UNIVERSIDAD TÉCNICA DE COTOPAXI

DIRECCIÓN DE POSTGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

MODALIDAD: PROPUESTA METODOLÓGICA Y TECNOLÓGICA AVANZADA

Título:

Metodología COBIT para el desarrollo de plan de gobernanza de Tecnologías de la Información y Comunicación en Hospitales Generales

---

Trabajo de titulación previo a la obtención del título de magister en Sistemas de Información

Autor:

Villacís Damacela Juan Miguel Ing.

Tutor:

Rodolfo Matius Mendoza Poma Msc.

LATACUNGA –ECUADOR

2023

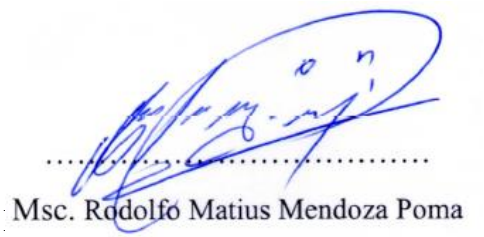
APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación "Metodología COBIT para el desarrollo de plan de gobernanza de Tecnologías de la Información y Comunicación en Hospitales Generales" presentado por Villacís Damacela Juan Miguel, para optar por el título magíster en Sistemas de Información.

CERTIFICO

Que dicho trabajo de investigación ha sido revisado en todas sus partes y se considera que reúne los requisitos y méritos suficientes para ser sometido a la presentación para la valoración por parte del Tribunal de Lectores que se designe y su exposición y defensa pública.

Latacunga, julio 25, 2023



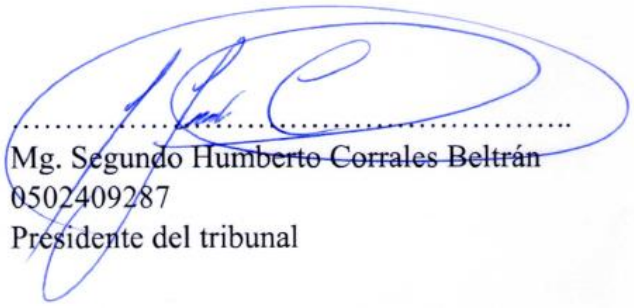
Msc. Rodolfo Matius Mendoza Poma

CC.: 1710448521

APROBACIÓN TRIBUNAL

El trabajo de Titulación: "Metodología COBIT para el desarrollo de plan de gobernanza de Tecnologías de la Información y Comunicación en Hospitales Generales", ha sido revisado, aprobado y autorizado su impresión y empastado, previo a la obtención del título de Magíster en Sistemas de Información; el presente trabajo reúne los requisitos de fondo y forma para que el estudiante pueda presentarse a la exposición y defensa.

Latacunga, julio, 25 2023



……..
Mg. Segundo Humberto Corrales Beltrán
0502409287
Presidente del tribunal

……
Mg. Verónica del Consuelo Tapia Cerda
0502053697
Lector 2

……
Mg. Luis Rene Quisaguano Collaguazo
1721895181
Lector 3

DEDICATORIA

Este logro alcanzado se la dedico especialmente a mi familia, ya que han sido el pilar fundamental de constancia, dedicación, esfuerzo y el motor principal de que este sueño de ser magister sea alcanzado, a mi madre por ser el gran ejemplo para seguir de fortaleza y esperanza, por su apoyo incondicional quien supo darme consejos y palabras de aliento en el transcurso de este trabajo y logro realizado.

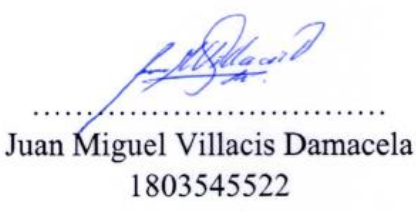
AGRADECIMIENTO

A Dios y mi familia, Bertha Damacela por permitir que este sueño de alcanzar un nuevo nivel de formación académica y profesional se haya cristalizado, lo que fue un impulso de motivación, trabajo, esfuerzo y dedicación para lograr esta meta que me abre nuevas puertas de oportunidades en mi vida profesional.

RESPONSABILIDAD DE AUTORÍA

Quien suscribe, declara que asume la autoría de los contenidos y los resultados obtenidos en el presente trabajo de titulación.

Latacunga, julio, 25, 2023



.....

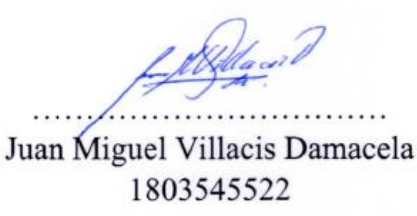
Juan Miguel Villacis Damacela

1803545522

RENUNCIA DE DERECHOS

Quien suscribe, cede los derechos de autoría intelectual total y/o parcial del presente trabajo de titulación a la Universidad Técnica de Cotopaxi.

Latacunga, julio 25, 2023



.....

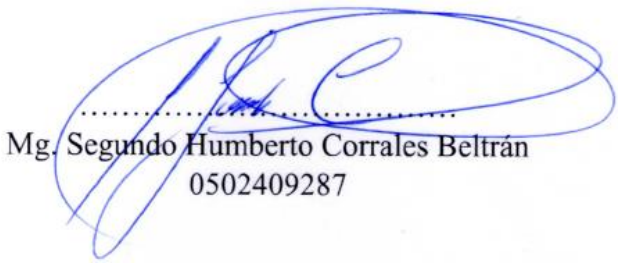
Juan Miguel Villacis Damacela

1803545522

AVAL DEL VEEDOR

Quien suscribe, declara que el presente Trabajo de Titulación: "Metodología COBIT para el desarrollo de plan de gobernanza de Tecnologías de la Información y Comunicación en Hospitales Generales" contiene las correcciones a las observaciones realizadas por los lectores en sesión científica del tribunal.

Latacunga, julio 25, 2023



Mg. Segundo Humberto Corrales Beltrán
0502409287

UNIVERSIDAD TÉCNICA DE COTOPAXI

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Título:

Metodología COBIT para el desarrollo de plan de gobernanza de Tecnologías de la Información y Comunicación en Hospitales Generales

Autor: Juan Miguel Villacís Damacela
Tutor: Rodolfo Matius Mendoza Poma Msc.

RESUMEN

Las tecnologías de la información hoy en la actualidad se han convertido en el pilar fundamental de las organizaciones, instituciones y empresas; su uso se incrementó donde la tecnología juega un papel importante en el desarrollo de actividades organizacionales que en varios casos ya no es necesario la presencia del usuario y/o del operador de atención, todo se ha convertido en teleasistencia. Las normativas existentes que gobiernan las instituciones se apoyan en un gobierno TI correctamente estructurado; La presente investigación desarrolla un plan de gobernanza TI en la Unidad de Tecnologías de la Información y Comunicación del Hospital General Ambato para el control y alcance de metas institucionales, la información recolectada a través de un enfoque cualitativo descriptivo y el análisis con metodología COBIT 2019 logra establecer un plan como marco de referencia en gobernabilidad TI que involucra a todos los usuarios en procesos que generen valor a la organización, reduzca riesgos y optimice recursos que permitan la viabilidad del alcance y logro de metas en la entidad; plan que se verifica con el cálculo de coeficiente de fiabilidad y la evaluación por expertos en temas de fundamento teórico, pertinencia y coherencia metodológica, factibilidad e importancia.

PALABRAS CLAVE:
COBIT, TIC, plan de gobernanza, Hospitales Generales

UNIVERSIDAD TÉCNICA DE COTOPAXI

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Title:

COBIT methodology for the development of a governance plan of Information and Communication Technologies in General Hospitals

Author: Juan Miguel Villacís Damacela
Tutor: Rodolfo Matius Mendoza Poma Msc.

ABSTRACT

Today the Information Technologies have become a fundamental pillar of organizations, institutions and companies; Its use increased where technology plays an important role in the development of organizational activities where in several cases, the presence of the user and the service operator is no longer necessary, everything has become telecare. Existing regulations governing institutions are supported by a properly structured IT governance; The present investigation develops an IT governance plan in the Information and Communication Technologies Unit of the Ambato General Hospital for the control and achievement of institutional goals, the information collected through a descriptive qualitative approach and the analysis with the COBIT 2019 methodology achieves establish a plan as a reference framework in IT governance that involves all users in processes that generate value for the organization, reduce risks and optimize resources that allow the viability of the scope and achievement of goals in the entity; plan that is verified with the calculation of the reliability coefficient and the evaluation by experts in topics of theoretical foundation, relevance and methodological coherence, feasibility and importance.

KEYWORD:

COBIT, TIC, governance plan, General Hospitals

NELSON WILFRIDO GUAGCHINGA CHICAIZA con cédula de identidad número: 0503246415 MAGISTER EN LA ENSEÑANZA DEL IDIOMA INGLES COMO LENGUA EXTRANJERA con número de registro de la SENESCYT: 1010-2019-2041252; CERTIFICO haber revisado y aprobado la traducción al idioma inglés del resumen del trabajo de investigación con el título Metodología COBIT para el desarrollo de plan de gobernanza de Tecnologías de la Información y Comunicación en Hospitales Generales de: Juan Miguel Villacis Damacela, aspirante a magister en Sistemas de Información.

Latacunga, julio, 25, 2023

……Nelson Guagchinga……

NELSON WILFRIDO GUAGCHINGA CHICAIZA
C.I. 0503246415

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Como **antecedentes** en el desarrollo de esta investigación, se considera que la información debe ser considerada el activo más importante de las organizaciones, ya que la tecnología y los sistemas de información pueden llegar a ser vulnerables como resultado del factor humano, siendo así en ocasiones que se invierta en tecnología, seguridad, software y/o hardware; y en estos puede llegar a prevalecer la vulnerabilidad debido a errores en factores internos de manejo, administración y gobernanza de las TI, viéndose bloqueado el logro de los objetivos como organización. [1]

En el caso de Hospitales Generales instituciones pertenecientes al Ministerio de Salud del Ecuador ha crecido la necesidad de los pacientes y la exigencia de las autoridades por tener un servicio de salud de calidad ante la detección y tratamiento de enfermedades respiratorias que se incrementó en los años 2020, 2021 y 2022 [2], como consecuencia se crearon nuevos sistemas de información, se incrementó la infraestructura tecnológica, y se dio un gran salto en los servicios de teleasistencia y videoconferencias, lo que produjo el aumento de datos y flujo de información.

La unidad de Tecnologías de la Información del Hospital General Ambato considerando el Estatuto Orgánico de Gestión Organizacional por Procesos de los Hospitales del Ministerio de Salud Pública; siendo parte de los procesos habilitantes de apoyo en el área de gestión administrativo financiero tiene como misión: "*aplicar las normas y procedimientos que efectivicen la gestión y administración de las tecnologías de la información y comunicaciones, orientadas a la optimización de los recursos y fortalecimiento de la red interna para mejorar la eficiencia en la atención a los pacientes"*.[3]

La Dirección Nacional de Tecnologías de la Información y Comunicación del Ministerio de Salud Pública del Ecuador como institución central que corresponde a la coordinación de ingeniería de software, proyectos tecnológicos, manejo de redes comunicaciones e infraestructura, seguridad informática y soporte tecnológico, dispone de un conjunto de políticas a ser cumplidas como directriz por acuerdo ministerial 2880 publicado en el registro oficial 889 del 8 de febrero de

2013 en noviembre de 2013[4] en el que se detalla cómo como misión: garantizar la integridad de la información, optimización de recursos, sistematización y automatización de los procesos institucionales.

Actualmente, se ve de una manera limitada las posibilidades de un gobierno de administración TI en Hospitales Generales, ya que los procesos que se alineen o cumplan con las normas o políticas establecidas no se encuentran correctamente definidos al logro de estos objetivos, la especificación o dotación de un marco de referencia es esencial para alcanzar una optimización de estos recursos tecnológicos que mejoren la gestión de TI y de la información.

COBIT promueve un marco de mejores prácticas de gobierno y gestión TI empresarial, con una dirección que atiende las necesidades condiciones y opciones de las partes interesadas a base de monitoreos en el desempeño y cumplimiento de responsabilidades con un enfoque específico en el gobierno empresarial de la Información y tecnología.[5]

Al conocer estas directrices institucionales aplicables y alineadas a los objetivos, misión y visión del Ministerio de Salud Pública del Ecuador, se considera el siguiente **Planteamiento del Problema;** En el Hospital General Docente de Ambato ubicado en las Avs. Unidad Nacional y Pasteur sector Cashapamba del cantón Ambato, provincia de Tungurahua, se maneja gran cantidad de información sobre tratamientos de salud en los pacientes de la zona 3 del país, esta información es esencial tanto para realimentar la evolución de salud en el Ecuador como desarrollo de investigación en el área médica, y el Hospital no cuenta con un modelo de buenas prácticas en Tecnologías de la Información para garantizar una correcta administración y gobierno de la información. Situaciones como: la falta de toma de decisiones oportunas y adecuadas, dificultad de anexar nuevo personal, altos tiempos de respuesta en atenciones a requerimientos, identificación de riesgos, documentación de actividades; son razones por las que en ocasiones se sufre retardos en atenciones a pacientes o interrupciones en la continuidad de labores hospitalarias y se plantea la necesidad de establecer un plan metodológico COBIT que mejore el gobierno y administración de TI en la institución.

Por tal razón se **Formula el Problema** de Investigación:

¿Como desarrollar un plan de gobernanza de Tecnologías de la Información y Comunicación en el Hospital General Docente Ambato, donde se evidencia la ausencia de un marco metodológico qué garantice una correcta administración y gobierno de TI?

El **Objetivo General** planteado es proponer mediante metodología COBIT un plan de gobernanza de Tecnologías de la Información y Comunicación para el control de metas institucionales en el Hospital General Docente Ambato.

Los **Objetivos Específicos** propuestos para este proyecto de investigación son:

- Fundamentar teóricamente los conocimientos que se relacionen con el marco de referencia COBIT aplicado a la organización y conformación del Plan de Gobernabilidad TI en el Hospital General Docente Ambato.
- Establecer el diseño metodológico para las métricas del Plan de Gobernanza de Tecnologías de la Información y Comunicación en el Hospital General Docente Ambato.
- Desarrollar un Plan de Gobernanza TI que establezca parámetros de medición a las Tecnologías de la Información y Comunicación en el logro de metas institucionales del Hospital General Ambato.

Para lograr la ejecución de la propuesta investigativa, se detalla la siguiente tabla de sistema de **Tareas**.

Tabla 1. Sistema de Tareas.

Objetivo	Actividad (tareas)
1. Objetivo específico 1: Fundamentar teóricamente los conocimientos que se relacionen con el marco de referencia COBIT aplicado a la	1. Revisión de la Metodología COBIT 2019 - ISACA
	2. Establecer el conocimiento metodológico en Gobernanza y Objetivos de Gestión

organización y conformación del Plan de Gobernabilidad TI en el Hospital General Docente Ambato	3. Establecer el conocimiento metodológico en diseño de solución de gobierno de la información y la tecnología
	4. Establecer el conocimiento metodológico en implementación y optimización de una solución de gobierno de la información y la tecnología
	5. Revisión de la documentación oficial de los estatutos de gestión organizacional por procesos del MSP del Ecuador en Hospitales Generales
	6. Revisión de los lineamientos y/o políticas de gestión en servicios informáticos, ingeniería de software, proyectos tecnológicos, comunicaciones y centros de soporte TI para establecimientos de Salud Pública del Ecuador.
2. Objetivo específico 2: Establecer el diseño metodológico para las métricas del Plan de Gobernanza de Tecnologías de la Información y Comunicación en el Hospital General Docente Ambato.	1. Definir la cascada de metas
	2. Identificar metas empresariales
	3. Definir Metas de alineamiento.
	4. Relacionar metas empresariales vs metas de alineamiento
	5. Determinar el resultado del proceso entre objetivos de gobierno y gestión por dominio
	1. Definir los factores de diseño

3. Objetivo específico 3: Desarrollar un Plan de Gobernanza TI que establezca parámetros de medición a las Tecnologías de la Información y Comunicación en el logro de metas institucionales del Hospital General Ambato.	2. Determinar los aplicativos de instrumentos en los factores de diseño
	3. Establecer los objetivos de Gobierno y Gestión COBIT

Elaborado por: Investigador

Son tres etapas que conforman el desarrollo de la investigación que se determinan a continuación:

Tabla 2. Etapas del proceso.

Etapas	Descripción
Etapa 1. Diagnóstica	Desarrollo del estudio exploratorio: Análisis de la problemática en la Gobernanza de TI en Hospitales Generales
Etapa 2. Planificación	Determinación de las diferentes partes que conforman la elaboración del documento y del estudio del tema (Formulación del problema, objetivo general, objetivos específicos, metodologías, población y muestra y cronograma de trabajo)
Etapa 3. Acción	Recopilación de información bibliográfica marco metodológico COBIT: Sistemas de Gobernanza y sus componentes, niveles, procesos, enfoque, modelos, diseño, guías de implementación; Estructuras Hospitalarias de Salud Pública del Ecuador, metas objetivos ministeriales institucionales en salud pública,

	dominios TI en Hospitales Generales de atención pública, Políticas de recursos y uso de red tecnológicos de Dirección Nacional de Tecnologías de la Información y Comunicación.

Elaborado por: Investigador

Como **justificación**, el presente proyecto pretende implementar a través de metodología COBIT un Plan de Gobernanza de Tecnologías de la Información y Comunicación en el Hospital General Docente Ambato, con el fin de reducir las vulnerabilidades en los procesos de TI, siendo así que los funcionarios Analistas de Tecnologías, Analistas de Redes Comunicaciones e Infraestructura, Analistas de Soporte Técnico y Asistentes tengan conocimiento claro de gestión y administración TI en la institución. Con la implementación de un plan de gobernanza TI se pretende conocer el estado actual de los procesos TICs, definir los procesos estratégicos que serán de mayor prioridad para apalancar el logro de los objetivos hospitalarios, establecer los requisitos TICs sobre gobierno y administración TI, Relacionar las metas hospitalarias con las metas TI en la Unidad de Tecnologías de la Información y Comunicación del Hospital General, alcanzar la eficiencia operativa en base a los procesos COBIT a implementarlos.

La propuesta de investigación como plan de gobernabilidad de TI en Hospitales Generales está orientada a aplicar una guía de procedimientos y técnicas que efectivicen el proceso de logro de objetivos institucionales hospitalarios, las TICs de Hospitales Generales agregarán valor de servicios como habilitante de apoyo a las demás unidades que conforman la institución.

Los beneficiarios directos serán las diferentes unidades hospitalarias de gestión administración y personal médico operativo; lo que reflejará un mejoramiento de calidad en el logro de los objetivos institucionales en atención hospitalaria al paciente. Ya que según la sección séptima de la constitución Art.32 indica: "*La prestación de los servicios de salud se regirá por los principios de equidad, universalidad, solidaridad, interculturalidad, calidad, eficiencia, eficacia, precaución y bioética, con enfoque de género y generacional."*[6]; y es esencial

que la Unidad de Tecnologías de la Información en Hospitales cuente con un marco de referencia COBIT que norme las acciones y procedimientos en la prestación de servicios de salud.

Para el desarrollo de la investigación la **metodología** a utilizar será de tipo exploratorio y descriptivo, ya que para la obtención de la información del presente proyecto se realizaron observaciones en las diferentes áreas del hospital, encuestas con el personal líder de los servicios y entrevistas con las autoridades de salud que dirigen el Hospital General Docente Ambato.

La investigación está orientada a resolver el problema de la ausencia de un plan de gobernanza basado en un marco metodológico que guíe el logro de objetivos institucionales para facilitar la toma de decisiones oportunas.

En cuanto se refiere a la metodología COBIT se usará la observación científica y el estudio documental que nos permitirá conocer la realidad de los procesos internos en la toma de decisiones ante la necesidad de soporte y actividades TI en el momento que las unidades de proceso de asesoría, procesos habilitantes de apoyo y procesos agregados de valor lo requieran.

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA

1.1. Antecedentes

Al haber realizado el estudio bibliográfico se ha verificado que existen investigaciones sobre metodología COBIT aplicado a la gobernanza de TI en distintos tipos de instituciones que decidieron optar la implementación de una guía metodológica con el fin de mitigar riesgos y crear valor en un marco efectivo de gobierno.

Andrés Cortés [7] presenta una investigación con metodología COBIT aplicado a gobiernos de municipalidad para migración de sistemas informáticos, partiendo de expectativas y objetivos obtenidas de un plan estratégico municipal se establecen las metas empresariales a las cual se desean llegar, la metodología COBIT permite reorganizar e identificar los objetivos de gobierno y gestión de la municipalidad de Carrillo para así poder pasar a la etapa de especificación de factores de diseño.

Los Factores Diseño influyen en la forma en que se adecua un sistema de gobierno, en el caso de procesos de migración de sistemas operativos en municipalidades COBIT permitió seleccionar los objetivos de gobierno , gestión y relacionarlos a la migración de sistemas operativos implementando estrictos procesos de planificación, elaboración, ejecución y control de actividades TI con el fin de apoyar el cumplimiento de la transformación tecnológica digital del Gobierno Local, además la normalización de los procesos en transformación digital se plasman en la entidad como un apoyo de logro de objetivos institucionales que logra mitigar la cantidad de errores cometidos y posibles riesgos que puedan producirse.

La investigación realizada logra demostrar, la evaluación del desempeño de acciones realizadas en el campo de TI con el uso de los recursos establecidos COBIT, determina acciones no realizadas y que son indispensables para la institución consideradas como brechas de ejecución, lo que pronuncia a las autoridades la toma de decisiones oportunas en la ejecución de los parámetros identificados que causa impedimento en el logro de los objetivos de gobierno.

En la investigación efectuada por Fabara López, Fabricio Bolívar y Quiroga Chauca, Liceth Alejandra[8] se implementó procesos de Gobierno de COBIT 2019 en la Dirección de Tecnologías de la Información y Comunicaciones del Ejército del Ecuador, proyecto que presenta la situación actual de cada uno de los procesos TI que emplean la institución, define las estrategias institucionales a través del establecimiento de las metas corporativas y emplea un marco de referencia que sea tomado como guía en procedimientos y técnicas en la gobernanza TI del ejército ecuatoriano basándose en las metas empresariales como: ambiente financiero, clientes, gestión interna y crecimiento.

Según problemas detectados relacionados con TI en base al marco de referencia COBIT se determinan los riesgos como: toma de decisiones en inversiones tecnológicas, gestión de ciclo de vida de proyectos, costo y control TI, comportamiento TI, arquitectura empresarial, adopción de software y problemas de uso, incidentes de hardware y software, ataques y vulnerabilidad de la información, innovación, gestión de la data.

Se establecen objetivos de gestión que garanticen el establecimiento y mantenimiento del marco de gobierno, optimización de riesgos y recursos, con transparencia en las partes interesadas.

Como modelo de gestión y gobernanza TI establecido en la institución muestra y genera un valor agregado con indicadores tanto de gestión como de cumplimiento de trabajo y aporte al Ejército Ecuatoriano; COBIT 2019 permitió establecer un modelo de gestión de calidad y mejora continua identificando 7 metas de alineación para la institución como son la gestión de riegos, la prestación de servicios de TI, la seguridad de la información, y la calidad de la información; con factores de diseño propuestos a la mejora del sistema de gobierno, 40 objetivos de gobierno y gestión, 2 en dominios de administración y/o dirección como EDM01 EDM03 y 18 objetivos en gestión AP01, APO03, APO011, APO012, APO013, APO014, BAI02, BAI03,BAI06, BAI07, BAI10, DSS02, DSS03, MEA02, MEA03.[8]

Con la información establecida de gobernanza de TI aportando al Ejército Ecuatoriano se identifica que modelos de madurez se encuentran en nivel cero, que al implementar las nuevas estrategias y propósitos de gobierno se alcanza un porcentaje de 55% por lo que como indicador resulta que las estrategias necesitan un mayor esfuerzo de gobierno y gestión, las métricas COBIT logran estimar los porcentajes avance de gobierno en cuanto se refiere al logro de objetivos institucionales logrando así un determinante de mejora continua para reducir riesgos institucionales que afecten a la institución.

Por las investigaciones realizadas del marco de gobierno TI con la metodología COBIT se identifica tanto el alcance de logro de objetivos propuestos por las instituciones como la detección de acciones que se están ejecutando o realizando de una manera insuficiente, lo que permite establecer parámetros de medición o métricas de acción, convirtiéndose en un plan estratégico institucional como órgano de conocimiento sobre las necesidades, expectativas y metas de la organización de las partes interesadas de gobierno.

1.2. Fundamentación Epistemológica

1.2.1. Hospitales Generales

Según acuerdo ministerial 1537 de la Republica del Ecuador, por registro oficial 339 publicada el 25 de septiembre de 2012 se emite el "ESTATUTO ORGÁNICO DE GESTIÓN ORGANIZACIONAL POR PROCESOS DE LOS HOSPITALES" en el cual se manifiesta que: "*Los Hospitales establecen un modelo de gestión en red que permite satisfacer todas las necesidades de salud de forma integral, de calidad y gratuidad*"[3]. Determinando la identificación de los distintos procesos, clientes, productos y/o servicios que conforman las unidades hospitalarias de salud.

Cada uno de los procesos se categorizan de acuerdo con la manera que éstos contribuyen o añaden el valor agregado al cumplimiento de la misión en los servicios de salud pública nacional.

1.2.2. Misión y Visión de Hospitales

La misión establecida en los hospitales generales del MSP[9] está determinada de la siguiente manera:

> Prestar servicios de salud con calidad y calidez en el ámbito de la asistencia especializada, a través de su cartera de servicios, cumpliendo con la responsabilidad de promoción, prevención, recuperación, rehabilitación de la salud integral, docencia e investigación, conforme a las políticas del Ministerio de Salud Pública y el trabajo en red, en el marco de la justicia y equidad social. [3]

Mientras que la visión:

> Ser reconocidos por la ciudadanía como hospitales accesibles, que prestan una atención de calidad que satisface las necesidades y expectativas de la población bajo principios fundamentales de la salud pública y bioética, utilizando la tecnología y los recursos públicos de forma eficiente y transparente [3]

La descripción del objetivo y la visión en la prestación de servicios de salud en el ámbito de la asistencia especializada presenta una meta clara de ofrecer servicios de salud con calidad, calidez y una atención integral que abarque la promoción, prevención, recuperación y rehabilitación de la salud.

Además, el cumplimiento de las políticas y fomento del trabajo en red en aras de la justicia y equidad social que permitirá ser reconocidos por la ciudadanía como instituciones accesibles, capaces de proporcionar una atención de calidad que satisfaga las necesidades y expectativas de la población.

1.2.3. Estructura organizacional de gestión por procesos

El Ministerio de Salud Pública del Ecuador reconocida como autoridad sanitaria nacional se encarga de garantizar a la población el derecho a la salud, gobernando programas de salud, prevención de enfermedades, vigilancia tanto epidemiológica como en el ámbito médico, productos y servicios de calidad, investigación en

diferentes patologías que son causadas en la población y provisión de servicios de atención al paciente[10].

Por ello los hospitales del MSP[9] se estructuran de acuerdo con la misión y visión ministerial, esto nos indica que el tipo de administración mantiene una filosofía y enfoque de gestión clasificándose por procesos de salud para atención de pacientes, generar productos, brindar servicios y así promover una atención de calidad en las diferentes unidades hospitalarias y centros de atención primaria.

1.2.4. Procesos de los Hospitales

Según la función y de acuerdo con el valor agregado que contribuyen al cumplimiento de la misión hospitalaria[3], los procesos han sido clasificados de la siguiente manera:

- Procesos Gobernantes,
- Procesos Agregadores de Valor
- Procesos Habilitantes de Asesoría y
- Procesos Habilitantes de Apoyo

Los Procesos Gobernantes dirigen y orientan la gestión administrativa en la institución contribuyendo con políticas, estableciendo directrices, generando normas, ejecutando procedimientos, desarrollando planes, formando acuerdos y emitiendo resoluciones que norman legalmente a la institución, estos procesos están compuestos por: la gerencia hospitalaria y la dirección asistencial.[11]

Los Procesos Agregadores de Valor son aquellos que generan y a la vez administran los productos y servicios hospitalarios y se relacionan directamente con el paciente por lo que permiten efectuar las actividades que conllevan al cumplimiento de la misión y los objetivos estratégicos institucionales, estos están compuestos por las gestiones de especialidades clínicas y/o quirúrgicas, apoyo diagnóstico y terapéutico, cuidados de enfermería, y docencia e investigación.[11]

Los Procesos Habilitantes de Asesoría y de Apoyo son aquellos que generan productos y brindan servicios a los procesos gobernantes, agregan valor de apoyo a la gestión de la institución.[11]

Estos procesos han sido clasificados de acuerdo con las actividades que realizan internamente en la institución con el fin de proveer productos y servicios además de interrelacionarse entre sí y poder brindar una atención en salud oportuna y eficaz de acuerdo a la misión y visión ministerial e institucional, como se observa en la siguiente figura.

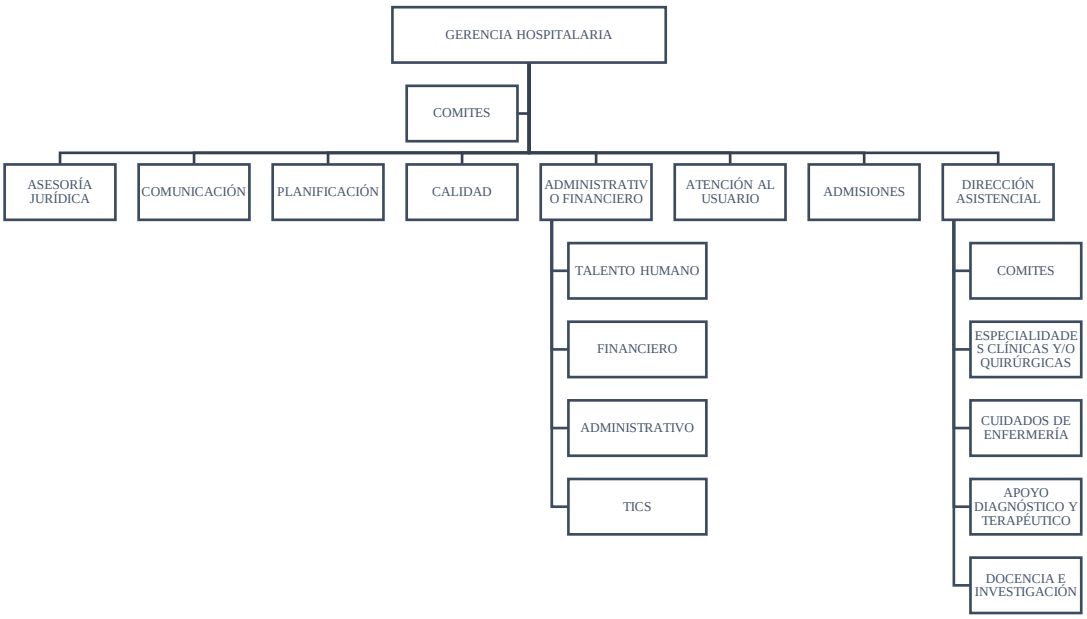


Figura 1. Hospitales Generales Especializados, y de Especialidades

Fuente: Tomado de Estatuto orgánico por procesos MSP[3]

1.2.5. Gobernanza Empresarial de TI (GETI)

La Gobernanza Empresarial de Tecnologías de la Información por sus siglas conocida como GETI o EGIT (Enterprise Governance of IT) organiza y ejecuta acciones entre los altos directivos y los gestores de TI, tiene como objetivo, mantener control sobre el diseño e implementación de las estrategias empresariales de TI; además asegura alinear el negocio con las TI y se convierte en el pilar fundamental en el logro de objetivos.[12]

La GETI o EGIT es determinante al tomar decisiones y establecer un marco de rendición de cuentas en el comportamiento deseado en el uso de las TI en la organización; así como tambien, el aseguramiento de la inversión TI es esencial para la reducción de riesgos en rangos aceptables, esto implica que genera un aporte en la cultura organizacional de rendición de cuentas, distribución de estructuras, madurez y estrategia.

Estándares como el Internacional para el Gobierno Corporativo de las Tecnologías de la Información (ISO/IEC 38500) [13]fue desarrollado por expertos del gobierno y la industria en donde se establece la importancia de colocar al Gobierno de las TIC en ámbitos de negocios, manteniendo como ente principal aspectos tecnológicos y de innovación.

La importancia de que las TI se centralicen en la gestión de riesgo y a la generación de valor y formen parte del gobierno corporativo, permite a las TI supervisar actividades en las organizaciones como la implementación de procesos, estructuras y mecanismos, que orientan al área comercial y organizativa ejecutar sus responsabilidades en apoyo de la alineación de objetivos comerciales o institucionales para la creación de valor, como indica la figura a continuación.

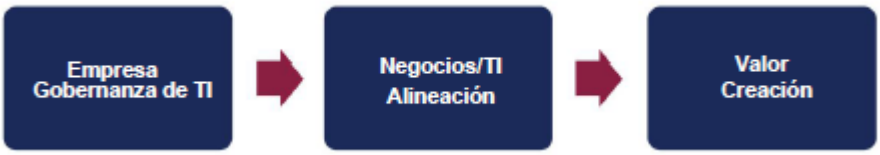


Figura 2. Importancia de la GETI

Fuente: COBIT 2019 [14]

1.2.6. COBIT

COBIT proviene de sus siglas Control Objectives for Information Systems and related Technology[14], que en nuestro idioma español tiene el significado como: Objetivos de Control para Tecnología de Información y Tecnologías; este modelo es el resultado de investigaciones realizadas por expertos de varios lugares del

mundo publicado por ISACA (Information Systems Audit and Control Association)[15].

El Marco metodológico COBIT 2019 no se limita tan solo al departamento de TI sino también a la gestión de la información, la tecnología empresarial, y la participación, toma de decisiones en los jerárquicos superiores de las organizaciones. Existen dos estructuras organizacionales que son el gobierno y la gestión en donde se detalla sus propósitos a continuación:

COBIT establece componentes de construcción de un sistema de gobierno compuesto por diferentes procesos, políticas, procedimientos, flujo de información que crean una cultura empresarial y el modo de comportamiento, habilidades e infraestructura, con el uso y definición de factores de diseño que se deben considerar para la construcción del sistema de gobierno.[14]

1.2.7. Aporte de Gobierno TI

El gobierno de TI mediante la innovación tecnológica crea valor, reduce riesgos de negocio en el proceso de apoyo y sostén para las demás unidades de la organización, la GETI asume tres retos fundamentales:

1.2.7.1. Optimización del riesgo

Cuando una institución o empresa decide implementar tecnologías de la información (TI), existe la posibilidad de enfrentar riesgos en términos de su implementación, su impacto en las operaciones internas y su influencia en otras unidades. Al referirnos a los riesgos, nos referimos al potencial impacto que podría afectar la idea de negocio. [14]

1.2.7.2. Entrega de Valor

Mediante la aplicación de la gestión de riesgos empresariales y la integración de las tecnologías de la información, es posible evaluar cuantitativamente las actividades internas, demostrando el impacto y las contribuciones para optimizar el riesgo en la idea de negocio. [14]

1.2.7.3. Optimización de recursos

Este proceso proporciona los elementos suficientes, apropiados y efectivos para garantizar que la infraestructura de TI a implementarse sea económica e integral, es decir cada vez que la institución tenga la necesidad implementar nuevas tecnologías, actualizaciones o reemplazos de sistemas obsoletos el personal de TI reconozca la importancia de ejecutarlos y mantenga los lineamientos necesarios para solventar las necesidades producidas sin afectar o caer en los riesgos que afecten la idea de negocio.[14]

El Gobierno de TI desempeña un papel importante al generar valor y reducir riesgos en la implementación de TI en una organización. Se enfoca en tres desafíos principales: optimización del riesgo, entrega de valor y optimización de recursos.

1.2.8. Partes de interés en Gobernanza

Las partes de interés de Gobernanza COBIT son los conocidos "stakeholders" [14],y son internos como externos que se presentan a continuación:

Tabla 3. Partes de Interés COBIT "Stakeholders"

COBIT Stakeholders	
Stakeholders	**Beneficios de COBIT**
Partes de interés interno	
Tablas	Proporciona información sobre cómo obtener valor del uso de TI y explica responsabilidades relevantes
Dirección Ejecutiva	Orienta sobre cómo organizar y monitorizar el desempeño de TI
Gerentes de negocios	Ayuda a comprender cómo obtener las soluciones TI que se requiere, y como explotar la nueva tecnología para nuevas oportunidades estratégicas
Gerentes de TI	Orienta la mejor manera de construir y estructurar el departamento de TI, gestionar el rendimiento de TI, ejecutar una operación de TI eficiente y eficaz,

	controlar los costos de TI, alinear la estrategia de TI con las prioridades comerciales, etc.
Proveedores de aseguramiento	Ayuda a gestionar la dependencia de proveedores de servicios externos, obtener aseguramiento sobre TI, y asegurar la existencia de un sistema eficaz y eficiente
Gestión de riesgos	garantiza la identificación y gestión de todos los riesgos relacionados con TI
Partes de interés externo	
Reguladores	Garantiza que la empresa cumpla con las normas y regulaciones además cuenta con el sistema de gobierno adecuado para administrar y mantener el cumplimiento
Proveedores de negocio	Garantiza que las operaciones de un socio comercial sean seguras y confiables, cumpliendo con las normas y reglamentos establecidos.
Proveedores de TI	Garantiza que las operaciones de un proveedor TI sean seguras y confiables conforme a las normas y reglamentos

Fuente: COBIT 2019[14]

1.2.9. Principios de un Sistema de Gobierno

Los principios de un sistema de gobierno se refieren a las características indispensables que deben estar presentes para establecer y mantener un sistema efectivo de gobierno. Estos principios son:

- Proporcionar valor a los sitios de interés.
- El enfoque holístico.
- El sistema de gobierno dinámico.
- Separar el gobierno de la gestión.
- Adaptar las necesidades de la empresa.
- Sistema de Gobierno Íntegro.

Figura 3. Principios del sistema de gobierno

Fuente: ISACA [14]

1.2.10. Partes interesadas en el gobierno

El público objetivo de COBIT son las partes interesadas en la GETI y, por extensión, las partes interesadas en el gobierno corporativo. Estas partes interesadas y los beneficios que pueden obtener de COBIT [5]

Tabla 4. Partes interesadas de gobierno

Parte interesada	Beneficio de COBIT
Internas	
Partes interesadas	Contribuye cómo obtener valor del uso de las TI y explica las responsabilidades relevantes del consejo
Dirección ejecutiva	Directrices de monitorización y desempeño de las TI_
Gerentes de negocio	Obtención de soluciones de TI, explotación nuevas tecnologías, acceso a nuevas oportunidades estratégicas
Gerentes de TI	Directrices para crear y estructurar el departamento de TI, gestión de desempeño de TI, operación de calidad de TI eficiente, costos de TI. _
Proveedores de aseguramiento	Gestión en dependencia de proveedores externos de servicio, aseguramiento de TI, controles de calidad
Gestión de riesgos	Asegurar la identificación y gestión de riesgo TI

externas	
Entidades reguladoras	Asegura que la empresa cumpla con toda la normativa y regulaciones aplicables, sistema de gobierno adecuado.
Socios de negocios	Garantiza seguridad en operaciones de un socio empresarial cumpla con toda la normativa y regulaciones
Proveedores de TI	Asegura que un proveedor de TI se confiable y cumplan con las normativas.

Fuente: ISACA[5]

Las partes interesadas de gobierno existen tanto internas como externas coma las internas están compuestas por las unidades de interés, la dirección, la gerencia, adiós los proveedores de aseguramiento y la gestión de riesgo; mientras que las partes de interés externas son las conocidas entidades reguladoras coma también los socios de negocios y los proveedores de TI, cada uno de estos aseguran o garantizan procesos que contribuyen al gobierno.

1.2.11. Objetivos de gobierno y gestión.

Los objetivos de gobierno y gestión se diseñaron para establecer y mantener un sistema efectivo de gobierno TI a las organizaciones, y se agrupan en cinco dominios principales [14], que incluye un total de 40 objetivos de gobierno y gestión que apuntan a un propósito clave en las áreas de acción de cada objetivo:

En COBIT (Control Objectives for Information and Related Technologies), los objetivos y gobiernos de gestión están diseñados para ayudar a las organizaciones a establecer y mantener un sistema efectivo de gobierno de TI. Estos objetivos y gobiernos de gestión se agrupan en cinco dominios principales:

1.2.11.1. EDM - evaluación dirección y monitoreo

Establece un marco sólido de gobierno de TI, se ocupa de la entrega de valor, la gestión de riesgos y la optimización de recursos de TI.

1.2.11.2. APO – alineación, planificación, organización

Alinea la estrategia de TI con los objetivos del negocio, planifica la gestión de TI y organiza la estructura de TI de manera eficiente.

1.2.11.3. BAI – Construcción, adquisición, implementación

Se enfoca en la implementación efectiva de soluciones tecnológicas y la gestión de cambios, incluyendo la gestión de programas y proyectos de TI, la adquisición e implementación de soluciones y la entrega de sistemas de TI.

1.2.11.4. DSS – entrega, servicio y soporte

Este dominio se centra en la entrega y el soporte continuo de servicios de TI, incluyendo la gestión del desempeño

Cada dominio tiene diferentes objetivos de gestión y gobierno como se puede observar en la figura 4:

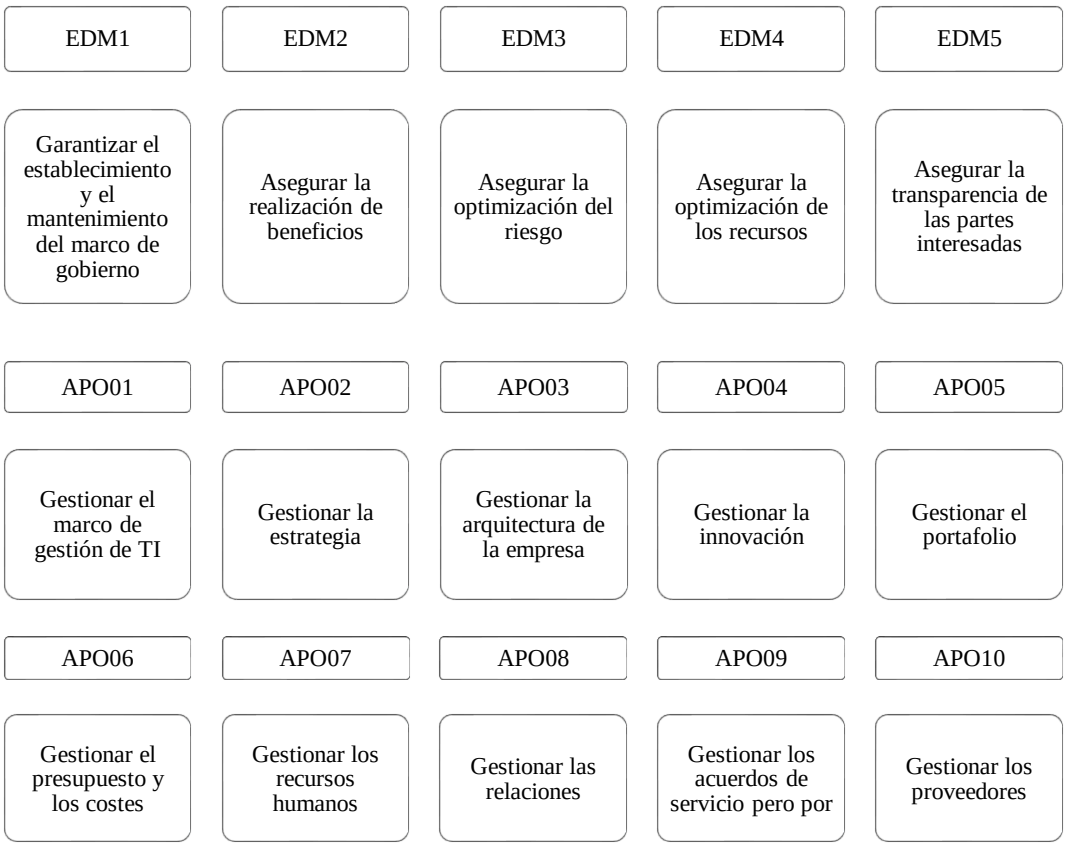


Figura 4. Objetivos de Gobierno y Gestión

Fuente: ISACA [5]

1.2.12. Factores de diseño.

Los factores de diseño del marco de referencia COBIT influyen en el posicionamiento de éxito a través del sistema de gobernanza TI, se compone de 10 tipos de factores que hacen que el sistema de gobierno influya en el manejo de los los 40 objetivos de gobierno y gestión.[5]

1.2.12.1. Estrategia empresarial

La estrategia empresarial nos indica cómo las instituciones o empresas funcionan, es decir su enfoque puede estar guiado al crecimiento, innovación, liderazgo o servicio y no necesariamente puede ser que su estrategia se base en una sola sino también con más prototipos.

Tabla 5. Factor de diseño de estrategia empresarial

Factor de diseño de estrategia empresarial	
Crecimiento/Adquisición	enfoque en el crecimiento.
Innovación/Diferenciación	enfoque en ofrecer productos diferentes y/o innovadores, y servicios a sus clientes.
Liderazgo en costos	enfoque en la minimización de costos a corto plazo.
Servicio al Cliente/Estabilidad	brindar un servicio estable y orientado al cliente.

Fuente: ISACA [16]

1.2.12.2. Objetivos empresariales

Toda institución Intenta alcanzar un equilibrio integrado y estratégico con el fin de crecer producir y competir a través de cuatro categorías de innovación y crecimiento, procesos internos, clientes y financieros conocidos como objetivos de empresariales, estos objetivos se encuentran determinados de la siguiente manera:

Tabla 6. Factores de diseño de objetivos empresariales

Factor de diseño de objetivos empresariales		
Referencia	**Cuadro de Mando Integral Dimensión**	**Objetivo empresarial**
EG01	Financiero	Portafolio de productos y servicios competitivos.

EG02	Financiero	Riesgo empresarial gestionado.
EG03	Financiero	Cumplimiento de leyes y reglamentos externos.
EG04	Financiero	Calidad de la información financiera.
EG05	Cliente	Cultura de servicio orientada al cliente.
EG06	Cliente	Continuidad y disponibilidad del servicio comercial.
EG07	Cliente	Calidad de la información de gestión.
EG08	Interno	Optimización de la funcionalidad del proceso de negocio interno.
EG09	Interno	Optimización de costes de procesos de negocio.
EG10	Interno	Habilidades, motivación y productividad del personal.
EG11	Interno	Cumplimiento de políticas internas.
EG12	Crecimiento	Programas de transformación digital gestionados.
EG13	Crecimiento	Innovación de productos y negocios.

Fuente: ISACA [5]

1.2.12.3. Perfil de riesgo

El perfil de riesgo de una institución y los problemas que están relacionados con TI nos indica que áreas de riesgo podrían estar excediendo y exponiendo a la empresa en posibles fracasos retrasos sobrecostos falta de fondos comose refiere a la evaluación de los riesgos de seguridad de la información y los controles necesarios para minimizar esos riesgos. El factor de diseño se refiere a la capacidad de un sistema de información para soportar los controles necesarios para mitigar los riesgos identificados.

En COBIT, los componentes del diseño del perfil de riesgo se conforman por tres elementos principales:

Factores de riesgo inherentes: Estos factores se refieren a las características específicas de la organización que pueden aumentar su exposición a los riesgos. Incluyen aspectos como la industria en la que opera, la complejidad de los procesos, la sensibilidad de la información y la importancia de los servicios que brinda.

Categorías de riesgo: Estas categorías representan las áreas clave en las que se deben identificar y evaluar los riesgos. COBIT propone cuatro categorías

principales: estratégicos, operativos, de cumplimiento y de informes financieros. Cada categoría abarca diferentes tipos de riesgos relacionados con los objetivos de la organización.

Factores de influencia del entorno: Estos factores consideran el contexto externo en el que la organización opera y pueden impactar su perfil de riesgo. Incluyen aspectos como cambios en la regulación, condiciones económicas, tendencias tecnológicas y amenazas cibernéticas.

Estos componentes del diseño del perfil de riesgo en COBIT ayudan a la organización a comprender y evaluar de manera efectiva los riesgos a los que se enfrenta, y brindan una base sólida para establecer un enfoque adecuado de gestión de riesgos.

1.2.12.4. Problemas relacionados con la TI

Indica el riesgo que se ha materializado con respecto a TI, estos pueden ser de distinta índole.

Tabla 7. Problemas relacionados con TI

Factor de diseño de problemas relacionados con TI	
Referencia.	**Descripción**
A	Baja contribución a valor de negocio.
B	Errores de iniciativas o una percepción de baja contribución
C	Incidentes relacionados con TI, pérdida de datos, brechas de seguridad, fallas en proyectos, errores de aplicación, entre otros.
D	Problemas de prestación de servicios en subcontratistas de TI
E	Incumplimiento de requisitos regulatorios o contractuales relacionados con TI
F	Desempeño de TI deficiente.
G	Gastos de TI ocultos y no autorizados.
H	Duplicaciones de iniciativas, despilfarro de recursos.
I	Recursos de TI insuficientes, personal inadecuado, agotamiento/insatisfacción.
J	proyectos no cumplen con las necesidades, entregas tardías o por encima del presupuesto
K	falta de compromiso patrocinadores comerciales para TI.
L	Modelo operativo de TI complejo y/o mecanismos de decisión poco claros para decisiones relacionadas con TI.
M	Costo de TI alto.

N	Implementaciones fallidas causadas por la arquitectura de TI actual
O	Brecha conocimiento comercial y técnico hablan diferentes idiomas.
P	Problemas integración de datos a través de diferentes fuentes.
Q	Falta de supervisión y control de calidad sobre las aplicaciones que se están desarrollando y poniendo en funcionamiento.
R	Departamentos con poca o ninguna participación del TI.
S	Incumplimiento de normas de seguridad y privacidad.
T	Incapacidad para innovar usando TI.

Fuente: ISACA [5]

1.2.12.5. Panorama de amenazas

El panorama de amenazas se determina según la empresa lo establezca ya puede ser de tipo normal o alto, cuando es de tipo normal de tipo Normal nos indica que la empresa o institución se desarrolla en un entorno con niveles de amenaza normales, mientras que alto nos indica que el entorno de amenazas en el cual se desarrolla es elevado, estas consideraciones pueden catalogarse debido a diferentes factores cómo situación geopolítica, sector industrial o perfil específico.

1.2.12.6. Requerimientos de cumplimiento

Pueden ser de tipo bajos, normales y altos cada uno de ellos tienen su explicación coma en el caso de requisitos de cumplimiento bajo nos indica que la empresa está sujeta a un mínimo de requerimientos regulares para su cumplimiento mientras que los de cumplimiento normal nos indica que su nivel de cumplimiento es regular y común a diferencia del cumplimiento de tipo alto que los requisitos deben ser mayores a la media y por lo general están relacionados al sector industrial o a condiciones geopolíticas

1.2.12.7. Diseño de TI

Puede clasificarse en Soporte, Fábrica, Cambio y Estratégico.

Tabla 8.Factor de diseño TI

Papel del factor de diseño de TI	
Rol de TI	**Explicación**
Soporte (Support)	TI no es crucial para el funcionamiento y la continuidad de los servicios y procesos de negocio, ni para su innovación.
Fábrica (Factory)	Cuando TI falla, el impacto es inmediato tanto en el funcionamiento como la continuidad de procesos y servicios. TI no se ve como motor de innovación.
Cambio (Turnaround)	TI es un motor de innovación de procesos y servicios. no depende en su totalidad la continuidad de los procesos comerciales y servicios.
Estratégico (Strategic)	La TI es fundamental para ejecución e innovación de procesos y servicios.

Fuente: ISACA [5]

Si la institución u organización cuenta con tan solo soporte TI Nos dará una idea de que las TI tan sólo se dedicará al proceso de soporte y no jugará un papel importante en la continuidad de procesos y servicios las TI no serán responsables en su totalidad de impulsar el desarrollo e innovación mientras que si las TI asumen el rol de fábrica esto nos indicará que las TI podrán a actuar inmediatamente pero aun así no son el motor de innovación, el rol de las TI como un cambio asumirá el papel de un motor de innovación pero aun así no depende en su totalidad de ser o actuar como un ente de ejecución e innovación de procesos como lo es el rol estratégico de TI

1.2.12.8. Abastecimientos TI

Se puede clasificar en Externalización/Tercerización (outsourcing), Nube, Internalizado (insourced) e Híbrido

Tabla 9. Abastecimiento TI

Modelo de abastecimiento para factor de diseño de TI	
modelo de abastecimiento	**Explicación**
Subcontratación	Se recurre a servicios de un tercero para proporcionar servicios de TI.
Nube	Se maximiza el uso de la nube para brindar servicios de TI a sus usuarios.
Internalizado	Se proporciona su propio personal y servicios de TI.

Híbrido	Se aplica un modelo mixto, combinando los tres modelos anteriores en diversos grados.

Fuente: ISACA [5]

La subcontratación es uno de los modelos de abastecimiento a la cual la empresa recurre a los servicios de un tercero para proporcionar servicios de TI. Cuando la empresa maximiza el uso de la nube y brinda servicios a sus usuarios es otro modo de abastecimiento TI, mientras que el internalizado proporciona a la empresa su propio personal y servicio de TI, y se hace mención del híbrido se aplica como modelo mixto combinando los tres modelos anteriores en diversos grados.

1.2.12.9. Métodos de implementación de TI

Los métodos de implementación se clasifican en Ágiles, DevOps, Tradicionales e Híbridos:

Tabla 10. Métodos de implementación TI

Factor de diseño de métodos de implementación de TI	
Método de implementación TI	**Explicación**
Agile	métodos de trabajo de desarrollo ágil para desarrollo de software.
DevOps	Uso DevOps para la construcción, implementación y operaciones de software.
Tradicional	enfoque clásico hacia el desarrollo de software como método cascada y separa el desarrollo de software y las operaciones.
Híbrido	combinación de implementación de TI tradicional y moderna, a menudo denominada "TI bimodal".

Fuente: ISACA [5]

1.2.12.10. Estrategia de adopción de tecnología

Las estrategias de adopción de tecnología son enfoques diseñados para una implementación exitosa de nuevas tecnologías en una organización.[5] Estas estrategias están destinadas a garantizar que la adopción de la tecnología sea efectiva y que los beneficios esperados se logren de manera óptima. Estas

estrategias pueden clasificarse en el que primero se mueve (First mover); Seguidor (Follower) y adaptadores lentos (Slow adopter).

Tabla 11.Estrategia de adopción de tecnología

Factor de diseño de estrategia de adopción de tecnología	
Estrategia de adopción de tecnología	**Explicación**
Primer movimiento	La empresa generalmente adopta nuevas tecnologías lo antes posible y obtiene la ventaja de ser el primero en ventaja.
Seguidor	Espera a que la nueva tecnología se generalice y se pruebe antes de adoptarla.
Adoptador lento	La adopción de nuevas tecnologías es lenta.

Fuente: ISACA [5]

1.2.12.11. Dimensión de la empresa

Se identifican dos categorías Empresas Grandes (predeterminada), Pequeñas y medianas empresas

Tabla 12. Dimensión de la empresa

Explicación del factor de diseño del tamaño	
Tamaño de las empresas	**Explicación**
Gran empresa (predeterminado)	Empresas con más de 250
Pequeña y mediana empresa	Empresa con 50 a 250

Fuente: ISACA [5]

1.2.13. Cascada de metas.

A partir de las necesidades de las partes interesadas, se establecen las metas empresariales. Estas metas se convierten en prioridades, que se traducen en metas de alineamiento. Estas metas de alineamiento se desglosan en una serie de objetivos de gobierno. La cascada de metas permite la priorización de los objetivos, basándose en la priorización de las metas institucionales.[5]

Las metas empresariales y las metas de alineamiento permiten determinar los objetivos de gobierno y gestión, estas metas son establecidas a través de los

conceptos procesos y actividades que se realizan por las unidades o partes interesadas de la institución.

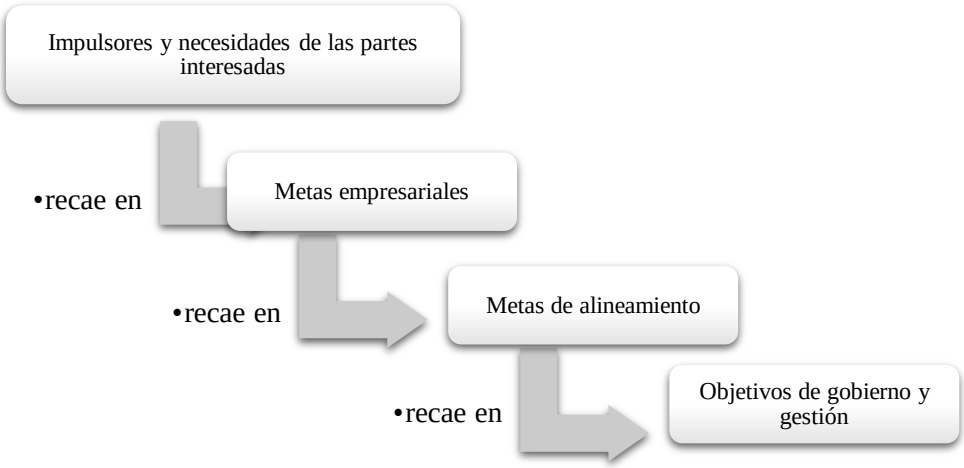


Figura 5. Cascada de metas COBIT

Fuente:[5]

1.2.13.1. Metas empresariales

Las metas empresariales se refieren a los objetivos que una organización se propone alcanzar en relación con la gobernanza y gestión de la tecnología de la información. Estas metas están alineadas con los objetivos estratégicos y operativos de la organización. Las metas empresariales en COBIT 2019 son amplias y abarcan diferentes aspectos relacionados con el uso efectivo de la tecnología de la información para lograr resultados efectivos. Algunos ejemplos de metas empresariales en COBIT pueden incluir:

Alcance de la alineación estratégica: Asegurar que la TI esté alineada con los objetivos estratégicos de la organización y que contribuya a su éxito empresarial.

Entrega de valor: Maximizar los beneficios y el valor generado por los activos de TI, asegurando una inversión adecuada y una gestión eficiente de los recursos de TI.

Gestión de riesgos: Identificar, evaluar y gestionar los riesgos asociados con la tecnología de la información, incluyendo la seguridad de la información, la protección de los activos y la continuidad del negocio.

Optimización de recursos: Utilizar los recursos de TI de manera eficiente y efectiva para lograr los objetivos empresariales, optimizando el uso de sistemas, infraestructura, datos y personal.

Cumplimiento normativo: Cumplir con los requisitos legales, regulaciones y estándares relacionados con la tecnología de la información, asegurando la transparencia y el cumplimiento de las políticas y normas establecidas.

Estas metas empresariales en COBIT proporcionan una guía para el diseño, implementación y mejora de los procesos de gobernanza y gestión de TI en una organización, ayudando a alinear la TI con los objetivos y prioridades empresariales, maximizando el valor de la inversión en TI y gestionando los riesgos asociados de manera efectiva.

1.2.14. Diseño e Implementación de un Sistema de Gobierno de TI

Para el diseño e implementación del sistema de Gobierno de TI en la Dirección de Tecnologías de la Información y Comunicación (DTIC), nos enfocaremos en los 4 aspectos principales que nos brinda el modelo de Gestión COBIT 2019.

La metodología de gestión COBIT nos brinda distintas etapas y pasos del proceso de diseño, como se visualizar en la figura, los cuales inician con diversas recomendaciones para priorizar los objetivos de gobierno y gestión o componentes del sistema de gobierno relacionados con estos, para alcanzar niveles de capacidad, o para adoptar variantes específicas de un componente del sistema de gobierno.

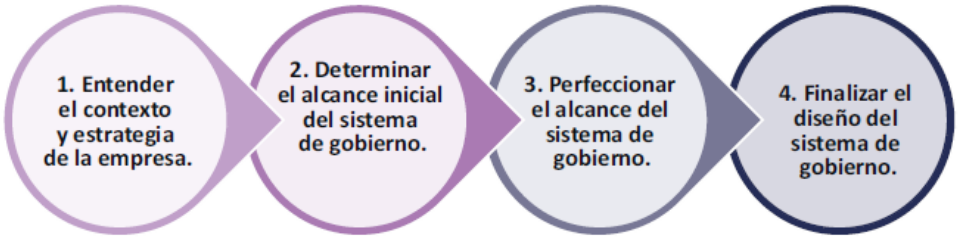


Figura 6. Diseño de un sistema de Gobierno de TI

Fuente: ISACA [5]

Algunos de estos pasos o subpasos podría derivar en recomendaciones contradictorias, lo cual es inevitable cuando se consideran un gran número de factores de diseño, la naturaleza genérica en su conjunto de la guía de factores de diseño y las tablas de asignación utilizadas.

Si se logran adaptar dichos pasos previamente mencionados la Dirección de Tecnologías de la Información y Comunicación (DTIC) logrará contar con un sistema de gobierno adaptado a sus necesidades

1.3. Fundamentación del Estado del Arte

Estudios demuestran que el marco metodológico COBIT 2019 es un marco de gobierno de tecnología de la información (TI) utilizado para ayudar a las empresas a gestionar los riesgos y los recursos de TI de manera efectiva. Problemas como:

Falta de alineación con los objetivos en las organizaciones en donde puede haber una desconexión entre los procesos de gobierno de TI, controles inadecuados que conducen a riesgos para la seguridad, ineficacia en la gestión de la TI, falta de recursos para implementación de nuevas tecnologías, expansión de servicios, entre otros; han generado la necesidad de crear controles adecuados que comprometan y participen junto con las TI y mantengan las ideas de negocio en constante evolución.

Cortes, 2019 [17] presenta su investigación de evaluación por medio de la metodología COBIT 2019 del modelo de gestión de TI en la Municipalidad de Carrillo producto de los procesos de migración de sistemas operativos e informáticos, en el cual propone reunir 7 componentes para el diseño de un sistema de gobierno y asi poder determinar los niveles actuales de la municipalidad además

de la identificación de brechas de complimiento en periodos de gobernabilidad y migración de sistemas operativos e informáticos.

El estudio arroja información que la entidad la denominó “brechas de cumplimiento”, en donde el investigador deja como una representación de oportunidades de mejora continua para cumplimiento de su misión como municipalidad, además deja como valor agregado un instrumento electrónico como plan de acción de brechas con el cual la municipalidad podrá tomar acciones, planificarlas y priorizarlas para el desarrollo e innovación institucional.

COBIT 2019 es una herramienta valiosa para la gestión de TI, pero también puede presentar desafíos significativos. Es importante que las organizaciones comprendan completamente los controles adecuados, tengan los recursos necesarios y esté dispuesta a comprometerse con un marco de gobierno de TI complejo y en constante evolución.

Esta metodología se ha implementado en diversas organizaciones, en una amplia gama de sectores como es el caso tambien del ejército ecuatoriano, investigadores como López, Bolívar, Chauca, 2020 [18] realizan un análisis de implementación de procesos de gobierno COBIT 2019 en la dirección de tecnologías de la información y comunicaciones del ejército ecuatoriano, en donde se detecta la problemática de ausencia de procedimientos adecuados que le permita a la institución lograr un gobierno y gestión de TI eficaz.

Al aplicar el modelo obtenido COBIT y realizar el análisis con respecto a los objetivos estratégicos institucionales resulta que el 80% de alineamiento a los objetivos estratégicos genera un alto impacto en el modo de actuar a los diferentes procesos de la institución.

Se identificaron 7 metas de alineación TI-Institucional como: la gestión de riegos, prestación de servicios de TI, seguridad de la información, calidad en la gestión e información, entre otros, lo que beneficia a la institución conocer el estado en el cual se encuentra en cuanto a procesos internos, papel fundamental que juega las TI en la institución, y poder tener las rutas de mejora continua.

De las propuestas de investigación se puede observar que las instituciones muchas de las veces no cuentan con un servicio de TI que participe y promueva la gobernanza de TI, una vez conocido y establecido un marco metodológico de gobernanza las instituciones logran la generación de valor e impulsan el desarrollo y mantención de la misión y visión empresarial, reducen las posibilidades de riesgo en las actividades y procesos cotidianos.

1.4. Conclusiones Capítulo I

COBIT presenta un alto grado de importancia en alineación estratégica TI con los objetivos organizacionales, promueve un enfoque holístico en la gobernanza de TI, reconociendo que la gobernanza no se limita solo a aspectos tecnológicos, sino que abarca también aspectos organizativos de procesos, personas y cultura.

COBIT gestiona riesgos, destaca la importancia identificar, evaluar y gestionar los riesgos asociados con la tecnología de la información de manera efectiva en un proceso gobernante que tiene como objetivo el proteger la continuidad del establecimiento o institución.

COBIT fundamenta la cultura de generación de valor a las TI, las organizaciones deben asegurarse de que las TI esté generando beneficios y valor tangible para la organización, maximizando el retorno de la inversión y optimizando el uso de los recursos de TI.

COBIT promueve una cultura de mejora continua en la gobernanza de TI, mantiene el compromiso de perfeccionamiento constante de procesos y prácticas de gobernanza, utilizando métricas y evaluaciones para identificar áreas de intervención de mejora y realizar ajustes necesarios.

En instituciones como la Municipalidad de Carrillo en Costa Rica[17], Ejercito Ecuatoriano en Ecuador [18]se han desarrollado marcos teóricos de gobernanza TI en donde la parte gerencial y administrativa tienen ya conocimiento de buenas prácticas y lineamientos efectivos en dónde cada una de las áreas participantes dentro de estas instituciones tienen ya identificado, definido y comunicado los roles

y responsabilidades a través de políticas internas de cumplimiento y así garantizar una rendición de cuentas en el uso de los recursos de TI.

CAPÍTULO II

PROPUESTA

La presente propuesta metodológica y tecnológica avanzada pretende proporcionar un conjunto de prácticas y lineamientos de gobernanza efectivos de las TI en el Hospital General Docente Ambato, para lo cual se desarrollará el diseño de un plan de gobernanza TI utilizando el marco COBIT 2019 a través de un diagnóstico de evaluación de madurez en gobernanza de TI, identificar áreas de mejora y establecer objetivos específicos para el plan, para esto se utilizará una metodología mixta que combina la recopilación de datos cualitativos y cuantitativos. Se llevarán a cabo entrevistas con stakeholders clave de la organización para comprender la situación actual de la gobernanza de TI y recopilar información relevante. También se realizará un análisis documental de los procesos y controles existentes. En el desarrollo de este plan participaron: Ing. Juan Villacis como investigador y el Mg. Matius Mendoza como tutor del proyecto, además con la colaboración de los funcionarios líderes de servicios directivo y administrativo del Hospital General Docente Ambato que su participación generará un aporte efectivo en la toma de decisiones en beneficio de los pacientes de esta casa de salud.

2.1. Diagnóstico del problema.

La ciudad de Ambato localizada en la región centro del país, tiene una población qué representa el 65.1% del total de la provincia de Tungurahua el cual ha tenido un ritmo de crecimiento del 2% promedio anual con un total de 287282 habitantes. [19]

Como institución de regulación de salud nacional que forma parte del ministerio de Salud Pública del Ecuador genera una atención promedio de 40 operaciones diarias entre ellos partos, cesáreas, neurocirugías, ginecoobstetras, etc. Reconocido como hospital centinela de tratamientos de salud para las poblaciones de las provincias de Tungurahua, Bolívar, Pastaza, Cotopaxi, Chimborazo y Morona Santiago. [20]

En la actualidad el Hospital General Docente Ambato ubicado en el sector de Cashapamba parroquia la Merced en las avenidas Luis Pasteur y Unidad Nacional

cuenta con 132 profesionales especialistas de salud entre ellos son especialistas médicos residentes y especialistas médicos devengantes de beca y un total de 1198 funcionarios en donde se atienden áreas medicas como: medicina interna, cirugía, traumatología, pediatría, ginecoobstetricia, neonatología, emergencia, odontología, imagenología, rehabilitación y terapia física, laboratorio, centro de transfusión, nutrición y dietética, medicamentos e insumos médicos, centro quirúrgico, terapia intensiva, anatomía patológica y audiología. [21]

Además áreas administrativas como: gerencia, dirección asistencial, comunicación, asesoría jurídica, planificación, seguimiento y evaluación de la gestión, calidad, vigilancia epidemiológica, dirección administrativa financiera, gestión administrativa, mantenimiento, contratación pública, activos fijos, servicios generales, gestión financiera, administración de caja, contabilidad, recaudación, talento humano, tecnologías de la información y comunicación, atención al usuario, gestión de riesgos, sala primera cogida y admisiones.

La unidad de Gestión de Tecnologías de la Información y Comunicaciones según el estatuto de estructura básica de Hospitales del Ministerio de Salud Pública del Ecuador su misión es el "aplicar las normas y procedimientos que efectivicen la gestión y administración de las tecnologías de la información y comunicaciones, orientadas a la optimización de los recursos y fortalecimiento de la red interna para mejorar la eficiencia en la atención a los pacientes".[11]

Según el Estatuto Orgánico Gestión Organizacional por Procesos de Hospitales del Ministerio de Salud Pública del Ecuador, la Unidad de Tecnologías de la Información y Comunicaciones (TICs) tiene como:

2.1.1. Misión TIC

Aplicar las normas y procedimientos que efectivicen la gestión y administración de las tecnologías de la información y comunicaciones, orientadas a la optimización de los recursos y fortalecimiento de la red interna para mejorar la eficiencia en la atención a los pacientes. [3]

Las TICs en el Hospital General Docente Ambato aplica esta misión que hereda de la Dirección Nacional de Tecnologías para cumplimiento de sus actividades internas y de apoyo a las demás unidades tanto medicas como administrativas.

2.1.2. Productos y Servicios TIC

La Unidad de TI tiene como productos y servicios el de: mantener líneas de red, tomar acciones de prevención y corrección de software y Hardware, Informar y dar a conocer cuáles son las acciones realizadas dentro de la unidad además acciones en cuanto se refieren a redes de conectividad; Planes de mejoramiento y contingencias en respaldos de la información, mantenimiento de software, sistemas de información, central telefónica, servicios de internet, correos institucionales; inventarios, actas de equipamiento tecnológico computacional coordinados con activos fijos; Informes de funcionamiento y traslados de equipamiento tecnológico igualmente con activos fijos y bodega.

2.1.3. Estructura Organizacional TIC

La unidad de Tecnologías de la Información y Comunicaciones se encuentra dirigida directamente por la Dirección Administrativa Financiera que ésta a su vez se encuentra dirigida por la Gerencia que es la máxima autoridad de la institución hospitalaria, además la unidad de TICs recibe directrices de la Coordinación Zonal 3 Salud, y también del Ministerio de Salud del Ecuador.

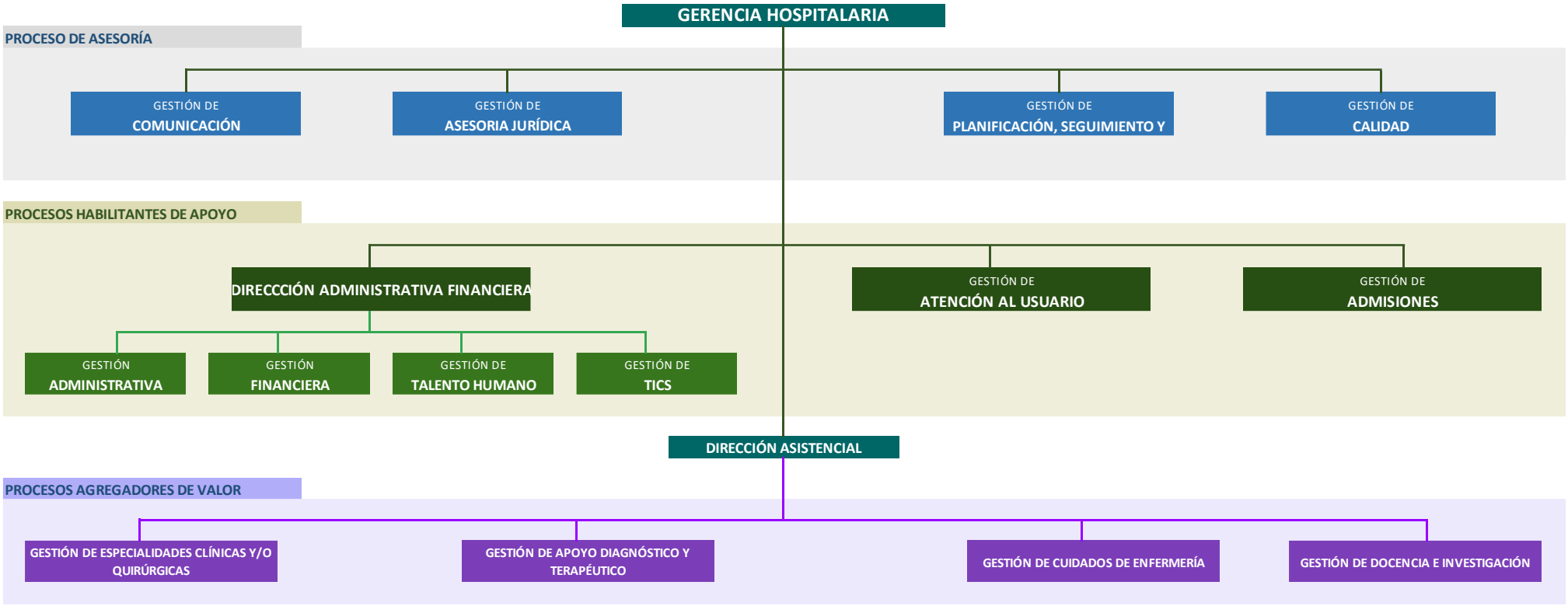


Figura 7. Estructura de Hospitales

Fuente: Tomado de Acuerdo Ministerial 1537 MSP [11]

La unidad de Tecnologías de la Información y Comunicaciones está conformada por 3 subáreas que son: Tecnologías de la Información, Redes Comunicaciones e Infraestructura y Soporte Técnico [22], conformándose por un grupo de 6 servidores públicos entre analistas y asistentes de la siguiente manera:

Tabla 13. Grupo de Analistas y Asistentes TIC

	ÁREA	**ANALISTAS Y ASISTENTES**
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	TECNOLOGÍAS DE LA INFORMACIÓN	Analista de Tecnologías de la Información y Comunicaciones 3
		Analista de Tecnologías de la Información y Comunicaciones 2
		Analista de Tecnologías de la Información y Comunicaciones 1
	REDES COMUNICACIONES E INFRAESTRUCTURA	Analista de Redes. Comunicaciones e Infraestructura
	SOPORTE TÉCNICO	Analista de Soporte Técnico
		Asistente de Soporte Técnico

Fuente: Tomado de Clasificación de puestos Hospitales [22]

2.1.4. Disposiciones Generales:

Según [3] a todas las unidades técnicas de Hospitales deberán sujetarse al esquema del estatuto orgánico gestión por procesos, así como también las normas y procedimientos internos para la ejecución administrativa.

2.1.5. Servicios TIC:

La Unidad de Tecnologías de la Información y Comunicaciones del Hospital General Docente Ambato realiza varias actividades de soporte técnico que son recibidas a través de la mesa de ayuda que las demás unidades reportan.

Tabla 14. Actividades TIC

No.	ACTIVIDAD
1	Quipux Creación cuenta
2	Quipux Activación cuenta
3	Quipux Desactivación cuenta
4	Quipux Actualización cuenta
5	Quipux Reseteo cuenta
6	Quipux Solicitud de Respaldos
7	Quipux Descarga y Entrega de Respaldos
8	Quipux Creación/Actualización lista de envío
9	Correo institucional/Zimbra Creación cuenta
10	Correo institucional/Zimbra Activación cuenta
11	Correo institucional/Zimbra Desactivación cuenta
12	Correo institucional/Zimbra Actualización cuenta
13	Correo institucional/Zimbra Reseteo cuenta
14	Correo institucional/Zimbra Respaldo información cuenta
15	Correo institucional/Zimbra Creación/Actualización lista de difusión
16	Apoyo en Aplicaciones web y Navegadores
17	Instalación/Configuración de Aplicaciones web y Navegadores
18	Nube institucional
19	Apoyo en Programas Utilitarios / S.O.
20	Instalación de Programas Utilitarios
21	Hw Portátil/CPU/Monitor/Mouse/Teclado
22	Formateo de computador
23	Sw Impresora/Escáner
24	Hw Impresora/Escáner

25	Toner/tinta/cinta
26	Sw Dispositivos externos Flash/Disco Externo/Cámara/Micrófono/Audífonos/Tablet/Lector Barras/Otros
27	Hw Dispositivos externos Flash/Disco Externo/Cámara/Micrófono/Audífonos/Tablet/Lector Barras/Otros
28	Telefonía IP / Analógica
29	Respaldo parcial computador/dispositivo
30	Respaldo total/recuperación información de computador-dispositivo
31	Virus en dispositivos extraíbles
32	Virus en Portátil/PC Escritorio
33	Videoconferencias
34	Manejo de audio y video en eventos
35	Configuración de internet en Portátil/PC Escritorio
36	Instalación de nuevo punto de red/LAN/wifi
37	Apoyo proyector/cámara videovigilancia/televisor
38	Asesoría/Capacitación N1 y N2
39	Sw Servidor de Internet
40	Hw Servidor de Internet
41	Sw Servicios de la intranet
42	Hw Servicios de la intranet
43	Sw Servidor de Nube Institucional
44	Hw Servidor de Nube Institucional
45	Sw Servidor de Correo Institucional
46	Hw Servidor de Correo Institucional
47	Sw Otros servidores
48	Hw Otros servidores
49	Sw Dispositivos red
50	Hw Dispositivos red
51	Notificación a Proveedor de Servicios TI (ticket)
52	Seguimiento a la Notificación a Proveedor de Servicios TI (ticket)
53	Notificación a Administrativo EOD

54	Seguimiento a la Notificación Administrativo EOD
55	Notificación a Proveedor (Garantía Equipo Tecnológico)
56	Seguimiento a Notificación Proveedor (Garantía Equipo Tecnológico)
57	COVID19-PCR / Otros Aplicativos Creación cuenta
58	COVID19-PCR / Otros Aplicativos Activación cuenta
59	COVID19-PCR / Otros Aplicativos Desactivación cuenta
60	COVID19-PCR / Otros Aplicativos Actualización cuenta
61	COVID19-PCR / Otros Aplicativos Reseteo cuenta
62	Organización de cableado / cambio de puesto
63	Administraciones listas negras
64	Difusión Oficial de Comunicados
65	Criterio Técnico TICs - Informe

Elaborado por: Investigador

Las 65 actividades TIC que se realizan en el hospital no se lo realizan mediante niveles de atención simplemente se han dividido en diferentes áreas para cada analista determinando y un índice de satisfacción calificador de los usuarios a través de una encuesta de solución de problemas reportados y atendidos.

Sin embargo, las actividades en la unidad de TI no cuentan con marco referencial que se alinee con los objetivos estratégicos hospitalarios y que el servicio TI impulse el logro de los objetivos institucionales.

Además, las actividades anteriormente nombradas de TI no se encuentran estructuradas para el desarrollo de buenas prácticas para la gestión de procesos, y las ineficiencias operativas se encuentran latentes, por lo que la falta de cumplimiento de políticas internas y la implementación de normativas no generan un espacio de transparencia en la rendición de cuentas que minimicen desperdicios de recursos y maximicen retornos de inversión en TI.

2.2. Métodos Específicos de la Investigación

Se ha decidido usar la metodología COBIT 2019 compuesta por 4 fases para el diseño de sistema de gobierno TI y son las siguientes: entender el contexto de los planes estratégicos del hospital, el alcance inicial del sistema de gobierno, perfección del sistema de gobierno, solución de conflictos y finalización del sistema de gobierno. [16]

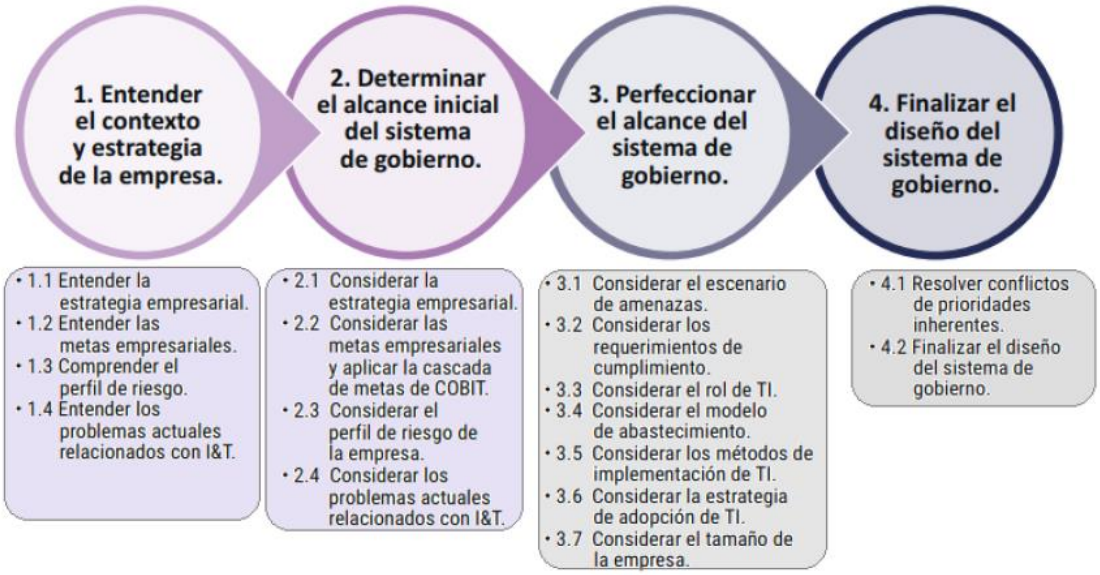


Figura 8. Fases del diseño del sistema de gobierno

Fuente: ISACA [16]

2.2.1. Metodología COBIT 2019

Como se vio en el Capítulo anterior COBIT 2019 a través de sus principios, políticas y procesos esta metodología ofrece orientación para mejorar la eficiencia operativa, la toma de decisiones basada en información confiable, la gestión de riesgos y la transparencia en la organización. Para comprender el contexto y estrategia del hospital se analizan 4 secciones, en donde se identifica los puntos fuertes y áreas de mejora para la correcta alineación estratégica de TI.

2.2.1.1. Estrategia empresarial

El hospital tiene diferentes estrategias en las cuales se mantiene como un nivel prioritario el Servicio al Cliente/Estabilidad por su naturaleza el de servir a la

ciudadanía en servicios de salud, seguido por Innovación/Diferenciación ya que por temas presupuestarios a nivel nacional la institución depende de un presupuesto aprobado por el Ministerio de Finanzas[23] asignados para el sector Salud, no se deja de lado procesos de renovación e innovación, y finalmente un grado bajo en los temas de liderazgo de costos y crecimiento/adquisición, considerándose 5 como el punto más importante y 1 el menos importante.

Tabla 15. Estrategia empresarial

Valor	Importancia (1-5)
Crecimiento/Adquisición	1
Innovación/Diferenciación	2
Liderazgo en costes	1
Servicio al cliente/Estabilidad	5

Adaptado: [16]

El grado de importancia más alto es el servicio al cliente y estabilidad ya que por ser una institución de salud el servicio al paciente es primordial por lo que se considera que la importancia tiene un grado 5, seguido de la innovación y diferenciación lo que nos indica que también es importante para el hospital mantener la innovación tanto en infraestructura como servicios, el liderazgo en costes y el crecimiento tienen una importancia baja debido a que la conformación del hospital es un hospital general que tendrá que realizar estudios de proyección para poder habilitar o considerar un grado alto al igual que el liderazgo en costes ya que el liderazgo se depende al 100% del presupuesto nacional. Los niveles de importancia son datos obtenidos de la encuesta realizada que se encuentra en el **Anexo 1.** Arrojando resultados siguientes:

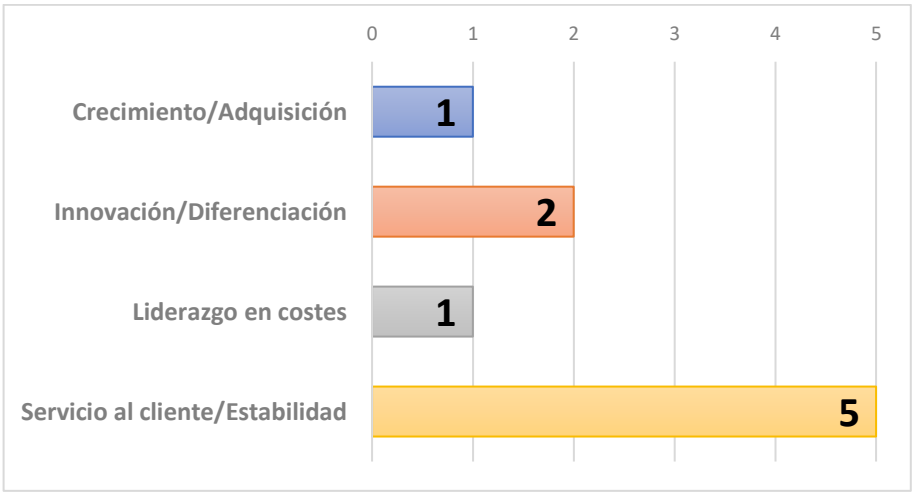


Figura 9. Factores de diseño estrategia empresarial

Adaptado de: [5]

2.2.1.2. Objetivos empresariales

Los objetivos institucionales respaldan la estrategia empresarial ya que están basados y estructurados a lo largo del cuadro de mando integral en áreas como Financiero, atención al usuario, entre otros que promueven los controles internos y de crecimiento.[5]

Tabla 16. Objetivos empresariales

Valor	Importancia (1-5)
EG01—Portafolio de productos y servicios competitivos	4
EG02—Gestión de riesgo del negocio	3
EG03—Cumplimiento de leyes y regulaciones externas	5
EG04—Calidad de la información financiera	1
EG05—Cultura de servicio orientada al cliente	4
EG06—Continuidad y disponibilidad del servicio del negocio	5
EG07—Calidad de la información de gestión	2
EG08—Optimización de la funcionalidad de los procesos internos del negocio	3
EG09—Optimización de costes de los procesos del negocio	1
EG10—Habilidades, motivación y productividad del personal	4
EG11—Cumplimiento con las políticas internas	5

EG12—Gestión de programas de transformación digital	3
EG13—Innovación de productos y negocios	4

Adaptado: [16]

Estos objetivos de estrategia empresarial se los cataloga en un rango de uno a cinco considerándose 5 como el nivel más alto de importancia que tendría cada uno para cumplir estás meta, entre ellos se determina como metas más importantes por cumplir: el cumplimiento de leyes y regulaciones externas, también el cumplimiento con las políticas internas ya que por acción ministerial el hospital debe cumplir los catálogos de normas, políticas, reglamentos, protocolos, manuales, planes y guías del ministerio de salud. Los niveles de importancia son datos obtenidos de la encuesta realizada que se encuentra en el **Anexo 1.** Arrojando resultados siguientes:

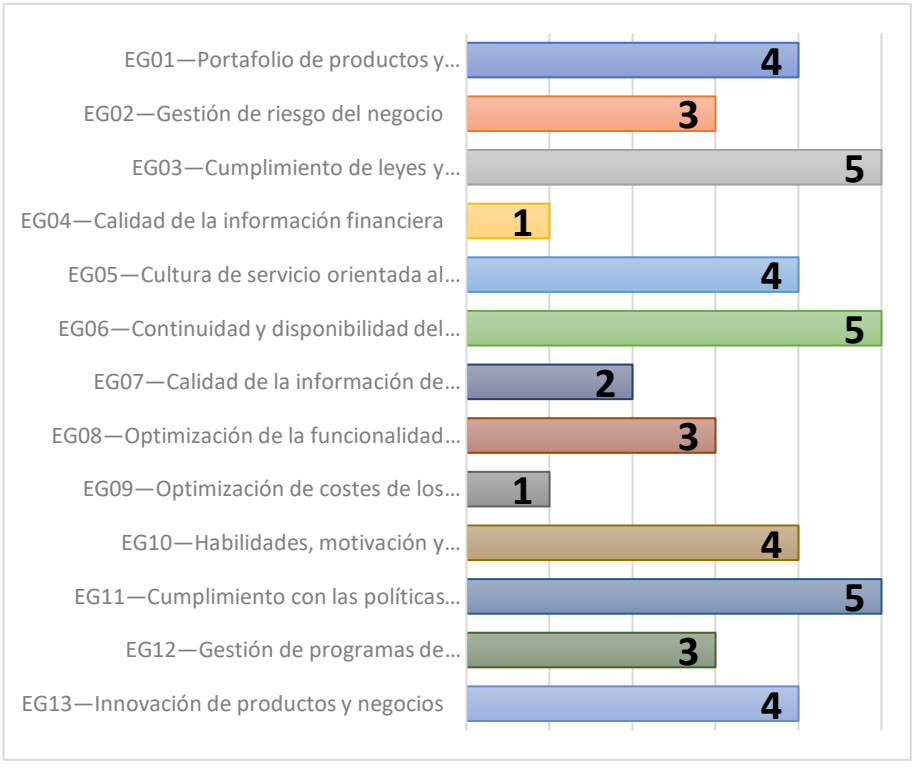


Figura 10. Factores de diseño metas empresariales

Adaptado de: [5]

2.2.1.3. Perfil de riesgo

Comprender el perfil de riesgo de un sistema de gobierno es tener en cuenta el perfil de riesgo que podría causarse en la institución esto conlleva a conocer los diferentes y posibles escenarios de riesgo que pueden causar afectaciones a la empresa por lo que su evaluación en su impacto y probabilidad de materializarse es importante es por ello que se toma en cuenta el listado de categorías de escenarios en la tabla siguiente evaluando la probabilidad de que el escenario pueda ocurrir teniendo en cuenta también controles de mitigación y calificación de riesgos.

Tabla 17. Perfil de Riesgo

Categoría del escenario de riesgo	Impacto (1-5)	Probabilidad (1-5)
Toma de decisiones sobre inversiones en TI, definición y mantenimiento del portafolio	5	1
Gestión del ciclo de vida de los programas y proyectos	4	3
Coste y control de TI	2	2
Comportamiento, habilidades y conocimiento de TI	4	4
Arquitectura de la empresa/TI	2	2
Incidentes de infraestructura operativa de TI	3	2
Acciones no autorizadas	3	4
Adopción de software/problemas de uso	4	3
Incidentes de hardware	2	2
Fallos de Software	3	3
Ataques lógicos (hacking, malware, etc.)	4	5
Incidentes de terceros/proveedores	2	2
Incumplimiento	3	3
Problemas geopolíticos	2	2
Acción industrial	1	3
Actos de la naturaleza	3	3
Innovación basada en la tecnología	5	3
Medio ambiente	2	3
Gestión de datos e información	4	4

Adaptado: [16]

Cada uno de los escenarios de riesgo presenta un nivel de impacto en la institución al igual que la probabilidad de que suceda cada evento, así mismo cada uno de estos escenarios se clasifica depende al nivel de riesgo en el que se pueden presentar, estos pueden ser muy alto normal y bajo por lo que nos representa y nos categoriza cada uno de estos riesgos a tomar en cuenta en el diseño de sistema de gobierno de información y tecnología.

En la siguiente figura se presenta las categorías de los escenarios de riesgo con su correspondiente clasificación probabilidad e impacto.

Tabla 18. Categorización de riesgo de TI

Categoría del escenario de riesgo	**Impacto (1-5)**	**Probabilidad (1-5)**	**Clasificación**
Toma de decisiones sobre inversiones en TI, definición y mantenimiento del portafolio	**5**	**1**	
Gestión del ciclo de vida de los programas y proyectos	**4**	**3**	
Coste y control de TI	**2**	**2**	
Comportamiento, habilidades y conocimiento de TI	**4**	**4**	
Arquitectura de la empresa/TI	**2**	**2**	
Incidentes de infraestructura operativa de TI	**3**	**2**	
Acciones no autorizadas	**3**	**4**	
Adopción de software/problemas de uso	**4**	**3**	
Incidentes de hardware	**2**	**2**	
Fallos de Software	**3**	**3**	
Ataques lógicos (hacking, malware, etc.)	**4**	**5**	
Incidentes de terceros/proveedores	**2**	**2**	
Incumplimiento	**3**	**3**	
Problemas geopolíticos	**2**	**2**	
Acción industrial	**1**	**3**	
Actos de la naturaleza	**3**	**3**	
Innovación basada en la tecnología	**5**	**3**	
Medio ambiente	**2**	**3**	
Gestión de datos e información	**4**	**4**	

	Riesgo muy alto
	Riesgo alto
	Riesgo normal
	Riesgo bajo

Adaptado: [16]

Los niveles de importancia son datos obtenidos de la encuesta realizada que se encuentra en el **Anexo 1.** Arrojando resultados siguientes:

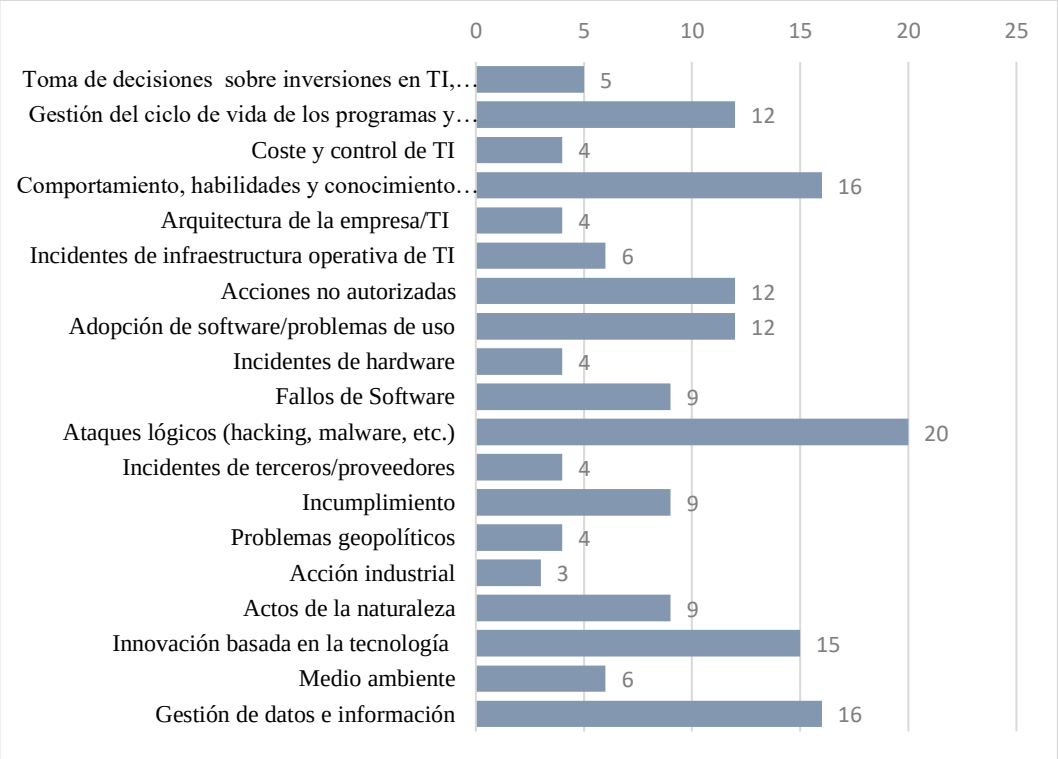


Figura 11. Escenario de Riesgos de TI

Adaptado: [16]

La categoría genérica del riesgo de TI está determinada por la multiplicación del impacto por el grado de probabilidad lo que nos dará un resultado en el rango de cero a 25 componiéndose por los niveles de riesgo, alto, medio, normal y bajo.

2.2.1.4. Problemas relacionados con TI

Para el diseño de gobierno de información y tecnologías el factor de diseño que nos permite conocer los problemas relacionados con las TI nos permite determinar problemas como frustraciones en distintas unidades y departamentos, incidentes significativos, problemas de ejecución de servicios, gastos sustanciales ocultos, etc. La importancia de los problemas relacionados con TI se determina en 3 tipos de niveles sin problema coma problema coma problema grave cómo se puede observar en la siguiente tabla.

Tabla 19. Importancia de problema relacionado con TI

Problemas relacionados con I&T	**Importancia (1-3)**
Frustración entre distintas unidades de TI en toda la organización debido a una percepción de baja contribución al valor del negocio	
Frustración entre distintos departamentos de la empresa (como el cliente de TI) y el departamento de TI debido a iniciativas fracasadas o una percepción de baja contribución al valor del negocio	
Incidentes significativos relacionados con **TI**, como pérdida de datos, violaciones de seguridad, fallo del proyecto y errores de la aplicación, relacionados con TI	
Problemas de ejecución del servicio por parte de los subcontratistas de TI	
Incumplimiento de los requerimientos regulatorios o contractuales relacionados con TI	
Hallazgos de auditoría regulares u otros informes de evaluación sobre un pobre desempeño de TI o notificación de problemas de calidad y servicio de TI	
Gasto sustancial oculto y fraudulento en **TI**, es decir, gasto en TI por departamentos de usuarios fuera del control de los mecanismos de decisión de inversión en IT normales y los presupuestos aprobados	
Duplicaciones o coincidencias entre varias iniciativas u otras formas de recursos malgastados	
Insuficientes recursos de TI, personal con habilidades inadecuadas o personal agotado / insatisfecho	
Cambios o proyectos facilitados por TI que suelen no satisfacer a menudo las necesidades del negocio y que se ejecutan tarde o por encima del presupuesto	

Resistencia de los miembros del consejo de administración, ejecutivos o alta gerencia a involucrarse con las TI o una falta de compromiso empresarial para patrocinar a TI	
Modelo operativo de TI complejo y/o mecanismos de decisión confusos para las decisiones relacionadas con TI	
Excesivamente alto coste de TI	
Implementación obstaculizada o fracasada de nuevas iniciativas o innovaciones causada por la arquitectura y sistemas de TI actuales	
Brecha entre conocimiento tecnológico y empresarial, lo que lleva a que los usuarios del negocio y/o los especialistas en TI hablen un idioma distinto	
Problemas regulares con la calidad de los datos y la integración de datos de distintas fuentes	
Nivel elevado de cómputo para usuarios finales, lo que genera (entre otros problemas) una falta de supervisión y control de calidad de las aplicaciones que se están desarrollando e implementando	
Los departamentos del negocio implementan sus propias soluciones de información con poca o ninguna participación del departamento de TI de la empresa (relacionado con la computación de usuarios finales, que suele surgir de la insatisfacción con las soluciones y servicios de TI)	
Ignorancia sobre y/o incumplimiento de las regulaciones de privacidad	
Incapacidad para explotar nuevas tecnologías o innovar con las TI	

	Sin problema
	Problema
	Problema grave

Adaptado:[16]

El modelo COBIT 2019 permite organizar en jerarquías en 3 niveles: sin problema, problema, problema grave.

Una vez establecido el contexto y estrategia del hospital en sus cuatro componentes principales del entendimiento de la estrategia empresarial: las metas, el perfil de riesgo y los problemas actuales con TI, se puede determinar el alcance inicial de un sistema de gobernanza para el hospital en este paso toda la información reunida del contexto y la estrategia del hospital permitirá generar el sistema de gobierno

personalizado inicial para esta casa de salud, consta de cuatro pasos que son los que se describen a continuación.

2.2.1.5. Importancia del escenario de amenazas

La importancia del escenario de amenazas como parte integral de la gestión de la seguridad de la información y riesgos. Por tal razón se considera una vez que se ha identificado y evaluado las posibles amenazas estas podrían afectar a la organización y comprometer al hospital en posibles problemas de confidencialidad, integridad y disponibilidad tanto de procesos como servicios por lo que se evalúa el grado de importancia en niveles porcentuales a los tipos de riesgos que tienen una categoría alta y normal.

Tabla 20. Importancia del escenario de amenazas

Valor	**Importancia (100 %)**
Alto	**75%**
Normal	**25%**

Adaptado: [5]

Para el modelo de gobernanza de TI, se diseña para amenazas de tipo alto se le dé una importancia del 75% mientras que a las amenazas de tipo normal se le mantenga con un nivel de importancia del 25%.

2.2.1.6. Importancia de los requisitos de cumplimiento

La importancia de los requisitos de cumplimiento en el modelo de gobernanza radica en asegurar que el hospital cumpla con los estándares, regulaciones y políticas relevantes relacionadas con la tecnología de la información (TI) y la gobernanza de TI.

Tabla 21. Importancia de los requisitos de cumplimiento

Valor	Importancia (100 %)
Alto	75%
Normal	50%
Bajo	15%

Adaptado: [5]

Mediante el ajuste realizado por la herramienta de diseño de gobernanza de TI se obtiene cada uno de los niveles de importancia de cumplimiento para los parámetros alto normal y bajo de la siguiente manera:

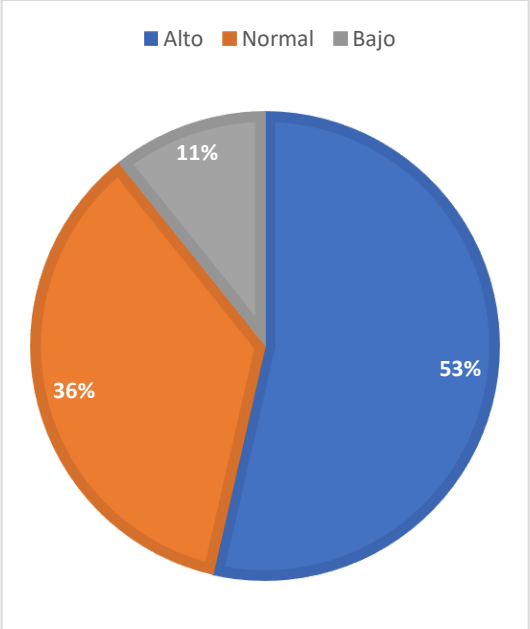


Figura 12. Importancia de los requisitos de cumplimiento

2.2.1.7. Importancia del rol de TI

En el factor de diseño donde se consigue era la importancia del rol de TI se realiza un ajuste en base a la categorización de comportamiento de TI en el cual este se comporte como TI de soporte, fábrica, cambio y estratégico.

Tabla 22. Importancia del rol de TI

Valor	**Importancia (1-5)**
Soporte	3
Fábrica	1
Cambio	2
Estratégico	5

Adaptado: [5]

2.2.1.8. Importancia del modelo de abastecimiento de proveedores para TI

Para para el diseño de gobernanza TI en el hospital se considera que el valor de importancia para externalización se considera un 30% de importancia mientras que para elementos de la nube se le asigna un grado de importancia del 20% y para personal interno y actividades que tengan o estén relacionados directamente con otras unidades del hospital se le toma como el 50% de importancia

Tabla 23. Importancia de abastecimiento de proveedores TI

Valor	**Importancia (100 %)**
Externalización (outsourcing)	30%
Nube	20%
Personal interno (Insourced)	50%

Adaptado: [5]

2.2.1.9. Importancia de los métodos de implementación de TI

Una vez establecidos los grados de importancia de abastecimiento de proveedores TI, se diseña como marco de trabajo para en el hospital bajo el método ágil de implementación a un 50% mientras que para metodologías tradicionales trabajar a un 40% y un 10% en metodología de DevOps.

Tabla 24.Importancia de los métodos de implementación de TI

Valor	Importancia (100 %)	Referencia
Ágil	50%	15%
DevOps	10%	10%
Tradicional	40%	75%

Adaptado: [5]

2.2.1.10. Importancia de la estrategia de adopción de tecnología

Para el diseño de adopción de tecnologías se establece que la estrategia a utilizar denominada primero en reaccionar será un 75% y el hospital trabajará de esa manera mientras que para estrategias como seguidor tendrá un 15% y adaptadores lentos tendrá un modelo del 10%.

Tabla 25.Importancia adopción de tecnología

Valor	Importancia (100 %)
Primero en reaccionar (First mover)	75%
Seguidor (Follower)	15%
Adoptadores lentos (Slow adopter)	**10%**

Adaptado: [5]

2.3. Método de criterio de experto

La técnica para utilizar, evaluar la calidad, determinar la relevancia y validez de esta investigación será a través del método de validación de expertos, se realizará la consulta y participación de profesionales y expertos de las demás unidades hospitalarias y la unidad de Tecnologías de la Información para obtener las respectivas opiniones, comentarios y retroalimentación de estas personas con experiencia y conocimientos especializados en las áreas que corresponden a los distintos procesos.

Una vez obtenidos los resultados de esta investigación se compartirá este trabajo y se solicitará su evaluación y comentarios. Estos expertos en las diferentes áreas del hospital revisarán el estudio, analizarán la metodología utilizada, examinarán los hallazgos y conclusiones, y brindarán su opinión sobre la calidad y validez de este marco metodológico COBIT, el cuestionario utilizado medirá parámetros como consistencia teórica, pertinencia del tema, coherencia metodológica, factibilidad e importancia del plan de gobernanza como propuesta del tema de investigación en el **Anexo 1.**

2.4. Descripción Metodológica de la Valoración Económica, Tecnológica, Operacional y Medio Ambiental de la Propuesta

2.4.1. Valoración Económica

El plan de gobernanza COBIT por ser una herramienta y un marco metodológico que gestiona los riesgos de TI implica que tiene la posibilidad de identificar, evaluar y gestionar los riesgos asociados con la seguridad de la información la privacidad la continuidad del negocio y el cumplimiento normativo con el fin de mitigar aquellos riesgos que se podrían ocasionar indeterminadamente.

Esto nos da la idea de que el Hospital General Docente Ambato puede reducir sus costos ante posibles riesgos que se pudieran ocasionar como, por ejemplo: incidentes de hardware, fallos de hardware, ataques lógicos, incidentes de terceros como pueden ser proveedores, innovación basada en la tecnología coma medio ambiente, coste y control de TI, entre otros.

Costos que pueden significar que se priorice o se cambien los presupuestos asignados en los planes operativos de las diferentes unidades del hospital por lo que también se verían afectados en la continuidad de procesos y servicios.

2.4.2. Valoración Tecnológica

El valor tecnológico de COBIT 2019 radica en su capacidad que tiene para proporcionar un marco de referencia completo y actualizado que ayudará al hospital a gobernar y gestionar eficazmente la tecnología de la información, basándose en

procesos, que abarcan todas las áreas de la gestión de TI, desde la planificación estratégica hasta la entrega de servicios y el control de los procesos.

El hospital podrá mejorar su eficiencia operativa, gestionar los riesgos de TI de manera efectiva, garantizar el cumplimiento normativo y aprovechar al máximo sus inversiones en tecnología, convirtiéndose en un impulsor clave de éxito empresarial y obtener un valor tangible y sostenible de sus iniciativas tecnológicas:

2.4.3. Valoración Ambiental

El marco metodológico de gobernanza de TI COBIT 2019 proporciona un valor importante al ambiente empresarial al brindar una distribución y enfoque sólidos para la gobernanza y gestión de la tecnología de la información (TI), y que estos estén alineados a las metas del hospital.

Al adoptar un plan de gobernabilidad en TI se tomará en cuenta varios puntos importantes de estrategias administrativas y de control como la mejora de toma de decisiones, transparencia y responsabilidad TI, gestión de riesgos, optimización de recursos, y cumplimiento de normas, esto se resumen en la obtención de una guía completa y estructurada que genere confianza en el apoyo de las TI en la institución.

2.5. Conclusiones Capítulo II.

Las encuestas realizadas arrojan que la Estrategia Empresarial Hospitalaria está orientada al servicio al cliente, y debe mantener un grado de importancia moderadamente bajo en Innovación ya que por temas presupuestarios no sería un objetivo para lograr si éste se estimara alto, ya que no solo se depende de la entidad hospitalaria sino de presupuestos nacionales, y mantener los costes y el crecimiento igual que las adquisiciones tal y como se les ha venido realizando.

Las metas empresariales con grado de importancia alto detectadas y analizadas en el diseño de gobernanza son: EG04 - continuidad y disponibilidad del servicio de negocio, EG11 - cumplimiento con las políticas internas, EG03 - cumplimiento de leyes y regulaciones externas, seguidas en un grado 4 de menor importancia las EG01 - el portafolio de productos y servicios competitivos, EG05 - cultura de

servicio orientada al cliente, EG10 - habilidades, motivación y productividad del personal, EG013 – EG04 - innovación de productos y negocios.

En los escenarios de riesgos con grado alto se han detectado 2 categorías que son: toma de decisiones sobre inversiones en ti, definición, mantenimiento del portafolio e Innovación basada en tecnología, seguidamente de adopción de software con problemas de uso, ataques lógicos, gestión de datos de información, gestión del ciclo de vida de los programas y proyectos; y escenarios de riesgos moderados cómo: incidentes de infraestructura operativa de TI, acciones no autorizadas, fallos de software, incumplimientos, actos de TI.

Los problemas relacionados con TI de igual manera se han detectado por su nivel de importancia en cuanto se refiere a niveles de importancia alto los problemas detectados son: las frustraciones entre distintas unidades de ti en toda la organización debido a una percepción de baja contribución al valor del negocio, frustración entre distintos departamentos de la empresa como iniciativas fracasadas joven percepción baja de contribución al valor como incumplimiento de los requerimientos regulatorios o contractuales relacionados con TI, hallazgos de auditorías regulares u otros informes de evaluación sobre un pobre desempeño de ti o notificación de problemas de calidad y servicios, excesivamente alto coste implementación de servicios de ti, problemas regulares con la calidad de datos en la integración de datos cómo falta de supervisión y control de calidad de las aplicaciones que se están desarrollando o implementando, ignorancia sobre incumplimiento de regulaciones de privacidad.

CAPÍTULO III.

APLICACIÓN Y/O VALIDACIÓN DE LA PROPUESTA

3.1. Resultados del Diagnóstico del Problema

La presente investigación permite una visión clara de la gobernanza y gestión de TI en el hospital general, identificando las áreas que deben tener una intervención para mejora con la optimización de los procesos y controles de TI, lo que impulsa a esta institución a alinear los objetivos de TI con los objetivos estratégicos institucionales.

El marco metodológico de gobernanza TI en el Hospital General Docente Ambato reúne las características tanto de estrategia empresarial, objetivos empresariales, el, requisitos de cumplimiento, el rol de las TI, el abastecimiento de los proveedores como la importancia de la implementación TI, además de la adopción de las tecnologías.

3.1.1.1. Estrategia empresarial

La estrategia empresarial del Hospital General Docente Ambato presenta una orientación hacia el servicio al cliente como se muestra en la figura 13.

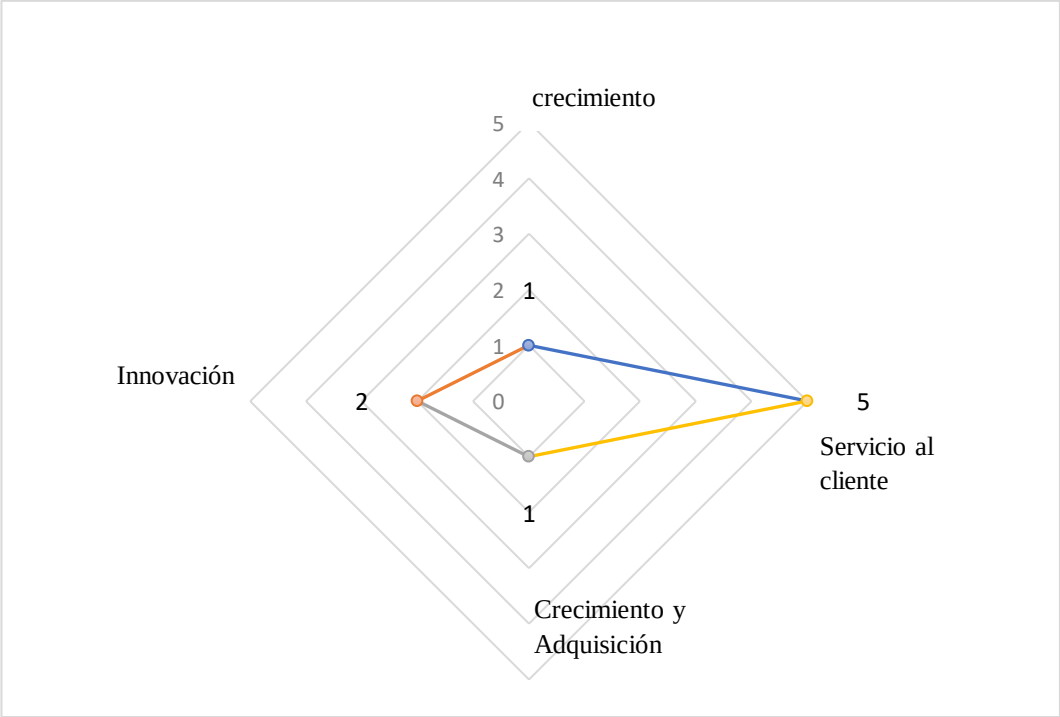


Figura 13. Importancia de las estrategias empresariales

Los objetivos de gobierno que presentan una importancia relativa alta a considerar son: EDM02 - asegurar la realización de beneficios, EDM03- asegurar la optimización del riesgo.

Y las metas de gestión más relevantes a considerar son: APO11 - gestión de la calidad, APO8 - gestionar las relaciones internas del hospital, APO9- gestionar los acuerdos del servicio, APO12 - gestionar el riesgo, AP013 - gestionar la seguridad; BAI04 - gestionar la disponibilidad y capacidad; DSS02 - gestionar las solicitudes e incidentes del servicio, DSS03 - gestionar los problemas, DSS04 - gestionar la continuidad, DSS05 - gestionar los servicios de seguridad.

Tabla 26 Importancia - objetivos de gobierno.

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	**Valoración**	**Referencia**	**Importancia relativa**
EDM01	12	15	**5**
EDM02	23	24	**30**

EDM03	14	15	**25**
EDM04	12,5	22,5	**-25**
EDM05	15,5	18	**15**
APO01	9	12	**0**
APO02	17	28,5	**-20**
APO03	14	24	**-20**
APO04	15	21	**-5**
APO05	19	33	**-25**
APO06	12,5	22,5	**-25**
APO07	10	15	**-10**
APO08	22,5	21	**45**
APO09	24,5	22,5	**45**
APO10	14	21	**-10**
APO11	24	21	**50**
APO12	17,5	18	**30**
APO13	16,5	16,5	**35**
APO14	9	12	**0**
BAI01	17	27	**-15**
BAI02	9,5	13,5	**-5**
BAI03	9,5	13,5	**-5**
BAI04	19	18	**40**
BAI05	16,5	25,5	**-15**
BAI06	14,5	19,5	**0**
BAI07	14	18	**5**
BAI08	14	19,5	**-5**
BAI09	9	12	**0**
BAI10	9	12	**0**
BAI11	16	27	**-20**
DSS01	11,5	13,5	**15**
DSS02	24	21	**50**
DSS03	19	18	**40**
DSS04	24	21	**50**
DSS05	16,5	16,5	**35**
DSS06	11,5	13,5	**15**
MEA01	9	12	**0**
MEA02	9	12	**0**
MEA03	9	12	**0**
MEA04	9	12	**0**

Adaptado: [5]

Estos parámetros de medición nos indica que debemos estar atentos y alertas a la realización de procesos benéficos que podrían estar presentes siempre y cuando

teniendo también la idea de que ahí la presencia de posibles riesgos, en donde la gestión tanto de calidad, relaciones internas, acuerdos como gestión de riesgos y seguridad nos permitan tener la disponibilidad y capacidad de atención teniendo en cuenta aquellas solicitudes e incidentes registrados para poder gestionar problemas y mantener la continuidad del de los servicios.

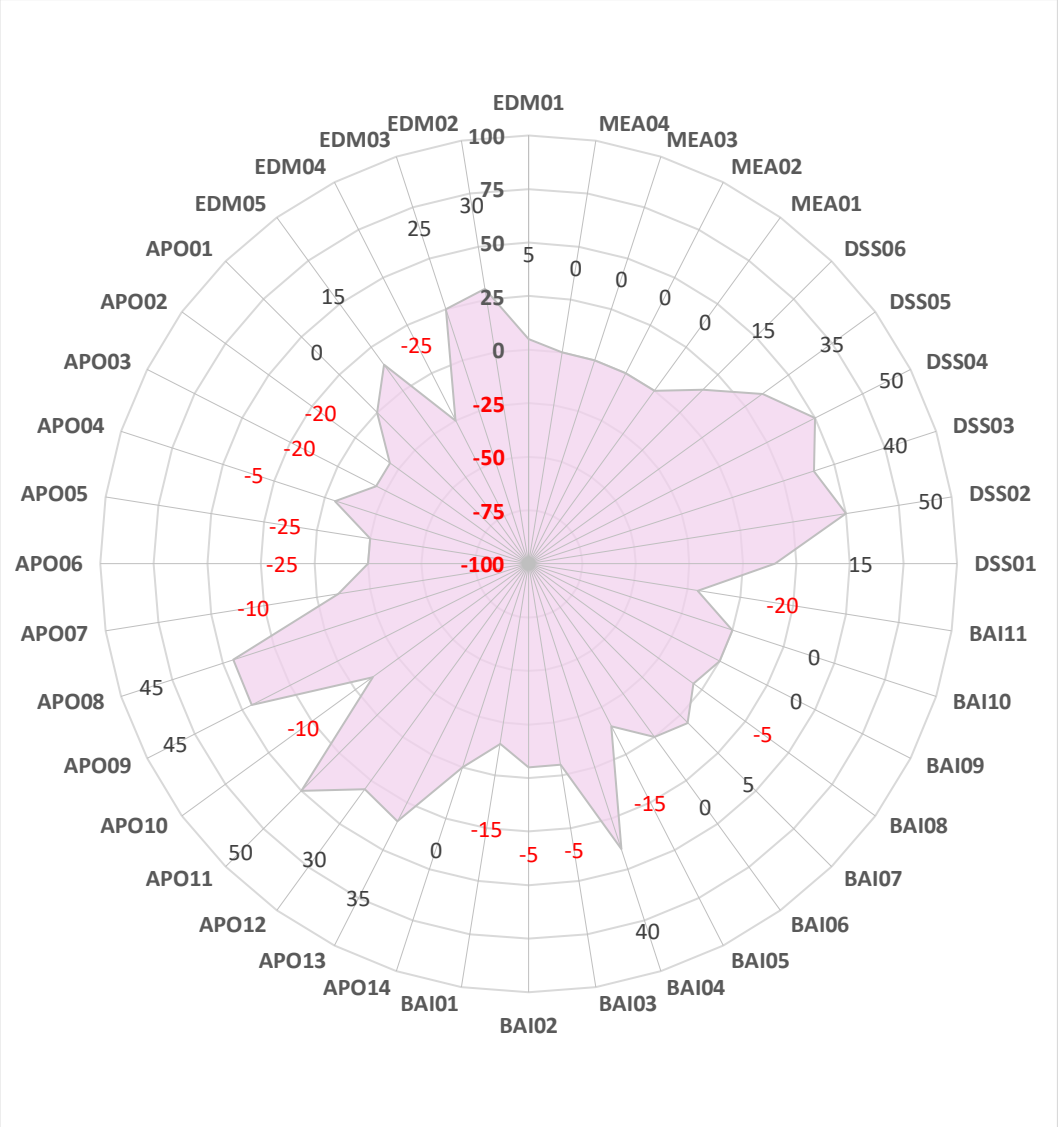


Figura 14. Factor de diseño estrategia empresarial

3.1.1.2. Objetivos empresariales

Para la obtención y desarrollo de las metas empresariales que presentan una importancia relativa alta a considerar son: EDM01 - Garantizar el establecimiento

y el mantenimiento del marco de gobierno, EDM03- asegurar la optimización del riesgo.

Y las metas de gestión más relevantes a considerar son: APO12 - gestionar el riesgo, AP013 - gestionar la seguridad, APO3 - Gestionar la arquitectura de la empresa, APO9 - gestionar los acuerdos de servicio; BAI10 - gestionar la configuración, BAI04 – gestionar la disponibilidad y capacidad, BAI06 - gestionar los cambios de TI; DSS02 - gestionar las solicitudes e incidentes del servicio; DSS05 - gestionar los servicios de seguridad, DSS2 - gestionar las solicitudes de incidentes del servicio, DSS3 -gestionar los problemas , DSS4 - gestionar la continuidad; MEA03 - gestionar el cumplimiento de los requisitos externos.

Tabla 27.Importancia objetivos empresariales

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	**Valoración**	**Referencia**	**Importancia relativa**
EDM01	121	99	**10**
EDM02	133	114	**5**
EDM03	89	63	**25**
EDM04	148	129	**0**
EDM05	45	63	**-35**
APO01	213	180	**5**
APO02	160	132	**5**
APO03	164	135	**10**
APO04	145	120	**5**
APO05	163	141	**0**
APO06	93	117	**-30**
APO07	129	108	**5**
APO08	229	189	**5**
APO09	79	63	**10**
APO10	94	78	**5**
APO11	115	132	**-25**
APO12	48	36	**20**
APO13	55	39	**25**
APO14	64	78	**-25**
BAI01	143	129	**0**
BAI02	205	174	**5**
BAI03	193	165	**5**

BAI04	85	69	**10**
BAI05	211	183	**0**
BAI06	111	90	**10**
BAI07	81	69	**5**
BAI08	161	135	**5**
BAI09	23	51	**-60**
BAI10	23	18	**15**
BAI11	155	138	**0**
DSS01	79	63	**10**
DSS02	70	54	**15**
DSS03	70	54	**15**
DSS04	70	54	**15**
DSS05	112	81	**25**
DSS06	136	105	**15**
MEA01	145	135	**-5**
MEA02	152	135	**0**
MEA03	59	39	**35**
MEA04	126	111	**0**

Adaptado: [5]

Estos parámetros de medición nos indica que para garantizar el establecimiento y el mantenimiento del marco de gobierno conjuntamente con la optimización del riesgo, se debe gestionar las posibilidades de riesgo coma la seguridad de respectivas para mitigarlos, tener siempre presente la arquitectura de la empresa y los acuerdos que tiene cada servicio que lo conforman; Para así gestionar la disponibilidad y capacidad de cada una de las unidades que conforman el hospital además de gestionar las solicitudes e incidentes del servicio para brindar servicios con seguridad, y velar por el fiel cumplimiento de los requisitos externos.

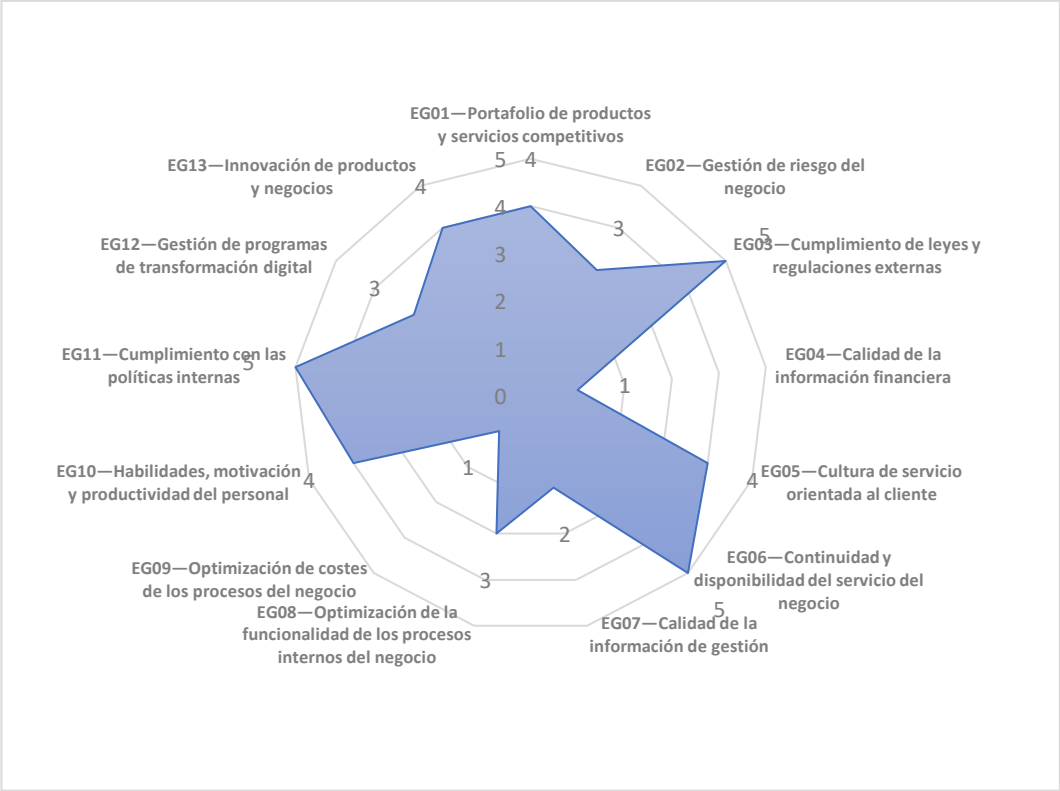


Figura 15. Factor de diseño metas empresariales

3.1.1.3. Riesgos TI

Para la obtención y desarrollo de análisis de los posibles escenarios que presentan una importancia relativa alta a considerar en riesgos TI son: EDM02 - asegurar la realización de beneficios, EDM03- asegurar la optimización del riesgo.

Y las metas de gestión más relevantes a considerar son: APO12 - gestionar el riesgo, AP013 - gestionar la seguridad, APO8 - Gestionar la innovación ,APO8 - Gestionar las relaciones; BAI05 - gestionar los cambios organizativos , BAI06 - gestionar los cambios de TI, BAI10- gestionar la configuración, BAI11 – Gestionar los proyectos; DSS06 - gestionar los controles de procesos de negocio, DSS2 - gestionar las solicitudes de incidentes del servicio, DSS5 -gestionar los servicios de seguridad; MEA03 - gestionar el cumplimiento de los requisitos externos, MEA04 - gestionar el aseguramiento, MEA01 - gestionar la monitorización del rendimiento y la conformidad.

Tabla 28. Importancia riesgos TI

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	**Valoración**	**Referencia**	**Importancia relativa**
EDM01	184	189	**0**
EDM02	155	135	**15**
EDM03	182	162	**15**
EDM04	170	198	**-15**
EDM05	159	189	**-15**
APO01	368	324	**15**
APO02	136	144	**-5**
APO03	194	171	**15**
APO04	64	45	**45**
APO05	122	144	**-15**
APO06	120	153	**-20**
APO07	250	216	**15**
APO08	213	153	**40**
APO09	129	117	**10**
APO10	196	216	**-10**
APO11	128	99	**30**
APO12	132	90	**50**
APO13	155	99	**55**
APO14	263	198	**35**
BAI01	92	81	**15**
BAI02	136	117	**15**
BAI03	155	117	**35**
BAI04	12	9	**35**
BAI05	104	72	**45**
BAI06	192	135	**45**
BAI07	148	117	**25**
BAI08	151	135	**15**
BAI09	42	36	**15**
BAI10	138	99	**40**
BAI11	48	36	**35**
DSS01	128	135	**-5**
DSS02	184	144	**30**
DSS03	125	108	**15**
DSS04	241	216	**10**
DSS05	256	216	**20**
DSS06	196	144	**35**

MEA01	235	216	**10**
MEA02	257	243	**5**
MEA03	186	153	**20**
MEA04	265	225	**20**

Adaptado: [5]

Estos parámetros de medición nos indica que para garantizar la mitigación de los posibles riesgos TI se debe gestionar el riesgo además la seguridad con proyectos de innovación que interrelacionen las unidades hospitalarias, mediante cambios organizativos no solo de las unidades hospitalaria sino también de TI asignando cuáles son sus roles y funciones para la generación de nuevos proyectos cumpliendo las normas o requisitos externos que nos guían al aseguramiento y monitorización del rendimiento y la conformidad.

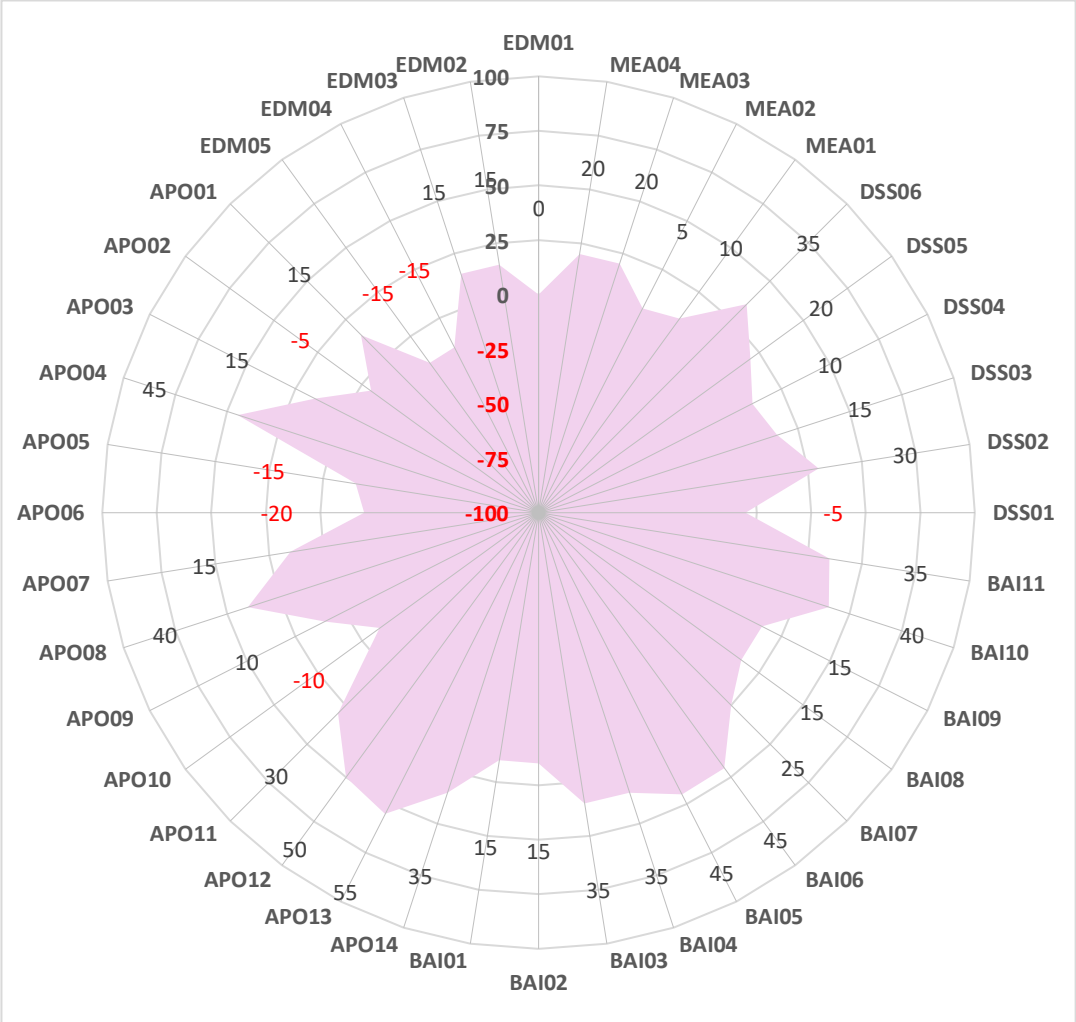


Figura 16. Factor de diseño perfil de riesgo TI

3.1.1.4. Problemas relacionados con TI

Para la obtención y desarrollo de análisis de los posibles problemas relacionados con TI que presentan una importancia relativa alta a considerar son: EDM04 - asegurar la optimización de los recursos.

Y las metas de gestión más relevantes a considerar son: APO04 - gestionar la innovación, APO07 - gestionar los recursos humanos, APO03- gestionar la estructura de la empresa, APO02 - gestionar las estrategias; BAI08 - gestionar el conocimiento, BAI11 - gestionar los proyectos, BAI05 - gestionar los cambios organizativos, gestionar los acuerdos del servicio.

Tabla 29.Importancia problemas relacionados con TI

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	**Valoración**	**Referencia**	**Importancia relativa**
EDM01	59,5	70	**-10**
EDM02	61	70	**-5**
EDM03	39	47	**-10**
EDM04	65,5	67	**5**
EDM05	33	41	**-15**
APO01	50	56	**-5**
APO02	48	50	**5**
APO03	64,5	66	**5**
APO04	35,5	32	**20**
APO05	61	68	**-5**
APO06	52	62	**-10**
APO07	49	47	**15**
APO08	67,5	70	**5**
APO09	36,5	43	**-10**
APO10	33	39	**-10**
APO11	34	43	**-15**
APO12	44,5	52	**-5**
APO13	26,5	33	**-15**
APO14	48,5	60	**-15**

BAI01	37,5	35	**15**
BAI02	47	51	**0**
BAI03	35	41	**-10**
BAI04	18,5	23	**-15**
BAI05	27,5	28	**5**
BAI06	38	42	**0**
BAI07	34	38	**-5**
BAI08	34,5	31	**20**
BAI09	22	23	**5**
BAI10	23	25	**0**
BAI11	46,5	45	**10**
DSS01	21	27	**-15**
DSS02	24,5	33	**-20**
DSS03	28	32	**-5**
DSS04	16,5	21	**-15**
DSS05	22,5	29	**-15**
DSS06	20	29	**-25**
MEA01	52,5	61	**-5**
MEA02	38	48	**-15**
MEA03	18,5	29	**-30**
MEA04	47	58	**-10**

Adaptado: [5]

Estos parámetros de medición nos indica que para garantizar minimizar los problemas relacionados con TI se debe asegurar la optimización con proyectos de innovación, gestión de recursos humanos, mejorar la estructura organizacional, gestionar estrategias tanto de conocimiento como de proyectos con cambios organizativos y establecimiento de acuerdos del servicio.

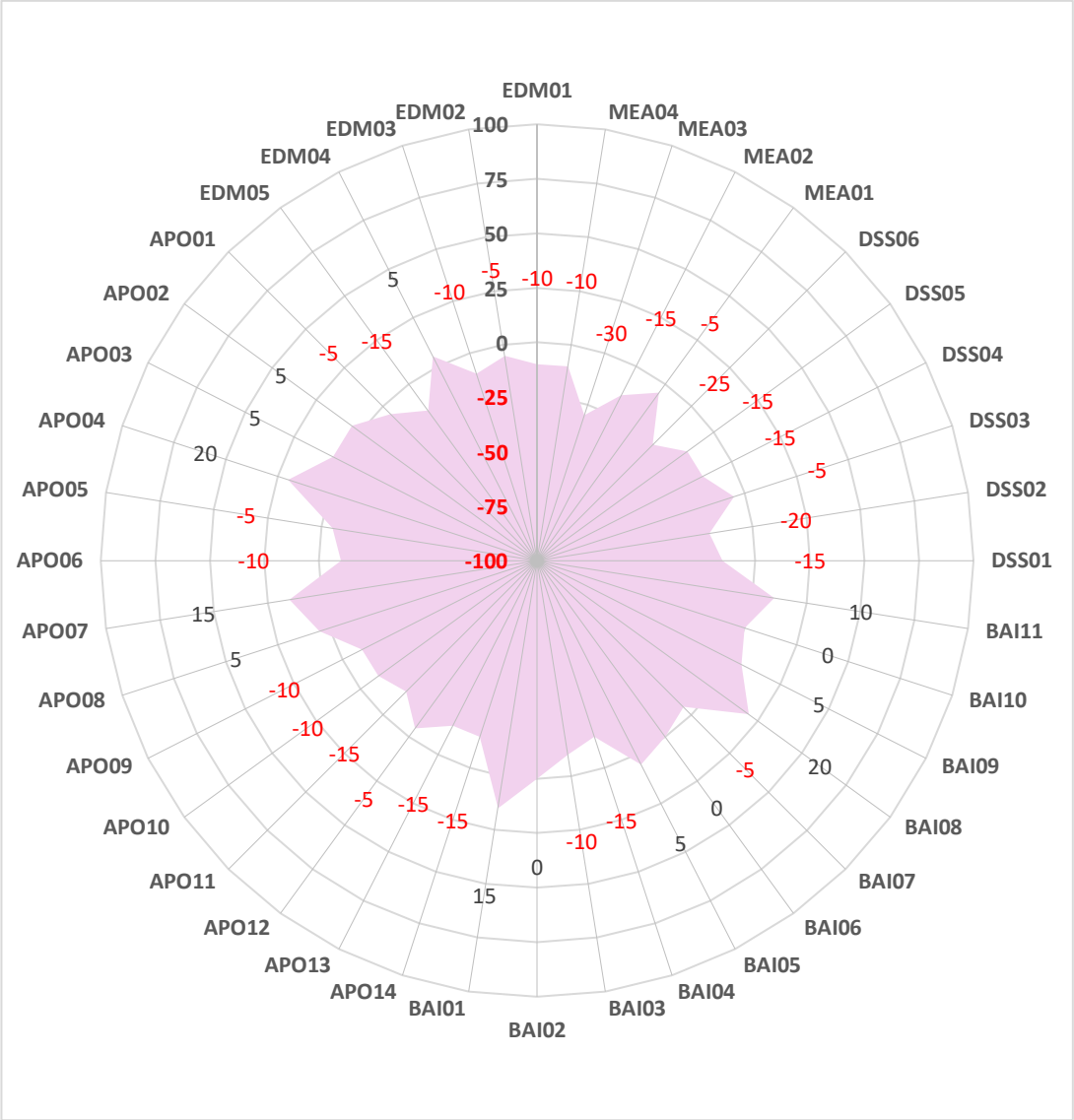


Figura 17. Factor de diseño problemas relacionados con TI

3.1.1.5. Escenario de amenazas

Para la obtención y desarrollo de análisis de posibles escenarios de amenazas que presentan una importancia relativa alta a considerar son: EDM03 - asegurar la optimización de los recursos, EDM01 - garantizar el establecimiento y el mantenimiento del marco de gobierno, EDM05 - asegurar la transparencia de las partes interesadas.

Y las metas de gestión más relevantes a considerar son: APO12 - gestionar el riesgo, APO13 - gestionar la seguridad, APO10- gestionar los proveedores, APO03 -

gestionar la arquitectura de la empresa; BAI10 - gestionar configuración, BAI06 - gestionar los cambios de TI, BAI04 - gestionar la capacidad y disponibilidad; DSS04 - gestionar la continuidad, DSS03 - gestionar los problemas, DSS02 - gestión de las solicitudes e incidentes del servicio; MEA01 - gestionar la monitorización del rendimiento y la conformidad, MEA03 - gestionar el cumplimiento de los requisitos de externos, MEA04 - gestionar el aseguramiento, MEA02 -gestionar el sistema de control interno.

Tabla 30. Importancia Escenario de amenazas

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	**Valoración**	**Referencia**	**Importancia relativa**
EDM01	2,50	1,66	**50**
EDM02	1,00	1,00	**0**
EDM03	3,25	1,99	**65**
EDM04	1,00	1,00	**0**
EDM05	1,75	1,33	**30**
APO01	2,50	1,66	**50**
APO02	1,00	1,00	**0**
APO03	2,50	1,66	**50**
APO04	1,00	1,00	**0**
APO05	1,00	1,00	**0**
APO06	1,00	1,00	**0**
APO07	1,75	1,33	**30**
APO08	1,00	1,00	**0**
APO09	1,75	1,33	**30**
APO10	2,50	1,66	**50**
APO11	1,75	1,33	**30**
APO12	3,25	1,99	**65**
APO13	3,25	1,99	**65**
APO14	2,50	1,66	**50**
BAI01	1,00	1,00	**0**
BAI02	1,00	1,00	**0**
BAI03	1,00	1,00	**0**
BAI04	1,75	1,33	**30**
BAI05	1,00	1,00	**0**
BAI06	2,50	1,66	**50**
BAI07	1,00	1,00	**0**

BAI08	1,00	1,00	**0**
BAI09	1,00	1,00	**0**
BAI10	2,50	1,66	**50**
BAI11	1,00	1,00	**0**
DSS01	1,00	1,00	**0**
DSS02	2,50	1,66	**50**
DSS03	1,75	1,33	**30**
DSS04	3,25	1,99	**65**
DSS05	2,50	1,66	**50**
DSS06	2,50	1,66	**50**
MEA01	2,50	1,66	**50**
MEA02	1,75	1,33	**30**
MEA03	2,50	1,66	**50**
MEA04	2,50	1,66	**50**

Adaptado: [5]

Estos parámetros de medición nos indica que para garantizar el establecimiento y mantenimiento del marco teórico al igual que la transparencia de las partes interesadas se debe asegurar la gestión en el riesgo, la seguridad como al cumplimiento de los proveedores, la arquitectura de la empresa, los cambios de TI, tener en cuenta la capacidad y disponibilidad del servicio, gestionar la continuidad, los problemas, las solicitudes de incidentes de servicio además la monitorización del rendimiento y la conformidad, el cumplimiento de requisitos como el aseguramiento de la información y controles internos.

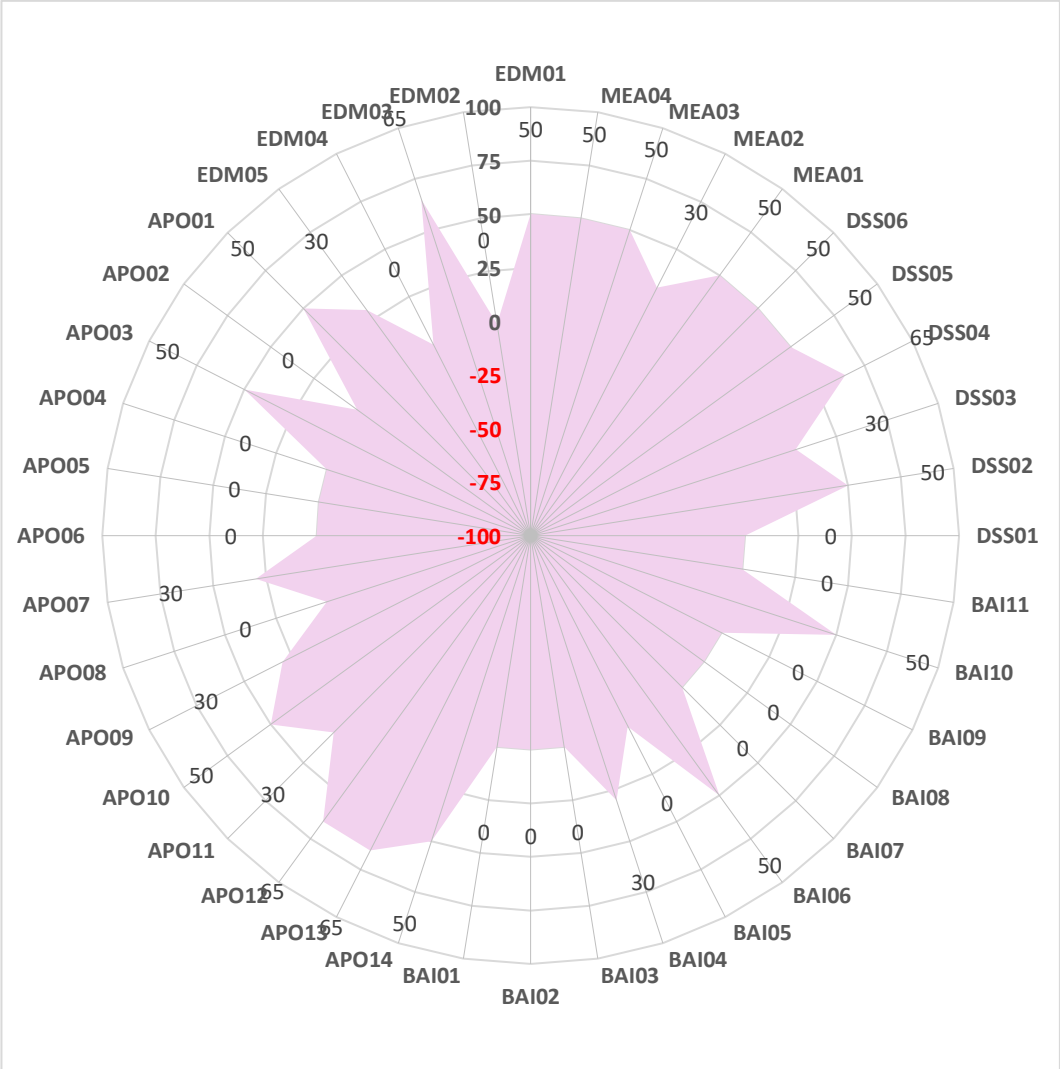


Figura 18. Factor de diseño escenario de amenazas

3.1.1.6. Requisitos de cumplimiento

Para la obtención y desarrollo de análisis de requisitos de cumplimiento que presentan una importancia relativa a EDM03 - Gestionar la arquitectura de la empresa, EDM01 - Garantizar el establecimiento y el mantenimiento del marco de gobierno, EDM05 - Asegurar la transparencia de las partes interesadas, mientras que las metas de gestión más relevantes son: APO12 - Gestionar el riesgo, APO10 - Gestionar los proveedores, APO13 - Gestionar la seguridad, DSS05 - Gestionar los controles de proceso de negocio, DSS04 - Gestionar la continuidad, MEA03 - Gestionar el cumplimiento de los requisitos externos y MEA04 - Gestionar el aseguramiento.

Tabla 31. Importancia de requisitos de cumplimiento

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	**Valoración**	**Referencia**	**Importancia relativa**
EDM01	3,40	2,00	**70**
EDM02	1,40	1,00	**40**
EDM03	4,15	2,00	**110**
EDM04	1,40	1,00	**40**
EDM05	1,78	1,00	**80**
APO01	2,40	1,50	**60**
APO02	1,40	1,00	**40**
APO03	1,40	1,00	**40**
APO04	1,40	1,00	**40**
APO05	1,40	1,00	**40**
APO06	1,40	1,00	**40**
APO07	1,40	1,00	**40**
APO08	1,40	1,00	**40**
APO09	1,40	1,00	**40**
APO10	1,78	1,00	**80**
APO11	1,40	1,00	**40**
APO12	4,15	2,00	**110**
APO13	1,78	1,00	**80**
APO14	2,40	1,50	**60**
BAI01	1,40	1,00	**40**
BAI02	1,40	1,00	**40**
BAI03	1,40	1,00	**40**
BAI04	1,40	1,00	**40**
BAI05	1,40	1,00	**40**
BAI06	1,40	1,00	**40**
BAI07	1,40	1,00	**40**
BAI08	1,40	1,00	**40**
BAI09	1,40	1,00	**40**
BAI10	1,40	1,00	**40**
BAI11	1,40	1,00	**40**
DSS01	1,40	1,00	**40**
DSS02	1,40	1,00	**40**

DSS03	1,40	1,00	**40**
DSS04	1,78	1,00	**80**
DSS05	2,15	1,00	**115**
DSS06	1,40	1,00	**40**
MEA01	1,40	1,00	**40**
MEA02	1,40	1,00	**40**
MEA03	4,15	2,00	**110**
MEA04	3,78	2,00	**90**

Adaptado: [5]

La siguiente figura nos indica que en la importancia de requisitos de requerimiento es muy importante la gestión de la arquitectura de la empresa al igual que el mantenimiento del marco de gobierno y el funcionamiento transparente de las partes interesadas coma en cuanto se refiere a las metas de gestión es importante la gestión del riesgo coma el manejo de proveedores, la gestión de la seguridad, el control de procesos de negocio, el mantenimiento De la continuidad de servicios, la gestión del cumplimiento de los requisitos externos y la gestión de aseguramiento.

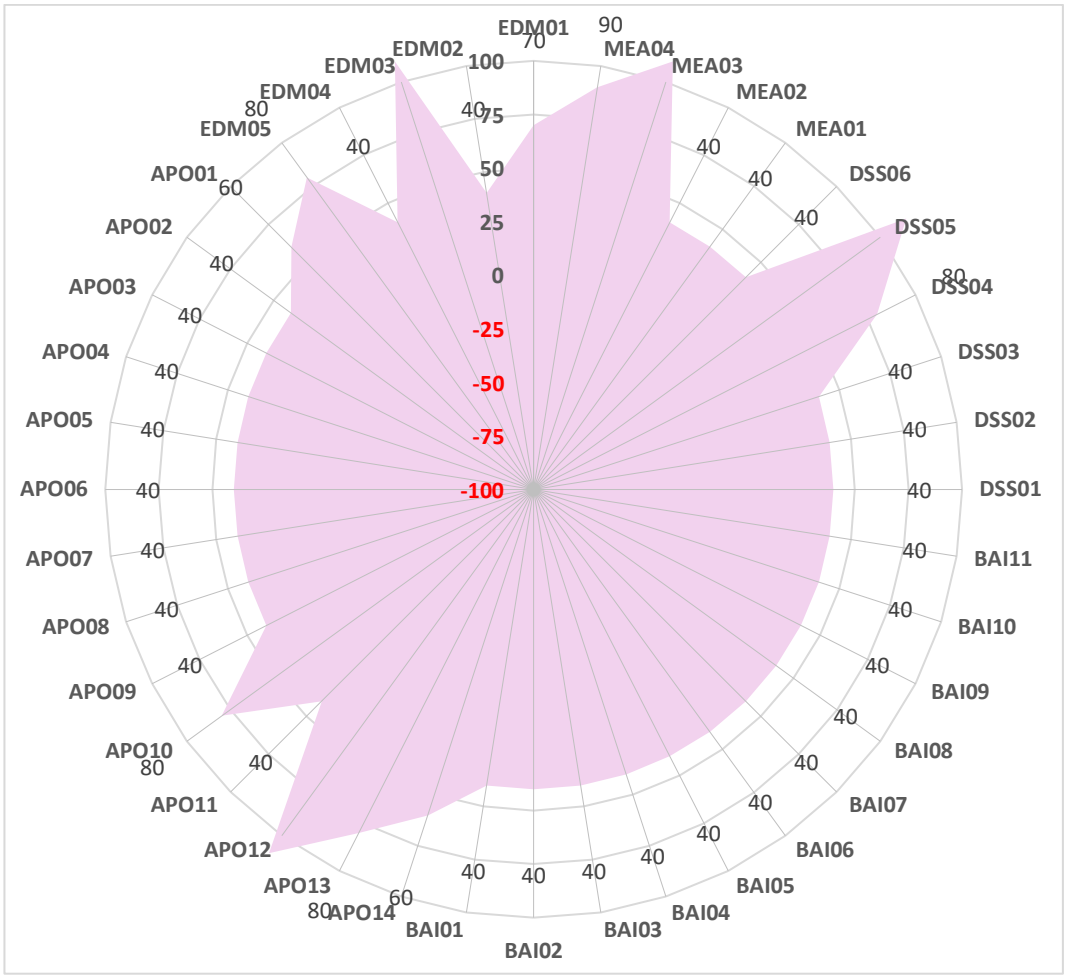


Figura 19. Factor de diseño requisitos de cumplimiento

3.1.1.7. Rol de TI

Para la obtención y desarrollo de análisis de rol de TI que presentan una importancia relativa alta en los objetivos de gobierno: EDM01 - Garantizar el establecimiento y el mantenimiento del marco de gobierno, EDM02 - Asegurar la realización de beneficios, EDM04 - Asegurar la optimización de los recursos, EDM05 - Asegurar la transparencia de las partes interesadas, APO02 - Gestionar la estrategia, APO04 - Gestionar la innovación, APO05 - Gestionar la estrategia, APO06 - Gestionar el presupuesto y los costes, APO08 - Gestionar las relaciones, BAI01 - Gestionar los programas, BAI02 - Gestionar la definición de requisitos, BAI03 - Gestionar identificación y construcción de soluciones, BAI05 - Gestionar cambios organizativos, BAI08 - Gestionar conocimiento, BAI09 - Gestionar los activos, DSS06 - Gestionar los controles de procesos de negocio, DSS04 - Gestionar la

continuidad, MEA01 - Gestionar la monitorización del rendimiento y la conformidad, MEA02 - Gestionar el sistema de control interno, MEA04 - Gestionar el aseguramiento.

Tabla 32. Importancia de rol de TI

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	**Valoración**	**Referencia**	**Importancia relativa**
EDM01	28,0	25,5	**20**
EDM02	24,0	22,5	**15**
EDM03	23,0	24,0	**5**
EDM04	16,0	15,0	**15**
EDM05	16,0	15,0	**15**
APO01	20,0	19,5	**10**
APO02	25,0	24,0	**15**
APO03	18,0	18,0	**10**
APO04	29,5	27,0	**20**
APO05	24,0	22,5	**15**
APO06	16,0	15,0	**15**
APO07	13,5	13,5	**10**
APO08	20,5	19,5	**15**
APO09	18,0	19,5	**0**
APO10	18,5	21,0	**-5**
APO11	17,5	18,0	**5**
APO12	22,5	22,5	**10**
APO13	23,0	22,5	**10**
APO14	20,0	19,5	**10**
BAI01	20,5	19,5	**15**
BAI02	25,0	24,0	**15**
BAI03	25,0	24,0	**15**
BAI04	18,5	21,0	**-5**
BAI05	16,0	15,0	**15**
BAI06	17,5	19,5	**0**
BAI07	18,0	18,0	**10**
BAI08	16,0	15,0	**15**
BAI09	16,0	15,0	**15**
BAI10	16,5	16,5	**10**
BAI11	18,0	18,0	**10**
DSS01	23,5	25,5	**0**
DSS02	24,0	25,5	**5**

DSS03	26,5	27,0	**5**
DSS04	26,5	27,0	**5**
DSS05	27,5	27,0	**10**
DSS06	18,5	16,5	**20**
MEA01	16,0	15,0	**15**
MEA02	16,0	15,0	**15**
MEA03	13,5	13,5	**10**
MEA04	16,0	15,0	**15**

Adaptado: [5]

Estos parámetros de medición nos indica que el rol de TI no se relaciona con la gestión de proveedores ni con la disponibilidad y capacidad, pero sí puede gestionar innovación e identificación y construcción de soluciones que permitirán gestionar de igual manera la continuidad de los controles de proceso y de negocio

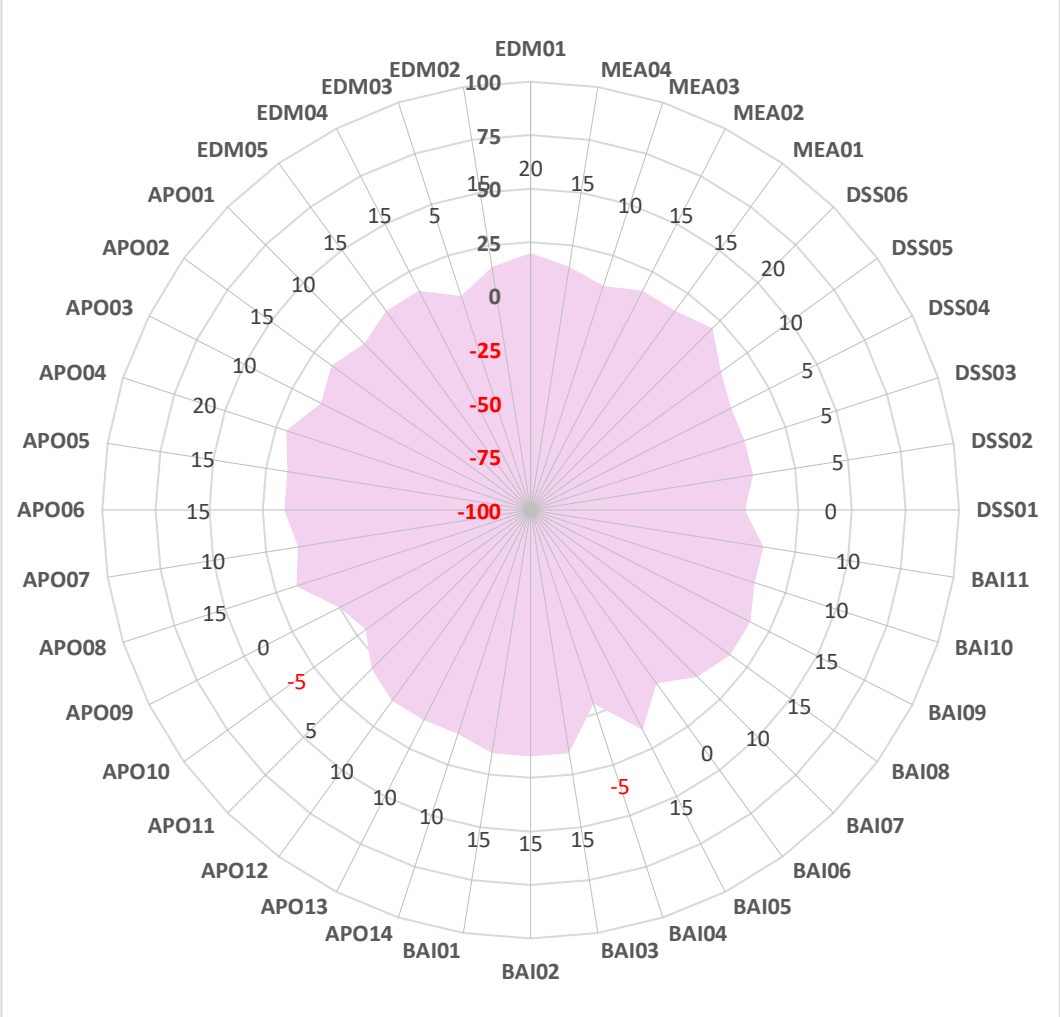


Figura 20. Factor de diseño rol de TI

3.1.1.8. Abastecimiento de proveedores para TI

Para la obtención y desarrollo de análisis de abastecimiento de proveedores para TI que presentan una importancia relativa alta a considerar no existen ya que la unidad de tecnologías de la información cuenta con servicios nacionales que necesitan ser tan sólo parametrizados y monitorizados en su funcionamiento y apoyo.

Tabla 33. Importancia de abastecimiento de proveedores TI

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	**Valoración**	**Referencia**	**Importancia relativa**
EDM01	1,00	1,00	**0**
EDM02	1,00	1,00	**0**
EDM03	1,20	1,33	**-10**
EDM04	1,00	1,00	**0**
EDM05	1,00	1,00	**0**
APO01	1,00	1,00	**0**
APO02	1,00	1,00	**0**
APO03	1,00	1,00	**0**
APO04	1,00	1,00	**0**
APO05	1,00	1,00	**0**
APO06	1,00	1,00	**0**
APO07	1,00	1,00	**0**
APO08	1,00	1,00	**0**
APO09	2,50	2,98	**-15**
APO10	2,50	2,98	**-15**
APO11	1,00	1,00	**0**
APO12	1,50	1,66	**-10**
APO13	1,00	1,00	**0**
APO14	1,00	1,00	**0**
BAI01	1,00	1,00	**0**
BAI02	1,00	1,00	**0**
BAI03	1,00	1,00	**0**
BAI04	1,00	1,00	**0**
BAI05	1,00	1,00	**0**
BAI06	1,00	1,00	**0**
BAI07	1,00	1,00	**0**
BAI08	1,00	1,00	**0**
BAI09	1,00	1,00	**0**

BAI10	1,00	1,00	**0**
BAI11	1,00	1,00	**0**
DSS01	1,00	1,00	**0**
DSS02	1,00	1,00	**0**
DSS03	1,00	1,00	**0**
DSS04	1,00	1,00	**0**
DSS05	1,00	1,00	**0**
DSS06	1,00	1,00	**0**
MEA01	2,00	2,32	**-15**
MEA02	1,00	1,00	**0**
MEA03	1,00	1,00	**0**
MEA04	1,00	1,00	**0**

Adaptado: [5]

Estos parámetros de medición nos indica que para el modelo de abastecimiento de proveedores para ti el hospital permanece tranquilo con el personal interno que ejecuta las acciones y controles que no dependen de proveedores externos

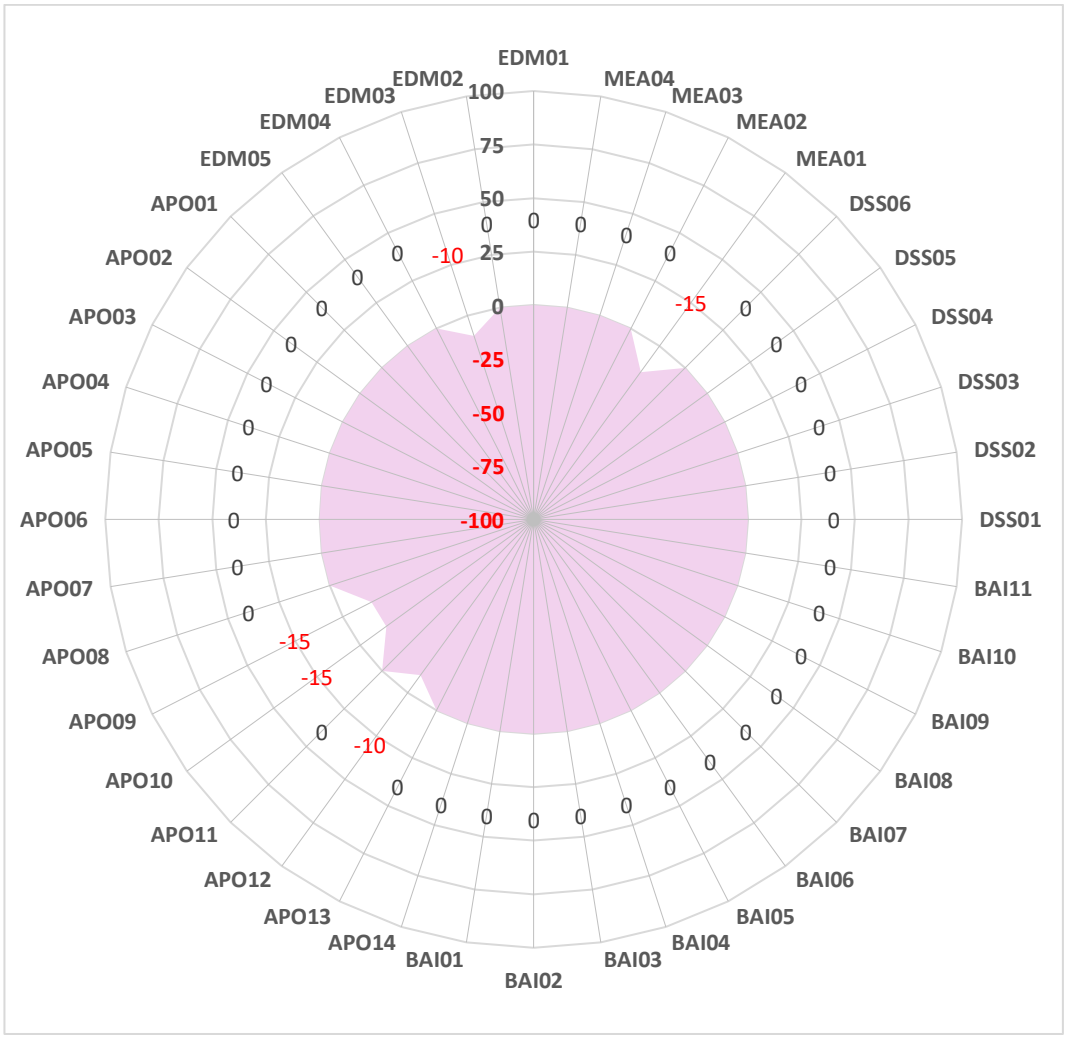


Figura 21. Factor de diseño Abastecimiento de proveedores para TI

3.1.1.9. Implementación de TI

Para el diseño de objetivos por implementación de ti, se obtiene a un nivel de importancia de nivel 60 en cuanto se refiere a la gestión de cambios que se producen en el hospital y estos corresponden al conocido como objetivo BAI03, seguido de BAI02 y BAI06 que corresponden al facilitador de cambio organizacional y a la gestión de aceptación de transición de cambio, cómo se puede observar en la tabla 34 y en la figura 22.

Tabla 34. Importancia de implementación TI

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	**Valoración**	**Referencia**	**Importancia relativa**
EDM01	1,00	1,00	**0**
EDM02	1,00	1,00	**0**
EDM03	1,00	1,00	**0**
EDM04	1,00	1,00	**0**
EDM05	1,00	1,00	**0**
APO01	1,00	1,00	**0**
APO02	1,00	1,00	**0**
APO03	1,10	1,10	**0**
APO04	1,00	1,00	**0**
APO05	1,00	1,00	**0**
APO06	1,00	1,00	**0**
APO07	1,05	1,05	**0**
APO08	1,00	1,00	**0**
APO09	1,00	1,00	**0**
APO10	1,00	1,00	**0**
APO11	1,00	1,00	**0**
APO12	1,05	1,05	**0**
APO13	1,00	1,00	**0**
APO14	1,00	1,00	**0**
BAI01	1,55	1,20	**30**
BAI02	2,35	1,48	**60**
BAI03	2,70	1,65	**65**
BAI04	1,00	1,00	**0**
BAI05	1,80	1,28	**40**
BAI06	2,35	1,48	**60**
BAI07	1,90	1,38	**40**
BAI08	1,00	1,00	**0**
BAI09	1,00	1,00	**0**
BAI10	1,35	1,18	**15**
BAI11	1,75	1,23	**45**
DSS01	1,15	1,15	**0**
DSS02	1,05	1,05	**0**
DSS03	1,05	1,05	**0**
DSS04	1,00	1,00	**0**
DSS05	1,00	1,00	**0**

DSS06	1,00	1,00	**0**
MEA01	1,30	1,13	**15**
MEA02	1,00	1,00	**0**
MEA03	1,00	1,00	**0**
MEA04	1,00	1,00	**0**

Adaptado: [5]

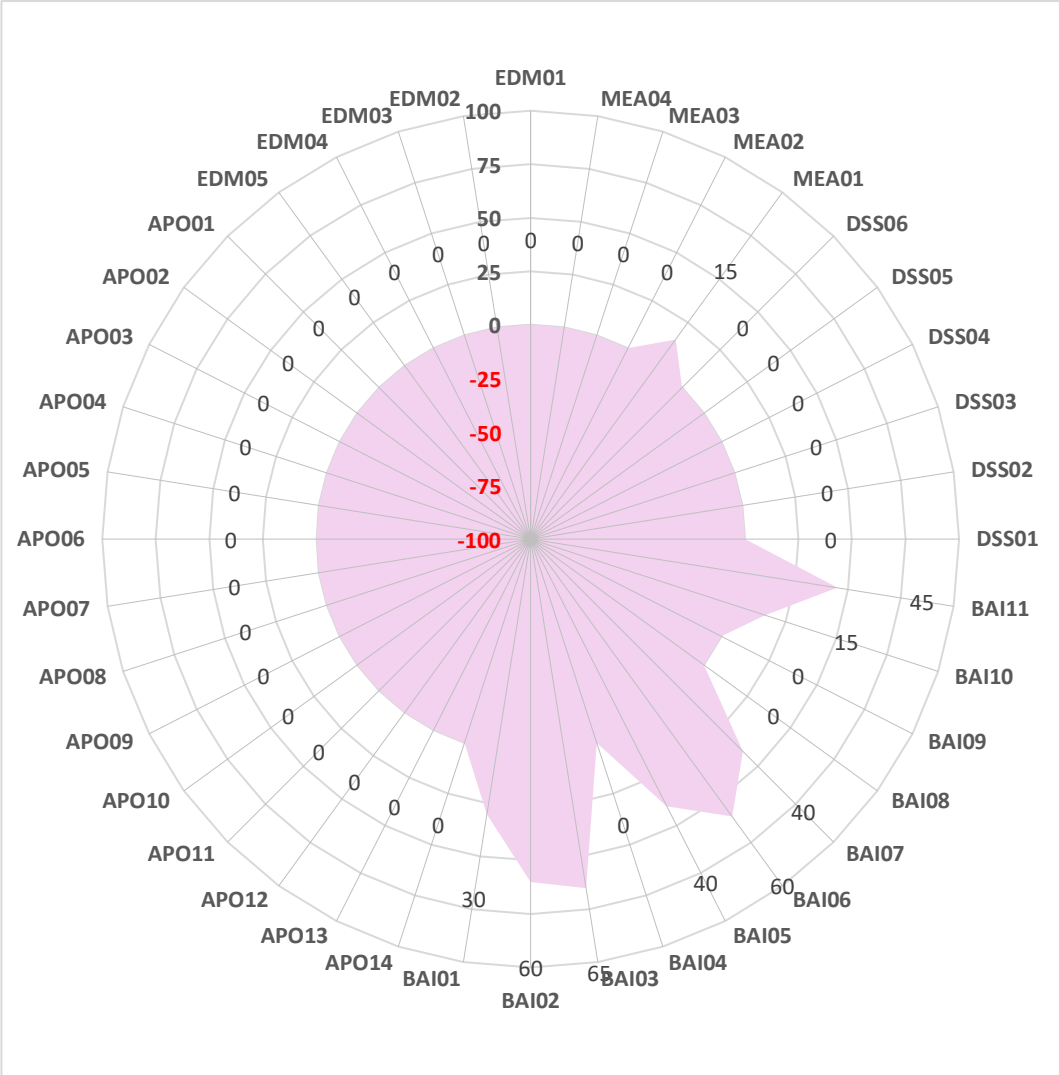


Figura 22. Factor de diseño implementación de TI

3.1.1.10. Adopción de Tecnología

para la adopción de tecnología se tiene un punto importante a considerar en el objetivo de gestión conocido como APO07, APO08 en donde es importante la gestión de recursos humanos y relaciones internas y de procesos para

funcionamiento de las actividades en el hospital. Además, en los objetivos de gobierno el punto principal de establecimiento será la gestión, definición y mantención del sistema de gobierno para la implementación de nuevas TI como se puede observar en la figura 35.

Tabla 35. Importancia de adopción de TI

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/ gestión	**Valoración**	**Referencia**	**Importancia relativa**
EDM01	3,15	2,50	**25**
EDM02	3,53	2,58	**35**
EDM03	1,38	1,08	**30**
EDM04	2,33	2,00	**15**
EDM05	1,38	1,08	**30**
APO01	2,20	1,58	**40**
APO02	3,60	2,93	**25**
APO03	1,75	1,15	**50**
APO04	3,55	2,85	**25**
APO05	3,48	2,50	**40**
APO06	1,08	1,35	**-20**
APO07	2,13	1,23	**75**
APO08	2,58	1,65	**55**
APO09	1,45	1,43	**0**
APO10	2,20	1,58	**40**
APO11	1,45	1,43	**0**
APO12	1,83	1,50	**20**
APO13	1,00	1,00	**0**
APO14	2,28	1,93	**20**
BAI01	3,60	2,93	**25**
BAI02	3,10	2,43	**30**
BAI03	3,48	2,50	**40**
BAI04	1,45	1,43	**0**
BAI05	2,65	2,00	**35**
BAI06	2,28	1,93	**20**
BAI07	3,10	2,43	**30**
BAI08	1,38	1,08	**30**
BAI09	1,00	1,00	**0**
BAI10	1,38	1,08	**30**
BAI11	3,10	2,43	**30**

DSS01	1,00	1,00	**0**
DSS02	1,00	1,00	**0**
DSS03	1,38	1,08	**30**
DSS04	1,38	1,08	**30**
DSS05	1,38	1,08	**30**
DSS06	1,00	1,00	**0**
MEA01	2,65	2,00	**35**
MEA02	1,00	1,00	**0**
MEA03	1,00	1,00	**0**
MEA04	1,00	1,00	**0**

Adaptado: [5]

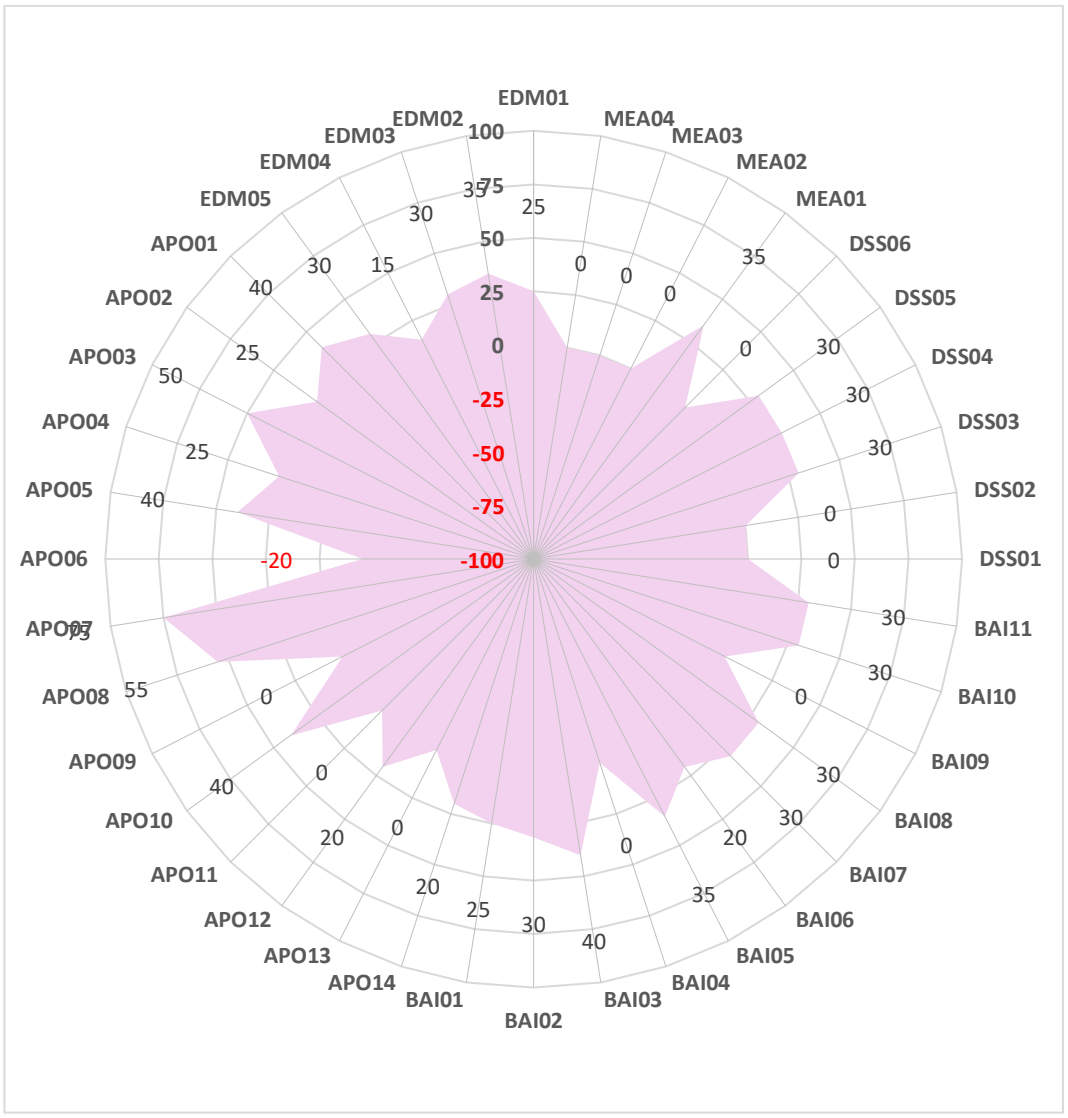


Figura 23. Factor de diseño Adopción de tecnología

3.2. Resultados de los Métodos Específicos

3.2.1. Diseño Inicial de Gobierno

La consideración de los 40 objetivos detallados a continuación según su nivel de importancia nos da un alcance inicial de valoración de los objetivos de gobierno y gestión, basándose en los parámetros de la estrategia empresarial, metas empresariales, perfiles de riesgo y problemas relacionados con las tecnologías de la información.

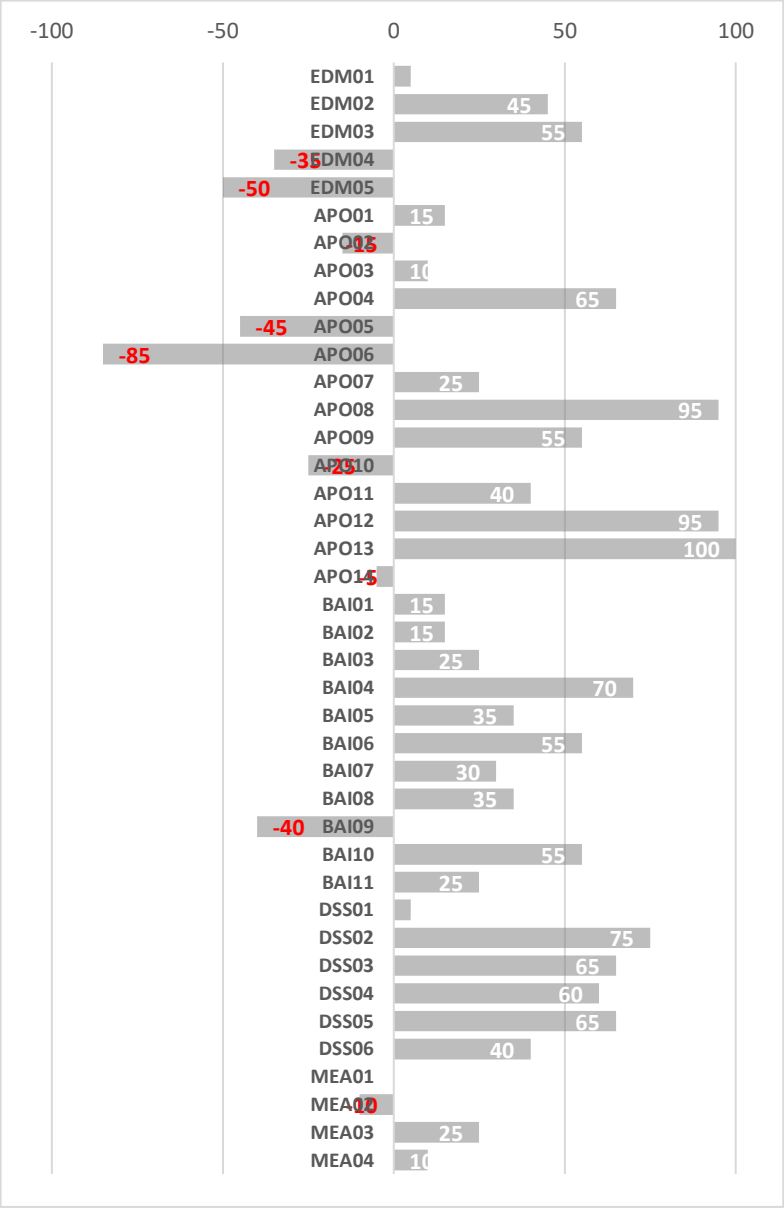


Figura 24. Diseño inicial Obj. de Gobierno y Gestión

Al determinar la importancia de los objetivos de gobierno y gestión como diseño inicial nos da una referencia amplia de utilización para abordar una variedad de problemas relacionados con la gobernanza de TI los cuales incluyen los siguientes objetivos de gobierno y gestión considerados desde el 75% como indica el diseño como valor importante y los escenarios de amenazas los cuales se detallan en la siguiente tabla.

Tabla 36. Importancia de Objetivos de Gobierno y Gestión

CODIGO OBJETIVOS	PORCENTAJE DE IMPORTANCIA	OBJETIVOS DE GOBIERNO Y GESTIÓN
APO08	95%	Relaciones de administración
APO12	95%	Gestión de riesgo
APO13	100%	Gestión de seguridad
DSS02	75%	Solicitudes e incidentes de servicios gestionados

Fuente: Investigador

Los objetivos de gobierno que evalúan dirigen y monitorean como el EDM04, EDM05, APO02, APO05, APO06, APO10, APO15, BAI09, MEA02, No se consideran relevantes para el logro de objetivos establecidos en el diseño pero posterior a la consideración de los niveles de importancia tanto en escenarios de amenaza, cumplimiento de requisitos, importancia del rol de las TI, la importancia del abastecimiento de proveedores, la importancia de los métodos de implementación de las TI, y la consideración de las estrategias de adopción de tecnologías nos permite restablecer la importancia de todos los factores de diseño dándonos un resultado de alcance y perfeccionamiento en la valoración de los objetivos gobernantes de gestión en el hospital.

La siguiente tabla contiene la información total del alcance inicial del sistema de gobierno lo que permitirá posteriormente desarrollar un perfeccionamiento en base al ajuste de cada uno de los 40 objetivos de gobierno y gestión, que en este caso los ajustes no sufrirán ningún cambio por lo que se mantendrá los objetivos originales al diseño de alcance inicial.

Tabla 37. Sistema de Gobierno Inicial

	Paso 2: Determinar el alcance inicial del sistema de gobierno					
:	Estrategia empresarial	Metas empresariales	Perfil de riesgo	Problemas relacionados con I&T		Alcance inicial: Valoración de los objetivos de gobierno/gestión
Ponderación	1	1	1	1		
EDM01—Asegurar el establecimiento y el mantenimiento del marco de gobierno	5	10	0	-10		5
EDM02—Asegurar la entrega de beneficios	30	5	15	-5		45
EDM03—Asegurar la optimización del riesgo	25	25	15	-10		55
EDM04—Asegurar la optimización de recursos	-25	0	-15	5		-35
EDM05—Asegurar el compromiso de las partes interesadas	15	-35	-15	-15		-50
APO01—Gestionar el marco de gestión de I&T	0	5	15	-5		15
APO02—Gestionar la estrategia	-20	5	-5	5		-15
APO03 —Gestionar la arquitectura empresarial	-20	10	15	5		10
APO04—Gestionar la innovación	-5	5	45	20		65

APO05—Gestionar el portafolio	-25	0	-15	-5		-45
APO06—Gestionar el presupuesto y los costes	-25	-30	-20	-10		-85
APO07—Gestionar los recursos humanos	-10	5	15	15		25
APO08—Gestionar las relaciones	45	5	40	5		95
APO09—Gestionar los acuerdos de servicio	45	10	10	-10		55
APO10—Gestionar los proveedores	-10	5	-10	-10		-25
APO11—Gestionar la calidad	50	-25	30	-15		40
APO12—Gestionar los riesgos	30	20	50	-5		95
APO13—Gestionar la seguridad	35	25	55	-15		100
APO14—Gestionar los datos	0	-25	35	-15		-5
BAI01—Gestionar los programas	-15	0	15	15		15
BAI02—Gestionar la definición de requisitos	-5	5	15	0		15
BAI03—Gestionar la identificación y construcción de soluciones	-5	5	35	-10		25
BAI04—Gestionar la	40	10	35	-15		70

disponibilidad y la capacidad						
BAI05— Gestionar el cambio organizativo	-15	0	45	5		35
BAI06— Gestionar los cambios de TI	0	10	45	0		55
BAI07— Gestionar la aceptación y la transición del cambio de TI	5	5	25	-5		30
BAI08— Gestionar el conocimiento	-5	5	15	20		35
BAI09— Gestionar los activos	0	-60	15	5		-40
BAI10— Gestionar la configuración	0	15	40	0		55
BAI11— Gestionar los proyectos	-20	0	35	10		25
DSS01— Gestionar las operaciones	15	10	-5	-15		5
DSS02— Gestionar las peticiones y los incidentes de servicio	50	15	30	-20		75
DSS03— Gestionar los problemas	40	15	15	-5		65
DSS04— Gestionar la continuidad	50	15	10	-15		60
DSS05— Gestionar los servicios de seguridad	35	25	20	-15		65
DSS06— Gestionar los controles de	15	15	35	-25		40

procesos de negocio						
MEA01—Gestionar la monitorización del rendimiento y la conformidad	**0**	**-5**	**10**	**-5**		**0**
MEA02—Gestionar el sistema de control interno	**0**	**0**	**5**	**-15**		**-10**
MEA03—Gestionar el cumplimiento de los requisitos externos	**0**	**35**	**20**	**-30**		**25**
MEA04—Gestionar el aseguramiento	**0**	**0**	**20**	**-10**		**10**

Adaptado: [5]

3.2.2. Perfeccionamiento del Sistema de Gobierno

Para el perfeccionamiento del sistema de gobierno luego de obtener el diseño de alcance inicial se consideran criterios de importancia en escenarios de amenazas, requisitos de cumplimiento, rol de las TI, modelos de abastecimiento a TI, métodos de implementación de TI, y estrategias de adopción de las tecnologías. Lo que nos da como resultado una valoración diferente en los objetivos de gobierno cómo se observa en la tabla siguiente.

Tabla 38. Perfeccionamiento de EGIT

Paso 3: Perfeccionar el alcance del sistema de gobierno						
Escenario de amenazas	**Requisitos de cumplimiento**	**Rol de TI**	**Modelo de abastecimiento de proveedores para TI**	**Métodos de implementación de TI**	**Estrategia de adopción de tecnología**	**Alcance perfeccionado: Valoración de los objetivos de gobierno/gestión**
1	**1**	**1**	**1**	**1**	**1**	
50	**70**	**20**	**0**	**0**	**25**	**60**

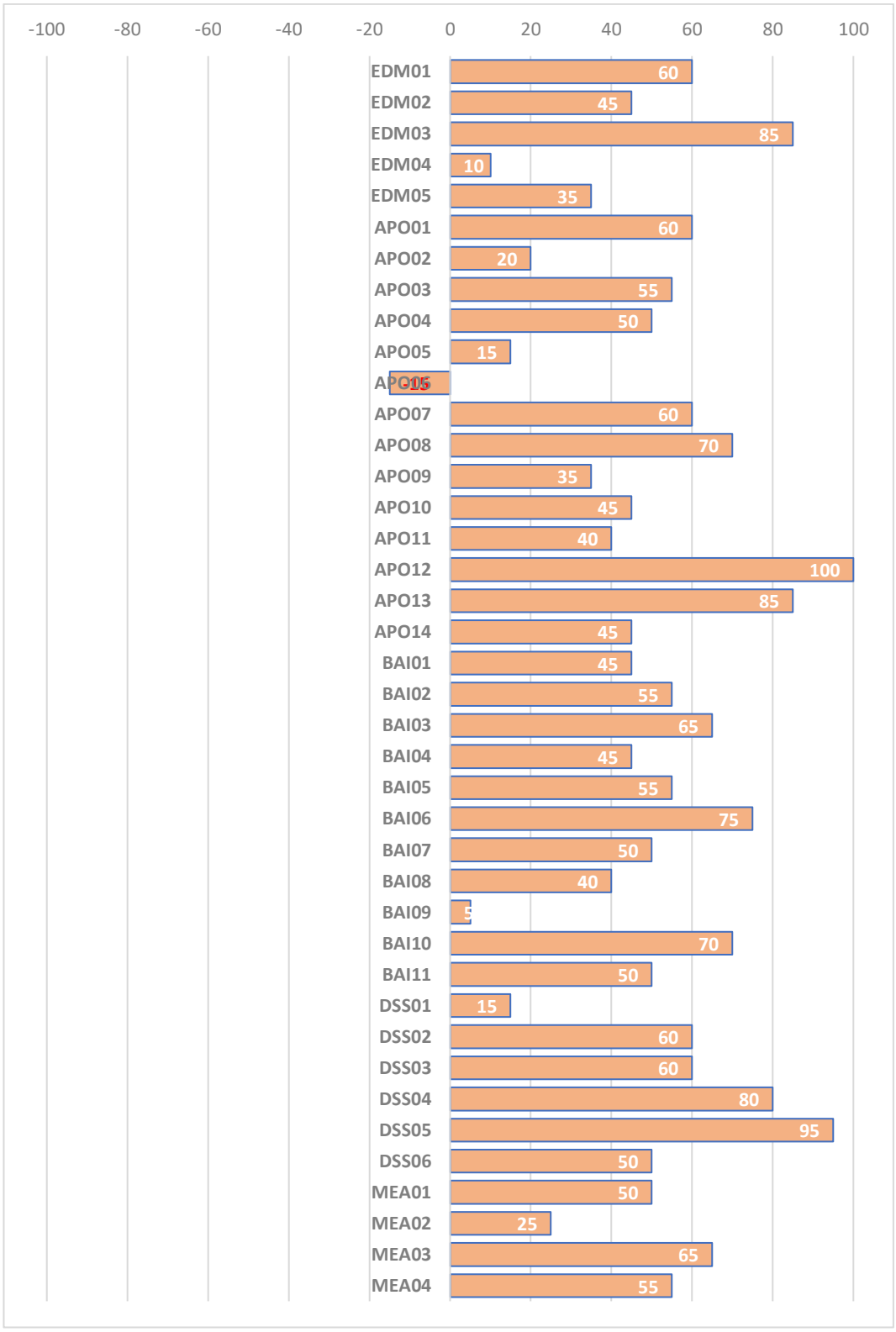
0	40	15	0	0	35	45
65	110	5	-10	0	30	85
0	40	15	0	0	15	10
30	80	15	0	0	30	35
50	60	10	0	0	40	60
0	40	15	0	0	25	20
50	40	10	0	0	50	55
0	40	20	0	0	25	50
0	40	15	0	0	40	15
0	40	15	0	0	-20	-15
30	40	10	0	0	75	60
0	40	15	0	0	55	70
30	40	0	-15	0	0	35
50	80	-5	-15	0	40	45
30	40	5	0	0	0	40
65	110	10	-10	0	20	100
65	80	10	0	0	0	85
50	60	10	0	0	20	45
0	40	15	0	30	25	45
0	40	15	0	60	30	55
0	40	15	0	65	40	65
30	40	-5	0	0	0	45
0	40	15	0	40	35	55

50	**40**	**0**	**0**	**60**	**20**	**75**
0	**40**	**10**	**0**	**40**	**30**	**50**
0	**40**	**15**	**0**	**0**	**30**	**40**
0	**40**	**15**	**0**	**0**	**0**	**5**
50	**40**	**10**	**0**	**15**	**30**	**70**
0	**40**	**10**	**0**	**45**	**30**	**50**
0	**40**	**0**	**0**	**0**	**0**	**15**
50	**40**	**5**	**0**	**0**	**0**	**60**
30	**40**	**5**	**0**	**0**	**30**	**60**
65	**80**	**5**	**0**	**0**	**30**	**80**
50	**115**	**10**	**0**	**0**	**30**	**95**
50	**40**	**20**	**0**	**0**	**0**	**50**
50	**40**	**15**	**-15**	**15**	**35**	**50**
30	**40**	**15**	**0**	**0**	**0**	**25**
50	**110**	**10**	**0**	**0**	**0**	**65**
50	**90**	**15**	**0**	**0**	**0**	**55**

Adaptado: [5]

Los objetivos de gobierno y gestión que superan el 75% de importancia y son considerados formar parte del sistema de gobierno de TI son EDM03, APO08, PO12, APO13, BAI06, DSS04, DSS05.

Figura 25. Importancia de los Obj. de Gobierno y Gestión todos los factores de diseño


-100
-80
-60
-40
-20
0
20
40
60
80
100
EDM01 60
EDM02 45
EDM03 85
EDM04 10
EDM05 35
APO01 60
APO02 20
APO03 55
APO04 50
APO05 15
APO06
APO07 60
APO08 70
APO09 35
APO10 45
APO11 40
APO12 100
APO13 85
APO14 45
BAI01 45
BAI02 55
BAI03 65
BAI04 45
BAI05 55
BAI06 75
BAI07 50
BAI08 40
BAI09
BAI10 70
BAI11 50
DSS01 15
DSS02 60
DSS03 60
DSS04 80
DSS05 95
DSS06 50
MEA01 50
MEA02 25
MEA03 65
MEA04 55

Adaptado: [5]

3.2.3. Sistema de Gobierno Final

El sistema de gobierno TI final a través de la metodología COBIT 2019, Nos permite visualizar la prioridad de los objetivos de gobierno y gestión alineados a las metas empresariales lo que nos sugiere un nivel de capacidad en el rango de 0 a 5, lo cual nos indica que:

Nivel 0 - Sin capacidad: Indica que el proceso no está implementado o no tiene capacidad para lograr sus objetivos. Es el nivel más bajo de madurez.

Nivel 1 - Realizado: El proceso se realiza de manera ad hoc y es de naturaleza informada principalmente por las personas involucradas. Puede haber poca consistencia y dependencia de individuos clave.

Nivel 2 - Gestionado: El proceso está gestionado de manera planificada y controlada. Se establecen objetivos y se toman medidas para asegurar que se cumplan. Existen políticas y procedimientos documentados.

Nivel 3 - Establecido: El proceso está establecido y se siguen prácticas estandarizadas. Los procedimientos están documentados y se siguen de manera consistente en toda la organización.

Nivel 4 - Predecible: El proceso está medido, controlado y se sigue de manera predecible. Los resultados son monitoreados y se toman acciones correctivas cuando sea necesario para mantener la efectividad del proceso.

Nivel 5 - Optimizado: El proceso está completamente optimizado y se mejora continuamente. Se utilizan las mejores prácticas y se implementan innovaciones para lograr la excelencia en el desempeño.

De igual manera los niveles de objetivos acordados cuentan con el mismo nivel de capacidad que los sugeridos cómo se pueden observar en la siguiente tabla.

Tabla 39. Niveles de capacidad Objetivos

Paso 4: Finalizar el alcance del sistema de gobierno					
Ajuste (entre -100 y +100)	Motivo	Conclusión del alcance: Prioridad de los objetivos de gobierno/gestión	Nivel de capacidad objetivo sugerido	Nivel de capacidad objetivo acordado	Motivo
		60	3	3	
		45	2	2	
		85	4	4	
		10	1	1	
		35	2	2	
		60	3	3	
		20	1	1	
		55	3	3	
		50	3	3	
		15	1	1	
		-15	1	1	
		60	3	3	
		70	3	3	
		35	2	2	
		45	2	2	
		40	2	2	
		100	4	4	
		85	4	4	

		45	**2**	**2**	
		45	**2**	**2**	
		55	**3**	**3**	
		65	**3**	**3**	
		45	**2**	**2**	
		55	**3**	**3**	
		75	**4**	**4**	
		50	**3**	**3**	
		40	**2**	**2**	
		5	**1**	**1**	
		70	**3**	**3**	
		50	**3**	**3**	
		15	**1**	**1**	
		60	**3**	**3**	
		60	**3**	**3**	
		80	**4**	**4**	
		95	**4**	**4**	
		50	**3**	**3**	
		50	**3**	**3**	
		25	**2**	**2**	
		65	**3**	**3**	
		55	**3**	**3**	

Adaptado: [5]

Tabla 40. Importancia de Objetivos de Gobierno y Gestión Final

CODIGO OBJETIVOS	PORCENTAJE DE IMPORTANCIA	OBJETIVOS DE GOBIERNO Y GESTIÓN
EDM03	85%	Aseguramiento de optimización de riesgos
APO12	100%	Gestión de riesgo
APO13	85%	Gestión de seguridad
BAI06	75%	Gestión en Cambios de TI
DSS04	80%	Gestión de continuidad
DSS05	85%	Gestión de Servicios de seguridad

Fuente: Investigador

Cada uno de estos objetivos presenta un grado de importancia esencial para el marco de gobernanza de TI en los cuáles se pueden conocer su descripción, su propósito, sus metas empresariales a las cuales deseamos llegar; además de las metas de alineamiento de las TI, con sus respectivos parámetros de métricas tanto para las metas empresariales como las metas de alineamiento TI.

Además, nos permite conocer los componentes que ejecuta los procesos de práctica y cuáles son sus actividades a desarrollarse para ejecutar cada uno de estos objetivos con su nivel de capacidad sugerido cómo se puede observar en el **anexo 3.**

3.3. Resultado del diseño experimental y/o método de criterio de experto que demuestren la validación de la propuesta

En el cuestionario aplicado a expertos en las diferentes áreas de gobierno y gestión del Hospital General Docente Ambato se obtuvieron los siguientes resultados que han sido analizados para la correspondiente validación de la propuesta de investigación de acuerdo con su consistencia teórica, pertinencia, coherencia de la metodología, importancia y factibilidad de plan de gobernanza de TI para el logro de los objetivos institucionales en servicios de salud.

Se cuenta con el criterio de un especialista en administración de instituciones de salud Gerente de hospital con 7 años de experiencia, de un Magíster en Gestión Local y Políticas Públicas, Directora Administrativo Financiera con Diplomado

Superior en Planificación Estratégica del Sector Público con 14 años de experiencia; con un Magister en Gestión Local y Políticas Públicas, Director Asistencial con 4 años de experiencia; con un Magister en Gestión de Bases de Datos, Analista de TIC 3 con 5 años de experiencia, un Magister en Enfermería, Responsable de Gestión de Calidad con 4 años de experiencia; y un Ingeniero en Sistemas, Analista de Soporte Técnico de TI con 5 años de experiencia como se observa en la tabla 41.

Tabla 41. Profesionales expertos

Profesional Experto	**Años de Experiencia**	**Perfil**
Edwin Fabián Chango Zumba	7	Especialista en administración de instituciones de salud, Gerente
Mayda Amalia Robalino Gavilanes	14	Diplomado Superior en Planificación Estratégica del Sector Publico / Magister en Gestión Local y Políticas Públicas, Directora Administrativo Financiera
Jorge Enrique Lana Cisneros	4	Magister en Gestión Local y Políticas Públicas, Director Asistencial
Jorge Danilo Naranjo Calderón	5	Magister en Gestión de Bases de Datos, Analista de TIC 3
Diana Nathalie Navarrete Tinajero	4	Magister en Enfermería, Responsable de Gestión de Calidad
Juan Pablo Rodríguez Betancourt	5	Ingeniero en Sistemas, Analista de Soporte Técnico de TI

Elaborado por: autor.

Con el criterio de expertos se consultó las siguientes preguntas como indica el ANEXO1:

¿Considera que el marco de referencia COBIT 2019 aborda áreas de gobernanza TI y maneja considerablemente desafíos que impulsan el logro de objetivos institucionales?

En donde 6 personas indican que se encuentran totalmente de acuerdo con el fundamento teórico para el desarrollo del plan de gobernanza COBIT.

¿Considera que el uso de COBIT 2019 como marco de referencia es apropiado y relevante para abordar los desafíos de gobernanza TI como en el caso del Hospital General Docente Ambato?

6 personas se encuentran totalmente de acuerdo que la metodología aborda el tema y desafíos para implementar un plan de gobernanza TI en un hospital.

¿Considera que el enfoque de medición, factores, evaluación de diseño y gestión propuesto es adecuado para evaluar el impacto y los resultados de la implementación del plan de gobernanza a través de metodología COBIT 2019 en el Hospital General Docente Ambato?

6 personas están totalmente de acuerdo COBIT enfoca factores de evaluación en diseño y gestión TI para impulsar el desarrollo de actividades que encaminen al logro de objetivos institucionales y entrega de valor a las demás unidades del Hospital General Docente Ambato

¿Considera que la metodología planteada para el desarrollo del plan de gobernanza TI se asocia con los objetivos estratégicos hospitalarios y tenga las herramientas de control y efectividad de aplicación progresivo, considerando el entorno de trabajo de las demás unidades y servicios que tiene el Hospital General Docente Ambato?

1 persona se encuentra de acuerdo y 5 personas se encuentran totalmente de acuerdo que es factible una implementación de un plan de gobernanza TI y que el hospital cuente con una herramienta de control y efectividad en logro de objetivos alineados a las estrategias de negocio del Hospital General Docente Ambato.

¿Considera que la presente propuesta contribuye positivamente en el desarrollo de actividades y servicios que se generan en el Hospital General Docente Ambato?

1 persona se encuentra de acuerdo y 5 personas se encuentran totalmente de acuerdo que el plan de gobernanza TI impulsará el desarrollo de toma de decisiones institucionales y que contribuirán positivamente acciones tecnológicas en bien de la comunidad como usuarios de servicios de salud.

Tabla 42. Juicio de expertos

VALORACIÓN DE EXPERTOS					
	Totalmente en desacuerdo	**En desacuerdo**	**Medianamente de acuerdo**	**De acuerdo**	**Totalmente de acuerdo**
Consistencia teórica				2	4
Pertinencia				2	4
Coherencia metodológica				1	5
Factibilidad				1	5
Importancia				1	5

Elaborado por: autor.

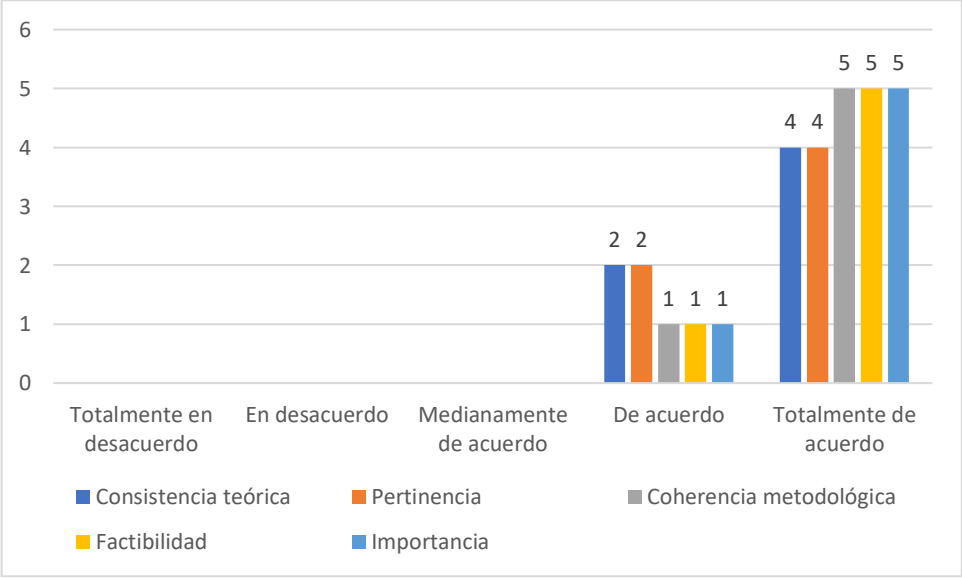


Figura 26. Juicio de expertos

Fuente: Investigador

3.3.1. Confiabilidad de la Validación

Luego de realizar la valoración a través del test a los expertos, se identifica el conjunto de preguntas que nos permitirá medir la confiabilidad de la validación, para lo cual se usa la escala de Likert [24] para organizar los datos y aplicar alfa de Cronbach [25] que se calcula de la siguiente fórmula:

$$\alpha = \frac{k}{k-1}\left[1 - \frac{\sum V_i}{V_t}\right]$$

$\propto: alfa\ de\ cronbach$

$k: Número\ de\ ítems$

$V_i: Varianza\ de\ cada\ ítem$

$V_t: Varianza\ del\ total$

En la tabla 43 se observan las valoraciones que los expertos asignaron a la validación de la propuesta de plan de gobernabilidad TI.

Tabla 43. Datos Confiabilidad de Validación de propuesta

EXPERTO	ITEM 1	ITEM 2	ITEM 3	ITEM 4	ITEM 5	TOTAL
1	5	5	5	5	5	**25**
2	5	5	5	5	5	**25**
3	5	5	5	5	5	**25**
4	5	5	5	5	5	**25**
5	4	4	5	5	5	**23**
6	4	4	4	4	4	**20**
VARIANZA	**0,222222**	**0,222222**	**0,138889**	**0,138889**	**0,138889**	**3,47222222**

Elaborado por: autor

En donde se obtuvieron los siguientes datos:

$$\alpha = \frac{5}{5-1}\left[1 - \frac{0.861111}{3.472222}\right]$$

Tabla 44. Coeficiente Alfa de Cronbach

Numero de ítems **K**	5
Sumatoria de varianzas de cada ítem **Vi**	0,861111
Varianza Total **Vt**	3,472222
Alfa de Cronbach **α**	0,94

Elaborado por: autor

El coeficiente alfa de 0.94 se considera excelente ya que muestra una alta fiabilidad de la escala y representa una mayor confianza en las puntuaciones obtenidas mediante esta escala que se acerca al valor de 1, valor máximo del coeficiente.[25]

3.4. Resultados de la valoración económica, tecnológica, operacional y ambiental

Para el desarrollo de este proyecto Metodología COBIT para el desarrollo de plan de gobernanza de Tecnologías de la Información y Comunicación en Hospitales Generales se considera 2 tipos de gastos, directos y los indirectos:

Tabla 45. Gastos directos

GASTOS DIRECTOS				
DESCRIPCIÓN	**DETALLE**	**CANT./HORAS**	**PRECIO**	**TOTAL**
Fundamentar teóricamente los conocimientos que se relacionen con el marco de referencia COBIT aplicado a la organización y conformación del Plan de Gobernabilidad TI en el Hospital General Docente Ambato	Revisión de la Metodología COBIT 2019 - ISACA	24	6.00	144.00
	Conocimiento metodológico en Gobernanza y Objetivos de Gestión	24	6.00	144.00
	Conocimiento metodológico en diseño de solución de gobierno de la información y la tecnología	24	6.00	144.00
	conocimiento metodológico en implementación y optimización de una solución de gobierno de la información y la tecnología	24	6.00	144.00
	Revisión de la documentación oficial de los estatutos de gestión organizacional por	24	6.00	144.00

	procesos del MSP del Ecuador en Hospitales Generales			
	Revisión de los lineamientos y/o políticas de gestión en servicios informáticos, ingeniería de software, proyectos tecnológicos, comunicaciones y centros de soporte TI para establecimientos de Salud Pública del Ecuador.	24	6.00	144.00
Establecer el diseño metodológico para las métricas del Plan de Gobernanza de Tecnologías de la Información y Comunicación en el Hospital General Docente Ambato.	Definir la cascada de metas	32	15.00	480.00
	Identificar metas empresariales	32	15.00	480.00
	Definir Metas de alineamiento	32	15.00	480.00
	Relacionar metas empresariales vs metas de alineamiento	32	15.00	480.00
	Determinar el resultado del proceso entre objetivos de gobierno y gestión por dominio	32	15.00	480.00
Desarrollar un Plan de Gobernanza de TI de acuerdo a las métricas obtenidas del Plan de Gobernanza de Tecnologías de la Información y Comunicación en el Hospital General Ambato.	Definir los factores de diseño	48	15.00	720.00
	Determinar los aplicativos de instrumentos en los factores de diseño	48	15.00	720.00
	Establecer los objetivos de Gobierno y Gestión COBIT	48	15.00	720.00
Equipo Tecnológico	Computador	1	1500	1500
	Internet	448	0.80	358.40
Insumos Oficina	Impresiones	200	0.10	20,00
	Papel A4	1	4,70	4,70
	Carpeta	2	0,75	1,50

	TOTAL	7308,60

Tabla 46. Gastos Indirectos

GASTOS INDIRECTOS				
DESCRIPCIÓN	**DETALLE**	**CANT. /HORAS**	**PRECIO**	**TOTAL**
OTROS	Transporte	56	2,50	140,00
	Alimentación	56	3,50	196,00
	Imprevistos	1	100.00	100,00
TOTAL				436,00

Tabla 47.Gastos Totales

COSTO TOTAL DEL PROYECTO	
DETALLE	**TOTAL**
Gastos Directos	7308,60
Gastos Indirectos	436,00
TOTAL	**7744,60**

El proyecto de investigación tiene un costo total de 7744,60 dólares; pero hay que tomar en cuenta que este costo podría ser un monto de inversión ya que se han detectado riesgos que pueden causar pérdidas de diferente índole al hospital, como pérdida de activos fijos, pérdida de productos de inversión, pérdidas en proyectos tecnológicos entre otros.

3.5. Discusión de la aplicación y/o validación de la propuesta

El desarrollo del plan de gobernanza de TI utilizando metodología COBIT 2019 es altamente ventajosa para el Hospital General Docente Ambato al proporcionar un amplio y reconocido marco de referencia a nivel internacional estableciendo una gobernanza efectiva de la tecnología de la información.

A la línea los objetivos estratégicos con los de TI se garantiza que las TI sea un habilitador y generación de valor para el logro de resultados institucionales deseados. Las TI al definir una estrategia que se encuentra en sintonía con la visión y los objetivos de la institución establece un conjunto claro de controles y procesos para gestionar las TI de forma efectiva.

La socialización con los directivos del Hospital General Docente Ambato de esta herramienta como plan de gobernanza de TI permitió conocer y dar un espacio a las tecnologías de la información en la toma de decisiones directivas que impulsen la generación de valor para las demás áreas que brindan servicios de salud hacia los siempre a la vanguardia de la implementación de nuevas tecnologías, seguridades de la información y desarrollo de la salud en el país.

3.6. Conclusiones Capítulo III

La finalización de este capítulo permitió la elaboración del plan de gobernanza de TI a través de la metodología COBIT2019 para que el personal que lidera cada uno de los servicios en esta casa de salud puedan contar con un marco metodológico y la unidad de tecnologías de la información y comunicación se convierta en el apoyo tecnológico con normas y políticas internas que impulsen el desarrollo institucional.

Se analizaron cada uno de los 40 objetivos de gobierno y gestión que la metodología COBIT 2019 emplea para el desarrollo de gobernanza de TI con el grupo de profesionales que lideran cada uno de los servicios gerenciales y administrativos para establecer un enfoque estructurado y medible que generen mejores prácticas y procesos definidos internos y así la institución pueda maximizar el valor y los beneficios que las TI aportarán al hospital.

El presente plan con metodología COBIT en gobernanza de TI para el Hospital General Docente Ambato contiene los siguientes objetivos de gobierno y gestión conocidos como EDM3- aseguramiento y optimización de riesgos, APO08 - relaciones de administración, APO12 - gestión de riesgos, APO13 - gestión de seguridad, BAI06 - gestión en cambios de TI, DSS04 - gestión de solicitudes e incidentes de servicio, DSS05 - gestión de continuidad de procesos; cada uno contiene las correspondientes prácticas de gestión, ejemplos de métricas, actividades a establecerse con la asignación de responsables en el cumplimiento de esta normativa de gobierno.

El plan metodológico COBIT para el gobierno de TI en el Hospital General Docente Ambato tiene componentes estructurales organizacionales en el cual se asignan los responsables de gobierno, gestión y control que ayudarán a identificar y ejecutar las

diferentes acciones que deben realizarse para cumplimiento de los objetivos institucionales.

CONCLUSIONES GENERALES

Para la finalización de esta investigación se revisó Fuentes bibliográficas que permitieron fundamentar teóricamente los conocimientos que se relacionen con la metodología del marco de referencia COBIT aplicado a la conformación de planes de gobernabilidad TI.

Se logró establecer el diseño metodológico para conocer las métricas del plan de gobernanza de tecnologías de la información y comunicación en el Hospital General Docente Ambato.

Se logró el desarrollo del plan de gobernanza de TI de acuerdo con las métricas y objetivos de gobierno y gestión obtenidas a través de la metodología COBIT alineado a los objetivos institucionales para mejorar la eficiencia y la efectividad de la gestión de TI, como un manual de buenas prácticas en el manejo de las TI para mejorar eficiencia y efectividad de gestión en el hospital, con un coeficiente de confiabilidad de validación por expertos de 0.94 lo que representa una mayor confianza en las puntuaciones obtenidas de aceptación del plan desarrollado.

RECOMENDACIONES

Se recomienda a las autoridades del Hospital General Docente Ambato que en el presente plan se consideren las actualizaciones constantes en base a los objetivos que la institución desea alcanzar ya que contiene un conjunto bien definido de mejores prácticas y procesos en la gestión de riesgos, cumplimiento normativo, seguridad de la información y optimización de recursos TI, y estos no serán permanentes ya sea por el cambio de nuevas autoridades o contratación de nuevo personal.

El presente plan de gobernanza de TI para el Hospital General Docente Ambato puede ser implementado como un marco de control interno para el funcionamiento de la unidad de tecnologías de la información y comunicación, por lo que se recomienda la constante capacitación al personal sobre los conceptos principios y prácticas COBIT que ayuden a garantizar el conocimiento de sus responsabilidades en este marco de gobernanza.

Se recomienda al Hospital General Docente Ambato la implementación de este plan de gobierno de TI que contiene diferentes objetivos de gobierno y gestión determinados por actividades, métricas, metas TI, metas institucionales, métricas de acción, prácticas de gestión, que beneficiará al manejo de TI y el impulso de la institución en innovación, seguridad de la información, mitigación de riesgos que permitan la continuidad de procesos y no genere interrupción de servicios a pacientes en tratamientos de salud.

Se recomienda para el caso de que el hospital intente entrar en proceso de mejora continua a través del uso de este plan de gobernanza fomente la colaboración entre los diferentes departamentos que involucra el compromiso de la institución.

REFERENCIAS BIBLIOGRÁFICAS

[1] L. G. Molina Marin Yeison - Orozco Nott, "Vulnerabilidades de los Sistemas de Información: una revisión", 2020. [En línea]. Disponible en: https://dspace.tdea.edu.co/handle/tdea/1398

[2] Observatorio Social del Ecuador, "Monitoreo del coronavirus covid-19 en Ecuador", *Monitoreo del coronavirus covid-19 en Ecuador*, 12 de septiembre de 2022. https://www.covid19ecuador.org/ecuador (accedido 7 de marzo de 2023).

[3] MINISTERIO DE SALUD PUBLICA, *ESTATUTO ORGANICO GESTION ORGANIZACIONAL POR PROCESOS DE HOSPITALES*. ECUADOR: Registro Oficial Edición Especial 339 de 25-sep.-2012, 2012, pp. 26–27. Accedido: 31 de enero de 2022. [En línea]. Disponible en: https://www.salud.gob.ec/wp-content/uploads/2019/04/ESTATUTO-GESTION-ORGANIZACIONES-HOSPITALES-RO-339-25-09-2012.pdf

[4] Ministerio de Salud Pública del Ecuador, *Acuerdo Ministerial 2880*. Ecuador, 2013, pp. 1–2.

[5] ISACA, *COBIT® 2019 Framework : introduction and methodology*. Accedido: 27 de diciembre de 2021. [En línea]. Disponible en: www.isaca.org

[6] Asamblea Constituyente Ecuador 2008, "Constitución de la República del Ecuador", 2008. Accedido: 6 de febrero de 2022. [En línea]. Disponible en: https://www.gob.ec/sites/default/files/regulations/2020-06/CONSTITUCION%202008.pdf

[7] A. Cortés, "Evaluación por medio de COBIT 2019, del modelo de gestión de tecnologías de información y comunicación de la municipalidad de carrillo, producto de los procesos de migración de sistemas operativos e informáticos", Universidad de Costa Rica, Costa Rica, 2021.

[8] F. Lopez, F. Bolivar, Q. Chauca, y A. Liceth, "Implementación de los procesos de Gobierno de COBIT 2019 en la Dirección de Tecnologías de la Información y Comunicaciones del Ejército del Ecuador", Maestría en Gerencia de Sistemas, Universidad de las Fuerzas Armadas ESPE, Sangolqui, 2020.

[9] Gobierno de la República del Ecuador, "Ministerio de Salud Pública del Ecuador", *Plataforma Gubernamental de Desarrollo Social*, 2023.

[10] Ministerio de Salud Publica del Ecuador, "VALORES, MISIÓN, VISION MSP", *"Planificación, gestión, coordinación y control de la salud pública"*, 8 de febrero de 2022. https://www.salud.gob.ec/valores-mision-vision/ (accedido 7 de febrero de 2022).

[11] MINISTERIO DE SALUD PUBLICA, *ESTATUTO ORGANICO GESTION ORGANIZACIONAL POR PROCESOS DE HOSPITALES*. Ecuador: https://www.salud.gob.ec/wp-content/uploads/2019/04/ESTATUTO-GESTION-ORGANIZACIONES-HOSPITALES-RO-339-25-09-2012.pdf, 2012, p. 40.

[12] V. Grembergen, *Strategies for Information Technology Governance*. London.

[13] ISACA Serving IT Governance Professionals, *Standar ISO/IEC 38500*. 2015.

[14] Information Systems Audit and Control Association, *COBIT® 2019 Framework : introduction and methodology*.

[15] ISACA, "ISACA sobre nosotros", 1 de julio de 2023. https://www.isaca.org/about-us (accedido 30 de junio de 2023).

[16] ISACA, *Designing an Information and Technology Governance Solution*. 2018.

[17] ANDRÉS ALBERTO CORTÉS FUENTES, "EVALUACIÓN POR MEDIO DE COBIT 2019, DEL MODELO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA MUNICIPALIDAD DE CARRILLO, PRODUCTO DE LOS PROCESOS DE MIGRACIÓN DE SISTEMAS OPERATIVOS E INFORMÁTICOS", Ciudad Universitaria Rodrigo Facio, Costa Rica, 2021.

[18] F. B. y Q. C. L. A. Fabara López, "Implementación de los procesos de Gobierno de COBIT 2019 en la Dirección de Tecnologías de la Información y Comunicaciones del Ejército del Ecuador", Universidad de las Fuerzas Armadas ESPE, Sangolqui, 2020.

[19] Instituto Nacional de Estadisticas y Censos, "Fasículo Ambato población de cantón", Ambato, 2001. Accedido: 25 de abril de 2023. [En línea]. Disponible en: https://www.ecuadorencifras.gob.ec/documentos/web-inec/Bibliotecas/Fasciculos_Censales/Fasc_Cantonales/Tungurahua/Fasciculo_Ambato.pdf

[20] Ministerio de Salud Pública del Ecuador, "Hospital Docente de Ambato se renueva luego de 46 años", *Comunicados Noticias*, 2023. https://www.salud.gob.ec/hospital-docente-de-ambato-se-renueva-luego-de-46-anos/ (accedido 25 de abril de 2023).

[21] Hospital General Docente Ambato, "Rendicion de cuentas HGDA 2019", *Rendicion de cuentas*, Ambato, 2019. Accedido: 25 de abril de 2023. [En línea]. Disponible en: https://www.salud.gob.ec/wp-content/uploads/2020/09/PPT-RENDICIÓN-CUENTAS-2019-HGDA.pdf

[22] Ministerio del Trabajo, *Resolución para la expedición de los Manuales de Descripción, Valoración y Clasificación de Puestos de Planta Central y sus Niveles Desconcentrados, Hospitales y Establecimientos de Salud de Primer Nivel de Atención del Ministerio de Salud Pública.* Ecuador, 2015, pp. 41–41.

[23] Subsecretaría de presupuesto General del Estado, "PROFORMA DEL PRESUPUESTO GENERAL DEL ESTADO CORRESPONDIENTE AL EJERCICIO ECONÓMICO 2022 Y LA PROGRAMACIÓN PRESUPUESTARIA CUATRIANUAL 2022- 2025", 2021, pp. 6–14.

[24] Á. G. Canto de Gante, W. E. Sosa González, Bautista Ortega, J. Escobar Castillo, y A. Santillán Fernández, " Escala de Likert: Una alternativa para elaborar e interpretar un instrumento de percepción social", *Revista de la alta tecnología y sociedad*, 2020.

[25] J. González Alonso y M. Pazmiño Santacruz, "Calculation and interpretation of Cronbach's Alpha for the validation of the internal consistency of a questionnaire, with two possible Likert scales", *Revista Publicando,* 2015.

ANEXOS

ANEXO 1. Cuestionario validación por expertos

Apellidos y Nombres:

Cargo que desempeña:

Experiencia en años:

Marque con una X de acuerdo con el cuadro del cuestionario si:

a. Fundamento Teórico

¿Considera que el marco de referencia COBIT 2019 aborda áreas de gobernanza TI y maneja considerablemente desafíos que impulsan el logro de objetivos institucionales?

Totalmente en desacuerdo	En desacuerdo	Medianamente de acuerdo	De acuerdo	Totalmente de acuerdo

b. Pertinencia

¿Considera que el uso de COBIT 2019 como marco de referencia es apropiado y relevante para abordar los desafíos de gobernanza TI como en el caso del Hospital General Docente Ambato?

Totalmente en desacuerdo	En desacuerdo	Medianamente de acuerdo	De acuerdo	Totalmente de acuerdo

c. Coherencia metodológica

¿Considera que el enfoque de medición, factores, evaluación de diseño y gestión propuesto es adecuado para evaluar el impacto y los resultados de la implementación del plan de gobernanza a través de metodología COBIT 2019 en el Hospital General Docente Ambato?

Totalmente en desacuerdo	En desacuerdo	Medianamente de acuerdo	De acuerdo	Totalmente de acuerdo

d. Factibilidad

¿Considera que la metodología planteada para el desarrollo del plan de gobernanza TI se asocia con los objetivos estratégicos hospitalarios y tenga las herramientas de control y efectividad de aplicación progresivo, considerando el entorno de trabajo de las demás unidades y servicios que tiene el Hospital General Docente Ambato?

Totalmente en desacuerdo	En desacuerdo	Medianamente de acuerdo	De acuerdo	Totalmente de acuerdo

e. Importancia

Considera que la presente propuesta contribuye positivamente en el desarrollo de actividades y servicios que se generan en el Hospital General Docente Ambato.

Totalmente en desacuerdo	En desacuerdo	Medianamente de acuerdo	De acuerdo	Totalmente de acuerdo

Gracias por su colaboración.

ANEXO 2. RESULTADOS ENCUESTA METAS EMPRESARIALES

RESULTADOS ESTRATEGIA EMPRESARIAL

Resultados de encuesta realizada:

PREGUNTAS	PERSONAS																	RESULT
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
Crecimiento/Adquisición	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Innovación/Diferenciación	3	3	2	2	2	4	1	4	1	2	2	2	2	3	2	2	1	2
Liderazgo en costes	3	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1
Servicio al cliente/Estabilidad	5	5	5	5	5	5	4	5	5	5	4	4	5	5	5	5	5	5

RESULTADOS META EMPRESARIAL

Resultados de encuesta realizada:

PREGUNTAS	PERSONAS																	RESULT
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
EG01—Portafolio de productos y servicios competitivos	4	4	3	2	4	3	3	4	3	4	4	3	4	4	3	4	4	4
EG02—Gestión de riesgo del negocio	5	4	3	3	3	4	3	4	3	4	3	3	4	3	3	4	3	3
EG03—Cumplimiento de leyes y regulaciones externas	5	5	5	5	5	4	5	4	5	5	4	5	5	4	5	4	5	5
EG04—Calidad de la información financiera	5	2	2	1	1	1	1	1	1	1	1	1	2	1	2	1	1	1
EG05—Cultura de servicio orientada al cliente	5	3	4	3	3	3	4	4	3	3	3	4	3	3	4	3	5	4
EG06—Continuidad y disponibilidad del servicio del negocio	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
EG07—Calidad de la información de gestión	5	5	2	3	2	2	2	3	2	2	2	2	2	2	2	1	1	2
EG08—Optimización de la funcionalidad de los procesos internos del negocio	5	5	4	3	3	3	4	3	4	3	3	3	3	4	3	3	3	3
EG09—Optimización de costes de los procesos del negocio	5	3	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
EG10—Habilidades, motivación y productividad del personal	5	4	5	4	4	3	4	4	3	4	4	4	3	3	3	4	4	4
EG11—Cumplimiento con las políticas internas	5	5	5	5	5	5	5	4	5	5	5	5	4	5	4	4	5	5
EG12—Gestión de programas de transformación digital	5	5	3	3	2	2	3	2	2	3	2	2	3	3	3	2	3	3
EG13—Innovación de productos y negocios	5	5	5	4	4	5	4	4	4	5	4	4	3	4	4	4	5	4

RESULTADOS ENCUESTA FACTOR DE DISEÑO 2

PREGUNTAS	PERSONAS						RESULT.	
	1	2	3	4	5	6	IMP.	PROB.
Toma de decisiones sobre inversiones en TI, definición y mantenimiento del portafolio	5	5	5	1	1	1	5	1
Gestión del ciclo de vida de los programas y proyectos	5	4	3	2	3	3	4	3
Coste y control de TI	2	1	3	2	1	2	2	2
Comportamiento, habilidades y conocimiento de TI	4	5	4	4	4	5	4	4
Arquitectura de la empresa/TI	1	2	2	2	1	2	2	2
Incidentes de infraestructura operativa de TI	3	2	3	1	2	2	3	2
Acciones no autorizadas	2	2	4	4	5	4	3	4
Adopción de software/problemas de uso	4	4	4	4	3	3	4	3
Incidentes de hardware	2	3	2	1	2	2	2	2
Fallos de Software	3	2	3	3	3	3	3	3
Ataques lógicos (hacking, malware, etc.)	4	4	5	5	5	4	4	5
Incidentes de terceros/proveedores	2	1	2	2	2	1	2	2
Incumplimiento	3	3	3	3	3	3	3	3
Problemas geopolíticos	2	1	3	1	2	2	2	2
Acción industrial	1	1	1	3	2	3	1	3
Actos de la naturaleza	3	2	3	3	3	2	3	3
Innovación basada en la tecnología	5	5	5	3	3	2	5	3
Medio ambiente	2	2	1	3	2	3	2	3
Gestión de datos e información	4	3	4	4	4	3	4	4

ANEXO 3. TABLAS DE GOBERNANZA, MAPEO, METAS, MÉTRICAS

ASEGURAMIENTO DE OPTIMIZACIÓN DE RIESGOS

Dominio: Evaluación, Dirección, Monitoreo Objetivo de gestión: EDM03 — Aseguramiento de optimización de riesgos			
Descripción			
Asegurar de la orientación y tolerancia al riesgo de la empresa se entiendan, articulen y comuniquen, y que el riesgo para el valor de la empresa esté relacionado con la identificación y gestión el uso de TI.			
Propósito			
Asegurar de que el riesgo empresarial relacionado con TI no exceda la orientación al riesgo y la tolerancia al riesgo de la empresa, el impacto del riesgo de TI en el valor de la empresa es identificado, gestionado, y se minimiza el potencial de fallas en el cumplimiento.			
El objetivo de gestión respalda el logro de un conjunto de metas empresariales y de alineación principales:			
Metas empresariales		**Metas de alineamiento**	
• EG02 Riesgo empresarial gestionado • EG06 Continuidad y disponibilidad de servicios		• AG02 Riesgo relacionado con TI gestionado • AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones y privacidad	
Ejemplo de métricas para metas empresariales		**Ejemplo de métricas para metas de alineamiento**	
EG02	a. Porcentaje de objetivos y servicios comerciales críticos cubiertos por la evaluación de riesgos	AG02	a. Frecuencia de actualización del perfil de riesgo

	b. Reconocimiento de incidentes significativos que no fueron identificados en evaluaciones de riesgos vs. incidentes totales c. Frecuencia de actualización del perfil de riesgo		b. Porcentaje de evaluaciones de riesgos empresariales, incluidas las relacionadas con TI riesgo c. Número de incidentes significativos relacionados con TI que no fueron identificado en una evaluación de riesgos
EG06	a. Número de interrupciones de servicio al cliente o proceso comercial que causan incidentes significativos b. Coste empresarial de los incidentes c. Número de horas de procesamiento comercial perdidas debido a interrupciones del servicio no planificadas d. Porcentaje de quejas en función de los cometidos objetivos de disponibilidad del servicio	AG07	a. Número de interrupciones de incidentes de confidencialidad que causan pérdidas financieras o de aceptación b. Número de interrupciones de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o de aceptación C. Número de pérdidas de incidentes de integridad que causan pérdidas financieras o interrupción del negocio o aceptación.

Componente: Proceso		
Práctica de gestión	**Ejemplo de métrica**	
EDM03.01 Evaluar la gestión de riesgos. Examinar y evaluar continuamente el efecto del riesgo en el estado actual y uso futuro de I&T en la empresa. Considere si el riesgo de la empresa apetito es apropiado y asegurar que el riesgo para el valor de la empresa relacionado con se identifica y gestiona el uso de TI	a. Nivel de impacto empresarial inesperado b. Porcentaje de riesgo de TI que excede la tolerancia al riesgo empresarial c. Tasa de actualización de la evaluación de factores de riesgo	
Actividades		
1. Comprender la organización y su contexto relacionado con el riesgo de TI		2
2. Determinar la orientación de riesgo de la organización, es decir, el nivel de riesgo relacionado con TI que la empresa está dispuesta a asumir en su búsqueda de objetivos		
3. Determinar los niveles de tolerancia al riesgo frente a la orientación por el riesgo, es decir, desviaciones temporalmente aceptables de desviación por el riesgo.		
4. Determinar el grado de alineación de la estrategia de riesgo de TI con la estrategia de riesgo empresarial y asegurarse de que la orientación al riesgo esté por debajo la capacidad de riesgo de la organización.		

5. Evaluar proactivamente los factores de riesgo de TI antes de las decisiones empresariales estratégicas pendientes y garantizar que las consideraciones de riesgo forman parte del proceso de decisión empresarial estratégica.	3
6. Evaluar las actividades de gestión de riesgos para garantizar la alineación con la capacidad de la empresa para pérdidas relacionadas con TI, liderazgo y tolerancia de la misma.	
7. Atraer y mantener las habilidades y el personal necesarios para la gestión de riesgos de TI	

Práctica de gestión	**Ejemplo de métrica**
EDM03.02 Gestión directa de riesgos. Dirigir el establecimiento de prácticas de gestión de riesgos para proporcionar seguridad razonable de que las prácticas de gestión de riesgos de TI son apropiadas y que el riesgo real de TI no exceda el riesgo de la empresa.	a. Nivel de alineación entre el riesgo de TI y el riesgo empresarial b. Porcentaje de proyectos empresariales que consideran el riesgo de TI

Actividades	
1. Dirigir la traducción e integración de la estrategia de riesgo de TI en las prácticas de gestión de riesgos y actividades operativas.	2
2. Dirigir el desarrollo de planes de comunicación de riesgos (que cubran todos los niveles de la empresa).	
3. Dirigir la implementación de los mecanismos apropiados para responder rápidamente a los cambios en el riesgo e informar de inmediato a niveles apropiados de gestión, respaldados por principios acordados de escalamiento (qué informar, cuándo, dónde y cómo).	
4. Indicar que los riesgos, las oportunidades, los problemas y las inquietudes pueden ser identificados e informados por cualquier persona a la parte correspondiente en cualquier momento o tiempo. El riesgo debe gestionarse de acuerdo con las políticas y los procedimientos publicados y escalarse a la decisión pertinente	
5. Identificar los objetivos y métricas clave de los procesos de gobierno y gestión de riesgos a monitorear, y aprobar los enfoques, métodos, técnicas y procesos para capturar y reportar la información de medición.	3

Práctica de gestión	**Ejemplo de métrica**
EDM03.03 Supervisar la gestión de riesgos. Supervisar los objetivos y métricas clave de los procesos de gestión de riesgos. Determinar cómo las desviaciones o problemas serán identificados, rastreados y reportado para remediación.	a. Número de posibles áreas de riesgo de TI identificadas y gestionadas b. Porcentaje de riesgo crítico que ha sido efectivamente mitigado C. Porcentaje de planes de acción de riesgo de TI ejecutados a tiempo

Actividades

1. Informar cualquier problema de gestión de riesgos a la junta o al comité ejecutivo.	2
2. Supervisar hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de tolerancia y apetito de riesgo de la empresa.	3
3. Supervisar los objetivos y métricas clave de los procesos de gobierno y gestión de riesgos frente a los objetivos, analizar la causa de cualquier desviación e iniciar acciones correctivas para abordar las causas subyacentes.	4
4. Permitir que las partes interesadas clave revisen el progreso de la empresa hacia las metas identificadas.	

Práctica de gestión	**Ejemplo de métrica**							
Componente: Estructura organizacional								
Práctica de gestión	Junta	Comité Ejecutivo	Director ejecutivo	Director de riesgos	Director de información	Comité Gobierno de TI	Comité de Riesgo Empresarial	Director de seguridad de la información
EDM03.01 Evaluar la gestión de riesgos	A	R	R	R	R	R	R	
EDM03.02 Gestión directa de riesgos.	A	R	R	R	R	R	R	
EDM03.03 Supervisar la gestión de riesgos.	A	R	R	R	R	R	R	R

RELACIONES DE ADMINISTRACIÓN

Dominio: alineación, planificación y organización
Objetivo de gestión: APO08 — Relaciones de administración

Descripción

Gestionar las relaciones con las partes interesadas del hospital de manera formalizada y transparente que asegure la confianza mutua y un enfoque combinado en el logro los objetivos estratégicos dentro de las limitaciones de los presupuestos y la tolerancia al riesgo. Basar las relaciones en una comunicación abierta y transparente, un lenguaje y la voluntad de asumir la propiedad y la responsabilidad de las decisiones clave en ambos lados. El negocio y TI deben trabajar juntos para crear resultados empresariales exitosos en apoyo de los objetivos de la empresa.

Propósito

Habilitar el conocimiento, las habilidades y los comportamientos correctos para crear mejores resultados, mayor confianza, confianza mutua y uso efectivo de recursos. que estimulen una relación productiva con las partes interesadas del negocio.

El objetivo de gestión respalda el logro de un conjunto de metas empresariales y de alineación principales:

Metas empresariales	Metas de alineamiento
• EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad de procesos comerciales internos • EG10 Habilidades, motivación y productividad del personal • EG13 Innovación de productos y negocios	• AG05 Entrega de servicios de TI en línea con los requisitos del negocio • AG06 Agilidad para convertir los requisitos comerciales en soluciones operativas • AG12 Personal competente y motivado con comprensión mutua de tecnología y negocios • AG13 Conocimiento, experiencia e iniciativas para la innovación empresarial

Ejemplo de métricas para metas empresariales		Ejemplo de métricas para metas de alineamiento	
EG01	a. Porcentaje de productos y servicios que cumplen o superan objetivos en ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o superan objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan ventaja competitiva	AG05	a. Porcentaje de partes interesadas del negocio satisfechas con el servicio de TI la entrega cumple con los niveles de servicio acordados b. Número de interrupciones comerciales debido a incidentes en el servicio de TI

	d. Tiempo de comercialización de nuevos productos y servicios
EG08	a. Niveles de satisfacción del directorio y la gerencia ejecutiva con capacidades de proceso de negocio b. Niveles de satisfacción de los clientes con la prestación del servicio. C. Niveles de satisfacción de los proveedores con la cadena de suministro
EG010	a. Productividad del personal en comparación con los puntos de referencia b. Nivel de satisfacción de las partes interesadas con la experiencia del personal y habilidades C. Porcentaje de personal cuyas habilidades son insuficientes para competencia en su rol d. Porcentaje de personal satisfecho
EG013	a. Nivel de conocimiento y comprensión del negocio. oportunidades de innovación b. Satisfacción de las partes interesadas con los niveles de producto y experiencia e ideas de innovación c. Número de iniciativas de productos y servicios aprobadas resultado de ideas innovadoras

	c. Porcentaje de usuarios satisfechos con la calidad del servicio de TI entrega
AG06	a. Nivel de satisfacción de los ejecutivos TI capacidad de respuesta a los nuevos requisitos b. Tiempo medio de comercialización de nuevos servicios relacionados con TI y aplicaciones c. Tiempo promedio para convertir los objetivos estratégicos de TI en acuerdos e iniciativas aprobadas d. Número de procesos comerciales críticos respaldados por actualizaciones infraestructura y aplicaciones
AG012	a. Porcentaje de empresarios expertos en TI (es decir, aquellos que tienen el conocimiento y la comprensión necesarios de TI para guiar, dirigir, innovar y ver oportunidades de TI en su dominio de experiencia empresarial) b. Porcentaje de personas de TI con conocimientos de negocios (es decir, aquellos que tienen el conocimiento y la comprensión necesarios de los dominios comerciales para guiar, dirigir, innovar y ver TI oportunidades para el dominio empresarial) C. Número o porcentaje de empresarios con tecnología experiencia administrativa
AG013	a. Nivel de conocimiento y comprensión de los ejecutivos de negocios de las posibilidades de innovación de TI b. Número de iniciativas aprobadas resultantes de iniciativas innovadoras ideas de TI C. Número de campeones de la innovación reconocidos/premiados

Componente: Proceso		
Práctica de gestión	**Ejemplo de métrica**	
APO08.01 Comprender las expectativas comerciales. Comprender los problemas comerciales actuales, los objetivos y las expectativas de TI. Garantizar que los requisitos se comprendan, gestionen y comuniquen, y su estado acordado y aprobado.	a. Número de problemas comerciales actuales identificados b. Número de requisitos comerciales definidos para servicios habilitados por TI	
Actividades		
1. Identificar los stakeholders del negocio, sus intereses y sus áreas de responsabilidad.		2
2. Revisar la dirección actual de la empresa, los problemas, los objetivos estratégicos y la alineación con la arquitectura empresarial.		
3. Comprender el entorno empresarial actual, las limitaciones o problemas de los procesos, la expansión o contracción geográfica.		
4. Mantener un conocimiento de los procesos comerciales y actividades asociadas. Comprender los patrones de demanda que se relacionan con el servicio. volúmenes y uso.		
5. Gestionar las expectativas asegurándose de que las unidades de negocio comprendan las prioridades, las dependencias, las limitaciones financieras y la necesidad de programar solicitudes.		3
6. Aclarar las expectativas comerciales para los servicios y soluciones habilitados para TI. Asegúrese de que los requisitos estén definidos con los criterios y métricas de aceptación comercial.		4
7. Confirme que existe un acuerdo entre TI y todos los departamentos comerciales sobre las expectativas y cómo se medirán. Asegúrese de que este acuerdo sea confirmado por todas las partes interesadas.		
Práctica de gestión	**Ejemplo de métrica**	
APO08.02 Alinear la estrategia de TI con las expectativas comerciales e identificar oportunidades para que TI mejore el negocio. Alinear las estrategias TI con los objetivos y expectativas comerciales actuales para permitir que TI sea un socio de valor agregado para el negocio y un gobierno componente para mejorar el rendimiento empresarial.	a. Tasa de inclusión de oportunidades tecnológicas en las propuestas de inversión b. Encuesta a las partes interesadas empresariales sobre su nivel de conciencia tecnológico	
Actividades		
1. Posicionar a TI como socio del negocio. Desempeñar un papel proactivo en la identificación y comunicación con las partes interesadas clave en oportunidades, riesgos y limitaciones. Esto incluye tecnologías, servicios y modelos de procesos comerciales actuales y emergentes.		3
2. Colaborar en nuevas iniciativas importantes con la gestión de carteras, programas y proyectos. Garantizar la participación de TI. organización desde el comienzo de una nueva iniciativa al brindar asesoramiento y recomendaciones de valor agregado (desarrollo, definición de requisitos, diseño de soluciones) y asumiendo la propiedad de los flujos de trabajo de TI.		
Práctica de gestión	**Ejemplo de métrica**	

APO08.03 Gestionar la relación comercial. Gestionar la relación entre la organización de servicios de TI y sus compañeros de negocio. Asegúrese de que los roles y las responsabilidades de la relación sean definido y asignado, y se facilita la comunicación.	a. Calificaciones de encuestas de satisfacción de usuarios y personal de TI b. Porcentaje de roles y responsabilidades de relación definidos, asignados, y comunicados	
Actividades		
1. Asigne un gerente de relaciones como único punto de contacto para cada unidad de negocios importante. Asegúrese de que una sola contraparte está identificada en la organización empresarial y la contraparte tiene comprensión empresarial, conocimiento tecnológico suficiente y el nivel apropiado de autoridad.		3
2. Gestionar la relación de manera formalizada y transparente que asegure un enfoque en el logro de un objetivo común y compartido de resultados empresariales exitosos en apoyo de los objetivos estratégicos y dentro de las limitaciones de los presupuestos y la tolerancia al riesgo.		
3. Definir y comunicar un procedimiento de quejas y escalamiento para resolver cualquier problema de relación.		
4. Asegurarse de que las partes interesadas responsables relevantes acuerden y aprueben las decisiones		
5. Planificar interacciones y cronogramas específicos basados en objetivos mutuamente acordados y lenguaje común (servicio y desempeño). reuniones de revisión, revisión de nuevas estrategias o planes, etc.).		4
Práctica de gestión	**Ejemplo de métrica**	
APO08.04 Coordinar y comunicar. Trabajar con todas las partes interesadas relevantes y coordinar el proceso de principio a fin entrega de servicios y soluciones de TI proporcionados al negocio.	a. Tiempo desde la última actualización del plan de comunicación de extremo a extremo para el negocio b. Porcentaje de satisfacción de los dueños de negocios con la coordinación del fin de entrega final de servicios y soluciones de TI	
Actividades		
1. Coordinar y comunicar los cambios y las actividades de transición, como planes de proyectos o cambios, cronogramas, políticas de lanzamiento, liberación de errores conocidos y formación de conciencia.		2
2. Coordinar y comunicar actividades operativas, roles y responsabilidades, incluida la definición de tipos de solicitudes, escalamiento jerárquico, interrupciones importantes (planificadas y no planificadas) y contenido y frecuencia de los informes de servicio.		
3. Apropiarse de la respuesta al negocio ante eventos importantes que puedan influir en la relación con el negocio. Proporcionar apoyo directo si es necesario.		
4. Mantener un plan de comunicación de extremo a extremo que defina el contenido, la frecuencia y los destinatarios de la información de prestación de servicios, incluyendo el estado del valor entregado y cualquier riesgo identificado.		3
Práctica de gestión	**Ejemplo de métrica**	
APO08.5 Proporcionar información para la mejora continua de los servicios. Mejorar y evolucionar continuamente los servicios habilitados para TI y la	a. Porcentaje de alineación de los servicios de TI con los requerimientos de negocio empresarial	

prestación de servicios a la empresa para alinearse con los objetivos de la empresa y tecnología	b. Porcentaje de causas raíz identificadas y resueltas para cualquier problema

Actividades	
1. Realizar análisis de satisfacción de clientes y proveedores. Asegurarse de que se aborden los problemas; informe de resultados y estado	4
2. Trabajar juntos para identificar, comunicar e implementar iniciativas de mejora.	5
3. Trabajar con la gestión de servicios y los propietarios de procesos para garantizar que los servicios habilitados para TI y los procesos de gestión de servicios se mejoran continuamente y se identifican y resuelvan las causas raíz de cualquier problema.	

Componente: Estructura organizacional																
Práctica de gestión	Director ejecutivo	Director financiero	Director de operaciones	Director de información	Jefe de Tecnología	Director de operaciones digitales	Junta de Gobierno de I&T	Propietarios de procesos de negocio	Gerente de Relaciones	Jefe de ejecución	jefe de desarrollo	Jefe de operaciones de TI	Supervisor	Gerente de Seguridad de la Información	Gerente de Continuidad de Negocios	Oficial de Privacidad
APO08.01 Comprender las expectativas comerciales				A	R	R		R	R		R	R	R	R	R	R
APO08.02 Alinear la estrategia de I&T con las expectativas comerciales e identificar oportunidades para que TI mejorar el negocio.				A	R	R	R	R	R	R	R	R	R			
APO08.03 Gestionar la relación comercial.	R	R	R	A	R	R		R	R		R	R	R			
APO08.04 Coordinar y comunicar.	R	R	R	A	R	R		R	R		R	R	R			
APO08.05 Proporcionar información para la mejora continua de los servicios				A	R	R		R	R		R	R	R			

GESTIÓN DE RIESGO

Dominio: alineación, planificación y organización Objetivo de gestión: APO08 — Gestión de riesgo	
Descripción	
Identifique, evalúe y reduzca continuamente el riesgo relacionado con TI dentro de los niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.	
Propósito	
Integre la gestión del riesgo empresarial relacionado con la TI con la gestión general del riesgo empresarial (ERM) y equilibre los costos y beneficios de la gestión del riesgo empresarial relacionado con la TI.	
El objetivo de gestión respalda el logro de un conjunto de metas empresariales y de alineación principales:	
Metas empresariales	**Metas de alineamiento**
• EG02 Riesgo empresarial gestionado • EG06 Continuidad y disponibilidad del servicio comercial	• AG02 Riesgo relacionado con I&T gestionado • AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones y privacidad
Ejemplo de métricas para metas empresariales	**Ejemplo de métricas para metas de alineamiento**
EG02 — a. Porcentaje de objetivos y servicios comerciales críticos cubiertos por la evaluación de riesgos b. Ratio de incidentes significativos que no fueron identificados en evaluaciones de riesgos vs. incidentes totales C. Frecuencia de actualización del perfil de riesgo	AG02 — a. Frecuencia de actualización del perfil de riesgo b. Porcentaje de evaluaciones de riesgos empresariales que incluyen riesgo relacionado con TI C. Número de incidentes significativos relacionados con TI que no fueron identificado en una evaluación de riesgos
EG06 — a. Número de servicio al cliente o proceso comercial interrupciones que causan incidentes significativos b. Coste empresarial de los incidentes C. Número de horas de procesamiento comercial perdidas debido a interrupciones del servicio no planificadas d. Porcentaje de quejas en función de los cometidos objetivos de disponibilidad del servicio	AG07 — a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o vergüenza pública b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o vergüenza pública C. Número de incidentes de integridad que causan

		pérdidas financieras, interrupción del negocio o vergüenza pública

Componente: Proceso		
Práctica de gestión	**Ejemplo de métrica**	
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para permitir un riesgo efectivo relacionado con TI. Identificación, análisis e informes.	a. Número de eventos de pérdida con características clave capturados en repositorios. b. Porcentaje de auditorías, eventos y tendencias capturados en repositorios. C. Porcentaje de sistemas críticos con problemas conocidos.	
Actividades		
1. Establecer y mantener un método para la recopilación, clasificación y análisis de datos relacionados con el riesgo de TI.		2
2. Registrar datos relevantes y significativos relacionados con el riesgo de TI en el entorno operativo interno y externo de la empresa.		
3. Adoptar o definir una taxonomía de riesgo para definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad.		3
4. Registrar datos sobre eventos de riesgo que hayan causado o puedan causar impactos en el negocio según las categorías de impacto definidas en la taxonomía de riesgos. Capture datos relevantes de asuntos relacionados, incidentes, problemas e investigaciones.		
5. Inspeccionar y analizar los datos históricos de riesgo de TI y la experiencia de pérdidas a partir de datos y tendencias disponibles externamente, pares de la industria a través de registros de eventos basados en la industria, bases de datos y acuerdos de la industria para la divulgación de eventos comunes.		4
6. Para clases de eventos similares, organice los datos recopilados y destaque los factores contribuyentes. Determinar la contribución común factores a través de múltiples eventos.		
7. Determinar las condiciones específicas que existían o estaban ausentes cuando ocurrieron los eventos de riesgo y la forma en que las condiciones afectaron frecuencia del evento y magnitud de la pérdida.		
8. Realizar análisis periódicos de eventos y factores de riesgo para identificar problemas de riesgo nuevos o emergentes y para obtener una comprensión de los factores de riesgo internos y externos asociados.		
Práctica de gestión	**Ejemplo de métrica**	
APO12.02 Analizar el riesgo. Desarrollar una visión fundamentada sobre el riesgo real de I&T, en apoyo de las decisiones de riesgo	a. Número de escenarios de riesgo de TI identificados b. Tiempo desde la última actualización de los escenarios de riesgo de TI	
Actividades		
1. Definir el alcance apropiado de los esfuerzos de análisis de riesgo, considerando todos los factores de riesgo y/o la criticidad comercial de los activos.		3

2. Construir y actualizar regularmente escenarios de riesgo de TI; exposiciones a pérdidas relacionadas con TI; y escenarios de riesgo reputacional, incluyendo escenarios compuestos de tipos y eventos de amenazas en cascada y/o coincidentes. Desarrollar expectativas para un control específico. Actividades y capacidades para detectar.	
3. Estimar la frecuencia (o probabilidad) y la magnitud de la pérdida o ganancia asociada con los escenarios de riesgo de TI. tener en cuenta todo factor de riesgo aplicables y evaluar los controles operativos conocidos.	
4. Comparar el riesgo actual (exposición a pérdidas relacionadas con TI) con el apetito por el riesgo y la tolerancia al riesgo aceptable. Identificar inaceptable o riesgo elevado.	
5. Proponer respuestas de riesgo para el riesgo que exceda los niveles de apetito y tolerancia al riesgo.	
6. Especificar requisitos de alto nivel para proyectos o programas que implementarán las respuestas de riesgo seleccionadas. Identificar requisitos y expectativas de controles clave apropiados para las respuestas de mitigación de riesgos.	
7. Validar los resultados del análisis de riesgos y del análisis de impacto en el negocio (BIA) antes de utilizarlos en la toma de decisiones. Confirme que el análisis se alinea con los requisitos de la empresa y verifica que las estimaciones se calibraron correctamente y se examinaron en busca de sesgos.	4
8. Analizar el costo/beneficio de las posibles opciones de respuesta al riesgo, como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/aprovechar. Confirmar la respuesta óptima al riesgo.	5

Práctica de gestión	**Ejemplo de métrica**
APO12.03 Mantener un perfil de riesgo. Mantener un inventario de riesgos conocidos y atributos de riesgo, incluidos frecuencia esperada, impacto potencial y respuestas. Documento relacionado recursos, capacidades y actividades de control vigentes relacionadas con los elementos de riesgo.	a. Completitud de atributos y valores en el perfil de riesgo b. Porcentaje de procesos comerciales clave incluidos en el perfil de riesgo
Actividades	
1. Inventariar los procesos comerciales y documentar su dependencia de los procesos de gestión de servicios de I&T y la infraestructura de TI recursos. Identificar personal de apoyo, aplicaciones, infraestructura, instalaciones, registros manuales críticos, proveedores, proveedores y subcontratistas	2
2. Determinar y acordar qué servicios de I&T y recursos de infraestructura de TI son esenciales para sostener la operación del negocio de procesos. Analice las dependencias e identifique los vínculos débiles.	
3. Agregar los escenarios de riesgo actuales por categoría, línea de negocio y área funcional.	
4. Capturar regularmente toda la información del perfil de riesgo y consolidarla en un perfil de riesgo agregado.	3

5. Capturar información sobre el estado del plan de acción de riesgo para su inclusión en el perfil de riesgo de TI de la empresa.	
6. Con base en todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación y el seguimiento rápidos del riesgo actual y tendencias de riesgo.	4
7. Capturar información sobre eventos de riesgo de TI que se han materializado para su inclusión en el perfil de riesgo de TI de la empresa.	

Práctica de gestión	**Ejemplo de métrica**
APO12.04 Riesgo articulado. Comunicar información sobre el estado actual de las exposiciones relacionadas con TI y oportunidades de manera oportuna a todas las partes interesadas requeridas para respuesta apropiada.	a. Nivel de satisfacción de las partes interesadas con los informes de riesgo proporcionados b. Integridad de los informes de perfil de riesgo (incluida la información en línea con los requisitos de las partes interesadas) C. Uso de informes de riesgo en la toma de decisiones de gestión

Actividades	
1. Informar los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para respaldar las decisiones empresariales. Siempre que sea posible, incluya probabilidades y rangos de pérdida o ganancia junto con niveles de confianza, para permitir que la gerencia equilibrio riesgo-rentabilidad.	3
2. Proporcionar a los tomadores de decisiones una comprensión de los escenarios más probables y peores, las exposiciones a pérdidas relacionadas con TI y reputación significativa, consideraciones legales y regulatorias, o cualquier otra categoría de impacto según la taxonomía de riesgo.	
3. Informar el perfil de riesgo actual a todas las partes interesadas. Incluir información sobre la eficacia del proceso de gestión de riesgos, eficacia del control, brechas, inconsistencias, redundancias, estado de remediación y sus impactos en el perfil de riesgo.	
4. Periódicamente, para áreas con riesgo relativo y paridad de capacidad de riesgo, identificar oportunidades relacionadas con TI que permitirían la aceptación de un mayor riesgo y mayor crecimiento y rentabilidad.	
5. Revisar los resultados de las evaluaciones objetivas de terceros y las revisiones de control de calidad y auditoría interna. Incluirlos en el perfil de riesgo. Revise las brechas identificadas y las exposiciones a pérdidas relacionadas con TI para determinar la necesidad de un análisis de riesgo adicional.	4

Práctica de gestión	**Ejemplo de métrica**
APO12.05 Definir una cartera de acciones de gestión de riesgos. Gestionar oportunidades para reducir el riesgo a un nivel aceptable como cartera.	a. Número de incidentes significativos no identificados e incluidos en el riesgo cartera de gestión b. Porcentaje de propuestas de proyectos de gestión de riesgos rechazadas debido a la falta de consideración de otros riesgos relacionados

Actividades

1. Mantener un inventario de las actividades de control que existen para mitigar el riesgo y que permiten tomar el riesgo en línea con el riesgo apetito y tolerancia. Clasificar las actividades de control y asignarlas a escenarios de riesgo de TI específicos y agregaciones de riesgo de TI escenarios.	2
2. Determinar si cada entidad organizacional monitorea el riesgo y acepta la responsabilidad por operar dentro de sus niveles de tolerancia de la cartera.	
3. Definir un conjunto equilibrado de propuestas de proyectos diseñadas para reducir el riesgo y/o proyectos que permitan empresas estratégicas oportunidades, considerando costos, beneficios, efecto en el perfil de riesgo actual y normativa.	3
Práctica de gestión	**Ejemplo de métrica**
APO12.06 Responder al riesgo. Responder en tiempo y forma a los eventos de riesgo materializados con medidas para limitar la magnitud de la pérdida.	a. Número de incidentes significativos no identificados e incluidos en el riesgo cartera de gestión b. Porcentaje de propuestas de proyectos de gestión de riesgos rechazadas debido a la falta de consideración de otros riesgos relacionados
Actividades	
1. Preparar, mantener y probar planes que documenten los pasos específicos a seguir cuando un evento de riesgo puede causar un impacto operativo significativo o incidente de desarrollo con un impacto comercial grave. Asegúrese de que los planes incluyan vías de escalamiento en toda la empresa.	2
2. Aplicar el plan de respuesta adecuado para minimizar el impacto cuando se produzcan incidentes de riesgo.	
3. Definir un conjunto equilibrado de propuestas de proyectos diseñadas para reducir el riesgo y/o proyectos que permitan empresas estratégicas oportunidades, considerando costos, beneficios, efecto en el perfil de riesgo actual y normativa.	3
4. Examinar eventos adversos/pérdidas pasadas y oportunidades perdidas y determinar las causas fundamentales.	
5. Comunicar la causa raíz, los requisitos adicionales de respuesta al riesgo y las mejoras del proceso a los responsables de la toma de decisiones. Asegúrese de que la causa, los requisitos de respuesta y la mejora del proceso estén incluidos en los procesos de gobierno del riesgo.	4
Componente: Estructura organizacional	

Práctica de gestión	Director de riesgos	Director de información	Jefe de Tecnología	director de operaciones digitales	Comité de Riesgo Empresarial	Director de seguridad de la información	Propietarios de procesos de negocio	Propietarios de procesos de negocio	Función de gestión de datos	Arquitecto Jefe	Desarrollo de la cabeza	Jefe de operaciones de TI	Jefe de administración de TI	Supervisor	Gerente de Seguridad de la Información	Gerente de Continuidad de Negocios	Oficial de Privacidad
APO12.01 Recopilar datos.	A	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
APO12.02 Analizar el riesgo.	A	R			R		R										
APO12.03 Mantener un perfil de riesgo.	A	R			R		R										
APO12.04 Riesgo articulado.	A	R			R		R										
APO12.05 Definir una cartera de acciones de gestión de riesgos.	A	R			R		R										
APO12.06 Responder al riesgo	R	A	R	R		R	R	R		R	R	R	R	R	R	R	R

GESTIÓN DE SEGURIDAD

Dominio: alineación, planificación y organización Objetivo de gestión: APO13 – Gestión de seguridad	
Descripción	
Definir, operar y monitorear un sistema de gestión de seguridad de la información	
Propósito	
Mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito por el riesgo de la empresa.	
El objetivo de gestión respalda el logro de un conjunto de metas empresariales y de alineación principales:	
Metas empresariales	**Metas de alineamiento**
• EG02 Riesgo empresarial gestionado • EG06 Continuidad y disponibilidad del servicio comercial	• AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones y privacidad
Ejemplo de métricas para metas empresariales	**Ejemplo de métricas para metas de alineamiento**
EG02 — a. Porcentaje de objetivos y servicios comerciales críticos cubiertos por la evaluación de riesgos b. Ratio de incidentes significativos que no fueron identificados en evaluaciones de riesgos vs. incidentes totales C. Frecuencia de actualización del perfil de riesgo	AG07 — a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o vergüenza pública b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o vergüenza pública C. Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o vergüenza pública
EG06 — a. Número de servicio al cliente o proceso comercial interrupciones que causan incidentes significativos b. Coste empresarial de los incidentes C. Número de horas de procesamiento comercial perdidas debido a interrupciones del servicio no planificadas d. Porcentaje de quejas en función de los cometidos objetivos de disponibilidad del servicio	
Componente: Proceso	

Práctica de gestión	Ejemplo de métrica
APO13.01 Establecer y mantener una gestión de seguridad de la información(SGSI). Establecer y mantener un sistema de gestión de la seguridad de la información. (SGSI) que proporciona un enfoque estándar, formal y continuo para gestión de la seguridad de la información, que permite la tecnología segura y procesos de negocio que están alineados con los requisitos del negocio.	a. Nivel de satisfacción de las partes interesadas con el plan de seguridad a lo largo del empresa

Actividades	
1. Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, la organización, su ubicación, activos y tecnología. Incluya detalles y justificación de cualquier exclusión del alcance.	2
2. Definir un SGSI de acuerdo con la política empresarial y el contexto en el que opera la empresa.	
3. Alinear el SGSI con el enfoque empresarial general para la gestión de la seguridad.	
4. Obtener autorización de la gerencia para implementar y operar o cambiar el SGSI.	
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.	
6. Definir y comunicar las funciones y responsabilidades de gestión de la seguridad de la información.	
7. Comunicar el enfoque SGSI.	

Práctica de gestión	Ejemplo de métrica
APO13.02 Definir y gestionar un riesgo de seguridad y privacidad de la información plan de tratamiento. Mantener un plan de seguridad de la información que describa cómo la información el riesgo de seguridad debe gestionarse y alinearse con la estrategia empresarial y arquitectura empresarial. Asegúrese de que las recomendaciones para implementar las mejoras de seguridad se basan en casos comerciales aprobados, implementado como parte integral del desarrollo de servicios y soluciones y operado como una parte integral de la operación comercial.	a. Porcentaje de simulaciones exitosas de escenarios de riesgo de seguridad b. Número de empleados que han completado correctamente la información entrenamiento de concientización de seguridad

Actividades	
1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la empresa arquitectura. Asegúrese de que el plan identifique las prácticas de gestión y las soluciones de seguridad adecuadas y óptimas, con recursos asociados, responsabilidades y prioridades para gestionar el riesgo de seguridad de la información identificado.	3

2. Mantener como parte de la arquitectura de la empresa un inventario de los componentes de la solución que están implementados para administrar los servicios relacionados con la seguridad riesgo.	
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, respaldadas por casos de negocios adecuados que incluyan consideración de la financiación y la asignación de funciones y responsabilidades.	
4. Proporcionar insumos para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas de la seguridad de la información. plan de tratamiento de riesgos.	
5. Implementar programas de capacitación y concientización sobre seguridad y privacidad de la información.	
6. Integrar la planificación, diseño, implementación y seguimiento de los procedimientos de seguridad y privacidad de la información y otros controles capaces de permitir la pronta prevención, detección de eventos de seguridad y respuesta a incidentes de seguridad.	
7. Definir cómo medir la efectividad de las prácticas de gestión seleccionadas. Especificar cómo estas medidas deben ser se utiliza para evaluar la eficacia para producir resultados comparables y reproducibles.	4

Práctica de gestión	**Ejemplo de métrica**
APO13.03 Supervisar y revisar la gestión de la seguridad de la información (SGSI). Mantener y comunicar periódicamente la necesidad y los beneficios de mejora continua en la seguridad de la información. Recoger y analizar datos sobre el sistema de gestión de seguridad de la información (SGSI), y mejorar su eficacia. Corregir las no conformidades para evitar que se repitan.	a. Frecuencia de las revisiones de seguridad programadas b. Número de hallazgos en revisiones de seguridad programadas regularmente C. Nivel de satisfacción de las partes interesadas con el plan de seguridad d. Número de incidentes relacionados con la seguridad causados por el incumplimiento del plan de seguridad
Actividades	
1. Realizar revisiones periódicas de la eficacia del SGSI. Incluir el cumplimiento de la política y los objetivos del SGSI y la revisión de la seguridad y prácticas de privacidad.	4
2. Realizar auditorías del SGSI a intervalos planificados.	
3. Llevar a cabo una revisión de gestión del SGSI de forma periódica para garantizar que el alcance siga siendo adecuado y las mejoras en el proceso ISMS son identificados.	
4. Registrar acciones y eventos que podrían tener un impacto en la efectividad o desempeño del SGSI.	
5. Proporcionar información para el mantenimiento de los planes de seguridad para tener en cuenta los resultados de las actividades de seguimiento y revisión.	5
Componente: Estructura organizacional	

Práctica de gestión	Director de información	Jefe de Tecnología	Comité de Riesgo Empresarial	Director de seguridad de la información	Propietarios de procesos de negocio	Oficina de Gestión de Proyectos	Arquitecto jefe	Desarrollo de la cabeza	Jefe de operaciones de TI	Jefe de administración de TI	Supervisor	Gerente de Seguridad de la Información	Gerente de Continuidad de Negocios	Oficial de Privacidad
APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	R		R	A						R		R		
APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad y privacidad de la información.	R		R	A						R		R		R
APO13.03 Supervisar y revisar el sistema de gestión de seguridad de la información (SGSI).	R	R		A	R	R	R	R	R	R	R	R	R	R

GESTIÓN EN CAMBIOS DE TI

Dominio: Construir, adquirir e implementar Objetivo de gestión: BAI06 — Gestión en Cambios de TI			
Descripción			
Administre todos los cambios de manera controlada, incluidos los cambios estándar y el mantenimiento de emergencia relacionados con los procesos comerciales, las aplicaciones e infraestructura Esto incluye estándares y procedimientos de cambio, evaluación de impacto, priorización y autorización, cambios de emergencia, seguimiento, informes, cierre y documentación.			
Propósito			
Habilite la entrega rápida y confiable de cambios a la empresa. Mitigar el riesgo de impactar negativamente en la estabilidad o integridad del entorno modificado.			
El objetivo de gestión respalda el logro de un conjunto de metas empresariales y de alineación principales:			
Metas empresariales		**Metas de alineamiento**	
EG01 Portafolio de productos y servicios competitivos		AG06 Agilidad para convertir los requisitos comerciales en soluciones operativas	
Ejemplo de métricas para metas empresariales		**Ejemplo de métricas para metas de alineamiento**	
EG01	a. Porcentaje de productos y servicios que cumplen o superan objetivos en ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o superan objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan ventaja competitiva	AG06	a. Nivel de satisfacción de los ejecutivos de empresas con TI capacidad de respuesta a los nuevos requisitos b. Tiempo medio de comercialización de nuevos servicios relacionados con TI y aplicaciones

	d. Tiempo de comercialización de nuevos productos y servicios		C. Tiempo promedio para convertir los objetivos estratégicos de TI en acuerdos e iniciativas aprobadas d. Número de procesos comerciales críticos respaldados por actualizaciones infraestructura y aplicaciones
Componente: Proceso			
Práctica de gestión		**Ejemplo de métrica**	
BAI06.01 Evaluar, priorizar y autorizar solicitudes de cambio. Evaluar todas las solicitudes de cambio para determinar el impacto en el negocio procesos y servicios de I&T, y para evaluar si el cambio afectará negativamente afectar el entorno operativo e introducir un riesgo inaceptable. Asegúrese de que los cambios se registren, prioricen, categoricen, evalúen, autorizado, planificado y programado.		a. Cantidad de reelaboración causada por cambios fallidos b. Porcentaje de cambios fallidos debido a un impacto inadecuado evaluaciones	
Actividades			
1. Utilice solicitudes de cambio formales para permitir que los propietarios de procesos comerciales y TI soliciten cambios en los procesos comerciales, la infraestructura y los cambios, sistemas o aplicaciones. Asegúrese de que todos esos cambios surjan solo a través del proceso de gestión de solicitudes de cambio.			
2. Categorizar todos los cambios solicitados (p. ej., procesos comerciales, infraestructura, sistemas operativos, redes, sistemas de aplicación, software de aplicación comprado/empaquetado) y relacione los elementos de configuración afectados.			
3. Priorizar todos los cambios solicitados en función de los requisitos comerciales y técnicos; recursos requeridos; y el marco legal, reglamentario y motivos contractuales del cambio solicitado.			2
4. Aprobar formalmente cada cambio por parte de los propietarios de los procesos comerciales, los administradores de servicios y las partes interesadas técnicas de TI, según corresponda. Los cambios que son de bajo riesgo y relativamente frecuentes deben aprobarse previamente como cambios estándar.			
5. Planificar y programar todos los cambios aprobados.			
6. Planificar y evaluar todas las solicitudes de manera estructurada. Incluir un análisis de impacto en el proceso de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad comercial (BCP) y proveedores de servicios para garantizar que todos los componentes afectados hayan sido identificado. Evaluar la probabilidad de afectar negativamente el entorno operativo y el riesgo de implementar el cambio. Considere las implicaciones de seguridad, privacidad, legales, contractuales y de cumplimiento del cambio solicitado. Considere también las interdependencias entre cambios. Involucrar a los propietarios de los procesos de negocio en el proceso de evaluación, según corresponda.			3

7. Considere el impacto de los proveedores de servicios contratados (por ejemplo, de procesamiento comercial, infraestructura, aplicación desarrollo y servicios compartidos) en el proceso de gestión del cambio. Incluir la integración de la gestión del cambio organizacional procesos con los procesos de gestión de cambios de los proveedores de servicios y el impacto en los términos contractuales y SLA.	
Práctica de gestión	**Ejemplo de métrica**
BAI06.02 Gestionar cambios de emergencia. Administre cuidadosamente los cambios de emergencia para minimizar más incidentes. Asegúrese de que el cambio de emergencia esté controlado y se lleve a cabo de forma segura. Verificar que los cambios de emergencia se evalúen adecuadamente y autorizado después del cambio.	a. Número de cambios de emergencia no autorizados tras el incidente b. Porcentaje del total de cambios que son arreglos de emergencia
Actividades	
1. Definir lo que constituye un cambio de emergencia	2
2. Asegurar que exista un procedimiento documentado para declarar, evaluar, aprobar preliminarmente, autorizar después del cambio y registrar un cambio de emergencia.	
3. Verificar que todos los arreglos de acceso de emergencia para cambios estén debidamente autorizados, documentados y revocados después de la se ha aplicado el cambio.	3
4. Supervisar todos los cambios de emergencia y realizar revisiones posteriores a la implementación que involucren a todas las partes interesadas. La revisión debe considerar e iniciar acciones correctivas basadas en causas raíz, como problemas con el proceso comercial, el sistema de aplicación desarrollo y mantenimiento, entornos de desarrollo y prueba, documentación y manuales, e integridad de datos.	4
Práctica de gestión	**Ejemplo de métrica**
BAI06.03 Seguimiento e informe de estado de cambio. Mantener un sistema de seguimiento y generación de informes para documentar los cambios rechazados y comunicar el estado de aprobado, en proceso y completos cambios. Asegúrese de que los cambios aprobados se implementen como planificado.	a. Número y antigüedad de las solicitudes de cambio pendientes b. Porcentaje del estado de la solicitud de cambio informado a las partes interesadas en una manera oportuna
Actividades	
1. Categorizar las solicitudes de cambio en el proceso de seguimiento (p. ej., rechazadas, aprobadas, pero aún no iniciadas, aprobadas y en proceso, y cierre).	4

2. Implementar informes de estado de cambios con métricas de desempeño para permitir la revisión y el monitoreo de la administración tanto de los detalles el estado de los cambios y el estado general (p. ej., análisis antiguo de las solicitudes de cambio). Asegúrese de que los informes de estado formen un registro de auditoría por lo que los cambios se pueden rastrear posteriormente desde el inicio hasta la disposición final.	
3. Supervise los cambios abiertos para garantizar que todos los cambios aprobados se cierren de manera oportuna, según la prioridad.	
4. Mantener un sistema de seguimiento y generación de informes para todas las solicitudes de cambio.	
Práctica de gestión	**Ejemplo de métrica**
BAI06.04 Cerrar y documentar los cambios. Cada vez que se implementen cambios, actualice la solución, el usuario documentación y procedimientos afectados por el cambio.	a. Número de errores de revisión encontrados en la documentación b. Porcentaje de actualizaciones de procedimientos y documentación del usuario realizadas en de manera oportuna
Actividades	
1. Incluir cambios en la documentación dentro del procedimiento de gestión. Ejemplos de documentación incluyen negocios y Procedimientos operativos de TI, continuidad del negocio y documentación de recuperación ante desastres, información de configuración, aplicación documentación, pantallas de ayuda y materiales de formación.	2
2. Definir un período de retención adecuado para la documentación de cambios y la documentación del usuario y del sistema anterior y posterior al cambio.	3
3. Someter la documentación al mismo nivel de revisión que el cambio real	
Componente: Estructura organizacional	

Práctica de gestión	Director de información	Propietarios de procesos de negocio	Director del programa	Gerente de proyecto	Líder de desarrollo	Jefe de operaciones de TI	Supervisor	Gerente de Seguridad de la Información	Gerente de Continuidad de Negocios	Oficial de Privacidad
BAI06.01 Evaluar, priorizar y autorizar solicitudes de cambio.	A	R			R	R	R	R	R	R
BAI06.02 Gestionar cambios de emergencia.	A				R	R	R	R		R
BAI06.03 Seguimiento e informe de estado de cambio.	A	R	R	R	R	R	R			
BAI06.04 Cerrar y documentar los cambios.	A	R	R	R	R	R	R		R	

SOLICITUDES E INCIDENTES DE SERVICIOS GESTIONADOS

Dominio: entrega, servicio y soporte Objetivo de gestión: DSS02 — Solicitudes e incidentes de servicios gestionados
Descripción
Dar respuesta oportuna y eficaz a las solicitudes de los usuarios y resolución de todo tipo de incidencias. Restaurar el servicio normal; registrar y cumplir con el usuario peticiones; registrar, investigar, diagnosticar, escalar y resolver incidentes.
Propósito
Lograr una mayor productividad y minimizar las interrupciones mediante la resolución rápida de consultas e incidentes de los usuarios. Evaluar el impacto de los cambios y hacer frente a las incidencias del servicio. Resolver solicitudes de usuarios y restaurar el servicio en respuesta a incidentes.
El objetivo de gestión respalda el logro de un conjunto de metas empresariales y de alineación principales:

Metas empresariales	**Metas de alineamiento**
• EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad de procesos comerciales internos	AG05 Entrega de servicios de TI en línea con los requerimientos del negocio

Ejemplo de métricas para metas empresariales		**Ejemplo de métricas para metas de alineamiento**	
EG01	a. Porcentaje de productos y servicios que cumplen o superan objetivos en ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o superan objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan ventaja competitiva	AG05	a. Porcentaje de partes interesadas del negocio satisfechas con el servicio de TI la entrega cumple con los niveles de servicio acordados b. Número de interrupciones comerciales debido a incidentes en el servicio de TI

	d. Tiempo de comercialización de nuevos productos y servicios	c. Porcentaje de usuarios satisfechos con la calidad del servicio de TI entrega
EG08	a. Niveles de satisfacción del directorio y la gerencia ejecutiva con capacidades de proceso de negocio b. Niveles de satisfacción de los clientes con la prestación del servicio. C. Niveles de satisfacción de los proveedores con la cadena de suministro	

Componente: Proceso	
Práctica de gestión	**Ejemplo de métrica**
DSS02.01 Definir esquemas de clasificación para incidentes y solicitudes de servicio. Definir esquemas de clasificación y modelos para incidentes y solicitudes de servicio.	a. Número total de solicitudes de servicio e incidentes por nivel de prioridad b. Número total de incidentes escalados
Actividades	
1. Definir esquemas de clasificación y priorización de incidentes y solicitudes de servicio, y criterios para el registro de problemas. Utilizar esta información para asegurar enfoques consistentes para manejar e informar a los usuarios sobre problemas y realizar análisis de tendencias.	3
2. Definir modelos de incidentes para errores conocidos para permitir una resolución eficiente y efectiva.	
3. Defina modelos de solicitud de servicio según el tipo de solicitud de servicio para habilitar la autoayuda y un servicio eficiente para solicitudes estándar.	
4. Definir reglas y procedimientos de escalada de incidentes, especialmente para incidentes importantes e incidentes de seguridad.	
5. Definir fuentes de conocimiento sobre incidentes y solicitudes y describir cómo utilizarlas.	
Práctica de gestión	**Ejemplo de métrica**
DSS02.02 Registrar, clasificar y priorizar solicitudes e incidencias. Identificar, registrar y clasificar las solicitudes de servicio e incidencias y	a. Número de tipos y categorías definidas para el registro de solicitudes de servicio e incidentes

asignar una prioridad de acuerdo a la criticidad del negocio y acuerdos de servicio.	b. Número de solicitudes de servicio e incidentes que no están categorizados	
Actividades		
1. Registrar todas las solicitudes de servicio e incidentes, registrando toda la información relevante, para que puedan ser manejados de manera efectiva y un historial completo se puede mantener el registro.		2
2. Para habilitar el análisis de tendencias, clasifique las solicitudes de servicio y los incidentes identificando el tipo y la categoría.		
3. Priorizar las solicitudes de servicio y los incidentes en función de la definición de servicio SLA de impacto comercial y urgencia.		
Práctica de gestión	**Ejemplo de métrica**	
DSS02.03 Verificar, aprobar y cumplir con las solicitudes de servicio. Seleccione los procedimientos de solicitud apropiados y verifique que el servicio y las solicitudes cumplen los criterios de solicitud definidos. Obtener la aprobación, si es necesario, y cumplir con las solicitudes.	a. Tiempo medio transcurrido para atender cada tipo de solicitud de servicio b. Porcentaje de solicitudes de servicio que cumplen con los criterios de solicitud definidos	
Actividades		
1. Verificar el derecho a las solicitudes de servicio, cuando sea posible, un flujo de proceso predefinido y cambios estándar.		2
2. Obtener aprobación o aprobación financiera y funcional, si es necesario, o aprobaciones predefinidas para cambios estándar acordados.		
3. Cumplir con las solicitudes realizando el procedimiento de solicitud seleccionado. Siempre que sea posible, utilice menús automatizados de autoayuda y modelos de solicitud predefinidos para artículos solicitados con frecuencia.		3
Práctica de gestión	**Ejemplo de métrica**	
DSS02.04 Investigar, diagnosticar y asignar incidentes. Identificar y registrar los síntomas del incidente, determinar las posibles causas y asignar para la resolución.	a. Número de síntomas incidentes identificados y registrados b. Número de causas de síntomas determinadas correctamente c. Número de problemas duplicados en el registro de referencia	
Actividades		
1. Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes. Referencia disponible recursos de conocimiento (incluidos errores y problemas conocidos) para identificar posibles resoluciones de incidentes (soluciones temporales y/o soluciones permanentes).		2
2. Si aún no existe un problema relacionado o un error conocido y si el incidente cumple con los criterios acordados para el registro del problema, registrar un nuevo problema.		

3. Asigne incidentes a funciones especializadas si se necesita una experiencia más profunda. Involucrar al nivel apropiado de gestión, donde y si es necesario.		
Práctica de gestión	**Ejemplo de métrica**	
DSS02.05 Resolver y recuperarse de incidentes. Documente, aplique y pruebe las soluciones o soluciones provisionales identificadas. Realizar acciones de recuperación para restaurar el servicio relacionado con TI	a. Porcentaje de incidentes resueltos dentro del SLA acordado b. Porcentaje de satisfacción de las partes interesadas con la resolución y la recuperación del incidente	
Actividades		
1. Seleccionar y aplicar las resoluciones de incidentes más adecuadas (solución temporal y/o solución permanente).		2
2. Registrar si se utilizaron soluciones alternativas para la resolución de incidentes.		
3. Realice acciones de recuperación, si es necesario.		
4. Documentar la resolución de incidentes y evaluar si la resolución se puede utilizar como fuente de conocimiento en el futuro.		
Práctica de gestión	**Ejemplo de métrica**	
DSS02.06 Cerrar solicitudes de servicio e incidencias. Verificar la resolución satisfactoria de incidentes y/o cumplimiento de solicitudes, y cierre	a. Nivel de satisfacción del usuario con el cumplimiento de la solicitud de servicio b. Porcentaje de incidentes resueltos dentro de un período acordado/aceptable de tiempo	
Actividades		
1. Verificar con los usuarios afectados que la solicitud de servicio ha sido atendida satisfactoriamente o la incidencia ha sido resuelta satisfactoriamente y en un plazo de tiempo acordado/aceptable.		2
2. Cerrar solicitudes de servicio e incidencias.		
Práctica de gestión	**Ejemplo de métrica**	
DSS02.07 Seguimiento del estado y producción de informes. Realizar un seguimiento, analizar y reportar periódicamente las incidencias y el cumplimiento de las solicitudes. Examine las tendencias para proporcionar información para la mejora continua.	a. Tiempo medio entre incidentes para el servicio habilitado para TI b. Número y porcentaje de incidentes que causan interrupción procesos críticos para el negocio	
Actividades		
1. Supervisar y realizar un seguimiento de las escalaciones y resoluciones de incidentes y solicitar procedimientos de manejo para avanzar hacia la resolución o terminación.		2

2 Identificar las partes interesadas en la información y sus necesidades de datos o informes. Identificar la frecuencia y el medio de los informes.	3
3. Producir y distribuir informes oportunos o proporcionar acceso controlado a datos en línea.	4
4. Analizar incidentes y solicitudes de servicio por categoría y tipo. Establecer tendencias e identificar patrones de problemas recurrentes, SLA incumplimientos o ineficiencias.	
5. Utilice la información como entrada para la planificación de la mejora continua.	5

Componente: Estructura organizacional

Práctica de gestión	Jefe de Tecnología	Propietarios de procesos de negocio	Líder de Desarrollo	Jefe de operaciones de TI	Supervisor	Gerente de Seguridad de la Información
DSS02.01 Definir esquemas de clasificación para incidentes y solicitudes de servicio.	A		R	R	R	
DSS02.02 Registrar, clasificar y priorizar solicitudes e incidencias.	A			R	R	
DSS02.03 Verificar, aprobar y cumplir con las solicitudes de servicio.	A	R	R	R	R	
DSS02.04 Investigar, diagnosticar y asignar incidentes.	A	R		R	R	
DSS02.05 Resolver y recuperarse de incidentes.	A		R	R	R	R
DSS02.06 Cerrar solicitudes de servicio e incidencias.	A			R	R	R
DSS02.07 Seguimiento del estado y producción de informes.	A			R	R	

GESTIÓN DE CONTINUIDAD

Dominio: entrega, servicio y soporte
Objetivo de gestión: DSS04 - Gestión de continuidad

Descripción

Establecer y mantener un plan para permitir que las organizaciones comerciales y de TI respondan a incidentes y se adapten rápidamente a las interrupciones. Esto permitirá operaciones continuas de procesos comerciales críticos y servicios de TI requeridos y mantener la disponibilidad de recursos, activos e información en un nivel aceptable para la empresa.

Propósito

Adaptarse rápidamente, continuar con las operaciones comerciales y mantener la disponibilidad de recursos e información a un nivel aceptable para la empresa en caso de una interrupción significativa (por ejemplo, amenazas, oportunidades, demandas).

El objetivo de gestión respalda el logro de un conjunto de metas empresariales y de alineación principales:

Metas empresariales	Metas de alineamiento
• EG01 Portafolio de productos y servicios competitivos • EG02 Riesgo empresarial gestionado • EG06 Continuidad y disponibilidad del servicio comercial • EG08 Optimización de la funcionalidad de procesos comerciales internos	• AG05 Entrega de servicios de TI en línea con los requisitos del negocio • AG07 Seguridad de la información, infraestructura de procesamiento , aplicaciones y privacidad

Ejemplo de métricas para metas empresariales		Ejemplo de métricas para metas de alineamiento	
EG01	a. Porcentaje de productos y servicios que cumplen o superan objetivos en ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o superan objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que	AG05	a. Porcentaje de partes interesadas del negocio satisfechas con el servicio de TI la entrega cumple con los niveles de servicio acordados b. Número de interrupciones comerciales debido a incidentes en el servicio de TI

	proporcionan ventaja competitiva d. Tiempo de comercialización de nuevos productos y servicios		c. Porcentaje de usuarios satisfechos con la calidad del servicio de TI entrega
EG02	a. Porcentaje de objetivos y servicios comerciales críticos cubiertos por la evaluación de riesgos b. Cantidad de incidentes significativos que no fueron identificados en evaluaciones de riesgos vs. incidentes totales C. Frecuencia de actualización del perfil de riesgo	AG07	a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o conflicto b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o conflicto C. Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o conflicto
EG06	a. Número de servicio al cliente o proceso comercial interrupciones que causan incidentes significativos b. Coste empresarial de los incidentes C. Número de horas de procesamiento comercial perdidas debido a interrupciones del servicio no planificadas d. Porcentaje de quejas en función de los cometidos objetivos de disponibilidad del servicio		
EG08	a. Niveles de satisfacción del directorio y la gerencia ejecutiva con capacidades de proceso de negocio b. Niveles de satisfacción de los clientes con la prestación del servicio. C. Niveles de satisfacción de los proveedores con la cadena de suministro		
Componente: Proceso			

Práctica de gestión	Ejemplo de métrica	
DSS04.01 Definir la política, los objetivos y el alcance de la continuidad del negocio. Definir la política y el alcance de la continuidad del negocio, alineados con la empresa y objetivos de las partes interesadas, para mejorar la resiliencia empresarial.	a. Porcentaje de objetivos y alcance de continuidad del negocio reelaborados debido a procesos y actividades mal identificados b. Porcentaje de partes interesadas clave que participan, definen y acuerdan política de continuidad y alcance	
Actividades		
1. Identificar los procesos comerciales internos y subcontratados y las actividades de servicio que son fundamentales para las operaciones de la empresa o necesarios para cumplir con las obligaciones legales y/o contractuales.		2
2. Identificar las partes interesadas clave y los roles y responsabilidades para definir y acordar la política y el alcance de la continuidad.		
3. Definir y documentar los objetivos de política mínimos acordados y el alcance para la resiliencia empresarial.		
4. Identificar los procesos empresariales de apoyo esenciales y los servicios de TI relacionados.		
Práctica de gestión	**Ejemplo de métrica**	
DSS04.02 Mantener la resiliencia empresarial. Evaluar las opciones de resiliencia empresarial y elegir una opción rentable y estrategia viable que asegurará la continuidad de la empresa, la recuperación ante desastres y respuesta a incidentes frente a un desastre u otro incidente importante o interrupción.	a. Tiempo de inactividad total resultante de un incidente o interrupción importante b. Porcentaje de partes interesadas claves involucradas en los análisis de impacto comercial evaluar el impacto a lo largo del tiempo de una interrupción en el negocio crítico funciones y el efecto que una interrupción tendría sobre ellas	
Actividades		
1. Identificar escenarios potenciales que puedan dar lugar a eventos que podrían causar incidentes disruptivos significativos.		2
2. Llevar a cabo un análisis de impacto comercial para evaluar el impacto a lo largo del tiempo de una interrupción de las funciones críticas del negocio y el efecto que una interrupción tendría sobre ellos.		
3. Establecer el tiempo mínimo requerido para recuperar un proceso de negocio y soporte de TI, basado en una duración aceptable de interrupción del negocio y máxima interrupción tolerable.		
4. Determinar las condiciones y dueños de las decisiones clave que harán invocar los planes de continuidad.		
5. Evaluar la probabilidad de amenazas que podrían causar la pérdida de continuidad del negocio. Identificar medidas que reducirán la probabilidad y el impacto a través de una mejor prevención y una mayor resiliencia.		3
6. Analizar los requisitos de continuidad para identificar posibles opciones comerciales y técnicas estratégicas.		
7. Identificar los requisitos de recursos y costos para cada opción técnica estratégica y hacer recomendaciones estratégicas.		

8. Obtener la aprobación comercial ejecutiva para las opciones estratégicas seleccionadas.	

Práctica de gestión	**Ejemplo de métrica**
DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio. Desarrollar un plan de continuidad del negocio (BCP) y un plan de recuperación ante desastres (DRP) en base a la estrategia. Documentar todos los procedimientos necesarios para la empresa para continuar con las actividades críticas en caso de un incidente.	a. Número de sistemas comerciales críticos no cubiertos por el plan b. Porcentaje de partes interesadas claves involucradas en el desarrollo de BCP y DRP

Actividades	
1. Definir las acciones de respuesta a incidentes y las comunicaciones que se tomarán en caso de interrupción. Definir roles relacionados y responsabilidades, incluida la responsabilidad por la política y la implementación.	2
2. Asegúrese de que los proveedores clave y los socios externos tengan planes de continuidad efectivos. Obtener evidencia auditada según sea necesario.	
3. Definir las condiciones y los procedimientos de recuperación que permitirían la reanudación del procesamiento comercial. Incluye actualización y reconciliación de bases de datos de información para preservar la integridad de la información.	
4. Desarrollar y mantener BCP y DRP operativos que contengan los procedimientos a seguir para permitir la operación continua de procesos comerciales críticos y/o arreglos de procesamiento temporal. Incluir enlaces a planes de proveedores de servicios subcontratados.	
5. Definir y documentar los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI.	
6. Definir y documentar los requisitos de respaldo de información necesarios para respaldar los planes. Incluye planos y documentos en papel. así como archivos de datos. Considere la necesidad de seguridad y almacenamiento fuera del sitio.	
7. Determinar las habilidades requeridas para las personas involucradas en la ejecución del plan y los procedimientos.	
8. Distribuir los planos y la documentación de respaldo de manera segura a las partes interesadas debidamente autorizadas. Asegúrese de que los planes y la documentación son accesibles en todos los escenarios de desastre.	3

Práctica de gestión	**Ejemplo de métrica**
DSS04.04 Ejercicio, prueba y revisión del plan de continuidad del negocio (BCP) y plan de respuesta a desastres (DRP). Pruebe la continuidad regularmente para ejercitar planes contra resultados predeterminados, mantener la resiliencia empresarial y permitir soluciones innovadoras a desarrollar	a. Frecuencia de las pruebas b. Número de ejercicios y pruebas que lograron los objetivos de recuperación

Actividades	
1. Definir objetivos para el ejercicio y prueba de las funciones empresariales, técnicas, logísticas, administrativas, procedimentales y operativas. sistemas del plan para verificar la integridad del BCP y DRP en el cumplimiento del riesgo comercial.	2
2. Definir y acordar ejercicios de partes interesadas que sean realistas y validen los procedimientos de continuidad. Incluir funciones y responsabilidades y arreglos de retención de datos que causen una interrupción mínima en los procesos comerciales.	
3. Asignar roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad.	
4. Programar ejercicios y actividades de prueba según lo definido en los planes de continuidad.	3
5. Llevar a cabo un informe y análisis posterior al ejercicio para considerar el logro	4
6. Con base en los resultados de la revisión, desarrollar recomendaciones para mejorar los planes de continuidad actuales.	5
Práctica de gestión	**Ejemplo de métrica**
DSS04.05 Revisar, mantener y mejorar los planes de continuidad. Llevar a cabo una revisión de la gestión de la capacidad de continuidad en forma periódica. intervalos para asegurar su idoneidad, adecuación y eficacia continuas. Gestionar los cambios en los planes de acuerdo con el control de cambios. proceso para garantizar que los planes de continuidad se mantengan actualizados y reflejan continuamente los requisitos comerciales reales.	a. Porcentaje de mejoras acordadas al plan que se han reflejado en el plano b. Porcentaje de planes de continuidad y evaluaciones de impacto comercial q
Actividades	
1. De manera regular, revise los planes de continuidad y la capacidad frente a cualquier suposición realizada y las operaciones comerciales actuales y objetivos estratégicos.	3
2. Revisar periódicamente los planes de continuidad para considerar el impacto de cambios nuevos o importantes en la organización de la empresa, procesos comerciales, acuerdos de subcontratación, tecnologías, infraestructura, sistemas operativos y sistemas de aplicación.	
3. Considere si se puede requerir una evaluación de impacto comercial revisada, dependiendo de la naturaleza del cambio.	
4. Recomendar cambios en políticas, planes, procedimientos, infraestructura y funciones y responsabilidades. Comunicarlos como apropiado para la aprobación y el procesamiento de la gerencia a través del proceso de gestión de cambios de TI	
Práctica de gestión	**Ejemplo de métrica**

DSS04.06 Llevar a cabo la capacitación del plan de continuidad. Brindar capacitación periódica a todas las partes internas y externas interesadas sesiones sobre los procedimientos y sus funciones y responsabilidades en caso de interrupción	a. Porcentaje de partes interesadas internas y externas que recibieron capacitación b. Porcentaje de partes internas y externas relevantes cuyas habilidades y las competencias son actuales
Actividades	
1. Implementar la concientización y capacitación sobre BCP y DRP.	**2**
2. Definir y mantener los requisitos y planes de capacitación para quienes realizan la planificación de continuidad, las evaluaciones de impacto, el riesgo evaluaciones, comunicación con los medios y respuesta a incidentes. Asegurar que los planes de capacitación consideren la frecuencia de la capacitación y mecanismos de impartición de formación.	**3**
3. Desarrollar competencias a partir de la formación práctica, incluida la participación en ejercicios y pruebas.	
4. Con base en los resultados del ejercicio y las pruebas, monitorear las habilidades y competencias.	4
Práctica de gestión	**Ejemplo de métrica**
DSS04.07 Administrar arreglos de respaldo. Mantener la disponibilidad de información crítica para el negocio.	a. Porcentaje de medios de copia de seguridad transferidos y almacenados de forma segura b. Porcentaje de restauración exitosa y oportuna a partir de una copia de seguridad o alternativa copias de medios
Actividades	
1. Realizar copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo con un cronograma definido. Considere la frecuencia (mensual, semanal, diario, etc.), modo de copia de seguridad (por ejemplo, espejo de disco para copias de seguridad en tiempo real frente a DVD-ROM para retención a largo plazo), tipo de copia de seguridad (por ejemplo, completa o incremental) y tipo de medio. Considere también copias de seguridad en línea automatizadas, tipos de datos (por ejemplo, voz, ópticos), creación de registros, datos informáticos críticos del usuario final (por ejemplo, hojas de cálculo), ubicación física y lógica de las fuentes de datos, seguridad y derechos de acceso, y encriptación.	2
2. Definir los requisitos para el almacenamiento en el sitio y fuera del sitio de los datos de respaldo que cumplan con los requisitos comerciales. Considera la accesibilidad necesaria para realizar una copia de seguridad de los datos.	
3. Pruebe y actualice periódicamente los datos archivados y de copia de seguridad.	
4. Garantizar que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceros estén adecuadamente respaldados o asegurado de otra manera. Considere solicitar la devolución de copias de seguridad de terceros. Considere acuerdos de depósito o depósito en garantía.	

Práctica de gestión	Ejemplo de métrica
DSS04.08 Realizar una revisión posterior a la reanudación. Evaluar la adecuación del plan de continuidad del negocio (BCP) y desastre plan de respuesta (DRP) luego de la reanudación exitosa del negocio procesos y servicios después de una interrupción.	a. Porcentaje de problemas identificados y posteriormente abordados en el plan b. Porcentaje de problemas identificados y posteriormente abordados en la capacitación materiales

Actividades	
1. Evaluar el cumplimiento del BCP y DRP documentados.	4
2. Determinar la efectividad de los planes, continuidad capacidades, roles y responsabilidades, habilidades y competencias, resiliencia al incidente, la infraestructura técnica y las estructuras y relaciones organizacionales.	
3. Identificar debilidades u omisiones en los planes y capacidades y hacer recomendaciones de mejora. Obtener aprobación de la gerencia para cualquier cambio en los planes y aplicar a través del proceso de control de cambios de la empresa.	5

Componente: Estructura organizacional													
Práctica de gestión	Comité Ejecutivo	director de operaciones	Director de información	Jefe de Tecnología	Director de seguridad de la información	Propietarios de procesos de negocio	Función de gestión de datos	Jefe de arquitectura	Desarrollo de la cabeza	Jefe de operaciones de TI	Supervisor	Gerente de Seguridad de la Información	Gerente de Continuidad de Negocios
DSS04.01 Definir la política, los objetivos y el alcance de la continuidad del negocio.	R	A	R		R	R				R	R		R
DSS04.02 Mantener la resiliencia empresarial.	R	A	R			R		R		R		R	R

DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio.			R	R		R				R		R	A
DSS04.04 Ejercer, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta a desastres (DRP).			R	R		R				R		R	A
DSS04.05 Revisar, mantener y mejorar los planes de continuidad.		A	R	R	R	R				R			R
DSS04.06 Llevar a cabo la capacitación del plan de continuidad.			R	R		R			R	R		R	A
DSS04.07 Administrar arreglos de respaldo				A			R			R		R	R
DSS04.08 Realizar una revisión posterior a la reanudación.			R	R	R	R				R			A

GESTIÓN DE SERVICIOS DE SEGURIDAD

Dominio: alineación, planificación y organización Objetivo de gestión: DSS05 - Gestión de Servicios de seguridad			
Descripción			
Proteger la información de la empresa para mantener el nivel de riesgo de seguridad de la información aceptable para la empresa de acuerdo con la política de seguridad. Establecer y mantener roles de seguridad de la información y privilegios de acceso. Realizar monitoreo de seguridad.			
Propósito			
Minimice el impacto comercial de las vulnerabilidades e incidentes de seguridad de la información operativa.			
El objetivo de gestión respalda el logro de un conjunto de metas empresariales y de alineación principales:			
Metas empresariales		**Metas de alineamiento**	
• EG02 Riesgo empresarial gestionado • EG06 Continuidad y disponibilidad del servicio comercial		• AG02 Riesgo relacionado con I&T gestionado • AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones y privacidad	
Ejemplo de métricas para metas empresariales		**Ejemplo de métricas para metas de alineamiento**	
EG02	a. Porcentaje de objetivos y servicios comerciales críticos cubiertos por la evaluación de riesgos b. Ratio de incidentes significativos que no fueron identificados en evaluaciones de riesgos vs. incidentes totales C. Frecuencia de actualización del perfil de riesgo	AG02	a. Frecuencia de actualización del perfil de riesgo b. Porcentaje de evaluaciones de riesgos empresariales que incluyen riesgo relacionado con TI C. Número de incidentes significativos relacionados con TI que no fueron identificado en una evaluación de riesgos
EG06	a. Número de servicio al cliente o proceso comercial interrupciones que causan incidentes significativos b. Coste empresarial de los incidentes C. Número de horas de procesamiento comercial perdidas debido a interrupciones del servicio no planificadas d. Porcentaje de quejas en función de los cometidos objetivos de disponibilidad del servicio	AG07	a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o vergüenza pública b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o vergüenza pública C. Número de incidentes de integridad que causan pérdidas financieras,

		interrupción del negocio o vergüenza pública

Componente: Proceso		
Práctica de gestión	**Ejemplo de métrica**	
DSS05.01 Proteger contra software malicioso. Implementar y mantener medidas preventivas, detectivas y correctivas. (especialmente parches de seguridad actualizados y control de virus) en toda la empresa para proteger los sistemas de información y la tecnología de maliciosos software (por ejemplo, ransomware, malware, virus, gusanos, spyware, spam).	a. Número de ataques exitosos de software malicioso b. Porcentaje de empleados que no pasan las pruebas de ataques maliciosos (p. ej., prueba de correo electrónico de phishing)	
Actividades		
1. Instalar y activar herramientas de protección de software malicioso en todas las instalaciones de procesamiento, con archivos de definición de software malicioso que se actualizan según sea necesario (automática o semiautomáticamente).		2
2. Filtre el tráfico entrante, como correo electrónico y descargas, para protegerse contra información no solicitada (por ejemplo, spyware, correos electrónicos de phishing).		
3. Comunicar el conocimiento del software malicioso y hacer cumplir los procedimientos y responsabilidades de prevención. Realizar capacitaciones periódicas sobre el malware en el correo electrónico y el uso de Internet. Capacite a los usuarios para que no abran, pero informen, correos electrónicos sospechosos y no instalen correos electrónicos compartidos o software no aprobado.		3
4. Distribuya todo el software de protección de forma centralizada (nivel de versión y parche) utilizando la configuración centralizada y la administración de cambios de TI.		
5. Revisar y evaluar periódicamente la información sobre nuevas amenazas potenciales (por ejemplo, revisar la seguridad de los productos y servicios de los proveedores).		4
Práctica de gestión	**Ejemplo de métrica**	
DSS05.02 Administrar la seguridad de la red y la conectividad. Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger información sobre todos los métodos de conectividad.	a. Número de infracciones de cortafuegos b. Número de vulnerabilidades descubiertas C. Porcentaje de tiempo que la red y los sistemas no están disponibles debido a la seguridad incidente	
Actividades		
1. Permita que solo los dispositivos autorizados tengan acceso a la información corporativa y la red empresarial. Configure estos dispositivos para forzar entrada de contraseña.		2
2. Implementar mecanismos de filtrado de red, como firewalls y software de detección de intrusos. Aplicar políticas apropiadas para controlar el tráfico entrante y saliente.		

3. Aplicar protocolos de seguridad aprobados a la conectividad de la red.	
4. Configurar equipos de red de forma segura.	
5. Cifrar la información en tránsito según su clasificación.	3
6. Con base en las evaluaciones de riesgos y los requisitos comerciales, establezca y mantenga una política para la seguridad de la conectividad.	
7. Establecer mecanismos confiables para apoyar la transmisión y recepción segura de información.	
8. Realice pruebas de penetración periódicas para determinar la idoneidad de la protección de la red.	4
9. Llevar a cabo pruebas periódicas de seguridad del sistema para determinar la idoneidad de la protección del sistema.	

Práctica de gestión	**Ejemplo de métrica**
DSS05.03 Administrar la seguridad de puntos finales. Asegúrese de que los puntos finales (por ejemplo, portátiles, ordenadores de sobremesa, servidores y otros dispositivos móviles) y dispositivos de red o software) están asegurados a un nivel que es igual o superior a los requisitos de seguridad definidos para la información procesada, almacenada o transmitida.	a. Número de incidentes que involucran dispositivos de punto final b. Número de dispositivos no autorizados detectados en la red o en el entorno de usuario final C. Porcentaje de personas que reciben capacitación de concientización relacionada con el uso de dispositivos de punto final
Actividades	
1. Configurar sistemas operativos de forma segura.	2
2. Implementar mecanismos de bloqueo de dispositivos.	
3. Administrar el acceso y control remoto (por ejemplo, dispositivos móviles, teletrabajo).	
4. Administre la configuración de la red de manera segura.	
5. Implemente el filtrado del tráfico de red en los dispositivos finales.	
6. Proteger la integridad del sistema.	
7. Proporcionar protección física de los dispositivos de punto final.	
8. Deseche los dispositivos terminales de forma segura.	
9. Administre el acceso malicioso a través del correo electrónico y los navegadores web. Por ejemplo, bloquee ciertos sitios web y desactive los clics en enlaces para smartphones.	
10. Cifrar la información almacenada según su clasificación.	3

Práctica de gestión	**Ejemplo de métrica**

DSS05.04 Administrar la identidad del usuario y el acceso lógico. Asegúrese de que todos los usuarios tengan derechos de acceso a la información de acuerdo con requisitos comerciales. Coordinar con las unidades de negocio que gestionan sus propios derechos de acceso dentro de los procesos de negocio.	a. Tiempo medio entre cambio y actualización de cuentas b. Número de cuentas (frente al número de usuarios/personal autorizados) C. Número de incidentes relacionados con el acceso no autorizado a la información
Actividades	
1. Mantener los derechos de acceso de los usuarios de acuerdo con la función comercial, los requisitos del proceso y las políticas de seguridad. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, con base en privilegios mínimos, necesidad de tener y principios de necesidad de saber.	2
2. Administrar todos los cambios a los derechos de acceso (creación, modificaciones y eliminaciones) de manera oportuna con base únicamente en los datos aprobados y transacciones documentadas autorizadas por los administradores designados.	2
3. Segregar, reducir al mínimo necesario y gestionar activamente las cuentas de usuarios privilegiados. Garantizar el seguimiento de todos actividad en estas cuentas.	
4. Identificar de manera única todas las actividades de procesamiento de información por roles funcionales. Coordinar con las unidades de negocio para asegurar que todos los roles están definidos de forma coherente, incluidas las funciones definidas por la propia empresa dentro de las aplicaciones de procesos empresariales.	
5. Autentique todos los accesos a los activos de información según el rol de la persona o las reglas comerciales. Coordinar con las unidades de negocio, que gestionan la autenticación dentro de las aplicaciones utilizadas en los procesos comerciales para garantizar que los controles de autenticación han sido correctamente administrados.	
6. Garantizar que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas de TI (aplicación comercial, infraestructura de TI, operaciones, desarrollo y mantenimiento del sistema) son identificables de forma única.	
7. Mantener un registro de auditoría del acceso a la información según su sensibilidad y los requisitos reglamentarios.	4
8. Realizar una revisión de gestión regular de todas las cuentas y privilegios relacionados.	
Práctica de gestión	**Ejemplo de métrica**
DSS05.05 Administrar el acceso físico a los activos de TI Definir e implementar procedimientos (incluidos los procedimientos de emergencia) conceder, limitar y revocar el acceso a locales, edificios y áreas, de acuerdo a la necesidad del negocio. Acceso a locales, edificios y áreas debe ser justificado, autorizado, registrado y monitoreado. Este requisito se aplica a todas las personas que ingresan a las instalaciones, incluido el personal, personal, clientes, proveedores, visitantes o cualquier otro tercero.	a. Calificación promedio para evaluaciones de seguridad física b. Número de incidentes relacionados con la seguridad de la información física

Actividades	
1. Registre y supervise todos los puntos de entrada a los sitios de TI. Registre a todos los visitantes, incluidos los contratistas y proveedores, en el sitio.	2
2. Asegúrese de que todo el personal muestre una identificación debidamente aprobada en todo momento.	
3. Requerir que los visitantes sean escoltados en todo momento mientras estén en el sitio.	
4. Restrinja y controle el acceso a sitios de TI confidenciales mediante el establecimiento de restricciones perimetrales, como vallas, muros y seguridad.	
5. Gestionar las solicitudes para permitir el acceso debidamente autorizado a las instalaciones informáticas.	3
6. Asegúrese de que los perfiles de acceso permanezcan actualizados. Base el acceso a los sitios de TI (salas de servidores, edificios, áreas o zonas) en función del trabajo y responsabilidades	
7. Llevar a cabo capacitaciones periódicas de concientización sobre la seguridad de la información física.	
Práctica de gestión	**Ejemplo de métrica**
DSS05.06 Administrar documentos confidenciales y dispositivos de salida. Establecer salvaguardas físicas apropiadas, prácticas contables y gestión de inventario con respecto a activos sensibles de TI, como especiales formularios, instrumentos negociables, impresoras especiales o fichas de seguridad.	a. Número de dispositivos de salida robados b. Porcentaje de documentos confidenciales y dispositivos de salida identificados en inventario
Actividades	
1. Establecer procedimientos para regir la recepción, el uso, la extracción y la eliminación de documentos confidenciales y dispositivos de salida en, dentro de, y fuera de la empresa.	2
2. Asegúrese de que existan controles criptográficos para proteger la información confidencial almacenada electrónicamente.	

3. Asigne privilegios de acceso a documentos confidenciales y dispositivos de salida según el principio de privilegio mínimo, equilibrando el riesgo y requisitos comerciales.	3
4. Establezca un inventario de documentos confidenciales y dispositivos de salida, y realice conciliaciones periódicas.	
5. Establecer protecciones físicas apropiadas sobre documentos confidenciales.	

Práctica de gestión	**Ejemplo de métrica**
DSS05.07 Administrar vulnerabilidades y monitorear la infraestructura para eventos relacionados con la seguridad. Usar una cartera de herramientas y tecnologías (por ejemplo, detección de intrusos herramientas), administrar vulnerabilidades y monitorear la infraestructura para Acceso no autorizado. Garantizar que las herramientas, tecnologías y la detección se integran con el monitoreo general de eventos e incidentes gestión."	a. Número de pruebas de vulnerabilidad realizadas en dispositivos perimetrales b. Número de vulnerabilidades descubiertas durante las pruebas C. Tiempo necesario para remediar cualquier vulnerabilidad d. Porcentaje de tickets creados de manera oportuna al monitorear los sistemas identifican posibles incidentes de seguridad

Actividades	
1. Usar continuamente una cartera de tecnologías, servicios y activos compatibles (por ejemplo, escáneres de vulnerabilidades, fuzzers y sniffers, analizadores de protocolo) para identificar vulnerabilidades de seguridad de la información.	2
2. Defina y comunique los escenarios de riesgo, para que puedan reconocerse fácilmente y se comprenda la probabilidad y el impacto.	
3. Revise periódicamente los registros de eventos para detectar posibles incidentes.	3
4. Asegúrese de que los tickets de incidentes relacionados con la seguridad se creen de manera oportuna cuando el monitoreo identifique incidentes potenciales.	
5. Registrar eventos relacionados con la seguridad y conservar los registros durante el período apropiado. Orientación relacionada (estándares, marcos, requisitos de cumplimiento)	
Componente: Estructura organizacional	

Práctica de gestión	Director de información	Director de seguridad de la información	Propietarios de procesos de negocio	Jefe de Recursos Humanos	Líder de Desarrollo	Jefe de operaciones de TI	Gerente de Seguridad de la Información	Oficial de Privacidad
DSS05.01 Proteger contra software malicioso.		A	R	R	R	R	R	
DSS05.02 Administrar la seguridad de la red y la conectividad.		A			R	R	R	
DSS05.03 Administrar la seguridad de puntos finales.		A			R	R	R	
DSS05.04 Administrar la identidad del usuario y el acceso lógico.		A	R			R	R	R
DSS05.05 Administrar el acceso físico a los activos de TI		A				R	R	R
DSS05.06 Administrar documentos confidenciales y dispositivos de salida.	A					R		R
DSS05.07 Administrar vulnerabilidades y monitorear la infraestructura para eventos relacionados con la seguridad.		A				R	R	R