuada	Evaluar periódicamente las necesidades de personal en el proceso de atención de pacientes de forma de asegurar que los recursos pueden soportar dicho proceso de negocio. Incluye evaluar necesidad de personal de TI.
	Dentro de los procesos de contratación, incluir controles de antecedentes de acuerdo a la función o rol dentro del proceso de atención.
	Asegurar que los requisitos de seguridad se incorporan en el proceso de contratación.
	Brindar capacitaciones y garantizar que existe personal capaz de cubrir funciones críticas de otro para reducir la dependencia.
Identificar personal clave de TI	Asegurar la segregación de funciones en roles críticos del proceso.
	Minimizar la dependencia de una sola persona en una función crítica dentro del proceso de atención al paciente a través de captura e intercambio de conocimiento.

Mantener las habilidades y competencias del personal	Definir habilidades y competencias necesarias que deben tener los recursos para lograr los objetivos del proceso y poder escalar hacia los objetivos de alto nivel.
	Brindar capacitaciones y programas de seguridad de información al personal que ejecuta los procesos.
	Proporcionar facilidades a los actores de este proceso para lograr el desarrollo profesional para fomentar las oportunidades de progreso personal y menor dependencia de personas clave.
	Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos. A partir de estas identificar si se requieren habilidades adicionales para cubrir el proceso y ejecutar el plan de acción para desarrollarlas.
Evaluar el desempeño laboral de los empleados	Dentro de la evaluación del desempeño, considerar criterios con respecto a la función de seguridad de información.
	Establecer objetivos individuales alineados con los objetivos del proceso de atención. Estos deben reflejar competencias básicas, valores empresariales y habilidades para las funciones.
	Proporcionar instrucciones para uso y almacenamiento de información personal dentro del proceso de evaluación.
	Desarrollar planes para la mejora de desempeño del personal que ejecuta el proceso de atención.
	Implementar un proceso de reconocimiento a medida que el personal logre o desarrolle sus objetivos.
Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio	Comprender la demanda actual y futura de recursos humanos involucrados dentro del proceso de atención para apoyar el logro de objetivos de TI y necesidades operativas del día a día salvaguardando los objetivos de la función de seguridad de información.
	Realizar el inventario del personal del proceso e identificar sus respectivas funciones.
	Mantener información adecuada sobre el tiempo

	dedicado a diferentes tareas, trabajos, servicios o proyectos
Gestionar el personal contratado	Obtener un acuerdo formal por parte del personal sobre las políticas y requisitos de la seguridad de información a aplicarse en el proceso de atención al paciente.
	Llevar a cabo revisiones para asegurarse que el personal cumple con sus funciones, que el derecho de acceso es adecuado y alineado con los acuerdos pactados al firmar el contrato.
	Implementar políticas que permitan identificar como se debe gestionar el personal, es decir si es necesario contratar servicios o nuevo personal siguiendo los parámetros de seguridad de información.

Tabla 9.1.36 - Proceso atención. Actividades de gestión habilitador: Gestionar los recursos humanos

Matriz de responsabilidades (RACI)

APO07: Gestionar los recursos humanos	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Mantener dotación de personal suficiente y adecuado									R	I	C		R		A	C	C	C	R	C
Identificar personal clave de TI						C		I	R		R		R		A	C	R	C	R	C
Mantener habilidad y competencia del personal						I			R		C		R		A	R	C	C	R	C
Evaluar desempeño laboral del empleado									R		R		R		A	R	R	R	R	R
Planificar y realizar seguimiento del uso recursos humanos de TI y negocio					R	C	A	R	R		C		I		R	R	C	C	R	C
Gestionar personal contratado						I	I	I	R		C		R		A	R	C	C	R	C

Tabla 9.1.37 - Matriz de responsabilidades para el proceso habilitador APO07 - Proceso Atención

c. Proceso habilitador: Gestionar el riesgo

Por medio de este proceso habilitador se pretende garantizar que, por medio de sus actividades de gestión, los riesgos de seguridad de información del proceso de atención se encuentren controlados.

Se muestra la respectiva matriz de acuerdo a las actividades y fines del proceso de atención.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Recopilar datos	Identificar y recolectar datos para la identificación, análisis y comunicación de los riesgos de seguridad de información dentro del proceso de atención al paciente.
	Medir y analizar los riesgos de TI y seguridad de información suscitados dentro del proceso de atención a lo largo del tiempo. Verificar las pérdidas experimentadas por la materialización de estos.
	Ejecutar análisis del entorno para verificar los factores de riesgo que se presentan en el proceso.
Analizar el riesgo	Identificar, analizar y evaluar los riesgos de información dentro del proceso.
	Construir los escenarios de riesgo de TI y seguridad dentro del proceso. Identificar las amenazas para detectar medidas de emergencia.
	Identificar los riesgos residuales dentro del proceso y las exposiciones que puedan requerir una respuesta al riesgo.
	Especificar controles apropiados para la mitigación de riesgos de seguridad de información que garanticen que el proceso se vea afectado lo mínimo posible.
	Validar los resultados del análisis de riesgos del proceso antes de usarlos para la toma de decisiones. Verificar alineamiento con requerimientos organizacionales.
Mantener un perfil del riesgo	Crear e informar el nivel aceptable de exposición al riesgo que incluya los aspectos de seguridad de acuerdo

	al proceso.
	Identificar dentro del proceso los servicios esenciales para sostenerlo y que este alineado con el perfil de riesgo a tolerar. Analizar dependencias e identificar debilidades.
	Definir un conjunto de indicadores que permitan la supervisión de los riesgos de seguridad del proceso y sus tendencias.
Expresar el riesgo	Informar los resultados del análisis de riesgos del proceso de atención a los stakeholders en términos adecuados y entendibles para decisiones empresariales.
	Informar el perfil del riesgo a los stakeholders junto con la efectividad del proceso de atención y los controles asociados. Identificar oportunidades de TI para mayor tolerancia al riesgo e incrementar la capacidad de gestión.
Definir un portafolio de acciones para la gestión de riesgos	Monitorear periódicamente los riesgos de seguridad de información del proceso de atención y verificar que el riesgo este alineado con el apetito y tolerancia al riesgo.
	Definir propuestas para reducir el riesgo o proyectos para incrementar las oportunidades estratégicas de acuerdo a la ley de protección de datos personales y la norma técnica peruana de la historia clínica.
Responder al riesgo	Aplicar las prácticas y controles para la mitigación de riesgos de seguridad. Se recomienda aplicar en este caso la norma ISO/IEC 27002:2013. Se recomienda incluir controles preventivos y correctivos.

Tabla 9.1.38 - Proceso atención. Actividades de gestión habilitador: Gestionar el riesgo

Matriz de responsabilidades (RACI)

APO12: Gestionar el riesgo																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Recopilar datos		I				R		I	R	R	R	I		I	A	C	C	C	R	C
Analizar el riesgo		I				R		I	C	R	C	I		C	A	C	C	C	R	C
Mantener un perfil del riesgo		I				R		I	C	A	C	I		I	R	C	C	C	R	C
Expresar el riesgo		I				R		I	C	R	C	I		I	A	C	C	C	C	C
Definir portafolio de acciones para gestión del riesgo		I				R		I	C	A	R	I		I	R	I	C	I	C	C
Responder al riesgo		I				R		I	R	R	R	I		C	A	R	R	R	R	R

Tabla 9.1.39 - Matriz de responsabilidades para el proceso habilitador APO12 - Proceso Atención

d. Proceso habilitador: Gestionar la seguridad

Similar al proceso de admisión, se considera que este proceso debe también formar parte del alcance de un SGSI y a partir de este establecer las medidas y controles para tratar los riesgos de seguridad de información que puedan impactar de forma negativo a los procesos críticos de la organización.

Dado que este proceso va de la mano con el proceso de admisión, se considera que la declaración de aplicabilidad de este último es válida para ambos. Se presenta también la matriz de responsabilidades.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Establecer y mantener un SGSI	Definir el alcance del SGSI de acuerdo a las características de la organización y sus políticas.
	Diseñar un enfoque de gestión de seguridad y alinearlo al SGSI.
	Comunicar los roles y responsabilidades en la gestión de la seguridad de información y el enfoque del SGSI.
	Comprometer a la alta dirección para iniciar las actividades de implementación del SGSI.
Definir y gestionar un plan de tratamiento del riesgo de la seguridad de información	Diseñar, mantener y aplicar un plan de tratamiento de riesgos de seguridad de información alineados con los objetivos estratégicos de la organización y fines del proceso.
	Desarrollar propuestas de mejora al plan de riesgos basados en casos de negocio de acuerdo a los roles y responsabilidades a necesitar para su aplicación y acorde a los drivers identificados.
	Integrar la planificación, diseño, implementación y supervisión de procedimientos de seguridad y controles para prevención y detección temprana de eventos dentro del proceso de atención y la respuesta a incidentes.
Supervisar y revisar el SGSI	Realizar revisiones periódicas del SGSI incluyendo las políticas y objetivos definidos en la etapa de concepción del SGSI
	Realizar evaluaciones o auditorías al SGSI de forma periódica para determinar su cumplimiento e identificar mejoras en el proceso.
	Registrar acciones y eventos que podrían tener impacto en la efectividad o desempeño del SGSI.

Tabla 9.1.40 - Proceso atención. Actividades de gestión habilitador: Gestionar la seguridad

Matriz de responsabilidades (RACI)

APO13: Gestionar la seguridad																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Establecer y mantener un SGSI		C		C	C	C	C	I	I	C	A	C		I	R	I	I	I	R	C
Definir gestionar plan tratamiento de riesgos de seguridad información		C		C	C	C	C	I	I	C	A	C		I	R	C	C	C	R	C
Supervisar y revisar el SGSI					C	R	C	I	R		A			C	R	R	R	R	R	R

Tabla 9.1.41 - Matriz de responsabilidades para el proceso habilitador APO13 - Proceso Atención

e. Proceso habilitador: Gestionar los programas y proyectos

Dentro del proceso de atención se requiere la gestión de programas y proyectos a alto nivel y garantizar su alineamiento con las estrategias y objetivos del proceso de negocio. Se presenta la matriz de responsabilidades para gestionar el habilitador y conducirlo al nivel de madurez esperado por los stakeholders.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Mantener un enfoque estándar para la gestión de programas y proyectos.	Incorporar los requerimientos de seguridad de información dentro de los proyectos asociados al proceso de atención.
	Establecer procedimientos para asegurar que todos los proyectos relacionados al proceso e información cuentan con las medidas de seguridad requeridas o exigibles.
	Actualizar el enfoque de gestión de programas y proyectos. Aplicar las mejoras que se desprenden del uso de estrategias dentro del proceso de atención.

Desarrollar y mantener el plan del programa.	Desarrollar un plan de seguridad de información que incluya los controles a implementar en el proyecto.
	Incluir recursos dentro del proyecto para identificar e implementar requerimientos de seguridad de información.
	Mantener el plan de programa para asegurar su actualización de acuerdo a los proyectos y el proceso de atención. Actualizar el caso de negocio que lo justifica y garantiza el alineamiento estratégico.
Planificar proyectos	Integrar la seguridad de información y las tecnologías con la gestión de proyectos de negocio.
	Desarrollar un plan de proyecto con información que permita a la dirección controlar su progreso. Incluir recursos, responsabilidades e hitos que marcan el cierre de cada una de las etapas.
	Mantener los planes de proyectos y sus dependencias, asegurando la comunicación entre estos y que al realizar un cambio en uno de éstos se refleje en los demás.
	Establecer un marco base para gestión de proyectos, el cual es revisado, aprobado e incorporado a los planes de proyecto vigentes.
Gestionar la calidad de los programas y proyectos.	Identificar actividades y prácticas para garantizar la calidad de los proyectos. Asegurar que las tareas cumplan los requerimientos de seguridad de información
Gestionar el riesgo de los programas y proyectos.	Registrar los riesgos de seguridad de información del proyecto y sus acciones correctivas. Revisar y actualizarlos periódicamente.
	Integrar proyectos de seguridad de información al programa y proceso de atención de pacientes. Alinearlos a los procesos de gestión de proyectos.
	Asignar responsabilidades al personal capacitado para la gestión del riesgo de los proyectos.
Supervisar y controlar proyectos.	Programar evaluaciones a los proyectos para asegurar que los requerimientos de seguridad de información del proceso son implementados efectivamente.
	Supervisar los cambios al programa y revisar requerimientos de desempeño para verificar el avance.

	Obtener la aprobación y firma de los entregables producidos en cada iteración de los proyectos asociados.

Tabla 9.1.42 - Proceso atención. Actividades de gestión habilitador: Gestionar los programas y proyectos

Matriz de responsabilidades (RACI)

BAI01: Gestionar programas y proyectos	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Mantener enfoque para gestión de programas y proyectos	I	A	C	C	R		R		C	C	C			I	R				C	
Desarrollar y mantener el plan del programa			C	C	A	C		R	R	C	R			I	C	I	I	I	R	C
Planificar proyectos						C	I	A	R		C				C	C	C	C	R	C
Gestionar la calidad de los programas y proyectos					C	R	I	A	R	C	R			I	C	I	C		C	C
Gestionar el riesgo de los programas y proyectos					R	R	I	A	R	C	R			I	C	C	C	C	R	C
Supervisar y controlar proyectos					I	R	I	A	R	C	C			C	C	I	C	C	R	C

Tabla 9.1.43 - Matriz de responsabilidades para el proceso habilitador BAI01 - Proceso Atención

f. Proceso habilitador: Gestionar el cambio

Este proceso habilitador dentro del proceso de atención presenta la particularidad de que no cuenta con infraestructura tecnológica compleja, por ello el personal de TI del proceso es menor, por eso derivan algunas actividades. Se recomienda por lo tanto que el cierre de los cambios se haga en conjunto con el proceso de atención.

Adicionalmente se presenta la matriz de responsabilidades respectiva.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Evaluar, priorizar y autorizar solicitudes de cambio	Asegurar que los cambios dentro del proceso de atención se alinean a las políticas de seguridad de información.
	Realizar el análisis de impacto al realizar cambios en seguridad de información y a nivel general dentro del proceso.
	Asegurar que los cambios sean validados por los dueños del proceso de negocio de atención al paciente. Evaluar los tipos de cambios permitidos en él.
	Estandarizar las solicitudes de cambio de manera que todo cambio a nivel del proceso sea a través de procedimientos formales.
	Considerar el impacto de los cambios en la gestión de proveedores de acuerdo a la de seguridad de información, procurando que estos no afecten los acuerdos de servicio.
Gestionar cambios de emergencia	Desarrollar medidas para atender cambios de emergencia en el proceso y relacionados a seguridad de información.
	Registrar los riesgos de seguridad de información a partir de cambios de emergencia realizados en el proceso.
	Supervisar los cambios de emergencia dentro del proceso de atención y realizar las revisiones post-implantación involucrando a las partes interesadas.
Hacer seguimiento e informar cambios de estado	Mantener y supervisar un sistema de seguimiento e informe para las solicitudes de cambio del proceso de acuerdo a las exigencias de seguridad de información.
	Elaborar informes respecto a los cambios de seguridad de información realizados en el proceso.
	Supervisar los cambios de seguridad de información que aún no han sido cerrados.

Tabla 9.1.44 - Proceso atención. Actividades de gestión habilitador: Gestionar el cambio

Matriz de responsabilidades (RACI)

BAI06: Gestionar el cambio																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Evaluar, priorizar y autorizar solicitudes de cambio					A	R			C	C	R			I	R	C	C	R	R	
Gestionar cambios de emergencia					A	I				C	R		I	I	R	C	R	I	R	
Hacer seguimiento e informar cambios de estado					C	R			C		C				A	C	C	C	R	

Tabla 9.1.45 - Matriz de responsabilidades para el proceso habilitador BAI06 - Proceso Atención

g. Proceso habilitador: Gestionar los activos

Se muestra a continuación las actividades a considerar para realizar gestión de activos involucrados dentro del proceso de atención al paciente hospitalizado. Se requiere identificar los requerimientos de seguridad de información a los que están asociados.

Se presenta la matriz de responsabilidades. Se observa que no aplica la actividad administrar licencias debido a que parte de esta se realizará en el proceso de admisión de pacientes, similar con la optimización de costos, la cual se gestiona desde el proceso de gobierno como fue anteriormente señalado.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Identificar y registrar activos actuales	Identificar los activos relacionados al proceso de atención al paciente hospitalizado y los requerimientos de seguridad asociados a estos.
	Identificar la dependencia entre estos activos y su nivel de criticidad dentro del proceso.

	Identificar si los activos del proceso de atención están sujetos a alguna regulación adicional a la ley de protección de datos personales y la norma técnica peruana de la historia clínica. Verificar los aspectos contractuales de seguridad de información.
	Verificar y determinar si los activos se encuentran en condiciones útiles para soportar dicho proceso y si es que genera valor al negocio.
Gestionar activos críticos	Identificar que activos del proceso de atención pueden ser considerados como crítico. Supervisar su rendimiento por medio de evaluaciones o planes en los que se definan las políticas de reparación o reemplazo.
	Determinar los niveles de criticidad de los activos dentro del proceso de atención.
	Garantizar que los activos críticos del proceso cumplan los niveles de seguridad de información establecidos en el proceso y el negocio.
	Determinar el tiempo de inactividad máximo para estos activos críticos de manera que se garantice la reducción de un impacto adverso en el negocio.
	Establecer políticas para el cambio de estos activos críticos de acuerdo a los riesgos de seguridad de información identificados.
Gestionar el ciclo de vida de los activos	Identificar y comunicar los riesgos de seguridad de información de estos activos que soportan el proceso.
	Realizar adquisiciones de nuevos activos previamente autorizadas de acuerdo a procedimientos seguros que verifique un nivel de riesgo aceptable.
	Establecer políticas para eliminar activos de forma segura.
	Asegurar que las medidas de seguridad de información se apliquen a los activos durante todo su ciclo de vida.

Tabla 9.1.46 - Proceso atención. Actividades de gestión habilitador: Gestionar los activos

Matriz de responsabilidades (RACI)

BAI09: Gestionar los activos																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Identificar y registrar activos actuales			C			C					C				I	R	A	C	C	
Gestionar activos críticos			C		I	C				C	C			C		R	A	C	C	C
Gestionar el ciclo de vida de los activos						C				I	C					R	A	C	I	

Tabla 9.1.47 - Matriz de responsabilidades para el proceso habilitador BAI09 - Proceso Atención

h. Proceso habilitador: Gestionar las solicitudes de servicio e incidentes

Se identifican las actividades de gestión a aplicar para este proceso habilitador tomando en cuenta como referencia para el análisis el proceso de atención al paciente. El enfoque de seguridad brinda prioridad a solicitudes e incidentes de información. Se muestra también la matriz de responsabilidades que permite la gestión adecuada de este proceso habilitador.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Definir esquemas de clasificación de incidentes y solicitudes de servicio	Definir y comunicar las características de los potenciales incidentes de seguridad de información para su reconocimiento y entendimiento del impacto en caso se materialicen.
	Definir modelos de solicitudes de servicio relacionados a la seguridad de información para facilitar su atención y respuesta dentro del proceso de atención.
	Definir la clasificación y priorización de incidentes y solicitudes de servicio relacionados al proceso de

	atención de acuerdo a los requerimientos de seguridad de información y el impacto en el negocio.
Registrar, clasificar y priorizar solicitudes e incidentes	Investigar los incidentes de seguridad y elaborar, en base a estos, procedimientos de respuesta. Asegurar que las medidas sean definidas y protejan los pilares de seguridad y que sean difundidas.
	Registrar incidentes y solicitudes de servicio relacionados a la seguridad de información del proceso de atención.
	Priorizar y clasificar incidentes de acuerdo al impacto dentro del negocio y el proceso de atención.
Verificar, aprobar y resolver solicitudes de servicio	Seguir procedimientos y modelos de solicitud de seguridad de información para elementos frecuentes de manera que se atiendan en menor tiempo.
Investigar, diagnosticar y localizar incidentes	Registrar un nuevo problema en caso no exista dentro de la base de datos y si el incidente de seguridad de información satisface los criterios para registro.
	Identificar soluciones temporales o permanentes para los incidentes de seguridad de información, asignar su tratamiento a los especialistas respectivos dentro del proceso de atención.
Resolver y recuperarse de incidentes	Definir un plan de respuesta de seguridad de información para los incidentes dentro del proceso de atención.
	Ejecutar las acciones de recuperación para restablecer el proceso de atención completamente.
	Documentar la solución e identificar si es temporal o permanente para tomarlo en cuenta a futuro.
Cerrar solicitudes de servicio e incidentes	Verificar con los usuarios del proceso si se ha completado la solicitud del servicio o si el incidente de seguridad fue resuelto. En caso afirmativo cerrar la solicitud o incidente,
Seguir el estado y emitir informes	Asegurar que los incidentes de seguridad de información, el análisis y seguimiento de estos, siguen los procedimientos de gestión existentes.
	Elaborar informes y distribuirlos periódicamente a los stakeholders como parte de la mejora continua.

Tabla 9.1.48 - Proceso atención. Actividades de gestión habilitador: Gestionar las solicitudes de servicio e incidentes

Matriz de responsabilidades (RACI)

DSS02: Gestionar solicitudes de servicio e incidentes																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Definir esquema de clasificación de incidentes y solicitud de servicio						C				I	I				A	I	R	R	R	C
Registrar, clasificar y priorizar solicitudes e incidentes						I				I	C						A	R	C	
Verificar, aprobar y resolver solicitudes de servicio						R				C	C				I	C	R	A	C	
Investigar, diagnosticar y localizar incidentes						R				I	C				I	I	R	A	C	
Resolver y recuperarse de incidentes						I				I	I			I	I	C	R	A	C	
Cerrar solicitudes de servicio e incidentes						C				I	C				I	I	A	C	R	
Seguir el estado y emitir informes						I				I	C	I		I	I	I	A	R	I	

Tabla 9.1.49 - Matriz de responsabilidades para el proceso habilitador DSS02 - Proceso Atención

i. Proceso habilitador: Gestionar la continuidad

Se señala a continuación las actividades que aplican para gestionar la continuidad del proceso de atención al paciente hospitalizado. Se muestra seguidamente la matriz de responsabilidades definida.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Definir las políticas de continuidad de negocio, objetivos y alcance	Determinar la criticidad del proceso de atención de pacientes de acuerdo a la seguridad de información y el cumplimiento con la ley de protección de datos personales y la norma técnica peruana de la historia clínica para verificar si forma parte del programa de

	continuidad.
	Asegurar que la seguridad de información forma parte del ciclo de vida de continuidad de negocio.
	Identificar interesados, roles y responsabilidades dentro del proceso para alinearlos a los objetivos y políticas del SGCN
Mantener una estrategia de continuidad	Identificar e incluir escenarios que den pie a eventos de información que afecten la continuidad del proceso.
	Realizar el análisis de impacto de negocio de acuerdo a los lineamientos del proceso, incluyendo los factores de seguridad de información y el máximo tolerable de interrupción en estos aspectos.
	Analizar las amenazas de seguridad que afecten la continuidad del proceso para mejorar métodos preventivos e incrementar la resiliencia.
Desarrollar e implementar una respuesta a la continuidad de negocio	Definir los procedimientos de recuperación para reanudar el proceso de egreso y que cumpla con los requerimientos de seguridad de información definidos.
	Definir y documentar recursos necesarios para recuperar el proceso. Documentar los planes considerando las necesidades de seguridad y almacenamiento de la información en otro lugar. Distribuir los planes.
Ejecutar, probar y revisar el plan de continuidad	Planificar actividades para probar el plan definido en los documentos. Asignar roles y responsabilidades para esta actividad y coordinar que no afecten el proceso.
	Realizar el análisis y revisión para determinar el logro.
Revisar, mantener y mejorar el plan de continuidad	Revisar el plan periódicamente tomando en cuenta los objetivos de negocio, objetivos de TI y los lineamientos del proceso de atención. Considerar posibles cambios producto del entorno.
	Comunicar los cambios del plan de continuidad que puedan afectar el proceso o los requerimientos de seguridad de información
	Reconocer qué incidentes de seguridad de información pueden ocasionar la interrupción del negocio, por ello se debe incrementar el nivel de gestión de éstos.

Gestionar acuerdos de respaldo	Asegurar que los requerimientos de seguridad se cumplen en los procesos de backup y restauración de información.
	Realizar las copias de seguridad respectivas y establecer políticas para su gestión de acuerdo a la ley de protección de datos personales y la norma técnica peruana de la historia clínica entre otras exigencias dentro del proceso de atención, salvaguardando los datos del paciente.
	Probar y mantener las copias de seguridad recientes, y aquellas archivadas, de manera periódica para garantizar la disponibilidad de la información y su integridad.
Ejecutar revisiones post-reanudación	Evaluar la efectividad del plan de acuerdo a los tiempos definidos en el análisis de impacto de negocio de acuerdo al proceso de atención al paciente.
	Identificar debilidades u omisiones como parte de la mejora continua para asegurar que el proceso de atención podrá llevarse a cabo sin inconvenientes ante cualquier evento asegurando la información de los involucrados.

Tabla 9.1.50 - Proceso atención. Actividades de gestión habilitador: Gestionar la continuidad

Matriz de responsabilidades (RACI)

DSS04: Gestionar la continuidad	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Definir la política de continuidad de negocio, objetivos y alcance				A	C	R				C	C			C	R	I	C	C	C	R

Mantener una estrategia de continuidad				A	C	R				I	I			C	R	I	C		R	R
Desarrollar e implementar una respuesta a la continuidad.					I	R					C		I	C	R	I	C		R	A
Ejercitar, probar y revisar el plan de continuidad					I	R				I	I		I	R	R	I	C	I	R	A
Revisar, mantener y mejorar el plan de continuidad				A	I	R				I	C				R		C		C	R
Gestionar acuerdos de respaldo											I					C	I		C	R
Ejecutar revisiones post-reanudación					C	R				I	C				R	I			C	A

Tabla 9.1.51 - Matriz de responsabilidades para el proceso habilitador DSS04 - Proceso Atención

j. Proceso habilitador: Gestionar los servicios de seguridad

Se presenta las actividades de gestión que aplican al proceso habilitador de acuerdo a la realidad de la organización y sus necesidades y requerimientos del proceso. Se muestra también la matriz de responsabilidades para su gestión.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Proteger contra software malicioso	Instalar y activar herramientas de protección frente a software malicioso en las estaciones o activos que brindan soporte al proceso de atención. Concientizar al usuario sobre el empleo de estas.
	Filtrar el tráfico entrante de información como correos electrónicos y descargas para protegerse frente a información no solicitada.
Gestionar la seguridad de la red y las conexiones	Mantener una política para la seguridad de conexiones de red entre los activos que soportan el proceso de atención.
	Cifrar la información en tránsito de acuerdo con su clasificación verificando el cumplimiento la ley de protección de datos personales.
Gestionar la seguridad de los puestos de usuario final	Cifrar la información almacenada dentro de los activos de acuerdo a su clasificación y nivel de criticidad.
	Configurar los sistemas operativos de forma correcta y segura en las estaciones del personal que ejecuta el

	proceso de atención.
	Implementar mecanismos de bloqueo en los dispositivos.
	Deshacerse de los dispositivos de usuario final de forma segura.
Gestionar la identidad del usuario y el acceso lógico	Según los requerimientos del proceso, mantener los derechos de acceso
	Segregar y gestionar cuentas de usuario privilegiadas.
	Realizar regularmente revisiones de la gestión de cuentas y privilegios que abarca el proceso de atención. Verificar que la identificación de estas es unequívoca.
Gestionar documentos sensibles y dispositivos de salida	Establecer procedimientos de empleo, eliminación y destrucción de formularios especiales como las historias clínicas y actas de conformidad.
	Asignar privilegios de acceso a documentación y a su modificación durante el proceso de atención al paciente.
	Realizar un inventario de documentos sensibles o dispositivos de salida críticos involucrados durante el proceso de atención.
	Establecer políticas de protección física apropiadas sobre formularios o documentos que contienen información sensible.

Tabla 9.1.52 - Proceso atención. Actividades de gestión habilitador: Gestionar los servicios de seguridad

Matriz de responsabilidades (RACI)

DSS05: Gestionar los servicios de seguridad																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Proteger contra software malicioso						R				C	A		R		C	I	R	I	C	

Gestionar seguridad de red y conexiones						I				C	A			C	C	I	R	I	C	
Gestionar seguridad de puestos de usuario final						I				C	A		I		C		C	I	R	
Gestionar identidad del usuario y acceso lógico						R				C	A		I	C	C		C	I	R	C
Gestionar documentos sensibles y dispositivo de salida						C	I			I	C			I	A	I	C		R	

Tabla 9.1.53- Matriz de responsabilidades para el proceso habilitador DSS05 - Proceso Atención

1.1.4 Proceso Egreso del paciente

El siguiente proceso es parte del macro-proceso hospitalario, a diferencia del proceso de atención, sus actividades involucran mayor interacción con sistemas de información sin dejar de lado actividades manuales.

Aunque entre sus actores no está el personal de TI, se necesita el apoyo de éstos para definir estrategias, capacidades y funciones, de manera que los usuarios del proceso puedan llevarlo a cabo de forma exitosa y cumpliendo con la regulación, entre estas ley de protección de datos personales, norma técnica peruana de la historia clínica y en menor grado, debido a que es proceso hospitalario, la ley de emergencia.

Los procesos habilitadores a aplicar para esta modelo de gobierno de TI son las siguientes:

a. <u>Proceso habilitador: Gestionar la estrategia</u>

Dentro del proceso de negocio egreso del paciente se requiere identificar oportunidades y capacidades para garantizar que las actividades que comprenden el proceso cumplen requerimientos de seguridad definidos y las regulaciones a las cuales está sujeto el proceso.

Se muestra también la matriz de responsabilidades para llevar a cabo su gestión a nivel del proceso egreso del paciente hospitalizado.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Comprender la dirección de la empresa	Entender como la seguridad de información debe respaldar los objetivos de la organización y del proceso. Garantizar con estos el cumplimiento de la ley de protección de datos personales y la norma técnica peruana de la historia clínica.
	Desarrollar y entender las estrategias, objetivos de negocio, entorno y retos operativos actuales dentro del proceso y la seguridad de información.
	Determinar prioridades para desarrollar cambios estratégicos en el proceso.
Evaluar entorno, capacidades y rendimientos actuales	Establecer la línea base de seguridad de información dentro del proceso egreso del paciente.
	Crear criterios de seguridad de información claros y relevantes de acuerdo con las actividades del proceso de egreso. Identificar riesgos.
	Identificar diferencias entre el proceso de negocio actual y las capacidades de TI según estándares y mejores prácticas sugeridas por la división calidad y procesos.
	Identificar debilidades, fortalezas, oportunidades y amenazas del entorno actual del proceso de egreso Evaluar dentro de él el desempeño de la función de seguridad de información.
Realizar un análisis de brecha	Identificar dentro del proceso las brechas a cerrar y los cambios requeridos para llegar al nivel deseado.
	Examinar el nivel de cumplimiento con la ley de protección de datos personales, norma técnica peruana de la historia clínica y la ley de emergencia dentro del proceso de egreso al paciente.
	Definir las metas del proceso y establecer los beneficios que se obtienen al llegar a estas.
Definir el plan estratégico y la hoja de ruta	Definir la estrategia de seguridad de información y alinearla a la estrategia de negocio para cumplir los objetivos del proceso.
	Crear la hoja de ruta que incluya la planificación e interdependencias de las iniciativas a nivel empresarial

	de acuerdo al proceso, la cual a su vez señale los riesgos y costos de los cambios.
	Asegurar que el plan estratégico de TI y la hoja de ruta contengan requerimientos de seguridad de información identificados para el proceso de egreso.
Comunicar la estrategia y la dirección de TI	Desarrollar el plan estratégico y el plan de seguridad de información que incluya el proceso de egreso de pacientes y comunicarlo a los stakeholders.
	Tomando como base el plan de comunicación de otros procesos como el de atención y el de admisión, actualizar el plan según los resultados en el personal que realiza el proceso de egreso del paciente.

Tabla 9.1.54 - Proceso Egreso. Actividades de gestión habilitador: Gestionar la estrategia.

Matriz de responsabilidades (RACI)

APO02: Gestionar la estrategia																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Comprender la dirección de la empresa		C	C	C	A	C	C			C	R	C			R	C	C	I	R	C
Evaluar entorno, capacidades y rendimiento actual		C	C	C	R	C	C			C	C			C	A	I	C	I	R	C
Realizar un análisis de brecha					R	R	C			C	C		C	C	A	I	C	I	R	C
Definir plan estratégico y hoja de ruta		C	I	C	C		C		R	C	C			C	A	C	C	I	C	C
Comunicar estrategia y dirección de TI	I	R	I	I	R	I	A	I	I	I	R	I	I	I	R	I	I	I	I	I

Tabla 9.1.55 - Matriz de responsabilidades para el proceso habilitador APO02 - Proceso Egreso

b. Proceso habilitador: Gestionar los recursos humanos

Se detalla las actividades sugeridas para la gestión de recursos humanos del proceso de egreso del paciente, lo cual incluye personal médico, administrativo y parte de soporte de TI.

Se muestra la respectiva matriz de responsabilidades para gestionar el proceso habilitador y llevarlo a un nivel de madurez.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Mantener la dotación del personal suficiente y adecuada	Evaluar periódicamente las necesidades de personal en el proceso de egreso de pacientes, de manera de asegurar que estos recursos puedan realizar con éxito el proceso de negocio. Incluye la evaluación de necesidad de nuevo personal de TI.
	Dentro de los procesos de contratación, incluir controles de antecedentes de acuerdo a la función o rol dentro del proceso de egreso.
	Asegurar que los requisitos de seguridad se incorporan en el proceso de contratación.
	Asegurar que existe personal capaz de cubrir funciones críticas de otro para reducir la dependencia en el proceso de egreso.
Identificar personal clave de TI	Asegurar la segregación de funciones en roles críticos del proceso.
	Tomar acciones o medidas para la gestión de cambios de personal, en especial en los temas de despido.
	Minimizar la dependencia en una sola persona en una función crítica dentro del proceso de egreso del paciente a través de captura e intercambio de conocimiento.
Mantener las habilidades y competencias del personal	Definir habilidades y competencias necesarias de los recursos para lograr los objetivos dentro del proceso y poder escalar hacia los objetivos de alto nivel.
	Brindar capacitaciones y programas de seguridad de información al personal que ejecuta los procesos.
	Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los

	recursos internos. A partir de estas identificar si se requieren habilidades adicionales para cubrir el proceso y ejecutar el plan de acción para desarrollarlas.
Evaluar el desempeño laboral de los empleados	Dentro de la evaluación del desempeño, considerar criterios con respecto a la función de seguridad de información.
	Establecer objetivos individuales alineados con los objetivos del proceso de egreso. Estos deben reflejar competencias básicas, valores empresariales y habilidades para las funciones.
	Proporcionar instrucciones para uso y almacenamiento de información personal dentro del proceso de evaluación.
	Implementar un proceso de reconocimiento a medida el personal logre sus objetivos dentro del proceso.
Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio	Comprender la demanda actual y futura de recursos humanos involucrados en el proceso de egreso para apoyar el logro de objetivos de TI y necesidades operativas del día a día salvaguardando los objetivos de la función de seguridad de información.
	Realizar el inventario del personal del proceso e identificar sus respectivas funciones.
	Mantener información adecuada sobre el tiempo dedicado a diferentes tareas, trabajos, servicios o proyectos
Gestionar el personal contratado	Obtener un acuerdo formal por parte del personal sobre las políticas y requisitos de la seguridad de información a aplicarse en el proceso de egreso del paciente.
	Llevar a cabo revisiones para asegurarse que el personal cumple con sus funciones, que el derecho de acceso es adecuado y alineado a los acuerdos pactados al firmar el contrato.
	Definir el trabajo a realizar por terceros o por otras áreas de le organización a través de contratos o documentos formales que carezcan de ambigüedades.
	Implementar políticas que permitan identificar como se

	debe gestionar el personal, es decir si es necesario contratar servicios o nuevo personal siguiendo los parámetros de seguridad de información.

Tabla 9.1.56 - Proceso Egreso. Actividades de gestión habilitador: Gestionar los recursos humanos

Matriz de responsabilidades (RACI)

APO07: Gestionar los recursos humanos	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Mantener personal suficiente y adecuado									R	I	C		R		A	C	C	C	R	C
Identificar personal clave de TI						C		I	R		R		R		A	R	R	C	R	C
Mantener habilidad y competencia del personal						I			R		C		R		A	R	R	C	R	C
Evaluar desempeño laboral del empleado									R		R		R		A	R	R	R	R	R
Planificar y realizar seguimiento del uso recursos humanos de TI y negocio					R	C	A	R	R		C		I		R	R	R	C	R	C
Gestionar personal contratado						I	I	I	R		C		R		A	R	R	C	R	C

Tabla 9.1.57 - Matriz de responsabilidades para el proceso habilitador APO07 - Proceso Egreso

c. Proceso habilitador: Gestionar el riesgo

A continuación se presentan las actividades que garantizan la gestión del riesgo de seguridad de información, su capacitación y los controles o plan de acción para mitigar y reducir el impacto.

Seguidamente se presenta la matriz de responsabilidades para realizar la gestión del proceso habilitador dentro del ciclo de vida de gobierno de TI.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Recopilar datos	Identificar y recolectar datos para la identificación, análisis y comunicación de los riesgos de seguridad de información dentro del proceso de egreso del paciente.
	Medir y analizar los riesgos de TI y seguridad de información suscitados dentro del proceso de egreso. Verificar pérdidas experimentadas por la materialización de estos.
	Determinar en qué condiciones del proceso se materializó el riesgo. Identificar el impacto en el negocio.
	Ejecutar análisis del entorno para verificar los factores de riesgo que se presentan en el proceso.
Analizar el riesgo	Identificar, analizar y evaluar los riesgos de información dentro del proceso.
	Construir los escenarios de riesgo de TI y seguridad dentro del proceso. Identificar las amenazar para detectar medidas de emergencia.
	Identificar los riesgos residuales en el proceso e identificar exposiciones que puedan requerir una repuesta al riesgo
	Validar resultados del análisis de riesgos del proceso antes de usarlos para la toma de decisiones. Verificar alineamiento con requerimientos organizacionales.
Expresar el riesgo	Informar los resultados del análisis de riesgos del proceso de egreso a los stakeholders en términos adecuados y entendibles para decisiones empresariales.
	Adoptar un perfil de riesgo de acuerdo al proceso de egreso de pacientes y comunicarlo a los stakeholders junto la efectividad del proceso y los controles asociados. Identificar oportunidades de TI para aceptar un mayor riesgo e incrementar la capacidad de gestión.
Definir un portafolio de acciones para la gestión de riesgos	Monitorear periódicamente los riesgos de seguridad de información del proceso de egreso. Verificar que estos riesgos estén alineados con el apetito de riesgo.

	Definir propuestas para reducir el riesgo o proyectos para incrementar las oportunidades estratégicas de acuerdo a la ley de protección de datos personales, norma técnica peruana de la historia clínica y ley de emergencia.
Responder al riesgo	Aplicar las prácticas y controles para la mitigación de riesgos de seguridad. Se recomienda aplicar la norma ISO/IEC 27002:2013. Incluir controles preventivos y correctivos.

Tabla 9.1.58 - Proceso Egreso. Actividades de gestión habilitador: Gestionar el riesgo

Matiz de responsabilidades (RACI)

APO12: Gestionar el riesgo																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Recopilar datos		I				R		I	R	R	R	I		I	A	C	R	C	R	C
Analizar el riesgo		I				R		I	C	R	C	I		C	A	C	C	C	R	C
Expresar el riesgo		I				R		I	C	R	C	I		I	A	C	C	C	C	C
Definir portafolio de acciones para gestión del riesgo		I				R		I	C	A	R	I		I	R	I	R	I	C	C
Responder al riesgo		I				R		I	R	R	R	I		C	A	R	R	R	R	R

Tabla 9.1.59 - Matriz de responsabilidades para el proceso habilitador APO12 - Proceso Egreso

d. Proceso habilitador: Gestionar la seguridad

Este habilitador indica la necesidad de establecer un SGSI, no obstante este proceso de negocio no se considera que deba de formar parte de él a diferencia de los procesos de admisión y atención debido a que el manejo de datos críticos es mínimo y

un SGSI debe priorizar aquellos procesos críticos que forman la base y posteriormente ampliar el alcance.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Establecer y mantener un SGSI	Realizar la declaración de la aplicabilidad del SGSI.
Definir y gestionar un plan de tratamiento del riesgo de la seguridad de información	Diseñar, mantener y aplicar un plan de tratamiento de riesgos de seguridad de información alineados con los objetivos estratégicos de la organización y el proceso.
	Desarrollar propuestas de mejora al plan de riesgos basados en casos de negocio de acuerdo a los roles y responsabilidades a necesitar para su aplicación.
	Definir la medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizarlas para producir resultados reproducibles y comparables.
	Integrar la planificación, diseño, implementación y supervisión de procedimientos se seguridad y controles para prevención y detección temprana de eventos dentro del proceso de egreso y la respuesta a incidentes.

Tabla 9.1.60 - Proceso Egreso. Actividades de gestión habilitador: Gestionar la seguridad

Matriz de responsabilidades (RACI)

APO13: Gestionar la seguridad																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Establecer y mantener un SGSI					I	I	I				C				R				R	
Definir gestionar plan tratamiento de riesgos de seguridad información		C		C	C	C	C	I	I	C	A	C		I	R	C	C	I	R	C

Tabla 9.1.61 - Matriz de responsabilidades para el proceso habilitador APO13 - Proceso Egreso

e. Proceso habilitador: Gestionar los programas y proyectos

Este proceso habilitador incida que dentro del proceso de egreso se deben gestionar proyectos que aporten soluciones estratégicas que permitan alcanzar la eficiencia del proceso y el cumplimiento de requerimientos de seguridad de información. Se muestra también la matriz de responsabilidades.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Mantener un enfoque estándar para la gestión de programas y proyectos.	Incorporar los requerimientos de seguridad de información dentro de los proyectos asociados al proceso de egreso.
	Asegurar que los stakeholders se comprometan en supervisar los proyectos del proceso para garantizar el cumplimiento del enfoque de seguridad de información.
	Actualizar el enfoque de gestión de programas y proyectos. Aplicar las mejoras que se desprenden del uso de estrategias dentro del proceso de egreso.
Gestionar el compromiso de las partes interesadas	Identificar y comprometer a las partes interesadas para tomar decisiones en los proyectos del proceso egreso y medir el cumplimiento con los aspectos de seguridad. Verificar como estos cumplen dicho compromiso.
Desarrollar y mantener el plan del programa.	Desarrollar un plan de seguridad de información que incluya los controles que deben ser implementados. Asignar a los responsables que los implementen en el proceso de egreso.
	Incluir recursos dentro del proyecto para identificar e implementar los requerimientos de seguridad de información.
	Mantener el plan de programa para asegurar su actualización de acuerdo a los proyectos y el proceso asociado.
Planificar proyectos	Integrar la seguridad de información y las tecnologías con la gestión de proyectos.
	Desarrollar plan de proyecto con información que permita a la dirección controlar su progreso. Incluir recursos,

	responsabilidades e hitos que marcan el cierre de cada una de las etapas.
	Mantener los planes de proyecto y sus dependencias, asegurando la comunicación entre estos y que al realizar cambios en uno se reflejen en los demás.
Gestionar el riesgo de los programas y proyectos.	Registrar los riesgos de seguridad de información y las acciones correctivas. Revisar y actualizarlos periódicamente.
	Integrar proyectos de seguridad de información al programa y proceso de egreso de pacientes. Alinearlos a procedimientos y estándares de gestión de proyectos.
	Asignar responsabilidades al personal capacitado para gestionar los riesgos de los proyectos del proceso egreso.
Supervisar y controlar proyectos.	Programar evaluaciones a los proyectos para asegurar que los requerimientos de seguridad de información del proceso son implementados de forma efectiva.
	Supervisar los cambios al programa y revisar requerimientos de desempeño para verificar el avance.
	Obtener la aprobación y firma de los entregables producidos en cada iteración de los proyectos asociados.

Tabla 9.1.62 - Proceso Egreso. Actividades de gestión habilitador: Gestionar los programas y proyectos

Matriz de responsabilidades (RACI)

BAI01: Gestionar programas y proyectos																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)

Mantener enfoque para gestión de programas y proyectos	I	A	C	C	R		R		C	C	C			I	R		C		C	
Gestionar el compromiso de las partes interesadas		A	C	C	R	C	C	R	I		I				R	I	I	I	C	I
Desarrollar y mantener el plan del programa			C	C	A	C		R	R	C	R			I	C	I	I	I	R	C
Planificar proyectos						C	I	A	R		C				C	C	C	C	R	C
Gestionar el riesgo de los programas y proyectos					R	R	I	A	R	C	R			I	C	C	R	C	R	C
Supervisar y controlar proyectos					I	R	I	A	R	C	C			C	C	I	R	C	R	C

Tabla 9.1.63 - Matriz de responsabilidades para el proceso habilitador BAI01 - Proceso Egreso

f. Proceso habilitador: Gestionar el cambio

El proceso habilitador consiste en cómo se debe gestionar los cambios dentro del proceso de egreso de acuerdo a los parámetros y requerimientos de seguridad de información. La actividad cierre de cambios y documentación, no aplica para el proceso de egreso dado que puede ser gestionada desde el proceso de admisión al contar con políticas y actores similares.

Se muestra también la matriz de responsabilidades que según la aplicación del habilitador y el proceso de negocio establecer cómo se debe realizar la gestión del primero.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Evaluar, priorizar y autorizar peticiones de cambio	Asegurar que los cambios dentro del proceso de egreso se alinean a las políticas de seguridad de información.
	Realizar el análisis de impacto al realizar cambios en seguridad de información y a nivel general dentro del proceso.
	Asegurar que los cambios sean validados por los dueños del proceso de negocio de egreso del paciente. Evaluar los tipos de cambios permitidos en él.
	Considerar el impacto de los cambios en la gestión de proveedores de acuerdo a la seguridad de información, procurando que estos no afecten los acuerdos de servicio.

Gestionar cambios de emergencia	Desarrollar medidas para atender cambios de emergencia en el proceso de egreso a nivel de la seguridad de información.
	Registrar y mantener un registro de riesgos de seguridad de información a partir de cambios de emergencia realizados en el proceso.
	Supervisar los cambios de emergencia dentro del proceso de egreso y realizar las revisiones post-implantación involucrando a las partes interesadas.
Hacer seguimiento e informar cambios de estado	Mantener y supervisar un sistema de seguimiento e informe para las solicitudes de cambio dentro del proceso de acuerdo a las exigencias de seguridad de información.
	Elaborar informes respecto a los cambios de seguridad de información realizados en el proceso.

Tabla 9.1.64 - Proceso Egreso. Actividades de gestión habilitador: Gestionar el cambio

Matriz de responsabilidades (RACI)

BAI06: Gestionar el cambio	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Evaluar, priorizar y autorizar peticiones de cambio					A	R			C	C	R			I	R	C	R	C	R	
Gestionar cambios de emergencia					A	I				C	R		I	I	R	C	R	I	R	
Hacer seguimiento e informar cambios de estado					C	R			C		C				A	C	R	C	R	

Tabla 9.1.65 - Matriz de responsabilidades para el proceso habilitador BAI06 - Proceso Egreso

g. Proceso habilitador: Gestionar los activos

A continuación se presenta las actividades de gestión que aplican para este proceso habilitador que garantiza que dentro del proceso de egreso se cumplen los requerimientos de seguridad de información para la lista de activos incluidos en las actividades del proceso. Así mismo se detalla la matriz de responsabilidades para gestionar el proceso habilitador bajo el enfoque de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Identificar y registrar activos actuales	Identificar los activos relacionados al proceso de egreso del paciente hospitalizado y los requerimientos de seguridad asociados a estos.
	Identificar la dependencia entre estos activos y el nivel de criticidad dentro del proceso.
	Identificar si los activos del proceso de egreso están sujetos a alguna regulación adicional a la ley de protección de datos personales y la norma técnica peruana de la historia clínica. Verificar los aspectos contractuales de seguridad de información.
	Verificar y determinar si los activos se encuentran en condiciones útiles para soportar dicho proceso y si es que genera valor al negocio.
Gestionar activos críticos	Identificar que activos del proceso egreso de pacientes pueden ser considerados críticos para su cumplimiento. Supervisar el rendimiento a través de evaluaciones o planes que definan políticas de reparación o reemplazo
	Determinar los niveles de criticidad de los activos del proceso de egreso.
	Garantizar que los activos críticos del proceso cumplan los niveles de seguridad de información establecidos en el proceso y el negocio.
	Establecer políticas para el cambio de estos activos críticos de acuerdo a los riesgos de seguridad de información identificados.
Gestionar el ciclo de vida	Identificar y comunicar los riesgos de seguridad de

de los activos	información de los activos que soportan el proceso.
	Realizar adquisiciones de nuevos activos previamente autorizadas de acuerdo a procedimientos seguros que garanticen un nivel aceptable de riesgo.
	Establecer políticas para eliminar activos de forma segura.
	Asegurar que las medidas de seguridad de información se apliquen a los activos durante todo su ciclo de vida.

Tabla 9.1.66 - Proceso Egreso. Actividades de gestión habilitador: Gestionar los activos

Matriz de responsabilidades (RACI)

BAI09: Gestionar los activos	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Identificar y registrar activos actuales			C			C					C				I	R	A	C	C	
Gestionar activos críticos			C		I	C				C	C			C		R	A	C	C	C
Gestionar el ciclo de vida de los activos						C				I	C				I	R	A	C	I	

Tabla 9.1.67 - Matriz de responsabilidades para el proceso habilitador BAI09 - Proceso Egreso

h. Proceso habilitador: Gestionar las solicitudes de servicio e incidentes

Se presenta la lista de actividades de gestión para dar soporte al habilitador y que se acople al proceso de negocio de egreso de pacientes para así garantizar que los incidentes que afecten a la realización del proceso.

Se muestra la matriz de responsabilidades de acuerdo al proceso habilitador y la gestión dentro del proceso de egreso.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Definir esquemas de clasificación de incidentes y solicitudes de servicio	Definir y comunicar las características de los potenciales incidentes de seguridad de información para su reconocimiento y entendimiento del impacto en el proceso de egreso en caso se materialicen.
	Definir modelos de solicitudes de servicio relacionados a la seguridad de información para facilitar su atención y respuesta.
	Definir la clasificación y priorización de incidentes y solicitudes de servicio relacionados al proceso de egreso de acuerdo a los requerimientos de seguridad de información y el impacto en el negocio.
Registrar, clasificar y priorizar solicitudes e incidentes	Investigar los incidentes de seguridad y elaborar, en base a estos, procedimientos de respuesta. Asegurar que las medidas sean difundidas y protejan los pilares de seguridad de información.
	Registrar incidentes y solicitudes de servicio relacionados a la seguridad de información del proceso de egreso.
	Priorizar y clasificar los incidentes de acuerdo al impacto dentro del negocio y el proceso de egreso.
Verificar, aprobar y resolver solicitudes de servicio	Seguir procedimientos y modelos de solicitudes e incidentes para elementos frecuentes de manera que sean atendidos en menor tiempo.
Investigar, diagnosticar y localizar incidentes	Registrar un nuevo problema en caso no exista dentro de la base de datos y si el incidente de seguridad de información satisface los criterios para registro.
	Asignar a personal capacitado la gestión de incidentes del proceso de egreso de pacientes si es estos requieren mayor conocimiento para tratarlos y reducir el impacto.
	Identificar soluciones temporales o permanentes para los incidentes de seguridad de información, asignar su tratamiento a los especialistas respectivos dentro del proceso de egreso.
Resolver y recuperarse de incidentes	Definir un plan de respuesta de seguridad de información para los incidentes dentro del proceso de egreso.

	Ejecutar las acciones de recuperación para restablecer el proceso de egreso completamente.
	Documentar la solución e identificar si es temporal o permanente para tomarlo en cuenta a futuro.
Seguir el estado y emitir informes	Asegurar que los incidentes de seguridad de información, el análisis y seguimiento de estos, siguen los procedimientos de gestión existentes.
	Elaborar informes y distribuirlos periódicamente a los stakeholders como parte de la mejora continua.

Tabla 9.1.68 - Proceso Egreso. Actividades de gestión habilitador: Gestionar las solicitudes de servicio e incidentes

Matriz de responsabilidades (RACI)

DSS02: Gestionar solicitudes de servicio e incidentes	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Definir esquema de clasificación de incidentes y solicitud de servicio						C				I	I				A	C	R	R	R	C
Registrar, clasificar y priorizar solicitudes e incidentes						I				I	C						A	R	C	
Verificar, aprobar y resolver solicitudes de servicio						R				C	C				I	C	R	A	C	
Investigar, diagnosticar y localizar incidentes						R				I	C				I	I	R	A	C	
Resolver y recuperarse de incidentes						I				I	I			I	I	C	R	A	C	
Seguir el estado y emitir informes						I				I	C	I		I	I	I	A	R	I	

Tabla 9.1.69 - Matriz de responsabilidades para el proceso habilitador DSS02 - Proceso Egreso

i. Proceso habilitador: Gestionar la continuidad

Se presenta la lista de actividades del habilitador gestionar la continuidad, las cuales deben ser adoptadas dentro del proceso de egreso para cumplir con los objetivos de acuerdo al enfoque de seguridad del gobierno de TI.

Se muestra también la matriz de responsabilidades para gestionar el proceso habilitador dentro del proceso de negocio egreso del paciente hospitalizado. Se destaca la función del oficial de seguridad de información que brinda los lineamientos, según el enfoque de seguridad del gobierno de TI, para establecer un SGCN.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Definir las políticas de continuidad de negocio, objetivos y alcance	Determinar la criticidad del proceso de egreso de pacientes de acuerdo con los requerimientos de seguridad de información y el cumplimiento con la ley de protección de datos personales, norma técnica peruana de la historia clínica y ley de emergencia. Verificar si el proceso debe formar parte del programa de continuidad.
	Asegurar que la seguridad de información forma parte del ciclo de vida de continuidad de negocio.
	Identificar interesados, roles y responsabilidades dentro del proceso para alinearlos a los objetivos y políticas del SGCN.
Mantener una estrategia de continuidad	Identificar e incluir escenarios que den pie a eventos de información que afecten la continuidad del proceso egreso del paciente.
	Realizar el análisis de impacto de negocio de acuerdo a los lineamientos del proceso, incluyendo los factores de seguridad de información y el máximo tolerable de interrupción en estos aspectos.
	Analizar las amenazas de seguridad que afecten la continuidad del proceso para mejorar métodos preventivos e incrementar la resiliencia.
Desarrollar e implementar una respuesta a la continuidad de negocio	Definir los procedimientos de recuperación para reanudar el proceso de egreso y que este cumpla con los requerimientos de seguridad de información definidos.

Ejecutar, probar y revisar el plan de continuidad	Planificar actividades para probar el plan definido en los documentos. Asignar roles y responsabilidades para esta actividad y coordinar que no afecten al proceso.
	Realizar el análisis y revisión para determinar el logro.
Revisar, mantener y mejorar el plan de continuidad	Revisar el plan periódicamente tomando en cuenta los objetivos de negocio, objetivos de TI y los lineamientos del proceso de egreso. Considerar posibles cambios producto del entorno.
	Reconocer qué incidentes de seguridad de información pueden ocasionar la interrupción del negocio, por ello se debe incrementar el nivel de gestión de éstos.
Gestionar acuerdos de respaldo	Asegurar que los requerimientos de seguridad se cumplen en los procesos de backup y restauración de información.
	Realizar las copias de seguridad respectivas y establecer políticas para su gestión de acuerdo a la ley de protección de datos personales y la norma técnica peruana de la historia clínica, salvaguardando los datos del paciente.
	Probar y mantener las copias de seguridad recientes y aquellas archivadas de manera periódica para garantizar la disponibilidad de la información y su integridad.
Ejecutar revisiones post-reanudación	Evaluar la efectividad del plan de acuerdo a los tiempos definidos en el análisis de impacto de negocio de acuerdo al proceso de egreso del paciente.
	Identificar debilidades u omisiones como parte de la mejora continua para asegurar que el proceso de egreso podrá llevarse a cabo sin inconvenientes ante cualquier evento asegurando la información de los involucrados, en otras palabras, su integridad.

Tabla 9.1.70 - Proceso Egreso. Actividades de gestión habilitador: Gestionar la continuidad

Matriz de responsabilidades (RACI)

DSS04: Gestionar la continuidad																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Definir la política de continuidad de negocio, objetivos y alcance				A	C	R				C	C			C	R	C	R	C	C	R
Mantener una estrategia de continuidad				A	C	R				I	I			C	R	I	R		R	R
Desarrollar e implementar una respuesta a la continuidad de negocio					I	R					C		I	C	R	C	R		R	A
Ejercitar, probar y revisar el plan de continuidad					I	R					C		I	R	R	C	R	I	R	A
Revisar, mantener y mejorar el plan de continuidad				A	I	R				I	C				R	I	C		C	R
Gestionar acuerdos de respaldo											I					C	C		C	R
Ejecutar revisiones post-reanudación					C	R				I	C				R	C	C	I	C	A

Tabla 9.1.71 - Matriz de responsabilidades para el proceso habilitador DSS04 - Proceso Egreso

j. Proceso habilitador: Gestionar los servicios de seguridad

El presente habilitador se encarga de asegurar por medio de la aplicación de las sub-actividades que el proceso de egreso cuenta con las medidas pertinentes para evitar incidentes a nivel de seguridad en sus actividades y protegiendo el procesamiento de datos.

Se muestra también la matriz de responsabilidades respectiva.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Proteger contra software malicioso	Instalar y activar herramientas de protección frente a software malicioso en las estaciones o activos que brindan soporte al proceso de egreso. Concientizar al usuario sobre el empleo de estas.
	Filtrar el tráfico entrante de información como correos electrónicos y descargas para protegerse frente a información no solicitada.
Gestionar la seguridad de la red y las conexiones	Mantener una política para la seguridad de conexiones de red entre los activos que soportan el proceso egreso.
	Cifrar la información en tránsito de acuerdo con su clasificación verificando el cumplimiento con la ley de protección de datos personales.
Gestionar la seguridad de los puestos de usuario final	Cifrar la información almacenada dentro de los activos de acuerdo a su clasificación y nivel de criticidad.
	Configurar los sistemas operativos de forma correcta y segura en las estaciones del personal que ejecuta el proceso de egreso.
	Implementar mecanismos de bloqueo en los dispositivos.
	Deshacerse de los dispositivos de usuario final de forma segura.
Gestionar la identidad del usuario y el acceso lógico	Segregar y gestionar cuentas de usuario privilegiadas.
	Realizar regularmente revisiones de la gestión de cuentas y privilegios que abarca el proceso de egreso. Verificar que la identificación de estas es unequívoca.
Gestionar documentos sensibles y dispositivos de salida	Establecer procedimientos de empleo, eliminación y destrucción de formularios especiales como las historias clínicas, solicitudes de alta y acta de egreso de paciente.
	Asignar privilegios de acceso a documentación y a su modificación durante el proceso de egreso del paciente.
	Realizar un inventario de documentos sensibles o dispositivos de salida críticos involucrados en el proceso.
	Establecer políticas de protección física apropiada sobre formularios o documentos que contienen información sensible.

Tabla 9.1.72 - Proceso Egreso. Actividades de gestión habilitador: Gestionar los servicios de seguridad

Matriz de responsabilidades (RACI)

DSS05: Gestionar los servicios de seguridad	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Proteger contra software malicioso						R				C	A		R		C	C	R	I	C	
Gestionar seguridad de red y conexiones						I				C	A			C	C	C	R	I	C	
Gestionar seguridad de puestos de usuario final						I				C	A			C	C	C	R	I	R	
Gestionar identidad del usuario y acceso lógico						R				C	A		I	I	C	C	R	I	R	C
Gestionar documentos sensibles y dispositivos de salida						C	I			I	C			I	A	I	R		R	

Tabla 9.1.73 - Matriz de responsabilidades para el proceso habilitador DSS05 - Proceso Egreso

1.1.5 Proceso Identificación del paciente hospitalizado

Este proceso es transversal a los tres (3) anteriores, es decir, puede ser empleado en dichos procesos en un instante determinado y debe estar alineado con la ley de protección de datos personales, ley de emergencia y norma técnica peruana de la historia clínica.

Los procesos habilitadores tienen una aplicación menos técnica respecto a los procesos anteriores, pero de acuerdo al enfoque de seguridad de información, se pretende cumplir con los requerimientos definidos y alinear al marco regulatorio expuesto.

a. Gestionar la estrategia

Se presenta a continuación la aplicación de las actividades de gestión para este proceso habilitador de acuerdo con las exigencias y requerimientos del proceso de identificación.

Se realiza la evaluación y se propone la matriz de responsabilidades para realizar la gestión bajo el enfoque de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Comprender la dirección de la empresa	Identificar como se puede adaptar la seguridad de información a este proceso de manera que garantice el cumplimiento de la ley de protección de datos personales y la ley de emergencia.
	Identificar los stakeholders del proceso y cuáles son sus requerimientos de seguridad de información.
	Determinar las prioridades para desarrollar los cambios estratégicos dentro del proceso.
Realizar un análisis de brecha	Identificar dentro del proceso las brechas a cerrar y los cambios requeridos para llegar al nivel deseado.
	Examinar el nivel de cumplimiento del proceso respecto a la ley de protección de datos personales, ley de emergencia y norma técnica peruana de la historia clínica.
	Mejorar la definición del estado deseado en el proceso y sus objetivos. Sustentarlos demostrando los beneficios a partir de este estado frente al impacto en caso no se llegara a esta meta.
Definir el plan estratégico y la hoja de ruta	Definir la estrategia de seguridad de información y alinearla las estrategias de negocio para el cumplimiento de objetivos dentro del proceso de identificación.
	Crear la hoja de ruta del proceso la cual a su vez señale los riesgos y costos de los cambios.
	Obtener el apoyo de las partes interesadas y la aprobación del plan.

Comunicar la estrategia y la dirección de TI	Desarrollar el plan estratégico y el plan de seguridad de información que abarque el proceso y comunicarlo a los stakeholders
	Desarrollar el plan de comunicación de acuerdo a público objetivo identificando los canales de comunicación y horarios disponibles.
	Obtener realimentación y actualizar el plan de comunicaciones y la estrategia de seguridad de información según sea necesario para mantener el impulso.

Tabla 9.1.74 - Proceso Identificación. Actividades de gestión habilitador: Gestionar la estrategia

Matriz de responsabilidades (RACI)

APO02: Gestionar la estrategia	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Comprender la dirección de la empresa		C	C	C	A	C	C			C	R	C			R	I	I	I	R	I
Realizar un análisis de brecha					R	R	C			C	C		C	C	A	I	C	I	R	I
Definir plan estratégico y hoja de ruta		C	I	C	C		C		R	C	C			C	A	I	C	I	C	I
Comunicar estrategia y dirección de TI	I	R	I	I	R	I	A	I	I	I	R	I	I	I	R	I	I	I	I	I

Tabla 9.1.75 - Matriz de responsabilidades para el proceso habilitador APO02 - Proceso Identificación

b. Proceso habilitador: Gestionar los recursos humanos

Se presenta las actividades y sub-actividades de gestión a aplicar para este proceso habilitador gestión de recursos humanos y cómo es que ayudan al proceso de identificación a alinearse con requerimientos externos.

Se muestra también la matriz de responsabilidades para conllevar al cumplimiento y evolución de niveles de madurez. Se destaca los roles ejercidos por el oficial de seguridad de información que imparte las medidas para el correcto alineamiento con las estrategias y los requerimientos definidos por los stakeholders.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Mantener la dotación del personal suficiente y adecuada	Asegurar que los requisitos de seguridad se incorporan en el proceso de contratación.
	Asegurar la existencia de capacitaciones y que existe personal capaz de cubrir funciones críticas de otro para reducir la dependencia.
Identificar personal clave de TI	Asegurar la segregación de funciones en roles críticos del proceso.
	Identificar y ejecutar acciones de acuerdo a los cambios laborales relacionados a los actores del proceso de identificación.
Mantener las habilidades y competencias del personal	Definir habilidades y competencias necesarias de los recursos para lograr los objetivos dentro del proceso y poder escalar hacia los objetivos de alto nivel.
	Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos. Identificar si se requieren habilidades adicionales para cubrir el proceso y ejecutar el plan de acción para desarrollarlas.
Evaluar el desempeño laboral de los empleados	Dentro de la evaluación del desempeño, considerar criterios con respecto a la función de seguridad de información.
	Proporcionar instrucciones para uso y almacenamiento de información personal dentro del proceso de evaluación.
	Implementar un proceso de reconocimiento a medida el personal alcance el compromiso y logre sus objetivos.

Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio	Comprender la demanda actual y futura de recursos humanos involucrados dentro del proceso de identificación para apoyar el logro de objetivos de TI y necesidades operativas del día a día.
Gestionar el personal contratado	Obtener un acuerdo formal por parte del personal sobre las políticas y requisitos de la seguridad de información a aplicarse en el proceso.
	Implementar políticas o procedimientos que describan como gestionar al personal que ejecuta el proceso
	Asegurar que el personal cumple con sus funciones y desempeño esperado en la ejecución del proceso.

Tabla 9.1.76 -Proceso Identificación. Actividades de gestión habilitador: Gestionar los recursos humanos

Matriz de responsabilidades (RACI)

APO07: Gestionar los recursos humanos	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Mantener personal suficiente y adecuado									R	I	C		R		A	C	C	I	R	I
Identificar personal clave de TI						C		I	R		C		R		A	C	C	I	R	I
Mantener habilidad y competencia del personal						I			R		C		R		A	C	C	C	R	I
Evaluar desempeño laboral del empleado									R		C		R		A	C	C	C	R	C
Planificar y realizar seguimiento del uso recursos humanos de TI y negocio					R	C	A	C	R		C		I		R	C	C	C	R	R
Gestionar personal contratado						I	I	I	R		C		R		A	C	C	C	R	C

Tabla 9.1.77 - Matriz de responsabilidades para el proceso habilitador APO07 - Proceso Identificación

c. Proceso habilitador: Gestionar el riesgo

Se muestra la aplicación del habilitador dentro del proceso identificación del paciente. Se prioriza los riesgos de seguridad de información y aquellos que generen el incumplimiento de la ley de protección de datos personales. Se presenta la matriz de responsabilidades respectiva.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Recopilar datos	Identificar y recolectar datos para la identificación, análisis y comunicación de los riesgos de seguridad de información.
	Determinar en qué condiciones del proceso se materializó el riesgo. Identificar el impacto en el negocio.
	Ejecutar análisis del entorno para verificar los factores de riesgo asociados al proceso.
Analizar el riesgo	Identificar, analizar y evaluar los riesgos de información dentro del proceso.
	Identificar los riesgos residuales dentro del proceso e identificar cuáles de ellos puedan requerir una repuesta al riesgo
	Validar resultados del análisis de riesgos del proceso antes de usarlos para la toma de decisiones. Verificar alineamiento con requerimientos organizacionales.
Expresar el riesgo	Definir e implementar evaluaciones y estrategias de respuesta frente a los riesgos del proceso de identificación.
	Informar los resultados del análisis de riesgos a los stakeholders sobre el proceso en términos adecuados y entendibles para soportar decisiones empresariales.
	Informar el perfil del riesgo a los stakeholders junto con la efectividad del proceso de identificación y los controles asociados. Identificar oportunidades de TI para aceptar un mayor riesgo e incrementar la capacidad de gestión.
Definir un portafolio de acciones para la gestión de riesgos	Monitorear continuamente los riesgos de seguridad de información del proceso y verificar que el riesgo este alineado con el apetito y tolerancia al riesgo.

	Definir conjunto de propuestas para reducir el riesgo o proyectos para incrementar las oportunidades estratégicas y retorno de beneficios.
Responder al riesgo	Aplicar las prácticas y controles para la mitigación de riesgos de seguridad. Se recomienda aplicar en este caso la norma ISO/IEC 27002:2013.

Tabla 9.1.78 Proceso Identificación. Actividades de gestión habilitador: Gestionar el riesgo

Matriz de responsabilidades (RACI)

APO12: Gestionar el riesgo																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Recopilar datos		I				R			R	R	R	I		I	A	C	C	C	R	C
Analizar el riesgo		I				R			C	R	C	I		C	A	C	C	C	R	C
Expresar el riesgo		I				R			C	R	C	I		I	A	I	C	I	C	I
Definir portafolio de acciones para gestión del riesgo		I				R			C	A	C	I		I	R	I	I	I	C	C
Responder al riesgo		I				R			R	R	R	I		C	A	C	R	C	R	C

Tabla 9.1.79 - Matriz de responsabilidades para el proceso habilitador APO12 - Proceso Identificación

d. Proceso habilitador: Gestionar la seguridad

Se presenta la aplicación del proceso habilitador al proceso. Debido a que es transversal al macro-proceso hospitalario, no se considera que deba formar parte del SGSI, pero sí debe de considerar sus actividades y su implicancia con los procesos de admisión y atención. Se presenta la matriz de responsabilidades.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Establecer y mantener un SGSI	Realizar la declaración de la aplicabilidad del SGSI. En este caso determinar cómo alinea el proceso de identificación con los que soportan el SGSI.
Definir y gestionar un plan de tratamiento del riesgo de la seguridad de información	Diseñar, mantener y aplicar un plan de tratamiento de riesgos de seguridad de información alineados con los objetivos estratégicos de la organización y fines del proceso.
	Desarrollar propuestas de mejora al plan de riesgos basados en casos de negocio de acuerdo a los roles y responsabilidades a necesitar para su aplicación y acorde a los drivers identificados.
	Definir la medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizarlas para producir resultados reproducibles y comparables.
	Integrar la planificación, diseño, implementación y supervisión de procedimientos se seguridad y controles para prevención y detección temprana de eventos dentro del proceso de egreso y la respuesta a incidentes.

Tabla 9.1.80 - Proceso Identificación. Actividades de gestión habilitador: Gestionar la seguridad

Matriz de responsabilidades (RACI)

APO13: Gestionar la seguridad	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Establecer y mantener un SGSI					I	I	I				C				R				R	
Definir gestionar plan tratamiento de riesgos de seguridad información		C		C	C	C	C	I	I	C	A	C		I	R	I	C	I	R	I

Tabla 9.1.81 - Matriz de responsabilidades para el proceso habilitador APO13 - Proceso Identificación

e. Proceso habilitador: Gestionar los programas y proyectos

Se detalla las actividades y sub-actividades de gestión para el proceso habilitador dentro del proceso identificación de pacientes. Los proyectos deben estar alineados a los requerimientos de seguridad de información y a la ley de protección de datos personales y la ley de emergencia. Se presenta también la matriz de responsabilidades para la gestión de este a lo largo del ciclo de vida de gobierno.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Mantener un enfoque estándar para la gestión de programas y proyectos.	Incorporar los requerimientos de seguridad de información dentro de los proyectos asociados al proceso de identificación.
	Asegurar que los stakeholders se comprometan a supervisar proyectos enfocados a la seguridad de información.
	Actualizar el enfoque de gestión de programas y proyectos y aplicar las mejoras que se desprenden del uso de estrategias dentro del proceso de identificación.
Desarrollar y mantener el plan del programa.	Desarrollar un plan de seguridad de información que incluya los controles que deben ser implementados. Asignar a los responsables que los implementen en el proceso de identificación.
	Incluir recursos dentro del proyecto para identificar e implementar requerimientos de seguridad de información.
	Mantener el plan de programa para asegurar su actualización de acuerdo al proyecto y el proceso asociado.
Planificar proyectos	Integrar la seguridad de información al proyecto e identificar medidas u oportunidades tecnológicas.
	Desarrollar plan de proyecto con información que permita a la dirección controlar su progreso. Incluir recursos, responsabilidades e hitos que marcan el cierre de cada una de las etapas.
	Mantener los planes de proyecto y sus dependencias, asegurando que los cambios en uno se reflejen en los

	demás.
Gestionar el riesgo de los programas y proyectos.	Registrar los riesgos de seguridad de información y las acciones correctivas. Revisar y actualizarlos periódicamente.
	Integrar proyectos de seguridad de información al programa y proceso de identificación. Alinearlos a procedimientos y estándares de gestión de proyectos.
Supervisar y controlar proyectos.	Programar evaluaciones a los proyectos para asegurar que los requerimientos de seguridad de información del proceso son implementados de forma efectiva.
	Supervisar los cambios al programa y revisar requerimientos de desempeño para verificar el avance.

Tabla 9.1.82 - Proceso Identificación. Actividades de gestión habilitador: Gestionar los programas y proyectos

Matriz de responsabilidades (RACI)

BAI01: Gestionar programas y proyectos	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Mantener enfoque para gestión de programas y proyectos	I	A	C	C	R		R		C	C	C				R				C	
Desarrollar y mantener el plan del programa			C	C	A	C		C	R	C	R			I	C	I	I	I	C	I
Planificar proyectos						C	I	A	R		C				C	C	C	I	C	C
Gestionar el riesgo de los programas y proyectos					R	R	I	A	R	C	R				C	C	C		C	C
Supervisar y controlar proyectos					I	R	I	A	R	C	C				C	I	C	I	R	I

Tabla 9.1.83 - Matriz de responsabilidades para el proceso habilitador BAI01 - Proceso Identificación

f. Proceso habilitador: Gestionar el cambio

Se presentan las actividades de gestión a aplicar para la gestión de cambios dentro del proceso de acuerdo a lo establecido por el gobierno de TI con enfoque a la seguridad de información. Se muestra también la matriz de responsabilidades para llevar a cabo su gestión durante el ciclo de vida.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Evaluar, priorizar y autorizar peticiones de cambio	Asegurar que los cambios dentro del proceso de identificación se alinean a las políticas de seguridad de información y de acuerdo a la ley de protección de datos personales y la ley de emergencia.
	Realizar el análisis de impacto al realizar cambios dentro del proceso y verificar cómo estos afectan a la seguridad de información.
	Asegurar que los cambios sean validados por los dueños del proceso de negocio de identificación del paciente. Evaluar los tipos de cambios para esta validación.
	Considerar el impacto de los cambios en el proceso de acuerdo a los requerimientos de seguridad de información
Gestionar cambios de emergencia	Desarrollar medidas para atender cambios de emergencia en el proceso de identificación a nivel de la seguridad de información.
	Registrar y mantener un registro de riesgos de seguridad de información a partir de cambios de emergencia realizados en el proceso.
	Supervisar los cambios de emergencia en el proceso de identificación y realizar las revisiones post-implantación.
Hacer seguimiento e informar cambios de estado	Mantener y supervisar un sistema de seguimiento e informe para las solicitudes de cambio dentro del proceso de acuerdo a las exigencias de seguridad de información.
	Elaborar informes respecto a los cambios en seguridad de información a nivel de proceso.

Tabla 9.1.84 - Proceso Identificación. Actividades de gestión habilitador: Gestionar el cambio

Matriz de responsabilidades (RACI)

BAI06: Gestionar el cambio																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Evaluar, priorizar y autorizar peticiones de cambio					A	R			C	C	R				R	I	C	I	R	
Gestionar cambios de emergencia					A	I				C	R		I	I	R	C	R	I	R	
Hacer seguimiento e informar cambios de estado					C	R			C		C				A	I	C		R	

Tabla 9.1.85 - Matriz de responsabilidades para el proceso habilitador BAI06 - Proceso Identificación

g. Proceso habilitador: Gestionar los activos

Se muestra la aplicación de las actividades de gestión para el proceso habilitador, de manera que se cumpla con las iniciativas de gobierno bajo el enfoque de seguridad. Se presenta también la matriz de responsabilidades respectiva.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Identificar y registrar activos actuales	Identificar los activos del proceso de identificación del paciente y los requerimientos de seguridad asociados.
	Identificar la criticidad de los activos dentro del proceso.
	Identificar si los activos del proceso cumplen con los aspectos de seguridad de información.
	Verificar y determinar si los activos se encuentran en condiciones útiles para soportar dicho proceso y si es que genera valor al negocio.
Gestionar activos críticos	Identificar qué activos del proceso pueden ser considerados como. Supervisar su rendimiento por medio

	de evaluaciones o planes en los que se definan las políticas de reparación o reemplazo.
	Garantizar que los activos críticos del proceso cumplan los niveles de seguridad de información establecidos para el proceso.
	Establecer las políticas para el cambio de estos activos críticos de acuerdo a los riesgos de seguridad de información previamente identificados.
Gestionar el ciclo de vida de los activos	Identificar y comunicar los riesgos de seguridad de información relacionados a los activos que soportan el proceso de identificación del paciente hospitalizado.
	Gestionar activos desde su adquisición hasta su eliminación de forma segura y con la aprobación de los interesados, siguiendo los lineamientos de seguridad de información.
	Asegurar que las medidas de seguridad de información se apliquen a los activos durante todo su ciclo de vida.

Tabla 9.1.86 - Proceso Identificación. Actividades de gestión habilitador: Gestionar los activos

Matriz de responsabilidades (RACI)

BAI09: Gestionar los activos	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Identificar y registrar activos actuales			C			C					C				I	R	A		C	
Gestionar activos críticos			C		I	C				C	C			C		R	A		C	I
Gestionar el ciclo de vida de los activos						C				I	C					R	A		I	

Tabla 9.1.87 - Matriz de responsabilidades para el proceso habilitador BAI09 - Proceso Identificación

h. Proceso habilitador: Gestionar las solicitudes de servicio e incidentes

Se presenta la aplicación de las actividades para el proceso habilitador de acuerdo al proceso de negocio identificación de pacientes. Se detalla la matriz de responsabilidades para llevar a cabo su gestión dentro del ciclo de vida de gobierno.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Definir esquemas de clasificación de incidentes y solicitudes de servicio	Definir y comunicar las características de los incidentes de seguridad de información para su reconocimiento del impacto en caso se materialicen dentro del proceso.
Registrar, clasificar y priorizar solicitudes e incidentes	Registrar incidentes y solicitudes de servicio relacionados a seguridad de información del proceso de identificación.
Verificar, aprobar y resolver solicitudes de servicio	Seguir procedimientos y modelos de solicitudes e incidentes para elementos frecuentes de manera que sean atendidos en menor tiempo.
Investigar, diagnosticar y localizar incidentes	Identificar posibles soluciones temporales o permanentes para los incidentes de seguridad de información, asignar su tratamiento a los especialistas respectivos.
Resolver y recuperarse de incidentes	Definir un plan de respuesta de seguridad de información para los incidentes dentro del proceso de identificación.
	Ejecutar las acciones de recuperación para restablecer el proceso de identificación completamente.
	Documentar la resolución e identificar si es temporal o permanente para tomarlo en cuenta a futuro.
Seguir el estado y emitir informes	Asegurar que los incidentes de seguridad de información, el análisis y seguimiento de estos, siguen los procedimientos de gestión existentes.
	Elaborar informes y distribuirlos periódicamente a los stakeholders como parte de la mejora continua.

Tabla 9.1.88 - Proceso Identificación. Actividades de gestión habilitador: Gestionar las solicitudes de servicio e incidentes

Matriz de responsabilidades (RACI)

DSS02: Gestionar solicitudes de servicio e incidentes																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Definir esquema de clasificación de incidentes y solicitud de servicio						C				I	I				A	C	C	I	C	I
Registrar, clasificar y priorizar solicitudes e incidentes						I				I	C						A	C	R	
Verificar, aprobar y resolver solicitudes de servicio						R				C	C				I	C	R	A	C	
Investigar, diagnosticar y localizar incidentes						R				I	C				I	C	C	A	C	
Resolver y recuperarse de incidentes						I				I	C			C	I	C	R	A	R	
Seguir el estado y emitir informes						I				I	C			I	I	I	A	R	I	

Tabla 9.1.89 - Matriz de responsabilidades para el proceso habilitador DSS02 - Proceso Identificación

i. Proceso habilitador: Gestionar la continuidad

Se presenta la aplicación de las actividades de gestión para el proceso habilitador gestión de la continuidad dentro del proceso de identificación a nivel estratégico. Así mismo, se presenta la matriz de responsabilidades para llevar a cabo el seguimiento y la gestión del habilitador durante el ciclo de vida de gobierno de TI bajo el enfoque de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Mantener una estrategia de continuidad	Identificar e incluir escenarios que den pie a eventos de información que afecten la continuidad del proceso.
	Analizar las amenazas de seguridad que afecten la

	continuidad del proceso para mejorar métodos preventivos e incrementar la resiliencia.
Desarrollar e implementar una respuesta a la continuidad de negocio	Definir los procedimientos de recuperación para reanudar el proceso de identificación y que cumpla con los requerimientos de seguridad de información definidos.
Revisar, mantener y mejorar el plan de continuidad	Reconocer qué incidentes de seguridad de información pueden ocasionar la interrupción del negocio, por ello se debe incrementar el nivel de gestión de éstos.
Gestionar acuerdos de respaldo	Asegurar que los requerimientos de seguridad se cumplen en los procesos de backup y restauración de información.
	Realizar las copias de seguridad respectivas y establecer políticas para su gestión de acuerdo a la ley de protección de datos personales.
	Probar y mantener las copias de seguridad recientes, y aquellas archivadas, de manera periódica para garantizar la disponibilidad de la información y su integridad.
Ejecutar revisiones post-reanudación	Evaluar la efectividad de las estrategias de acuerdo a los tiempos definidos en el análisis de impacto de negocio.
	Identificar debilidades u omisiones como parte de la mejora continua para asegurar que el proceso podrá llevarse a cabo sin inconvenientes ante cualquier evento.

Tabla 9.1.90 - Proceso Identificación. Actividades de gestión habilitador: Gestionar la continuidad

Matriz de responsabilidades (RACI)

DSS04: Gestionar la continuidad																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Mantener una estrategia de continuidad				A	C	R				I	C				R	C	C		R	R

Desarrollar e implementar una respuesta a la continuidad de negocio					I	R					C		I	C	R	I	C		R	A
Revisar, mantener y mejorar el plan de continuidad				A	I	R				I	C				R	C	C		C	R
Gestionar acuerdos de respaldo											I					C	I		C	R
Ejecutar revisiones post-reanudación					C	R				I	C				R	I	C		C	A

Tabla 9.1.91 - Matriz de responsabilidades para el proceso habilitador DSS04 - Proceso Identificación

j. Proceso habilitador: Gestionar los servicios de seguridad

Se muestra las actividades de gestión que aplican de acuerdo al proceso de identificación de pacientes y como esta se lleva a cabo de acuerdo a los requisitos de seguridad de información. Se presenta la matriz de responsabilidades para gestionar el habilitador durante el ciclo de vida de gobierno.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Proteger contra software malicioso	Instalar y activar herramientas de protección frente a software malicioso las estaciones o activos que brindan soporte al proceso de identificación. Concientizar al usuario sobre el empleo de estas.
	Filtrar el tráfico entrante de información como correos electrónicos y descargas para protegerse frente a información no solicitada.
Gestionar la seguridad de los puestos de usuario final	Cifrar la información almacenada dentro de los activos de acuerdo a su clasificación y nivel de criticidad.
	Configurar los sistemas operativos de forma correcta y segura en las estaciones del personal que ejecuta el proceso de identificación.
	Implementar mecanismos de bloqueo en los dispositivos.
	Deshacerse de los dispositivos de usuario final de forma segura.
Gestionar la identidad del usuario y el acceso lógico	Según los requerimientos del proceso, mantener los derechos de acceso
	Segregar y gestionar cuentas de usuario privilegiadas.

Gestionar documentos sensibles y dispositivos de salida	Establecer procedimientos de empleo, eliminación y destrucción de los brazaletes de identificación.
	Asignar privilegios de acceso a documentación y a su modificación durante el proceso de identificación.
	Realizar un inventario de documentos sensibles o dispositivos de salida críticos involucrados durante el proceso.
	Establecer políticas de protección física apropiadas sobre documentos y activos sensibles empleados para identificar pacientes.

Tabla 9.1.92 - Proceso Identificación. Actividades de gestión habilitador: Gestionar los servicios de seguridad

Matriz de responsabilidades (RACI)

DSS05: Gestionar los servicios de seguridad																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Proteger contra software malicioso						R				C	A		R		C	I	C		R	
Gestionar seguridad de puestos de usuario final						I				C	A		I		C		C		R	
Gestionar identidad del usuario y acceso lógico						R				C	A		I	I	C	C	C		R	
Gestionar documentos sensibles y dispositivos de salida						C				I	C			I	A	I	C		R	

Tabla 9.1.93 - Matriz de responsabilidades para el proceso habilitador DSS05 - Proceso Identificación

ANEXO J: Aplicación norma ISO/IEC 27002:2013

10.1 Mapeo actividades de gestión a norma ISO/IEC 27002:2013

Dominio	Apartado del dominio y objetivo	Actividad de control
Políticas de seguridad	**Administrar la dirección de la seguridad de información:** Brindar dirección a la gestión y soporte de la información de seguridad de información de acuerdo con requerimientos de negocio relevantes y la ley de protección de datos personales y norma técnica peruana de la historia clínica.	Establecer políticas de seguridad de información
		Revisar las políticas de seguridad de información
Organización de la seguridad de información	**Organización interna:** Establecer un framework para la gestión y control de la seguridad de la información dentro de la organización.	Organización interna
		Roles y responsabilidades de seguridad de información
		Segregación de funciones
		Seguridad de información en la gestión de proyectos
Seguridad en Recursos humanos	**Antes del empleo:** Asegurar que los trabajadores, contratistas y los usuarios externos entiendan sus responsabilidades y sean los adecuados para ocupar ese rol	Términos y condiciones de empleo
		Revisión
	Durante el empleo: Asegurar que los trabajadores y contratistas conozcan y cumplan sus responsabilidades de seguridad de información.	Gestión de responsabilidades
		Educación y entrenamiento sobre los requerimientos y funciones de seguridad de información
	Término de empleo: Proteger los intereses de la organización como parte de los procesos de cambio o término del empleo.	Finalización o cambio de las responsabilidades del trabajador.

Gestión de activos	**Responsabilidad de activos:** Identificar los activos de la organización y definir las responsabilidades de protección adecuadas	Inventario de activos
		Uso aceptable de activos
	Clasificación de la información: Asegurar que la información recibe un nivel apropiado de protección de acuerdo a su importancia en la organización.	Clasificar la información
	Gestión de medios: asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización	Gestión de medios extraíbles
		Medios físicos de transferencia
Control de accesos	**Requisitos de negocio de control de accesos:** limitar el acceso a la información y a las instalaciones de procesamiento de información	Políticas de control de accesos
		Acceso a redes y servicios de red
	Gestión de acceso del usuario: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios	Registro de usuarios y cancelación de registros
		Brindar accesos a usuarios
		Gestión de derechos de acceso privilegiados
		Gestionar la información secreta de autentificación
		Revisión de los derechos de acceso
		Eliminación o cambio de derechos de acceso
	Responsabilidades del usuario: Hacer que los usuarios sean responsables de salvaguardar su información de autenticación	Uso de la información de autenticación secreta
	Sistema y aplicación de control de acceso: Evitar el acceso no autorizado a los sistemas y aplicaciones	Restricción de acceso a la información
		Sistema de gestión de contraseñas

		Procedimientos de accesos seguros
Seguridad física y ambiental	**Áreas seguras:** impedir el acceso físico no autorizado, daño e interferencia a la información de la organización y las instalaciones de procesamiento de información	Asegurar habitaciones e instalaciones
		Protección contra amenazas externas y ambientales
		Trabajo en áreas seguras
	Equipos: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización	Desplazamiento de equipos y protección
		Mantenimiento de equipos
		Eliminación de activos
		Eliminación segura o reutilización de equipo
		Limpieza de escritorios y políticas de pantalla transparente.
Seguridad de operaciones	**Procedimientos y responsabilidades operacionales:** Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información	Procedimientos operativos documentados
		Gestión de cambios
	Protección contra malware: Asegurar que las instalaciones de procesamiento de información y esta estén protegidas contra malware.	Controles contra el malware
	Backup: Evitar la pérdida de datos	Backup de información
	Registro de eventos: Registrar eventos y generar evidencias	Registro de eventos
	Control de software operativo: Garantizar la integridad de los sistemas operativos	Instalación de software en sistemas operativos
	Gestión de Vulnerabilidades técnica: evitar la explotación de vulnerabilidades	Restricciones de instalación de software

	técnicas	
	Consideraciones de auditoría de sistemas de información: minimizar el impacto de las actividades de auditoría en los sistemas operativos	Consideraciones de auditoría de sistemas de información
Seguridad de comunicaciones	**Transferencia de información:** mantener la seguridad de información que se transfiere dentro de una organización y con cualquier entidad externa	Políticas y procedimientos de transferencia de información
		Mensajería electrónica
		Acuerdos de confidencialidad o no divulgación
Relaciones con los proveedores	**Gestión de proveedores de servicios de entrega:** Mantener un nivel adecuado de la seguridad y la prestación de servicios de información en línea con acuerdos con proveedores	Seguimiento y revisión de los servicios de proveedores
		Gestión de cambios en los servicios de proveedores
Gestión de incidentes de seguridad de información	**Gestión de incidentes de seguridad de información y mejoras:** Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de información, incluida la comunicación de eventos de seguridad y debilidades	Reportes de eventos de seguridad de información
		Vulnerabilidades de seguridad de información
		Evaluación y decisión sobre los eventos de seguridad de información
		Respuesta a incidentes de seguridad de información
		Reunión de evidencias
Aspectos de seguridad de información de la gestión de continuidad de negocio	**Continuidad de la seguridad de información:** garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de información, incluida la comunicación de eventos de seguridad y vulnerabilidades	Planificación de la continuidad de seguridad de información
		Implementación de la continuidad de seguridad de información
		Verificar, revisar y evaluar

		la continuidad de la seguridad de información
	Redundancias: asegurar la disponibilidad de instalaciones de procesamiento de información	Disponibilidad de instalaciones de procesamiento de información
Cumplimiento	**Cumplimiento de los requisitos legales y contractuales:** evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de información y con los requisitos de seguridad	Identificación de los requerimientos aplicables legales y contractuales
		Privacidad y protección de datos personales
	Revisiones de la seguridad de información: Asegurar que la seguridad de información es implementado y operado de acuerdo con las políticas y procedimientos de la organización	Cumplimiento de las políticas y normas de seguridad

Tabla 10.1.1 - Aplicación de la norma ISO/IEC 27002:2013 a las actividades sugeridas por COBIT

ANEXO K: Políticas de seguridad de Información

11.1 Estructura

De acuerdo a la investigación bibliográfica, se elabora la siguiente estructura o esquema de los elementos que debe contener las políticas planteadas. Se recomienda su aplicación dentro de la organización y adicionalmente realizar un control de versiones sobre las políticas definidas.

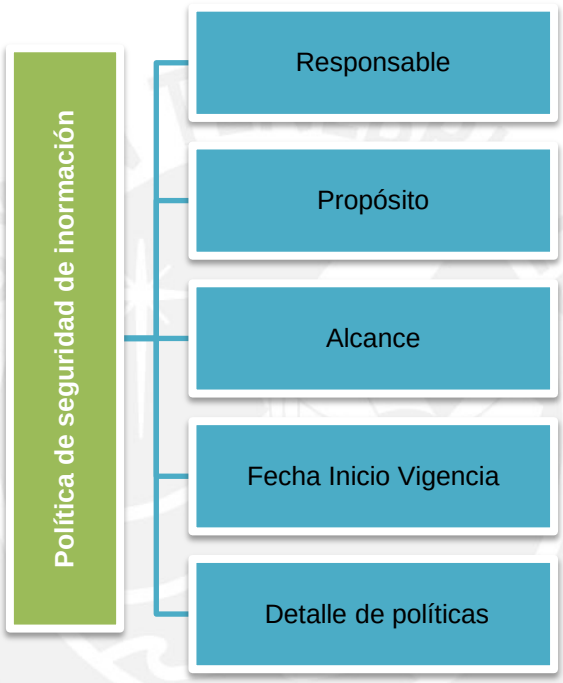


Figura 11.1.1 - Estructura para las políticas de la organización

11.2 Políticas de seguridad de información

Según el mapeo con la norma para identificar aspectos que debe tomar en cuenta las políticas de seguridad de información, se procede a la redacción de acuerdo a la estructura propuesta.

Política de seguridad de información

Responsable: Oficial de seguridad de información

Propósito

Encaminar y dirigir la seguridad de información de acuerdo al enfoque de gobierno de TI y que estas estén alineadas a los requerimientos de negocio y a la ley de protección de datos personales, norma técnica peruana de la historia clínica y la ley de emergencia.

Alcance: Proceso de admisión, atención, egreso e identificación de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Establecer las políticas de seguridad de información

La alta dirección proporcionan actividades de acuerdo a la ejecución de sus procesos y dentro de ellas como se gestionan la tecnologías de información, por lo cual se comprometen a preservar la confidencialidad, integridad y disponibilidad de los activos físicos y electrónico a través de las gerencias de la organización.

De acuerdo a las actividades realizadas para cada proceso, se identifican la información y requerimientos de seguridad, los cuales deben formar parte de un proceso continuo de gestión y estar alineados a los objetivos estratégicos de la organización para reducir riesgos de información al nivel de tolerancia escogido por la organización.

De acuerdo a los procesos y la declaración de aplicación de los dominios de seguridad de información para la empresa según la norma ISO/IEC 27001:2013, se obtienen los objetivos de control que comprenden las políticas de seguridad de información soportadas por los procesos base del proyecto gobierno de TI.

2. Revisar las políticas de seguridad de información

El responsable de velar por las políticas de la seguridad de información es el oficial de seguridad. Debe verificar la vigencia de éstas respecto a los aspectos de negocio y

los procesos que quiera cubrir y en base a los requerimientos de seguridad de información que propone los stakeholders y que aquellos que son producto de la adecuación a una regulación o requerimiento externo. Todo el personal de la organización está obligado a cumplir con estas políticas de acuerdo a sus roles y responsabilidades dentro de los procesos de negocio y según su función.

Se debe por lo tanto diseñar un sistema y ejecutar procedimientos de revisión de las políticas, el cumplimiento y las brechas que indican el estado actual y el estado ideal al que se quiere llegar a partir de la implantación de éstas políticas.

Sobre la organización de seguridad de información

Responsable: Oficial de seguridad de información, comité estratégico

Propósito

Establecer los roles y responsabilidades para la gestión y difusión de la seguridad de información en la organización y garantizar el alineamiento con las estrategias y objetivos de negocio.

Alcance: Proceso de admisión, atención, egreso e identificación de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Organización Interna

Dentro de la organización interna, se debe proponer y respetar una estructura alineada a los requerimientos de seguridad de información de la empresa y que permita su gestión, lo cual incluye incorporación de nuevos roles dentro de la estructura organizacional.

Para soportar un gobierno de TI e iniciativas de seguridad de información e incluso proyectos de Sistema de Gestión de seguridad de Información se propone incorporar:

- Comité estratégico de Seguridad de información

Entre sus funciones principales se tiene:

a. Revisar y proponer a la máxima autoridad de la empresa para aprobar políticas y funciones de seguridad de información.
b. Supervisar investigación y monitoreo de incidentes relativos a la seguridad de información.
c. Aprobar iniciativas para incrementar niveles de seguridad de información de acuerdo a competencias y responsabilidades asignadas a cada área.
d. Evaluar y coordinar la implementación de controles de seguridad de información para sistemas o servicios.
e. Promover difusión y apoyo de actividades relacionadas con la seguridad de información y las capacitaciones.
f. Revisar anualmente las políticas, de manera de asegurar su actualización.

- Oficial de seguridad de información

  El oficial dentro de sus funciones tiene la supervisión de todos los aspectos inherentes a la seguridad dentro de la organización, incluyendo el gobierno de TI, y velar por las siguientes políticas:

a. Política de seguridad de información
b. Política de estructura organizacional interna
c. Política de recursos humanos
d. Política de gestión de activos
e. Política de control de accesos
f. Política de seguridad física y ambiental
g. Política de operaciones y comunicaciones
h. Política de gestión de proveedores
i. Política de gestión de incidentes de seguridad de información
j. Política de continuidad de negocio
k. Política de cumplimiento

2. Roles y responsabilidades de seguridad de información

De acuerdo a los requerimientos de seguridad de información y capacidades y exigencias dentro de los procesos de negocio se proponen los roles y las nuevas responsabilidades de acuerdo a la seguridad de información según sea el caso. Se pretende garantizar:

- Confidencialidad de información: Verificar que la información puede ser accedida solo por personas autorizadas. Proteger datos críticos de la organización.
- Integridad de Información: Verificar que los datos almacenados sean íntegros y que no exista una pérdida que genere vacíos dentro de un histórico de datos de la empresa.
- Disponibilidad de información: Garantizar que todo tipo de información crítica se encuentre disponible o que pueda ser recuperada dentro de períodos de tiempo adecuados para minimizar el impacto en el negocio.

De acuerdo a esos tres requerimientos, se definen nuevas responsabilidades para que dentro de los procesos de negocio se vele por el cumplimiento de los tres pilares de la seguridad de información.

3. Segregación de funciones

El oficial de seguridad de información en conjunto con el comité estratégico y jefe de recursos humanos deben proponer una estructura de roles de acuerdo a los procesos de negocio sobre el cual aplican las políticas de manera que garantice:

- Evitar redundancia de las actividades dentro de los procesos, es decir que dos personas no ejerzan un mismo rol
- Los roles y requerimientos de seguridad son ejercidos por distintas personas de acuerdo a sus capacidades, funciones y competencias, así como sus permisos y accesos en los sistemas y a la documentación física.

4. Seguridad de información en la gestión de proyectos

El oficial de seguridad bajo la aprobación del comité estratégico, identifica los requisitos de seguridad de información a aplicar en la gestión de proyectos de la empresa asegurando:

- Objetivos de seguridad de información incluidos en los objetivos del proyecto y que éstos últimos estén alineados a los objetivos y estrategias de la organización.
- La seguridad de información es parte de todas las fases de la metodología del proyecto solicitado.

- Gestión de riesgos de seguridad de información dentro del ciclo de vida del proyecto.

Se debe definir y asignar responsabilidades de seguridad de información a los roles específicos de acuerdo a la gestión o marcos de proyecto que adopta la organización.

Sobre la seguridad en recursos humanos

Responsable: Jefe de recursos humanos

Propósito

Establecer mecanismos de seguridad en la gestión de personal antes, durante y al término de su contrato garantizando la preservación de la información y brindándoles responsabilidades y roles de acuerdo a sus funciones y capacidades

Alcance: Proceso de admisión, atención, egreso e identificación de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Antes del empleo

Se define, bajo coordinación con el jefe de proyecto de recursos humanos, los requisitos de seguridad de información dentro de los procesos de contratación de empleo, los cuales deberán ser implementados y verificados periódicamente.
Al publicar una oferta laboral y tener una lista de candidatos y postulantes a una vacante se debe garantizar lo siguiente:

- Identidad correcta del postulante y documentos vigentes.
- El postulante cuenta con recomendaciones o referencias que garanticen sus habilidades y desempeño profesional.
- El postulante no tiene antecedentes policiales y judiciales que puedan afectar el desarrollo de sus funciones.
- El postulante cuenta con los estudios adecuados para poder acceder a las entrevistas de acuerdo a la función y rol que desee ocupar.

Al momento de realizar la contratación, se debe verificar y firmar los términos de contrato de acuerdo a los requerimientos de seguridad de información definidos. Se toma en cuenta lo siguiente:

- En caso el trabajador tengo acceso a información y datos sensibles, se firmará un acuerdo de confidencialidad y no divulgación.
- Definir las responsabilidades del trabajador y alinearlas a la ley de protección de datos personales
- En caso gestione directamente activos o información confidencial, entrega los procedimientos y políticas a seguir.
- Asegurar que nuevo trabajador tenga conocimiento en el código de ética y seguridad de información.

2. Durante el empleo

El oficial de seguridad de información y el jefe de recursos humanos verifican el desenvolvimiento del personal y el logro de sus objetivos y desempeño sobre sus responsabilidades asignadas a nivel de proceso y a nivel de los requerimientos de seguridad de información.

Se realizan también las actualizaciones de responsabilidades de acuerdo al desempeño y los cambios organizacionales dentro de los procesos, cumpliendo los requerimientos de seguridad de información y los lineamientos del contrato firmado con el trabajador.

En caso no exista un cumplimiento, se toman acciones correctivas como las que se señala a continuación:

- Concientización sobre cumplimiento de funciones y seguridad de información.
- Actuar de acuerdo a lo estipulado en el contrato, términos y condiciones y las políticas y requerimientos de seguridad de información.

Como parte de la gestión al personal se educa y concientiza sobre las iniciativas de seguridad de información a aplicar dentro de los procesos. Para esto se debe contar con lo siguiente:

- Programas y planes de capacitación sobre seguridad de información y desempeño de capacidades actualizado y validado.
- Actividades desarrolladas de acuerdo a las normas y requerimientos externos que puedan afectar la seguridad de información.

3. Término del empleo o cambios de responsabilidades

En el caso de despidos o contratos concluidos se considera lo siguiente:

- Comunicar al personal del área el fin de contrato o despido de la persona y las responsabilidades y funciones que cumplía. Se redistribuyen responsabilidades.
- De acuerdo a los acuerdos de confidencialidad, garantizar que los recursos humanos respeten el tiempo establecido en el cual no puede divulgar información y que respeten los demás términos y condiciones relacionados con seguridad de información.
- Se identifica los activos y fuentes de información que pertenecían a la labor realizada por el trabajador y de acuerdo a las políticas, se realiza el proceso de reasignación, eliminación o protección del activo.
- Se informa los cambios de personal.

Si se realiza un cambio de responsabilidades del personal, se debe de verificar los acuerdos y condiciones del contrato, para alinearlos a las nuevas tareas que debe de cumplir. Se concientiza al personal sobre los cambios y se informa a las autoridades respectivas para los cambios y mantener el esquema de segregación de funciones y sus mecanismos de cambio.

Sobre la gestión de activos

Responsable: Administrador de plataformas de TI, Gestor de seguridad de información

Propósito

Establecer mecanismos y políticas que garanticen los niveles de seguridad en los activos de acuerdo al tipo de información que contienen o gestionan.

Alcance: Proceso de admisión, atención, egreso e identificación de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Responsabilidad de activos

Respecto al inventario de activos de la organización, se establece clasificación de activos que componen los sistemas que soportan los procesos y se priorizan de acuerdo el nivel de criticidad. Se establecen procedimientos para registrar y consultar un activo de acuerdo a parámetros de información.

Clasificación de activos o información gestionada en los activos:

- Información Confidencial
- Información Reservada o Información interna

Los colaboradores de la organización pueden sugerir la clasificación de algún nuevo activo o información, lo cual deberá ser evaluado según los criterios establecidos.

Se recomienda la identificación de los activos de información dentro de la empresa que soporten los procesos, así no gestionen información clasificada, y garantizar que estos sean empleados por los usuarios finales de forma correcta. Monitorear además la vida útil de estos activos.

2. Clasificación de la información

La información puede ser clasificada bajo ciertos criterios de acuerdo a los parámetros de seguridad de información. Estos son:

- Confidencialidad:
  Información que al ser divulgada puede impactar gravemente la economía y deteriorar la imagen pública y el derecho de privacidad de las personas incumpliendo la ley de protección de datos personales, ley de emergencia, norma técnica peruana de la historia clínica. La divulgación de esta información solo se permite a través de una autorización formal por parte de la directiva

Tratamiento de información Interna

Información necesaria para desempeñar las funciones de negocio. Su divulgación puede afectar económicamente a la empresa pero sin mayor impacto ni afectar su imagen frente al público. Esta información será accesible para el personal interno o aquellos que interactúen con la organización y sus procesos.

Tratamiento de información restringida

Información de uso interno exclusiva de grupos o áreas específicas. No debe divulgarse libremente en la organización. Solo tendrán acceso a ella personal que requiera estos datos para sus actividades laborales.

Tratamiento específico de información confidencial:

- Datos personales: Estos datos, de pacientes, personal y stakeholders, deben ser tratados bajo procedimientos establecidos de acuerdo a la ley de protección de datos personales y garantizar su trato confidencial.
- Datos secretos: Datos que permiten acceso y operaciones en sistemas que son secretos y de uso exclusivo de un único usuario, por ello el personal tiene la obligación de no divulgarlos ni solicitar ajenos. De manera excepcional, el personal de soporte tendrá acceso para restablecer claves o desbloquear cuentas y para que posteriormente el usuario las cambie.
- Archivos temporales: Aquellos archivos que contengan datos personales de acuerdo a lo establecido por los procedimientos, deberán ser eliminados finalizado el tratamiento de los mismos.
- Destrucción: Se debe eliminar información de acuerdo a procedimientos y cuando esta se encuentre en desuso.

- Integridad

  De acuerdo a los requerimientos de seguridad de información, se evalúa los riesgos de preservar información no integra y su impacto monetario, legal y a nivel de reputación. Se debe de identificar cuáles de éstos datos genera un impacto mayor y se debe de priorizar y probar su integridad bajo diversos escenarios como cambios a través de sistema o procesos físicos de almacenamiento de acuerdo a su sensibilidad y el nivel de exposición.

- Disponibilidad

  La información crítica que ha sido identificada por las áreas de negocio como críticas, debe estar siempre disponible y para esto se empleará estrategias de

contingencia correspondiente. Estas deben de estar documentadas y asegurar correctas políticas de respaldo de acuerdo a procedimientos y estableciendo responsabilidades claras y niveles de acceso a estos backups.

3. Gestión de medios

Dentro de la organización se tiene dispositivos de almacenamiento y transferencia de datos empleados en los procesos de negocio por ello se deben tener las siguientes consideraciones sobre medios extraíbles para preservar la seguridad de datos:

- Las unidades de medios extraíbles deben de habilitarse bajo alguna razón o exigencia dentro de los procesos de negocio.
- En caso la información almacenada en medios extraíbles no sea ya necesaria, deben retirarse o eliminarse estos medios y la información debe ser irrecuperable.
- Los medios extraíbles comunicación y transferencia deben ser almacenados en un ambiente seguro.
- Se debe realizar un inventario de los medios extraíbles para limitar la posibilidad de la pérdida de datos.
- Se debe controlar y monitorear el uso de medios extraíbles, así como documentar los procedimientos y niveles de autorización.

Respecto a los medios de transferencia de datos se señala lo siguiente:

- Preservar una lista de correos autorizados para el intercambio de información.
- Verificar la identificación de los correos de acuerdo a procedimientos establecidos.
- Identificar y mantener los registros que señalen el contenido de los medios de comunicación y el nivel de protección aplicada, así como los tiempos de transferencia y recepción.
- En caso de transporte fuera de la sede de algún medio físico como discos de backup, deberá garantizarse un embalaje seguro para evitar algún daño sobre este dispositivo que pueda afectar la información contenida en él.

Sobre el control de accesos

Responsable: Jefe de operaciones de TI, Gestor de seguridad de información

Propósito

Velar por la seguridad de información por medio de mecanismos y políticas de accesos a los sistemas y a la información clasificada que gestionan los procesos de negocio.

Alcance: Proceso de admisión, atención, egreso e identificación de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Requisitos de negocio de control de accesos

Se define los requisitos de control de acceso de acuerdo a los requerimientos del negocio de acuerdo al mapa de procesos y actividad que realiza la empresa. Estos se basan en principios de seguridad de acuerdo a la función que realizan los usuarios

La política de control de accesos específica:

- Definir accesos a sistemas de información, recursos, servicios y redes de comunicaciones de acuerdo a la naturaleza del usuario y los roles existentes dentro de la organización
- Controlar los accesos de acuerdo a los perfiles y privilegios existentes en los sistemas.
- Identificación de niveles de acceso para cada área y procesos dentro de la hospitalización de usuarios, en especial en el procesamiento de datos de los pacientes.
- Los responsables de la asignación y autorización de acceso comunicarán las políticas y monitorearan el cumplimiento de estos.

Otras consideraciones:

- Segregación de funciones en los sistemas, procesos de negocio y la administración de la seguridad de los mismos.
- Legislaciones aplicables a la realidad de la empresa.
- Niveles y criterios de acceso de acuerdo a la seguridad de información y el acceso a los datos.
- La empresa junto con el oficial de seguridad y comité de riesgos están en obligación a controlar los riesgos de acuerdo a los permisos otorgados a los usuarios.

Así mismo, se debe de controlar en particular los accesos a los servicios de red por parte de personal interno y externo asegurando:

- Control de tráfico en la trasferencia de datos y las conexiones a la red de la empresa.
- Identificación de dispositivos de acceso a la red, es decir si son internos o externos. En este último caso, determinar que sea un acceso autorizado previo acuerdo con las partes responsables.

2. Gestión de acceso del usuario

De acuerdo a la gestión de accesos de los usuarios se toma en cuenta los requerimientos y niveles de seguridad definidos para los sistemas que comprenden los procesos de negocio. Por lo tanto se debe garantizar que cada usuario sea único, individual, independiente, persistente frente a los cambios

Respecto a registro y eliminación de usuarios se deben tener las siguientes consideraciones:

- Establecer los procedimientos de registros que comprueben la identidad del usuario, asignar el ID y mantener la asociación.
- Los mecanismos de verificación de identidad debe ser de acuerdo a cada tipo de usuario y el acceso que tiene a la información.
- Comunicar requerimiento de baja o eliminación de un usuario al departamento de recursos humanos para gestionar con el personal de seguridad de información la eliminación de usuarios.

- En caso la eliminación de usuario genere situaciones conflictivas se debe de comunicar al propietario.
- En caso de los contratos temporales, la eliminación de registros de usuario debe coincidir con el tiempo de contrato para programar su expiración de autenticación.
- Antes de eliminar un usuario, se debe de verificar la existencia de un administrador general del sistema que pueda proveer permisos y gestionar los cambios.

Respecto a los accesos a los usuarios se toma en cuenta lo siguiente:

- Los permisos deben ser de acuerdo a las funciones que realiza dentro de su actividad laboral y a los requerimientos de consulta de información:

  - Para acceso interno:
    Mecanismos básicos de autenticación empleando una contraseña de uso personal. Estos pueden ser de mayor seguridad si se requiere acceso a aplicaciones que contengan información crítica que pueda generar alto riesgo económico.
  - Para acceso externo:
    En el caso de acceso a datos personales se empleará un mecanismo de seguridad elevado en caso se requiera consultar aplicaciones críticas. Se hace hincapié en la política de la no divulgación de contraseñas incluso en el caso de proveedores y servicios a tercero que requieran acceso.

Respecto a la gestión de derechos de acceso privilegiados se debe garantizar:

- La asignación de derechos de acceso privilegiados deben ser controlada por medio de un proceso formal alineado a la política a la gestión de accesos.
- Se debe mantener un proceso de autorización y registro de privilegios asignados. Los derechos de acceso no deben concederse sin haber terminado la fase de autorización.
- Definir el tiempo de expiración del acceso privilegiado.
- Los usuarios administradores deben preservar la confidencialidad de los datos a los que acceden por medio de mecanismos adecuados y alineados a las políticas de acceso.

Sobre la gestión de información secreta de autentificación:

- Para la generación de credenciales de acceso se debe garantizar la confidencialidad y evitar que sean predecibles por otros.
- En caso el usuario sea quien elija la clave, garantizar que cumpla con requerimientos y mecanismos de seguridad elevados para que pueda ser generada.
- Para reactivar contraseñas se debe considerar las medidas de seguridad pertinentes. Solo en caso de bloqueos temporales, las contraseñas se reactivaran automáticamente.
- Los cambios de contraseña deben realizarse periódicamente. Solo en caso de olvido de clave o bloqueo, los administradores generan una nueva contraseña y el usuario la modifica al primer ingreso.
- Las contraseñas podrán ser bloqueadas al ser solicitado por el usuario o por exigencia del administrador al detectar alguna irregularidad o filtración de datos.

Respecto a la revisión, eliminación o cambios de los derechos de acceso se debe garantizar:

- Revisión periódica de los derechos de acceso y después de cambios como promoción o despido.
- Los derechos deben ser revisados y asignados nuevamente cuando se pasa de un rol a otro dentro de la misma organización.
- Revisión de los métodos de asignación de privilegios para asegurar que no se hayan obtenido privilegios no autorizados.
- Los accesos son eliminados por medio de una autorización solicitada por el usuario o de acuerdo a un cambio, promoción de puesto o según las políticas de despido de la organización.

3. Responsabilidades de usuario

Los usuarios son los responsables de las actividades y operaciones realizadas bajo su identificador en los sistemas, por lo cual se deben emplear de forma adecuada y custodiar el uso de contraseñas, claves u otro tipo de credenciales personales para su autenticación.

Por lo tanto, se debe tomar en cuenta las siguientes consideraciones para el uso de contraseñas:

- Escoger contraseñas debidamente seguras y no predecibles para que terceros no puedan suplantarlos fácilmente.
- No escribir contraseñas en caso los sistemas lo soliciten de forma repetitiva, reportar este incidente. Solo en caso esta solicitud de contraseña forme parte del proceso, ingresarla.
- No emplear mecanismos de recuerdo de contraseña ofrecidos por sistemas o aplicaciones comerciales.
- Cambiar contraseñas periódicamente con frecuencia que determine la organización para distintos sistemas o aplicaciones que lo soliciten.
- En caso el usuario de acceso esté bloqueado, deberá utilizar mecanismos de desbloqueo o reseteo.

4. Sistema y aplicación de control de acceso

Dentro del sistema y aplicación de control de acceso se debe, según los requerimientos de seguridad de información previamente identificados, restringir el acceso de la información de acuerdo a los siguientes puntos:

- Acceso de los sistemas de información
    - Se controlará el acceso mediante mecanismos que garanticen que los usuarios no acceden con privilegios no autorizados.
    - Un sistema de información también requiere comunicarse con otros sistemas por ello debe monitorearse que este requerimiento técnico salvaguarde la información.

- Perfiles de acceso
    - Los perfiles de acceso a sistemas y a documentación deben estar alineados a los procesos de negocio y que permitan la adecuada segregación de funciones.
    - Cada usuario pertenecerá a uno o varios perfiles, por lo cual sus privilegios serán los mínimos resultantes de los diferentes permisos que pueda tener.

- Tiempo de expiración de una conexión

  Los sistemas borrarán la información en la pantalla y suspenderán la sesión que tenga un tiempo de inactividad. Este tiempo debe estar sujeto a lo establecido por el responsable de la seguridad de información y manejar también las excepciones del caso.

Por otro lado, para el sistema de gestión de contraseñas se debe tomar en cuenta lo siguiente:

- Permitir a los usuarios seleccionar y cambiar sus contraseñas e incluir un procedimiento de confirmación para manejar errores de entrada
- Cumplir los parámetros de calidad de una contraseña de acuerdo a las políticas.: Longitud de contraseña mayor o igual a diez (10) caracteres, los cuales deben incluir números, letras y símbolos especiales.
- No mostrar contraseñas en pantalla al ingreso al sistema
- Guardar contraseñas en archivos distintos a los de las aplicaciones
- Almacenar y trasmitir contraseñas de forma protegida

No obstante se presenta algunas **políticas de contraseñas**:

- Composición

  La longitud de la contraseña debe ser mayor o igual a diez (10) caracteres, la cual debe incluir números, letras y símbolos especiales.

  Verificar reglas de sintaxis básicas que impidan que las contraseñas coincidan con el identificador de usuario

- Cambio de contraseña

  El sistema, en caso sea técnicamente posible, se verifica que la nueva contraseña sea diferente a contraseñas utilizadas anteriormente. El número de búsqueda de coincidencias debe ser definido por el área responsable.

- El usuario tiene la posibilidad del cambio de contraseñas en cualquier momento.

Sobre la seguridad física y ambiental

Responsable: Administrador de plataformas de TI, Gestor de seguridad de información

Propósito

Brindar dirección y garantizar ambientes seguros para los recursos humanos y para los equipos o activos de información de acuerdo a los requerimientos legales.

Alcance: Proceso de admisión, atención, egreso e identificación de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Áreas seguras

Dentro del entorno en el cual se desarrollan las actividades del proceso de negocio y de acuerdo a la ubicación de las estaciones o puestos de los usuarios que la ejecutan se debe tener en cuenta lo siguiente:

- Instalaciones y puestos de trabajo situados estratégicamente.
- Las instalaciones deben estar configuradas para evitar que información confidencial pueda ser visible desde el exterior.

Respecto a cómo el personal se desenvuelve dentro de las instalaciones seguras:

- Asegurar que el personal sea consciente de las medidas de seguridad a adoptar dentro de los procesos de negocio y las actividades para su cumplimiento.

- Registrar elementos o medios extraíbles que se ingresan al local, y que podrían afectar el desarrollo del proceso, por esta razón se debe monitorear y en caso de alto riesgo no permitir el ingreso de estos dispositivos.

2. Equipos

Se procede a detallar las políticas y consideraciones de seguridad de información sobre los equipos que forman parte de los activos de los procesos de negocio tomados como referencia. Entre algunas consideraciones, se señala inicialmente como deben protegerse y ubicarse los activos:

- Los equipos deben ubicarse estratégicamente de forma que se minimice el acceso innecesario a las áreas de soporte y/o procesamiento.
- Las instalaciones en las cuales se guarden datos de almacenamiento o se encuentren los activos del proceso deben contar con mecanismos de seguridad para evitar accesos no autorizados.
- Las instalaciones y equipos de procesamiento de datos sensibles deben ser ubicadas estratégicamente para reducir los riesgos de información y cumplir con la ley de protección de datos personales.
- Los mecanismos adoptados para protección de equipos deben estar alineados a la necesidad de reducir riesgos e incidentes que puedan suscitarse en el entorno.
- Establecer las condiciones ambientales bajo las cuales deben preservarse los activos. Monitorear dichas condiciones y reportar en caso no se cumpla alguno de estos parámetros definidos

De acuerdo al mantenimiento de los equipos, se debe garantizar:

- Brindar mantenimiento continuo a los activos para asegurar la continuidad de su disponibilidad e implementación.
- Únicamente el personal de mantenimiento está autorizado para llevar a cabo las reparaciones de equipos para restablecer los servicios.
- Aplicar los controles adecuados antes de realizar el mantenimiento al equipo. Estos controles pueden variar de acuerdo a que personal realiza la actividad de mantenimiento, en qué lugar se realizará y si está de por medio información crítica.
- Luego del mantenimiento, inspeccionar para asegurar que el equipo no ha sido manipulado fuera de los parámetros señalados y que no presenta averías.

De acuerdo a la eliminación, eliminación segura o reutilización de activos se tiene las siguientes consideraciones:

- Identificar quienes son los responsables y tienen autoridad para permitir el retiro o eliminación de un archivo fuera de las instalaciones.
- Establecer y verificar los plazos del retiro de activo. Estos plazos podrían ser modificados de acuerdo a los resultados de las evaluaciones periódicas.
- Verificar, de acuerdo a la información gestionada, si un equipo debe ser eliminado en forma segura o si se puede volver a utilizar bajo ciertas medidas y criterios de seguridad.
- En el caso de los equipos dañados y que no puedan repararse para volver a utilizados, se realiza el procedimiento de eliminación segura el cual consiste primero en destruir la información contenida en dicho archivo bajo ciertas medidas que garanticen que esta información es irrecuperable. Posteriormente se procede a eliminar el activo dañado y su retiro de la organización.

De acuerdo a la limpieza de escritorios y políticas de pantalla transparente, la cual es empleada para brindar un trato especial a la información almacenada dentro de los equipos, se señala lo siguiente:

- En caso se tenga información crítica almacenada, esta debe ser bloqueada para que no todos los usuarios puedan acceder a ella y difundirla.
- Las computadoras y terminales deben tener implementados mecanismos protectores de pantalla en caso cumpla un tiempo de inactividad prudente. Para volver a la pantalla en la cual se encuentran desarrollando sus actividades, se exige el ingreso de la contraseña para su autenticación.

Sobre la seguridad de operaciones

Responsable: Jefe de operaciones de TI, Administrador de plataformas de TI

Propósito

Brindar mecanismos que garanticen la seguridad de información dentro de las operaciones del día a día para evitar algún incidente que afecte a la continuidad o disponibilidad de los datos.

Alcance: Proceso de admisión, atención, egreso e identificación de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Procedimientos y responsabilidades operacionales

De acuerdo a los requerimientos organizacionales, se determina que debe de existir procedimientos documentados para cubrir las operaciones del día a día, ya que estos son la fuente de captura y difusión del conocimiento. Por ello se menciona lo siguiente:

- Mantenimiento y elaboración de documentos que detallen los pasos para realizar actividades diarias como:
- Instalar y configurar sistemas
- Procesar información clasificada dentro de los sistemas
- Documentar los procesos de recuperación y almacenamiento de datos para poder realizarlos ante cualquier eventualidad suscitada.

Según la gestión de cambios, se debe realizar un seguimiento a todo tipo de cambios que han sido aprobados, rechazados y que se encuentren pendiente. Estos cambios son realizados a nivel de red, sistemas y organizacionales. Dentro del procedimiento de cambios se incluyen los siguientes aspectos:

- Identificar y registrar cambios significativos dentro de toda la arquitectura empresarial y la arquitectura de TI.
- Planificar y probar todo tipo de cambios que a realizarse, así como validarlo en posterior con los usuarios de negocio.
- Autorización formal de los cambios propuestos, señalar quien o quienes fueron los responsables de conceder dicha autorización.
- El área de seguridad de información participa en el proceso de cambios y verifica si se producen o no riesgos de información.

2. Protección contra malware

Se debe garantizar que todo dispositivo de usuario final esté libre de virus. Con estos fines, se debe de establecer una serie de controles para evitar contaminación y materialización de impacto negativo. Se presenta a continuación las acciones a tomar:

Protección de puestos de trabajo: Todos los dispositivos de usuario final con riesgo de propagar o verse afectados por virus, deben contar con un antivirus instalado y actualizado. Se toma medidas para minimizar el impacto de existencia de virus, así como el desarrollo de procedimientos de instalación, actualización, configuración y monitoreo.

Protección en equipos portátiles: Se desarrollan los procedimientos de instalación, actualización, configuración y monitoreo de la actividad del antivirus, tomando en cuenta las características de dichos equipos.

Protección de servidores: Todo servidor susceptible a contaminación de virus por red, debe tener un antivirus instalado y actualizado. Se desarrollan los procedimientos de instalación, actualización, configuración, y monitoreo para evitar el impacto en los sistemas de información.

Protección de correo electrónico: El correo electrónico debe comunicarse con un sistema de antivirus capaz de analizar la bandeja de entrada. En caso se detecte virus en un archivo adjunto del mensaje de correo, se debe enviar una notificación al receptor indicando que el archivo fue eliminado. Se desarrollan los procedimientos de instalación, actualización, configuración y monitoreo.

Protección de la navegación web: El acceso a internet debe ser controlado por medio de un antivirus que restrinjan el acceso a sitios web maliciosos que acceden a descarga de malware.

Distribución de medios de almacenamiento y contenidos por intranet/internet: Se comprobará que estos medios están libres de virus al analizarlos con la última versión del antivirus instalado. Se comprobará que todo contenido susceptible de virus se encuentra libre de este al ser publicado en intranet o internet de acuerdo al análisis con el antivirus en su última versión.

Sobre el antivirus, se debe tener en cuenta las siguientes consideraciones:

- Instalación y configuración: Se debe establecer los responsables de la instalación, configuración y mantenimiento de los antivirus. Mantener un inventario de las licencias adquiridas, de ser el caso, para determinar la protección.
- Se debe establecer procedimientos de acción sobre incidentes al localizar la infección de virus. Estos deberán tomar en cuenta la protección de la información y procesos de restablecimiento de operatividad de los sistemas afectados.

Estos incidentes de virus pueden catalogarse por su gravedad de acuerdo a lo siguiente:

- Velocidad de propagación de la infección: En caso sea grave, el número de sistemas afectados representa un porcentaje significativo del total de estaciones, servidores o dispositivos para llevar a cabo los procesos de negocio.
- Impacto en los sistemas: Se considera grave si releva los datos confidenciales, si se eliminan gran cantidad de archivos, si se modifica el contenido del archivo o se verifica datos del disco duro eliminados.
- Impacto en la red de comunicación: Se considera grave si el virus provoca disminución del rendimiento de las comunicaciones.
- Impacto en el negocio: Se considera grave si alguna actividad o proceso de negocio se ve afectado por el incidente.

3. Backup

La información de la organización es uno de los activos más importantes de la organización, además debe estar alineada a la ley de protección de datos personales. En caso se dañe o pierda una parte de la información, se ve afectada la continuidad y la seguridad de información pues afecta al pilar de la disponibilidad.

Por esta razón, dentro de la organización, para reducir el riesgo de inoperatividad, se realiza copias de respaldo para que la información pueda ser recuperada en caso pérdida. Se considera por lo tanto lo siguiente:

- El backup de los sistemas deberá estar alineado a las estrategias y planes de continuidad de negocio definidos. En caso incidentes pequeños, no se necesitará la activación del plan.
- Las cintas de backup deben de gestionarse y ser protegidas tomando en cuenta el entorno de almacenamiento para evitar que éstos tengan daños físicos.
- Los incidentes que requieran recuperación de datos se archivarán en el registro de incidencias bajo el siguiente formato: nombre del sistema afectado, fecha del incidente, fecha y hora de recuperación, medios o archivos usados para la recuperación y la fecha y hora en la que fue realizada la copia.
- El alcance de la recuperación de datos efectuada debe ser informado a las áreas de negocio y partes interesadas. En el caso de los usuarios afectados, ellos deberán evaluar el impacto operacional y a nivel de proceso al momento del incidente y verificar el restablecimiento total del incidente.

4. Registro de eventos

Se deben registrar los eventos y los datos significativos para identificar el origen del evento, la fecha y hora en la cual se ha generado, los datos asociados al evento. No deben almacenarse datos secretos.

Sobre el registro de eventos:

- Deben ser registrados en un sistema o lugar especial habilitado por el sistema.
- Deben ser almacenados en repositorios centrales para que esta información y evento sea monitoreado para determinar posibles incidentes o fallas.
- Los eventos deben ser almacenados de acuerdo a lo establecido a la ley vigente de acuerdo a la información crítica asociada a estos.
- En el caso de datos confidenciales en los eventos, se debe almacenar y proteger estos registros de forma segura de igual manera como se protegen los sistemas en los que fueron generados.
- El acceso a los eventos estarán limitados solo para personas especializas y cuya función y rol sea el análisis de estos empleando mecanismos de control que eviten la divulgación.

5. Control de software operativo:

Dentro de los procesos de negocio se identifica sistemas o software que se emplean como parte de sus actividades. Por ello se debe de tener en cuenta algunas consideraciones para alinearlas a las estrategias de seguridad de información:

- Los sistemas y software antes de ser actualizados, deben ser sometidos al control de cambios para autorizar si estos puedan ser aplicados o no.
- Las aplicaciones y sistemas o software operacionales solo serán implementados si se realizan pruebas excesivas sobre él y que todas estas hayan resultado satisfactorias. Se debe verificar que todos sus componentes están actualizados.
- Se debe tener una estrategia de rollback antes de que los cambios sean implementados para que ante cualquier eventualidad se pueda regresar a un estado anterior.
- Se debe conservar las versiones anteriores al sistema como medida de contingencia en caso la nueva aplicación falle.
- Se debe guardar un log de auditoría con todas las actualizaciones operacionales, nuevas instalaciones y nuevas librerías.

6. Gestión de Vulnerabilidades técnica:

La organización debe definir cuáles son las aplicaciones seguras y que tipos de usuarios pueden tener privilegios para la instalación de software, teniendo en cuenta los roles y funciones.

Se debe realizar una lista de software seguro como las actualizaciones y parches de seguridad en algún software existente y también la lista de software potencialmente dañino o empleados para fines personales fuera de las actividades realizadas en la organización.

De no controlar la instalación en plataformas informáticas, se pueden introducir nuevas vulnerabilidades y luego una fuga de información o pérdida de integridad de datos, ente otros incidentes.

7. Consideraciones de auditoría de sistemas de información:

Se debe tomar en cuenta algunas consideraciones para auditorías posteriores de sistemas de información, entre ellas:

- Se debe gestionar adecuadamente los requisitos de auditoría y acceso a los sistemas.
- El alcance de las pruebas técnicas de auditoría debe ser acordada y controlada para que estas no afecten a la información y al proceso de negocio, por ello se debe trabajar con copias aisladas en caso requiera operar datos reales.
- Las pruebas de auditoría que podrían afectar la disponibilidad del sistema deberán ser ejecutadas fuera del horario.

Sobre la seguridad de comunicaciones

Responsable: Oficial de seguridad de información, Gestor de seguridad de información

Propósito

Garantizar que la transferencia de datos a través de la red tenga implementado los mecanismos de seguridad de información para garantizar el cumplimiento de la protección de datos de acuerdo a su clasificación.

Alcance: Proceso de admisión, atención y egreso de pacientes.

Fecha Inicio Vigencia: Enero 2014

---

1. Transferencia de la información

Para transferir información, de acuerdo a la ley de protección de datos personales se debe tener ciertas salvedades, por ello se consideran los siguientes elementos para efectuar esta operación:

- Procedimientos de protección de la información ante intercepción, copia, modificación, mal enrutamiento y destrucción.

- Procedimientos para proteger la información electrónica sensible, incluyendo la protección contra malware que pueda ser transmitida por comunicaciones electrónicas.
- Garantizar que el personal interno y externo no pongan en peligro la organización por medio de difamación o reenvío de mensajes encadena a través de la red de comunicaciones.
- Emplear recursos de cifrado para proteger la confidencialidad, integridad y autenticidad de la información.
- Controles y restricciones asociadas con el uso de los medios de comunicación, como el correo electrónico.
- Evitar que los mensajes que contienen información confidencial sean divulgados por contestadoras automáticas para evitar su reproducción por personal no autorizado.
- Asesorar al personal sobre los problemas en empleo de máquinas o servicios de comunicación relacionados a la seguridad de información y accesos no autorizados.
- Los servicios de transferencia de información deben cumplir todos los requerimientos legales sujetos a la realidad del negocio.

Respecto a los mensajes electrónicos, o intercambio de información a través de sistemas o correos se debe tener en cuenta las siguientes salvedades:

- Control de entradas y salidas de comunicaciones con registro de origen, destino y tipo de información intercambiada.
- Seguridad física o cifrado de datos que garantice la integridad del tránsito por medio de los sistemas. Aplicar estas técnicas de acuerdo a las exigencias de seguridad de las regulaciones como la ley de protección de datos personales.
- Asegurar la correcta dirección para transporte del mensaje y garantizar la disponibilidad de este servicio.

Por último se debe tomar en cuenta los aspectos relacionados a los acuerdos de no divulgación que han sido firmados:

- Definir la información que debe ser protegida de acuerdo a la criticidad de los datos y las regulaciones en torno a estos

- Establecer la duración del acuerdo de confidencialidad durante el contrato y al final de este. Se podría definir acuerdos de confidencialidad indefinidos de acuerdo al nivel de criticidad de la información
- Determinar las acciones requeridas cuando finalizan los acuerdos de confidencialidad.
- Verificar que se debe hacer con la información habiendo terminado los acuerdos de confidencialidad, en este caso al ser destruidos, se deben seguir los procedimientos en base a los requerimientos de seguridad de información.

Sobre las relaciones con los proveedores

Responsable: Gestor de servicio, Jefe de operaciones de TI

Propósito

Garantizar que se gestione las relaciones con los proveedores para asegurar el cumplimiento con los requerimientos de seguridad de información y lo establecido en los acuerdos de servicio firmados

Alcance: Proceso de admisión, atención, egreso de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Gestión de proveedores de servicios de entrega

De acuerdo a los procesos de negocio establecidos, se debe garantizar una gestión correcta y segura de los proveedores y los acuerdos para la entrega de servicio. Se toman en cuenta las siguientes consideraciones:

- Monitorear el nivel de performance del servicio entregado de acuerdo con sus acuerdos firmados. Por ejemplo determinar el tiempo de entrega de servicio y como este afecta las actividades del proceso de negocio.
- Revisar los reportes de servicio e identificar momentos para realizar auditorías sobre los acuerdos de servicio firmados. En este caso para evitar el sesgo, se recomienda auditorías externas.

- Brindar información de los incidentes de seguridad suscitados dentro de la entrega de los servicios frente a las exigencias de los acuerdos firmados y los procedimientos realizados por el proveedor para restablecer la operación normal
- Asegurar que los proveedores tengan capacidad suficiente para trabajar de acuerdo a planes diseñados que garanticen la continuidad de los servicios de acuerdo al nivel de incidente o desastre que haya afectado la entrega de estos.
- Se debe asignar un responsable para la gestión de proveedores o un equipo capacitado para el monitoreo de las consideraciones que fueron detalladas para cumplir requerimientos de seguridad de información y la calidad de los servicios entregados por medio de los procesos de negocio.

Respecto a los cambios en los acuerdos de servicio o cambios en los proveedores se debe considerar lo siguiente:

- Los cambios en los proveedores deberán ser revisados y las acciones correctivas que suplan el servicio deberán ser implementados por la organización, lo cual podría implicar el desarrollo de sistema, modificaciones en las políticas y procedimientos o cambios sobre los controles para mitigar incidentes de seguridad de información

En caso se cambien los acuerdos de servicio se debe verificar:

- Uso de nuevas tecnologías de acuerdo a las obligaciones contractuales y que beneficien el proceso de negocio.
- En caso la sub-contratación, se deberá monitorear sobre la cadena para la entrega del servicio.
- Cambios realizados que puedan afectar la red de comunicaciones y que impliquen un mayor acceso a la información de la organización deberán ser previamente autorizados.

Sobre la gestión de incidentes de seguridad de información

Responsable: Gestor de servicio

Propósito

Garantizar y establecer mecanismos para una adecuada gestión de incidentes de seguridad de información que asegure la disponibilidad, confidencialidad e integridad de datos.

Alcance: Proceso de admisión, atención, egreso e identificación de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Gestión de incidentes de seguridad de información y mejoras

Se debe realizar un seguimiento a la gestión de incidentes de seguridad de información e identificar mejoras que garanticen una mejor entrega del servicio y la disponibilidad y confidencialidad de la información.

Respecto a los reportes de eventos o incidentes ser debe tener las siguientes consideraciones:

- Se consideran incidentes de seguridad aquellas anomalías o eventos que afecten los sistemas de información, redes de comunicación, violación de acuerdos y divulgación de información por parte de acciones externas o internas a la organización.
- La comunicación de incidentes debe ser realizada por medio de los canales establecidos en los procedimientos.
- Se debe reportar: errores humanos, controles de seguridad ineficientes, incumplimiento con normas legales, brechas en la integridad, confidencialidad y disponibilidad de información esperadas, descontrol en los sistemas de cambios, funcionamiento incorrecto de hardware o software, violación sobre los derechos de acceso y permisos otorgados.

Dentro de la gestión de incidentes se verifica y realiza un análisis de vulnerabilidades que son el aporte inicial para un análisis de riesgo posterior. Se debe considera lo siguiente:

- Los trabajadores deben reportar las vulnerabilidades identificadas lo antes posible para evitar la materialización de incidentes de seguridad de información. El mecanismo de reporte debe ser claro, accesible y debe estar disponible.

- Las vulnerabilidades deben ser comunicadas a todo el personal de la organización como parte de los planes de concientización para evitar la materialización de riesgos que afecten el servicio y los procesos de negocio.

Respecto a los eventos de seguridad de información y la gestión de estos, se debe tener en cuenta realizar la priorización de incidentes de acuerdo a la clasificación asignada por los responsables del registro. Determinar los mecanismos de respuesta ante estos incidentes.

Dentro de los incidentes es necesario recolectar evidencia como parte de la gestión e investigación que ayude a determinar el origen de estos y como estar preparados para incidentes similares en el futuro. Se debe tomar en cuenta:

- Seguir procedimientos para recolección de evidencias relacionadas a la materialización de los incidentes de seguridad de información que incluya:

    - Custodia de la evidencia recolectada y asegurarla.
    - Definir los roles y responsabilidades del personal involucrado en la recolección de evidencias y verificar cuáles son sus competencias.
    - Documentar la evidencia recolectada.

De acuerdo a los incidentes suscitados se debe establecer una respuesta frente a estos, para la cual se debe de considerar:

- Colectar la evidencia tan rápido como sea posible luego del incidente.
- Determinar en qué momento es pertinente escalar incidencias de seguridad de información de acuerdo a un procedimiento establecido de acuerdo a la criticidad el incidente y el impacto en el negocio, así como establecer los tiempos máximos de solución y confirmar cual será el siguiente nivel de resolución de incidencias.
- Comunicar la existencia de incidentes de seguridad de información. Brindar los detalles de acuerdo a la necesidad de información al personal interno y externo.
- Realizar análisis forense de ser necesario o requerido.
- En caso el incidente produzca eliminación de datos, brindar la autorización para iniciar la recuperación de datos.

Sobre la continuidad del negocio

Responsable: Gestor de continuidad de negocio

Propósito

Garantizar que las estrategias de continuidad de negocio estén alineadas a los requerimientos de seguridad de información para asegurar que en medio de desastres o incidentes que interrumpen la entrega de servicios, se preserva la confidencialidad e integridad de los datos.

Alcance: Proceso de admisión, atención, egreso e identificación de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Continuidad de la seguridad de información:

Se debe planificar los aspectos de la continuidad de negocios dentro de la organización y alinearlas a los requerimientos de seguridad y los aspectos legales como la ley de protección de datos personales y la norma técnica peruana de la historia clínica. De acuerdo a los planes de continuidad se toma en cuenta lo siguiente:

- La organización debe determinar cómo es respaldada la seguridad de información desde la gestión del plan de continuidad de negocios o el plan de recuperación de desastres.
- Los requerimientos de seguridad de información deben estar contenidos en el plan de continuidad y el plan de recuperación de desastres.
- En caso los planes de continuidad no estén formalizados, el área de seguridad de información asumirá que los requerimientos de seguridad son los mismos en situaciones adversas y deberán realizar un análisis de impacto en caso se materialice algún incidente que afecte a la confidencialidad, integridad y disponibilidad de datos.

En cuanto a la implementación de los planes de continuidad de negocios, se debe tomar en cuenta las siguientes consideraciones:

- Asegurar una estructura de roles que esté preparada para actuar frente a los incidentes que causen una interrupción en el negocio y puedan mitigar y brindar una respuesta de acuerdo a su experiencia y competencias bajo la autorización de un superior.
- La seguridad debe estar controlada dentro de la continuidad de negocios, por lo cual debe existir un personal responsable de responder frente a estos incidentes y garantizar el alineamiento con los requerimientos de seguridad de información.
- Los procedimientos y planes de acción y respuesta deben estar documentados y detallarán como la organización hace frente a eventos que afecten la seguridad de información y la continuidad de negocio. Estos planes deben estar alineados a las estrategias definidas en la continuidad de negocio de la organización.
- Verificar que los procesos para los cuales se establecen las estrategias de continuidad, sean los procesos de los cuales se desprenden los requerimientos de seguridad de información, de esta manera se logra que ambas estrategias estén alineadas hacia un mismo fin.

Según las evaluaciones realizadas al plan de continuidad, adicionalmente se deberá revisar la continuidad de la seguridad de información en los procesos para identificar posibles cambios a nivel operacional que afecten la estrategia planteada, por lo cual determina lo siguiente para garantizar la continuidad de la seguridad de información:

- Probar la funcionalidad de los procesos que abarcan la continuidad de la seguridad de información, los procedimientos y controles para determinar la coherencia con los objetivos de continuidad y seguridad.
- Revisión de la validez y eficacia de la continuidad de seguridad de información, los niveles de información, los controles y la estabilidad de los procesos garantizando el cumplimiento de los requerimientos establecidos ante algún cambio que ha sido realizado.

2. Redundancia

La organización debe identificar los requerimientos de negocio de para la disponibilidad de los sistemas de información. Si esta no puede ser garantizada se debe considerar arquitecturas redundantes, los cuales deben ser probados para asegurar que frente a un error en un componente, el otro componente funciona según lo esperado.

Este tipo de arquitectura presenta riesgos los cuales deben ser evaluados dentro de una gestión integral de riesgos organizacionales y a nivel de proyecto.

Sobre el cumplimiento

Responsable: Oficial de seguridad de información, Gerente general

Propósito

Garantizar el cumplimiento de leyes en los procesos de negocio y los requerimientos externos relacionados a la seguridad de información: La ley de protección de datos personales.

Alcance: Proceso de admisión, atención, egreso e identificación de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Cumplimiento de los requisitos legales y contractuales

En la organización, debido al rubro del negocio, deben identificarse todos los requerimientos externos a nivel legal, es otras palabras, las leyes aplicables a la organización según el tipo de negocio.

Si la actividad de la empresa tiene contacto con otros países, los gerentes deberán garantizar el cumplimiento con los requisitos regulatorios aquellos para evitar multas o daño a la reputación debido al incumplimiento.

Así mismo, debido a la línea de negocio a la cantidad de pacientes de la organización, no obstante en línea a las leyes a cumplir, se debe garantizar la privacidad y protección de datos personales tomando en cuenta los siguientes puntos:

- Las políticas sobre la protección de datos personales debe ser comunicada.
- Establecer la estructura pertinente para velar por el cumplimiento de las políticas y la ley de protección de datos personales.

- La clasificación de la información debe formar parte de las políticas de datos personales para verificar las medidas y técnicas de protección a aplicar e implementar sobre cada nivel.

2. Revisiones de la seguridad de información

De acuerdo a las políticas planteadas y alineadas a los requerimientos de seguridad de información producto de la evaluación de los procesos el oficial de seguridad de información y el comité estratégico debe cumplir con las siguientes actividades:

- Monitorear el cumplimiento de las políticas. En caso se identifiquen políticas que no se cumplen o no se aplican:
    - Identificar las causas del cumplimiento
    - Aplicar las medidas correctivas para garantizar que a partir de un tiempo establecido se alcanzará el cumplimiento de las políticas internas.
- Revisar las acciones correctivas que han sido aplicadas ante algún incumplimiento para determinar su eficacia o sus debilidades.
- Deben registrar los resultados de las evaluaciones y las acciones a tomar de acuerdo al cumplimento de las políticas y la satisfacción de la organización frente a estas.

ANEXO L: Evaluación

10.1 Evaluación de nivel de madurez de los procesos habilitadores

A continuación se realiza la evaluación del nivel de madurez para cada proceso habilitador y su aplicación dentro de los procesos de negocio.

El estado de cumplimiento es determinado por la organización basándose en las actividades diarias, los controles establecidos y el entorno del negocio antes de implementar las políticas de seguridad de información. Luego de esto, se determina el nivel de madurez deseado y el tiempo, usualmente se refiere al tiempo para la revisión del gobierno de TI de la empresa, para realizar la próxima evaluación.

En la siguiente tabla se muestra criterios de evaluación de la norma ISO/IEC 15504 y los criterios para identificar la escala de cumplimiento para cada nivel de madurez.

Leyenda	Descripción
N : "Not achieved"	No existe evidencia de la entrega o gestión del proceso habilitador. El cumplimiento de las actividades está entre cero (0) y quince (15) por ciento.
P: "Partially achieved"	Existe evidencia de la entrega de las actividades definidas para el proceso. Algunos aspectos deben ser no predecibles. El cumplimiento de las sub – actividades de gestión está entre quince (15) y cincuenta (50) por ciento.
L: "Largely achieved"	Existe evidencia sistemática y significativa sobre la entrega de y cumplimiento de actividades dentro del proceso. El cumplimiento está entre cincuenta (50) y ochenta y cinco (85) por ciento.
F: "Fully achieved"	Existe evidencia total y sistemática sobre el cumplimiento de las actividades de gestión definidas el proceso. El cumplimiento está entre ochenta y cinco (85) y cien (100) por ciento.

Tabla 10.1.1 - Leyenda para especificar el nivel de madurez de un proceso habilitador

10.1.1 Procesos habilitadores comunes para los procesos de negocio

De acuerdo al estado actual de los cuatro procesos y su cumplimiento en la organización se procede a completar el estado de cumplimiento para cada actividad y sus sub-actividades. En caso no esté desarrollándose dicha sub-actividad, se hace la observación y recomendación respectiva.

a. <u>Proceso habilitador: Garantizar el mantenimiento y configuración del marco de control de gobierno</u>

EDM01	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Evaluar el sistema de gobierno	Analizar e identificar los factores de entorno interno y externo relacionados a la seguridad de información, los cuales afectan directamente al proceso, junto con las tendencias en el negocio que puedan influir en el diseño del gobierno.	Cumple
	Evaluar el nivel de la seguridad de información dentro del negocio y el cumplimiento con regulaciones externas dentro del proceso. Entre estas se tiene: Ley de protección de datos personales, Ley de emergencia y la norma técnica peruana de la historia clínica.	No se alinea a la ley de protección de datos personales todavía.
	Articular los principios que guiarán el diseño óptimo del modelo de toma de decisiones sobre el gobierno de TI y su enfoque a la seguridad de información.	Se tiene un modelo de toma de decisiones, pero no se considera el enfoque de seguridad de información.
	Considerar cómo serán aplicadas o enfocadas la ley de protección de datos personales, la ley de emergencia y la norma técnica peruana de la historia clínica en el gobierno de TI de la empresa y en los procesos base.	Cumple, pero no se han formalizado los resultados y consideraciones.

Dirigir el sistema de gobierno	Exigir la función de seguridad de información para toda la empresa y como esta se aplicará a los procesos.	Cumple, pero todavía no se ha creado esta función.
	Contar con un comité estratégico que esté enfocado a la seguridad de información (ISSC)	No cumple
	Alinear la estrategia de seguridad de información con la estrategia empresarial	No cumple
	Obtener el compromiso de la alta dirección para verificar la seguridad de información y la gestión de riesgos de información.	No cumple
	Asignar responsabilidad para que se apliquen principios de gobierno, modelos de toma de decisión acordados.	Cumple
Monitorear el sistema de gobierno	Supervisar mecanismos para asegurar que los sistemas para medir el desempeño de seguridad de información cumplen con la ley de protección de datos personales y la norma técnica peruana de historia clínica.	No cumple
	Proporcionar supervisión de la efectividad y el cumplimiento con el sistema de control de la empresa.	Auditoría se encarga de la supervisión pero no comunica los resultados.
	Evaluar la efectividad y rendimiento de los stakeholders en los que se ha delegado responsabilidad y autoridad para el gobierno de TI de la empresa.	Cumple.

Tabla 10.1.2 – Evaluación de cumplimiento para proceso habilitador EDM01

- **Nivel de madurez actual: Proceso Incompleto (0) – "P"**

  Se puede verificar que, de acuerdo a los requisitos de la norma ISO/IEC 15504, el proceso habilitador y sus actividades no han sido aplicadas dentro del negocio, al menos no desde el punto de vista de seguridad de información, teniendo como resultado actividades que no son comunicadas y que no están debidamente formalizadas, lo cual no está alineado a los principios de gobierno de TI.

No obstante al verificar que existe evidencia parcial del cumplimiento de algunas de las sub-actividades y de acuerdo a lo que define la norma, se considera que el nivel interno de madurez es “Partially Achieved” – (P).

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

La organización se establece como meta alcanzar el nivel de madurez siguiente en la escala definida por la norma, proceso ejecutado. Antes de llegar a este, se debe recorrer las escalas restantes dentro del proceso habilitador en madurez cero (0) para posteriormente ejecutar cada una de las sub-actividades definidas.

Luego de la siguiente iteración para la revisión del gobierno de TI de la empresa se vuelve a realizar esta mecánica para identificar el logro de este objetivo y a qué nivel, de manera que se implementen las mejoras y se defina la nueva meta de madurez para la siguiente evaluación.

b. <u>Proceso habilitador: Garantizar la entrega de beneficios</u>

EDM02	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Evaluar la optimización del valor	Identificar y registrar los requisitos de los stakeholders en relación con los procesos base para la protección de sus intereses y la entrega de valor tomando en cuenta los parámetros de seguridad de información. Establecer la dirección respectiva.	Cumple
	Comprender y discutir periódicamente sobre las oportunidades que pueden surgir a partir de los cambios dentro de los procesos base al emplear tecnologías actuales y optimizar el valor de estas oportunidades.	Cumple
	Comprender el significado del valor en la empresa y como se ha comunicado, entendido y aplicado a través de los procesos de la organización.	Cumple
	Evaluar la efectividad de la integración y	No cumple, no existe

	alineamiento de las estrategias de TI y seguridad de información en la empresa con los objetivos para aportar valor, así como la alineación de estos últimos con el portafolio de inversiones	función de seguridad de información.
Dirigir la optimización del valor	Asegurar que se empleen medidas financieras y no financieras para describir el valor añadido de las iniciativas de seguridad de información en los procesos base.	No cumple
	Establecer un método para demostrar el valor de la seguridad de información para garantizar el uso eficiente (considerando los niveles de seguridad) de los activos dentro de los procesos identificados.	No cumple
	Dirigir los cambios necesarios en el portafolio de inversiones y servicios para realinearlos con los objetivos actuales, los esperados y/o sus limitaciones.	Cumple
	Dirigir los cambios necesarios en asignación de imputaciones y responsabilidades del portafolio de inversión y entrega de valor a partir de los servicios y procesos de negocio enfocados a la seguridad de información.	Cumple, pero no está enfocado a la seguridad de información.
Monitorear la optimización del valor	Monitorear el resultado de las iniciativas de seguridad de información frente a las expectativas para asegurar la entrega de valor de acuerdo a los objetivos de negocio	No cumple
	Definir objetivos de desempeño, métricas, metas y puntos de referencia. Revisarlos y formalizarlo junto con los stakeholders.	Cumple, pero solo a alto nivel, no están alineadas a la seguridad de información.
	Tomar medidas de gestión para asegurar la optimización del valor. En caso sean medidas correctivas, asegurarse de que sean iniciadas y controladas.	Cumple

Tabla 10.1.3 - Evaluación de cumplimiento para proceso habilitador EDM02

- **Nivel de madurez actual: Proceso Incompleto (0) – "P"**

  De acuerdo a la norma ISO/IEC 15504, el proceso habilitador tiene un nivel de madurez cero (0) porque sus actividades no han sido totalmente aplicadas dentro del negocio. La falta de la función de seguridad de información y los requerimientos da como resultado que no se cumplan todas las actividades y solo alcance un porcentaje de cumplimiento que lleva a una calificación interna igual a "P".

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  La organización se establece como meta alcanzar el nivel de madurez siguiente en la escala definida por la norma, proceso ejecutado.

  Para llegar a la meta se debe completar la escala interna del nivel de madurez anterior, lo cual implica la definición y formalización de la sección y función de seguridad de información y los roles respectivos para asignar sobre ellos la responsabilidad de acuerdo a sus capacidades. Verificar este cumplimiento en la siguiente iteración de gobierno.

c. <u>Proceso habilitador: Garantizar la optimización del riesgo</u>

EDM03	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Evaluar la gestión de riesgos	Determinar junto con la directiva de la empresa el nivel de apetito por el riesgo.	Cumple
	Medir el nivel de integración de la gestión de riesgos de seguridad de información con el modelo general de riesgos de la organización.	No cumple
	Determinar el grado de alineamiento de la estrategia de riesgos de TI y seguridad de información con la estrategia de riesgos empresariales.	No cumple
	Determinar si las tecnologías empleadas en los procesos base están sujetas a una evaluación	No cumple, la gestión de riesgos es un proyecto a

	de riesgos adecuada según lo descrito en estándares relevantes que pueda adoptar la organización.	futuro.
Dirigir la gestión de riesgos	Integrar la gestión de riesgos de seguridad de información dentro del modelo general de riesgos.	No cumple
	Dirigir la elaboración de planes de comunicación y acción de riesgos promoviendo una cultura consciente sobre estos y su impacto dentro del negocio.	Cumple
	Dirigir la implantación de mecanismos apropiados para responder a los riesgos cambiantes y notificar a los niveles adecuados según el principio de escalamiento.	No cumple
	Dirigir para que los riesgos de seguridad de información dentro de los procesos puedan ser identificados por cualquier persona en cualquier momento según las políticas y procedimientos publicados.	No cumple
Monitorear la gestión del riesgos	Monitorear el perfil frente al riesgo o el apetito del riesgo de la empresa para lograr un equilibro óptimo entre riesgos y oportunidades de negocio	No cumple
	Incluir las salidas de los procesos de gestión de riesgos de información como entradas las la gestión de riesgos de la organización.	No cumple
	Comunicar los problemas de la gestión de riesgos al directorio.	No cumple
	Monitorear las metas y métricas de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos. Iniciar medidas correctivas para casos especiales	Cumple pero solo a alto nivel, no se comunica las medidas a tomar.

Tabla 10.1.4 - Evaluación de cumplimiento para proceso habilitador EDM03

- **Nivel de madurez actual: Proceso incompleto (0) – "N"**

  De acuerdo a la evaluación y ajustes a los criterios de la norma que integra el marco COBIT 5.0 se determina la falta de aplicación de las actividades, la madurez identificada es cero (0). Por ello el proceso habilitador es entregado con fallas y debilidades que no permite el desarrollo del enfoque de seguridad de información.

  El incumplimiento de la mayoría de las actividades relacionadas y los procedimientos no formalizados ni integrados, determina que el nivel interno de madurez es "Not achieved".

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

  Se establece como objetivo el nivel de madurez superior debido a que dentro de los proyectos futuros de la empresa referencia es implementar mecanismos y realizar el análisis de riesgo dentro del cual se incluyan las brechas y vulnerabilidades de seguridad de información.

d. <u>Proceso habilitador: Gestionar el marco de control de TI</u>

APO01	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Definir la estructura organizativa	Alinear la seguridad de la información de la organización con la arquitectura de negocio de la empresa.	No cumple
	Establecer el comité estratégico de TI bajo el enfoque de seguridad de información	No cumple
	Definir la función de la seguridad de información, capacidades y decisiones necesarias	Se identifica la necesidad de seguridad de información pero no se encuentra formalizada.
	Identificar las decisiones necesarias para alcanzar los resultados corporativos y estrategia de TI y seguridad de información para la gestión y ejecución de servicios de TI.	Se tiene modelos de decisiones, pero no está formalizado dentro del área de TI.

	Establecer un comité estratégico de TI a nivel de consejo administrativo, el cual se asegure que el gobierno de TI está contemplado de forma adecuada y que priorice programas de inversión según la estrategia y objetivos de negocio.	Cumple
	Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre el negocio y las funciones de TI dentro de la empresa y terceros.	Cumple
	Verificar la adecuación y eficacia de la estructura organizativa.	Cumple
Establecer roles y responsabilidades	Establecer, acordar y comunicar los roles de CISO e ISM[13]	No cumple
	Determinar las funciones de la organización que tienen la obligación de seguridad de información y añadirlas a la descripción de puestos.	No cumple
	Tomar como referencia los requisitos de la empresa y continuidad del servicio de TI para la definición de roles.	Cumple
	Estructurar los roles y responsabilidades para reducir la posibilidad de que un solo rol pueda comprometer un proceso crítico.	Cumple
	Implementar prácticas para monitorear que los roles y responsabilidades se pongan en práctica de forma correcta. El nivel de supervisión o monitoreo debe estar en consonancia con este puesto y las responsabilidades asignadas.	Cumple
Mantener los elementos habilitadores del modelo de gobierno	Considerar el ambiente interno de la empresa incluyendo la gestión de la cultura y filosofía, tolerancia al riesgo, valores éticos, código de conducta, responsabilidad y requisitos de seguridad de información.	No se definen los requisitos de seguridad de información.
	Alinear con estándares nacionales e internacionales de seguridad de información	No cumple

[13] ISM: Information Security Manager

	que sean viables. Evaluar buenas prácticas de seguridad de información.	
	Desarrollar las políticas de seguridad de información de acuerdo al negocio, procesos y requisitos legales o regulatorio dentro del ambiente interno de la empresa.	No cumple
	Evaluar y actualizar las políticas como mínimo una vez al año, para ajustarlas de acuerdo a los cambios operativos o a nivel de negocio	No cumple
	Implantar las políticas de TI y seguridad de información a todo el personal relevante y establecer los métodos y procedimientos de medición de su cumplimiento.	No cumple, existen políticas pero no alineadas a seguridad de información.
Comunicar los objetivos y la dirección de gestión	Desarrollar un programa de sensibilización sobre seguridad de información	Cumple
	Establecer indicadores para medir comportamientos con respecto a la seguridad de información	No cumple. Falta implementar. se derivaran de proyectos futuros
	Proporcionar recursos suficientes y calificados para dar soporte al proceso comunicativo.	Cumple
	Garantizar que la información comunicada engloba una clara articulación del entorno empresarial y con un nivel de detalle adecuado para cada área de la empresa.	Cumple
Definir la propiedad de la información y del sistema	Definir sistemas y accesos de datos a nivel empresarial dentro de los procesos de gestión de seguridad de información que involucran procesos base.	No cumple
	Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) en toda la empresa.	Cumple
	Crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones. Incluir sistemas tercerizados y aquellos cuya propiedad debe permanecer	Cumple

	dentro de la empresa.	
	Definir e implementar procedimientos para asegurar la integridad y consistencia de la información almacenada en formato electrónico.	No cumple
Gestionar la mejora continua de los procesos	Examinar informes que detallan el control de la seguridad de información y las debilidades del proceso.	No cumple
	Contemplar medidas para mejorar la eficiencia y eficacia de la seguridad de información.	No cumple, pero se tiene proyectos para evaluar controles de seguridad a nivel técnico
	Identificar procesos críticos de negocio basándose en el rendimiento, cumplimiento y los riesgos relacionados. Evaluar la capacidad del proceso e identificar objetivos de mejora.	Cumple
	Aplicar prácticas de gestión de calidad y en base estas realizar la actualización de los procesos o la implementación de mejoras.	Cumple, pero no es satisfactorio. Incompleto
Mantener el cumplimiento de las políticas y procedimientos	Programar y realizar evaluaciones periódicas para determinar el cumplimiento con las políticas y procedimientos de seguridad de información para tomar las acciones correctivas de ser necesario.	Cumple a nivel de TI pero no en los aspectos de seguridad de información
	Integrar el rendimiento y el cumplimiento dentro de los objetivos individuales del personal.	Cumple en base al marco COBIT 4.1
	Evaluar el desempeño de los procesos habilitadores del marco de referencia y adoptar las acciones necesarias	La evaluación se realiza en base a la aplicación de COBIT 4.1

Tabla 10.1.5 - Evaluación de cumplimiento para proceso habilitador APO01

- **Nivel de madurez actual: Proceso incompleto (0) – "P"**

  De acuerdo a la evaluación y ajustes a los criterios de la norma, el nivel de madurez es cero (0). Esto indica que el proceso habilitador es entregado con fallas y debilidades debido a que el gobierno de TI no se encuentra alineado al

enfoque de seguridad de información y se omite la aplicación de leyes que puede afectar directamente a los procesos de negocio.

No obstante de acuerdo a las actividades cumplidas, el nivel interno de este proceso es “Partially achieved”.

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

Se establece como objetivo el nivel de madurez, proceso ejecutado, lo cual implica el alineamiento bajo el enfoque de seguridad de información y la formalización y comunicación de la iniciativa junto con el establecimiento y cumplimiento de los roles y responsabilidades que garanticen el cumplimiento de las actividades y sub-actividades definidas para el proceso habilitador y establecer las mejoras posteriores para iteraciones siguientes.

e. <u>Proceso habilitador: Monitorear, evaluar y medir el rendimiento y la conformidad</u>

MEA01	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Establecer un enfoque de la supervisión	Identificar las partes interesadas de mantener un enfoque de seguridad de información dentro de la organización y dentro del proceso para cumplimiento de objetivos.	No cumple
	Alinear y mantener el control de la seguridad de información dentro de los procesos base. Realizar la evaluación del enfoque de gobierno de TI y su alineamiento con la organización.	No cumple
	Validar el enfoque empleado de seguridad de información para gobierno de TI e identificar nuevos drivers o recursos que permitan alinear otro enfoque de gobierno según sea el caso.	No cumple
	Solicitar, priorizar y asignar recursos para la supervisión de la función de seguridad de información bajo procedimientos establecidos y dentro de los procesos base.	No cumple

Establecer los objetivos de cumplimiento y rendimiento	Definir y revisar los objetivos y métricas con los stakeholders respecto a la seguridad de información de acuerdo con los procesos para identificar omisiones y establecer la validez de métricas o tolerancias.	No cumple
	Comunicar los cambios relacionados con la seguridad de información, su desempeño y el cumplimiento con los stakeholders tomando como base el conjunto de procesos que forman parte del gobierno de TI.	No cumple
	Evaluar si los objetivos de seguridad de información y las métricas son adecuados para la verificación y medir la performance de los procesos de acuerdo a la ley de protección de datos personales, norma técnica peruana de la historia clínica y la ley de emergencia.	No cumple
Recopilar y procesar los datos de cumplimiento y rendimiento	Coleccionar datos y analizar la performance y conformidad relacionada a la seguridad de información y la gestión de riesgos de información.	No cumple
	Evaluar la integridad, eficacia e idoneidad de los datos recolectados y consolidarlos.	No cumple
Analizar e informar sobre el rendimiento	Diseñar informes de rendimiento del proceso desde el enfoque de seguridad de información. Implementar mecanismos para su elaboración de acuerdo a lo esperado por los stakeholders.	No cumple
	Comparar los valores de rendimiento internos y externos de acuerdo al proceso.	Cumple
	Distribuir informes a las partes interesadas relevantes, tanto de rendimiento como de las incidencias suscitadas dentro del proceso.	Cumple, pero los informes se manejan solo a nivel de comité.
Asegurar la implantación de medidas correctivas	Desarrollar medidas correctivas para tratar los problemas relacionados al proceso y que afecten a la seguridad de información.	No cumple
	Asegurar la asignación de responsabilidades	No cumple

	dentro de las acciones correctivas y emitir los informes respectivos.	

Tabla 10.1.6 - Evaluación de cumplimiento para proceso habilitador MEA01

- **Nivel de madurez actual: Proceso Incompleto (0) – "N"**

  De acuerdo al cumplimiento de las actividades y lo que indica la norma ISO/IEC 15504, el proceso habilitador tiene madurez cero debido a la falta de formalización de un enfoque de seguridad en la organización y que a partir de este se puedan identificar métricas y métodos para la evaluación. Según las actividades cumplidas y que pueden se evidencian, el nivel interno de este proceso es "Not Achieved".

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

  Para la siguiente iteración el nivel al cual la organización quiere llegar es uno (1): proceso ejecutado. Se debe tomar en cuenta las brechas cerrar para alcanzar el enfoque de seguridad de información e iniciar las actividades de monitoreo y evaluación de la conformidad interna y externa.

f. <u>Proceso habilitador: Monitorear, evaluar y medir el cumplimiento de requerimientos externos</u>

MEA03	Sub-actividades para el cumplimiento de actividad	Estado de Cumplimiento
Identificar requisitos externos de cumplimiento	Identificar los requerimientos externos de seguridad de información que deben de cumplirse dentro del proceso de acuerdo a la ley de protección de datos personales, norma técnica peruana de la historia clínica y ley de emergencia.	No cumple
	Establecer mecanismos de monitoreo sobre el cumplimiento de requerimientos externos relacionados a la seguridad de información.	No cumple
	Identificar posibles cambios en las regulaciones que conlleven a modificaciones dentro del proceso y a la identificación de nuevos	Se contemplan posibles cambios en las regulaciones, pero no se

	requerimientos y exigencias a nivel de seguridad de información.	verifica exigencias o requerimientos de seguridad de información.
	Mantener un inventario sobre normas, leyes o requerimientos que debe de cumplir la organización.	Cumple
Optimizar la respuesta a requisitos externos	Revisar y comunicar los requerimientos externos y regulaciones a todos los stakeholders.	No cumple
	Revisar periódicamente las políticas y estándares relacionados al proceso para mantener la eficacia y asegurar el cumplimiento y gestión de riesgos.	No cumple
Confirmar el cumplimiento de requisitos externos	Colectar y analizar datos para garantizar el cumplimiento de la seguridad de información y la gestión de riesgos.	No cumple
	Evaluar periódicamente las políticas relacionadas al proceso bajo el enfoque de seguridad de información.	No cumple
Obtener garantía de cumplimiento de requisitos externos	Obtener la conformidad del cumplimiento de políticas que garanticen el alineamiento con requerimientos externos. Determinar el nivel de satisfacción.	Cumple solo al determinar el nivel de satisfacción, no sobre las políticas
	Garantizar que los proveedores de TI cumplan con los requerimientos de seguridad de información.	Existen medidas para verificar el cumplimiento pero no se alinean con indicadores para medir la seguridad de información.
	Consolidar a nivel empresarial los informes sobre requerimientos externos e internos y difundirlos a todas las unidades de negocio que abarcan el proceso.	Cumple, pero estos informes solo se manejan a nivel de gerencia.

Tabla 10.1.7 - Evaluación de cumplimiento para proceso habilitador MEA03

- **Nivel de madurez actual: Proceso incompleto (0) – "P"**

  De acuerdo a la evaluación y ajustes a los criterios de la norma, el nivel de madurez es cero (0). Debido a la falta de alineamiento con regulaciones como lo es la ley de protección de datos personales y la falta de formalización de la función de seguridad de información que permita identificar otros requerimientos externos y dar seguimiento al cumplimiento regulatorio alineados a datos e información..

  No obstante de acuerdo a las actividades cumplidas, el nivel interno de este proceso es "Partially achieved".

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

  Se establece como objetivo el nivel de madurez uno (1), proceso ejecutado, lo cual implica el alineamiento bajo el enfoque de seguridad de información y la formalización y comunicación de la iniciativa de acuerdo a las normas externas como la ley de protección de datos personales, norma técnica peruana de la historia clínica y la ley de emergencia.

10.1.2 Proceso de admisión de pacientes

A continuación, se muestra la evaluación de los procesos habilitadores para cada uno de los procesos de negocio en particular, iniciando esta evaluación con el proceso de admisión de pacientes. Tal como se mencionó en el capítulo anterior, este proceso debe cumplir con la regulación de protección de datos personales, Norma técnica peruana de la historia clínica y la Ley de emergencia.

a. <u>Proceso habilitador: Gestionar la estrategia</u>

APO02	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Comprender la dirección de la empresa	Entender como la seguridad de información debe respaldar los objetivos de la empresa y proteger los intereses de los stakeholders, cumpliendo con la ley de protección de datos	Cumple pero no está documentado y tampoco formalizado y alineado con ley de protección de

	personales, norma técnica peruana de la historia clínica y ley de emergencia.	datos personales.
	Entender la arquitectura de negocio y de sistemas de la empresa empleada para dar soporte al proceso e identificar posibles brechas de seguridad de información.	No cumple
	Identificar los interesados del dentro del proceso y sus requerimientos.	Cumple, pero no está formalizado.
	Determinar las prioridades para desarrollar los cambios estratégicos a nivel de proceso.	Cumple
Definir el objetivo de las capacidades de TI	Asegurar que los requerimientos de seguridad de información estén incluidos dentro de las capacidades de TI.	No cumple
	Definir y acordar el impacto de los requerimientos de seguridad de información dentro de la arquitectura de la empresa que soporta el proceso de admisión, según lo que los stakeholders consideren relevante.	No cumple
	Definir de acuerdo al proceso de admisión, las capacidades y servicios de TI a entregar.	Cumple
	Definir los objetivos de TI a alto nivel y cómo contribuirán a los objetivos de negocio empresariales y como soporta este proceso al cumplimiento de ambos.	Cumple
Realizar un análisis de brecha	Identificar dentro del proceso las brechas a cerrar y los cambios requeridos para llegar al nivel deseado.	Cumple
	Examinar el nivel de cumplimiento del proceso respecto a la ley de protección de datos personales, norma técnica peruana de la historia clínica y la ley de emergencia.	No existe cumplimiento ni alineamiento a la ley de protección de datos personales.
	Mejorar la definición del estado deseado en el proceso y sus objetivos. Sustentarlos demostrando los beneficios a partir de este estado frente al impacto en caso no se llegara a esta meta	Cumple

Definir el plan estratégico y la hoja de ruta	Definir la estrategia de seguridad de información y alinearla con la de TI y las estrategias de negocio para el cumplimiento de objetivos dentro del proceso de admisión.	No cumple
	Crear la hoja de ruta que incluya la planificación e interdependencias de las iniciativas a nivel empresarial de acuerdo al proceso, la cual a su vez señale los riesgos y costos de los cambios.	No cumple
	Asegurar que el plan estratégico de TI y la hoja de ruta contengan los requerimientos de seguridad de información identificados en el proceso de admisión	No cumple
	Obtener el apoyo de las partes interesadas y la aprobación del plan.	No cumple
Comunicar la estrategia y la dirección de TI	Desarrollar el plan estratégico y el plan de seguridad de información que incluya aspectos relacionados al proceso de admisión y comunicarlo a los stakeholders	Se tiene un plan estratégico de información pero no un plan de seguridad de información.
	Desarrollar el plan de comunicación de acuerdo a público objetivo identificando los canales de comunicación.	Cumple
	Obtener retroalimentación y actualizar el plan de comunicaciones y la estrategia de seguridad de información y TI según sea necesario para mantener el impulso.	Cumple, pero no se alinea a la estrategia de seguridad de información.

Tabla 10.1.8 – Admisión. Evaluación de cumplimiento para proceso habilitador APO02

- **Nivel de madurez actual: Proceso Incompleto (0) – "P"**

  De acuerdo a lo que especifica la norma ISO/IEC 15504, de acuerdo a la evidencia y cantidad de actividades que han sido aplicadas para la mejora del proceso de negocio y en consecuencia apoyan al proceso habilitador, se determina que el nivel de madurez es cero (0).

  No obstante, realizando la evaluación interna, el habilitador tiene un logro parcial para el actual nivel de madurez.

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

  El objetivo de la organización es que este proceso habilitador alcance una madurez de uno (1) para la siguiente revisión, por lo cual tendría que incluir los requerimientos de seguridad de información y alinear el proceso de acuerdo a la ley de protección de datos personales.

b. <u>Proceso habilitador: Gestionar los recursos humanos</u>

APO07	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Mantener la dotación del personal suficiente y adecuado	Evaluar las necesidades de personal periódicamente o frente a cambios organizacionales de forma de asegurar que tanto TI como la empresa cuenta con recursos para soportar el proceso de admisión y la iniciativa de TI	Cumple
	Dentro de los procesos de contratación, incluir controles de antecedentes de acuerdo a la función a realizar.	Cumple
	Asegurar que los requisitos de seguridad se incorporan en el proceso de contratación.	No existen requerimientos de seguridad de información identificados o definidos.
	Asegurar la existencia de capacitaciones y que existe personal capaz de cubrir funciones críticas de otro para reducir la dependencia.	Cumple
Identificar personal clave de TI	Asegurar la segregación de funciones en roles críticos del proceso.	Cumple
	Minimizar dependencia de una persona en la realización de una función crítica dentro del proceso de admisión a través de captura e intercambio de conocimiento.	No se encuentra totalmente implementada esta sub-actividad de gestión.

	Identificar y ejecutar acciones según cambios laborales relacionados a los actores del proceso de admisión.	Cumple. Falta afianzar la gestión de proveedores.
Mantener las habilidades y competencias del personal	Definir habilidades y competencias necesarias de los recursos para lograr los objetivos dentro del proceso y poder escalar hacia los objetivos de alto nivel.	Cumple
	Brindar capacitaciones y programas de seguridad de información al personal que ejecuta los procesos y a nivel transversal para formar conciencia.	No cumple, se brindan capaciones, pero no existen programas de seguridad.
	Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. A partir de estas identificar si se requieren habilidades adicionales para cubrir el proceso y ejecutar el plan de acción para desarrollarlas.	Cumple.
	Asegurar conocimientos y habilidades del personal solicitando certificaciones según la función a realizar. En caso de la seguridad de información, si aplicase, se podría solicitar certificaciones como ISO/IEC 27002, CISM, ISO/IEC 27001: Leed Auditor.	Cumple sin solicitar certificaciones, emplean otros métodos como cartas de recomendación y resultados de evaluación.
Evaluar el desempeño laboral de los empleados	Dentro de la evaluación del desempeño, considerar criterios con respecto a la seguridad de información.	No cumple
	Establecer objetivos individuales alineados con los objetivos del proceso de admisión. Deben reflejar competencias básicas, valores empresariales y habilidades para las funciones.	Cumple
	Proporcionar instrucciones para uso y almacenamiento de información personal dentro del proceso de evaluación.	Cumple.
	Implementar un proceso de reconocimiento a medida que el personal alcance el compromiso, desarrollo de competencias y logro de objetivos.	Cumple.

Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio	Gestionar la ubicación del personal de seguridad de información de acuerdo a los requerimientos de negocio.	No cumple
	Comprender la demanda actual y futura de recursos humanos involucrados dentro del proceso de admisión para apoyar el logro de objetivos de TI y necesidades operativas del día a día.	Cumple
	Mantener información adecuada sobre el tiempo dedicado a diferentes tareas, trabajos, servicios o proyectos	Cumple
Gestionar el personal contratado	Obtener un acuerdo formal por parte del personal sobre las políticas y requisitos de la seguridad de información a aplicarse en el proceso de admisión.	No cumple
	Implementar políticas o procedimientos que describan como gestionar el personal para identificar necesidad de tercerizar algún servicio de TI.	Los procedimientos y políticas existentes no son suficiente
	Llevar a cabo revisiones para asegurar que el personal cumple con sus funciones, que el derecho de acceso son adecuados y alineados con los acuerdos pactados al firmar el contrato.	Cumple

Tabla 10.1.9 – Admisión. Evaluación de cumplimiento para proceso habilitador APO07

- **Nivel de madurez actual – Proceso Incompleto (0) – "L"**

  De acuerdo a lo descrito por la norma ISO/IEC 15504, es nivel de madurez es cero (0) debido a la falta de un enfoque de seguridad formal a partir del cual se establezcan requerimientos a cumplir para cada proceso de negocio y en consecuencia sus habilitadores.

  A diferencia de los procesos anteriores, existe mayor cantidad de sub-actividades de gestión que se evidencian en la entrega del servicio, por lo cual la escala interior es "Largely Achieved"

- **Nivel de madurez objetivo – Proceso Gestionado (2)**

El objetivo trazado para la siguiente revisión de gobierno de TI es un proceso gestionado, lo cual implica que no solo se cumplen todas las sub-actividades sino que existe evidencia de mejora y se realiza un monitoreo constante sobre cada una de las actividades de gestión y se realiza el ajuste requerido para que el proceso habilitador continúe la mejora de acuerdo a las capacidades y necesidades reales del proceso de admisión. La brecha a superar será la formalización de la función de seguridad de información.

c. Proceso habilitador: Gestionar el riesgo

APO12	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Recopilar datos	Identificar y recolectar datos para la identificación, análisis y comunicación de los riesgos de seguridad de información.	No cumple, la gestión de riesgos es un proyecto a futuro en la organización.
	Medir y analizar datos históricos de riesgo de TI y seguridad de información suscitados dentro del proceso de admisión y de pérdidas experimentadas de acuerdo a las tendencias externas.	No cumple
	Determinar condiciones específicas que existían o faltaban cuando se materializaron los riesgos dentro de los procesos y como afectaban la frecuencia del evento y la pérdida.	No cumple
	Ejecutar análisis del entorno para verificar los factores de riesgo asociados al proceso.	Cumple
Analizar el riesgo	Identificar, analizar y evaluar los riesgos de información dentro del proceso.	No cumple
	Construir los escenarios de riesgo de TI y seguridad dentro del proceso. Incluir las asociaciones y dependencias entre las amenazas, para detectar medidas de emergencia.	No cumple
	Identificar los riesgos residuales dentro del proceso e identificar exposiciones que puedan	No cumple

	requerir una repuesta al riesgo	
	Validar resultados del análisis de riesgos del proceso antes de usarlos para la toma de decisiones. Verificar alineamiento con requerimientos organizacionales.	No cumple
Mantener un perfil del riesgo	Crear e informar el nivel aceptable y exposición al riesgo que incluya los aspectos de seguridad de acuerdo al proceso.	No cumple
	Identificar dentro del proceso los servicios esenciales para sostenerlo. Analizar la dependencia e identificar debilidades.	No cumple
	Definir un conjunto de indicadores que permitan la identificación rápida y supervisión de los riesgos de seguridad del proceso y sus tendencias.	No cumple
Expresar el riesgo	Definir e implementar evaluaciones y estrategias de respuesta frente a los riesgos del proceso de admisión.	No cumple
	Informar los resultados del análisis de riesgos a los stakeholders sobre el proceso de admisión en términos adecuados y entendibles para soportar decisiones empresariales.	No cumple
	Informar el perfil del riesgo a los stakeholders junto con la efectividad del proceso de admisión y los controles asociados y a la vez identificar oportunidades de TI para aceptar un mayor riesgo e incrementar la capacidad de gestión.	No cumple
Definir un portafolio de acciones para la gestión de riesgos	Monitorear continuamente los riesgos de seguridad de información del proceso de admisión y verificar que el riesgo este alineado con el apetito y tolerancia al riesgo definido por la organización.	No cumple
	Definir conjunto de propuestas para reducir el riesgo o proyectos para incrementar las oportunidades estratégicas de acuerdo a los beneficios y regulaciones.	No cumple

Responder al riesgo	Aplicar las prácticas y controles para la mitigación de riesgos de seguridad. Se recomienda aplicar en este caso la norma ISO/IEC 27002:2013. Incluir controles preventivos y correctivos.	No cumple
	Catalogar los incidentes y comunicar los impactos de negocio a los responsables.	Cumple.

Tabla 10.1.10 – Admisión. Evaluación de cumplimiento para proceso habilitador APO12

- **Nivel de madurez actual – Proceso Incompleto (0) – "N"**

  Tomando en cuenta que dentro de la organización no existe un tratamiento de riesgos de negocio, de TI y específicamente de seguridad de información, se considera que este proceso habilitador está incompleto.

  Dado a que no se presenta evidencias sobre las sub-actividades realizadas y solo tienen algunas iniciativas sobre como evaluar el entorno y los incidentes, dentro del nivel de madurez le corresponde la categoría de "Not Achieved".

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

  Para la siguiente iteración de gobierno se pretende alcanzar un nivel de madurez equivalente a uno (1), debido a que este proceso será una de las bases para el enfoque de seguridad de información y requiere ser priorizado.

d. <u>Proceso habilitador: Gestionar la seguridad</u>

APO13	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Establecer y mantener un SGSI	Definir el alcance del SGSI de acuerdo a las características de la organización y sus políticas.	No cumple, la seguridad de información no está formalizada, su implementación es proyecto futuro
	Diseñar un enfoque de gestión de seguridad y alinear el SGSI a este.	No cumple

	Realizar la declaración de la aplicabilidad del SGSI.	No cumple
	Comunicar los roles y responsabilidades en la gestión de la seguridad de información y el enfoque del SGSI.	No cumple
	Comprometer a la alta dirección para iniciar las actividades de implementación del SGSI.	No cumple
Definir y gestionar un plan de tratamiento del riesgo de la seguridad de información	Diseñar, mantener y aplicar un plan de tratamiento de riesgos de seguridad de información alineados con los objetivos estratégicos de la organización y fines del proceso.	No cumple
	Desarrollar propuestas de mejora al plan de riesgos basados en casos de negocio de acuerdo a los roles y responsabilidades a necesitar para su aplicación y acorde a los drivers identificados.	No cumple
	Definir la medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizarlas para producir resultados reproducibles y comparables.	No cumple
	Integrar la planificación, diseño, implementación y supervisión de procedimientos de seguridad y controles para prevención y detección temprana de eventos dentro del proceso de admisión y la respuesta a incidentes.	No cumple
Supervisar y revisar el SGSI	Realizar revisiones periódicas del SGSI incluyendo las políticas, objetivos definidos en la etapa de concepción del SGSI	No cumple
	Realizar evaluaciones o auditorías al SGSI de forma periódica para determinar su cumplimiento e identificar mejoras en el proceso.	No cumple
	Registrar acciones y eventos que podrían tener impacto en la efectividad o desempeño del SGSI.	No cumple

Tabla 10.1.11 – Admisión. Evaluación de cumplimiento para proceso habilitador APO13

- **Nivel de madurez actual – Proceso Incompleto (0) – "N"**

  Según la norma ISO/IEC 15504 y la evaluación realizada, se determina que al no contar con una gestión de riesgos que encamine establecer un SGSI ni estrategias de seguridad de información, el nivel de madurez del habilitador es igual a cero (0).

  De acuerdo al nivel interno de madurez, ninguna de las sub-actividades son realizadas, por ello le corresponde la calificación "Not Achieved".

- **Nivel de madurez objetivo – Proceso Incompleto (0) – "L"**

  El objetivo establecido para la siguiente iteración de gobierno es mantenerse en el mismo nivel de madurez pero incrementando las actividades de gestión entregadas hasta llegar a una clasificación "Largely Achieved".

  Esto se debe a que el proceso de la implementación del SGSI debe ser realizado posterior a un análisis de riesgos, lo cual puede durar más del tiempo definido para volver a revisar el gobierno bajo el enfoque de seguridad de información.

e. <u>Proceso habilitador: Gestionar los programas y proyectos</u>

BAI01	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Mantener un enfoque estándar para la gestión de programas y proyectos.	Incorporar los requerimientos de seguridad de información dentro de los proyectos asociados al proceso de admisión.	No cumple
	Establecer procedimientos para asegurar que todos los proyectos relacionados al proceso e información cuentan con las medidas de seguridad requeridas o exigibles.	No cumple
	Actualizar el enfoque de gestión de programas y proyectos en base a mejoras a partir del uso de estas estrategias.	Cumple

Gestionar el compromiso de las partes interesadas.	Identificar como las partes interesadas se asocian a los proyectos relacionados con el proceso y comprometerlos para que se involucren y tomen medidas respecto a estos programas o proyectos.	Cumple
Desarrollar y mantener el plan del programa.	Desarrollar un plan de seguridad de información que incluya controles a implementar por parte del equipo de proyecto dentro del proceso.	No cumple
	Incluir recursos dentro del proyecto para identificar e implementar los requerimientos de seguridad de información.	No cumple
	Asignar la responsabilidad ejecutiva para cada proyecto en forma clara y sin ambigüedades, incluyendo beneficios, control de costos, la gestión de riesgos y la coordinación de las actividades de los proyectos.	Cumple
	Mantener el plan de programa para asegurar su actualización de acuerdo al proyecto y el proceso al que está asociado, así como la actualización del caso de negocio que lo justifica y garantiza el alineamiento estratégico.	Cumple, pero no mantiene un caso de negocio
Planificar proyectos	Integrar la seguridad de información y las tecnologías con la gestión de proyectos.	No cumple
	Desarrollar plan de proyecto con información que permita a la dirección controlar el progreso del proyecto. Incluir recursos, responsabilidades e hitos que marcan el cierre de cada una de las etapas.	Cumple
	Mantener los planes de proyecto y sus dependencias, asegurando la comunicación entre estos y que al realizar un cambio en uno de éstos se refleje en los demás.	Cumple
	Establecer un marco base para proyectos, el cual es revisado, aprobado e incorporado a los	Cumple

	planes de proyecto vigentes.	
Gestionar la calidad de los programas y proyectos.	Identificar las actividades y prácticas para garantizar la calidad de los proyectos. Asegurar que las tareas provean garantías del cumplimiento de los requerimientos definidos.	Cumple, pero sigue en proceso de desarrollo.
	Definir los requerimientos de validación y verificación de la calidad de entregables de los proyectos asociados al proceso.	Cumple
Gestionar el riesgo de los programas y proyectos.	Registrar riesgos de seguridad de información y las acciones correctivas frente a estos. Revisar y actualizar la matriz de riesgos de proyecto periódicamente.	Cumple, pero solo se gestionan riesgos a nivel de proyecto bajo un formato simple.
	Integrar proyectos de seguridad de información al programa y proceso de admisión de pacientes. Alinearlos a los procesos de gestión de proyectos.	No cumple
	Asignar la responsabilidad al personal con capacidades adecuadas para ejecutar el proceso de gestión del riesgo de los proyecto.	Cumple
Supervisar y controlar proyectos.	Determinar evaluaciones periódicas a los proyectos para asegurar que los requerimientos de seguridad de información asociados al proceso son implementados de forma efectiva.	No cumple
	Supervisar los cambios al programa y revisar requerimientos claves de desempeño para verificar el avance.	Cumple
	Obtener la aprobación y firma de los entregables producidos en cada iteración del proyecto asociado al proceso.	Cumple

Tabla 10.1.12 – Admisión. Evaluación de cumplimiento para proceso habilitador BAI01

- **Nivel de madurez actual – Proceso Incompleto (0) – "L"**

Según la norma ISO/IEC 15504 se determina que la falta de un enfoque de seguridad de información conlleva a que no puedan aplicarse todas las sub-actividades y exista una brecha respecto de cómo gestionar los proyectos de

acuerdo a un requerimiento de seguridad de información, por lo tanto el nivel de madurez actual es cero (0).

Se determina, dado la evidencia y la evaluación, se aplican una serie de sub-actividades de gestión y se evidencia tras una mejora a nivel de proceso de negocio y el cumplimiento de objetivos. Por ello su calificación es “Largely Achieved”.

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

El nivel de madurez objetivo para la siguiente revisión de gobierno de TI es de uno (1), para garantizar un alineamiento con seguridad de información y mejorar las prácticas de gestión dentro de la cartera de proyectos garantizando el alineamiento estratégico entre objetivos de TI y objetivos de negocio.

f. <u>Proceso habilitador: Gestionar el cambio</u>

BAI06	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Evaluar, priorizar y autorizar solicitudes de cambio	Asegurar que los cambios se ajustan a la política de seguridad de información.	No cumple
	Asegurar que se realice la evaluación del impacto potencial de los cambios en seguridad de información	No cumple
	Garantizar la aprobación del cambio por parte de los dueños del proceso de admisión, gestores de servicio y los respectivos stakeholders. Considerar los tipos de cambio para su aprobación.	Cumple
	Formalizar las solicitudes de cambio y estandarizarlas de manera que todo cambio a nivel del proceso sea a través de un procedimiento definido. Realizar la respectiva clasificación para identificar y mejorar la gestión.	Cumple
	Evaluar las solicitudes de manera estructurada	Cumple

	en base a su priorización y de acuerdo a las funciones del proceso. Realizar el análisis de impacto dentro de los planes y servicios que involucra este proceso considerando a los proveedores y los acuerdos de servicio.	
Gestionar cambios de emergencia	Desarrollar medidas para atender cambios de emergencia en el proceso de admisión a nivel de la seguridad de información.	Existen medidas para cambios de emergencia pero no alineados a la seguridad de información.
	Mantener un registro de los riesgos de seguridad de información a partir de cambios de emergencia realizados en el proceso.	No cumple
	Supervisar los cambios de emergencia dentro del proceso de admisión y realizar las revisiones post-implantación involucrando a las partes interesadas.	Cumple
Hacer seguimiento e informar cambios de estado	Mantener un sistema de seguimiento e informe para todas las solicitudes de cambio enfocados en seguridad de información dentro del proceso de admisión.	No cumple
	Supervisar los cambios de seguridad de información abiertos para asegurar que sean cerrados en los plazos previstos.	No cumple
	Elaborar los informes de cambio en seguridad de información dentro del proceso y que incluyan las métricas de rendimiento para facilitar su revisión y seguimiento	No cumple
Cerrar y documentar los cambios	Realizar la documentación sobre las revisiones de cambios de seguridad de información.	No cumple
	Definir un periodo válido para preservar la información sobre los cambios realizados dentro del proceso bajo los enfoques de seguridad.	No cumple

Tabla 10.1.13 – Admisión. Evaluación de cumplimiento para proceso habilitador BAI06

- **Nivel de madurez actual: Proceso incompleto (0) – "P"**

Según los requerimientos de la norma ISO/IEC 15504 y la evaluación sobre las sub-actividades de gestión para este proceso habilitador, se señala que alcanza un nivel de madurez igual a cero (0), debido a las falta del enfoque de seguridad que ocasiona inconsistencias en el proceso.

Evaluando el cumplimiento interno en el nivel de madurez, se determina la clasificación interna “Partially Achieved”, debido a la cantidad y los ítems de mejora que se evidencian dentro del proceso de admisión.

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

Para la siguiente corrida del gobierno de TI, se determina un nivel de madurez objetivo igual a uno (1) que garantice la entrega de todas las actividades para empezar a implementar mejoras a nivel de gestión para una de las revisiones posteriores a partir de métricas establecidas.

g. <u>Proceso habilitador: Gestionar los activos</u>

BAI09	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Identificar y registrar activos actuales	Identificar los activos asociados al proceso, registrarlos indicando su estado actual. Alinearlos con procesos de gestión de cambios y enfocarlos a la función de seguridad de información.	Cumple pero no están alineados a la seguridad de información
	Identificar requerimientos de seguridad de información de acuerdo a los activos del proceso de admisión. Tener en cuenta sus dependencias entre ellos.	No cumple
	Identificar requerimientos legales o reglamentarios sobre seguridad de información que deban de considerarse dentro de la gestión de activos del proceso.	No cumple
	Determinar si el activo proporciona valor dentro del proceso y si continúa en condiciones útiles	Cumple, pero solo se gestiona a nivel contable

	para soportar dicho proceso.	
Gestionar activos críticos	Garantizar el cumplimiento de requisitos de seguridad de información en los activos que comprenden el proceso.	No cumple
	Definir niveles de criticidad. De acuerdo a esto, identificar activos críticos y registrarlos. Esta evaluación deberá realizarse en torno a los requerimientos de seguridad de información.	Se identifican los niveles de seguridad pero no se alinea a requerimientos de seguridad de información.
	Considerar el riesgo de falla, necesidad de cambio o reemplazo total del activo crítico dentro del proceso para cumplir la función de seguridad de información.	No cumple
	Supervisar el rendimiento de los activos críticos por medio de evaluaciones o planes en los cuales se definan procesos para reparación o reemplazos.	Cumple
Gestionar el ciclo de vida de los activos	Identificar y comunicar los riesgos de seguridad de información y los incumplimientos respecto a las medidas para mitigarlos a lo largo del ciclo de vida de los activos del proceso de admisión.	No cumple
	Asegurar que las medidas de seguridad de información y los requerimientos estén alineados al ciclo de vida.	No cumple
	Realizar adquisiciones de activos en base a solicitudes aprobadas de acuerdo a las políticas y prácticas de la empresa bajo los criterios de la seguridad de información y alineados al proceso de admisión de pacientes.	No se tiene en cuenta criterios de seguridad de información, pero se siguen procedimientos de autorización.
	Eliminar activos de forma segura siguiendo procedimientos que garanticen la protección y destrucción de datos que alguna vez estuvieron almacenados en ellos.	Cumple en activos físicos, pero no existen procedimientos para destrucción de documentos
Administrar licencias	Establecer procedimientos de control en base a instalaciones de sistemas o software dentro de los activos de TI.	Cumple

	Mantener un registro de todas las licencias de software adquiridas para los activos que soportan el proceso base.	Cumple
	Realizar auditorías para identificar si existe software no autorizado o si se cumplen los mecanismos de control evidenciados en el inventario y registro de activos.	Cumple

Tabla 10.1.14 - Admisión. Evaluación de cumplimiento para proceso habilitador BAI09

- **Nivel de madurez actual: Proceso Incompleto (0) - "P"**

  De acuerdo a los lineamientos de la norma, el nivel de madurez identificado según el cumplimiento y entrega de las actividades del proceso habilitador, es igual a (cero), debido a que no se puede garantizar el alineamiento con las estrategias de seguridad de información y la ley de protección de datos personales. Dentro del habilitador, su estado o calificación interna, de acuerdo al cumplimiento de sus actividades entregadas, es "Partially Achieved".

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  El objetivo o meta definida por la organización es el nivel de madurez "Proceso ejecutado", lo cual indica cubrir y escalar todos los niveles del estado de madurez anterior y cerrar las brechas por no contar con una función de seguridad de información formalizada.

h. <u>Proceso habilitador: Gestionar las solicitudes e incidentes de servicio</u>

DSS02	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Definir esquemas de clasificación de incidentes y solicitudes de servicio	Definir y comunicar las características de los incidentes potenciales de seguridad de información para su reconocimiento y comprender el impacto que podría tener en el proceso.	No cumple
	Definir modelos de solicitudes de servicio	No cumple

	relacionados a la seguridad de información para facilitar la su atención y respuesta dentro del proceso de admisión.	
	Definir la clasificación y priorización de incidentes y solicitudes de servicio relacionados al proceso de admisión tomando en cuenta los requerimientos de seguridad de información.	No cumple
Registrar, clasificar y priorizar solicitudes e incidentes	Investigar los incidentes de seguridad y elaborar, en base a estos, procedimientos de respuesta. Asegurar que las medidas sean definidas y protejan los pilares de seguridad y que sean difundidas.	No cumple
	Registrar incidentes y solicitudes de servicio relacionados a la seguridad de información dentro del proceso de admisión.	No cumple
	Realizar la priorización y clasificación de los incidentes de acuerdo al impacto dentro del negocio y al proceso de admisión.	Cumple
Verificar, aprobar y resolver solicitudes de servicio	Seguir procedimientos y modelos de solicitudes para elementos frecuentes de seguridad de información, para así resolver solicitudes de forma estandarizada.	No cumple
Investigar, diagnosticar y localizar incidentes	Mantener procedimientos para recopilar evidencias sobre incidentes de acuerdo a requisitos externos y el marco legal al cual se encuentra sujeto el proceso. Asegurar que el personal esté al tanto de los requisitos.	Cumple
	Registrar un nuevo problema en caso no exista dentro de la base de datos y/o si el incidente de seguridad de información es recurrente.	No cumple
	Identificar posibles soluciones temporales o permanentes para los incidentes de seguridad de información, asignar su tratamiento a los especialistas respectivos.	No cumple

Resolver y recuperarse de incidentes	Definir un plan de respuesta para los incidentes de seguridad de información en el cual se detalla las soluciones apropiadas.	No cumple, no se identifican o clasifican incidentes de seguridad de información. Tienen un trato similar a los demás
	Ejecutar las acciones de recuperación para restablecer el proceso de admisión completamente.	Cumple
	Documentar la solución e identificar si es temporal o permanente para tomarlo en cuenta a futuro.	No cumple, no existe documentación
Cerrar solicitudes de servicio e incidentes	Verificar con los usuarios del proceso si se ha completado la solicitud del servicio o si el incidente ha sido resuelto. En caso afirmativo cerrar la solicitud o incidente.	Cumple
Seguir el estado y emitir informes	Asegurar que los incidentes de seguridad de información, el análisis y seguimiento de estos, siguen los procedimientos existentes.	No cumple
	Informar el resultado de las investigaciones sobre los incidentes de seguridad a las partes interesadas y a la gerencia ejecutiva.	No cumple
	Elaborar informes y distribuirlos periódicamente a los stakeholders como parte de la mejora continua.	Cumple, pero solo para la gerencia.

Tabla 10.1.15 – Admisión. Evaluación de cumplimiento para proceso habilitador DSS02

- **Nivel de madurez actual: Proceso Incompleto (0) - "N"**

De acuerdo a la ISO/IEC 15504, el nivel de madurez identificado para el proceso habilitador, es igual a (cero), debido a que no se identifica ni clasifican los incidentes de seguridad de información ni medidas para mitigación o investigación alrededor de estos. Dentro del habilitador, su estado o calificación interna, de acuerdo al cumplimiento de sus actividades entregadas, es "Not Achieved", ya que muchas de estas no pueden ser evidenciadas por la organización.

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

El objetivo o meta definida por la organización es el nivel de madurez “Proceso ejecutado”, garantizando la gestión de incidentes y solicitudes relacionadas a la seguridad de información alineados a los requerimientos y las políticas de esta función.

i. Proceso habilitador: Gestionar la continuidad

DSS04	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Definir las políticas de continuidad de negocio, objetivos y alcance	Determinar el nivel de criticidad del proceso de admisión de pacientes a nivel de seguridad de información y de acuerdo a la ley de protección de datos personales, norma técnica peruana de la historia clínica y ley de emergencia, para verificar que su aplicación en el programa de continuidad.	Cumple
	Asegurar que la seguridad de información forma parte del ciclo de vida de continuidad de negocio.	No cumple
	Identificar partes interesadas, roles y responsabilidades claves dentro del proceso para alinearlos a los objetivos y políticas del SGCN.	No cumple, Falta formalización
Mantener una estrategia de continuidad	Identificar e incluir escenarios que den pie a eventos que afecten la continuidad del proceso de admisión dentro del enfoque de la seguridad de información.	Cumple
	Realizar el análisis de impacto de negocio para el proceso de admisión, incluyendo los factores de seguridad de información y el máximo tolerable de interrupción en estos aspectos.	Cumple, pero solo a nivel de negocio y no de TI y seguridad de información.
	Analizar las amenazas que afecten la continuidad del proceso bajo el enfoque de la seguridad de información para mejorar métodos preventivos e incrementar la resiliencia.	No cumple

	Obtener la aprobación de los ejecutivos y dar pie a las estrategias seleccionadas que cubran los requerimientos definidos para el SGCN bajo el enfoque de seguridad de información.	No cumple, no está alineado a los enfoques de seguridad.
Desarrollar e implementar una respuesta a la continuidad de negocio	Alinear los aspectos de seguridad de información del proceso de admisión a las estrategias de continuidad y el SGCN. Incluirlas en el Plan de continuidad de negocios.	No cumple
	Asegurar que los proveedores clave del proceso definan estrategias de continuidad de negocio y recuperación. Evaluar cómo afecta que no se cuente con estas para considerarlo dentro de las políticas del SGCN.	No cumple
	Definir los procedimientos de recuperación para reanudar el proceso de admisión y que este cumpla con los requerimientos de seguridad de información definidos.	No cumple
	Definir y documentar recursos necesarios para recuperar el proceso, incluyendo todos los planes documentados y considerando las necesidades de seguridad y almacenamiento de la información en otro lugar. Distribuir los planes.	No cumple
Ejecutar, probar y revisar el plan de continuidad	Planificar actividades para probar el plan como está definido en los documentos. Asignar roles y responsabilidades para esta actividad.	No cumple
	Realizar el análisis y revisión para determinar el logro.	No cumple
Revisar, mantener y mejorar el plan de continuidad	Considerar que los incidentes de seguridad de información, dentro del proceso de admisión, son fuentes para probar y verificar las repuestas del plan de continuidad de negocios.	No cumple
	Revisar el plan periódicamente tomando en cuenta los objetivos de negocio, objetivos de TI y los lineamientos del proceso de admisión junto con sus estrategias de seguridad.	No cumple

	Considerar posibles cambios producto del entorno.	
	Comunicar los cambios en torno al plan de continuidad que puedan afectar los procesos o los requerimientos de seguridad de información	No cumple
Gestionar acuerdos de respaldo	Asegurar que los requerimientos de seguridad se cumplen en los procesos de backup y restauración de la información dentro del proceso de admisión de pacientes.	No cumple
	Realizar las copias de seguridad respectivas y establecer políticas para su gestión de acuerdo a las regulaciones y exigencias dentro del proceso de admisión, salvaguardando los datos del paciente.	Cumple
	Probar y mantener las copias de seguridad recientes y aquellas archivadas de manera periódica para garantizar la disponibilidad de la información y su integridad.	Se mantienen copias de seguridad pero no se realizan pruebas
Ejecutar revisiones post-reanudación	Asegurar que los parámetros y niveles de seguridad estén incluidos luego de la reanudación del proceso de admisión.	No cumple
	Evaluar la efectividad del plan de acuerdo a los tiempos definidos en el análisis de impacto de negocio de acuerdo al proceso de admisión.	No cumple
	Identificar debilidades u omisiones como parte de la mejora continua para asegurar que el proceso de admisión podrá llevarse a cabo sin inconvenientes ante cualquier evento bajo condiciones seguras.	No cumple

Tabla 10.1.16 – Admisión. Evaluación de cumplimiento para proceso habilitador DSS04

- **Nivel de madurez actual: Proceso Incompleto (0) - "N"**

De acuerdo a los lineamientos de la norma, el nivel de madurez identificado según el cumplimiento de las actividades del proceso habilitador, es igual a (cero), debido a que no se puede garantizar el alineamiento con las estrategias de

seguridad de información y no se cuenta con un plan de continuidad de negocio que abarque las tecnologías de información.

Dentro del habilitador, su estado o calificación interna, de acuerdo al cumplimiento de sus actividades entregadas, es “Not Achieved”, debido a la falta de entrega y comunicación de estos planes que impide incrementar el nivel interno de madurez.

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

El objetivo o meta definida por la organización es el nivel de madurez “Proceso ejecutado”, garantizando al final un plan de continuidad alineado a las estrategias de seguridad de información en beneficio de la empresa y cubriendo las regulaciones del entorno.

j. <u>Proceso habilitador: Gestionar los servicios de seguridad</u>

DSS05	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Proteger contra software malicioso	Instalar y activar herramientas de protección frente a software malicioso en todas las estaciones que procesan la información del paciente. Concientizar al usuario de estas sobre las amenazas y forzar la responsabilidad de prevención.	Cumple Instalación de antivirus.
	Revisar y evaluar sobre nuevas amenazas que afecten las fuentes de procesamiento de información de los pacientes.	Cumple, está automatizado por el servicio que brinda el antivirus.
	Filtrar el tráfico entrante, como los correos electrónicos y descargas para protegerse frente a información no solicitada y sensible.	Cumple.
Gestionar la seguridad de la red y las conexiones	De acuerdo al análisis de riesgo, mantener una política de seguridad para conexiones.	Cumple de acuerdo a un análisis de riesgo básico
	Cifrar la información en tránsito de acuerdo con su clasificación verificando el cumplimiento con la ley de protección de datos personales y norma técnica peruana de la historia clínica.	No cumple, no hay alineamiento con la ley de protección de datos personales.

	Establecer mecanismos para recepción segura de la información.	Cumple
	Realizar pruebas sobre la seguridad del sistema para determinar la protección sobre los datos intercambiados dentro del proceso de admisión de pacientes.	No cumple
Gestionar la seguridad de los puestos de usuario final	Configurar los sistemas operativos de forma correcta y segura en las estaciones que abarcan el proceso de admisión.	Cumple
	Cifrar la información almacenada y gestionada de acuerdo a su clasificación	No cumple
	Implementar mecanismos de bloqueo de los dispositivos.	Cumple
	Implementar el filtrado del tráfico de la red en dispositivos de usuario final dentro del proceso de admisión	Cumple. Se realiza a través del monitoreo.
	Deshacerse de los dispositivos de usuario final de forma segura.	Cumple
Gestionar la identidad del usuario y el acceso lógico	Mantener los derechos de acceso de los usuarios de acuerdo a los requerimientos del proceso de admisión.	Cumple
	Autenticar los accesos a los activos de información de acuerdo al nivel de seguridad y según los lineamientos de los procesos de negocio.	No cumple, se tiene acceso pero se restringe las carpetas disponibles por usuario.
	Segregar y gestionar cuentas de usuario privilegiadas.	Cumple
	Realizar revisiones periódicas de la gestión de cuentas y privilegios dentro del proceso de admisión. Verificar que la identificación de estas es unequívoca.	Cumple
Gestionar documentos sensibles y dispositivos de salida	Establecer procedimientos de empleo, eliminación y destrucción de las historias clínicas y actas de conformidad y garantía.	No cumple
	Asignar privilegios de acceso a información de historias clínicas, actas de conformidad y	No cumple

	garantía.	
	Realizar un inventario de documentos sensibles y dispositivos de salida críticos para llevar a cabo el proceso de admisión de pacientes.	No cumple
	Establecer políticas de protección física apropiadas sobre formularios o documentos que contienen información sensible.	No cumple

Tabla 10.1.17 – Admisión. Evaluación de cumplimiento para proceso habilitador DSS05

- **Nivel de madurez actual: Proceso Incompleto (0) - "P"**

  De acuerdo a los lineamientos de la norma, el nivel de madurez identificado para este proceso habilitador, es igual a (cero), debido a que los servicios de seguridad entregados no se alinean ni responden de acuerdo a necesidades formalizadas y establecidas de seguridad de información y la ley de protección de datos personales.

  Dentro del habilitador, su estado o calificación interna, de acuerdo al cumplimiento de sus actividades entregadas, es "Partially Achieved".

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  El objetivo o meta definida por la organización es el nivel de madurez "Proceso ejecutado", de manera que garanticen la existencia y el alineamiento con la función y requerimientos de seguridad de información producto de exigencias internas y aplicando sobre estas el cumplimiento regulatorio.

10.1.3 Proceso Atención del paciente

Se procede a verificar la aplicación y nivel de madurez de los habilitadores en el proceso de atención del paciente hospitalizado. Las regulaciones a las cuales se encuentra alineada es la ley de protección de datos personales y la norma técnica peruana de la historia clínica.

a. <u>Proceso habilitador: Gestionar la estrategia</u>

APO02	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Comprender la dirección de la empresa	Entender como la seguridad de información debe respaldar los objetivos de la organización dentro del proceso de atención al paciente hospitalizado, cumpliendo con la ley de protección de datos personales y la norma técnica peruana de la historia clínica.	Cumple pero no está documentado y tampoco formalizado ni alineado con ley de protección de datos personales.
	Identificar los stakeholders e interesados del proceso de atención y sus requerimientos.	Cumple, pero no está formalizado.
	Desarrollar y mantener un entendimiento de las estrategias, objetivos de negocio, entorno y retos operativos actuales dentro del proceso de admisión acorde con la seguridad de información.	No cumple, falta el alineamiento a la seguridad de información
	Determinar las prioridades para desarrollar los cambios estratégicos a nivel de proceso.	Cumple
Evaluar entorno, capacidades y rendimientos actuales	Establecer la línea base de seguridad de información dentro del proceso de atención al paciente.	No cumple
	Crear criterios de seguridad de información claros y relevantes dentro del proceso de atención de pacientes. Identificar los riesgos.	No cumple
	Identificar diferencias entre el proceso de negocio actual y las capacidades de TI según estándares de calidad y mejores prácticas.	Cumple, pero no está documentado
	Identificar debilidades, fortalezas, oportunidades y amenazas del proceso de atención y las capacidades y servicios para evaluar el desempeño actual de las funciones de seguridad de información.	No cumple
Realizar un análisis de brecha	Identificar dentro del proceso las brechas a cerrar y los cambios requeridos para llegar al nivel deseado.	Cumple

	Examinar el nivel de cumplimiento con la ley de protección de datos personales, norma técnica peruana de la historia clínica dentro del proceso de atención al paciente.	Cumple, pero no se adecúa a la ley de protección de datos personales
	Definir las metas deseadas del proceso y establecer los beneficios que se obtienen al llegar a estas.	Cumple, los responsables son la división de calidad y procesos
Definir el plan estratégico y la hoja de ruta	Definir la estrategia de seguridad de información y alinearla a la estrategia de negocio para cumplir los objetivos del proceso.	No cumple
	Crear la hoja de ruta que incluya la planificación e interdependencias de las iniciativas a nivel empresarial de acuerdo al proceso, la cual a su vez señale los riesgos y costos de los cambios.	No cumple
	Asegurar que el plan estratégico de TI y la hoja de ruta contengan los requerimientos de seguridad de información identificados en el proceso de atención.	No cumple
Comunicar la estrategia y la dirección de TI	Desarrollar el plan estratégico y el plan de seguridad de información que incluya el proceso de atención de pacientes y comunicarlo a los stakeholders.	Se tiene un plan estratégico institucional, pero no un plan de seguridad de información
	Desarrollar el plan de comunicación de la estrategia aplicada dentro del proceso de atención. Identificar canales de comunicación.	Cumple
	Actualizar el plan de comunicación según la retroalimentación del personal y a la estrategia de seguridad de información dentro del proceso de atención.	Cumple pero no sigue estrategias de seguridad de información

Tabla 10.1.18 - Atención. Evaluación de cumplimiento para proceso habilitador APO02

- **Nivel de madurez actual: Proceso Incompleto (0) – "P"**

De acuerdo a lo que especifica la norma ISO/IEC 15504, de acuerdo a la evidencia de actividades que han sido aplicadas para la mejora del proceso de

negocio, se determina que el nivel de madurez es cero (0), faltando aplicar las estrategias alineadas a la función de seguridad.

No obstante, realizando la evaluación interna, el habilitador tiene un logro parcial para el actual nivel de madurez.

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

El objetivo de la organización es que este proceso habilitador alcance una madurez de uno (1) para la siguiente revisión, por lo cual tendría que incluir los requerimientos de seguridad de información y alinear el proceso de acuerdo a la ley de protección de datos personales.

b. <u>Proceso habilitador: Gestionar los recursos humanos</u>

APO07	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Mantener la dotación del personal suficiente y adecuada	Evaluar periódicamente las necesidades de personal en el proceso de atención de pacientes de forma de asegurar que los recursos pueden soportar dicho proceso de negocio. Incluye evaluar necesidad de personal de TI.	Cumple
	Dentro de los procesos de contratación, incluir controles de antecedentes de acuerdo a la función o rol dentro del proceso de atención.	Cumple
	Asegurar que los requisitos de seguridad se incorporan en el proceso de contratación.	No cumple, no se tiene requisitos de seguridad
	Brindar capacitaciones y garantizar que existe personal capaz de cubrir funciones críticas de otro para reducir la dependencia.	Cumple
Identificar personal clave de TI	Asegurar la segregación de funciones en roles críticos del proceso.	Cumple
	Minimizar la dependencia de una sola persona en una función crítica dentro del proceso de	Cumple, pero no se documenta ni formaliza

	atención al paciente a través de captura e intercambio de conocimiento.	como compartir el conocimiento.
Mantener las habilidades y competencias del personal	Definir habilidades y competencias necesarias que deben tener los recursos para lograr los objetivos del proceso y poder escalar hacia los objetivos de alto nivel.	Cumple
	Brindar capacitaciones y programas de seguridad de información al personal que ejecuta los procesos.	No cumple
	Proporcionar facilidades a los actores de este proceso para lograr el desarrollo profesional para fomentar las oportunidades de progreso personal y menor dependencia de personas clave.	Cumple
	Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos. A partir de estas identificar si se requieren habilidades adicionales para cubrir el proceso y ejecutar el plan de acción para desarrollarlas.	Cumple
Evaluar el desempeño laboral de los empleados	Dentro de la evaluación del desempeño, considerar criterios con respecto a la función de seguridad de información.	No cumple
	Establecer objetivos individuales alineados con los objetivos del proceso de atención. Estos deben reflejar competencias básicas, valores empresariales y habilidades para las funciones.	Cumple
	Proporcionar instrucciones para uso y almacenamiento de información personal dentro del proceso de evaluación.	Cumple
	Desarrollar planes para la mejora de desempeño del personal que ejecuta el proceso de atención.	Cumple, pero no se formaliza el plan
	Implementar un proceso de reconocimiento a medida que el personal logre o desarrolle sus objetivos.	Cumple

Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio	Comprender la demanda actual y futura de recursos humanos involucrados dentro del proceso de atención para apoyar el logro de objetivos de TI y necesidades operativas del día a día salvaguardando los objetivos de la función de seguridad de información.	Cumple
	Realizar el inventario del personal del proceso e identificar sus respectivas funciones.	Cumple
	Mantener información adecuada sobre el tiempo dedicado a diferentes tareas, trabajos, servicios o proyectos	Cumple
Gestionar el personal contratado	Obtener un acuerdo formal por parte del personal sobre las políticas y requisitos de la seguridad de información a aplicarse en el proceso de atención al paciente.	Cumple
	Llevar a cabo revisiones para asegurarse que el personal cumple con sus funciones, que el derecho de acceso es adecuado y alineado con los acuerdos pactados al firmar el contrato.	Cumple
	Implementar políticas que permitan identificar como se debe gestionar el personal, es decir si es necesario contratar servicios o nuevo personal siguiendo los parámetros de seguridad de información.	No cumple, no está de acorde a niveles de seguridad de información.

Tabla 10.1.19 - Atención. Evaluación de cumplimiento para proceso habilitador APO07

- **Nivel de madurez actual: Proceso Implementado (0) - "L"**

  Según lo que establece la norma 15504, se determinar que el nivel de madurez es (cero) y con un nivel interno igual a "Largely Achieved". Esto se debe a que el proceso no puede ser totalmente implementado debido a la falta de la función de seguridad de información que permita alinear estrategias y políticas de acuerdo a la gestión del personal.

- **Nivel de madurez objetivo: Proceso Gestionado (2)**

Debido al entorno de negocio, la organización determina que el siguiente nivel de madurez a escalar es a un proceso gestionado, debido a regulaciones y a lo que el proceso demanda. Al ser la atención un proceso cuyos actores realizan actividades manuales críticas, se requiere afianzar este aspecto de seguridad.

c. <u>Proceso habilitador: Gestionar el riesgo</u>

APO12	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Recopilar datos	Identificar y recolectar datos para la identificación, análisis y comunicación de los riesgos de seguridad de información dentro del proceso de atención al paciente.	No cumple, la gestión de riesgos es un proyecto a futuro en la organización.
	Medir y analizar los riesgos de TI y seguridad de información suscitados dentro del proceso de atención a lo largo del tiempo. Verificar las pérdidas experimentadas por la materialización de estos.	No cumple
	Ejecutar análisis del entorno para verificar los factores de riesgo que se presentan en el proceso.	Cumple
Analizar el riesgo	Identificar, analizar y evaluar los riesgos de información dentro del proceso.	No cumple
	Construir los escenarios de riesgo de TI y seguridad dentro del proceso. Identificar las amenazas para detectar medidas de emergencia.	No cumple, pero se detectan algunas medidas de emergencia
	Identificar los riesgos residuales dentro del proceso y las exposiciones que puedan requerir una respuesta al riesgo.	No cumple
	Especificar controles apropiados para la mitigación de riesgos de seguridad de información que garanticen que el proceso se	No cumple

	vea afectado lo mínimo posible.	
	Validar los resultados del análisis de riesgos del proceso antes de usarlos para la toma de decisiones. Verificar alineamiento con requerimientos organizacionales.	No cumple
Mantener un perfil del riesgo	Crear e informar el nivel aceptable de exposición al riesgo que incluya los aspectos de seguridad de acuerdo al proceso.	No cumple
	Identificar dentro del proceso los servicios esenciales para sostenerlo y que este alineado con el perfil de riesgo a tolerar. Analizar dependencias e identificar debilidades.	No cumple, se identifican los servicios críticos
	Definir un conjunto de indicadores que permitan la supervisión de los riesgos de seguridad del proceso y sus tendencias.	No cumple
Expresar el riesgo	Informar los resultados del análisis de riesgos del proceso de atención a los stakeholders en términos adecuados y entendibles para decisiones empresariales.	No cumple
	Informar el perfil del riesgo a los stakeholders junto con la efectividad del proceso de atención y los controles asociados. Identificar oportunidades de TI para mayor tolerancia al riesgo e incrementar la capacidad de gestión.	No cumple
Definir un portafolio de acciones para la gestión de riesgos	Monitorear periódicamente los riesgos de seguridad de información del proceso de atención y verificar que el riesgo este alineado con el apetito y tolerancia al riesgo.	No cumple
	Definir propuestas para reducir el riesgo o proyectos para incrementar las oportunidades estratégicas de acuerdo a la ley de protección de datos personales y la norma técnica peruana de la historia clínica.	No cumple

Responder al riesgo	Aplicar las prácticas y controles para la mitigación de riesgos de seguridad. Se recomienda aplicar en este caso la norma ISO/IEC 27002:2013. Se recomienda incluir controles preventivos y correctivos.	No cumple

Tabla 10.1.20 - Atención. Evaluación de cumplimiento para proceso habilitador APO12

- **Nivel de madurez actual – Proceso Incompleto (0) – "N"**

  Tomando en cuenta que dentro de la organización no existe un tratamiento de riesgos de negocio, de TI y específicamente de seguridad de información, se considera que este proceso habilitador está incompleto.

  Dado a que no se presenta evidencias sobre las sub-actividades realizadas y solo tienen algunas iniciativas sobre como evaluar el entorno y los incidentes, dentro del nivel de madurez le corresponde la categoría de "Not Achieved".

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

  Para la siguiente iteración de gobierno se pretende alcanzar un nivel de madurez equivalente a uno (1), debido a que este proceso será una de las bases para el enfoque de seguridad de información y requiere ser priorizado para este proceso de negocio.

d. <u>Proceso habilitador: Gestionar la seguridad</u>

APO13	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Establecer y mantener un SGSI	Definir el alcance del SGSI de acuerdo a las características de la organización y sus políticas.	No cumple
	Diseñar un enfoque de gestión de seguridad y alinearlo al SGSI.	
	Comunicar los roles y responsabilidades en la gestión de la seguridad de información y el enfoque del SGSI.	No cumple

	Comprometer a la alta dirección para iniciar las actividades de implementación del SGSI.	No cumple
Definir y gestionar un plan de tratamiento del riesgo de la seguridad de información	Diseñar, mantener y aplicar un plan de tratamiento de riesgos de seguridad de información alineados con los objetivos estratégicos de la organización y fines del proceso.	No cumple
	Desarrollar propuestas de mejora al plan de riesgos basados en casos de negocio de acuerdo a los roles y responsabilidades a necesitar para su aplicación y acorde a los drivers identificados.	No cumple
	Integrar la planificación, diseño, implementación y supervisión de procedimientos de seguridad y controles para prevención y detección temprana de eventos dentro del proceso de atención y la respuesta a incidentes.	No cumple
Supervisar y revisar el SGSI	Realizar revisiones periódicas del SGSI incluyendo las políticas y objetivos definidos en la etapa de concepción del SGSI	No cumple
	Realizar evaluaciones o auditorías al SGSI de forma periódica para determinar su cumplimiento e identificar mejoras en el proceso.	No cumple
	Registrar acciones y eventos que podrían tener impacto en la efectividad o desempeño del SGSI.	No cumple

Tabla 10.1.21 - Atención. Evaluación de cumplimiento para proceso habilitador APO13

- **Nivel de madurez actual – Proceso Incompleto (0) – "N"**

  Según la norma ISO/IEC 15504 y la evaluación realizada, se determina que al no contar con una gestión de riesgos que encamine establecer un SGSI ni estrategias de seguridad de información, el nivel de madurez del habilitador es igual a cero (0).

De acuerdo al nivel interno de madurez, ninguna de las sub-actividades son realizadas, por ello le corresponde la calificación “Not Achieved”.

- **Nivel de madurez objetivo – Proceso Incompleto (0) – “L”**

  El objetivo establecido para la siguiente iteración de gobierno es mantenerse en el mismo nivel de madurez pero incrementando las actividades de gestión entregadas hasta llegar a una clasificación “Largely Achieved”, para seguir la secuencia del análisis de riesgos.

e. <u>Proceso habilitador: Gestionar los programas y proyectos</u>

BAI01	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Mantener un enfoque estándar para la gestión de programas y proyectos.	Incorporar los requerimientos de seguridad de información dentro de los proyectos asociados al proceso de atención.	No cumple
	Establecer procedimientos para asegurar que todos los proyectos relacionados al proceso e información cuentan con las medidas de seguridad requeridas o exigibles.	No cumple
	Actualizar el enfoque de gestión de programas y proyectos. Aplicar las mejoras que se desprenden del uso de estrategias dentro del proceso de atención.	Cumple
Desarrollar y mantener el plan del programa.	Desarrollar un plan de seguridad de información que incluya los controles a implementar en el proyecto.	No cumple
	Incluir recursos dentro del proyecto para identificar e implementar requerimientos de seguridad de información.	No cumple
	Mantener el plan de programa para asegurar su actualización de acuerdo a los proyectos y el proceso de atención. Actualizar el caso de negocio que lo justifica y garantiza el alineamiento estratégico.	Cumple, pero no actualiza el business case

Planificar proyectos	Integrar la seguridad de información y las tecnologías con la gestión de proyectos de negocio.	No cumple
	Desarrollar un plan de proyecto con información que permita a la dirección controlar su progreso. Incluir recursos, responsabilidades e hitos que marcan el cierre de cada una de las etapas.	Cumple
	Mantener los planes de proyectos y sus dependencias, asegurando la comunicación entre estos y que al realizar un cambio en uno de éstos se refleje en los demás.	Cumple
	Establecer un marco base para gestión de proyectos, el cual es revisado, aprobado e incorporado a los planes de proyecto vigentes.	Cumple
Gestionar la calidad de los programas y proyectos.	Identificar actividades y prácticas para garantizar la calidad de los proyectos. Asegurar que las tareas cumplan los requerimientos de seguridad de información	Cumple, pendiente de desarrollo y alineamiento con seguridad de información.
Gestionar el riesgo de los programas y proyectos.	Registrar los riesgos de seguridad de información del proyecto y sus acciones correctivas. Revisar y actualizarlos periódicamente.	Cumple, matriz de riesgo a nivel de proyecto
	Integrar proyectos de seguridad de información al programa y proceso de atención de pacientes. Alinearlos a los procesos de gestión de proyectos.	No cumple
	Asignar responsabilidades al personal capacitado para la gestión del riesgo de los proyectos.	Cumple
Supervisar y controlar proyectos.	Programar evaluaciones a los proyectos para asegurar que los requerimientos de seguridad de información del proceso son implementados efectivamente.	No cumple
	Supervisar los cambios al programa y revisar requerimientos de desempeño para verificar el	Cumple

	avance.	
	Obtener la aprobación y firma de los entregables producidos en cada iteración de los proyectos asociados.	Cumple

Tabla 10.1.22 - Atención. Evaluación de cumplimiento para proceso habilitador BAI01

- **Nivel de madurez actual – Proceso Incompleto (0) – "L"**

  Según la norma ISO/IEC 15504 se determina que la falta de un enfoque de seguridad de información conlleva a que no puedan aplicarse todas las sub-actividades y exista una brecha respecto a los requerimientos de seguridad de información, por lo tanto el nivel de madurez actual es cero (0).

  Se determina, dado la evidencia y la evaluación, se aplican una serie de sub-actividades de gestión y se evidencia tras una mejora a nivel de proceso de negocio y el cumplimiento de objetivos. Por ello su calificación es "Largely Achieved".

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

  El nivel de madurez objetivo para la siguiente revisión de gobierno de TI es de uno (1), para garantizar un alineamiento con seguridad de información y mejorar las prácticas de gestión de proyectos garantizando el alineamiento estratégico.

f. <u>Proceso habilitador: Gestionar el cambio</u>

BAI06	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Evaluar, priorizar y autorizar solicitudes de cambio	Asegurar que los cambios dentro del proceso de atención se alinean a las políticas de seguridad de información.	No cumple
	Realizar el análisis de impacto al realizar cambios en seguridad de información y a nivel general dentro del proceso.	No cumple
	Asegurar que los cambios sean validados por los dueños del proceso de negocio de atención	Cumple

	al paciente. Evaluar los tipos de cambios permitidos en él.	
	Estandarizar las solicitudes de cambio de manera que todo cambio a nivel del proceso sea a través de procedimientos formales.	Cumple
	Considerar el impacto de los cambios en la gestión de proveedores de acuerdo a la de seguridad de información, procurando que estos no afecten los acuerdos de servicio.	No cumple
Gestionar cambios de emergencia	Desarrollar medidas para atender cambios de emergencia en el proceso y relacionados a seguridad de información.	Existen medidas para atender los cambios de emergencia, pero no se relacionan o alinean a la seguridad de información
	Registrar los riesgos de seguridad de información a partir de cambios de emergencia realizados en el proceso.	No cumple
	Supervisar los cambios de emergencia dentro del proceso de atención y realizar las revisiones post-implantación involucrando a las partes interesadas.	Cumple
Hacer seguimiento e informar cambios de estado	Mantener y supervisar un sistema de seguimiento e informe para las solicitudes de cambio del proceso de acuerdo a las exigencias de seguridad de información.	No cumple
	Elaborar informes respecto a los cambios de seguridad de información realizados en el proceso.	No cumple
	Supervisar los cambios de seguridad de información que aún no han sido cerrados.	No cumple

Tabla 10.1.23 - Atención. Evaluación de cumplimiento para proceso habilitador BAI06

- **Nivel de madurez actual: Proceso incompleto (0) – "N"**

Según los requerimientos de la norma ISO/IEC 15504 y la evaluación sobre las sub-actividades de gestión para este proceso habilitador, se señala que alcanza

un nivel de madurez igual a cero (0), debido a las falta del enfoque de seguridad que ocasiona inconsistencias en el proceso.

Evaluando el cumplimiento interno en el nivel de madurez, se determina la clasificación interna “Not Achieved”.

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

Para la siguiente corrida del gobierno de TI, se determina un nivel de madurez objetivo igual a uno (1) que garantice la entrega de todas las actividades para empezar a implementar mejoras a nivel de gestión.

g. Proceso habilitador: Gestionar los activos

BAI09	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Identificar y registrar activos actuales	Identificar los activos relacionados al proceso de atención al paciente hospitalizado y los requerimientos de seguridad asociados a estos.	Se identifican activos pero no se alinean a requerimientos de seguridad de información.
	Identificar la dependencia entre estos activos y su nivel de criticidad dentro del proceso.	Cumple
	Identificar si los activos del proceso de atención están sujetos a alguna regulación adicional a la ley de protección de datos personales y la norma técnica peruana de la historia clínica. Verificar los aspectos contractuales de seguridad de información.	No cumple
	Verificar y determinar si los activos se encuentran en condiciones útiles para soportar dicho proceso y si es que genera valor al negocio.	Cumple, pero el valor solo es a nivel contable
Gestionar activos críticos	Identificar que activos del proceso de atención pueden ser considerados como crítico. Supervisar su rendimiento por medio de evaluaciones o planes en los que se definan las políticas de reparación o reemplazo.	Cumple

	Determinar los niveles de criticidad de los activos dentro del proceso de atención.	Cumple
	Garantizar que los activos críticos del proceso cumplan los niveles de seguridad de información establecidos en el proceso y el negocio.	No cumple
	Determinar el tiempo de inactividad máximo para estos activos críticos de manera que se garantice la reducción de un impacto adverso en el negocio.	Cumple, pero no se prueba que el tiempo definido sea el adecuado
	Establecer políticas para el cambio de estos activos críticos de acuerdo a los riesgos de seguridad de información identificados.	No cumple
Gestionar el ciclo de vida de los activos	Identificar y comunicar los riesgos de seguridad de información de estos activos que soportan el proceso.	No cumple
	Realizar adquisiciones de nuevos activos previamente autorizadas de acuerdo a procedimientos seguros que verifique un nivel de riesgo aceptable.	Cumple, pero no toma en cuenta los criterios de seguridad de información
	Establecer políticas para eliminar activos de forma segura.	Cumple
	Asegurar que las medidas de seguridad de información se apliquen a los activos durante todo su ciclo de vida.	No cumple

Tabla 10.1.24 - Atención. Evaluación de cumplimiento para proceso habilitador BAI09

- **Nivel de madurez actual: Proceso incompleto (0) – "P"**

  De acuerdo a los criterios de la norma ISO/IEC 15504 y la evaluación sobre las sub-actividades de gestión para este proceso habilitador, se señala que alcanza un nivel de madurez igual a cero (0) al no existir una congruencia con los requerimientos de seguridad de información y posibles incidentes que puedan afectar directamente a los activos críticos definidos.

Evaluando el cumplimiento interno en el nivel de madurez, se determina la clasificación interna “Partially Achieved” por la evidencia mostrada en la entrega y desarrollo de este proceso habilitador.

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

Para la siguiente corrida del gobierno de TI, se determina un nivel de madurez objetivo igual a uno (1) que garantice la entrega de todas las actividades para empezar a implementar mejoras a nivel de gestión y además verificando requerimientos y alineamiento con estrategias de seguridad de información sobre los activos de los procesos.

h. Proceso habilitador: Gestionar las solicitudes de servicio e incidentes

DSS02	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Definir esquemas de clasificación de incidentes y solicitudes de servicio	Definir y comunicar las características de los potenciales incidentes de seguridad de información para su reconocimiento y entendimiento del impacto en caso se materialicen.	No cumple
	Definir modelos de solicitudes de servicio relacionados a la seguridad de información para facilitar su atención y respuesta dentro del proceso de atención.	No cumple
	Definir la clasificación y priorización de incidentes y solicitudes de servicio relacionados al proceso de atención de acuerdo a los requerimientos de seguridad de información y el impacto en el negocio.	No cumple
Registrar, clasificar y priorizar solicitudes e incidentes	Investigar los incidentes de seguridad y elaborar, en base a estos, procedimientos de respuesta. Asegurar que las medidas sean definidas y protejan los pilares de seguridad y que sean difundidas.	No cumple
	Registrar incidentes y solicitudes de servicio relacionados a la seguridad de información del	No cumple

	proceso de atención.	
	Priorizar y clasificar incidentes de acuerdo al impacto dentro del negocio y el proceso de atención.	Cumple
Verificar, aprobar y resolver solicitudes de servicio	Seguir procedimientos y modelos de solicitud de seguridad de información para elementos frecuentes de manera que se atiendan en menor tiempo.	No cumple
Investigar, diagnosticar y localizar incidentes	Registrar un nuevo problema en caso no exista dentro de la base de datos y si el incidente de seguridad de información satisface los criterios para registro.	No cumple
	Identificar soluciones temporales o permanentes para los incidentes de seguridad de información, asignar su tratamiento a los especialistas respectivos dentro del proceso de atención.	No cumple
Resolver y recuperarse de incidentes	Definir un plan de respuesta de seguridad de información para los incidentes dentro del proceso de atención.	No cumple
	Ejecutar las acciones de recuperación para restablecer el proceso de atención completamente.	Cumple
	Documentar la solución e identificar si es temporal o permanente para tomarlo en cuenta a futuro.	No cumple, no existe documentación
Cerrar solicitudes de servicio e incidentes	Verificar con los usuarios del proceso si se ha completado la solicitud del servicio o si el incidente de seguridad fue resuelto. En caso afirmativo cerrar la solicitud o incidente.	Cumple
Seguir el estado y emitir informes	Asegurar que los incidentes de seguridad de información, el análisis y seguimiento de estos, siguen los procedimientos de gestión	No cumple

	existentes.	
	Elaborar informes y distribuirlos periódicamente a los stakeholders como parte de la mejora continua.	Cumple, pero solo se comunica a la gerencia

Tabla 10.1.25 - Atención. Evaluación de cumplimiento para proceso habilitador DSS02

- **Nivel de madurez actual: Proceso incompleto (0) – "N"**

  De acuerdo a los criterios de la norma ISO/IEC 15504, este proceso habilitador alcanza un nivel de madurez igual a cero (0). Se debe de tomar en cuenta que la brecha a cerrar corresponde a la identificación de los incidentes y requerimientos de seguridad de información.

  Evaluando el cumplimiento interno en el nivel de madurez, se determina la clasificación interna "Not Achieved".

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

  Para la siguiente corrida del gobierno de TI, se determina un nivel de madurez objetivo igual a uno (1), asegurando la formalización de un enfoque de seguridad que permita una mejor entrega de servicio alineado a requerimientos legales.

i. <u>Proceso habilitador: Gestionar la continuidad</u>

DSS04	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Definir las políticas de continuidad de negocio, objetivos y alcance	Determinar la criticidad del proceso de atención de pacientes de acuerdo a la seguridad de información y el cumplimiento con la ley de protección de datos personales y la norma técnica peruana de la historia clínica para verificar si forma parte del programa de continuidad.	Cumple
	Asegurar que la seguridad de información forma parte del ciclo de vida de continuidad de negocio.	No cumple

	Identificar interesados, roles y responsabilidades dentro del proceso para alinearlos a los objetivos y políticas del SGCN	No cumple
Mantener una estrategia de continuidad	Identificar e incluir escenarios que den pie a eventos de información que afecten la continuidad del proceso.	Cumple
	Realizar el análisis de impacto de negocio de acuerdo a los lineamientos del proceso, incluyendo los factores de seguridad de información y el máximo tolerable de interrupción en estos aspectos.	Cumple pero a nivel de negocio, falta implementar estrategias de continuidad a nivel de TI
	Analizar las amenazas de seguridad que afecten la continuidad del proceso para mejorar métodos preventivos e incrementar la resiliencia.	No cumple
Desarrollar e implementar una respuesta a la continuidad de negocio	Definir los procedimientos de recuperación para reanudar el proceso de egreso y que cumpla con los requerimientos de seguridad de información definidos.	No cumple
	Definir y documentar recursos necesarios para recuperar el proceso. Documentar los planes considerando las necesidades de seguridad y almacenamiento de la información en otro lugar. Distribuir los planes.	No cumple
Ejecutar, probar y revisar el plan de continuidad	Planificar actividades para probar el plan definido en los documentos. Asignar roles y responsabilidades para esta actividad y coordinar que no afecten el proceso.	No cumple
	Realizar el análisis y revisión para determinar el logro.	No cumple
Revisar, mantener y mejorar el plan de continuidad	Revisar el plan periódicamente tomando en cuenta los objetivos de negocio, objetivos de TI y los lineamientos del proceso de atención. Considerar posibles cambios producto del entorno.	No cumple
	Comunicar los cambios del plan de continuidad	No cumple

	que puedan afectar el proceso o los requerimientos de seguridad de información	
	Reconocer qué incidentes de seguridad de información pueden ocasionar la interrupción del negocio, por ello se debe incrementar el nivel de gestión de éstos.	No cumple
Gestionar acuerdos de respaldo	Asegurar que los requerimientos de seguridad se cumplen en los procesos de backup y restauración de información.	No cumple
	Realizar las copias de seguridad respectivas y establecer políticas para su gestión de acuerdo a la ley de protección de datos personales y la norma técnica peruana de la historia clínica entre otras exigencias dentro del proceso de atención, salvaguardando los datos del paciente.	No cumple, pero se realizan copias de seguridad y backup de datos
	Probar y mantener las copias de seguridad recientes, y aquellas archivadas, de manera periódica para garantizar la disponibilidad de la información y su integridad.	No cumple
Ejecutar revisiones post-reanudación	Evaluar la efectividad del plan de acuerdo a los tiempos definidos en el análisis de impacto de negocio de acuerdo al proceso de atención al paciente.	No cumple
	Identificar debilidades u omisiones como parte de la mejora continua para asegurar que el proceso de atención podrá llevarse a cabo sin inconvenientes ante cualquier evento asegurando la información de los involucrados.	No cumple

Tabla 10.1.26 - Atención. Evaluación de cumplimiento para proceso habilitador DSS04

- **Nivel de madurez actual – Proceso Incompleto (0) – "N"**

De acuerdo a los requerimientos de la norma, el nivel de madurez identificado para el proceso habilitador es igual a cero (0), debido a la falla y falta de un alineamiento a la seguridad de información y estrategias de recuperación de TI.

Dentro de la escala interna de madurez, el habilitador obtiene la calificación de "Not Achieved", pues no muestra mayor evidencia sobre su cumplimiento.

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

El objetivo trazado, es un nivel de madurez igual a uno (1) debido a que se debe de cumplir la regulación respectiva y alineamiento a la seguridad de información. El plan de continuidad de TI se encuentra en proyecto para complementar los proyectos existentes en la organización.

j. Proceso habilitador: Gestionar los servicios de seguridad

DSS05	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Proteger contra software malicioso	Instalar y activar herramientas de protección frente a software malicioso en las estaciones o activos que brindan soporte al proceso de atención. Concientizar al usuario sobre el empleo de estas.	Cumple
	Filtrar el tráfico entrante de información como correos electrónicos y descargas para protegerse frente a información no solicitada.	Cumple
Gestionar la seguridad de la red y las conexiones	Mantener una política para la seguridad de conexiones de red entre los activos que soportan el proceso de atención.	No cumple
	Cifrar la información en tránsito de acuerdo con su clasificación verificando el cumplimiento la ley de protección de datos personales.	No cumple
Gestionar la seguridad de los puestos de usuario final	Cifrar la información almacenada dentro de los activos de acuerdo a su clasificación y nivel de criticidad.	No cumple
	Configurar los sistemas operativos de forma correcta y segura en las estaciones del personal que ejecuta el proceso de atención.	Cumple
	Implementar mecanismos de bloqueo en los	Cumple

	dispositivos.	
	Deshacerse de los dispositivos de usuario final de forma segura.	Cumple
Gestionar la identidad del usuario y el acceso lógico	Según los requerimientos del proceso, mantener los derechos de acceso	Cumple
	Segregar y gestionar cuentas de usuario privilegiadas.	Cumple
	Realizar regularmente revisiones de la gestión de cuentas y privilegios que abarca el proceso de atención. Verificar que la identificación de estas es unequívoca.	Cumple
Gestionar documentos sensibles y dispositivos de salida	Establecer procedimientos de empleo, eliminación y destrucción de formularios especiales como las historias clínicas y actas de conformidad.	No cumple
	Asignar privilegios de acceso a documentación y a su modificación durante el proceso de atención al paciente.	No cumple
	Realizar un inventario de documentos sensibles o dispositivos de salida críticos involucrados durante el proceso de atención.	No cumple
	Establecer políticas de protección física apropiadas sobre formularios o documentos que contienen información sensible.	No cumple

Tabla 10.1.27 - Atención. Evaluación de cumplimiento para proceso habilitador DSS05

- **Nivel de madurez actual: Proceso Incompleto (0) - "P"**

  De acuerdo a los lineamientos de la norma, el nivel de madurez identificado para este proceso habilitador, es igual a (cero), debido a que los servicios no se alinean a requerimientos de seguridad de información y la ley de protección de datos personales.

  Dentro del habilitador, su estado o calificación interna, de acuerdo al cumplimiento de sus actividades entregadas, es "Partially Achieved".

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  El objetivo o meta definida por la organización es el nivel de madurez “Proceso ejecutado”, de manera que garanticen la existencia y el alineamiento con la función y requerimientos de seguridad de información producto de exigencias internas y aplicando sobre estas el cumplimiento regulatorio.

10.1.4 Proceso Egreso del paciente

Se presenta el estado de cumplimiento de las sub-actividades para cada actividad de gestión de los procesos habilitadores alineadas al proceso de negocio. Las regulaciones a cumplir en este caso son la ley de protección de datos personales, Ley de emergencia y la norma técnica peruana de la historia clínica.

a. <u>Proceso habilitador: Gestionar la estrategia</u>

APO02	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Comprender la dirección de la empresa	Entender como la seguridad de información debe respaldar los objetivos de la organización y del proceso. Garantizar con estos el cumplimiento de la ley de protección de datos personales y la norma técnica peruana de la historia clínica.	Cumple pero no está documentado y tampoco formalizado ni alineado con ley de protección de datos personales.
	Desarrollar y entender las estrategias, objetivos de negocio, entorno y retos operativos actuales dentro del proceso y la seguridad de información.	No cumple, no alineamiento a seguridad de información
	Determinar prioridades para desarrollar cambios estratégicos en el proceso.	Cumple
Evaluar entorno, capacidades y rendimientos actuales	Establecer la línea base de seguridad de información dentro del proceso egreso del paciente.	Cumple
	Crear criterios de seguridad de información claros y relevantes de acuerdo con las actividades del proceso de egreso. Identificar	No cumple

	riesgos.	
	Identificar diferencias entre el proceso de negocio actual y las capacidades de TI según estándares y mejores prácticas sugeridas por la división calidad y procesos.	Cumple, pero no lo documenta
	Identificar debilidades, fortalezas, oportunidades y amenazas del entorno actual del proceso de egreso Evaluar dentro de él el desempeño de la función de seguridad de información.	No cumple
Realizar un análisis de brecha	Identificar dentro del proceso las brechas a cerrar y los cambios requeridos para llegar al nivel deseado.	Cumple
	Examinar el nivel de cumplimiento con la ley de protección de datos personales, norma técnica peruana de la historia clínica y la ley de emergencia dentro del proceso de egreso al paciente.	Cumple, pero no alinea a la ley de protección de datos personales
	Definir las metas del proceso y establecer los beneficios que se obtienen al llegar a estas.	Cumple. Responsable: área calidad y procesos
Definir el plan estratégico y la hoja de ruta	Definir la estrategia de seguridad de información y alinearla a la estrategia de negocio para cumplir los objetivos del proceso.	No cumple
	Crear la hoja de ruta que incluya la planificación e interdependencias de las iniciativas a nivel empresarial de acuerdo al proceso, la cual a su vez señale los riesgos y costos de los cambios.	No cumple
	Asegurar que el plan estratégico de TI y la hoja de ruta contengan requerimientos de seguridad de información identificados para el proceso de egreso.	No cumple
Comunicar la estrategia y la dirección de TI	Desarrollar el plan estratégico y el plan de seguridad de información que incluya el proceso de egreso de pacientes y comunicarlo a los stakeholders.	Se cuenta con un plan estratégico institucional, pero no un plan de seguridad de información.
	Tomando como base el plan de comunicación de otros procesos como el de atención y el de	Cumple pero no se alinea a los requerimientos de

	admisión, actualizar el plan según los resultados en el personal que realiza el proceso de egreso del paciente.	seguridad de información.

Tabla 10.1.28 - Egreso. Evaluación de cumplimiento para proceso habilitador APO02

- **Nivel de madurez actual – Proceso Incompleto (0) – "P"**

  Según la norma ISO/IEC 15504 se determina que la falta de un enfoque de seguridad de información impide el cumplimiento de todas las sub-actividades y existe una brecha respecto a estrategias de negocio y seguridad de información, por lo tanto el nivel de madurez actual es cero (0). Se determina, dado la evidencia y la evaluación, se aplican una serie de sub-actividades de gestión y se evidencia tras una mejora a nivel de proceso de negocio y el cumplimiento de objetivos. Por ello su calificación es "Partially Achieved".

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

  El nivel de madurez objetivo para la siguiente revisión de gobierno de TI es de uno (1), para garantizar un alineamiento con seguridad de información y estrategia de negocio, que permitan evolucionar posteriormente a otros niveles de madurez.

b. <u>Proceso habilitador: Gestionar los recursos humanos</u>

APOO7	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Mantener la dotación del personal suficiente y adecuada	Evaluar periódicamente las necesidades de personal en el proceso de egreso de pacientes, de manera de asegurar que estos recursos puedan realizar con éxito el proceso de negocio. Incluye la evaluación de necesidad de nuevo personal de TI.	Cumple
	Dentro de los procesos de contratación, incluir controles de antecedentes de acuerdo a la función o rol dentro del proceso de egreso.	Cumple
	Asegurar que los requisitos de seguridad se incorporan en el proceso de contratación.	No cumple, no existen requerimientos de

		seguridad de información
	Asegurar que existe personal capaz de cubrir funciones críticas de otro para reducir la dependencia en el proceso de egreso.	Cumple
Identificar personal clave de TI	Asegurar la segregación de funciones en roles críticos del proceso.	Cumple
	Tomar acciones o medidas para la gestión de cambios de personal, en especial en los temas de despido.	Cumple
	Minimizar la dependencia en una sola persona en una función crítica dentro del proceso de egreso del paciente a través de captura e intercambio de conocimiento.	Cumple, pero no se documenta ni formaliza como compartir el conocimiento.
Mantener las habilidades y competencias del personal	Definir habilidades y competencias necesarias de los recursos para lograr los objetivos dentro del proceso y poder escalar hacia los objetivos de alto nivel.	Cumple
	Brindar capacitaciones y programas de seguridad de información al personal que ejecuta los procesos.	No cumple, solo se brinda capacitaciones.
	Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos. A partir de estas identificar si se requieren habilidades adicionales para cubrir el proceso y ejecutar el plan de acción para desarrollarlas.	Cumple
Evaluar el desempeño laboral de los empleados	Dentro de la evaluación del desempeño, considerar criterios con respecto a la función de seguridad de información.	No cumple
	Establecer objetivos individuales alineados con los objetivos del proceso de egreso. Estos deben reflejar competencias básicas, valores empresariales y habilidades para las funciones.	Cumple
	Proporcionar instrucciones para uso y almacenamiento de información personal dentro del proceso de evaluación.	Cumple

	Implementar un proceso de reconocimiento a medida el personal logre sus objetivos dentro del proceso.	Cumple
Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio	Comprender la demanda actual y futura de recursos humanos involucrados en el proceso de egreso para apoyar el logro de objetivos de TI y necesidades operativas del día a día salvaguardando los objetivos de la función de seguridad de información.	Cumple
	Realizar el inventario del personal del proceso e identificar sus respectivas funciones.	Cumple
	Mantener información adecuada sobre el tiempo dedicado a diferentes tareas, trabajos, servicios o proyectos	Cumple
Gestionar el personal contratado	Obtener un acuerdo formal por parte del personal sobre las políticas y requisitos de la seguridad de información a aplicarse en el proceso de egreso del paciente.	No cumple
	Llevar a cabo revisiones para asegurarse que el personal cumple con sus funciones, que el derecho de acceso es adecuado y alineado a los acuerdos pactados al firmar el contrato.	Cumple
	Definir el trabajo a realizar por terceros o por otras áreas de le organización a través de contratos o documentos formales que carezcan de ambigüedades.	Cumple, pero falta formalizar la interacción con terceros u otras áreas de negocio
	Implementar políticas que permitan identificar como se debe gestionar el personal, es decir si es necesario contratar servicios o nuevo personal siguiendo los parámetros de seguridad de información.	No cumple, las políticas actuales no son suficientes ni alineadas a la seguridad de información.

Tabla 10.1.29 - Egreso. Evaluación de cumplimiento para proceso habilitador APO07

- **Nivel de madurez actual – Proceso Incompleto (0) – "L"**

  De acuerdo a lo descrito por la norma ISO/IEC 15504, es nivel de madurez es cero (0) debido a la falta de un enfoque de seguridad formal a partir del cual se establezcan requerimientos de seguridad a aplicar dentro de la gestión de recursos humanos.

  Como existe mayor cantidad de sub-actividades de gestión que se evidencian en la entrega del servicio, por lo cual la escala interior es "Largely Achieved"

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

  El objetivo trazado para la siguiente revisión de gobierno de TI es un "proceso ejecutado", para cumplir todas las actividades definidas para este proceso habilitador e ir identificando oportunidades de mejora para poder aplicarlas para una siguiente revisión de este modelo para la organización.

c. <u>Proceso habilitador: Gestionar el riesgo</u>

APO12	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Recopilar datos	Identificar y recolectar datos para la identificación, análisis y comunicación de los riesgos de seguridad de información dentro del proceso de egreso del paciente.	No cumple, la gestión de riesgos es un proyecto futuro.
	Medir y analizar los riesgos de TI y seguridad de información suscitados dentro del proceso de egreso. Verificar pérdidas experimentadas por la materialización de estos.	No cumple
	Determinar en qué condiciones del proceso se materializó el riesgo. Identificar el impacto en el negocio.	No cumple
	Ejecutar análisis del entorno para verificar los factores de riesgo que se presentan en el proceso.	Cumple

Analizar el riesgo	Identificar, analizar y evaluar los riesgos de información dentro del proceso.	No cumple
	Construir los escenarios de riesgo de TI y seguridad dentro del proceso. Identificar las amenazar para detectar medidas de emergencia.	No cumple, pero tiene medidas de emergencia identificadas
	Identificar los riesgos residuales en el proceso e identificar exposiciones que puedan requerir una repuesta al riesgo	No cumple
	Validar resultados del análisis de riesgos del proceso antes de usarlos para la toma de decisiones. Verificar alineamiento con requerimientos organizacionales.	No cumple
Expresar el riesgo	Informar los resultados del análisis de riesgos del proceso de egreso a los stakeholders en términos adecuados y entendibles para decisiones empresariales.	No cumple
	Adoptar un perfil de riesgo de acuerdo al proceso de egreso de pacientes y comunicarlo a los stakeholders junto la efectividad del proceso y los controles asociados. Identificar oportunidades de TI para aceptar un mayor riesgo e incrementar la capacidad de gestión.	No cumple
Definir un portafolio de acciones para la gestión de riesgos	Monitorear periódicamente los riesgos de seguridad de información del proceso de egreso. Verificar que estos riesgos estén alineados con el apetito de riesgo.	No cumple
	Definir propuestas para reducir el riesgo o proyectos para incrementar las oportunidades estratégicas de acuerdo a la ley de protección de datos personales, norma técnica peruana de la historia clínica y ley de emergencia.	No cumple
Responder al riesgo	Aplicar las prácticas y controles para la mitigación de riesgos de seguridad. Se recomienda aplicar la norma ISO/IEC 27002:2013.	No cumple

Tabla 10.1.30 - Egreso. Evaluación de cumplimiento para proceso habilitador APO12

- **Nivel de madurez actual – Proceso Incompleto (0) – "N"**

  Tomando en cuenta que dentro de la organización no existe un tratamiento de riesgos de negocio, de TI y específicamente de seguridad de información, se considera que este proceso habilitador está incompleto.

  Dado a que no se presenta evidencias sobre las sub-actividades realizadas y solo tienen algunas iniciativas sobre como evaluar el entorno y los incidentes, dentro del nivel de madurez le corresponde la categoría de "Not Achieved".

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

  Para la siguiente iteración de gobierno se pretende alcanzar un nivel de madurez equivalente a uno (1), debido a que este proceso será una de las bases para el enfoque de seguridad de información y requiere ser priorizado.

d. <u>Proceso habilitador: Gestionar la seguridad</u>

APO13	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Establecer y mantener un SGSI	Realizar la declaración de la aplicabilidad del SGSI.	No cumple
Definir y gestionar un plan de tratamiento del riesgo de la seguridad de información	Diseñar, mantener y aplicar un plan de tratamiento de riesgos de seguridad de información alineados con los objetivos estratégicos de la organización y el proceso.	No cumple
	Desarrollar propuestas de mejora al plan de riesgos basados en casos de negocio de acuerdo a los roles y responsabilidades a necesitar para su aplicación.	No cumple
	Definir la medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizarlas para producir resultados reproducibles y comparables.	No cumple

	Integrar la planificación, diseño, implementación y supervisión de procedimientos se seguridad y controles para prevención y detección temprana de eventos dentro del proceso de egreso y la respuesta a incidentes.	No cumple. Solo define respuestas ante incidentes

Tabla 10.1.31 - Egreso. Evaluación de cumplimiento para proceso habilitador APO13

- **Nivel de madurez actual – Proceso Incompleto (0) – "N"**

  Según la norma ISO/IEC 15504 y la evaluación realizada, se determina que al no contar con una gestión de riesgos que encamine establecer un SGSI ni estrategias de seguridad de información, el nivel de madurez del habilitador es igual a cero (0).

  De acuerdo al nivel interno de madurez, ninguna de las sub-actividades son realizadas, por ello le corresponde la calificación "Not Achieved".

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

  El objetivo establecido para la siguiente iteración es un proceso ejecutado, debido a que sobre este proceso de negocio no forma parte del SGSI, pero si debe de tomarse en cuenta la declaración de aplicabilidad y estrategias para la gestión de los requerimientos de seguridad de información que aplican sobre él.

e. <u>Proceso habilitador: Gestionar los programas y proyectos</u>

BAI01	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Mantener un enfoque estándar para la gestión de programas y proyectos.	Incorporar los requerimientos de seguridad de información dentro de los proyectos asociados al proceso de egreso.	No cumple
	Asegurar que los stakeholders se comprometan en supervisar los proyectos del proceso para garantizar el cumplimiento del enfoque de seguridad de información.	No cumple
	Actualizar el enfoque de gestión de programas y	Cumple

	proyectos. Aplicar las mejoras que se desprenden del uso de estrategias dentro del proceso de egreso.	
Gestionar el compromiso de las partes interesadas	Identificar y comprometer a las partes interesadas para tomar decisiones en los proyectos del proceso egreso y medir el cumplimiento con los aspectos de seguridad. Verificar como estos cumplen dicho compromiso.	Cumple
Desarrollar y mantener el plan del programa.	Desarrollar un plan de seguridad de información que incluya los controles que deben ser implementados. Asignar a los responsables que los implementen en el proceso de egreso.	No cumple
	Incluir recursos dentro del proyecto para identificar e implementar los requerimientos de seguridad de información.	No cumple
	Mantener el plan de programa para asegurar su actualización de acuerdo a los proyectos y el proceso asociado.	Cumple
Planificar proyectos	Integrar la seguridad de información y las tecnologías con la gestión de proyectos.	No cumple
	Desarrollar plan de proyecto con información que permita a la dirección controlar su progreso. Incluir recursos, responsabilidades e hitos que marcan el cierre de cada una de las etapas.	Cumple
	Mantener los planes de proyecto y sus dependencias, asegurando la comunicación entre estos y que al realizar cambios en uno se reflejen en los demás.	Cumple
Gestionar el riesgo de los programas y proyectos.	Registrar los riesgos de seguridad de información y las acciones correctivas. Revisar y actualizarlos periódicamente.	Cumple, a través de gestión de matriz básica de riesgos
	Integrar proyectos de seguridad de información al programa y proceso de egreso de pacientes. Alinearlos a procedimientos y estándares de gestión de proyectos.	No cumple

	Asignar responsabilidades al personal capacitado para gestionar los riesgos de los proyectos del proceso egreso.	Cumple
Supervisar y controlar proyectos.	Programar evaluaciones a los proyectos para asegurar que los requerimientos de seguridad de información del proceso son implementados de forma efectiva.	No cumple
	Supervisar los cambios al programa y revisar requerimientos de desempeño para verificar el avance.	Cumple
	Obtener la aprobación y firma de los entregables producidos en cada iteración de los proyectos asociados.	Cumple

Tabla 10.1.32 - Egreso. Evaluación de cumplimiento para proceso habilitador BAI01

- **Nivel de madurez actual – Proceso Incompleto (0) – "L"**

  Según la norma ISO/IEC 15504 se determina un nivel de madurez igual a cero (0) producto de la falta de un enfoque de seguridad de información que abre una brecha respecto de cómo gestionar los proyectos de acuerdo a un requerimiento de seguridad de información. Se evidencia la aplicación de sub-actividades de gestión y mejoras en el proceso. Por ello su calificación es, aunque esté sobre los límites, "Largely Achieved".

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

  El nivel de madurez objetivo para la siguiente revisión de gobierno de TI es de uno (1), para garantizar un alineamiento con seguridad de información y mejorar las prácticas de gestión dentro de la cartera de proyectos.

f. Proceso habilitador: Gestionar el cambio

BAI06	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Evaluar, priorizar y autorizar peticiones de cambio	Asegurar que los cambios dentro del proceso de egreso se alinean a las políticas de seguridad de información.	No cumple
	Realizar el análisis de impacto al realizar cambios en seguridad de información y a nivel general dentro del proceso.	No cumple
	Asegurar que los cambios sean validados por los dueños del proceso de negocio de egreso del paciente. Evaluar los tipos de cambios permitidos en él.	Cumple
	Considerar el impacto de los cambios en la gestión de proveedores de acuerdo a la seguridad de información, procurando que estos no afecten los acuerdos de servicio.	No cumple
Gestionar cambios de emergencia	Desarrollar medidas para atender cambios de emergencia en el proceso de egreso a nivel de la seguridad de información.	No cumple. Tienen algunas medidas para atender cambios de emergencia
	Registrar y mantener un registro de riesgos de seguridad de información a partir de cambios de emergencia realizados en el proceso.	No cumple
	Supervisar los cambios de emergencia dentro del proceso de egreso y realizar las revisiones post-implantación involucrando a las partes interesadas.	Cumple
Hacer seguimiento e informar cambios de estado	Mantener y supervisar un sistema de seguimiento e informe para las solicitudes de cambio dentro del proceso de acuerdo a las exigencias de seguridad de información.	No cumple
	Elaborar informes respecto a los cambios de seguridad de información realizados en el proceso.	No cumple

Tabla 10.1.33 - Egreso. Evaluación de cumplimiento para proceso habilitador BAI06

- **Nivel de madurez actual: Proceso incompleto (0) – "P"**

  Según los requerimientos de la norma ISO/IEC 15504 y la evaluación sobre las sub-actividades de gestión para este proceso habilitador, se señala que alcanza un nivel de madurez igual a cero (0), debido a las falta del enfoque de seguridad que ocasiona fallas en prioridades y autorizaciones de cambios.

  Evaluando el cumplimiento interno en el nivel de madurez, se determina la clasificación interna "Partially Achieved", debido a la evidencia de mejora.

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

  Para la siguiente evaluación del gobierno de TI, se determina un nivel de madurez objetivo igual a uno (1) para garantizar la entrega de todas las actividades y empezar a implementar mejoras a nivel de gestión para el futuro

g. <u>Proceso habilitador: Gestionar los activos</u>

BAI09	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Identificar y registrar activos actuales	Identificar los activos relacionados al proceso de egreso del paciente hospitalizado y los requerimientos de seguridad asociados a estos.	Cumple, pero no se enfoca a seguridad de información
	Identificar la dependencia entre estos activos y el nivel de criticidad dentro del proceso.	Cumple
	Identificar si los activos del proceso de egreso están sujetos a alguna regulación adicional a la ley de protección de datos personales y la norma técnica peruana de la historia clínica. Verificar los aspectos contractuales de seguridad de información.	No cumple
	Verificar y determinar si los activos se encuentran en condiciones útiles para soportar dicho proceso y si es que genera valor al negocio.	No cumple

Gestionar activos críticos	Identificar que activos del proceso egreso de pacientes pueden ser considerados críticos para su cumplimiento. Supervisar el rendimiento a través de evaluaciones o planes que definan políticas de reparación o reemplazo	Cumple
	Determinar los niveles de criticidad de los activos del proceso de egreso.	Cumple
	Garantizar que los activos críticos del proceso cumplan los niveles de seguridad de información establecidos en el proceso y el negocio.	No cumple
	Establecer políticas para el cambio de estos activos críticos de acuerdo a los riesgos de seguridad de información identificados.	No cumple, no hay gestión de riesgos de seguridad de información.
Gestionar el ciclo de vida de los activos	Identificar y comunicar los riesgos de seguridad de información de los activos que soportan el proceso.	No cumple
	Realizar adquisiciones de nuevos activos previamente autorizadas de acuerdo a procedimientos seguros que garanticen un nivel aceptable de riesgo.	No cumple, pero si existen procesos para autorización de adquisiciones
	Establecer políticas para eliminar activos de forma segura.	Cumple
	Asegurar que las medidas de seguridad de información se apliquen a los activos durante todo su ciclo de vida.	Cumple

Tabla 10.1.34 - Egreso. Evaluación de cumplimiento para proceso habilitador BAI09

- **Nivel de madurez actual: Proceso incompleto (0) – "P"**

Según los requerimientos de la norma ISO/IEC 15504 y la evaluación sobre las sub-actividades de gestión para este proceso habilitador, se señala que alcanza un nivel de madurez igual a cero (0), ya que no existe un alineamiento entre los requerimientos de seguridad de información y la gestión de activos que manejan

información sensible, además de la falta de aplicación a la ley de protección de datos personales.

Evaluando el cumplimiento interno en el nivel de madurez, se determina la clasificación interna “Partially Achieved”, debido a la evidencia de mejora.

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

Para la siguiente evaluación del gobierno de TI, se determina un nivel de madurez objetivo igual a uno (1) para garantizar la entrega de todas las actividades y alinear los requerimientos de seguridad de información a los activos del proceso de negocio.

h. Proceso habilitador: Gestionar las solicitudes de servicio e incidentes

DSS02	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Definir esquemas de clasificación de incidentes y solicitudes de servicio	Definir y comunicar las características de los potenciales incidentes de seguridad de información para su reconocimiento y entendimiento del impacto en el proceso de egreso en caso se materialicen.	No cumple
	Definir modelos de solicitudes de servicio relacionados a la seguridad de información para facilitar su atención y respuesta.	No cumple
	Definir la clasificación y priorización de incidentes y solicitudes de servicio relacionados al proceso de egreso de acuerdo a los requerimientos de seguridad de información y el impacto en el negocio.	No cumple
Registrar, clasificar y priorizar solicitudes e incidentes	Investigar los incidentes de seguridad y elaborar, en base a estos, procedimientos de respuesta. Asegurar que las medidas sean difundidas y protejan los pilares de seguridad de información.	No cumple
	Registrar incidentes y solicitudes de servicio	No cumple

	relacionados a la seguridad de información del proceso de egreso.	
	Priorizar y clasificar los incidentes de acuerdo al impacto dentro del negocio y el proceso de egreso.	Cumple
Verificar, aprobar y resolver solicitudes de servicio	Seguir procedimientos y modelos de solicitudes e incidentes para elementos frecuentes de manera que sean atendidos en menor tiempo.	No cumple
Investigar, diagnosticar y localizar incidentes	Registrar un nuevo problema en caso no exista dentro de la base de datos y si el incidente de seguridad de información satisface los criterios para registro.	No cumple
	Asignar a personal capacitado la gestión de incidentes del proceso de egreso de pacientes si es estos requieren mayor conocimiento para tratarlos y reducir el impacto.	Cumple
	Identificar soluciones temporales o permanentes para los incidentes de seguridad de información, asignar su tratamiento a los especialistas respectivos dentro del proceso de egreso.	No cumple
Resolver y recuperarse de incidentes	Definir un plan de respuesta de seguridad de información para los incidentes dentro del proceso de egreso.	No cumple
	Ejecutar las acciones de recuperación para restablecer el proceso de egreso completamente.	Cumple
	Documentar la solución e identificar si es temporal o permanente para tomarlo en cuenta a futuro.	No cumple
Seguir el estado y emitir informes	Asegurar que los incidentes de seguridad de información, el análisis y seguimiento de estos, siguen los procedimientos de gestión existentes.	No cumple

	Elaborar informes y distribuirlos periódicamente a los stakeholders como parte de la mejora continua	Cumple, solo se informa a la gerencia

Tabla 10.1.35 - Egreso. Evaluación de cumplimiento para proceso habilitador DSS02

- **Nivel de madurez actual: Proceso Incompleto (0) - "N"**

  De acuerdo a la ISO/IEC 15504, el nivel de madurez identificado para el proceso habilitador, es igual a (cero). No se gestionan incidentes de seguridad de información ni medidas para mitigación o investigación alrededor de estos.

  Dentro del habilitador, su estado o calificación interna, de acuerdo al cumplimiento de sus actividades entregadas, es "Not Achieved".

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  El objetivo o meta definida por la organización es el nivel de madurez "Proceso ejecutado", garantizando la gestión de incidentes y solicitudes relacionadas a la seguridad de información alineados a los requerimientos y las políticas de esta función.

i. <u>Proceso habilitador: Gestionar la continuidad</u>

DSS04	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Definir las políticas de continuidad de negocio, objetivos y alcance	Determinar la criticidad del proceso de egreso de pacientes de acuerdo con los requerimientos de seguridad de información y el cumplimiento con la ley de protección de datos personales, norma técnica peruana de la historia clínica y ley de emergencia. Verificar si el proceso debe formar parte del programa de continuidad.	Cumple
	Asegurar que la seguridad de información forma parte del ciclo de vida de continuidad de negocio.	No cumple
	Identificar interesados, roles y responsabilidades dentro del proceso para	No cumple

	alinearlos a los objetivos y políticas del SGCN.	
Mantener una estrategia de continuidad	Identificar e incluir escenarios que den pie a eventos de información que afecten la continuidad del proceso egreso del paciente.	No cumple
	Realizar el análisis de impacto de negocio de acuerdo a los lineamientos del proceso, incluyendo los factores de seguridad de información y el máximo tolerable de interrupción en estos aspectos.	No cumple
	Analizar las amenazas de seguridad que afecten la continuidad del proceso para mejorar métodos preventivos e incrementar la resiliencia.	No cumple
Desarrollar e implementar una respuesta a la continuidad de negocio	Definir los procedimientos de recuperación para reanudar el proceso de egreso y que este cumpla con los requerimientos de seguridad de información definidos.	No cumple
Ejecutar, probar y revisar el plan de continuidad	Planificar actividades para probar el plan definido en los documentos. Asignar roles y responsabilidades para esta actividad y coordinar que no afecten al proceso.	No cumple
	Realizar el análisis y revisión para determinar el logro.	No cumple
Revisar, mantener y mejorar el plan de continuidad	Revisar el plan periódicamente tomando en cuenta los objetivos de negocio, objetivos de TI y los lineamientos del proceso de egreso. Considerar posibles cambios producto del entorno.	No cumple
	Reconocer qué incidentes de seguridad de información pueden ocasionar la interrupción del negocio, por ello se debe incrementar el nivel de gestión de éstos.	No cumple

Gestionar acuerdos de respaldo	Asegurar que los requerimientos de seguridad se cumplen en los procesos de backup y restauración de información.	No cumple
	Realizar las copias de seguridad respectivas y establecer políticas para su gestión de acuerdo a la ley de protección de datos personales y la norma técnica peruana de la historia clínica, salvaguardando los datos del paciente.	Cumple, pero no se alinea a la ley de protección de datos personales
	Probar y mantener las copias de seguridad recientes y aquellas archivadas de manera periódica para garantizar la disponibilidad de la información y su integridad.	No cumple, no se realizan pruebas
Ejecutar revisiones post-reanudación	Evaluar la efectividad del plan de acuerdo a los tiempos definidos en el análisis de impacto de negocio de acuerdo al proceso de egreso del paciente.	No cumple
	Identificar debilidades u omisiones como parte de la mejora continua para asegurar que el proceso de egreso podrá llevarse a cabo sin inconvenientes ante cualquier evento asegurando la información de los involucrados, en otras palabras, su integridad.	No cumple

Tabla 10.1.36 - Egreso. Evaluación de cumplimiento para proceso habilitador DSS04

- **Nivel de madurez actual: Proceso Incompleto (0) - "N"**

De acuerdo a los lineamientos de la norma, el nivel de madurez identificado según el cumplimiento de las actividades del proceso habilitador, es igual a (cero), debido a que no se puede garantizar el alineamiento con las estrategias de seguridad de información y no se cuenta con un plan de continuidad de negocio que abarque las tecnologías de información.

Dentro del habilitador, su estado o calificación interna, de acuerdo al cumplimiento de sus actividades entregadas, es "Not Achieved", debido a la falta de entrega y comunicación de estos planes que impide incrementar el nivel interno de madurez.

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  El objetivo o meta definida por la organización es el nivel de madurez “Proceso ejecutado”, garantizando al final un plan de continuidad alineado a las estrategias de seguridad de información en beneficio de la empresa y cubriendo las regulaciones del entorno.

j. Proceso habilitador: Gestionar los servicios de seguridad

DSS05	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Proteger contra software malicioso	Instalar y activar herramientas de protección frente a software malicioso en las estaciones o activos que brindan soporte al proceso de egreso. Concientizar al usuario sobre el empleo de estas.	Cumple
	Filtrar el tráfico entrante de información como correos electrónicos y descargas para protegerse frente a información no solicitada.	Cumple
Gestionar la seguridad de la red y las conexiones	Mantener una política para la seguridad de conexiones de red entre los activos que soportan el proceso de egreso.	No cumple
	Cifrar la información en tránsito de acuerdo con su clasificación verificando el cumplimiento con la ley de protección de datos personales.	No cumple
Gestionar la seguridad de los puestos de usuario final	Cifrar la información almacenada dentro de los activos de acuerdo a su clasificación y nivel de criticidad.	No cumple
	Configurar los sistemas operativos de forma correcta y segura en las estaciones del personal que ejecuta el proceso de egreso.	Cumple
	Implementar mecanismos de bloqueo en los dispositivos.	Cumple
	Deshacerse de los dispositivos de usuario final de forma segura.	Cumple

Gestionar la identidad del usuario y el acceso lógico	Segregar y gestionar cuentas de usuario privilegiadas.	Cumple
	Realizar regularmente revisiones de la gestión de cuentas y privilegios que abarca el proceso de egreso. Verificar que la identificación de estas es unequívoca.	Cumple
Gestionar documentos sensibles y dispositivos de salida	Establecer procedimientos de empleo, eliminación y destrucción de formularios especiales como las historias clínicas, solicitudes de alta y acta de egreso de paciente.	Cumple a nivel de activos físicos, no implementa métodos de destrucción de documentos.
	Asignar privilegios de acceso a documentación y a su modificación durante el proceso de egreso del paciente.	No cumple
	Realizar un inventario de documentos sensibles o dispositivos de salida críticos involucrados en el proceso.	No cumple
	Establecer políticas de protección física apropiada sobre formularios o documentos que contienen información sensible.	No cumple

Tabla 10.1.37 - Egreso. Evaluación de cumplimiento para proceso habilitador DSS05

- **Nivel de madurez actual: Proceso Incompleto (0) - "L"**

  De acuerdo a los lineamientos de la norma, el nivel de madurez identificado para este proceso habilitador, es igual a (cero), debido a que los servicios de seguridad entregados no se alinean a la seguridad de información y la ley de protección de datos personales.

  Dentro del habilitador, su estado o calificación interna, de acuerdo al cumplimiento de sus actividades entregadas, es "Largely Achieved" debido a las mejoras observadas.

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  El objetivo o meta definida por la organización es el nivel de madurez “Proceso ejecutado”, de manera que garanticen la existencia y el alineamiento con la función y requerimientos de seguridad de información producto de exigencias internas y aplicando sobre estas el cumplimiento regulatorio.

10.1.5 Proceso Identificación del paciente hospitalizado

Finalmente se realiza la evaluación de los procesos habilitadores que aplican para el proceso de identificación de pacientes. Se verifica las actividades y el cumplimiento de estas de acuerdo también a las regulaciones del proceso: Ley de protección de datos personales y la ley de emergencia.

a. <u>Gestionar la estrategia</u>

APO02	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Comprender la dirección de la empresa	Identificar como se puede adaptar la seguridad de información a este proceso de manera que garantice el cumplimiento de la ley de protección de datos personales y la ley de emergencia.	No cumple
	Identificar los stakeholders del proceso y cuáles son sus requerimientos de seguridad de información.	Cumple
	Determinar las prioridades para desarrollar los cambios estratégicos dentro del proceso.	Cumple
Realizar un análisis de brecha	Identificar dentro del proceso las brechas a cerrar y los cambios requeridos para llegar al nivel deseado.	Cumple
	Examinar el nivel de cumplimiento del proceso respecto a la ley de protección de datos personales, ley de emergencia y norma técnica peruana de la historia clínica.	No se alinea a la ley de protección de datos personales. Sobre las otras dos cumple.
	Mejorar la definición del estado deseado en el	Cumple

	proceso y sus objetivos. Sustentarlos demostrando los beneficios a partir de este estado frente al impacto en caso no se llegara a esta meta.	
Definir el plan estratégico y la hoja de ruta	Definir la estrategia de seguridad de información y alinearla las estrategias de negocio para el cumplimiento de objetivos dentro del proceso de identificación.	No cumple
	Crear la hoja de ruta del proceso la cual a su vez señale los riesgos y costos de los cambios.	No cumple
	Obtener el apoyo de las partes interesadas y la aprobación del plan.	No cumple
Comunicar la estrategia y la dirección de TI	Desarrollar el plan estratégico y el plan de seguridad de información que abarque el proceso y comunicarlo a los stakeholders	Se cuenta con un plan estratégico de información, pero no un plan de seguridad
	Desarrollar el plan de comunicación de acuerdo a público objetivo identificando los canales de comunicación y horarios disponibles.	Cumple
	Obtener realimentación y actualizar el plan de comunicaciones y la estrategia de seguridad de información según sea necesario para mantener el impulso.	Cumple, pero no se alinea a estrategias de seguridad de información

Tabla 10.1.38 - Identificación. Evaluación de cumplimiento para proceso habilitador APO02

- **Nivel de madurez actual: Proceso Incompleto (0) – "P"**

  De acuerdo a lo que especifica la norma ISO/IEC 15504, de acuerdo a la evidencia y cantidad de actividades que han sido aplicadas, el nivel de madurez del proceso habilitador es igual a cero (0) dado la falta de la función de seguridad de información. No obstante, realizando la evaluación interna, el habilitador tiene un logro parcial para el actual nivel de madurez.

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

  El objetivo de la organización es que este proceso habilitador alcance una madurez de uno (1) para la siguiente revisión, por lo cual tendría que incluir los requerimientos de seguridad de información y alinear el proceso a la ley de protección de datos personales.

b. Proceso habilitador: Gestionar los recursos humanos

APO07	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Mantener la dotación del personal suficiente y adecuada	Asegurar que los requisitos de seguridad se incorporan en el proceso de contratación.	No cumple, no hay requerimientos de seguridad
	Asegurar la existencia de capacitaciones y que existe personal capaz de cubrir funciones críticas de otro para reducir la dependencia.	Cumple
Identificar personal clave de TI	Asegurar la segregación de funciones en roles críticos del proceso.	Cumple
	Identificar y ejecutar acciones de acuerdo a los cambios laborales relacionados a los actores del proceso de identificación.	Cumple
Mantener las habilidades y competencias del personal	Definir habilidades y competencias necesarias de los recursos para lograr los objetivos dentro del proceso y poder escalar hacia los objetivos de alto nivel.	Cumple
	Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos. Identificar si se requieren habilidades adicionales para cubrir el proceso y ejecutar el plan de acción para desarrollarlas.	Cumple
Evaluar el desempeño laboral de los empleados	Dentro de la evaluación del desempeño, considerar criterios con respecto a la función de seguridad de información.	No cumple
	Proporcionar instrucciones para uso y	Cumple

	almacenamiento de información personal dentro del proceso de evaluación.	
	Implementar un proceso de reconocimiento a medida el personal alcance el compromiso y logre sus objetivos.	Cumple
Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio	Comprender la demanda actual y futura de recursos humanos involucrados dentro del proceso de identificación para apoyar el logro de objetivos de TI y necesidades operativas del día a día.	Cumple
Gestionar el personal contratado	Obtener un acuerdo formal por parte del personal sobre las políticas y requisitos de la seguridad de información a aplicarse en el proceso.	No cumple
	Implementar políticas o procedimientos que describan como gestionar al personal que ejecuta el proceso	Cumple, pero las políticas no están formalizadas
	Asegurar que el personal cumple con sus funciones y desempeño esperado en la ejecución del proceso.	Cumple

Tabla 10.1.39 - Identificación. Evaluación de cumplimiento para proceso habilitador APO07

- **Nivel de madurez actual: Proceso Incompleto (0) – "L"**

De acuerdo a la norma y a las actividades definidas para este proceso habilitador, el nivel de madurez identificado es de uno (1), debido a la falta de aplicación a la seguridad de información lo cual impide tener políticas formales para gestión y seguridad sobre recursos humanos.

El nivel interno alcanzado califica a un proceso "Largely Achieved", el cual debido a que son actividades manuales derivadas de otros procesos de mayor gestión está por completar al siguiente nivel "Full Achieved", logrando el escalamiento al siguiente nivel de madurez.

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  El nivel de madurez objetivo establecido por la organización es llegar a un proceso ejecutado. Aunque la brecha no es muy grande, falta formalizar la iniciativa de seguridad de información y priorizar el enfoque hacia actividades cuya distancia es mayor y tienen sobre esta necesidad de cumplimiento regulatorio.

c. <u>Proceso habilitador: Gestionar el riesgo</u>

APO12	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Recopilar datos	Identificar y recolectar datos para la identificación, análisis y comunicación de los riesgos de seguridad de información.	No cumple, la gestión de riesgos forma parte de un proyecto futuro.
	Determinar en qué condiciones del proceso se materializó el riesgo. Identificar el impacto en el negocio.	No cumple
	Ejecutar análisis del entorno para verificar los factores de riesgo asociados al proceso.	Cumple
Analizar el riesgo	Identificar, analizar y evaluar los riesgos de información dentro del proceso.	No cumple
	Identificar los riesgos residuales dentro del proceso e identificar cuáles de ellos puedan requerir una repuesta al riesgo	No cumple
	Validar resultados del análisis de riesgos del proceso antes de usarlos para la toma de decisiones. Verificar alineamiento con requerimientos organizacionales.	No cumple
Expresar el riesgo	Definir e implementar evaluaciones y estrategias de respuesta frente a los riesgos del proceso de identificación.	No cumple
	Informar los resultados del análisis de riesgos a los stakeholders sobre el proceso en términos adecuados y entendibles para soportar decisiones empresariales.	No cumple
	Informar el perfil del riesgo a los stakeholders	No cumple

	junto con la efectividad del proceso de identificación y los controles asociados. Identificar oportunidades de TI para aceptar un mayor riesgo e incrementar la capacidad de gestión.	
Definir un portafolio de acciones para la gestión de riesgos	Monitorear continuamente los riesgos de seguridad de información del proceso y verificar que el riesgo este alineado con el apetito y tolerancia al riesgo.	No cumple
	Definir conjunto de propuestas para reducir el riesgo o proyectos para incrementar las oportunidades estratégicas y retorno de beneficios.	No cumple
Responder al riesgo	Aplicar las prácticas y controles para la mitigación de riesgos de seguridad. Se recomienda aplicar en este caso la norma ISO/IEC 27002:2013.	No cumple

Tabla 10.1.40 Identificación. Evaluación de cumplimiento para proceso habilitador APO12

- **Nivel de madurez actual – Proceso Incompleto (0) – "N"**

  Tomando en cuenta que dentro de la organización no existe un tratamiento de riesgos de negocio, de TI y específicamente de seguridad de información, se considera que este proceso habilitador está incompleto.

  Dado a que no se presenta evidencias sobre las sub-actividades realizadas y solo tienen algunas iniciativas sobre como evaluar el entorno y los incidentes, dentro del nivel de madurez le corresponde la categoría de "Not Achieved".

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

  Para la siguiente iteración de gobierno se pretende alcanzar un nivel de madurez equivalente a uno (1), debido a que este proceso será una de las bases para el enfoque de seguridad de información y requiere ser priorizado.

d. Proceso habilitador: Gestionar la seguridad

APO13	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Establecer y mantener un SGSI	Realizar la declaración de la aplicabilidad del SGSI. En este caso determinar cómo alinea el proceso de identificación con los que soportan el SGSI.	No cumple
Definir y gestionar un plan de tratamiento del riesgo de la seguridad de información	Diseñar, mantener y aplicar un plan de tratamiento de riesgos de seguridad de información alineados con los objetivos estratégicos de la organización y fines del proceso.	No cumple
	Desarrollar propuestas de mejora al plan de riesgos basados en casos de negocio de acuerdo a los roles y responsabilidades a necesitar para su aplicación y acorde a los drivers identificados.	No cumple
	Definir la medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizarlas para producir resultados reproducibles y comparables.	No cumple
	Integrar la planificación, diseño, implementación y supervisión de procedimientos se seguridad y controles para prevención y detección temprana de eventos dentro del proceso de egreso y la respuesta No cumple a incidentes.	No cumple

Tabla 10.1.41 - Identificación. Evaluación de cumplimiento para proceso habilitador APO13

- **Nivel de madurez actual – Proceso Incompleto (0) – "N"**

Según la norma ISO/IEC 15504 y la evaluación realizada, se determina que al no contar con una gestión de riesgos que encamine establecer un SGSI ni estrategias de seguridad de información, el nivel de madurez del habilitador es igual a cero (0).

De acuerdo al nivel interno de madurez, ninguna de las sub-actividades son realizadas, por ello le corresponde la calificación “Not Achieved”.

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

El objetivo establecido para la siguiente iteración es un proceso ejecutado, debido a que sobre este proceso de negocio no forma parte del SGSI, pero si debe de tomarse en cuenta la declaración de aplicabilidad y estrategias para la gestión de los requerimientos de seguridad de información que aplican sobre él.

e. <u>Proceso habilitador: Gestionar los programas y proyectos</u>

BAI01	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Mantener un enfoque estándar para la gestión de programas y proyectos.	Incorporar los requerimientos de seguridad de información dentro de los proyectos asociados al proceso de identificación.	No cumple
	Asegurar que los stakeholders se comprometan a supervisar proyectos enfocados a la seguridad de información.	No cumple
	Actualizar el enfoque de gestión de programas y proyectos y aplicar las mejoras que se desprenden del uso de estrategias dentro del proceso de identificación.	Cumple
Desarrollar y mantener el plan del programa.	Desarrollar un plan de seguridad de información que incluya los controles que deben ser implementados. Asignar a los responsables que los implementen en el proceso de identificación.	No cumple
	Incluir recursos dentro del proyecto para identificar e implementar requerimientos de seguridad de información.	No cumple
	Mantener el plan de programa para asegurar su actualización de acuerdo al proyecto y el proceso asociado.	Cumple
Planificar proyectos	Integrar la seguridad de información al proyecto e identificar medidas u oportunidades tecnológicas.	No cumple

	Desarrollar plan de proyecto con información que permita a la dirección controlar su progreso. Incluir recursos, responsabilidades e hitos que marcan el cierre de cada una de las etapas.	Cumple
	Mantener los planes de proyecto y sus dependencias, asegurando que los cambios en uno se reflejen en los demás.	Cumple
Gestionar el riesgo de los programas y proyectos.	Registrar los riesgos de seguridad de información y las acciones correctivas. Revisar y actualizarlos periódicamente.	Cumple, se gestionan con una matriz de riesgo para el ámbito de proyectos
	Integrar proyectos de seguridad de información al programa y proceso de identificación. Alinearlos a procedimientos y estándares de gestión de proyectos.	No cumple
Supervisar y controlar proyectos.	Programar evaluaciones a los proyectos para asegurar que los requerimientos de seguridad de información del proceso son implementados de forma efectiva.	No cumple
	Supervisar los cambios al programa y revisar requerimientos de desempeño para verificar el avance.	Cumple

Tabla 10.1.42 - Identificación. Evaluación de cumplimiento para proceso habilitador BAI01

- **Nivel de madurez actual – Proceso Incompleto (0) – "P"**

  Según la norma ISO/IEC 15504 se determina un nivel de madurez igual a cero (0) producto de la falta de un enfoque de seguridad de información que abre una brecha respecto de cómo gestionar los proyectos de acuerdo a un requerimiento de seguridad de información. Se evidencia la aplicación de sub-actividades de gestión y mejoras en el proceso. Por ello su calificación es "Partially Achieved".

- **Nivel de madurez objetivo – Proceso Ejecutado (1)**

  El nivel de madurez objetivo para la siguiente revisión de gobierno de TI es de uno (1), para garantizar un alineamiento con seguridad de información y mejorar las prácticas de gestión dentro de la cartera de proyectos.

f. Proceso habilitador: Gestionar el cambio

BAI06	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Evaluar, priorizar y autorizar peticiones de cambio	Asegurar que los cambios dentro del proceso de identificación se alinean a las políticas de seguridad de información y de acuerdo a la ley de protección de datos personales y la ley de emergencia.	No cumple, no hay requerimientos de seguridad ni alineamiento con la ley de protección de datos personales
	Realizar el análisis de impacto al realizar cambios dentro del proceso y verificar cómo estos afectan a la seguridad de información.	No cumple
	Asegurar que los cambios sean validados por los dueños del proceso de negocio de identificación del paciente. Evaluar los tipos de cambios para esta validación.	Cumple
	Considerar el impacto de los cambios en el proceso de acuerdo a los requerimientos de seguridad de información	No cumple
Gestionar cambios de emergencia	Desarrollar medidas para atender cambios de emergencia en el proceso de identificación a nivel de la seguridad de información.	No cumple, pero se identifican medidas de cambio de emergencia.
	Registrar y mantener un registro de riesgos de seguridad de información a partir de cambios de emergencia realizados en el proceso.	No cumple
	Supervisar los cambios de emergencia en el proceso de identificación y realizar las revisiones post-implantación.	No cumple
Hacer seguimiento e informar cambios de estado	Mantener y supervisar un sistema de seguimiento e informe para las solicitudes de cambio dentro del proceso de acuerdo a las exigencias de seguridad de información.	No cumple
	Elaborar informes respecto a los cambios en seguridad de información a nivel de proceso.	No cumple

Tabla 10.1.43 - Identificación. Evaluación de cumplimiento para proceso habilitador BAI06

- **Nivel de madurez actual: Proceso Incompleto (0) – "N"**

  De acuerdo a la norma ISO/IEC 15504, se determina que el nivel de madurez para este proceso habilitador es igual a cero (0), debido a las fallas producto de la falta de la formalización de estrategias y funciones de seguridad de información incluyendo los análisis de riesgos.

  Tomando en cuenta la evidencia recolectada sobre el cumplimento de las sub-actividades se determina que el nivel interno de madurez califica a un proceso "Not Achieved".

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  El nivel de madurez objetivo para este proceso habilitador es de uno (1), el cual será revisado en la siguiente iteración de gobierno de TI, esperando formalizar las prioridades y autorizaciones de cambio de acuerdo a la seguridad de información.

g. <u>Proceso habilitador: Gestionar los activos</u>

BAI09	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Identificar y registrar activos actuales	Identificar los activos del proceso de identificación del paciente y los requerimientos de seguridad asociados.	Cumple, pero no se enfoca a la seguridad de información
	Identificar la criticidad de los activos dentro del proceso.	Cumple
	Identificar si los activos del proceso cumplen con los aspectos de seguridad de información.	No cumple
	Verificar y determinar si los activos se encuentran en condiciones útiles para soportar dicho proceso y si es que genera valor al negocio.	Cumple. El valor se muestra a nivel contable.
Gestionar activos críticos	Identificar qué activos del proceso pueden ser considerados como críticos. Supervisar su rendimiento por medio de evaluaciones o	Cumple

	planes en los que se definan las políticas de reparación o reemplazo.	
	Garantizar que los activos críticos del proceso cumplan los niveles de seguridad de información establecidos para el proceso.	No cumple
	Establecer las políticas para el cambio de estos activos críticos de acuerdo a los riesgos de seguridad de información previamente identificados.	No cumple
Gestionar el ciclo de vida de los activos	Identificar y comunicar los riesgos de seguridad de información relacionados a los activos que soportan el proceso de identificación del paciente hospitalizado.	No cumple
	Gestionar activos desde su adquisición hasta su eliminación de forma segura y con la aprobación de los interesados, siguiendo los lineamientos de seguridad de información.	Se gestionan los activos pero no se siguen lineamientos de seguridad de información
	Asegurar que las medidas de seguridad de información se apliquen a los activos durante todo su ciclo de vida.	No cumple

Tabla 10.1.44 - Identificación. Evaluación de cumplimiento para proceso habilitador BAI09

- **Nivel de madurez actual: Proceso incompleto (0) – "P"**

  Según los requerimientos de la norma ISO/IEC 15504 y la evaluación de este proceso habilitador, se señala que alcanza un nivel de madurez igual a cero (0), ya que no existe un alineamiento entre los requerimientos de seguridad de información y la gestión de activos que manejan información sensible, además de la falta de aplicación a la ley de protección de datos personales.

  Evaluando el cumplimiento interno en el nivel de madurez, se determina la clasificación interna "Partially Achieved", debido a la evidencia de mejora.

- **Nivel de madurez objetivo: Proceso ejecutado (1)**

  Para la siguiente evaluación del gobierno de TI, se determina un nivel de madurez objetivo igual a uno (1) para garantizar la entrega de todas las actividades y alinear los requerimientos de seguridad de información a los activos del proceso de negocio.

h. <u>Proceso habilitador: Gestionar las solicitudes de servicio e incidentes</u>

DSS02	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Definir esquemas de clasificación de incidentes y solicitudes de servicio	Definir y comunicar las características de los incidentes de seguridad de información para su reconocimiento del impacto en caso se materialicen dentro del proceso.	No cumple
Registrar, clasificar y priorizar solicitudes e incidentes	Registrar incidentes y solicitudes de servicio relacionados a seguridad de información del proceso de identificación.	No cumple
Verificar, aprobar y resolver solicitudes de servicio	Seguir procedimientos y modelos de solicitudes e incidentes para elementos frecuentes de manera que sean atendidos en menor tiempo.	No cumple
Investigar, diagnosticar y localizar incidentes	Identificar posibles soluciones temporales o permanentes para los incidentes de seguridad de información, asignar su tratamiento a los especialistas respectivos.	No cumple, no se documentan

Resolver y recuperarse de incidentes	Definir un plan de respuesta de seguridad de información para los incidentes dentro del proceso de identificación.	No cumple
	Ejecutar las acciones de recuperación para restablecer el proceso de identificación completamente.	Cumple
	Documentar la resolución e identificar si es temporal o permanente para tomarlo en cuenta a futuro.	No cumple
Seguir el estado y emitir informes	Asegurar que los incidentes de seguridad de información, el análisis y seguimiento de estos, siguen los procedimientos de gestión existentes.	No cumple
	Elaborar informes y distribuirlos periódicamente a los stakeholders como parte de la mejora continua.	Cumple, pero solo se comunica a gerencia

Tabla 10.1.45 - Identificación. Evaluación de cumplimiento para proceso habilitador DSS02

- **Nivel de madurez actual: Proceso Incompleto (0) - "N"**

  De acuerdo a la ISO/IEC 15504, el nivel de madurez identificado para el proceso habilitador, es igual a (cero), debido a que no se identifica ni clasifican los incidentes de seguridad de información ni medidas para mitigación o investigación alrededor de estos.

  Dentro del habilitador, su estado o calificación interna, de acuerdo al cumplimiento de sus actividades entregadas, es "Not Achieved".

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  El objetivo o meta definida por la organización es el nivel de madurez "Proceso ejecutado", garantizando la gestión de incidentes y solicitudes relacionadas a la seguridad de información alineados a los requerimientos y las políticas de esta función.

i. Proceso habilitador: Gestionar la continuidad

DSS04	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Mantener una estrategia de continuidad	Identificar e incluir escenarios que den pie a eventos de información que afecten la continuidad del proceso.	Cumple
	Analizar las amenazas de seguridad que afecten la continuidad del proceso para mejorar métodos preventivos e incrementar la resiliencia.	No cumple
Desarrollar e implementar una respuesta a la continuidad de negocio	Definir los procedimientos de recuperación para reanudar el proceso de identificación y que cumpla con los requerimientos de seguridad de información definidos.	No cumple
Revisar, mantener y mejorar el plan de continuidad	Reconocer qué incidentes de seguridad de información pueden ocasionar la interrupción del negocio, por ello se debe incrementar el nivel de gestión de éstos.	No cumple
Gestionar acuerdos de respaldo	Asegurar que los requerimientos de seguridad se cumplen en los procesos de backup y restauración de información.	No cumple
	Realizar las copias de seguridad respectivas y establecer políticas para su gestión de acuerdo a la ley de protección de datos personales.	No cumple
	Probar y mantener las copias de seguridad recientes, y aquellas archivadas, de manera periódica para garantizar la disponibilidad de la información y su integridad.	No cumple
Ejecutar revisiones post-reanudación	Evaluar la efectividad de las estrategias de acuerdo a los tiempos definidos en el análisis de impacto de negocio.	No cumple

	Identificar debilidades u omisiones como parte de la mejora continua para asegurar que el proceso podrá llevarse a cabo sin inconvenientes ante cualquier evento.	No cumple

Tabla 10.1.46 - Identificación. Evaluación de cumplimiento para proceso habilitador DSS04

- **Nivel de madurez actual: Proceso Incompleto (0) – "N"**

  De acuerdo a los lineamientos de la norma, el nivel de madurez identificado según el cumplimiento de las actividades del proceso habilitador, es igual a (cero), debido a que no se puede garantizar el alineamiento con las estrategias de seguridad de información

  Dentro del habilitador, su estado o calificación interna, de acuerdo al cumplimiento de sus actividades entregadas, es "Not Achieved", debido a la falta de entrega y comunicación de estos planes que impide incrementar el nivel interno de madurez. Cabe resaltar que este proceso es transversal al proceso de admisión, atención y egreso, por lo tanto algunas estrategias de estos tres aplicarán sobre este último.

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  El objetivo o meta definida por la organización es el nivel de madurez "Proceso ejecutado", garantizando al final un plan de continuidad alineado a las estrategias de seguridad de información en beneficio de la empresa y cubriendo las regulaciones del entorno.

j. <u>Proceso habilitador: Gestionar los servicios de seguridad</u>

DSS05	Sub-actividades para el cumplimiento de actividad.	Estado de Cumplimiento
Proteger contra software malicioso	Instalar y activar herramientas de protección frente a software malicioso las estaciones o activos que brindan soporte al proceso de identificación. Concientizar al usuario sobre el empleo de estas.	Cumple
	Filtrar el tráfico entrante de información como	Cumple

	correos electrónicos y descargas para protegerse frente a información no solicitada.	
Gestionar la seguridad de los puestos de usuario final	Cifrar la información almacenada dentro de los activos de acuerdo a su clasificación y nivel de criticidad.	No cumple
	Configurar los sistemas operativos de forma correcta y segura en las estaciones del personal que ejecuta el proceso de identificación.	Cumple
	Implementar mecanismos de bloqueo en los dispositivos.	Cumple
	Deshacerse de los dispositivos de usuario final de forma segura.	Cumple
Gestionar la identidad del usuario y el acceso lógico	Según los requerimientos del proceso, mantener los derechos de acceso	Cumple
	Segregar y gestionar cuentas de usuario privilegiadas.	Cumple
Gestionar documentos sensibles y dispositivos de salida	Establecer procedimientos de empleo, eliminación y destrucción de los brazaletes de identificación.	No cumple
	Asignar privilegios de acceso a documentación y a su modificación durante el proceso de identificación.	No cumple
	Realizar un inventario de documentos sensibles o dispositivos de salida críticos involucrados durante el proceso.	No cumple
	Establecer políticas de protección física apropiadas sobre documentos y activos sensibles empleados para identificar pacientes.	No cumple

Tabla 10.1.47 - Identificación. Evaluación de cumplimiento para proceso habilitador DSS05

- **Nivel de madurez actual: Proceso Incompleto (0) - "L"**

De acuerdo a los lineamientos de la norma, el nivel de madurez identificado para este proceso habilitador, es igual a (cero), debido a que los servicios de seguridad

entregados no se alinean ni responden de acuerdo a necesidades formalizadas y establecidas de seguridad de información y la ley de protección de datos personales.

Dentro del habilitador, su estado o calificación interna, de acuerdo al cumplimiento de sus actividades entregadas, es “Largely Achieved”, debido a la capacidad de mejora del proceso.

- **Nivel de madurez objetivo: Proceso Ejecutado (1)**

  El objetivo o meta definida por la organización es el nivel de madurez “Proceso ejecutado”, de manera que garanticen la existencia y el alineamiento con la función y requerimientos de seguridad de información producto de exigencias internas y aplicando sobre estas el cumplimiento regulatorio.