UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

MAESTRÍA EN AUDITORÍA GUBERNAMENTAL Y CONTROL DE GESTIÓN

Tema: EL ASEGURAMIENTO DE LA INFORMACIÓN Y EL MONITOREO DE RIESGOS EN EL HOSPITAL BÁSICO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL DE LATACUNGA.

Trabajo de Titulación previo a la obtención del Grado Académico de Magíster en Auditoría Gubernamental y Control de Gestión.

Modalidad de Titulación Proyecto de Investigación y Desarrollo

Autora: Ingeniera Yesenia Elizabeth Acurio Corrales

Directora: Ingeniera Bertha Jeaneth Sánchez Herrera Magíster

Ambato-Ecuador

2021

APROBACIÓN DEL TRABAJO DE TITULACIÓN

A la Unidad Académica de Titulación de la Facultad de Contabilidad y Auditoría

El Tribunal receptor de la Defensa del Trabajo de Titulación presidido por la Doctora Alexandra Tatiana Valle Álvarez Magíster, e integrado por los señores: Doctora Paula Marcela Vega Rivera Magíster y Doctor Joselito Ricardo Naranjo Santamaría Magíster, designados por la Unidad Académica de Titulación de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: "EL ASEGURAMIENTO DE LA INFORMACIÓN Y EL MONITOREO DE RIESGOS EN EL HOSPITAL BÁSICO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL DE LATACUNGA", elaborado y presentado por la señorita Ingeniera Yesenia Elizabeth Acurio Corrales, para optar por el Grado Académico de Magíster en Auditoria Gubernamental y Control de Gestión; una vez escuchada la defensa oral del Trabajo de Titulación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la Universidad Técnica de Ambato.

Firmado electrónicamente por:
ALEXANDRA TATIANA VALLE ALVAREZ

Dra. Alexandra Tatiana Valle Álvarez Mg.
Presidente y Miembro del Tribunal de Defensa

Firmado electrónicamente por:
PAULA MARCELA VEGA RIVERA

Dra. Paula Marcela Vega Rivera Mg.
Miembro del Tribunal de Defensa

Firmado electrónicamente por:
JOSELITO RICARDO NARANJO SANTAMARIA

Dr. Joselito Ricardo Naranjo Santamaría Mg.
Miembro del Tribunal de Defensa

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: EL ASEGURAMIENTO DE LA INFORMACIÓN Y EL MONITOREO DE RIESGOS EN EL HOSPITAL BÁSICO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL DE LATACUNGA, le corresponde exclusivamente a: Ingeniera Yesenia Elizabeth Acurio Corrales, Autora bajo la Dirección de la Ingeniera Bertha Jeaneth Sánchez Herrera Magíster, Directora del Trabajo de Titulación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

Firmado electrónicamente por:
YESENIA
ELIZABETH ACURIO
CORRALES

Ing. Yesenia Elizabeth Acurio Corrales

AUTORA

Firmado electrónicamente por:
BERTHA JEANETH
SANCHEZ HERRERA

Ing. Bertha Jeaneth Sánchez Herrera Mg.

DIRECTORA

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi Trabajo de Titulación, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad Técnica de Ambato.

Firmado electrónicamente por:
YESENIA ELIZABETH ACURIO CORRALES

Ing. Yesenia Elizabeth Acurio Corrales

c.c. 0503213399

ÍNDICE GENERAL

Contenido

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE FIGURAS

Pág.

AGRADECIMIENTO

Doy gracias en primer lugar a Dios por la vida y la salud en estos tiempos tan difíciles, a mis padres que son mi pilar y fortaleza para luchar por mis metas y que con su amor y paciencia me han apoyado para continuar preparándome para lograr ser mejor persona y una excelente profesional, a mi novio por su constante apoyo tan como en momentos buenos y malos y a mi familia que siempre han estado pendientes en cada momento de mi vida.

Yesenia.

DEDICATORIA

El presente trabajo, desarrollado con toda la dedicación y esfuerzo lo dedico a Dios quien me ha dado la vida, salud y la fuerza para superar cualquier adversidad por más fuerte que sea, de igual manera a mis padres por su apoyo incondicional y dedicación para formar la persona que hoy soy.

A mi familia por sus consejos y grandes ejemplos de personas y profesionales y a mi novio cuyo amor ha estado presente en cada paso que doy.

Yesenia.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORÍA
MAESTRÍA EN AUDITORÍA GUBERNAMENTAL Y CONTROL DE GESTIÓN

TEMA:

EL ASEGURAMIENTO DE LA INFORMACIÓN Y EL MONITOREO DE RIESGOS EN EL HOSPITAL BÁSICO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL DE LATACUNGA

AUTORA: Ingeniera Yesenia Elizabeth Acurio Corrales
DIRECTORA: Ingeniera Bertha Jeaneth Sánchez Herrera Magíster
LÍNEA DE INVESTIGACIÓN: Sistema de Control
FECHA: 29 de marzo de 2021

RESUMEN EJECUTIVO

El presente trabajo investigativo tiene como propósito determinar el aporte del aseguramiento de información al monitoreo de riesgos en el hospital básico del Instituto Ecuatoriano de Seguridad Social de Latacunga, con el fin de tomar las medidas correctivas en caso de ser necesario y mejorar su gestión para así lograr el cumplimiento de las metas y objetivos institucionales. La investigación se realizó bajo el enfoque mixto ya que se combina el enfoque cualitativo y cuantitativo. La modalidad de la investigación fue de campo y bibliográfica-documental, tomando en cuenta que se recopiló información en el lugar donde se suscita la problemática analizada; por otra parte, a través de una extensa revisión bibliográfica, tanto de libros, artículos científicos, tesis, entre otras fuentes.

Los instrumentos utilizados fueron una encuesta basada en COBIT la cual se realizó al jefe del departamento informático y otra encuesta basada en COSO ERM aplicada al Jefe Financiero del Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga.

Los resultados permitieron conocer que el nivel de madurez promedio para todos los dominios del aseguramiento de la información se caracterizan por ser repetible lo cual indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal mediante documentos oficiales como manuales, guías o planes y oficios para que esta comunicación tenga un registro y un seguimiento, de los procesos estándar que se realizan en el Hospital General del IESS de Latacunga entre estos dominios se destaca el adquirir e implementar; y el planificar y organizar.

Descriptores: Aseguramiento de la Información, Coso erm, Cobit, Control Interno, Impacto, Nivel de Madurez, Monitoreo de Riesgos, Probabilidad, Riesgos, Tecnología.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

MAESTRÍA EN AUDITORÍA GUBERNAMENTAL Y CONTROL DE GESTIÓN

THEME:

INFORMATION ASSURANCE AND RISK MONITORING IN THE BASIC HOSPITAL OF THE ECUADORIAN INSTITUTE OF SOCIAL SECURITY OF LATACUNGA

AUTHOR: Ingeniera Yesenia Elizabeth Acurio Corrales

DIRECTED BY: Ingeniera Bertha Jeaneth Sánchez Herrera Magíster

LINE OF RESEARCH: Control system

DATE: March 29th 2021

EXECUTIVE SUMMARY

The purpose of this investigative work is to determine the contribution of information assurance to risk monitoring in the basic hospital of the Ecuadorian Institute of Social Security of Latacunga, in order to take corrective measures if necessary and improve it is management in order to achieve the fulfillment of institutional goals and objectives. The research was carried out under the mixed approach since the qualitative and quantitative approach is combined. The research modality was field and bibliographic-documentary, taking into account that information was collected in the place where the analyzed problem arises; on the other hand, through an extensive bibliographic review, both of books, scientific articles, theses, among other sources.

The instruments used were a survey based on COBIT which was carried out to the Head of the IT department and another survey based on COSO ERM applied to the Chief Financial Officer of the Basic Hospital of the Ecuadorian Institute of Social Security of Latacunga.

The results allowed us to know that the average maturity level for all the information assurance domains is characterized by being repeatable, which indicates that the processes have been developed to the point where different people follow similar procedures performing the same task, which a lack of formal communication through official documents such as manuals, guides or plans and official letters is evident so that this communication has a record and a follow-up of the standard processes that are carried out in the Basic Hospital of the IESS in Latacunga among these domains, acquiring and implementing stands out; and planning and organizing. As well as risk monitoring, it shows a lack of integration in internal policies, as well as the scarce promotion of a culture for risk management in computer technologies that guarantee the security of the information that is generated and handled in the financial department. of the Basic Hospital of the IESS of Latacunga.

Keywords: Coso erm, Cobit, Internal Control, Information Assurance, Impact, Level of maturity, Probability, Risk Monitoring, Risks, Technology

INTRODUCCIÓN

El progreso de las tecnologías de información y comunicación ha sido un punto clave para el avance de la administración pública ya que ha surgido la idea de reemplazar los documentos y trámites burocráticos por las tecnologías de la información y de la comunicación (TIC) y así lograr un mejoramiento en la gestión pública en Ecuador; sin embargo debido a esta modernización en la gestión pública y al crecimiento en los riesgos tecnológicos es importante que las instituciones cuenten controles para el manejo de las tecnologías de información y a más estén preparadas para administrar sus posibles riesgos de esa manera se lograr un manejo adecuado de los recursos públicos asignados.

En el **Capítulo I**, se describe el planteamiento del problema de la investigación con aspectos internacionales y nacionales, referente al aseguramiento de la información y el monitoreo de riesgos con un enfoque en la tecnología

En el **Capítulo II**, en este capítulo se desarrolla un estudio teórico de las variables de estudio que fundamenta la investigación.

En el **Capítulo III**, se muestra la metodología empleada en este estudio, determinando un enfoque cualitativo y cuantitativo como método de trabajo; se define la población y muestra para determinar la unidad de análisis.

En el **Capítulo IV**, en este capítulo se efectúa el análisis e interpretación de los resultados concernientes a la aplicación COBIT Y COSO ERM.

En el **Capítulo V**, finalmente se emiten las conclusiones y recomendaciones de la aplicación y desarrollo de la presente investigación.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1 Tema

"El Aseguramiento de la información y el monitoreo de riesgos en el Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga."

1.2 Planteamiento del problema

1.2.1 Contextualización

Macrocontextalización

La información que forma parte de una Entidad Pública es crucial para su correcto desempeño dentro de la política pública y su relación con el ciudadano, sin importar qué tipo de información se trate en la Entidad, ésta será parte primordial en el cumplimiento de sus Objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de una Entidad o de un Estado (MINTIC, 2016).

Actualmente las instituciones a nivel mundial tanto públicas como privadas, debido a la rápida actualización de la tecnología actúan en un ambiente totalmente disímil, en relación con la década anteriores, se ha dispuesto a las empresas actualizar sus procesos, por lo que, se han tenido mejorías como también complicaciones, los trámites se ejecutan con rapidez, pero, al no contar con la vigilancia pertinente a los datos ingresados y procesados mediante la tecnología de la información las empresas corren el riesgo de ser vulneradas de varias formas.

Casi todas las organizaciones públicas o privadas, al igual que las personas, dependen de alguna manera de la tecnología de la información como una herramienta esencial para lograr sus objetivos de negocio o para poder desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy. La seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas. Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenaz y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones (Tarazona, 2007).

La actualización de las empresas públicas ha ido a la par con las circunstancias que se han dado en gran medida por los delitos informáticos relacionados con robo de información confidencial que han dejado una marca en la reputación de la seguridad de dichas instituciones ; de tal manera estas han actuado para tener una eficiente administración estratégica para el manejo y control de las tecnologías de la información y de esta forma lograr un aseguramiento de la información.

Las tecnologías y los sistemas de información (TSI) se han convertido en los elementos más esenciales para la supervivencia de las organizaciones, ya que de las TSI dependen el buen funcionamiento y la evolución de sus procesos de negocio,

así como la información que necesitan para tomar todas sus decisiones operacionales, tácticas y estratégicas. Esto significa que el diseño de nuevos productos y servicios, la eficiencia de las operaciones y la capacidad de reaccionar ante cambios en el entorno competitivo depende, en gran medida, de la capacidad de adquirir, procesar y analizar información, lo que permite a su vez brindar a la alta dirección información de forma continua, oportuna y condensada para un adecuado proceso de toma de decisiones respecto a riesgos y controles. Por ello cobran cada día más interés el gobierno y la gestión de las TSI, temas en los cuales el director de TI es llamado a desempeñar un papel crucial. El director de TI deberá implementar un conjunto de buenas prácticas de gobierno y de gestión en las diferentes áreas relacionadas con la prestación de servicios, desarrollo de software, seguridad, gestión de activos, etc (Celi, 2014).

Tomando en consideración lo anteriormente mencionado la gestión de riesgos y el control de las tecnologías de la información son dos puntos claves para lograr una administración estratégica ya que en la actualidad la naturaleza evolutiva de los riesgos tecnológicos y las expectativas sobre su administración está generando presión a las prácticas de administración tradicional debido a que el alcance de estos eventos imprevistos se extiende a múltiples áreas de las organizaciones tanto operacionales y financieras debido a que ninguna de estas categorías están separadas y más bien mantienen una interrelación para su adecuado funcionamiento.

Como consecuencia del incremento de la variedad de riesgos y la actual crisis ha obligado a los directivos o autoridades de las organizaciones a tener un

acercamiento más profundo al aseguramiento de la información ya que, es importante que las entidades tengan la protección sobre la información en la que se basan las decisiones estas deber ser confiables, seguras y disponible cuando sea requerido. Por lo tanto, con el adecuado control en las tecnologías de la información y comunicación, se lograría el aseguramiento de información lo que facilitaría la evaluación, identificación y monitoreo de los riesgos en las diferentes áreas y así tener una visión más crítica de cómo gestionarlos.

En 1996, la primera edición de COBIT fue publicada. Esta incluía la colección y análisis de fuentes internacionales reconocidas y fue realizada por equipos en Europa, Estados Unidos y Australia. En 1998, fue publicada la segunda edición; su cambio principal fue la adición de las guías de gestión. Para el año 2000, la tercera edición fue publicada y en el 2003, la versión en línea ya se encontraba disponible en el sitio de ISACA. Fue posterior al 2003 que el marco de referencia de COBIT fue revisado y mejorado para soportar el incremento del control gerencial, introducir el manejo del desempeño y mayor desarrollo del Gobierno de TI. En diciembre de 2005, la cuarta edición fue publicada y en Mayo de 2007, se liberó la versión 4.1 que es la que actualmente se maneja. El Marco de Referencia de COBIT 4.1, está conformado por 34 Objetivos de Control de alto nivel, todos diseñados para cada uno de los Procesos de TI, los cuales están agrupados en cuatro grandes secciones mejor conocidos como dominios, estos se equiparán a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear (García, 2011).

En vista de estos continuos cambios, el desarrollo de un Marco de Referencia sobre los objetivos de control para las tecnologías de la información (TI), juntamente con

una investigación continua, constituye una base fundamental para el adecuado desarrollo de las intervenciones de las TI que permitan maximizar el apoyo en cuánto al adecuado aseguramiento de información.

Mesocontextualización

El progreso de las tecnologías de información y comunicación ha sido un punto clave para el avance de la administración pública ya que ha surgido la idea de reemplazar los documentos y trámites burocráticos por las tecnologías de la información y de la comunicación (TIC) y así lograr un mejoramiento en la gestión pública en Ecuador. (Armijos, Enderica, Palomeque, & Berme, 2018). Por lo que en el año 2011 bajo el acuerdo Ministerial Nº571 del 26 de enero del 2011 se creó la subsecretaria de tecnologías de la información cuyo fin era el de contribuir a la modernización de la gestión pública a través de la ejecución, soporte, operación normalización de los proyectos y procesos de innovación tecnológica, posteriormente para el año 2014 se realiza el lanzamiento del primer Plan Nacional de gobierno electrónico y en el año 2018 se declara como política de Estado la mejora regulatoria y la simplificación administrativa y de trámites. (Ministerio de Telecomunicaciones y de la Sociedad de la Información., 2018)

Sin embargo, con el transcurso del tiempo y a pesar de contar con tecnología y plataformas que han permitido el uso de servicios públicos en línea, las actividades que ejerce y regula administración pública se ha ido convirtiendo un tanto complejas debido a la variedad de riesgos a los que pueden estar expuestas las instituciones, así afectando al correcto y eficiente manejo de los recursos público,

por lo que el control interno y la admiración de riesgos ha ido evolucionando a través de distintos planteamientos legales emitidos por el ente regulador que es la Contraloría General del Estado.

A partir de los años 90, eventos ocurridos en el escenario internacional, relacionados con el control interno y con la emisión del informe COSO, también marcaron una etapa importante el desarrollo del control interno en el contexto ecuatoriano (Cedeño & Morell, 2018, pág. 8). Por lo tanto, la Contraloría General del estado en el año 2002 publicó nuevas normas técnicas de control interno basadas en el informe COSO considerándose por primera vez como componente a la evaluación de riesgos.

Posteriormente la Contraloría General del Estado frente a los diferentes cambios en la legislación ecuatoriana debido a la emisión de la nueva Constitución de la República del Ecuador, las reformas a la Ley Orgánica de la CGE y otras disposiciones legales consideró necesario la actualización de las normas de control interno (Cedeño & Morell, 2018). Esta norma señala que "La máxima autoridad, el nivel directivo y todo el personal de la entidad serán responsables de efectuar el proceso de administración de riesgos, que implica la metodología, estrategias, técnicas y procedimientos." (Contraloria General del Estado, 2009)

Además, en esta norma debido al creciente uso de las tecnologías de información consideró la norma 410 para el manejo de las tecnologías de información en donde señala que "La máxima autoridad de la entidad aprobará todos los procesos que permitan a la organización un mejor desempeño sobre el área de las tecnología de

la información asignando adecuado recurso humano y con la infraestructura requerida.” (Contraloria General del Estado, 2009, pág. 69)

Por lo tanto, debido a la modernización en la gestión pública y al crecimiento en los riesgos tecnológicos es importante que las instituciones cuenten controles para el manejo de las tecnologías de información y a más estén preparadas para administrar sus posibles riesgos de esa manera se lograr un manejo adecuado de los recursos públicos asignados.

Microcontextualización

La recategorización del Hospital General Latacunga a Hospital Básico Latacunga, con domicilio en la ciudad de Latacunga, provincia de Cotopaxi, perteneciente al segundo nivel de atención como Hospital Básico, en base a las especificaciones señaladas en el Plan Médico Funcional Aprobado, encontrándose dotado de autonomía presupuestaria, financiera, económica, administrativa y de gestión (IESS, 2020).

El Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2016-2021 pretende ser el instrumento de planificación y gestión del sector de telecomunicaciones y Tecnologías de la Información y Comunicación (TIC) que articule las políticas de desarrollo sectorial e intersectorial en materia de Tecnologías de la Información y Comunicación, para conseguir una mayor inclusión digital y competitividad del país. Su visión es la de ubicar al Ecuador en el año 2021 como un referente regional en conectividad, acceso y producción de los servicios TIC, evidenciado en indicadores que demuestren el desarrollo económico

y social del país (Ministerio de telecomunicaciones y de la sociedad de la información, 2026).

La Gestión de las TI hoy en día es de gran importancia y que ha paso de ser un área de soporte para convertirse en un área de vital importancia en las organizaciones debido a que cada vez estas dependen de la tecnología.

El IESS es una de las entidades públicas más grandes del país, lo cual conlleva que la administración, gestión y control de los servicios, enfocándonos en TI, se vuelva complicado, pero aún más, en un cuello de botella que no permite estar aliado al permanente y cambiante desarrollo de la institución.

A este complicado escenario se suman la falta de guías, personal técnico capacitado, controles adecuados, planes de contingencia para salvaguardar y recuperar la información por distintos eventos que pongan en riesgo la misma, es por ello que se ha convertido en una preocupación constante para el Hospital Básico IESS de Latacunga y más aún para el área financiera ya que constantemente están propensos a múltiples riesgos asociados con los equipos y sistemas de información y comunicaciones por no contar controles de seguridad adecuados.

La Contraloría ha detallado irregularidades o casos de corrupción en los servicios públicos de salud. Sin embargo, los casos no avanzan en la vía penal. Y el Gobierno no ha concretado las correcciones. La Red Pública Integral de Salud está, ahora, en el centro de atención de la Contraloría. Esta Red incluye a los servicios que ofrecen las casas administradas por el Ministerio de Salud Pública, el Instituto Ecuatoriano de Seguridad Social (IESS), el Instituto de Seguridad Social de las Fuerzas Armadas (Issfa) y el Instituto de Seguridad Social de la Policía (Isspol). Estos

nuevos casos de presunta corrupción se suman a los ya conocidos que ocurrieron durante la administración de Ramiro González y María Sol Larrea en el IESS a nivel nacional. Y de Iván Espinel en Guayas (Escobar, 2020).

Como se conoce actualmente Ecuador y específicamente el IESS en los últimos años ha pasado por diversos conflictos por casos de corrupción en los que se ha manipulado la información por la falta de trasparencia en la misma tal como se menciona en el párrafo anterior y la evidente ausencia de controles en las tecnologías de la información que han ocasionado la desconfianza y la vulnerabilidad de información presentada, es por ello la importancia del aseguramiento de la información en todos los niveles de las entidades apoyándose en las buenas prácticas de la tecnología Informática.

1.2.2 Análisis critico

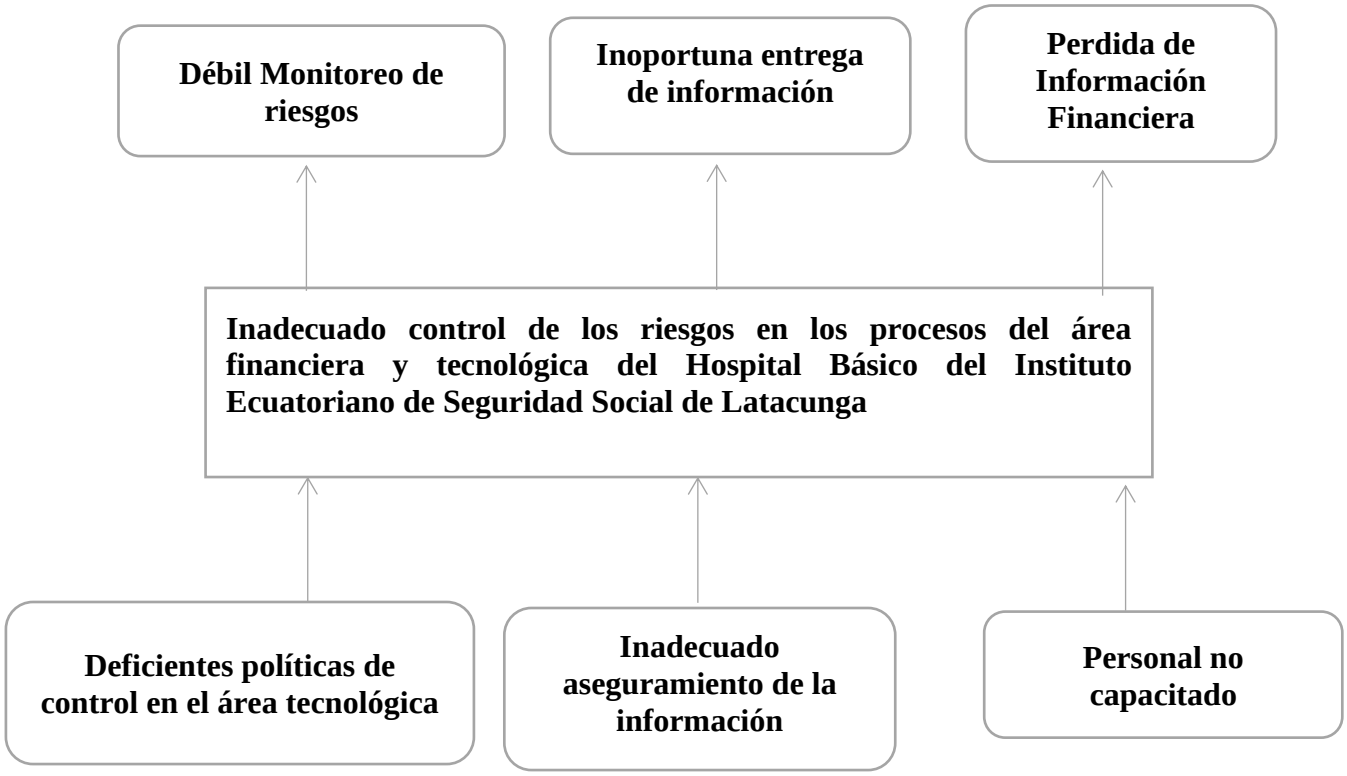


Figura 1: Árbol de Problemas

Elaborado por: Acurio, Y. (2020)

Actualmente el Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga esta pasando por diferentes conflictos para conseguir sus metas, objetivos y un marco de seguridad razonable lo que está ocasionando desconfianza sobre el manejo de los recursos públicos. Conejero (2013) afirma que "la globalización de los problemas públicos y la carencia de estructuras institucionales adecuadas para ofrecerles una solución hace necesario que se incorpore a la toma de decisiones públicas el manejo del riesgo".

La gestión de riesgos en las instituciones es la clave para su adecuado funcionamiento ya que es una herramienta que le permite a las instituciones conocer los riesgos a lo que se enfrenta para poder anticiparse a ellos y tomar acertadas decisiones y lograr que su impacto sea lo menor posible con el fin de defender el cumplimiento de los objetivos institucionales.

Sin embargo, el implantar un sistema de gestión de riesgos no es una tarea fácil debido a que se requiere cada vez mejorar el nivel de aseguramiento de la información, ya que la vulneración de esta incrementaría el riesgo lo cual ocasionaría desconfianza y dudas sobre las decisiones que se toman; para evitar esto se necesita un adecuado manejo de las tecnologías informáticas ya que actualmente son un gran facilitador para el manejo y almacenamiento de información que ingrese al área financiera de la institución de forma electrónica, por lo que se ha convertido también en una herramienta de apoyo para el control y monitoreo de riesgos.

1.2.3 Prognosis

En la actualidad el aseguramiento de la información se ha considerado de vital importancia ya que la tecnología Informática se ha convertido en un gran facilitador, pero también puede presentar riesgos en las diferentes áreas de las entidades que afecten importantemente a las organizaciones, es por ello que el asegurar la información permitirá que la misma no se manipulada o que tenga acceso a personas no autorizadas para el manejo de la misma, siendo que el manejo de información de forma electrónica o digital agilita los procesos de acceso de esta ya que se dispone la información de forma inmediata, agilitando la toma de decisiones.

En el ambiente que se desempeñan las entidades modernas tienen como premisa la incertidumbre, ocasionada por la globalización y los cambios constantes en la tecnología ya que actualmente existe varias amenazas en las tecnologías informáticas y están repartidas en los distintos niveles de las organizaciones es por ello que es de vital importancia establecer metodologías que permitan el monitoreo de los riesgos y de esta manera que sirva como herramienta de vigilancia, proporcionando información que sirva para mejorar la gestión mediante la adecuada administración de los riesgos presentados.

1.2.4 Formulación del Problema

¿Cómo el aseguramiento de la información aporta en el monitoreo de riesgos en el Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga?

1.2.5 Preguntas Directrices

- ¿Cuál es el nivel de aseguramiento de la información en los procesos de TI en Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga?
- ¿Existe monitoreo de riesgo en los procesos del área financiera en Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga?
- ¿Cuál es el aporte del aseguramiento de la información para el monitoreo de riesgos en el proceso del área financiera?

1.2.6 Delimitación del objeto de investigación

Campo: Auditoria
Área: Auditoria de Gestión
Aspecto: Control interno, seguridad de información, COSO ERM, COBIT
D. Temporal: Se desarrollará en el año 2020
D. Espacial: Cantón Latacunga, Provincia Cotopaxi, republica Ecuador
D. Poblacional: El director administrativo del área financiera y de TIC que labora en el Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga

1.3 Justificación

Justificación teórica

Dentro del marco de auditoria el aseguramiento es un fenómeno que está cambiando por completo la teórica y la practica en todo el mundo por lo que se hace necesario buscar su significado. De acuerdo con Mantilla (2015) menciona que: "se refiere al estado de estar asegurado, ya sea como valor, certeza en la mente, confianza en la mente, libertad ante la duda o la incertidumbre, auto-confianza; algo que inspira o intenta inspirar confianza y por ello es sinónimo de confianza." (pág. 4)

Partiendo de las definiciones anteriormente mencionadas se ha llegado al termino de Aseguramiento de la Información que como lo cita Avellaneda es (2010) “es la búsqueda de disponer de la protección de la información mediante diversas actividades operativas sobre sistemas y las redes de la institución con la finalidad de mantener la integridad, confidencialidad, autenticidad y el no repudio ante el impacto que puede tener un riesgo sobre determinado proceso”.

Por ende el aseguramiento de la información en la actualidad es un punto clave para las organizaciones debido a que las empresas públicas y privadas están valorando cada vez más la necesidad de contar con sistemas informáticos que apoyen a su crecimiento, sin embargo, es importante que consideren prepararse para gestionar los posibles riesgos que estén asociados con la implementación de tecnologías, los directivos deben entender los riesgos y limitaciones que conlleva el empleo de las tecnologías de la información y así puedan analizar y establecer controles que les permita asegurar su información y tener la certeza de que sus decisiones fueron tomadas en base a información confiable.

Justificación metodológica

Para apoyar el estudio investigativo sobre el aseguramiento de la información y el monitoreo de riesgos en el Hospital Básico del IESS de Latacunga se consideró el uso del marco de referencia COBIT que es “un modelo de evaluación que permite verificar y llevar un control de los sistemas de información de los negocios y la seguridad. Mediante este modelo, se vincula tecnología, orientado a todos los sectores de una organización.” (Mora, Joffre, Huilcapi, & Escobar, 2017, pág. 7). Por lo tanto, la aplicación de este marco de referencia permitirá conocer el grado de

madurez de los 34 procesos que referencia a la metodología COBIT en el departamento informático del Hospital Básico del IESS.

Para evaluar el monitoreo de riesgos se aplicará la metodología COSO ERM, que como lo cita Sanchez (2015) es un facilitador en la gestión de riesgos ya que permite a los administradores identificar y monitorear los riesgos, para así poder tomar decisiones acertadas que le permitan a las organizaciones operar con más eficacia aumentando su capacidad para afrontar los riesgos.

Justificación practica

La presente investigación es importante porque permitirá al estudiante aplicar modelos de control interno que amplíen su conocimiento sobre su aplicación y pueda apreciar claramente sus diferencias y similitudes; a la Institución le ayudará a conocer su nivel de aseguramiento de información y su efectividad en el monitoreo de riesgos Adicionalmente les permitirá aplicar controles que le favorezcan en la administración de riesgos. El impacto que tendrá esta investigación es que la Institución conozca la efectividad de los procesos en el departamento informático siendo estos gobierno y cultura, estrategia y objetivos, desempeño, evaluación y revisión e información comunicación y reporte, para asegurar la información con el fin de mejorarlos y de esa manera apoyar al monitoreo de riesgos en el departamento financiero, adicionalmente con su aplicación permitirá a la institución administrar los riesgos de TI de mejor manera y ser apoyo para todas las áreas de la institución.

1.4 Objetivos

1.4.1 Objetivo General

Analizar el aseguramiento de la información y el monitoreo de riesgos para el progreso de la gestión de riesgos en Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga en el periodo 2019.

1.4.2 Objetivos Específicos

- Diagnosticar el aseguramiento de la información determinado el grado de madurez de los procesos en referencia a COBIT en el departamento informático del Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga en el periodo 2019.
- Evaluar el monitoreo de riesgos mediante COSO ERM para la efectividad de la administración de riesgos en los procesos del área financiera del Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga en el periodo 2019.
- Contrastar el aseguramiento de la información en el monitoreo de riesgos del área financiera en el Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga en el periodo 2019.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes Investigativos

Para el desarrollo de esta investigación que se enfoca en el aseguramiento de la información y el monitoreo de riesgos en el Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga, se cuenta con algunas perspectivas estudiadas anteriormente por diferentes autores, mostrando que esta temática ha sido abordada y que cuenta con cierto grado de interés, para ser investigada.

La globalización de la economía ha exigido que las empresas implementen plataformas tecnológicas que soporten la nueva forma de hacer negocios. El uso de Internet para este fin, conlleva a que se desarrollen proyectos de seguridad informática que garanticen la integridad, disponibilidad y accesibilidad de la información. Se realizó una revisión bibliográfica en la cual se expone en el trabajo los riesgos, amenazas vulnerabilidades, que afectan a esa información y por ende al sistema (Quiroz & Macías, 2017).

Este documento presenta el análisis de riesgos realizado en un hospital público del Ecuador, que al ser una institución ligada al Estado, manejan información altamente sensible y confidencial. Tomando en cuenta todo esto, se realizó un análisis e identificación de los riesgos a los que está expuesto el Hospital General de Catacocha, a través de su Departamento de Tecnologías de la Información y Comunicación (TIC), para, de esta manera, identificar las vulnerabilidades que pueden atentar contra la seguridad de la información, y elaborar una comparativa que arroje el resultado de los riesgos que se pueden evaluar, logrando así el plan de

gestión que permita mitigar los riesgos, obtener conclusiones y recomendaciones que deben ser implementados en las instituciones, cumpliendo así con los pilares fundamentales de la seguridad de la información (Rivera, Herrera, Naranjo, & Narváez, 2019).

El presente artículo presenta una metodología integral para la gestión de riesgos informáticos basándose en los estándares mundialmente aceptados como son ISO 31000 e ISO/IEC 27005, los mismos que indican los requerimientos para una gestión adecuada de riesgos; sin embargo no indican, al menos de manera clara, como se puede realizar dicha gestión. Por ello se incluyen recomendaciones y buenas prácticas de otros estándares y guías internacionales para el manejo de riesgos. Con la aplicación de la metodología planteada en una empresa industrial de alimentos, se comprueba su validez; además, el equipo de trabajo que aplicó la metodología tuvo a su disposición herramientas sugeridas que ayudaron a valorar técnicamente los riesgos según su probabilidad de ocurrencia, sus consecuencias y dimensiones de seguridad afectadas (Arévalo, Cedillo, & Moscoso, 2017).

Este trabajo, se enfoca en permitir generar argumentos sólidos para identificar cuál es la metodología de análisis de riesgos que proporciona una mejor oportunidad de toma de decisiones dentro de una organización frente a la custodia de la información, la cual se ha convertido en uno de los activos más importantes del ámbito empresarial e implica una adecuada utilización y preservación para garantizar la seguridad y la continuidad del negocio. Existen varias metodologías de análisis de riesgos como: OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30, las cuales se orientan hacia el mismo objetivo, pero tienen

características propias que las hacen atractivas para las empresas en todos los sectores. A partir del estudio, se logra determinar que MAGERIT resulta ser la opción más efectiva y completa ya que protege la información en cuanto a integridad, confidencialidad, disponibilidad y otras características importantes para garantizar la seguridad de los sistemas y procesos de la organización. La aplicación de metodologías de análisis de riesgos es de utilidad a las organizaciones para tener un mayor control sobre sus activos, su valor y las amenazas que pueden impactarlas, obligándolas a implementar medidas de seguridad que garanticen el éxito de sus procesos y una mayor competitividad en el mundo empresarial (Tejena, 2018).

2.2 Fundamentación Filosófica

La investigación critico-propositiva, trabaja con sus propios métodos y herramientas científicas para el abordaje y gestión de los complejos, inciertos e inestables procesos de la Investigación Educativa, donde el marco teórico-epistemológico, exige una metodología con elevada reflexión teórica, que impide que las propuestas desarrolladas, se conviertan en una simple receta que se desploma ante la inestabilidad del contexto actual. Contexto donde la Investigación Cualitativa critico propositiva, como estrategia, adquiere su pertinencia (Vargas & Sabogal, 2017).

El presente trabajo de investigación se encuentra ubicado en el paradigma critico-propositivo ya que privilegia la interpretación, comprensión y explicación de los fenómenos sociales con el fin de contribuir al cambio y el mejoramiento de la aplicación de auditoria.

2.3 Fundamentación Legal

Para fines del presente proyecto se tomó en cuenta los aspectos legales, iniciando con la Constitución del Ecuador Agosto 2008, Sección Tercera, Articulo 212 que seña sobre la función de la Contraloría es "Dirigir todos el sistema que compete al control de la administración en el que toma en cuenta las auditorías internas, externas y de control de las instituciones que forman parte del sector público y de las entidades privadas que dispongan de recursos públicos." (Asamblea Nacional del Ecuador , 2008)

En segundo lugar, se debe mencionar la Ley de la Contraloría General de Estado que en el artículo 5 expone "Cada institución del Estado asuma la responsabilidad por la existencia y mantenimiento de su propio sistema de control interno" (Contraloria General del Estado , 2002)

Finalmente, se debe mencionar a las normas de control interno de la Contraloría General del Estado que señala "La máxima autoridad establecerá los mecanismos necesarios para identificar, analizar y tratar cada uno de los riesgos que se pueden presentar durante el proceso del cumplimiento de los objetivos" (La Contraloria General del Estado , 2009)

Artículo 26.- Políticas de información, comunicación y difusión.- El Órgano Máximo de Gobierno del IESS expedirá las políticas generales de información, comunicación y difusión, entre ellas las relacionadas con el estado financiero institucional, el nivel de riesgos asumidos por la entidad, las acciones de control e implementación de recomendaciones, gestión transparente, reclamos y aplicación del Código de Ética (Código de gobierno corporativo del instituto ecuatoriano de seguridad social, 2012).

Artículo 8.- Principio de Responsabilidad.- Los colaboradores del Instituto Ecuatoriano de Seguridad Social IESS serán responsables de las acciones u omisiones relativas al ejercicio de sus cargos, actuarán con claro concepto del deber y de la responsabilidad en el cumplimiento de las actividades a ellos encomendadas. Es deber y obligación de los colaboradores del IESS, responder sobre la forma en que cumplen sus obligaciones y encargos. Además, garantizará la exactitud de la información que maneja y proporciona, la cual estará respaldada documentadamente (Código de ética del instituto ecuatoriano de seguridad social, 2012).

Artículo 9.- Principio de Confidencialidad.- Los colaboradores del Instituto Ecuatoriano de Seguridad Social IESS, estarán obligados a guardar reserva sobre los documentos, hechos e información a que tienen acceso y conocimiento en razón del ejercicio del cargo, según lo que dispone la Ley Orgánica de Transparencia y Acceso a la Información Pública (Código de ética del instituto ecuatoriano de seguridad social, 2012).

Que, el Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, expedido mediante Resolución C.D. 535, vigente a partir del 6 de mayo de 2017, publicado en el Registro Oficial Edición Especial No. 5 de 01 de junio de 2017, reformado con Resolución No. C.D. 553, publicada en Registro Oficial Suplemento No. 59, de 16 de agosto de 2017; y, Resolución C.D. 583, publicada en Registro Oficial No. 511, de 18 de junio de 201, establece la estructura organizacional de la Institución, procesos gobernantes, procesos sustantivos, adjetivos de asesoría y de apoyo, con las responsabilidades y funciones de los

diversos órganos de gestión, operativa y de apoyo administrativo entre otras, de la Dirección Nacional de Tecnologías de la Información;

La Unidad de Tecnología de Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran (Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, 2019).

Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información (Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, 2019).

Será necesario establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización. Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos. Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos

(Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, 2019).

La Unidad de Tecnología de Información deberá promover y establecer convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como de programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con la tecnología de información" (Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, 2019).

POLÍTICAS QUE REGULAN USO DE TECNOLOGÍAS DE LA INFORMACIÓN

Art. 1.- Finalidad.- Las Políticas de Tecnología de la Información y Comunicación, tienen como finalidad el proteger la información, a la Institución y buscar un aumento en la seguridad y aprovechamiento de la tecnología, lo que contribuye de manera determinante a aumentar la efectividad en el trabajo y garantizar la continuidad de las operaciones de la Institución (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

Art. 2.- Ámbito.- Las Políticas de Tecnología de la Información y Comunicación serán aplicadas de manera obligatoria por las y los funcionarios, servidores y trabajadores que integran el IESS a nivel nacional, que utilicen el hardware, software y comunicaciones, para el cumplimiento de sus actividades diarias. La Dirección Nacional de Tecnologías de la Información, será la encargada de administrar y ejecutar estas políticas a través de procedimientos, asimismo las políticas deben cumplirse a nivel nacional por las dependencias que tienen a su

cargo el uso de recursos tecnológicos de forma desconcentrada. La Subdirección Provincial de Apoyo a la Gestión Estratégica, representará a la Dirección Nacional de Tecnologías de la Información en las Direcciones Provinciales del IESS a nivel nacional y, será la responsable de velar por el cumplimiento de estas políticas (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

Art. 3.- Recursos Tecnológicos.- Las Políticas de Tecnología de la Información, regularán y estandarizarán el uso de los recursos informáticos que el IESS pone a disposición de todo el personal para desarrollar sus actividades y cumplir con la misión de la Institución (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

Art. 8.- Propiedad de la información.- Los usuarios que tengan asignados cualquier equipo de cómputo del IESS deben estar informados, que los datos que ellos generan y manipulan en los sistemas de información y cualquier medio de procesamiento electrónico, durante el desarrollo normal de sus actividades laborales, son de propiedad y responsabilidad del IESS, para lo cual se respetará lo siguiente: 1. Los derechos patrimoniales de un sistema de información y de ofimática creados por uno o varios servidores en el ejercicio de sus actividades laborales corresponden al IESS. 2. Los usuarios que tengan asignado un equipo de cómputo del IESS, deberán respaldar la información, y, debiendo entregarlos al jefe inmediato al finalizar su relación laboral con la institución, mediante la respectiva acta de entrega recepción (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

TÍTULO V POLÍTICA DE USO DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN

Art. 19.- Lineamientos Generales.- Las y los usuarios internos cumplirán las siguientes recomendaciones: 1. El equipo informático debe estar configurado para que se bloquee automáticamente, cuando se detente inactividad a un tiempo determinado, es responsabilidad del usuario interno el bloquear su equipo de trabajo cuando este abandone su lugar de trabajo. 2. No modificar las configuraciones de dirección IP, DNS, hora, nombre de equipos y demás. En caso de requerir un cambio deberán notificar a los técnicos informáticos de su dependencia. 3. No modificar las configuraciones del equipo como fondo de pantalla y protector de pantalla, así como la configuración de software y hardware establecidos por la Dirección Nacional de Tecnologías de la Información. Si en su equipo se han realizado modificaciones, debe notificar a los técnicos informáticos de su dependencia, para que se realice la re-configuración del mismo. 4. Está prohibido instalar aplicaciones, programas, utilitarios, que no sean aprobados por su línea de supervisión o que difieran del software base determinado por la Dirección Nacional de Tecnologías de la Información, que no tengan licencias o que para su uso se deba romper la seguridad de licenciamiento del mismo. 5. En caso de funcionarios y/o servidores que tengan a su cargo computadores portátiles, estos deberán permanecer con el candado de seguridad durante todo el tiempo que el computador esté sin supervisión de dichos funcionarios y/o servidores. En caso de no disponer del candado, se deberá gestionar la adquisición del mismo a través de la Dirección o Unidad Administrativa a la que pertenece. 6. Para evitar pérdida de información, la o el usuario es responsable de respaldar su máquina periódicamente en medios

magnéticos externos y verificar que los respaldos generados se encuentren disponibles, e íntegros para su uso de ser requerido. 7. No pueden moverse los equipos o reubicarlos sin permiso. En caso de que necesite movilizar un equipo fuera de la Institución se requiere autorización del Director o titular de la Dependencia por escrito. 8. Está prohibido poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios y/o dañar o alterar los recursos informáticos. 9. Todo el personal que accede a los sistemas de información del IESS debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de uso. 10. Todo el personal del IESS, de acuerdo a su competencia deberá cumplir los lineamientos y directrices de seguridad informática emitidos por la Dirección Nacional de Tecnologías de la Información y bajo el amparo de seguridad de la información de la Dirección Nacional de Riesgos Institucionales (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

Art. 20.- Compromiso de Confidencialidad.- Las y los servidores de la institución deberán firmar compromisos de confidencialidad y de no-divulgación de información de conformidad con lo dispuesto en la Constitución de la República del Ecuador, las leyes y las necesidades de protección de información de la institución. La Subdirección Nacional de Gestión de Talento Humano será la encargada de controlar que los compromisos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción, gestionar la custodia de los compromisos firmados, en los expedientes, físicos o electrónicos, de cada funcionario y/o servidor, y controlar que la firma de los compromisos de confidencialidad sean parte de los procedimientos de incorporación de nuevos

funcionarios y/o servidores a la institución, sin excepción. El personal de otras entidades públicas o privadas; deberán de igual manera suscribir el compromiso de confidencialidad previo a acceder a la información (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

Art. 21.- Responsables de la seguridad informática.- La Dirección Nacional de Tecnologías de la Información y las áreas informáticas de las dependencias administrativas y médicas serán los responsables de los activos tecnológicos bajo su custodia, y los responsables de la seguridad de la información serán las dependencias del IESS, considerando los lineamientos y/o políticas emitidas por la Dirección Nacional de Riesgos Institucionales (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

Art. 22.- Responsables de la Información.- Los responsables de la información son definidos para asegurar adecuadamente la pertenencia, custodia y salvaguarda de los activos de la información, teniendo en cuenta una correcta segregación de funciones, que se diferencian entre: a) Responsables Directos: Los Responsables Directos de la información son aquellos que por la naturaleza de su posición en la Institución conocen el tipo de información que se genera o comunica o ingresen en los diversos sistemas o aplicativos, pueden ser las Gerencias, Seguros Especializados, Direcciones Nacionales, Direcciones Provinciales, Jefaturas o aquellos designados por el Director General o su delegado para dicha actividad, son responsables de: - La clasificación directa de la información, de la organización y autorización del acceso a la información. - Manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso. - Monitoreo del uso de

la información por parte de personal a su cargo - Asignar a los responsables del uso y manejo de la información. b) Monitorear el uso de la información por parte de los Responsables Directos: Los Responsables Directos de la información por tener una relación directa en el manejo de la información serán responsables de monitorear el uso que le dé el personal a su cargo. c) Responsables Secundarios: Los Responsables Secundarios de la información son aquellos que por la naturaleza de su cargo en la organización deben acceder, modificar o almacenar información. Son responsables de: - Manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso. d) Custodios: Los Custodios de la información son aquellos que por la naturaleza de su cargo en la organización deben custodiar, respaldar o almacenar la información. Se convierten en custodios el personal que tenga acceso a bases de información. Entre sus responsabilidades constan: - El manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso. - Mantener la disponibilidad e integridad de la información custodiada. - Mantener el acceso y permisos de acceso a la información custodiada. - Brindar soporte para evaluar e identificar la información para su clasificación (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

Art. 23.- Clasificación de la Información.- Los Responsables Directos de la información deberán clasificar adecuadamente la información que manejan y deben asegurarse de que se respete el acceso a la misma por parte del personal a su cargo considerando los lineamientos y/o políticas emitidas por la Dirección Nacional de Riesgos Institucionales (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

Art. 24.- Almacenamiento.- La información obtenida de cualquiera de los servicios y que sea almacenada localmente en el equipo de cómputo del usuario y de propiedad institucional, no podrá ser distribuida o transmitida por la red institucional, o por otros medios de comunicación sin la autorización del inmediato superior. La Dirección Nacional de Tecnologías de la Información revisará el aprovechamiento óptimo de los recursos compartidos en la red para mantener la integridad y para asegurar que los usuarios utilicen los recursos de manera responsable (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

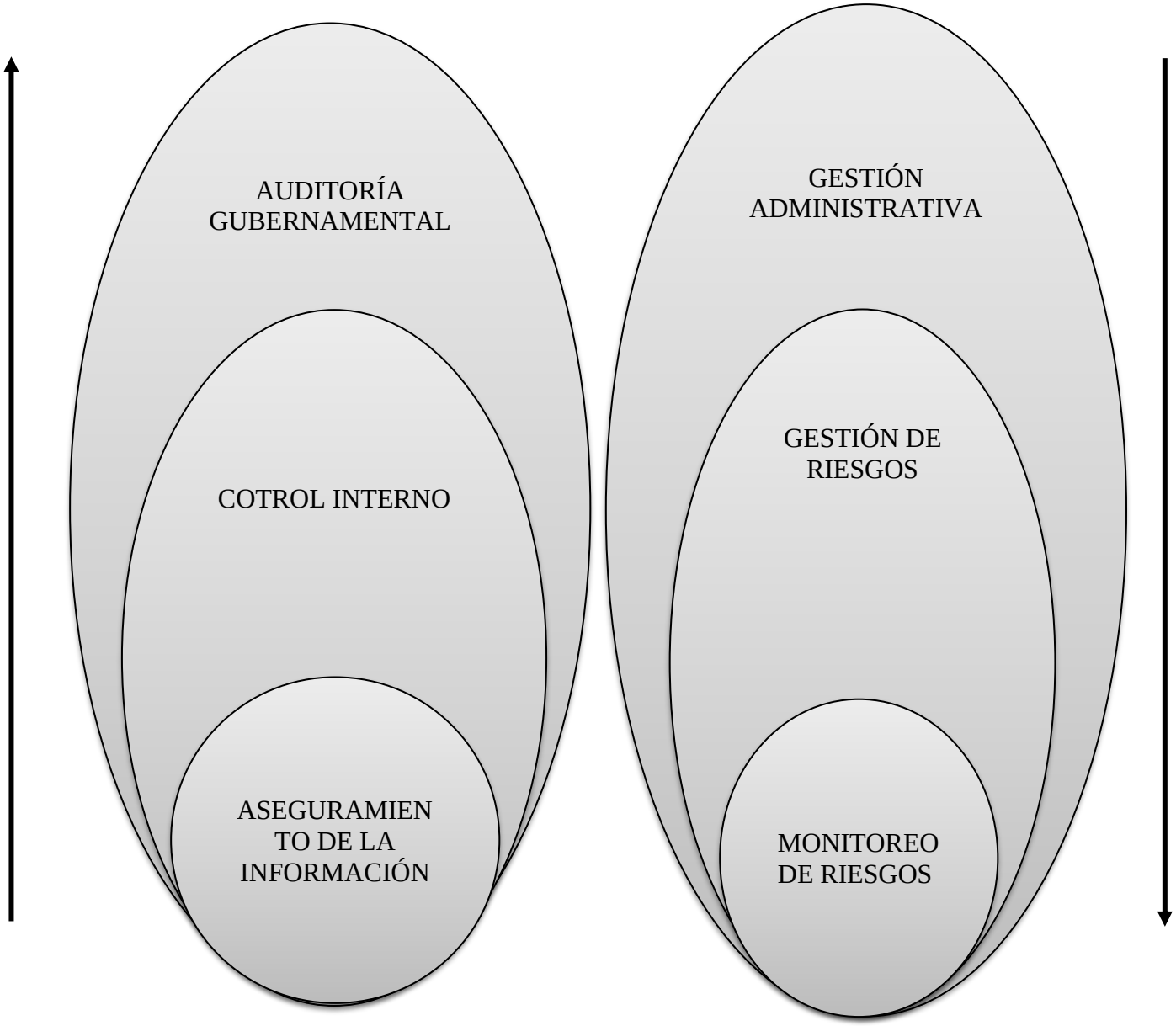
Art. 25.- Transmisión de datos.- A fin de garantizar la integridad y confidencialidad de la información obtenida de los sistemas y aplicativos informáticos de la institución y en razón de que los dispositivos móviles, magnéticos y los soportes extraíbles generan vulnerabilidades como divulgación no autorizada de datos, robo de datos, datos dañados o comprometidos, por la facilidad de uso, alta movilidad y capacidad de almacenamiento, la Dirección Nacional de Tecnologías de la Información y la respectiva Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial, de forma programada y bajo pedido de las unidades administrativas, procederá a salvaguardar la información que mantiene la institución, proporcionando el mecanismo tecnológico de encriptación y desencriptación a la correspondiente Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial. Las unidades administrativas de forma programada y bajo pedido solicitarán a la respectiva Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial, la encriptación y/o desencriptación de la

información digital (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

Art. 26.- Propiedad y Derechos de contenidos.- La información disponible en Internet, incluyendo textos, software, música, sonido, fotografía, video, gráficos u otro material contenido, está protegida por copyright, marcas registradas, patentes u otros derechos de propiedad y leyes. Sólo se permite el uso de este material bajo autorización expresa del autor. El bajar, cargar, archivar, copiar, imprimir o enviar cualquier material debe ser realizado solamente bajo la autorización del autor. Los usuarios no deben descargar ni instalar ningún tipo de software comercial, shareware o freeware en las unidades de disco o en cualquier disco, sin la autorización de los técnicos informáticos de cada dependencia (Políticas Que Regulan Uso De Tecnologías De La Información Del IESS, 2020).

En conclusión, podemos decir que el presente proyecto tiene la suficiente base legal para fundamentar y respaldar la realización del trabajo

2.4 Categorías Fundamentales



VARIABLE INDEPENDIENTE **VARIABLE DEPENDIENTE**

Figura 2: Red de Categorías conceptuales
Elaborado por: Acurio, Y. (2020)

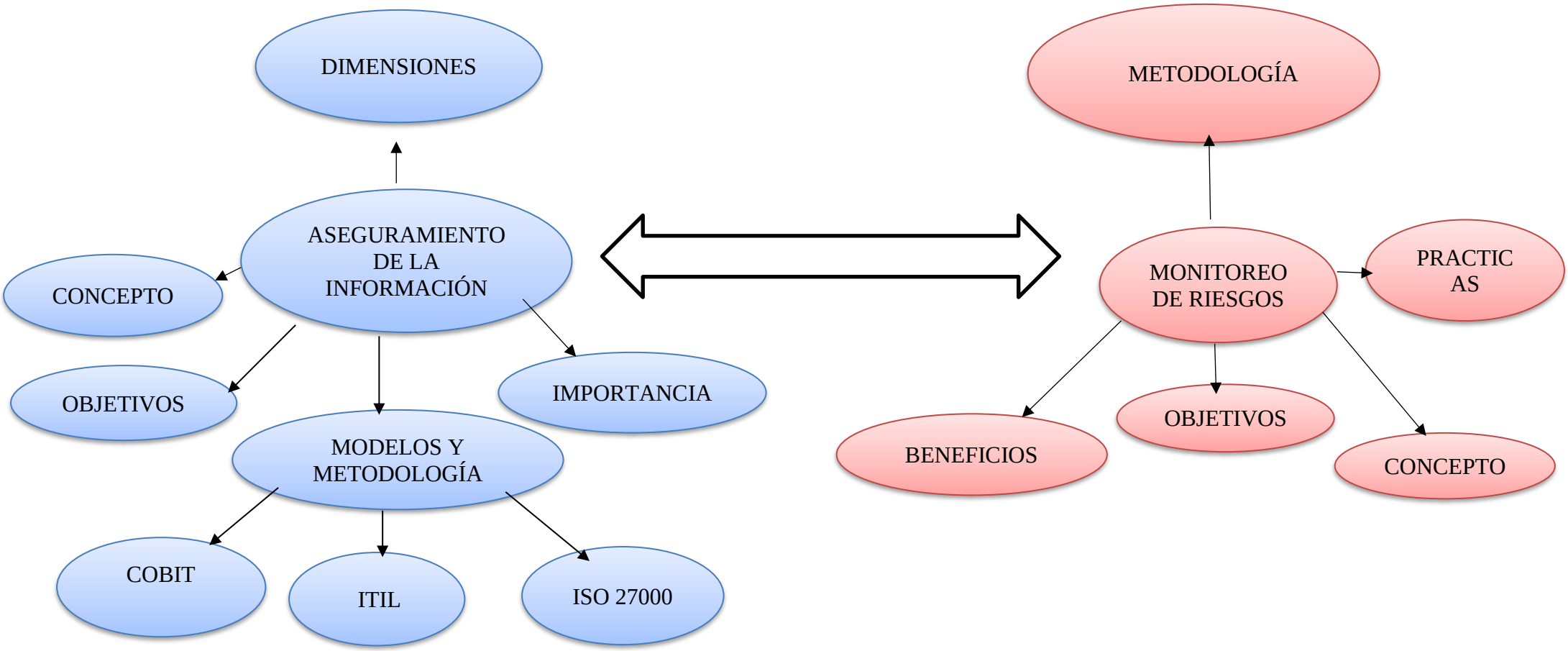


Figura 3: Constelación de ideas variable
Elaborado por: Acurio, Y. (2020)

2.4.1 Conceptualización de la variable Independiente

2.4.1.1 Auditoria Gubernamental

La auditoría gubernamental es aquella clase especial de auditoría que se enmarca en el proceso a través del cual el Estado desarrolla su función de control a fin de asegurar el correcto, transparente, y eficiente empleo y gestión de los bienes y recursos públicos. El control gubernamental es definido como la supervisión, vigilancia y verificación de los actos y resultados de la gestión pública en relación con la eficiencia, eficacia, transparencia, y economía en el uso y destino de los recursos y bienes del Estado, así como del cumplimiento de las normas legales, de lineamiento de políticas y de los planes de acción mediante la evaluación de los sistemas de administración y control con fines de mejorarlos a través de la adopción de acciones preventivas y correctivas (Dextre, 2016).

Objetivos de la Auditoria Gubernamental

La Auditoria Gubernamental tiene como objetivo General analizar cómo se está empleando los recursos públicos que una determinada Institución tiene asignada, sin embargo, la Contraloría General del Estado (2003) cita los siguientes objetivos específicos de la auditoria gubernamental.

a) Evaluarla efectividad económica y el óptimo manejo de todos los recursos financieros, humanos, tecnológicos y de tiempo.
b) Valorara el desempeño que conlleva al desarrollo de las metas y objetivos establecidos para la presentación de servicios o la producción de bienes, por los entes y organismos de la administración pública y de las entidades

privadas, que controla Contraloría, e identificar y de ser posible, cuantificar el impacto en la comunidad de las operaciones examinadas.

c) Dictaminar la razonabilidad de las cifras que constan en los estados de: Situación Financiera, Resultados, Ejecución Presupuestaria, Flujo del efectivo y Ejecución del Programa Periódico de Caja, de conformidad con los principios de contabilidad generalmente aceptados, las normas ecuatorianas de contabilidad y, en general, la normativa de contabilidad vigente.
d) Ejercer con eficiencia el control sobre los ingresos y gastos públicos.
e) Verificar el cumplimiento de las disposiciones constitucionales, legales, reglamentarias y normativas aplicables en la ejecución de las actividades desarrolladas por los entes públicos y privados que controla Contraloría General del Estado.
f) Propiciar el desarrollo de sistemas de información, de los entes públicos y privados que controla Contraloría, como una herramienta para la toma de decisiones y para la ejecución de la auditoria.
g) Formular recomendaciones dirigidas a mejorar el control interno, contribuir al fortalecimiento de la gestión institucional y promover su eficiencia operativa y de apoyo.

Características

La Contraloría General del Estado (2003) cita como características de la Auditoria Gubernamental las siguientes:

- Objetiva, ya que el auditor revisa hechos reales sustentados en evidencias susceptibles de comprobarse, siendo una condición fundamental que el auditor sea independiente e esas actividades.
- Sistemática, porque su realización es adecuadamente planificada y está sometida a las normas profesionales y al código de ética profesional.
- Profesional, porque es ejecutada por auditores o contadores públicos a nivel universitario o equivalentes, o equipos multidisciplinarios según la modalidad o tipo de auditoría y examen especial, que poseen capacidad, experiencia y conocimientos en el área de auditoría gubernamental, quienes deben emitir un informe profesional dependiendo del tipo de auditoría de la que se trate.
- Selectiva, porque su ejecución se basa en pruebas selectivas, técnicamente sustentadas.
- Imparcial, porque es ejecutada por auditores que actúen con criterio imparcial y no tienen conflicto de intereses respecto de las actividades y personas objeto y sujeto de examen.
- Integral porque cubre la revisión de las actividades operativas, administrativas, financieras y ecológicas, incluye los resultados de las evaluaciones de control interno, la legalidad de los actos administrativos, actos normativos y actos contractuales.
- Recurrente, porque el ejercicio de la auditoria gubernamental se ejecuta en forma periódica.

Proceso de la Auditoría Gubernamental

La Contraloría General del Estado (2003) divide en tres fases a la auditoria gubernamental.

- Planificación de la Auditoría

  Esta fase se fundamenta en la planificación anual de control de las entidades y a su vez comprende la Planificación Preliminar, que consiste en obtener y de ser necesario actualizar toda la información de la institución a través de la revisión documental (Contraloria General del Estado, 2003).

- Ejecución del Trabajo

  En la fase propuesta se procede a la aplicación de los procesos que se han detallado en el programa de auditoría, es importante desarrollar todos los hallazgos que representan significancia en el área y que se consideran críticos. (Contraloria General del Estado, 2003).

- Comunicación de Resultados

  La comunicación de resultados es cumplida en la ejecución del examen pese a ser la última fase de la auditoría, se lo realiza a los funcionarios de la entidad verbal y escrita de los hallazgos (Contraloria General del Estado, 2003).

Clases de Auditoría

La Contraloria General del Estado (2003) en la publicación de su Ley Orgánica clasifica a la Auditoria Gubernamental de la siguiente manera:

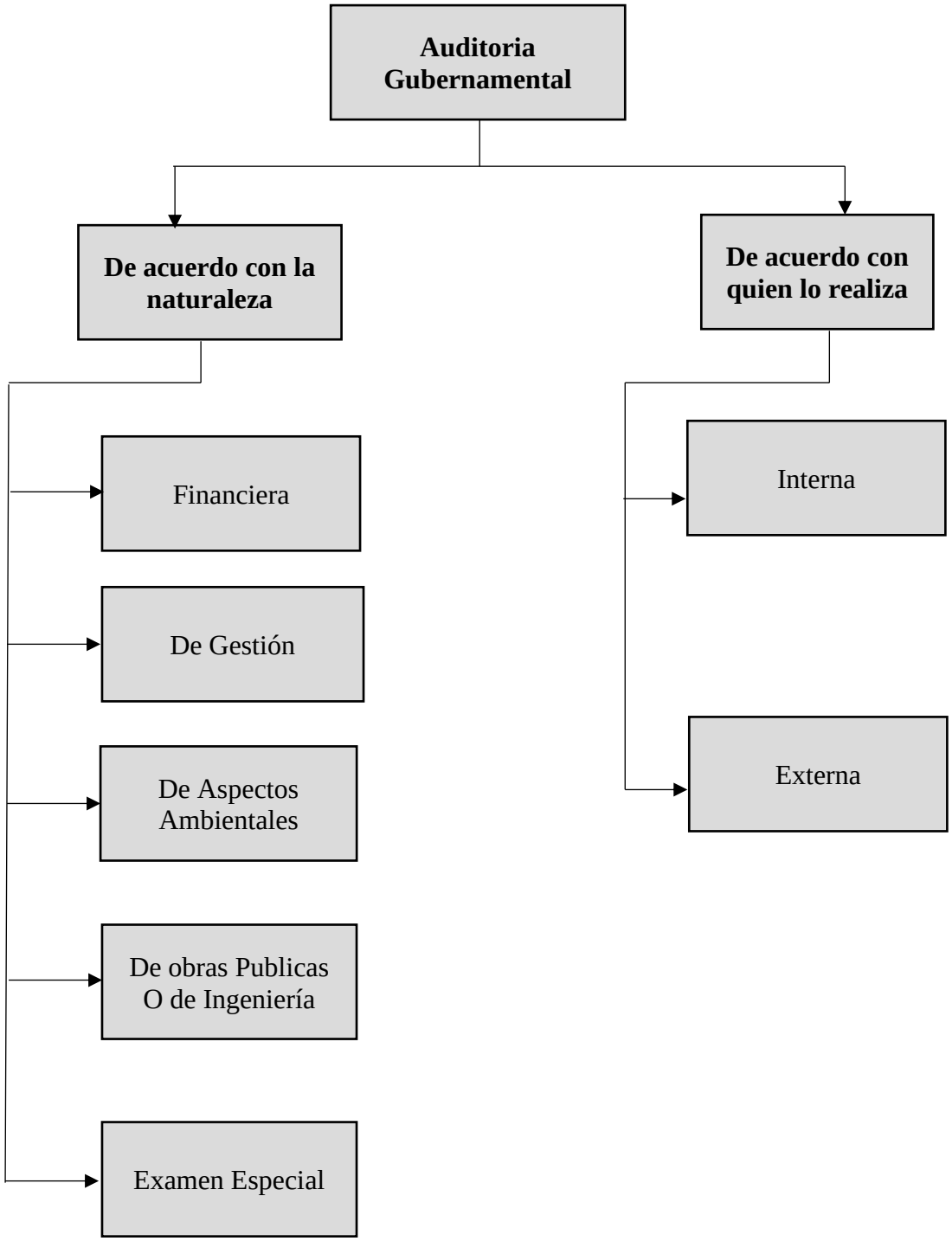


Figura 4: Clases de Auditoría Gubernamental
Fuente de cosnulta: Manual de Auditoria Gubernamental, (2003)

La Contraloria General del Estado (2003) señala que es:

> La acción fiscalizadora está encaminada a examinar para proceder a la evaluación del control interno con la participación del capital humano, el desempeño de la empresa, entidades contables y la ejecución de programas y proyectos para de este modo verificar si el proceso que

> se está llevando a cabo tiene concordancia con los principios de economía, eficiencia y efectividad.

Por lo tanto, la auditoria de gestión es un examen de eficiencia y eficacia con la que administran los recursos asignados a cierta institución.

Objetivos

La Contraloria General del Estado (2001) cita a los siguientes objetivos:

- Promover la optimización de los niveles de eficiencia, eficacia, economía, calidad e impacto de la gestión pública.
- Determinar el grado de cumplimiento de los objetivos y metas.
- Verificar el manejo eficiente de los recursos.
- Promover el aumento d la productividad, procurando la correcta administración del patrimonio público.
- Satisfacer las necesidades de la población.

Propósitos

La Contraloria General del Estado (2001) señala como propósitos de la auditoria de gestión a los siguientes:

- Determinar si todos los servicios prestados, obras y bienes entregados son necesarios y, si es necesario desarrollar nuevos; así como, efectuar sugerencias sobre formas más económicas de obtenerlos.
- Determinar lo adecuado de la organización de la entidad; la existencia de objetivos y planes coherentes y realistas; la existencia y cumplimiento de políticas adecuadas; la existencia y eficiencia de métodos y procedimientos adecuados; y, la confiabilidad de la información y de los controles establecidos.

- Comprobar si la entidad adquiere, protege y emplea sus recursos de manera económica y eficiente y si se realizan con eficiencia sus actividades y funciones.
- Cerciorarse si la entidad alcanzó los objetivos y metas previstas de manera eficaz y si son eficaces los procedimientos de operación y de controles internos, y,
- Conocer las causas de ineficiencias o practicas antieconómicas.

Enfoque

La Contraloría del Ecuador se proyecta a la ejecución de auditorías de gestión con un enfoque Integral, por lo tanto, se concibe como una Auditoría de Economía y Eficiencia, una Auditoría de Eficacia y una Auditoría de tipo Gerencial-Operativo y de Resultados. (Contraloria General del Estado, 2001, pág. 43)

2.4.1.2 Control interno

Según el Ministerio de Finanzas del Ecuador (2017) las Normas 100-01, 300-01,300-02, 300-03 y 300-04 de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de recursos públicos, las mismas que se citan a continuación.

- 100-01 Control Interno El control interno será responsabilidad de cada institución del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos y tendrá como finalidad crear las condiciones para el ejercicio del control. El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos. Constituyen

componentes del control interno el ambiente de control, la evaluación de riesgos, las actividades de control, los sistemas de información y comunicación y el seguimiento. El control interno está orientado a cumplir con el ordenamiento jurídico, técnico y administrativo, promover eficiencia y eficacia de las operaciones de la entidad y garantizar la confiabilidad y oportunidad de la información, así como la adopción de medidas oportunas para corregir las deficiencias de control.

- 300 EVALUACIÓN DEL RIESGO.- La máxima autoridad establecerá los mecanismos necesarios para identificar, analizar y tratar los riesgos a los que está expuesta la organización para el logro de sus objetivos. El riesgo es la probabilidad de ocurrencia de un evento no deseado que podría perjudicar o afectar adversamente a la entidad o su entorno. La máxima autoridad, el nivel directivo y todo el personal de la entidad serán responsables de efectuar el proceso de administración de riesgos, que implica la metodología, estrategias, técnicas y procedimientos, a través de los cuales las unidades administrativas identificarán, analizarán y tratarán los potenciales eventos que pudieran afectar la ejecución de sus procesos y el logro de sus objetivos.
- 300-01 Identificación de riesgos Los directivos de la entidad identificarán los riesgos que puedan afectar el logro de los objetivos institucionales debido a factores internos o externos, así como emprenderán las medidas pertinentes para afrontar exitosamente tales riesgos. Los factores externos pueden ser económicos, políticos, tecnológicos, sociales y ambientales. Los internos incluyen la infraestructura, el personal, la tecnología y los procesos.

Es imprescindible identificar los riesgos relevantes que enfrenta una entidad en la búsqueda de sus objetivos. La identificación de los riesgos es un proceso interactivo y generalmente integrado a la estrategia y planificación. En este proceso se realizará un mapa del riesgo con los factores internos y externos y con la especificación de los puntos claves de la institución, las interacciones con terceros, la identificación de objetivos generales y particulares y las amenazas que se puedan afrontar. Algo fundamental para la evaluación de riesgos es la existencia de un proceso permanente para identificar el cambio de condiciones gubernamentales, económicas, industriales, regulatorias y operativas, para tomar las acciones que sean necesarias. Los perfiles de riesgo y controles relacionados serán continuamente revisados para asegurar que el mapa del riesgo siga siendo válido, que las respuestas al riesgo son apropiadamente escogidas y proporcionadas, y que los controles para mitigarlos sigan siendo efectivos en la medida en que los riesgos cambien con el tiempo.

- 300-02 Plan de mitigación de riesgos Los directivos de las entidades del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos, realizarán el plan de mitigación de riesgos desarrollando y documentando una estrategia clara, organizada e interactiva para identificar y valorar los riesgos que puedan impactar en la entidad impidiendo el logro de sus objetivos. En el plan de mitigación de riesgos se desarrollará una estrategia de gestión, que incluya su proceso e implementación. Se definirán objetivos y metas, asignando responsabilidades para áreas específicas, identificando conocimientos

técnicos, describiendo el proceso de evaluación de riesgos y las áreas a considerar, detallando indicadores de riesgos, delineando procedimientos para las estrategias del manejo, estableciendo lineamientos para el monitoreo y definiendo los reportes, documentos y las comunicaciones necesarias. Los directivos de las entidades del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos, desarrollarán planes, métodos de respuesta y monitoreo de cambios, así como un programa que prevea los recursos necesarios para definir acciones en respuesta a los riesgos. Una adecuada planeación de la administración de los riesgos, reduce la eventualidad de la ocurrencia y del efecto negativo de éstos (impacto) y alerta a la entidad respecto de su adaptación frente a los cambios.

- 300-03 Valoración de los riesgos La valoración del riesgo estará ligada a obtener la suficiente información acerca de las situaciones de riesgo para estimar su probabilidad de ocurrencia, este análisis le permitirá a las servidoras y servidores reflexionar sobre cómo los riesgos pueden afectar el logro de sus objetivos, realizando un estudio detallado de los temas puntuales sobre riesgos que se hayan decidido evaluar. La administración debe valorar los riesgos a partir de dos perspectivas, probabilidad e impacto, siendo la probabilidad la posibilidad de ocurrencia, mientras que el impacto representa el efecto frente a su ocurrencia. Estos supuestos se determinan considerando técnicas de valoración y datos de eventos pasados observados, los cuales pueden proveer una base objetiva en comparación con los estimados. La metodología para analizar riesgos puede variar, porque

algunos son difíciles de cuantificar, mientras que otros se prestan para un diagnóstico numérico. Se consideran factores de alto riesgo potencial los programas o actividades complejas, el manejo de dinero en efectivo, la alta rotación y crecimiento del personal, el establecimiento de nuevos servicios, sistemas de información rediseñados, crecimientos rápidos, nueva tecnología, entre otros. La valoración del riesgo se realiza usando el juicio profesional y la experiencia.

2.4.1.3 Aseguramiento de la Información

Se define como la aplicación de varias actividades operativas cuya finalidad es la de proteger la información de una empresa así como también las redes y los sistemas de información, buscando siempre conservar la disponibilidad, confidencialidad y veracidad de la información (Avellaneda, 2010).

Proponer, implementar y administrar políticas, normas y procedimientos que optimicen la gestión y administración de las tecnologías de la información y comunicaciones (TIC's), garantizando la integridad de la información, optimización de recursos, sistematización y automatización de los procesos institucionales, así como el soporte tecnológico institucional (Ministerio de Salud Pública, 2019).

Importancia

El aseguramiento de la información es muy importante debido a que es la base para la adecuada y oportuna toma de decisiones de una empresa; hay que considerar que sin aseguramiento las entidades pierden credibilidad de información donde se baso para la toma de decisiones (Avellaneda, 2010)

Objetivo

Como menciona anteriormente el concepto de auditoria de gestión en el cual se examina la gestión de varios factores según el área o departamento a evaluar y el tipo de auditoria a realizar pudiendo ser esta contable, de desempeño del personal, etc. en el caso de las tecnologías de la información y comunicación se analiza la gestión de la información de tipo digital o electrónica y como se procesa dicha información para garantizar su acceso a las personas autorizadas evitando la vulnerabilidad de dicha información.

El aseguramiento de la información tiene como objetivo principal proteger los datos de las empresas basándose en los siguientes aspectos: la confidencialidad, la disponibilidad y la integridad (Avellaneda, 2010)**.**

Dimensiones

Integridad

La integridad hace referencia a que la información esté accesible cuando se la necesitemos. (Instituto Nacional de ciberseguridad, 2018)

Confidencialidad

La confidencialidad hace referencia a que la información sea correcta y esté libre de modificaciones y errores (Instituto Nacional de ciberseguridad, 2018).

Disponibilidad

La disponibilidad implica que la información es accesible únicamente por el personal autorizado (Instituto Nacional de ciberseguridad, 2018).

Modelos y metodologías

COBIT

Es una guía o modelo para realizar auditorías de la gestión y control de los sistemas de información y tecnología, orientado a los departamentos informáticos de una organización, es decir a los auditores involucrados en el proceso. Las principales características del Sistema COBIT, están orientadas al negocio u organización, pueden ser utilizadas por los usuarios y a su vez por los auditores, como una lista de verificación minuciosa para los encargados de cada proceso, este sistema está formado con estándares de control y auditoria (COSO), basado en una observación crítica y analítica de las actividades en las TI (Santacruz, Vega, Pinos, & Cárdenas, 2017).

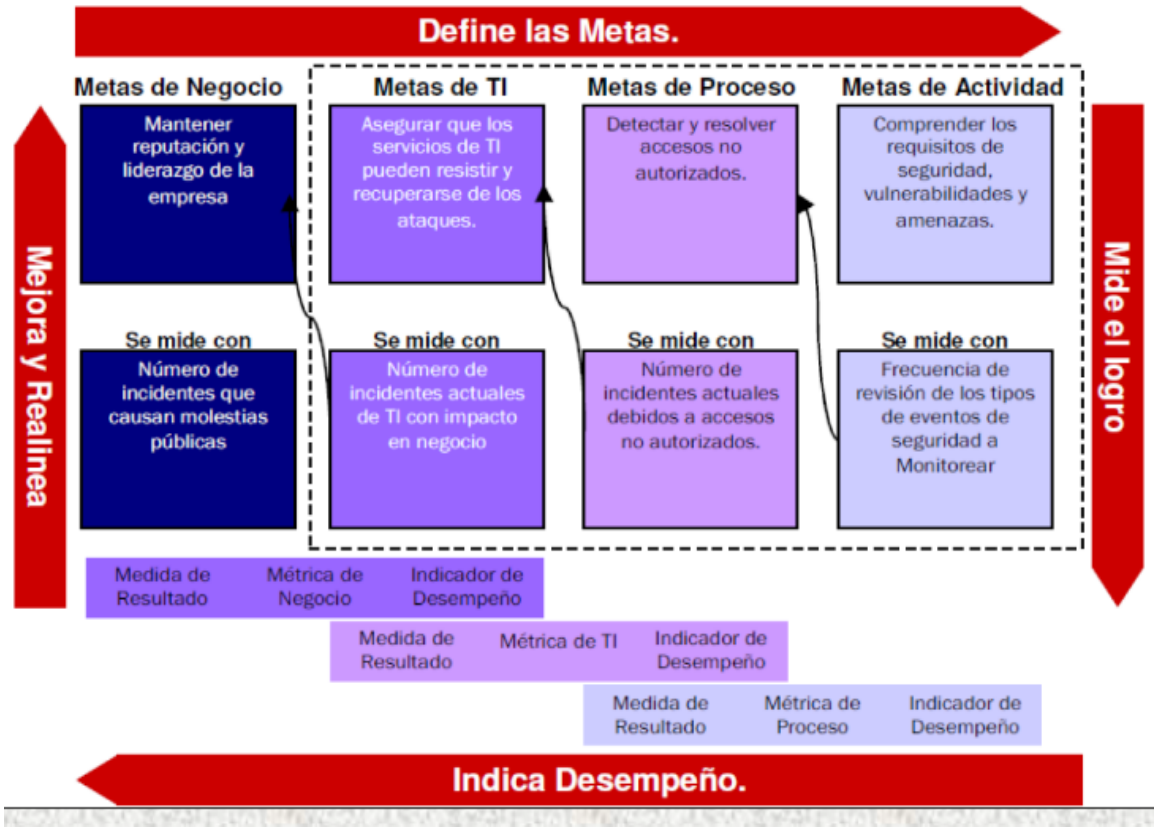


Figura 5: Diagrama misión de Cobit
Fuente de Consulta: IT Governance Institute (2007)

El marco referencial de COBIT usualmente se enfoca en tres puntos clave:

- Criterios de información
- Recursos de tecnología de información
- Procesos de tecnología de información

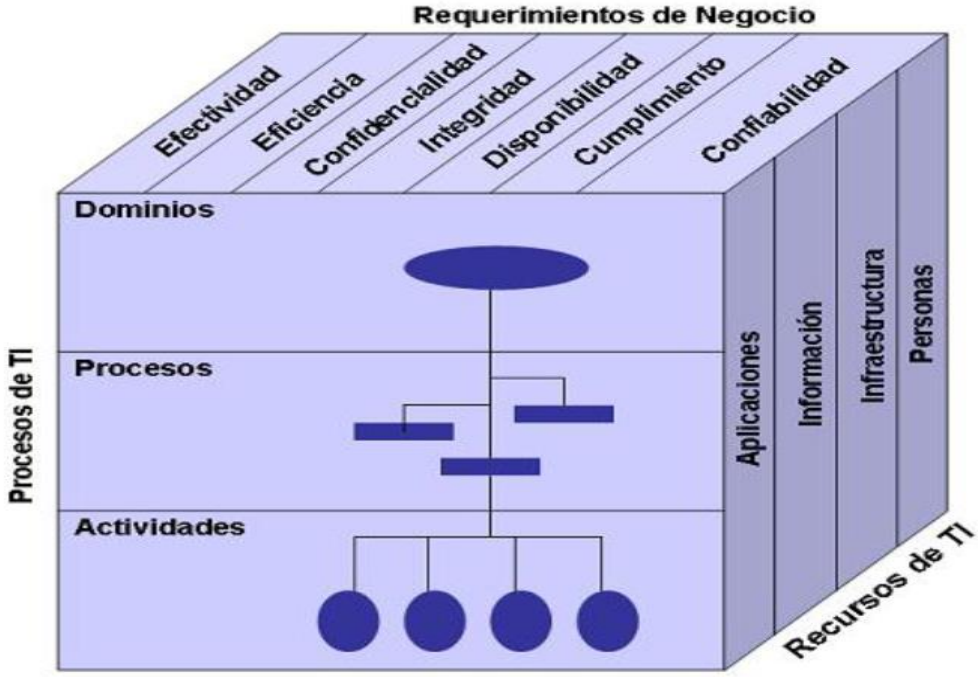


Figura 6: Cubo de Cobit
Fuente de Consulta: ISACA (2010)

El marco de referencia COBIT 4.1 está conformado por 34 objetivos siendo estos de P01 a P10, AI1 – AI7, DS1 – DS13, ME1 – ME4 de control y 4 dominios.

PO	PLANEAR Y ORGANIZAR
P01	Definir un plan estratégico de TI
P02	Definir la arquitectura de la información
P03	Determinar la dirección tecnológica
P04	Definir los procesos, organización y relaciones de TI
P05	Administrar la inversión de TI
P06	Comunicar las aspiraciones y la dirección de la gerencia
P07	Administrar recursos humanos de TI
P08	Administrar la calidad
P09	Evaluar y administrar los riesgos de TI
P10	Administrar proyecto

Figura 7: Procesos Cobit
Fuente de Consulta: IT Governance Institute (2008)

AI	ADQUIRIR E IMPLEMENTAR
AI1	Identificar soluciones automatizadas
AI2	Adquirir y mantener software aplicativo
AI3	Adquirir y mantener infraestructura tecnológica
AI4	Facilitar la operación y el uso
AI5	Adquirir recursos de TI
AI6	Administrar cambios
AI7	Instalar y acreditar soluciones y cambios

Figura 8: Procesos Cobit
Fuente de Consulta: IT Governance Institute (2008)

DS	ENTREGAR Y DAR SOPORTE
DS1	Definir y administrar los niveles de servicio
DS2	Administrar los servicios de terceros
DS3	Administrar el desempeño y la capacidad
DS4	Garantizar la continuidad del servicio
DS5	Garantizar la seguridad de los sistemas
DS6	Identificar y asignar costos
DS7	Educar y entrenar a los usuarios
DS8	Administrar la mesa de servicio y los incidentes
DS9	Administrar la configuración
DS10	Administrar los problemas
DS11	Administrar los datos
DS12	Administrar el ambiente físico
DS13	Administrar las operaciones

Figura 9: Procesos Cobit
Fuente de Consulta: IT Governance Institute (2008)

ME	MONITOREAR Y EVALUAR
ME1	Monitorear y evaluar el desempeño de TI
ME2	Monitorear y evaluar el control interno
ME3	Garantizar el cumplimiento regulatorio
ME4	Proporciona gobierno de TI

Figura 10: Procesos Cobit
Fuente de Consulta IT Governance Institute (2008)

Como lo cita García (2011), el modelo de madurez de Cobit 4.1 consta de 5 niveles de 0 a 5

- **0 Inexistente :** No se presenta ninguna información, tampoco se conoce sobre el gobierno de TI.

- **1 Inicial / Ad hoc:** Las tareas del proceso aun son indefinida sin embargo existe confianza de la iniciativa.

- **Repetible pero intuitivo:** En este paso las tareas ya son definidas y se cuenta con personal de calidad.
- **Definido:** El proceso ya es definido e institucionalizado, ya dispone de políticas y estándares establecidos.
- **Gestionable y medible:** El procedimiento esta completado en su totalidad y a su vez se realiza el análisis de desempeño.

Posteriormente se actualizo Cobit con la versión 5 cuyas diferencias son las siguientes:

Característica	Versión 4.1	Versión 5
Áreas de conocimiento	Única	Gobierno Corporativo de TI y Administración de TI Corporativa
Dominios	4 (PO, AI, DS, ME)	5 (EDM, PO,BAI, DSS, MEI)
Procesos	34	36
Procesos por dominio	PO – 10 procesos AI – 7 procesos DS – 13 procesos ME – 4 procesos	EDM – 5 procesos PO – 12 procesos BAI – 8 procesos DSS – 8 procesos MEI – 3 procesos
Niveles de madurez	6, modelo propio	6, basado en ISO 15504, niveles de capacidad

Figura 11: Comparativo de versiones
Fuente de Consulta: ISACA (2011)

ITIL

ITIL se formó a finales de 1980 por la Central Communication and Telecom Agency, CCTA, actual Office of Government Commerce, como un esfuerzo para disciplinar y permitir la comparación entre las propuestas de los distintos

proponentes a proveedores de servicios de TI para el gobierno británico. (Cestari, Cesar, & Dimmit, 2017)

En conclusión como lo cita Oltra (2016), ITIL es la agrupación de procesos que tienen una estructura lógica y permite a una institución gestionar los servicios de tecnología de información de una manera eficiente (pág. 3)

Itil se estructura a través de las 5 fases que se muestra a continuación.

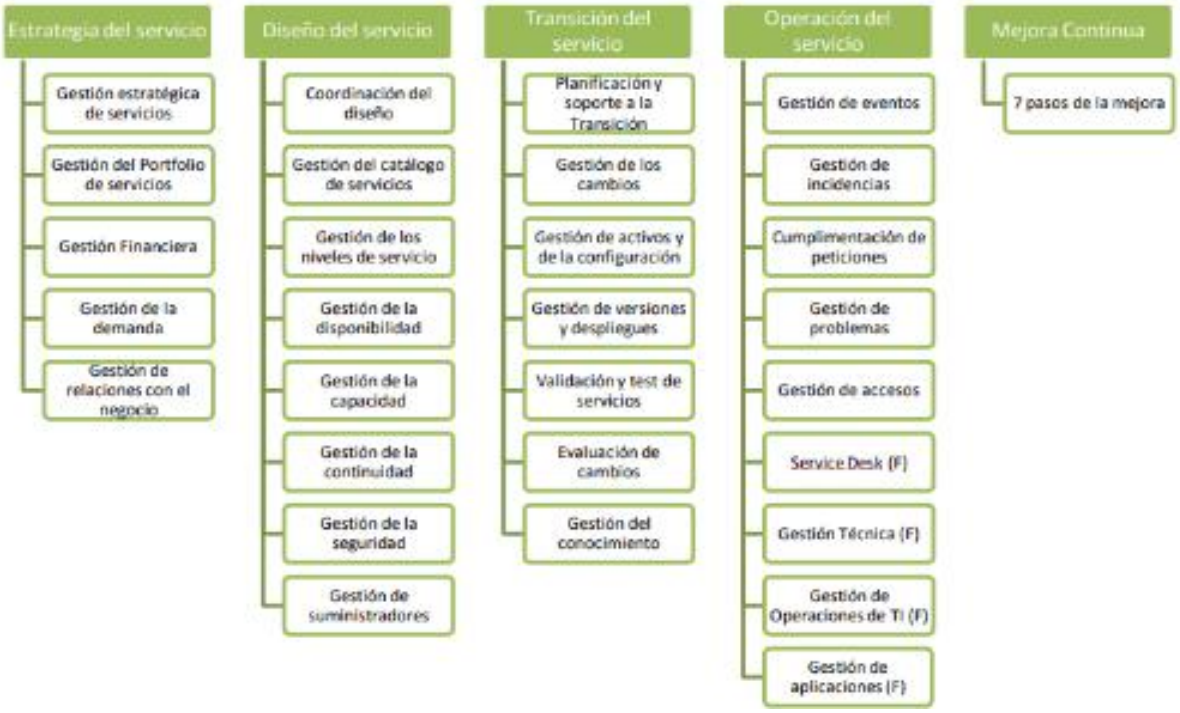


Figura 12: Fases de Itil
Fuente de Consulta: Oltra. (2016)

2.4.2 Conceptualización de la variable Dependiente

2.4.2.1 Gestión Administrativa

La gestión administrativa tiene un carácter sistémico, al ser portadora de acciones coherentemente orientadas al logro de los objetivos a través del cumplimiento de las funciones clásicas de la gestión en el proceso administrativo: planear, organizar, dirigir y controlar (Mendoza, 2017).

Dentro de la política de Gobierno de administrar los recursos públicos de manera transparente, el Ministerio de Finanzas emitió directrices y políticas de aplicación del proceso Integrado de Administración Financiera eSIGEF, mismo que ha sido estructurado con la normativa del Sistema de Administración. Este sistema debe ser actualizado en forma mensual, mediante reformas a través de la página Web del Ministerio de Finanzas, a fin de ingresar los movimientos del personal que se presentaron durante ese período, tales como: declarar y llenar vacantes, reclasificación de puestos, supresión y creación de puestos, traspasos en la misma entidad e ingreso de funcionarios a contrato, comisiones de servicios con y sin remuneración, las mismas que deberán ser aprobadas por dicho Ministerio (La Contraloría General del Estado del Ecuador, 2009).

Art. 226.- Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución (Constitución de la republica del Ecuador, 2012).

Art. 227.- La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación (Constitución de la republica del Ecuador, 2012).

2.4.2.2 Gestión de Riesgos

La metodología para la gestión de riesgos según el Ministerio de Finanzas del Ecuador (2017) se argumenta en las siguientes normativas o leyes vigentes:

- La Constitución de la República del Ecuador, publicada en el Registro Oficial No. 449 de 20 de octubre de 2008, en su artículo 390 señala que "Los riesgos se gestionarán bajo el principio de descentralización subsidiaria, que implicará la responsabilidad directa de las instituciones dentro de su ámbito geográfico. Cuando sus capacidades para la gestión del riesgo sean insuficientes, las instancias de mayor ámbito territorial y mayor capacidad técnica y financiera brindarán el apoyo necesario con respeto a su autoridad en el territorio y sin relevarlos de su responsabilidad".
- La Ley de Seguridad Pública y del Estado de 21 septiembre de 2009, en su artículo 11, literal d) indica: "De la gestión de riesgos. - La prevención y las medidas para contrarrestar, reducir y mitigar los riesgos de origen natural y antrópico o para reducir la vulnerabilidad, corresponden a las entidades públicas y privadas, nacionales, regionales y locales. La rectoría la ejercerá el Estado a través de la Secretaría Nacional de Gestión de Riesgos."
- El Código Orgánico de Planificación y Finanzas Públicas de 25 de Octubre de 2011, en el artículo 64 prevé: "Preeminencia de la producción nacional e incorporación de enfoques ambientales y de gestión de riesgo.- Incorporación de enfoques ambientales y de gestión de riesgos en el diseño e implementación de programas y proyectos de inversión pública; promoviendo acciones favorables de gestión de vulnerabilidades y riesgos antrópicos y naturales".

- El Manual del Comité de Gestión de Riesgos de 14 de Junio del 2014, emitido por la Secretaría de Gestión de Riesgos, establece dentro de los Principios de la gestión de riesgos: "Transversalidad: Todas las instituciones públicas y privadas deben incorporar obligatoriamente y en forma transversal la gestión de riesgos en su planificación y operación."
- El Acuerdo Ministerial Nro. 254 de 23 de noviembre de 2011, publicado en el Registro Oficial No 219 de 14 de diciembre de 2011, mediante el cual se aprobó el Estatuto Orgánico por Procesos del Ministerio de Finanzas, dispone en el numeral 3.1.2.1 como atribuciones y responsabilidades de la Dirección de Planificación e Inversión, entre otras:
    - Gestionar los procesos de planificación institucional; gestión de riesgos y seguridad integral.
    - Dirigir y participar en la formulación de programas, planes, políticas y proyectos de inversión institucionales, así como de gestión de riesgos y seguridad integral en función de la normativa legal vigente y directrices institucionales, sectoriales y nacionales.
    - Articular acciones claves, actividades y gestión institucional con las entidades vinculadas al ámbito de planificación e inversión y de gestión de riesgos y seguridad integral en forma intra e interinstitucional.
    - Brindar asistencia técnica en los procesos de planificación e inversión y de gestión de riesgos y seguridad integral.
    - Generar información especializada en el ámbito de gestión de riesgos y seguridad integral.

En conclusión, la Gestión de Riesgos es un proceso que incluye una serie de actividades relacionadas con el fin de administrar eficientemente los posibles eventos inesperados.

Propósitos

Para Brito (2018) La Gestión de Riesgos, tiene como propósitos los que se pueden citar a continuación:

- Contribuir al proceso de construcción de capacidades de los agentes del desarrollo, especialmente entre los organismos de la sociedad y el estado a la cooperación, a partir de facilitar elementos que permitan un mayor entendimiento de términos y definiciones sobre gestión de riesgos.
- Promover la reflexión y el debate para avanzar en la adopción concertada de un enfoque moderno sobre gestión de riesgos.
- Aportar a un proceso de discusión amplia que trascienda a los resabios de la concepción tradicional sobre el manejo de desastres.

Principios

Figura 14: Principios de la Gestión de Riesgos
Fuente de consulta: ISO 31000. (2018)

Modelos para la Gestión de Riesgos

Para la gestión de riesgos generalmente se aplica dos modelos que son ISO 31000 y COSO ERM que son marcos de referencia para dirigir y controlar riesgos.

ISO 31000

Esta norma está enfocada en la gestión de riesgos, se utiliza como una herramienta destinada a proporcionar a las empresas criterios y estándares que permiten una más eficiente de los eventos de riesgo y procesos, efectuado en las diversas fases organizacionales (Lizarzaburo, Barriga, Noriega, Lopez, & Mejía, 2017)

Procedimiento y Objetivos de ISO 31000

Como lo señala Lizarzaburo, Barriga, Noriega, Lopez, & Mejía (2017) Los procedimientos de administración de riesgos, contenido en las reglas ISO 31000 son:

1.-comunicación y consulta

2.-introducir el contexto,

3.-tasación de riesgos consistente en los tres pasos de identificación, análisis y aprobación

4.-Tratamiento del riesgo

5.-Seguimiento y revisión

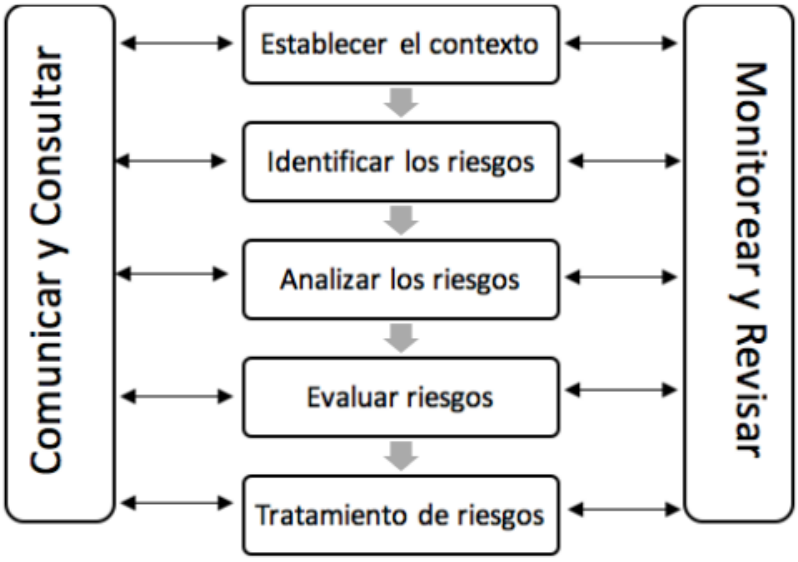


Figura 15: Proceso de la Gestión de riesgos 31000
Fuente de consulta: Castro, M. (2010)

COSO ERM

En la actualización de COSO ERM 2017 se destaca la importancia de la gestión del riesgo empresarial en la planificación estratégica y su integración en todos los niveles de la organización, ya que el riesgo influye y alinea la estrategia y el desempeño en todos los departamentos y funciones (Instituto de Auditores internos, 2017).

Figura 16: Gestión riesgo empresarial
Fuente de consulta: (Instituto de Auditores internos, 2017, pág. 10).

Gobierno y Cultura

El gobierno marca la importancia de la gestión de riesgos mientras la cultura se basa en la valores éticos y la compresión de los riesgo en la institución (Instituto de Auditores internos, 2017).

Estrategia y establecimiento de objetivos

Se establece un apetito al riesgo y se alinea con las estrategias; los objetivos del negocio ponen en práctica la estrategia al tiempo que sirven de base para identificar, evaluar y responder ante el riesgo (Instituto de Auditores internos, 2017).

Desempeño

Es importante que se identifique y valore los posibles riesgos que puedan afectar al cumplimiento de los objetivos; los riesgos se priorizaran de acuerdo a su gravedad para posterior seleccionar la respuesta adecuada al riesgo (Instituto de Auditores internos, 2017, pág. 10).

Revisión y monitorización

Al examinar el desempeño de la entidad, una organización puede determinar cómo funcionan los componentes de gestión del riesgo conocer los aspectos susceptibles de revisar y modificar (Instituto de Auditores internos, 2017, pág. 10).

Información, comunicación y reporte

La gestión del riesgo empresarial requiere un proceso continuo de obtención e intercambio de la información necesaria, tanto de fuentes internas como externas,

que fluya hacia arriba, hacia abajo y a lo largo de todos los niveles de la organización (Instituto de Auditores internos, 2017, pág. 10).

Estos cinco componentes cuentan con principios mismos que cubren todos los aspectos, desde el gobierno hasta información comunicación y reporte.

Figura 17: Principios de los componentes de COSO
Fuente de consulta: (Instituto de Auditores internos, 2017, pág. 10)

1.- Ejerce la supervisión de riesgos a través del consejo de administración

El consejo de administración supervisa la estrategia y lleva a cabo las responsabilidades de gobierno para apoyar a la dirección en la consecución de los objetivos estratégicos y de negocio (Instituto de Auditores internos, 2017, pág. 13).

2.- Establece estructuras operativas

La organización establece estructuras operativas con el fi n de alcanzar los objetivos estratégicos y de negocio (Instituto de Auditores internos, 2017, pág. 13).

3.- Define la cultura deseada

La organización define los comportamientos deseados que caracterizan la cultura a la que aspira la entidad (Instituto de Auditores internos, 2017, pág. 13).

4.- Demuestra compromiso con los valores clave

La organización demuestra su compromiso con los valores clave de la entidad (Instituto de Auditores internos, 2017, pág. 13).

5.- Atrae, desarrolla y retiene a profesionales capacitados

La organización está comprometida contar un capital humano alineado con los objetivos estratégicos y de negocio (Instituto de Auditores internos, 2017, pág. 13).

6.- Analiza el contexto empresarial

La organización considera los efectos potenciales del contexto empresarial sobre el perfil de riesgo (Instituto de Auditores internos, 2017, pág. 13).

7.- Define el apetito al riesgo

La organización define el apetito al riesgo en el contexto de la creación, preservación y materialización del valor (Instituto de Auditores internos, 2017, pág. 13).

8.- Evalúa estrategias alternativas

La organización evalúa las estrategias alternativas y el impacto potencial en el perfil de riesgos (Instituto de Auditores internos, 2017, pág. 13).

9.- Formula de objetivos

La empresa debe tener claro el riesgo en relación al tiempo en el que se establece los objetivos de una empresa en los distintos niveles, alineados y apoyados en la estrategia (Instituto de Auditores internos, 2017, pág. 13).

10.- Identifica el riesgo

La organización identifica el riesgo que impacta en la consecución de los objetivos estratégicos y de negocio (Instituto de Auditores internos, 2017, pág. 13).

11.- Evalúa la gravedad del riesgo

Evalúa la Gravedad del Riesgo (Instituto de Auditores internos, 2017, pág. 13).

12.- Prioriza riesgos

La organización prioriza los riesgos como base para la selección de respuestas a adoptar ante los riesgos (Instituto de Auditores internos, 2017, pág. 13).

13.- Implementa respuestas ante los riesgos

La organización identifica y selecciona las respuestas ante los riesgos (Instituto de Auditores internos, 2017, pág. 13).

14.- Desarrolla una visión a nivel de cartera

La organización desarrolla y evalúa una visión del riesgo a nivel de cartera (Instituto de Auditores internos, 2017, pág. 13).

15.- Evalúa los cambios significativos

La organización identifica y evalúa los cambios que pueden afectar sustancialmente a los objetivos estratégicos y de negocio (Instituto de Auditores internos, 2017, pág. 13).

16.- Revisa el riesgo y el desempeño

La organización revisa el desempeño de la entidad y tiene en consideración el riesgo (Instituto de Auditores internos, 2017, pág. 13).

17.- Persigue la mejora de la gestión del riesgo empresarial

La organización persigue mejorar la gestión del riesgo empresarial (Instituto de Auditores internos, 2017, pág. 13).

18.- Aprovecha los sistemas de información y la tecnología

La organización utiliza los sistemas de información y tecnología de la entidad para lograr la gestión del riesgo empresarial (Instituto de Auditores internos, 2017, pág. 13).

19.- Comunica información sobre riesgos

La organización utiliza canales de comunicación como soporte a la gestión del riesgo empresarial (Instituto de Auditores internos, 2017, pág. 13).

20.- Informa sobre el riesgo, la cultura y el desempeño

La organización informa sobre el riesgo, la cultura y el desempeño a múltiples niveles y a través de toda la entidad (Instituto de Auditores internos, 2017, pág. 13).

2.4.2.3Monitoreo de riesgos

Una vez diseñado y validado el plan para gestionar los riesgos, en el mapa de riesgos, es necesario monitorearlo teniendo en cuenta que estos nunca dejan de representar una amenaza para la organización y para el cumplimiento de los objetivos. Es importante detectar los cambios en el entorno, que puedan incrementar o disminuir la probabilidad de ocurrencia de los riesgos, así como su impacto. El propósito de la gestión del plan de acción es verificar que se está llevando a cabo, evaluar la eficiencia en su implementación, así como identificar nuevas acciones que puedan contribuir a una mejor gestión del riesgo. El plan deberá ser monitoreado por los responsables del manejo de los riesgos en cada una de las unidades del Ministerio de Finanzas y debe incluir propuestas de mejoramiento y tratamiento a las situaciones detectadas. La Dirección de Información, Seguimiento y Evaluación realizará revisiones trimestrales a nivel institucional con el propósito de sugerir los correctivos y ajustes necesarios y comunicar los resultados. Las unidades del Ministerio de Finanzas deberán realizar mínimo una revisión cada trimestre de los riesgos ingresados en la herramienta GPR, verificar si las condiciones inicialmente planificadas han cambiado y de ser el caso, actualizarlas. De la misma manera deberán dar seguimiento y registrar oportunamente el

cumplimiento del plan de acción programado, así como contar con los respaldos respectivos (Ministerio de Finanzas del Ecuador, 2017).

Es una actividad continua que da como resultado la conciencia de lo que realmente sucede en diferentes partes de la organización; a medida que pasa el tiempo, el monitoreo del riesgo permite a la administración: identificar tendencias críticas, responder de manera apropiada y eficiente, detectar oportunidades comerciales o mejoras de procesos que de otro modo no hubieran sido aparentes sin un monitoreo efectivo (Galvazine, 2020, pág. 2)

Por lo tanto, el monitoreo de riesgos es un proceso importante para la adecuada gestión de riesgos ya que permite a los administradores tener conocimiento de los riesgos identificados y los que pueden aparecer para así poder tener una respuesta eficaz.

Objetivos

Los objetivos primarios de monitorear son rastrear riesgos identificados, identificar los riesgos residuales, identificar nuevos riesgos, asegurar que los planes de respuesta a riesgos se ejecuten en el momento apropiado, y evaluar su efectividad. Además, otro de sus objetivos es la de rastrear y gestionar las acciones y respuesta al riesgo. (Dharma Consulting, 2013)

Beneficios

Los Beneficios del monitoreo de riesgos Fernández (2018) señala a continuación:

- Las respuestas a los riesgos implementadas son efectivas.
- Mejorar el enfoque de la gestión del riesgo.
- Se respetan las políticas y procedimientos de gestión de riesgos.

Prácticas de monitoreo de riesgos

Villanueva (2014) reconoce a practicas de monitoreo de riesgos como: la vigilancia tecnológica, la inteligencia competitiva, la inteligencia de negocios, los sistemas de alerta temprana, el diagnóstico organizacional, el cuadro de mando integral, A continuación se da una breve explicación del papel de cada una de ellas.

- **Sistemas de alertas tempranas (SAT)**

De acuerdo a (Comai, 2011) citado en Villanueva (2014) "Los STA se conforman por varios instrumentos de apoyo al logro de los objetivos de una compañía, identifican cambios del entorno, tendencias que están en sus primeras fases y demás variables que pueden tener efectos importantes en las organizaciones" (pág. 129).

- **Inteligencia Económica (IE)**

De acuerdo con (Juillet,2006) citado por Villanueva (2014) "es la utilización de técnicas que permite conocer el medio en el que desarrolla la empresa, identificando la competencia y a la vez anticipando a posibles amenazas que pueden aparecer en el proceso" (pág. 130).

- **Vigilancia tecnológica e inteligencia competitiva (IC)**

En base a (Múnera y Rodríguez, 2013) que cita Villanueva (2014) "Se define como el "proceso analítico que transforma los datos desagregados obtenidos de los competidores en conocimiento relevante, fiable y útil sobre los objetivos, recursos, capacidades y resultados de los competidores" (pág. 130).

- **Inteligencia de negocios**

Según (Barnt,1994) citado por Villanueva (2014) "Su objetivo es proporcionar la información sobre el entorno organizacional, identificar las amenazas y

oportunidades, evitar las sorpresas desagradables, mejorar la planificación, aumentar la probabilidad de tomar buenas decisiones, reducir el riesgo organizacional y personal" (pág. 130).

- **Cuadro de mando integral o Balanced Scorecard**

Como lo menciono (Blanco,2011) citado por Villanueva (2014) " Permite expresar la estrategia de una organización desde cuatro perspectivas básicas accionistas, clientes, procesos internos y aprendizaje y crecimiento y mediante un conjunto de medidas (indicadores) de gran utilidad para controlar la ejecución de los planes" (pág. 130).

- **Diagnóstico Organizacional**

De acuerdo con (Vidal,2004) mencionado por Villanueva (2014)" "Es un proceso de comparación entre dos situaciones, la presente que hemos llegado a conocer a través de la indagación, y otra ya definida y supuestamente conocida que nos sirve de pauta o modelo" (pág. 131).

Metodología

Primera fase: Definición del mecanismo de monitoreo

Esta primera fase tiene como fin establecer mecanismo de monitoreo de los riesgos que empleará la empresa y que le permitirá constituirse en un dispositivo de alerta temprana que le permitirá a la organización tener una actitud proactiva frente al riesgo (Villanueva, 2014).

Segunda fase. Recolección de información

Una vez seleccionados los riesgos que se van a monitorear, y definido el mecanismo de monitoreo, se establecerá donde se recopilara la información, como la utilizaran y como la documentaran. (Villanueva, 2014, pág. 132)

Tercera fase. Análisis de información

Una vez recopilada la información se procede al respectivo análisis en donde se compara los resultados que han sido obtenidos en el monitoreo junto con los objetivos iniciales o metas del comportamiento de los riesgos y finalmente se desarrolla un informe que se presenta a la alta dirección (Villanueva, 2014, pág. 132).

Cuarta fase. Toma de decisiones

En esta fase se toman decisiones como fruto de la discusión que genera en el grupo directivo de la empresa sobre la información obtenida en la fase anterior. (Villanueva, 2014)

2.5 Preguntas de investigación

- ¿Cuál es el nivel de aseguramiento de la información en los procesos de TI en el Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga?
- ¿Cuál es el nivel de riesgo en los procesos del área financiera en Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga?

2.6 Señalamiento de variables

Variable Independiente: Aseguramiento de la información

Variable Dependiente: Monitoreo de riesgos

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACION

3.1 Enfoque

La investigación según Ander-EGG (2011) es un procedimiento reflexivo, sistemático, controlado y crítico que tiene como finalidad descubrir, describir, explicar o interpretar los hechos, fenómenos, procesos, relaciones y constantes o generalizaciones que se dan en un determinado ámbito de la realidad y que a su vez usan de un modelo para llevarla a cabo.

En este sentido el enfoque de la presente investigación es mixto ya que se combina el enfoque cualitativo y cuantitativo.

Según Ander-EGG (2011) el enfoque cualitativo se caracteriza, entre otras cosas, por la obtención de información de manera inmediata y personal, utilizando técnicas y procedimientos basados en el contacto directo con la gente o realidad que se investiga.

Por otro lado, Hernandez, Collado, & Lucio (2003) mencionan que el enfoque cuantitativo utiliza la recolección de información y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confía en una medición numérica, el conteo y frecuentemente en el uso estadístico para establecer con exactitud patrones de comportamiento de una población.

Es así que la combinación de esto dos modelos se le denomina modelo mixto que como lo menciona Hernandez, Collado, & Lucio (2003) es un conjunto de procesos sistemáticos, empíricos y críticos de investigación, que implican la recolección y

análisis de datos tanto cuantitativos como cualitativos, además de la integración y discusión conjunta

3.2 Modalidad básica de la Investigación

3.2.1 Investigación de campo

Se trabajará con una investigación de campo ya que se tendrá contacto directo con el personal del departamento Financiero e Informático debido a que son el personal involucrado en el estudio y son quienes pueden aportar con la información y experiencias para el desarrollo de la investigación.

La investigación de campo según Arias (2006) consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes.

3.2.2 Investigación Bibliográfica-Documental

Por otro lado, también se utilizará la modalidad de investigación bibliográfica-documental ya que se revisará material bibliográfico como libros, revistas, artículos científicos que permitan fundamentar y conocer a profundidad sobre el aseguramiento de la información basado en el marco de referencia de COBIT y el monitoreo de riesgos basado en COSO ERM.

La investigación documental para Baena G. (2014) es la búsqueda de una respuesta específica a partir de la indagación en documentos, entendiendo por documento como refiere Maurice Duverger todo aquello donde ha dejado huella el hombre en su paso por el planeta.

Así mismo, Arias (2006) se refiere a la investigación documental–bibliográfica como un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas.

3.3 Nivel o Tipo de Investigación

Para el desarrollo de la presente investigación se aplicará los siguientes tipos de investigación:

Investigación asociación de variables (correlacional)

De acuerdo con lo que hace referencia Tamayo (1999) la investigación correlacional busca determinar el grado en el cual las variaciones en uno o varios factores son concomitantes con la variación en otro u otros factores. La existencia y fuerza de esta covariación normalmente se determina estadísticamente por medio de coeficientes de correlación.

Dentro del presente proyecto de investigación se aplicará los estudios correlaciónales utilizando el método estadístico de Pearson, pues se determinaron dos variables que son aseguramiento de la información y monitoreo de riesgos ya que se buscara medir y establecer la incidencia de ambas.

Investigación explicativa

El presente trabajo se ajusta a la investigación de tipo explicativo ya que busca el porqué de los hechos mediante el establecimiento de relaciones causa-efecto (Arias F. , 2006)

En este sentido la investigación explicativa va un paso más allá descripción de

conceptos o fenómenos de un tema planteado; es decir, esta direccionado a responder por las causas de los eventos y fenómenos físicos o sociales, básicamente su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta, o por qué se relacionan dos o más variables (Hernández, Fernandez, & Pilar, 2014).

3.4. Población y Muestra

3.4.1 Población

La población es un conjunto de casos, definido, limitado y accesible que servirá de referente para la elección de la muestra, es importante mencionar que la población no se refiere exclusivamente a seres humanos si no también puede referirse a muestras biológicas, animales, expedientes, hospitales, objetos, familias, organizaciones, etc. (Arias, Villasís, & Miranda, 2016)

Para Gonzáles & Salazar (2008) desde el punto de vista estadístico señala que la población es cualquier conjunto de elementos de los cuales se pretende indagar y conocer sus características, o una de ellas, y para el cual serán válidas las conclusiones obtenidas en la investigación.

De esta manera, para el desarrollo de la presente investigación la población se refiere a los 34 procesos de COBIT en el departamento informático y los 20 principios de COSO ERM en el departamento financiero del Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga.

Siendo la siguiente información objeto de análisis:

PO	PLANEAR Y ORGANIZAR
P01	Definir un plan estratégico de TI
P02	Establecer la arquitectura de la TI

P03	Establecer la dirección tecnológica
P04	Definir los procesos de TI
P05	Administración de inversión de TI
P06	Comunicar Aspiraciones
P07	Administrar el capital humano de TI
P08	Administración de la calidad
P09	Evaluar los riesgos
P10	Gerenciar el proyecto.

Tabla 1: Planear y Organizar
Elaborado por: Acurio, Y. (2020)

PO	ADQUIRIR E IMPLEMENTAR
AI1	Establecer soluciones automatizadas
AI2	Adquirir un software aplicativo
AI3	Adquirir infraestructura tecnológica
AI4	Facilitar la operación adecuada
AI5	Adquirir recursos de tecnología de información
AI6	Gerenciar cambios
AI7	Dar cambios y soluciones

Tabla 2: Adquirir e Implementar
Elaborado por: Acurio, Y. (2020)

PO	ENTREGAR Y DAR SOPORTE
DS1	Establecer los niveles de servicio
DS2	Guiar los servicios de tercero

DS3	Administrar el desempeño
DS4	Establecer la continuidad del servicio brindado
DS5	Garantizar la seguridad de los sistemas de información
DS6	Asignación de costos
DS7	Capacitar a los usuarios
DS8	Administrar las mesas de todos los servicios
DS9	Establecer la configuración
DS10	Administrar los problemas
DS11	Gerenciar datos
DS12	Administrar el ambiente
DS13	Administrar todas las operaciones

Tabla 3: Entregar y Dar Soporte
Elaborado por: Acurio, Y. (2020)

PO	MONITOREAR Y EVALUAR
ME1	Monitorear y realizar la evaluación del desempeño de TI.
ME2	Monitorear y evaluar el control interno
ME3	Certificar el cumplimiento
ME4	Proporcionar gobierno de tecnología de información

Tabla 4: Monitorear y Evaluar
Elaborado por: Acurio, Y. (2020)

PRINCIPIOS DE DE COSO ERM

GOBIERNO Y CULTURA
1.-Ejerce la supervisión de riesgos a través del consejo de administración
2.-Establecer estructuras operativas
3.-Define la cultura deseada
4.-Demuestra compromiso con los valores clave
5.-Atrae, desarrolla y retiene a profesionales capacitados

Tabla 5: Gobierno y Cultura
Elaborado por: Acurio, Y. (2020)

ESTRATEGIA Y ESTABLECIMIENTO DE OBJETIVOS
6.-Analiza el contexto empresarial
7.-Define el apetito al riesgo
8.-Evalua estrategias alternativas
9.-Formula objetivos de negocio

Tabla 6: Estrategia y Establecimiento de Objetivos
Elaborado por: Acurio, Y. (2020)

DESEMPEÑO
10.-Identifica el riesgo
11.-Evalua la gravedad del riesgo
12.-Prioriza riesgos
13.-Implementa respuestas ante los riesgos
14.-Desarrolla una visión a nivel de cartera

Tabla 7: Desempeño
Elaborado por: Acurio, Y. (2020)

REVISIÓN Y MONITORIZACIÓN
15.-Evalua los cambios significativos
16.-Revisa el riesgo y el desempeño
17.-Persigue la mejora de la gestión del riesgo empresarial

Tabla 8: Revisión y Monitorización
Elaborado por: Acurio, Y. (2020)

INFORMACIÓN, COMUNICACIÓN Y REPORTE
18.-Aprovechamiento de tecnología e información
19.-Comunica información sobre riesgos
20.-Informa sobre el riesgo, la cultura y el desempeño

Tabla 9: Información, Comunicación y reporte
Elaborado por: Acurio, Y. (2020)

3.4.2. Muestra

En palabras de Lopez (2004) la muestra se considera como un subconjunto o parte del universo o población en que se llevará a cabo la investigación y se puede obtener la cantidad de la muestra mediante fórmulas y lógica etc.

La investigación no utiliza muestra debido a que, la población refiere a procesos y estos son finitos.

3.5. Operacionalización de las variables

Una variable es operacionalizada con el objetivo de convertir un concepto abstracto en empírico, susceptible de ser medido a través de la aplicación de un instrumento, este proceso podría ser importante para el investigador ya que impedirá la posibilidad no perderse o cometer errores. (Betancur, 2000)

Para Espinoza (2019) a través de la operacionalización de las variables se intenta obtener la mayor información posible de las variables junto con el apoyo del marco teórico, además la operacionalización está estrechamente vinculada al tipo de técnica o metodología empleada para la recolección de datos.

La operacionalización de variables del estudio se presenta a continuación:

3.5.1. Operacionalización de la variable independiente

VARIABLE INDEPENDIENTE: Aseguramiento de la información				
CONCEPTUALIZACIÓN	CATEGORÍAS	INDICADORES	ITEMS GENERALS	TECNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN
Es el conjunto de diversas actividades que permiten la protección de la información y las redes para preservar la disponibilidad y confidencialidad de la información	PLANEAR Y ORGANIZAR	1. Definir un plan estratégico de TI 2. Establecer la arquitectura de la TI 3. Establecer la dirección tecnológica 4. Definir los procesos de TI 5. Administración de inversión de TI 6. Comunicar Aspiraciones 7. Administrar el capital humano de TI 8. Administración de la calidad 9. Evaluar los riesgos 10. Gerenciar el proyecto.	¿Se cumple con algún plan estratégico para TI? ¿El modelo de información institucional facilita el desarrollo de aplicaciones consistentes con TI? ¿Se analizan las tecnologías existentes? ¿Está definido un marco de trabajo para los procesos de TI? ¿Cuentan con presupuesto para inversiones de TI? ¿La institución cuenta con una fuerza de trabajo apropiada? ¿Se cuenta con un sistema de administración de calidad para TI?	**Técnica:** Encuesta **Instrumento**: Cuestionario (Matriz COBIT)

	ADQUIRIR E IMPLEMENTAR	1. Establecer soluciones automatizadas 2. Adquirir un software aplicativo 3. Adquirir infraestructura tecnológica 4. Facilitar la operación adecuada 5. Adquirir recursos de tecnología de información 6. Gerenciar cambios 7. Dar cambios y soluciones	¿Hay conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas? ¿El proceso para la adquisición e implementación de software es claro?	**Técnica:** Encuesta **Instrumento**: Cuestionario (Matriz COBIT)
	ENTREGAR Y DAR SOPORTE	1. Establecer los niveles de servicio 2. Guiar los servicios de tercero 3. Administrar el desempeño 4. Establecer la continuidad del servicio brindado 5. Garantizar la seguridad de los sistemas de información 6. Asignación de costos 7. Capacitar a los usuarios	¿Se monitorea los criterios de desempeño específicos para el nivel de servicios? ¿Se identifican todos los servicios de los proveedores de TI? ¿Se planifica para realizar una revisión del desempeño de TI? ¿La institución desarrolla un marco de trabajo de continuidad de TI?	**Técnica:** Encuesta **Instrumento**: Cuestionario (Matriz COBIT)

		8. Administrar las mesas de todos los servicios 9. Establecer la configuración 10. Administrar los problemas 11. Gerenciar datos 12. Administrar el ambiente 13. Administrar todas las operaciones	¿Hay un nivel apropiado de seguridad de TI dentro de la institución?	
	MONITOREAR Y EVALUAR	1. Monitorear y realizar la evaluación del desempeño de TI. 2. Monitorear y evaluar el control interno 3. Certificar el cumplimiento 4. Proporcionar gobierno de tecnología de información	¿Se monitorea la contribución de TI a la institución? ¿Se establecen acciones correctivas en caso de controles ineficientes? ¿Se evalúan las políticas, estándares, procedimientos y metodologías de TI?	**Técnica:** Encuesta **Instrumento**: Cuestionario (Matriz COBIT)

Tabla 10: Operacionalización variable Independiente
Elaborado por: Acurio, Y. (2020)

VARIABLE DEPENDIENTE: Monitoreo de riesgos				
CONCEPTUALIZACIÓN	CATEGORÍAS	INDICADORES	ITEMS GENERALS	TECNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN
Es una actividad continua que da como resultado la conciencia de lo que realmente sucede en diferentes partes de la organización; a medida que pasa el tiempo, el monitoreo del riesgo permite a la administración: identificar tendencias críticas, responder de manera apropiada y eficiente, detectar oportunidades comerciales o mejoras de procesos que de otro modo no hubieran sido aparentes sin un monitoreo efectivo	Gobierno y cultura	1.-Ejerce la supervisión de riesgos a través del consejo de administración 2.-Establecer estructuras operativas 3.-Define la cultura deseada 4.-Demuestra compromiso con los valores clave 5.-Atrae, desarrolla y retiene a profesionales capacitados.	¿La Dirección administrativa del hospital tiene conciencia sobre la responsabilidad de supervisar los riesgos en el manejo de información confidencial que genera el departamento financiero? ¿La Institución establece una estructura operativa para el cumplimiento de los objetivos del departamento financiero?	**Técnica:** Encuesta **Instrumento**: Cuestionario (Matriz de riesgos según COSO ERM)
	Estrategia y establecimiento de objetivos	6.-Analiza el contexto empresarial 7.-Define el apetito al riesgo 8.-Evalua estrategias alternativas 9.-Formula objetivos de negocio	¿El departamento Financiero identifica su entorno interno (capital, personas, proceso y tecnología) y las partes interesadas que pueden afectar su capacidad para lograr la presentación de informes a tiempo?	**Técnica:** Encuesta **Instrumento**: Cuestionario (Matriz de riesgos según COSO ERM)

			¿Se supervisa continuamente el apetito al riesgo en todos los niveles del departamento Financiero y se adapta al cambio cuando es necesario? ¿El Departamento Financiera establece objetivos que son específicos, medibles, alcanzables y relevantes sobre la seguridad de la información?	
	Desempeño	10.-Identifica el riesgo 11.-Evalua la gravedad del riesgo 12.-Prioriza riesgos 13.-Implementa respuestas ante los riesgos 14.-Desarrolla una visión a nivel de cartera	¿El departamento financiero considera como los cambios pueden crear riesgos nuevos o emergentes que afecten a la información? ¿El departamento financiero selecciona medidas para evaluar la gravedad del riesgo y el impacto en la información que genera?	**Técnica:** Encuesta **Instrumento**: Cuestionario (Matriz de riesgos según COSO ERM)
	Revisión y monitorización	15.-Evalua los cambios significativos 16.-Revisa el riesgo y el desempeño	¿Se identifica y evalúa los cambios tecnológicos que pueden afectar sustancialmente a la	**Técnica:** Encuesta **Instrumento**:

		17.-Persigue la mejora de la gestión del riesgo empresarial	información que genera el departamento financiero? ¿La Jefatura Financiera revisa los riesgos tecnológicos que afecten a la generación de la información?	Cuestionario (Matriz de riesgos según COSO ERM)
	Información, comunicación y Reporte	18.-Aprovecha la información y la tecnología 19.-Comunica información sobre riesgos 20.-Informa sobre el riesgo, la cultura y el desempeño	¿La Jefatura Financiera busca la mejorar la gestionar riesgos sobre la seguridad de la información? ¿La Jefatura Financiera se prepara constantemente a los posibles riesgos que afecten a la seguridad de la información?	**Técnica:** Encuesta **Instrumento**: Cuestionario (Matriz de riesgos según COSO ERM)

Tabla 11: Operacionalización variable Dependiente
Elaborado por: Acurio, Y. (2020)

3.6. Recolección de Información

La recolección de información para Moreno & Gallardo (1999) es un proceso planeado paso a paso, para que de forma coherente se puedan obtener resultados que contribuyan favorablemente al logro de los objetivos propuestos.

3.6.1. Plan para la recolección de información

Tomando en cuenta que el enfoque de la presente investigación es mixto, el plan para la recolección de información contemplan estrategias metodológicas que responden a los objetivos e hipótesis del presente trabajo. A continuación, se describe las estrategias en los siguientes elementos:

Definición de los sujetos; personas u objetos que van a ser investigados

Para el presente trabajo los objetos de estudio son los 34 procesos de COBIT en el departamento informático y los 20 principios de COSO ERM en el departamento financiero y las fuentes de información será el jefe financiero y al jefe del departamento informático ya que son los que conocen mejor sobre el funcionamiento de sus procesos.

Selección de las técnicas a emplear en el proceso de recolección de información.

En la investigación la recolección de información se la realizará a través de la técnica de: ENCUESTA.

Instrumentos seleccionados o diseñados de acuerdo con la técnica escogida para la investigación.

Para el desarrollo de la presente investigación la técnica utilizada es la encuesta tanto como para la variable independiente como dependiente y el instrumento es el cuestionario, mismo que serán en funciona a la información/ítems contenidos en las matrices de operacionalización de variables.

Selección de recursos de apoyo (equipos de apoyo).

La investigación contará con el aporte de personal del Departamento Informático y Financiero del Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga; que son dos el jefe del departamiento financiero y el jefe del departamento de informática funcionarios que, con sus años de experiencia y amplio conocimiento en el problema de investigación, permitirá realizar un adecuado análisis.

Explicitación de procedimientos para la recolección de información, cómo se va a aplicar los instrumentos, condiciones de tiempo y espacio, etc.

Técnicas	Procedimiento
Encuesta	**¿Cómo?** Se realizará mediante el método deductivo
	¿Dónde? Se aplicará al Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga, en específico a las áreas de Informática y Financiera
	¿Cuándo? Entre los meses de octubre y diciembre de 2020

Tabla 12: Procedimiento para la recolección de información
Elaborado por: Acurio, Y. (2020)

El método por utilizar es el deductivo ya que se comprobará la hipótesis partiendo de teorías generales y así poder establecer conclusiones con respecto tema investigado.

Neill & Cortez (2018) explica que el método deductivo se fundamenta en el razonamiento que permite formular juicios partiendo de argumentos generales para demostrar, comprender o explicar los aspectos particulares de la realidad.

3.6.2. Procesamiento y análisis de información

El procesamiento de la información es conocido como una serie actividades o pasos que están orientados para ordenar, almacenar y preparar los archivos con la información captada, asegurando su congruencia para finalmente presentar los resultados. (Instituto Nacional de Estadística y Geografía, 2012)

3.6.2.1. Plan para el procesamiento de información

Revisión crítica de la información recogida.

Toda la información recabada será depurada, con el fin que se elimine aquella que sea defectuosa y perjudique a los resultados de la investigación.

Tabulación o cuadros según variables

Mediante matrices donde se expone la información recaba sobre las dos variables en estudio. Además, se utiliza técnicas estadísticas que aportaran para presentar los resultados de la investigación.

Representaciones gráficas

Con el uso de graficas se podrá presentar de manera más clara los resultados obtenidos al final de la investigación.

3.6.3. Plan de análisis e interpretación de resultados

Análisis de los resultados estadísticos

Los datos obtenidos producto de la recolección de información se enfocarán en tendencias o relaciones fundamentales que estén de acuerdo a los objetivos e hipótesis planteados en la presente investigación.

Interpretación de los resultados

Con el apoyo y sustento del marco teórico que se encuentra en el capítulo II del presente trabajo de titulación.

Comprobación de Hipótesis

Para la comprobación de hipotesis será las respuestas a las preguntas de investigación planteadas para la variable dependiente y la variable independiente.

Establecimiento de conclusiones y recomendaciones

Las conclusiones son una reflexión final, que son resultado de análisis de la información recabada de cada uno de los objetivos planteados.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis e interpretación

Los datos que se presentan a continuación fueron recabados de fuentes primarias ya que se basó en la creación de un cuestionario de preguntas definidas en base a una metodología y a un criterio de medición, el cual fue entregado a la autoridad de la institución para la extracción de la información.

4.1.1 Análisis e interpretación de la primera metodología

La primera metodología a utilizar tiene como objetivo la medición del grado de madurez de cada uno de los 34 procesos de TI definidos en el marco de referencia, en base al modelo de madurez propuesto por Cobit, para lo cual se construyó un cuestionario determinando las preguntas en base a la metodología de Pederiva (2003) en la que propone:

> Las descripciones de los grados de madurez de un proceso pueden ser vistos como un conjunto de planteamientos atómicos. Estos planteamientos atómicos pueden ser calificados para cada grado de madurez y generar un nivel de cumplimiento de cada grado visto como un escenario.

Luego de que se construyan las preguntas en base a los planteamientos atómicos es necesario definir el formato de respuesta que se va a utilizar para cuantificar el nivel de cumplimiento. Como cada escenario de grado de madurez tendrá un conjunto de preguntas, se busca medir, que tan de acuerdo están director administrativo con los planteamientos indicados. El grado de acuerdo permitirá cuantificar el nivel de cumplimiento de cada grado de madurez.

Existen varios tipos de formatos, para cuantificar el nivel de acuerdo, sin embargo, el que más se ajusta y alinea con el Modelo de Madurez sugerido por COBIT es el tipo de formato “Likert”.

Para el cálculo del nivel de acuerdo con las preguntas de la entrevista se realizó los siguientes niveles, en base a la propuesta de (Pederiva, 2003), como se muestra en la siguiente tabla.

Formato de Respuestas	
Nivel de Acuerdo	**Valor de Cumplimiento**
De ningún modo	0
Un poco	0.33
Bastante	0.66
Completamente	1

Tabla 13: Formato de respuesta
Elaborado por: Pederiva, A. (2003)

Como la suma de los valores de cumplimiento dan un resultado distinto a 1, es necesario normalizar el valor de cumplimiento, refiriendo todos los resultados con respecto a 1. Para esto, se obtiene un total de los valores de cumplimiento, y se divide cada valor de cumplimiento de los grados de madurez para el total obtenido. Ejecutando este proceso para cada grado de madurez, permite normalizar los niveles de cumplimiento (Pederiva, 2003).

Finalmente, para procesar el grado de contribución que los valores de cada escenario, se multiplicará el valor de cumplimiento normalizado de cada escenario, por el grado de madurez del escenario. Este tipo de proceso se repite para todos los 6 escenarios, para obtener el valor de contribución de cada escenario. Finalmente se suma todas las contribuciones, y el resultado final es el grado de madurez del proceso evaluado.

Este procedimiento de cálculo se aplicará a los 34 procesos de TI para obtener el listado final de los grados de madurez de cada uno de los 4 dominios de COBIT (Pederiva, 2003).

4.1.1.1 Dominio 1. Planear y Organizar (po)

NV	N°	PO1 Definir un Plan Estratégico de TI	De ningún modo	Un poco	Bastante	Completamente	Calificación	TOTAL
0	**1**	¿La institución considera no necesario definir un plan estratégico de TI?		**X**			0,33	0,33
0	**2**	¿La institución no considera importante el control sobre las prácticas de TI?	**X**				0	
1	**3**	¿Los planes existentes son lo suficientemente detallado para conocer el estado actual de TI?		**X**			0,33	0,33
1	**4**	¿Los planes existentes detallan las áreas de la institución que dependen de forma crítica de TI?	**X**				0	
2	**5**	¿Las estrategias para el manejo de TI son tratadas, autorizadas y debidamente comunicadas?	**X**				0	0
2	**6**	¿Los directivos saben cómo capitalizar las oportunidades que ofrece TI?	**X**				0	
3	**7**	¿Los Administradores de la Tecnología de la Información son capacitados y comunicados sobre como los planes se cumplirán?		**X**			0,33	0,33
3	**8**	¿En el desempeño de los planes existentes se evalúa las fortalezas de TI?	**X**				0	
3	**9**	¿En el desempeño de los planes existentes se evalúa los costos de TI?	**X**				0	
4	**10**	¿En los planes se describen como se monitorean los recursos asignados para TI?			**X**		0,66	1,32
4	**11**	¿En el caso de desviaciones en los planes de TI se toman las medidas correctivas?			**X**		0,66	
5	**12**	¿La gestión y maneje de recursos de TI están alineados con las estrategias y prioridades de la institución?		**X**			0,33	0,99
5	**13**	¿El plan estratégico de TI se mejora continuamente?		**X**			0,33	
5	**14**	¿Se identifican nuevos proyectos para TI?		**X**			0,33	

Tabla 14: Cuestionario PO1
Elaborado por: Acurio, Y. (2020)

PROCESO: PO1 DEFINIR UN PLAN ESTRATÉGICO DE TI					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.33	2	0.17	0.12	0
1	0.33	2	0.17	0.12	0.12
2	0	2	0	0	0
3	0.33	3	0.11	0.08	0.24
4	1.32	2	0.66	0.46	1.84
5	0.99	3	0.33	0.23	1.15
TOTAL	3.3	14	1.44	1.01	**3.35**

Tabla 15: Nivel de madurez proceso Definir un Plan Estratégico de TI
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**3.35**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de tres (nivel de madurez 3 o definida); lo que en la escala del modelo de madurez de COBIT indica que los procesos han sido estandarizados, documentados y comunicados, sin los procedimientos no son sofisticados si no que son la formalización de las practicas existentes.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso P01: Definir un plan estratégico de TI podemos decir que la institución cuenta con un plan estratégico de TI que está documentado y comunicado a los responsables del proceso, sin embargo, en el plan no está bien detallado el estado actual de TI y ni las áreas que dependen de forma crítica, además la responsabilidad de supervisión e implementación del plan se ha dejado a la misma persona lo que no hace improbable que se detecten desviaciones y se las pueda corregir a tiempo.

NV	N°	PO2 Definir la Arquitectura de la Información	De ningún modo	Un poco	Bastante	Completamente	Calificación	TOTAL
0	**1**	¿La arquitectura de la información no es considerado un tema lo suficientemente importante para tratarlo?			**X**		0,66	1,66
0	**2**	¿En la institución se considera necesario contar con un esquema de clasificación de datos para toda la institución?				**X**	1	
1	**3**	¿Existe conciencia de la necesidad de contar con procedimientos que garanticen la integridad de los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos?			**X**		0,66	1,32
1	**4**	¿Se tiene poca consideración a los modelos de información que se maneja?			**X**		0,66	
2	**5**	¿El diccionario de datos facilita compartir elementos de datos entre los sistemas?		**X**			0,33	0,99
2	**6**	¿El modelo de información que se maneja permite que la información sea oportuna?			**X**		0,66	
3	**7**	¿Se usa un esquema que describa que tan críticos son los datos?		**X**			0,33	1,33
3	**8**	¿Se emplea un esquema para clasificar la información en pública, confidencial y secreta?				**X**	1	
4	**9**	¿Se evalúa que los niveles de seguridad de datos sean los apropiados?			**X**		0,66	0,99
4	**10**	¿Se evalúa que el modelo de información facilite las actividades de soporte, la toma de decisiones y sea consistente con los planes de TI?		**X**			0,33	
5	**11**	¿El diccionario de datos fomenta un entendimiento común de datos ente los usuarios y administradores de TI?		**X**			0,33	1,32
5	**12**	¿El esquema de información se utiliza como base para aplicar controles como el de acceso, archivo o cifrado?		**X**			0,33	
5	**13**	¿El modelo de información ha permite que la información se mantenga integra sin errores?			**X**		0,66	

Tabla 16: Cuestionario PO2
Elaborado por: Acurio, Y. (2020)

PROCESO: PO2 Definir la Arquitectura de la Información					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**

Nivel de Madurez	Suma de valores de cumplimiento	Número de declaraciones	Valor de cumplimiento (B/C)	Normalización del vector de cumplimiento (D/∑D)	Nivel de madurez (A*E)
0	1.66	2	0.83	0.23	0
1	1.32	2	0.66	0.18	0.18
2	0.99	2	0.50	0.14	0.28
3	1.33	2	0.67	0.19	0.57
4	0.99	2	0.50	0.14	0.56
5	1.32	3	0.44	0.12	0.60
TOTAL	**7.61**	**13**	**3.6**	**1**	**2.19**

Tabla 17: Nivel de madurez proceso Definir la Arquitectura de la Información
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.19**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso P02: Definir la arquitectura de la Información podemos decir que en la institución no hay conciencia sobre la importancia de organizar, disponer y estructurar la información que es de vital importancia para su funcionamiento, a pesar de que se cuenta con un sistema de gestión de información para todos los procesos no se le da el debido soporte a través de herramientas automatizadas como el de contar con un diccionario de datos que facilite el entendimiento común de información entre usuarios y administradores de TI.

NV	N°	PO3 Determinar la Dirección Tecnológica	De ningún modo	Un poco	Bastante	Completamente	Calificación	TOTAL

0	**1**	¿Para la institución es importante analizar qué dirección tecnológica es apropiada tomar para materializar la arquitectura de los sistemas?	**X**				0	0,33
0	**2**	¿La Institución considera importante contar con un plan de infraestructura tecnológica ?		**X**			0,33	
1	**3**	¿La institución esta consciente de que se necesita un análisis sobre las tecnologías existentes?		**X**			0,33	0,66
1	**4**	¿El plan de infraestructura tecnológica está acorde con los planes estratégicos de TI?		**X**			0,33	
2	**5**	¿El plan de infraestructura tecnológica es dialogado y difundido a las partes interesadas?	**X**				0	0,33
2	**6**	¿Se brinda guías sobre la tecnología selecciona para la institución?		**X**			0,33	
3	**7**	¿Se evalúa el funcionamiento de las tecnologías utilizadas por la institución?		**X**			0,33	0,99
3	**8**	¿Se mide el cumplimiento sobre los estándares tecnológicos?	**X**				0	
3	**9**	¿Se brindan asesoría sobre los productos de infraestructura tecnológica?			**X**		0,66	
4	**10**	¿Se monitorea las tendencias de infraestructura tecnológica?		**X**			0,33	1,99
4	**11**	¿Existe un proceso para monitorear el marco legal, y regulatorio sobre TI?				**X**	1	
4	**12**	¿Se proporcionan soluciones tecnológicas efectivas para todas las áreas de la institución?			**X**		0,66	
5	**13**	¿Se impulsa las prácticas tecnológicas con base en su importancia y riesgo para la institución y el cumplimiento de requerimientos externos?		**X**			0,33	0,66
5	**14**	¿El plan de infraestructura tecnológica apoya a la interoperabilidad de las plataformas?		**X**			0,33	

Tabla 18: Cuestionario PO3
Elaborado por: Acurio, Y. (2020)

PROCESO: PO3 Determinar la Dirección Tecnológica					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.33	2	0.17	0.08	0
1	0.66	2	0.33	0.17	0.17
2	0.33	2	0.17	0.08	0.16
3	0.99	3	0.33	0.17	0.51
4	1.99	3	0.66	0.33	1.32
5	0.66	2	0.33	0.17	0.85
TOTAL	4.96	14	1.99	1	3.01

Tabla 19: Nivel de madurez proceso Determinar la Dirección Tecnológica
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**3.01**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de tres (nivel de madurez 3 o definida); lo que en la escala del modelo de madurez de COBIT indica que los procesos han sido estandarizados, documentados y comunicados, sin los procedimientos no son sofisticados si no que son la formalización de las practicas existentes.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso P03: Determinar la dirección tecnológica podemos decir que en la institución si cuentan con un plan de infraestructura tecnológica como también realiza un monitoreo del marco legal y regulatorio sobre el manejo de las TI, sin embargo no hay conscientes de la importancia de analizar qué dirección tecnología es apropiada tomar para materializar la arquitectura de los sistemas, como también de que necesita realizar un análisis de las tecnologías existentes que le permitan modernizar y mejorar sus procesos.

NV	**N°**	PO4 Definir los Procesos, Organización y Relaciones de TI	De ningún modo	Un poco	Bastante	Completamente	Calificación	TOTAL
0	**1**	¿Está definido un marco de trabajo para los procesos de TI?			**X**		0,66	0,99
0	**2**	¿Hay procedimientos y herramientas que permitan enfrentar las responsabilidades de propiedad sobre los datos y los sistemas de información?		**X**			0,33	
1	**3**	¿En la estructura organizacional de TI interna se refleje las necesidades de la institución?			**X**		0,66	1,32
1	**4**	¿Existe conciencia sobre los roles y responsabilidades para el personal de TI?			**X**		0,66	
2	**5**	¿Se comunica los roles y responsabilidades para el personal de TI?				**X**	1	1,66

2	**6**	¿La alta dirección orienta con respecto al apetito de riesgo de TI?	**X**				0	
2	**7**	¿Se aseguran que el personal contratado para la administración de TI cumplan con las políticas organizacionales de protección de los activos de información ?			**X**		0,66	
3	**8**	¿Se revisan en forma general los indicadores claves de desempeño de TI?		**X**			0,33	
3	**9**	¿Existe un proceso que revise la estructura organizacional de TI de forma periódica para ajustar los requerimientos del personal?	**X**				0	
3	**10**	¿Se evalúan los requerimientos de personal de forma regular para garantizar que la función de TI cuente con los recursos suficientes para soportar adecuada y apropiadamente los objetivos institucionales?		**X**			0,33	1,65
3	**11**	¿Se tiene implementado una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico?			**X**		0,66	
3	**12**	¿Existe un proceso que revise las estrategias internas para satisfacer los objetivos institucionales y las circunstancias cambiantes?		**X**			0,33	
4	**13**	¿Los directivos toman decisiones para proteger los sistemas?	**X**				0	
4	**14**	¿Está establecida la seguridad para manejar los problemas a nivel de toda la institución?		**X**			0,33	0,66
4	**15**	¿Se tienen implementadas prácticas adecuadas de supervisión dentro de las funciones de TI?		**X**			0,33	
5	**16**	¿El marco de trabajo de procesos de TI está integrado en un sistema de administración de calidad?	**X**				0	
5	**17**	¿El marco de trabajo de procesos de TI está integrado en un marco de trabajo de control interno?			**X**		0,66	1,66
5	**18**	¿Se establecen responsabilidades de los riesgos relacionados con TI a un nivel superior apropiado?				**X**	1	

Tabla 20: Cuestionario PO4
Elaborado por: Acurio, Y. (2020)

PROCESO: PO4 Definir los Procesos, Organización y Relaciones de TI					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.99	2	0.50	0.17	0
1	1.32	2	0.66	0.23	0.23
2	1.66	3	0.55	0.20	0.40
3	1.65	5	0.33	0.12	0.36
4	0.66	3	0.22	0.08	0.32
5	1.66	3	0.55	0.20	1

TOTAL	7.94	18	2.81	1	2.31

Tabla 21: Nivel de madurez proceso Definir los Procesos, Organización y Relaciones de TI
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.31**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de COBIT indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso P04: Definir los Procesos, Organización y Relaciones de TI podemos decir que en la institución se aseguran que el personal contratado para la administración de TI realice los procesos de TI bajo los lineamientos de las normas de control internos de la Contraloría General del Estado lo que garantice una protección a los activos de información, sin embargo no se han incorporado políticas que establece la determinación de roles y funciones de cada trabajador para de esta manera reducir la posibilidad de que un solo trabajador afecte negativamente un proceso crítico.

NV	**N°**	PO5 Administrar la Inversión en TI	De ningún modo	Un poco	Bastante	Completamente	Calificación	TOTAL
0	**1**	¿Se cumple con un marco de trabajo financiero para administrar los servicios de TI?			**X**		0,66	0,99
0	**2**	¿Hay conciencia de la importancia de administrar las inversiones de TI?		**X**			0,33	
1	**3**	¿El presupuesto asignado cubre las necesidades para operar y		**X**			0,33	0,33

		mantener la infraestructura tecnológica?						
1	**4**	¿Existe un proceso para la toma de decisiones para dar prioridad a la asignación de recursos de TI?	**X**				0	
2	**5**	¿El presupuesto asignado para TI es analizado y comunicado con las partes interesadas?			**X**		0,66	1,32
2	6	¿Se comunica al personal encargado de las tecnologías de la Información sobre posibles inversiones de TI?			**X**		0,66	
3	**7**	¿Se evalúa el cumplimiento del presupuesto que fue asignado para administrar las inversiones de TI?			**X**		0,66	0,99
3	**8**	¿Se evalúa el impacto de las desviaciones sobre el presupuesto asignado para las inversiones de TI?		**X**			0,33	
4	**9**	¿Se cuenta con un proceso de monitoreo de beneficios de las inversiones realizadas en las TI?	**X**				0	0,66
4	**10**	¿Se identifica de forma oportuna si existen desviaciones en el presupuesto asignado y se los corrige?			**X**		0,66	
5	**11**	¿Se ha definido un marco de trabajo para administrar los programas de inversión de TI que abarquen costos, beneficios y prioridades dentro del presupuesto?			**X**		0,66	1,32
5	**12**	¿Los controles facilitan el uso efectivo de los recursos de TI y brinda transparencia y responsabilidad dentro del costo total de propiedad, la materialización de los beneficios y el retorno sobre las inversiones en TI?			**X**		0,66	

Tabla 22: Cuestionario PO5
Elaborado por: Acurio, Y. (2020)

PROCESO: PO5 Administrar la Inversión en TI					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.99	2	0.50	0.18	0
1	0.33	2	0.17	0.06	0.06
2	1.32	2	0.66	0.23	0.46
3	0.99	2	0.50	0.18	0.54
4	0.66	2	0.33	0.12	0.48
5	1.32	2	0.66	0.23	1.15
TOTAL	5.61	12	2.82	1	2.69

Tabla 23: Nivel de madurez proceso Administrar la Inversión en TI
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	2.69

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de COBIT indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso P05: Administrar la Inversión en TI podemos decir que en la Institución se analiza, prepara y comunica el presupuesto que será asignado para TI, así como también se asigna responsables para evaluar el cumplimiento de dicho presupuesto, sin embargo, el presupuesto que se asigna para TI no cubre las necesidades para operar y mantener la infraestructura tecnológica.

NV	N°	PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia	De ningún modo	Un poco	Bastante	Completamente	Calificación	TOTAL
0	**1**	¿Están definidos los elementos de un ambiente de control para TI?				**X**	1	1,33
0	**2**	¿Se considera importante contar con un marco de trabajo que establezca el enfoque gerencial hacia los riesgos?		**X**			0,33	
1	**3**	¿Los controles están alineados con las políticas de TI?		**X**			0,33	0,66
1	**4**	¿Las políticas son coherentes con las estrategias de TI?		**X**			0,33	
2	**5**	¿Las políticas de TI son difundidas a todo el personal relevante?		**X**			0,33	0,33
2	**6**	¿Se comunica a los usuarios internos sobre los objetivos de TI?	**X**				0	
3	**7**	¿Se verifica que las políticas de TI se implanten?			**X**		0,66	1,66
3	**8**	¿Se evalúa el cumplimiento de los objetivos de TI?				**X**	1	

4	**9**	¿Se identifica y corrige de forma oportuna posibles desviaciones en los objetivos de TI?		**X**			0,33	0,33
4	**10**	¿Se cuenta con un proceso de monitoreo para verificar el cumplimiento de las políticas de TI?	**X**				0	
5	**11**	¿La Dirección proporciona las políticas, procedimientos, directrices y otra documentación aprobada de forma precisa y entendible que se encuentre en el marco de trabajo de control de TI?		**X**			0,33	0,66
5	**12**	¿Las políticas de TI están incluidas y son parte integral de las operaciones institucionales?		**X**			0,33	

Tabla 24: Cuestionario PO6
Elaborado por: Acurio, Y. (2020)

PROCESO: PO6 COMUNICAR ASPIRACIONES					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	1.33	2	0.67	0.27	0
1	0.66	2	0.33	0.13	0.13
2	0.33	2	0.17	0.07	0.14
3	1.66	2	0.83	0.33	0.99
4	0.33	2	0.17	0.07	0.28
5	0.66	2	0.33	0.13	0.65
TOTAL	4.97	12	2.50	1	2.19

Tabla 25: Nivel de madurez proceso Comunicar Aspiraciones
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.19**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso P06: Comunicar las Aspiraciones y la Dirección de la institución podemos decir que en la Institución se han definido estándares y políticas de control para TI, sin embargo, el monitoreo de las mismas no se realiza de forma permanente, lo que indica que no existe una comunicación continua con la dirección que permita garantizar el logro de los objetivos y el cumplimiento de leyes y políticas.

NV	N°	PO7 Administrar Recursos Humanos de TI	De ningún modo	Un poco	Bastante	Completamente	Calificación	TOTAL
0	**1**	¿Está definido los requerimientos esenciales de habilidades para la contratación de personal encargado de TI?				**X**	1	1
0	**2**	¿Hay procesos que indique privilegios de acceso para contratación del personal de TI?	**X**				0	
1	**3**	¿Existe un proceso que garantice que la institución cuenta con una fuerza de trabajo apropiada?	**X**				0	0,66
1	**4**	¿Existe un marco de trabajo para la asignación de los roles y responsabilidades del personal de TI?			**X**		0,66	
2	**5**	¿Se proporciona a los empleados de TI entrenamiento continuo?		**X**			0,33	0,66
2	**6**	¿Los empleados reciben adiestramiento sobre su conducta?	**X**				0	
2	**7**	¿Se proporciona a los empleados de TI la orientación necesaria al momento de la contratación?		**X**			0,33	
3	**8**	¿Se verifican los antecedentes en el proceso de reclutamiento de TI?	**X**				0	1
3	**9**	¿Se realizan evaluaciones de desempeño al personal de TI?				**X**	1	
4	**10**	¿El nivel de supervisión es acorde con la sensibilidad del puesto y las responsabilidades asignadas?			**X**		0,66	1,66
4	**11**	¿Las evaluaciones se comparan contra los objetivos individuales derivados de las metas organizacionales?				**X**	1	
5	**12**	¿Los procesos de reclutamiento del personal están acorde a las políticas y procedimientos generales del personal de la institución?			**X**		0,66	1,66
5	**13**	¿Los procesos de selección y contratación del personal de TI son bajo el marco legal y regulatorio del Ministerio de Trabajo?				**X**	1	

Tabla 26: Cuestionario PO07
Elaborado por: Acurio, Y. (2020)

PROCESO: PO7 Administrar Recursos Humanos de TI					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	1	2	0.50	0.16	0
1	0.66	2	0.33	0.10	0.10
2	0.66	3	0.22	0.06	0.12
3	1	2	0.50	0.16	0.48
4	1.66	2	0.83	0.26	1.04
5	1.66	2	0.83	0.26	1.3
TOTAL	6.64	13	3.21	1	3.04

Tabla 27: Nivel de madurez proceso Administrar Recursos Humanos de TI
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**3.04**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de tres (nivel de madurez 3 o definida); lo que en la escala del modelo de madurez de cobit indica que los procesos han sido estandarizados, documentados y comunicados, sin los procedimientos no son sofisticados si no que son la formalización de las practicas existentes.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso P07: Administrar Recursos Humanos de TI podemos decir que los procesos para selección y contratación del personal encargado del manejo de TI están acorde a las políticas y procedimientos

generales de la institución como también bajo los lineamientos del marco legal y regulatorio del Ministerio del Trabajo, sin embargo no se proporciona la orientación necesaria sobre sus funciones, responsabilidades y conducta al momento de la contratación.

NV	N°	PO8 Administrar la Calidad	De ningún modo	Un poco	Bastante	Completamente	Calificación	TOTAL
0	**1**	¿Para la Gerencia es importante contar con un sistema de administración de calidad para TI?			**X**		0,66	0,66
0	**2**	¿En los requerimientos de calidad no se manifiestan y documentan con indicadores cuantificables y alcanzables?	**X**				0	
1	**3**	¿El sistema de calidad está alineado a los requerimientos de la institución?	**X**				0	1,66
1	**4**	¿están enfocados a la administración de calidad en los usuarios externos?			**X**		0,66	
1	**5**	¿Se incluye estándares para la interfaz de usuario?				**X**	1	
2	**6**	¿El sistema de calidad identifica los procesos claves de TI y se los comunica a las partes interesadas?	**X**				0	0,66
2	**7**	¿Se maneja interoperabilidad?			**X**		0,66	
3	**8**	¿Se cumple con estándares de codificación de software?			**X**		0,66	0,66
3	**9**	¿Se evalúa el sistema de administración de calidad de TI?	**X**				0	
3	**10**	¿Se evalúa el nivel de aceptación del sistema de administración de calidad?	**X**				0	
4	**11**	¿Se realiza un monitoreo a las metas de calidad de TI?	**X**				0	0
4	**12**	¿Se monitorea la efectividad del sistema de administración de calidad?	**X**				0	
5	**13**	¿El sistema de administración de calidad es sofisticado e identifica políticas para definir, detectar, corregir y prever las no conformidades?	**X**				0	0,33
5	**14**	¿Se promueve un plan global de calidad que aporte a la mejora continua para la administración de TI?		**X**			0,33	
5	**15**	¿El sistema de administración de calidad proporciona un enfoque estándar, formal y continuo?	**X**				0	

Tabla 28: Cuestionario PO8
Elaborado por: Acurio, Y. (2020)

PROCESO: PO8 Administrar la Calidad					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.66	2	0.33	0.21	0
1	1.66	3	0.55	0.36	0.36
2	0.66	2	0.33	0.21	0.42
3	0.66	3	0.22	0.14	0.42
4	0	2	0	0	0
5	0.33	3	0.11	0.08	0.4
TOTAL	3.97	15	1.54	1	1.6

Tabla 29: Nivel de madurez proceso Administrar la Calidad
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**1.6**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de uno (nivel de madurez 1 o inicial); lo que en la escala del modelo de madurez de COBIT indica que hay evidencia de que la organización ha reconocido los problemas existentes y que necesitan ser resueltos. El método general de la administración es desorganizado.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso P08: Administrar la Calidad podemos decir que la empresa no cuenta con un proceso de administración de calidad entre sus operaciones, sin embargo, está consciente de la necesidad de contar con un sistema de calidad para TI que garantice la mejora continua y la satisfacción de los usuarios interno y externos de la institución.

NV	**N°**	PO9 Evaluar y Administrar los Riesgos de TI	De ningún modo	Un poco	Bastante	Completamente	Calificación	TOTAL

0	**1**	¿Se ha establecido un marco de trabajo de administración de riesgos de TI?				**X**	1	1,33
0	**2**	¿Hay procedimientos que identifiquen las amenazas importantes con impacto potencial negativo sobre las metas o las operaciones de la institución?		**X**			0,33	
1	**3**	¿El marco de trabajo de administración de riesgos de TI está alineado al marco de trabajo de administración de riesgos de la institución?		**X**			0,33	0,33
1	**4**	¿El proceso de respuesta a riesgos considera los niveles de tolerancia a riesgos?	**X**				0	
2	**5**	¿Se comunica el impacto de los riesgos identificados de TI?				**X**	1	1,66
2	**6**	¿Se analiza y comunica los procedimientos para gestionar los riesgos identificados?			**X**		0,66	
3	**7**	¿Se evalúa la probabilidad e impacto de todos los riesgos identificados de TI?		**X**			0,33	0,99
3	**8**	¿Se aplica el marco de trabajo para la evaluación de riesgos?			**X**		0,66	
4	**9**	¿Se cuenta con un proceso de respuesta a riesgo diseñado para asegurar que los controles efectivos mitigan los riesgos?		**X**			0,33	0,99
4	**10**	¿Se monitorea la ejecución de planes para mitigar los riesgos identificados?			**X**		0,66	
5	**11**	¿Se prioriza las actividades de control a todos los niveles para implementar las respuestas a los riesgos?			**X**		0,66	0,99
5	**12**	¿El proceso de respuesta a riesgos identifica estrategias tales como evitar, reducir, compartir o aceptar riesgos?		**X**			0,33	

Tabla 30: Cuestionario PO
Elaborado por: Acurio, Y. (2020)

PROCESO: PO9 Evaluar y Administrar los Riesgos de TI					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	1.33	2	0.67	0.21	0
1	0.33	2	0.17	0.05	0.05
2	1.66	2	0.83	0.26	0.52
3	0.99	2	0.50	0.16	0.48
4	0.99	2	0.50	0.16	0.64
5	0.99	2	0.50	0.16	0.8
TOTAL	6.29	12	3.17	1	2.49

Tabla 31: Nivel de madurez proceso Evaluar y Administrar los Riesgos de TI
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.49**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso P09: Evaluar y Administrar los Riesgos de TI podemos decir que se ha definido un proceso para la mitigación de riesgos, sin embargo, este se aplica conforme se presenta los riesgos lo cual evidencia que no hay una adecuada gestión de riesgos que permita alinearlos a un nivel de tolerancia aceptable.

NV	**N°**	PO10 Administrar Proyectos	De ningún modo	Un poco	Bastante	Completamente	Calificación	TOTAL
0	**1**	¿Hay compromiso de los interesados en los proyectos de TI?				**X**	1	1,33
0	**2**	¿Existe un entendimiento común sobre el alcance de los proyectos de TI?		**X**			0,33	
1	**3**	¿Se define las responsabilidades y criterios de desempeño de los miembros del equipo del proyecto?				**X**	1	2
1	**4**	¿Está establecido un enfoque de administración de proyectos que corresponda al tamaño de cada proyecto?				**X**	1	
2	**5**	¿Se comunica a todos los interesados sobre las etapas de los proyectos?				**X**	1	2
2	**6**	¿Se comunica cualquier actividad requerida para alcanzar los resultados planteados los proyectos?				**X**	1	
3	**7**	¿Se evalúa el cumplimiento de los proyectos de TI?				**X**	1	2
3	**8**	¿Se realiza un control para los cambios que se realiza en los proyectos de TI?				**X**	1	
4	**9**	¿Se implementa medidas correctivas en caso de desviaciones en el desarrollo del proyecto?				**X**	1	2
4	**10**	¿Se supervisa que los responsables de la ejecución de los proyectos cumplan con los requerimientos de la institución?				**X**	1	

5	**11**	¿El marco de trabajo define las metodologías a ser adoptadas y aplicadas en cada proyecto emprendido?				**X**	1	2
5	**12**	¿Se aseguran de que todos los proyectos cuenten con presupuesto suficiente para su ejecución?				**X**	1	

Tabla 32: Cuestionario PO10
Elaborado por: Acurio, Y. (2020)

PROCESO: P010 Administrar Proyectos					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	1.33	2	0.67	0.12	0
1	2	2	1	0.18	0.18
2	2	2	1	0.18	0.36
3	2	2	1	0.18	0.54
4	2	2	1	0.18	0.72
5	2	2	1	0.18	0.9
TOTAL	11.33	12	5.67	1.02	2.7

Tabla 33: Nivel de madurez proceso Administrar Proyectos
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.7**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso P010: Administrar Proyectos podemos decir que se ha establecido un enfoque de administración de proyectos de acuerdo con su tamaño, así como también se define claramente el

presupuesto asignado, funciones y las actividades de desempeño de los miembros que conforman el proyecto, sin embargo, no hay un entendimiento común sobre el alcance de los proyectos de TI lo que evidencia una falta de comunicación.

4.1.1.2 Dominio 2: Adquirir e Implementar (AI)

NV	N°	AI1 Identificar soluciones automatizadas	De ningún modo	Un poco	Bastante	Completamente	Calificacion	Total
0	**1**	¿La institución identifica los requerimientos funcionales y operativos para el desarrollo, implementación o modificación de soluciones, como por ejemplo soluciones de sistema, de servicio, de infraestructura, de software y de datos?			**X**		0,66	0,99
0	**2**	¿La institución mantiene conciencia sobre las soluciones tecnológicas disponibles que son potencialmente relevantes para su desarrollo?		**X**			0,33	
1	**3**	¿Hay conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas??		**X**			0,33	0,66
1	**4**	¿Los grupos individuales tienden a reunirse para discutir necesidades de manera informal y los requerimientos por lo general no están documentados?		**X**			0,33	
2	**5**	¿Hay algunos enfoques intuitivos para identificar las soluciones de TI y los mismos varían en toda la institución??			**X**		0,66	2,98
2	**6**	¿Las soluciones son identificadas de manera informal sobre la base de la experiencia interna y de los conocimientos de la función de TI. El éxito de cada proyecto depende de la experiencia de unas pocas personas claves de TI.?				**X**	1	
2	**7**	¿La calidad de la documentación y de la toma de decisiones varía considerablemente?			**X**		0,66	
2	**8**	¿Se emplean enfoques sin estructura para definir los requerimientos e identificar las soluciones de tecnología??			**X**		0,66	
3	**9**	¿Se usan métodos claros y estructurados para determinar las soluciones de TI.?		**X**			0,33	1,32
3	**10**	¿El método para la determinación de soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del usuario o de la institución, las oportunidades tecnológicas, la factibilidad económica, los análisis de riesgos y otros factores?		**X**			0,33	

3	**11**	¿El proceso para la determinación de soluciones de TI se aplica a algunos proyectos basándose en factores como las decisiones hechas por el personal involucrado, la cantidad de tiempo de administración dedicado y el tamaño y la prioridad del requerimiento original de la institución??		**X**			0,33	
3	**12**	¿Se emplean métodos estructurados para definir los requerimientos e identificar las soluciones de TI.?		**X**			0,33	
4	**13**	¿Existe una metodología establecida para la identificación y evaluación de soluciones de TI y la misma se emplea para la mayoría de los proyectos??	**X**				0	1,65
4	**14**	¿La documentación de proyectos es de buena calidad y cada etapa es debidamente aprobada??			**X**		0,66	
4	**15**	¿Los requerimientos son bien articulados y están en conformidad con estructuras predefinidas.?		**X**			0,33	
4	**16**	¿Se consideran soluciones alternativas, incluyendo un análisis de costos y ganancias? ?		**X**			0,33	
4	**17**	¿La metodología es clara, definida, generalmente comprendida y medible.?	**X**				0	
4	**18**	¿Hay una interfaz claramente definida entre la administración de TI y la institución respecto a la identificación y evaluación de soluciones de TI.?		**X**			0,33	
5	**19**	¿La metodología para la identificación y evaluación de soluciones de TI se mejora continuamente??		**X**			0,33	2,28
5	**20**	¿La metodología de adquisición e implementación es lo suficientemente flexible para acomodar proyectos de pequeña y gran escala?		**X**			0,33	
5	**21**	¿La metodología es apoyada por bases de datos de conocimientos internas y externas que contienen materiales de referencia sobre soluciones tecnológicas.?		**X**			0,33	
5	**22**	¿La metodología misma produce documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento?		**X**			0,3	
5	**23**	¿La organización puede a menudo identificar nuevas oportunidades para utilizar la tecnología para ganar ventaja competitiva, influir en el proceso de reingeniería del negocio y mejorar la eficiencia general?		**X**			0,33	
5	**24**	¿La gerencia detecta y actúa en consecuencia si las soluciones de TI son aprobadas sin considerar tecnologías alternativas o requerimientos funcionales de negocio?			**X**		0,66	

Tabla 34: Cuestionario AI1
Elaborado por: Acurio, Y. (2020)

PROCESO: AI1 Identificar soluciones automatizadas					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**

Nivel de Madurez	Suma de valores de cumplimiento	Número de declaraciones	Valor de cumplimiento (B/C)	Normalización del vector de cumplimiento (D/∑D)	Nivel de madurez (A*E)
0	0.99	2	0.50	0.19	0
1	0.66	2	0.33	0.13	0.13
2	2.98	4	0.75	0.29	0.58
3	1.32	4	0.33	0.13	0.39
4	1.65	6	0.28	0.11	0.44
5	2.28	6	0.38	0.15	0.75
TOTAL	9.88	24	2.57	1	2.29

Tabla 35: Nivel de madurez proceso Identificar soluciones automatizadas
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.29**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso AI1: Identificar soluciones automatizadas podemos decir que en la institución las soluciones son identificadas de manera informal, una vez que hay surgido el problema actúan en base a la experiencia interna y sobre los conocimientos de TI por lo tanto el éxito de cada proyecto depende de la experiencia y responsabilidad de unas pocas personas, lo que indica un alto grado de confianza en sus conocimientos y por ende es probable que haya errores.

NV	N°	AI2 Adquirir y Mantener Software Aplicativo	De ningún modo	Un poco	Bastante	Completamente	calificación	Total

0	**1**	¿Existe un diseño y especificación de aplicaciones?			**X**		0,66	
0	**2**	¿Generalmente las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales?			**X**		0,66	1,32
1	**3**	¿Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones?			**X**		0,66	
1	**4**	¿Los enfoques para adquisición y mantenimiento de software aplicativo varían de un proyecto a otro?				**X**	1	1,99
1	**6**	¿Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño y adquisición de software aplicativo?		**X**			0,33	
2	**7**	¿Hay procesos diferentes pero similares para adquirir y mantener aplicaciones basados en la experiencia dentro de la función de TI?			**X**		0,66	
2	**8**	¿La tasa de éxito de las aplicaciones depende en gran medida de las habilidades internas y de los niveles de experiencia dentro de la TI?			**X**		0,66	
2	**9**	¿El mantenimiento es usualmente problemático y sufre cuando se perdieron conocimientos internos de la institución?		**X**			0,33	1,65
2	**10**	¿Al diseñar o adquirir el software de aplicación se presta poca o ninguna consideración a la seguridad y disponibilidad de la aplicación?	**X**				0	
3	**11**	¿Hay un proceso claro, definido y generalmente comprendido para la adquisición e implementación de software de aplicación?				**X**	1	
3	**12**	¿Se intentan aplicar coherentemente los procesos documentados en todos los proyectos y aplicaciones diferentes?				**X**	1	2,66
3	**13**	¿Las metodologías son generalmente inflexibles y difíciles de aplicar a todos los casos, de modo que los pasos son frecuentemente omitidos?		**X**			0,33	
3	**14**	¿Las actividades de mantenimiento son planificadas, programadas y coordinadas?		**X**			0,33	
4	**15**	¿Hay una metodología formal, clara y bien entendida que incluye un proceso de diseño y especificación, criterios para la adquisición de software de aplicación, un proceso para realizar pruebas y requerimientos para la documentación?			**X**		0,66	1,32
4	**17**	¿Las prácticas y procedimientos evolucionaron y se adecuan a la institución, son usados por todo el personal, y se aplican a la mayoría de los requerimientos de aplicación?			**X**		0,66	
5	**18**	¿Las prácticas de adquisición y mantenimiento de software de aplicación están alineadas con los procesos definidos?			**X**		0,66	
5	**20**	¿La metodología de adquisición y mantenimiento es avanzada, posibilita una rápida implementación y permite una alta capacidad de respuesta y flexibilidad para responder a los requerimientos cambiantes del negocio?		**X**			0,33	1,98
5	**21**	¿La metodología de adquisición e implementación de software de aplicación está sujeta a una mejora continua y es respaldada por bases de datos de conocimientos internas y externas que			**X**		0,66	

		contienen materiales de referencia y buenas prácticas?						
5	**22**	¿La metodología genera documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento?		**X**			0,33	

Tabla 36: Cuestionario AI2
Elaborado por: Acurio, Y. (2020)

PROCESO: AI2 Adquirir y Mantener Software Aplicativo					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	1.32	2	0.66	0.18	0
1	1.99	3	0.66	0.18	0.18
2	1.65	4	0.41	0.12	0.24
3	2.66	4	0.67	0.19	0.57
4	1.32	2	0.66	0.19	0.76
5	1.98	4	0.50	0.14	0.70
TOTAL	10.92	19	3.56	1	2.45

Tabla 37: Nivel de madurez proceso Adquirir y Mantener Software Aplicativo
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.45**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso AI2: Adquirir y Mantener Software Aplicativo podemos decir que para la institución no se considera un tema muy

importante el diseño, aplicación o adquisición de software aplicativo, razón por la que el mantenimiento y soporte de los mismos en ocasiones es problemático y más cuando hay perdidas de información.

NV	N°	AI3 Adquirir y Mantener Infraestructura Tecnológica	De ningún modo	Un poco	Bastante	Completamente	Calificacion	Total
0	**1**	¿La arquitectura de la tecnología no es considerada un tema lo suficientemente importante como para ser tratado?		**X**			0,33	0,33
1	**2**	¿Se hacen cambios a la infraestructura para cada nueva aplicación sin un plan general?			**X**		0,66	
1	**3**	¿A pesar de que hay conciencia de que la infraestructura de TI es importante, no hay un método general coherente?	**X**				0	0,99
1	**4**	¿Las actividades de mantenimiento reaccionan a las necesidades a corto plazo? ¿El entorno de producción es el entorno de pruebas?		**X**			0,33	
2	**5**	¿Hay coherencia entre los métodos tácticos, cuando se adquiere y se mantiene la infraestructura de TI?		**X**			0,33	
2	**6**	¿La adquisición y el mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que deben ser apoyadas?			**X**		0,66	1,98
2	**7**	¿Hay una comprensión de que la infraestructura de TI es importante, y dicha comprensión es apoyada por algunas prácticas formales?			**X**		0,66	
2	**8**	¿Se programa algún mantenimiento, pero el mismo no es programado y coordinado completamente?		**X**			0,33	
3	**9**	¿Existe un proceso claro, definido y generalmente entendido para adquirir y mantener la infraestructura de TI?		**X**			0,33	
3	**11**	¿Las actividades de mantenimiento son planificadas, programadas y coordinadas?		**X**			0,33	0,99
3	**12**	¿Existen entornos separados para pruebas y producción?		**X**			0,33	
4	**13**	¿El proceso de adquisición y mantenimiento para la infraestructura tecnológica se ha desarrollado hasta el punto de que funciona bien para la mayoría de las situaciones, es seguido coherentemente y se concentra en la reutilización?		**X**			0,33	
4	**14**	¿La infraestructura de TI soporta de manera adecuada las aplicaciones de negocio?		**X**			0,33	1,32
4	**15**	¿El proceso de adquisición y mantenimiento para la infraestructura tecnología está bien organizado y es proactivo?		**X**			0,33	
4	**16**	¿El costo y el tiempo para alcanzar el nivel esperado de escalabilidad, flexibilidad e integración está parcialmente optimizado?		**X**			0,33	
5	**17**	¿El proceso de adquisición y mantenimiento para la infraestructura tecnológica es proactivo y está estrechamente alineado con aplicaciones críticas de la institución y con la arquitectura de la tecnología?		**X**			0,33	0,99
5	**18**	¿Se siguen las mejores prácticas respecto a soluciones de tecnología y la organización		**X**			0,33	

		está al tanto de los últimos desarrollos en plataformas y herramientas de administración?						
5	**19**	¿Los costos son reducidos racionalizando y estandarizando los componentes de la infraestructura y usando la automatización?		**X**			0,33	
5	**20**	¿La infraestructura de TI es vista como el posibilitador clave para aprovechar el uso de la TI?	**X**				0	

Tabla 38: Cuestionario AI3
Elaborado por: Acurio, Y. (2020)

PROCESO: AI3 Adquirir y Mantener Infraestructura Tecnológica					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.33	1	0.33	0.16	0
1	0.99	3	0.33	0.16	0.16
2	1.98	4	0.50	0.24	0.48
3	0.99	3	0.33	0.16	0.48
4	1.32	4	0.33	0.16	0.64
5	0.99	4	0.25	0.12	0.60
TOTAL	6.60	19	2.07	1	2.36

Tabla 39: Nivel de madurez proceso Adquirir y Mantener Infraestructura Tecnológica
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.36**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso AI3: Adquirir y Mantener Infraestructura Tecnológica podemos decir que en la institución pese a existir

infraestructura tecnológica bien definida no existe un método adecuado ya que se evidencia pocos procesos claros y bien definidos para adquirir infraestructura de tecnología de información.

NV	N°	AI4 Facilitar la Operación y el Uso	De ningún modo	Un poco	Bastante	Completamente	Calificacion	Total
0	**1**	¿No hay ningún proceso establecido respecto a la producción de documentación de usuario, manuales de operaciones y material de capacitación?	**X**				0	0
0	**2**	¿Los únicos materiales que existen son los suministrados con los productos comprados?	**X**				0	
1	**3**	¿La organización está consciente de que se necesita un proceso que resuelva la documentación?		**X**			0,33	1,65
1	**4**	¿La documentación se produce ocasionalmente y está distribuida desigualmente entre grupos limitados?		**X**			0,33	
1	**5**	¿Gran parte de la documentación y de los procedimientos son obsoletos?		**X**			0,33	
1	**6**	¿Los materiales de capacitación tienden a ser esquemas que se usan una sola vez con calidad variable?		**X**			0,33	
1	**7**	¿Prácticamente no hay integración de los procedimientos en todos los diferentes sistemas y unidades de la institución?	**X**				0	
1	**8**	¿No hay colaboración por parte de las unidades de la institución en el diseño de programas de capacitación?		**X**			0,33	
2	**9**	¿Se usan enfoques similares para producir procedimientos y documentación, pero los mismos no están basados en un enfoque o marco estructurado?		**X**			0,33	0,66
2	**10**	¿No hay un enfoque uniforme para el desarrollo de procedimientos operativos y de usuario?	**X**				0	
2	**11**	¿Los procedimientos y la calidad del soporte de usuario varían de pobre a muy bueno, con muy poca coherencia e integración en toda la organización?	**X**				0	
2	**12**	¿Se proveen o facilitan los programas de capacitación para la institucion y los usuarios, pero no hay un plan general para la entrega e implementación de capacitación?		**X**			0,33	
3	**13**	¿Hay un marco claramente definido, aceptado y entendido para la documentación del usuario, los manuales de operaciones y los materiales de capacitación?		**X**			0,33	1,98
3	**14**	¿Los procedimientos son almacenados y mantenidos en una biblioteca formal y pueden ser accedidos por cualquiera que necesite saber?	**X**				0	
3	**15**	¿Se hacen correcciones a la documentación y los procedimientos de manera reactiva?		**X**			0,33	
3	**16**	¿Se cuenta con procedimientos fuera de línea y éstos pueden ser accedidos y mantenidos en caso de desastre?			**X**		0,66	
3	**17**	¿A pesar de la existencia de enfoques definidos, el contenido real varía porque no hay control para hacer cumplir las normas?		**X**			0,33	
3	**18**	¿Se usan cada vez más herramientas automatizadas para la generación y distribución de procedimientos?		**X**			0,33	

4	**19**	¿Los procedimientos y los materiales de capacitación están integrados para incluir interdependencias e interfaces?		**X**			0,33	
4	**20**	¿Existen controles para asegurar que las normas se cumplen y que los procedimientos se desarrollen y se mantengan para todos los procesos?			**X**		0,66	
4	**21**	¿La realimentación de la institución y de los usuarios acerca de la documentación y la capacitación se recopila y evalúa como parte de un proceso de mejora continua?		**X**			0,33	
4	**22**	¿La documentación y los materiales de capacitación están por lo general a un buen nivel predecible de confiabilidad y disponibilidad?			**X**		0,66	3,3
4	**23**	¿Está emergiendo un proceso para documentar y administrar procedimientos de forma automática?			**X**		0,66	
4	**24**	¿El desarrollo de procedimientos automatizados está cada vez más integrado con el desarrollo de sistemas de aplicación, facilitando la coherencia y el acceso de los usuarios?		**X**			0,33	
4	**25**	¿La gerencia de TI está desarrollando métricas para el desarrollo y la entrega de documentación, materiales de capacitación y programas de capacitación?		**X**			0,33	
5	**26**	¿El proceso para la documentación operativa y de usuarios es mejorado continuamente a través de la adopción de nuevas herramientas o métodos?		**X**			0,33	0,66
5	**27**	¿El material está actualizado para reflejar cambios organizacionales, operativos y de software?		**X**			0,33	

Tabla 40: Cuestionario AI4
Elaborado por: Acurio, Y. (2020)

PROCESO: AI4 Facilitar la Operación y el Uso					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0	2	0	0	0
1	1.65	6	0.26	0.17	0.17
2	0.66	4	0.17	0.11	0.22
3	1.98	6	0.33	0.21	0.63
4	3.3	7	0.47	0.30	1.2
5	0.66	2	0.33	0.21	1.05
TOTAL	8.25	27	1.56	1	3.27

Tabla 41: Nivel de madurez proceso Facilitar la Operación y el Uso
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**3.27**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de tres (nivel de madurez 3 o definida); lo que en la escala del modelo de madurez de cobit indica que los procesos han sido estandarizados, documentados y comunicados, sin los procedimientos no son sofisticados si no que son la formalización de las practicas existentes.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso AI4: Facilitar la Operación y el Uso podemos decir que en la institución si se han establecido procesos respecto a la producción de documentación de usuario, manuales de operaciones y material de capacitación, sin embargo, no se realiza controles para verificar el cumplimiento de los mismos por lo que es improbable que se detecten desviaciones.

NV	N°	AI5 Adquirir Recursos de TI	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	**1**	¿No está definido un proceso de abastecimiento de TI?	**X**				0	0
0	**2**	¿La institución no reconoce la importancia de mejorar los controles que garanticen el cumplimiento de reglamentos legales y regulatorios para la adquisición de todos los recursos de TI?	**X**				0	
1	**3**	¿Se desarrollan y administran contratos para la adquisición de los recursos de TI por parte de los administradores de proyecto y otras personas que emplean su juicio profesional en lugar de políticas y procedimientos formales?		**X**			0,33	0,99
1	**4**	¿Existe una relación ad hoc entre la TI y los procesos de adquisición corporativa y de administración de contratos?			**X**		0,66	
1	**5**	¿Los contratos de adquisición se administran al finalizar los proyectos en lugar de hacerlo de forma continua?	**X**				0	
2	**6**	¿Hay conciencia en la organización acerca de la necesidad de contar con políticas y procedimientos para la adquisición de TI?			**X**		0,66	1,65
2	**7**	¿Las responsabilidades para desarrollar el proyecto y administrar el contrato se han asignado a diferentes funcionarios?		**X**			0,33	
2	**8**	¿La persona asignada como administrador de contrato cumple con la experiencia y conocimientos para administrar el proyecto?			**X**		0,66	

2	**9**	¿Los procesos de contratos se utilizan mayormente para proyectos de gran porte y visibilidad?	**X**				0	
3	**10**	¿La gerencia establece políticas y procedimientos para la adquisición de TI?			**X**		0,33	
3	**11**	¿Existen estándares de TI para la adquisición de recursos de TI?			**X**		0,33	
3	**12**	¿Los proveedores de recursos de TI están integrados en los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos?				**X**	1	2,66
3	**13**	¿La gerencia de TI comunica la necesidad de una administración de adquisiciones y contratos adecuada en toda la función de TI?				**X**	1	
4	**14**	¿Los estándares de TI para la adquisición de recursos de TI se usan para todos los abastecimientos?	**X**				0	
4	**15**	¿Se realizan informes sobre las actividades de adquisición de TI?			**X**		0,66	
4	**16**	¿La gerencia generalmente es consciente de las excepciones a las políticas y procedimientos para la adquisición de TI?			**X**		0,66	2,65
4	**17**	¿Comienza a desarrollarse una administración estratégica de relacionamiento?		**X**			0,33	
4	**18**	¿La gerencia de TI exige el uso del proceso de adquisición y administración de contratos para todas las adquisiciones al revisar las mediciones de desempeño?				**X**	1	
5	**19**	¿La gerencia exige el cumplimiento de las políticas y procedimientos para la adquisición de TI?				**X**	1	
5	**20**	¿Los estándares, políticas y procedimientos de TI para la adquisición de recursos de TI se administran estratégicamente y responden a las medidas del proceso?		**X**			0,33	2,33
5	**21**	¿La gerencia de TI comunica la importancia estratégica de una administración de adquisiciones y contratos adecuada en toda la función de TI?				**X**	1	

Tabla 42: Cuestionario AI5
Elaborado por: Acurio, Y. (2020)

PROCESO: AI5 Adquirir Recursos de TI					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0	2	0	0	0
1	0.99	3	0.33	0.12	0.12
2	1.65	4	0.41	0.15	0.30
3	2.66	4	0.67	0.25	0.75
4	2.65	5	0.53	0.19	0.76
5	2.33	3	0.78	0.29	1.45
TOTAL	10.28	21	2.72	1	3.38

Tabla 43: Nivel de madurez proceso Adquirir Recursos de TI

Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**3.38**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de tres (nivel de madurez 3 o definida); lo que en la escala del modelo de madurez de cobit indica que los procesos han sido estandarizados, documentados y comunicados, sin los procedimientos no son sofisticados si no que son la formalización de las practicas existentes.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso AI5: Adquirir Recursos de TI podemos decir que en la institución reconoce la importancia de mejorar los controles que garanticen el cumplimiento de reglamentos legales y regulatorios para la adquisición de todos los recursos de TI, sin embargo, las responsabilidades no se han dividido adecuadamente ya que en ocasiones la persona que ha realizado el presupuesto del proyecto también se le asignado como administrador de contrato por lo que hace improbable que se detecten desviaciones ya que la responsabilidad se le ha dejado a un solo individuo.

NV	N°	AI6 Administrar Cambios	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	**1**	¿No hay un proceso definido de administración de cambios y se pueden hacer cambios prácticamente sin control alguno?		**X**			0,33	0,66
0	**2**	¿No hay consciencia de que los cambios pueden causar interrupciones tanto para la TI como para las operaciones de la institución, y ninguna conciencia de los beneficios de una buena administración de cambios?		**X**			0,33	
1	**3**	¿Se reconoce que los cambios deben ser administrados y controlados? Las prácticas varían y es probable que ocurran cambios no autorizados?		**X**			0,33	1,66
1	**4**	¿Hay documentación insuficiente o inexistente de cambios, y la documentación de		**X**			0,33	

		configuración está incompleta y no es confiable?						
1	**5**	¿Es probable que ocurran errores junto con interrupciones en el entorno de producción causados por una administración deficiente del cambio?				**X**	1	
2	**6**	¿Está establecido un proceso informal de administración de cambios y la mayoría de los cambios siguen este método; sin embargo, el mismo no está estructurado y es rudimentario y propenso a errores?			**X**		0,66	0,66
3	**9**	¿El análisis de impacto a los cambios de TI sobre las operaciones de la institución se están volviendo formales para apoyar la ejecución de los planes para nuevas aplicaciones y tecnologías?		**X**			0,33	0,33
4	**10**	¿El proceso de administración de cambios está bien desarrollado y es seguido de manera coherente para todos los cambios, y la gerencia tiene certeza de que apenas hay excepciones?		**X**			0,33	2,31
4	**12**	¿Todos los cambios están sujetos a una planificación y estudio de impacto exhaustivos para minimizar la probabilidad de problemas posteriores a la producción?		**X**			0,33	
4	**13**	¿Está establecido un proceso de aprobación para los cambios?			**X**		0,66	
4	**14**	¿La documentación de administración de cambios está al día y es correcta, y los cambios son seguidos formalmente?		**X**			0,33	
4	**15**	¿La documentación de configuración generalmente es precisa?			**X**		0,66	
4	**18**	¿Existe un proceso coherente para monitorear la calidad y el desempeño del proceso de administración de cambios?	**X**				0	
5	**19**	¿El proceso de administración de cambios es revisado y actualizado regularmente para mantenerse en línea con las mejores prácticas?		**X**			0,33	1,65
5	**20**	¿El proceso de revisión refleja los resultados del monitoreo?		**X**			0,33	
5	**21**	¿La información de configuración está automatizada y provee control de versiones?			**X**		0,66	
5	**22**	¿ El seguimiento de cambios es sofisticado e incluye herramientas para detectar software sin licencia o autorización?		**X**			0,33	

Tabla 44: Cuestionario AI6
Elaborado por: Acurio, Y. (2020)

PROCESO: AI6 Administrar Cambios					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.66	2	0.33	0.12	0
1	1.66	3	0.55	0.21	0.23
2	0.66	1	0.66	0.25	0.50
3	0.33	1	0.33	0.12	0.36
4	2.31	6	0.39	0.15	0.60

5	1.65	4	0.41	0.15	0.75
TOTAL	7.27	17	2.67	1	2.44

Tabla 45: Nivel de madurez proceso Administrar Cambios
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.44**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso AI6 Administrar Cambios podemos decir que en la institución si identifica que los cambios realizados deben ser gerenciados oportunamente, por lo que se ha establecido un proceso para aprobación de cambios, sin embargo no hay una planificación ni una evaluación del impacto que eviten las interrupciones tanto para TI como para las operaciones de la institución como tampoco hay un seguimiento sofisticado por lo que en ocasiones los cambios no se detecta software sin licencia o los cambios realizados no están autorizados.

NV	N°	AI7 Instalar y Acreditar Soluciones y Cambios	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	**1**	¿Hay una total falta de procesos formales de instalación o acreditación y ni la alta gerencia o el personal de TI reconoce la necesidad de verificar que las soluciones sean adecuadas para el propósito que se pretende?		**X**			0,33	0,33
1	**2**	¿No hay conciencia de la necesidad de verificar y confirmar que las soluciones implementadas sirven para el propósito que se pretende?	**X**				0	0,66
1	**3**	¿Se realizan pruebas para algunos proyectos, pero la iniciativa de realizar pruebas es dejada		**X**			0,33	

		en manos de los equipos individuales de proyecto y los enfoques emprendidos varían?						
1	**4**	¿La acreditación y autorización formal es poco frecuente o no existe en absoluto?		**X**			0,33	
2	**6**	¿Los equipos de desarrollo individual normalmente deciden el método de prueba y hay por lo general ausencia de pruebas de integración?		**X**			0,33	0,33
2	**7**	¿Hay un proceso informal de aprobación?	**X**				0	
3	**8**	¿Está establecida una metodología formal relativa a la instalación, migración, conversión y aceptación?			**X**		0,66	1,32
3	**9**	¿Los procesos de instalación y acreditación de TI están integrados en el ciclo de vida del sistema y están automatizados en cierta medida?			**X**		0,66	
4	**12**	¿Los procedimientos son formalizados y desarrollados para que estén bien organizados y sean prácticos, con entornos de prueba y procedimientos de acreditación definidos. En la práctica, todos los grandes cambios a los sistemas siguen este método formal?		**X**			0,33	1,98
4	**13**	¿La evaluación de la satisfacción de los requerimientos de usuario está estandarizada y se puede medir, produciendo métricas que pueden ser revisadas y analizadas efectivamente por la gerencia?		**X**			0,33	
4	**14**	¿La calidad de los sistemas que entran en producción es satisfactoria para la gerencia, con niveles razonables de problemas posteriores a la implementación?		**X**			0,33	
4	**16**	¿El sistema de pruebas refleja adecuadamente el entorno real?		**X**			0,33	
4	**17**	¿Las pruebas de estrés para los sistemas nuevos y las pruebas de regresión para los sistemas existentes se aplican para los proyectos de gran porte?			**X**		0,66	
5	**18**	¿Los procesos de instalación y acreditación han sido refinados hasta el nivel de la mejor práctica, basados en los resultados del mejoramiento y refinamiento continuo?		**X**			0,33	2,31
5	**19**	¿Los procesos de instalación y acreditación de TI están totalmente integrados en el ciclo de vida del sistema y automatizados donde es conveniente, facilitando la capacitación, prueba y transición al estado de producción de nuevos sistemas de forma más eficiente?			**X**		0,66	
5	**20**	¿Los entornos de prueba bien desarrollados, los registros de problemas y los procesos de resolución de fallas aseguran una transición eficiente y efectiva al entorno de producción?		**X**			0,33	
5	**22**	¿Las revisiones posteriores a la implementación están también estandarizadas, con lecciones aprendidas canalizadas nuevamente al proceso para asegurar una mejora continua de la calidad?		**X**			0,33	
5	**23**	¿Las pruebas de estrés para los sistemas nuevos y las pruebas de regresión para los sistemas existentes se aplican por igual?			**X**		0,66	

Tabla 46: Cuestionario AI7
Elaborado por: Acurio, Y. (2020)

PROCESO: AI7 Instalar y Acreditar Soluciones y Cambios					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**

Nivel de Madurez	Suma de valores de cumplimiento	Número de declaraciones	Valor de cumplimiento (B/C)	Normalización del vector de cumplimiento (D/∑D)	Nivel de madurez (A*E)
0	0.33	1	0.33	0.14	0
1	0.99	3	0.33	0.14	0.14
2	0.33	2	0.17	0.07	0.14
3	1.32	2	0.66	0.28	0.84
4	1.98	5	0.40	0.17	0.68
5	2.31	5	0.46	0.20	1
TOTAL	7.26	18	2.35	1	2.80

Tabla 47: Nivel de madurez proceso Instalar y Acreditar Soluciones y Cambios
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.80**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso AI7 Instalar y Acreditar Soluciones y Cambios podemos decir que en la institución los procesos para la instalación y acreditación de TI están integrados en el ciclo de vida de los sistemas y están automatizados en cierta medida, sin embargo en ocasiones estos procesos se realizan de manera informal así como también las pruebas de estrés para los sistemas nuevos y las pruebas de regresión para los sistemas existentes se deja en manos de diferentes personas por lo tanto los enfoques emprendidos varían ya que normalmente deciden el método de prueba.

4.1.1.3 Dominio 3: Dominio 3. Entregar y Dar Soporte

NV	N°	DS1 Definir y administrar los niveles de servicio	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	**1**	¿Hay convenios de asistencia a servicios para los procesos mas críticos de TI?			**X**		0,66	1,32
0	**2**	¿Hay un proceso formal de administración de niveles de servicio entre los usuarios y el prestador de servicios de TI?			**X**		0,66	
1	**3**	¿Se guían bajo algún un marco de trabajo que facilite el entendimiento entre los usuarios y los prestadores de los servicios de TI?		**X**			0,33	0,99
1	**4**	¿Se define los servicios de TI sobre las características del servicio y los requerimientos de la institución?			**X**		0,66	
2	**5**	¿Se notifica sobre los niveles de cumplimiento de los servicios de TI?			**X**		0,66	1,32
2	**6**	¿Los reportes sobre el cumplimiento de los niveles de servicio son entendibles para los interesados?			**X**		0,66	
3	**7**	¿Se revisa con los proveedores externos los acuerdos de los niveles de servicio y los controles de apoyo?		**X**			0,33	0,33
3	**8**	¿Se realiza una revisión con los proveedores internos los acuerdos de los niveles de servicio y los controles de apoyo?	**X**				0	
4	**9**	¿Se monitorea los criterios de desempeño específicos para el nivel de servicios?		**X**			0,33	1,33
4	**10**	¿En caso de encontrar irregularidades o desviaciones en el cumplimiento de los servicios de TI se toman las medidas correctivas?				**X**	1	
5	**11**	¿Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto?		**X**			0,33	0,66
5	**12**	¿El marco de trabajo brinda un proceso formal de administración de niveles de servicio entre el usuario y el prestador del servicio?		**X**			0,33	

Tabla 48: Cuestionario DS1
Elaborado por: Acurio, Y. (2020)

PROCESO: DS1 ESTABLECER LOS NIVELES DE SERVICIO					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	1.32	2	0.66	0.22	0
1	0.99	2	0.50	0.17	0.17
2	1.32	2	0.66	0.22	0.44
3	0.33	2	0.17	0.06	0.18
4	1.33	2	0.67	0.22	0.88
5	0.66	2	0.33	0.11	0.55

TOTAL	5.95	12	2.99	1	2.22

Tabla 49: Nivel de madurez proceso Definir y administrar los niveles de servicio
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.22**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS1: Definir y administrar los niveles de servicio podemos decir que en la institución se han definido todos los servicios de TI por lo que se han establecido formalmente los procesos para administrar los niveles de servicio entre los usuarios y el prestador de servicios de TI, sin embargo, no se evalúa y notifica frecuentemente el nivel de cumplimiento de estos servicios por ende no hay un efectivo monitoreo, lo que hace difícil emprender acciones correctivas donde los procesos parecen no estar funcionando efectivamente.

NV	N°	DS2 Administrar los Servicios de Terceros	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	**1**	¿No hay algún proceso para medir el número de quejas de los usuarios debidas a los servicios contratados?	**X**				0	0
0	**2**	¿No se categorizan los acuerdos según el tipo de proveedor y criticidad de los servicios?	**X**				0	
1	**3**	¿Se formalizan los documentos en los que se indica la relación técnica del proveedor y la institución?				**X**	1	1,33
1	**4**	¿Se planifica los servicios que se contrataran?		**X**			0,33	
2	**5**	¿Se comunica a la gerencia la necesidad de contratar un servicio a terceros en caso de emergencia?				**X**	1	2

2	**6**	¿Se comunica formalmente a los funcionarios que se encargaran de velar por el fiel cumplimiento de los acuerdos con terceros?				**X**	1	
3	**7**	¿Se verifica que el proveedor este cumpliendo con los requerimientos de la institución?			**X**		0,66	1,32
3	**8**	¿Se verifica que los contratos están de acuerdo con los requerimientos legales y de no estarlo se los corrige?			**X**		0,66	
4	**9**	¿Se verifica que las garantías de los contratos de servicios a terceros están renovadas?				**X**	1	2,33
4	**10**	¿Se monitorea la prestación del servicio de los proveedores?		**X**			0,33	
4	**11**	¿Se maneja adecuadamente las penalizaciones en caso de incumplimiento de los proveedores?				**X**	1	
5	**12**	¿Se identifican los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega de forma segura?			**X**		0,66	1,66
5	**13**	¿Se aseguran de la calidad de las relaciones con los proveedores basados en la confianza y transparencia?				**X**	1	

Tabla 50: Cuestionario DS2
Elaborado por: Acurio, Y. (2020)

PROCESO: DS2 Administrar los Servicios de Terceros					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0	2	0	0	0
1	1.33	2	0.67	0.17	0.17
2	2	2	1	0.25	0.50
3	1.32	2	0.66	0.17	0.51
4	2.33	3	0.78	0.20	0.80
5	1.66	2	0.83	0.21	1.05
TOTAL	8.64	13	3.94	1	3.03

Tabla 51: Nivel de madurez proceso Administrar los Servicios de Terceros
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**3.03**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas

siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS2: Administrar el Desempeño y la Capacidad podemos decir que la institución formaliza todos los documentos en los que se indica la relación técnica del proveedor y la institución, así como también verifica que todos los contratos están de acuerdo con los requerimientos legales y de no estarlo se los corrige, sin embargo, no se monitorea frecuentemente que la prestación de los servicios de los proveedores cumplan con los requerimientos de la institución por lo que a veces se ha generado quejas de los servicios contratados.

NV	N°	DS3 Administrar el Desempeño y la Capacidad	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	**1**	¿No se considera importante establecer un proceso de planeación para la revisión de la capacidad de los recursos de TI?			**X**		0,66	0,99
0	**2**	¿Los planes de capacidad y desempeño hacen uso de técnicas apropiadas para producir un modelo de desempeño y de capacidad de los recursos de TI, tanto actual como futura?		**X**			0,33	
1	**3**	¿Se toman en cuenta planes de contingencia en los ciclos de vida de los recursos de TI?		**X**			0,33	0,33
1	**4**	¿Se pronostica las necesidades futuras, basadas en los requerimientos de almacenamiento y contingencias de los servicios de TI?	**X**				0	
2	**5**	¿Se comunica formalmente el nivel de desempeño de los sistemas que se utiliza?			**X**		0,66	1,32
2	**6**	¿Se comunica los planes de contingencia en caso de no existir una capacidad y desempeño apropiado de los sistemas?			**X**		0,66	
3	**7**	¿Se evalúa el desempeño actual de los recursos de TI?		**X**			0,33	0,33
3	**8**	¿Se identifican las tendencias de cargas de trabajo en el departamento informático?	**X**				0	
4	**9**	¿Se realiza un pronóstico de desempeño de los recursos de TI para minimizar el riesgo de interrupciones?	**X**				0	1
4	**10**	¿Se toma medidas correctivas en caso de que no exista un apropiado nivel de desempeño en TI?				**X**	1	
5	**11**	¿La institución garantiza que los planes de contingencia se implementen de forma apropiada sobre los recursos de TI?		**X**			0,33	0,66
5	**12**	¿Hay seguridad de que los recursos de información soporten los requerimientos de la		**X**			0,33	

		entidad y estén disponibles de manera continua?						

Tabla 52: Cuestionario DS3
Elaborado por: Acurio, Y. (2020)

PROCESO: DS3 Administrar el Desempeño y la Capacidad					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.66	2	0.33	0.15	0
1	0.33	2	0.17	0.08	0.08
2	1.32	2	0.66	0.31	0.62
3	0.33	2	0.17	0.08	0.24
4	1	2	0.50	0.23	0.92
5	0.66	2	0.33	0.15	0.75
TOTAL	4.3	12	2.16	1	2.61

Tabla 53: Nivel de madurez proceso Administrar el Desempeño y la Capacidad
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.61**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS3: Administrar el Desempeño y la Capacidad podemos decir que para la institución es poco importante

establecer el procedimiento para la planeación de la capacidad de los recursos de tecnología de información razón por la que no se pronostica las necesidades futuras basadas en los requerimientos de almacenamiento y contingencias de los servicios de TI, lo cual hace evidente una falta de seguridad de que los recursos de información soporten los requerimientos de la entidad y estén disponibles de manera continua.

NV	N°	DS4 Garantizar la Continuidad del Servicio	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	1	¿La institución no considera importante garantizar la continuidad de los servicios?	X				0	0,66
0	2	¿Hay conciencia de la necesidad de contar con un plan de continuidad de TI para reducir el impacto de una interrupción de las funciones?			X		0,66	
1	3	¿El respaldo de la información se realiza bajo la política del contenido?		X			0,33	1,33
1	4	¿Se almacena en las instalaciones todos los medios de respaldo en caso de incidentes?				X	1	
2	5	¿Los involucrados están capacitados para actuar en caso de incidentes o desastres naturales que afecten a TI?		X			0,33	1,66
2	6	¿Se aseguran de que todas los involucrados reciban sesiones de habilitación respecto a sus roles en caso de incidentes o desastres?				X	1	
2	7	¿Se comunica a los involucrados el tiempo que tardara TI en recuperarse?		X			0,33	
3	8	¿Se evalúa los planes de continuidad de TI que garanticen que los sistemas de TI puedan ser recuperados de forma efectiva?	X				0	0,33
3	9	¿Se aseguran de que los tiempos de recuperación de TI no paralicen las actividades de la institución?		X			0,33	
4	10	¿Se toma las medidas correctivas en caso de que los planes de contingencia no funcionen adecuadamente?				X	1	1,66
4	11	¿Se planean acciones a tomar durante el período en que TI está recuperando y reanudando sus servicios?			X		0,66	
5	12	¿Se ejecutan procedimientos de control de cambios para asegurar que el plan de continuidad de TI se mantenga actualizado?		X			0,33	1,33
5	13	¿Se aseguran la compatibilidad de hardware y del software para poder recuperar los datos archivados?				X	1	

Tabla 54: Cuestionario DS4
Elaborado por: Acurio, Y. (2020)

PROCESO: DS4 Garantizar la Continuidad del Servicio					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	B	C	D	E	F
Nivel de Madurez	Suma de valores de cumplimiento	Número de declaraciones	Valor de cumplimiento (B/C)	Normalización del vector de cumplimiento (D/∑D)	Nivel de madurez (A*E)

0	0.66	2	0.33	0.10	0
1	1.33	2	0.67	0.21	0.21
2	1.66	3	0.55	0.17	0.34
3	0.33	2	0.17	0.05	0.15
4	1.66	2	0.83	0.26	1.04
5	1.33	2	0.67	0.21	1.05
TOTAL	6.97	13	3.22	1	2.79

Tabla 55: Nivel de madurez proceso Garantizar la Continuidad del Servicio
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.79**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS4: Garantizar la Continuidad del Servicio podemos decir que en la institución si hay consciencia de la necesidad de contar con plan estratégico que permita la reducción de impacto de las TI ante una interrupción del trabajo por lo que se establece plantea acciones que se deben implementar en un tiempo establecido en TI para la reanudación de los servicios , sin embargo los involucrados no reciben suficientes capacitaciones para actuar en caso de incidentes o desastres naturales que afecten a TI.

NV	N°	DS5 Garantizar la Seguridad de los Sistemas	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	1	¿La gerencia no es consciente de la necesidad de contar con políticas que garanticen la	X				0	0

		protección contra modificaciones o divulgaciones no autorizadas?						
0	2	¿La institución no considera importante que existan políticas aprobadas sobre la seguridad de TI?	**X**				0	
1	3	¿Se aseguran de que los derechos de acceso del usuario se solicitan por la gerencia para ser aprobados por el responsable de sistemas?			**X**		0,66	1,32
1	4	¿La institución usa técnicas de seguridad para autorizar acceso y controlar los flujos de información hacia las redes?			**X**		0,66	
2	5	¿Los usuarios se identifica a través de un mecanismo de autenticación para realizar sus diferentes actividades?				**X**	1	1,33
2	6	¿Se comunica formalmente las políticas que se aplicaran para garantizar la seguridad de TI?		**X**			0,33	
3	7	¿Se evalúa la seguridad de TI para garantizar el aseguramiento de la información?		**X**			0,33	0,66
3	8	¿Se evalúa que la tecnología relacionada con la seguridad sea resistente al sabotaje?		**X**			0,33	
4	9	¿Se realiza un monitoreo a la seguridad de TI para minimizar el impacto en la institución causado por vulnerabilidades o incidentes de seguridad?			**X**		0,66	0,99
4	10	¿Se cumplen con las medidas preventivas en toda la institución para proteger los sistemas de información?		**X**			0,33	
5	11	¿Se garantiza que la implementación de la seguridad en TI sea aprobada y monitoreada de forma proactiva?		**X**			0,33	0,99
5	12	¿Las transacciones de datos sensibles se intercambian a través de una ruta o medio con controles para proporcionar autenticidad de contenido?			**X**		0,66	

Tabla 56: Cuestionario DS5
Elaborado por: Acurio, Y. (2020)

PROCESO: DS5 Garantizar la Seguridad de los Sistemas					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	1.32	2	0.66	0.21	0
1	0.99	2	0.50	0.16	0.16
2	1.33	2	0.67	0.21	0.42
3	0.66	2	0.33	0.10	0.30
4	0.99	2	0.50	0.16	0.64
5	0.99	2	0.50	0.16	0.80
TOTAL	6.28	12	3.16	1	2.32

Tabla 57: Nivel de madurez proceso Garantizar la Seguridad de los Sistemas
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.32**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS5: Garantizar la Seguridad de los Sistemas podemos decir que para la gerencia se considera importante que existan políticas aprobadas sobre la seguridad de TI que garanticen la protección contra modificaciones o divulgaciones no autorizadas, razón por la que se propone que el acceso para los usuarios sean previamente autorizados por la alta gerencia para que luego sean aprobados por el funcionario responsable de sistemas, además se utilizan técnicas que permitan una seguridad más forzada del acceso y el recorrido de información hacia las como por ejemplo los usuarios se identifican a través de un mecanismo de autenticación para realizar sus diferentes actividades, sin embargo no se realiza un monitoreo constante que verifique que se cumplan todas las medidas preventivas para garantizar el aseguramiento de la información, así como tampoco se ha evaluado que la toda la tecnología que se fundamenta en la resistencia ante cualquier sabotaje lo que los hace vulnerables a posibles amenazas o robo de información.

NV	N°	DS6 Identificar y Asignar Costos	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	**1**	¿La institución no le da la debida importancia a los costos atribuibles a los servicios de TI?		**X**			0,33	0,66

0	**2**	¿Para el financiero no se considera importante contar con un modelo de costos para TI?		**X**			0,33	
1	**3**	¿Se identifican todos los costos de TI para soportar un modelo de costos transparente?			**X**		0,66	1,32
1	**4**	¿Hay conciencia general de la necesidad de identificar y asignar costos para TI?			**X**		0,66	
2	**5**	¿El reporte de los costos de los servicios de TI está ligado a los objetivos de la institución?		**X**			0,33	0,99
2	**6**	¿Se comunican los reportes de costos de los servicios de TI a los encargados de los procesos?			**X**		0,66	
3	**7**	¿Se verifica que los costos que incurran los servicios de TI estén registrados contablemente?			**X**		0,66	1,32
3	**8**	¿Se evalúa que los costos asignados sean coherentes y no sobrevalorados?			**X**		0,66	
4	**9**	¿Se monitorea los costos de TI y se toman medidas correctivas cuando se detectan desviaciones?				**X**	1	1,33
4	**10**	¿Las cifras obtenidas de los costos se usan para verificar la obtención de beneficios y para el proceso de presupuesto de la organización?		**X**			0,33	
5	**11**	¿El monitoreo y la evaluación del costo de los servicios optimiza el costo de los recursos de TI?				**X**	1	1,66
5	**12**	¿Los costos directos e indirectos están identificados y se reportan de forma oportuna y automatizada a la gerencia?			**X**		0,66	

Tabla 58: Cuestionario DS6
Elaborado por: Acurio, Y. (2020)

PROCESO: DS6 Identificar y Asignar Costos					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.99	2	0.50	0.14	0
1	1.32	2	0.66	0.19	0.19
2	0.99	2	0.50	0.14	0.28
3	1.32	2	0.66	0.19	0.57
4	1.33	2	0.67	0.20	0.80
5	0.99	2	0.50	0.14	0.70
TOTAL	6.94	12	3.49	1	2.54

Tabla 59: Nivel de madurez proceso Identificar y Asignar Costos
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.54**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS6: Identificar y Asignar Costos podemos decir que en la institución no se considera importante contar con un modelo de costos exclusivo para los servicios TI, sin embargo, si se identifica y registran los costos en base a las normativas y reglamentos legales de las diferentes entidades reguladoras, además se considera necesario que se realicen reportes de costos de los servicios de TI a la gerencia y a los encargados de los procesos para realizar un mejor seguimiento a los mismos y en caso de desviaciones tomar las medidas correctivas necesarias.

NV	N°	DS7 Educar y Entrenar a los Usuarios	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	**1**	¿Para la gerencia no se considera importante establecer un programa de entrenamiento para el personal que maneja TI?	**X**				0	0
0	**2**	¿Se identifican las necesidades de entrenamiento de cada grupo de usuarios?	**X**				0	
1	**3**	¿El programa de entrenamiento incluye valores corporativos?		**X**			0,33	0,66
1	**4**	¿Se organiza los entrenamientos para el personal con suficiente tiempo?		**X**			0,33	
2	**5**	¿Los programas de entrenamiento incluye habilidades, perfiles de competencia y certificaciones actuales?		**X**			0,33	0,66

2	**6**	¿El programa de entrenamiento incluye estrategias y requerimientos actuales y futuros de la institución?		**X**			0,33	
3	**7**	¿Se evalúa el contenido del entrenamiento al finalizar la capacitación respecto a la calidad?	**X**				0	0,66
3	**8**	¿Se evalúa el contenido del entrenamiento al finalizar la capacitación respecto a la percepción y retención del conocimiento?			**X**		0,66	
4	**9**	¿Se monitorea el cumplimiento de los programas de entrenamiento?		**X**			0,33	0,99
4	**10**	¿Se supervisa que no exista desviaciones en los recursos asignados para las capacitaciones programadas?			**X**		0,66	
5	**11**	¿El programa de entrenamiento incluye la implementación de nuevo software e infraestructura de TI?	**X**				0	0,33
5	**12**	¿Los programas de entrenamiento han incrementan el uso efectivo de la tecnología al disminuir los errores, incrementan la productividad y asegurar la información que se genera?		**X**			0,33	

Tabla 60: Cuestionario DS7
Elaborado por: Acurio, Y. (2020)

PROCESO: DS7 Educar y Entrenar a los Usuarios					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.33	2	0.17	0.09	0
1	0.66	2	0.33	0.18	0.18
2	0.66	2	0.33	0.18	0.36
3	0.66	2	0.33	0.18	0.54
4	0.99	2	0.50	0.28	1.12
5	0.33	2	0.17	0.09	0.45
TOTAL	3.63	12	1.83	1	2.65

Tabla 61: Nivel de madurez proceso Educar y Entrenar a los Usuarios
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.65**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS7: Educar y Entrenar a los Usuarios podemos decir que para la gerencia es importante establecer un programa de entrenamiento para el personal que maneja TI, sin embargo, no se programan frecuentes capacitaciones como tampoco se identifican las necesidades de entrenamiento de cada grupo de usuarios por lo que no se ha incrementado el uso efectivo de la tecnología, disminuir errores y asegurar la información que se genera.

NV	N°	DS8 Administrar la Mesa de Servicio y los Incidentes	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	1	¿No se ha diseñado una mesa de servicios para responder de manera oportuna las consultas y problemas de los usuarios de TI?	**X**				0	0,33
0	2	¿Existe conciencia sobre la importancia de administrar adecuadamente la mesa de servicios y sus incidentes?		**X**			0,33	
1	3	¿El sistema trabaja estrechamente con los procesos de administración de incidentes?		**X**			0,33	0,99
1	4	¿Se mantiene informados a los usuarios sobre el estatus de sus consultas?			**X**		0,66	
2	5	¿Cuándo se resuelve el incidente la mesa de servicios confirma que la acción tomada fue acordada con el usuario?	**X**				0	0,66
2	6	¿Se emiten los reportes de la actividad de la mesa de servicios a la gerencia?	**X**				0	
2	7	¿Cuándo se resuelve los incidentes de la mesa de servicios se registra las causas?			**X**		0,66	
3	8	¿Se mide la satisfacción del usuario final respecto a la calidad de la mesa de servicios de TI?		**X**			0,33	0,33

3	9	¿Se evalúa que el sistema permita el registro, rastreo de llamadas, incidentes, solicitudes de servicios y necesidades de información?	**X**				0	
4	10	¿Los procedimientos de monitoreo permiten clasificar cualquier problema?		**X**			0,33	0,66
4	11	¿Existen procedimientos para el monitoreo puntual sobre las consultas de los usuarios?		**X**			0,33	
5	12	¿Los reportes de emitidos por la mesa de servicios permite a la gerencia medir el desempeño del servicio y el tiempo de respuesta?	**X**				0	0
5	13	¿Los procedimientos de monitoreo han permitido priorizar cualquier problema?	**X**				0	

Tabla 62: Cuestionario DS8
Elaborado por: Acurio, Y. (2020)

PROCESO: DS8 Administrar la Mesa de Servicio y los Incidentes					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.66	2	0.33	0.20	0
1	0.99	2	0.50	0.30	0.30
2	0.66	3	0.33	0.20	0.40
3	0.33	2	0.17	0.10	0.30
4	0.66	2	0.33	0.20	0.8
5	0	2	0	0	0
TOTAL	3.3	13	1.66	1	1.8

Tabla 63: Nivel de madurez proceso Administrar la Mesa de Servicio y los Incidentes
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**1.8**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de uno (nivel de madurez 1 o inicial); lo que en la escala del modelo de madurez de COBIT indica que hay evidencia de que la organización ha reconocido los problemas existentes y que necesitan ser resueltos. El método general de la administración es desorganizado.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS8: Administrara la mesa de todos los servicios podemos decir que en la institución si se ha diseñado una mesa de servicios para responder de manera oportuna las consultas y problemas de los usuarios de TI, sin embargo, no se le da la debida importancia a una administración adecuada de la mesa de servicios y sus incidentes ya que no se realizan reportes ni un monitoreo de las actividades de la mesa de servicios lo que impide medir el desempeño del servicio y el tiempo de respuesta.

NV	N°	DS9 Administrar la Configuración	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	1	¿No se realizan procedimientos de configuración?	X				0	0,33
0	2	¿No se considera importante contar con un repositorio central que contenga toda la información relevante sobre los elementos de configuración?		X			0,33	
1	3	¿Es efectiva la herramienta de soporte que contiene toda la información relevante sobre los elementos de configuración?			X		0,66	0,66
1	4	¿Está integrado el procedimiento de configuración con la gestión de cambios?	X				0	
2	5	¿Se comunica al personal a tiempo cuando se realizara las configuraciones?		X			0,33	0,66
2	6	¿Después de realizar configuraciones se capacita al personal sobre los cambios efectuados?		X			0,33	
3	7	¿Se revisa que el software instalado no está contra las políticas de uso de software o no licencia?				X	1	1,66
3	8	¿Se evalúan los datos de configuración para verificar la integridad de la configuración actual e histórica?			X		0,66	
4	9	¿Se monitorean todos los activos de TI y sus cambios?		X			0,33	0,99
4	10	¿El proceso de monitoreo verifica que no exista perdidas de información debido a las configuraciones?			X		0,66	
5	11	¿La administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y			X		0,66	1,32

		resuelve los problemas más rápido?						
5	12	¿Se garantizar la integridad de las configuraciones de hardware y software?			X		0,66	

Tabla 64: Cuestionario PO
Elaborado por: Acurio, Y. (2020)

PROCESO: DS9 Administrar la Configuración					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	1.66	2	0.83	0.24	0
1	0.66	2	0.33	0.09	0.09
2	0.66	2	0.33	0.09	0.18
3	1.66	2	0.83	0.24	0.72
4	0.99	2	0.50	0.15	0.60
5	1.32	2	0.66	0.19	0.95
TOTAL	6.95	12	3.48	1	2.54

Tabla 65: Nivel de madurez proceso Administrar la Configuración
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.54**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS9: Administrar la Configuración podemos decir que en la institución si se realiza procedimientos de configuración, sin embargo, no existe una adecuada planificación ya que no se comunica al personal a tiempo cuando se realizan las configuraciones lo que ha ocasionado

algunas interrupciones en las labores, también hace falta un poco de capacitación sobre los cambios efectuados después de las configuraciones realizadas.

NV	N°	DS10 Administración de Problemas	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	1	¿No hay conciencia sobre la necesidad de administrar problemas relacionados con TI?	**X**				0	0
0	2	¿No hay algún procedimiento establecido para cerrar registro de problemas?	**X**				0	
1	3	¿Se evidencia el cumplimiento de procedimientos para administrar los problemas de TI?			**X**			
1	4	¿Las responsabilidades y la propiedad de los problemas están claramente establecidas?		**X**			0,33	0,66
1	5	¿El sistema categoriza los problemas en función del impacto, urgencia y prioridad?		**X**			0,33	
2	6	¿Se reportan formalmente los problemas que han sido identificados como parte de la administración de incidentes?		**X**			0,33	0,66
2	7	¿El personal de soporte técnico es capacitado para saber cómo debe actuar frente a los problemas identificados?			**X**		0,33	
3	8	¿Se evalúa la gestión para administrar los problemas identificados?	**X**				0	0
3	9	¿Se realiza evaluaciones sobre el tiempo de respuesta para solucionar los problemas identificados?	**X**				0	
4	10	¿La administración de problemas monitorea el continuo impacto de los problemas y errores conocidos en los servicios a los usuarios?	**X**				0	1
4	11	¿Las recomendaciones de auditoría sobre los sistemas ha permitido rastrear la causa de todos los problemas reportados?				**X**	1	
5	12	¿El sistema de administración de problemas es efectivo?		**X**			0,33	0,99
5	13	¿Se mejora los procesos de administración de cambios, configuración para minimizar los problemas?			**X**		0,66	

Tabla 66: Cuestionario DS10
Elaborado por: Acurio, Y. (2020)

PROCESO: DS10 Administración de Problemas					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**

Nivel de Madurez	Suma de valores de cumplimiento	Número de declaraciones	Valor de cumplimiento (B/C)	Normalización del vector de cumplimiento (D/∑D)	Nivel de madurez (A*E)
0	0.33	2	0.17	0.10	0
1	0.66	2	0.33	0.18	0.18
2	0.66	2	0.33	0.18	0.36
3	0	2	0	0	0
4	1	2	0.50	0.27	1.08
5	0.99	2	0.50	0.27	1.08
TOTAL	3.64	12	1.83	1	2.7

Tabla 67: Nivel de madurez proceso Administración de Problemas
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.7**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS10: Administración de Problemas podemos decir que en la institución si hay conciencia sobre la necesidad de administrar problemas relacionados con TI, sin embargo, no hay una efectiva administración ya que sistema no categoriza los problemas en función del impacto, urgencia y prioridad como tampoco se evalúa el tiempo de respuesta para solucionar los problemas identificados y no hay un monitorea continuo de los mismos.

NV	N°	DS11 Administración de Datos	De ningún modo	Un poco	Bastante	Completamente	calificación	Total

0	1	¿No se evidencia el cumplimiento de procedimientos para archivar, almacenar y retener los datos?	**X**				0	0
0	2	¿En la institución no hay conciencia de la necesidad de establecer procedimientos para proteger el software?	**X**				0	
1	3	¿Las necesidades de reinicio de función de TI están soportadas?			**X**		0,66	0,99
1	4	¿Se aplican mecanismos para identificar y aplicar requerimientos de seguridad a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos?		**X**			0,33	
2	5	¿Son claros los procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea?			**X**		0,66	0,99
2	6	¿Se realizan los reportes de salida de una forma clara y completa y su entrega es oportuna?		**X**			0,33	
3	7	¿Se verifica que todos los datos que se espera procesar se reciban completamente de forma precisa y a tiempo?		**X**			0,33	0,99
3	8	¿Se reciben los documentos originales con los datos necesarios para procesar la información de una forma precisa y oportuna?			**X**		0,66	
4	9	¿Se maneja adecuadamente el software desde los equipos o medios una vez que son eliminados o transferidos para otro uso?				**X**	1	1,33
4	10	¿Se monitorea los procedimientos establecidos para el almacenamiento de datos?		**X**			0,33	
5	11	¿Los procedimientos de respaldo de los sistemas en línea son adecuados?			**X**		0,66	1,32
5	12	¿Los datos que se esperan procesar se reciben y procesan completamente, de forma precisa y a tiempo, y los resultados se entregan de acuerdo a los requerimientos de la institución?			**X**		0,66	

Tabla 68: Cuestionario DS11
Elaborado por: Acurio, Y. (2020)

PROCESO: DS11 Administración de Datos					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	1.33	2	0.67	0.19	0

1	0.99	2	0.50	0.14	0.14
2	0.99	2	0.50	0.14	0.28
3	0.99	2	0.50	0.14	0.42
4	1.33	2	0.67	0.20	0.80
5	1.32	2	0.66	0.19	0.95
TOTAL	6.95	12	3.5	1	2.59

Tabla 69: Nivel de madurez proceso Administración de Datos
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.59**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS11: Administración de Datos podemos decir que en la institución si hay conciencia de la necesidad de establecer procedimientos para proteger el software por lo que se han establecido procedimientos para respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea, sin embargo no se realiza un adecuado monitoreo al cumplimiento de estos procedimientos que garanticen un adecuado almacenamiento de datos.

NV	N°	DS12 Administración del Ambiente Físico	De ningún modo	Un poco	Bastante	Completamente	calificación	Total

0	**1**	¿Para la gerencia no se considera importante seleccionar un centro de datos físicos para el equipo de TI?	**X**				0	0
0	**2**	¿No se considera importante definir los centros de datos físicos para el equipo de TI?	**X**				0	
1	**3**	¿La selección de un centro de datos toma en cuenta el riesgo asociado con desastres naturales y causados por el hombre?		**X**			0,33	0,66
1	**4**	¿Las medidas de seguridad físicas están alineadas con los requerimientos de la institución?		**X**			0,33	
2	**5**	¿Conoce las políticas seleccionadas para garantizar la seguridad de los equipos y del personal?			**X**		0,66	0,99
2	**6**	¿Se capacita sobre planes de contingencia en caso de daños al equipo de cómputo o robo?		**X**			0,33	
3	**7**	¿Se evalúan diferentes medidas de protección contra factores ambientales?		**X**			0,33	0,66
3	**8**	¿Se evalúa que el equipo de suministro de energía está administrado de acuerdo con los requerimientos técnicos de la institución y de acuerdo con los lineamientos de seguridad y salud?		**X**			0,33	
4	**9**	¿Se monitorea que el ambiente físico sea el adecuado para proteger los activos de cómputo y la información de la institución?		**X**			0,33	0,66
4	**10**	¿Se supervisa que la planta eléctrica de emergencia funciones en caso de apagones o cualquier otro incidente?		**X**			0,33	
5	**11**	¿Se realizan instalaciones con tierra física para todos los equipos?		**X**			0,33	0,99
5	**12**	¿Se cumplen con todas las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo?			**X**		0,66	

Tabla 70: Cuestionario PO
Elaborado por: Acurio, Y. (2020)

PROCESO: DS12 Administración del Ambiente Físico					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	2	2	1	0.32	0
1	0.66	2	0.33	0.10	0.10
2	1.32	2	0.66	0.22	0.44
3	0.66	2	0.33	0.10	0.30
4	0.66	2	0.33	0.10	0.40
5	0.99	2	0.50	0.16	0.8
TOTAL	6.29	12	3.15	1	2.04

Tabla 71: Nivel de madurez proceso Administración del Ambiente Físico
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.04**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS12: Administración del Ambiente Físico podemos decir que en la institución se considera importante seleccionar un centro de datos físicos para el equipo de TI por lo que si se han establecido algunas medidas de seguridad física para los equipos y del personal, sin embargo, no se realiza un monitoreo continuo que garantice su cumplimiento, además estas medidas no se analizan y actualizan para mejorarlas y así lograr la protección de los activos de cómputo y la información de la institución.

NV	N°	DS13 Administración de Operaciones	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	**1**	¿Se reconoce la necesidad de estructurar las funciones de soporte de TI?			**X**		0,66	1,32
0	**2**	¿Hay políticas definidas y procedimientos de operación para protección de datos de salida sensitivos?			**X**		0,66	
1	**3**	¿Las computadoras, sistemas y aplicaciones que soportan los procesos de la institución con frecuencia no están disponibles, se interrumpen o retrasan?		**X**			0,33	0,66
1	**4**	¿Se ha establecido un programa para el monitoreo de infraestructura y mantenimiento preventivo de hardware?	**X**				0	
1	**4**	¿El mantenimiento de la infraestructura de TI se realiza oportunamente?		**X**			0,33	

2	**5**	¿Se conoce la ubicación exacta de todos los activos de TI?	**X**				0	
2	**6**	¿El personal a cargo de TI está familiarizado con todas las tareas a cumplir?			**X**		0,66	0,66
3	**7**	¿Se verifica que se encuentran bien registrados y codificados todos los activos de TI?			**X**		0,66	
3	**8**	¿Los procedimientos para reducir la frecuencia y el impacto de las fallas de la infraestructura de TI son efectivos?		**X**			0,33	0,99
4	**9**	¿Los procedimientos para monitorear la infraestructura de TI son adecuados?		**X**			0,33	
4	**10**	¿Se supervisa que todos los activos de TI consten en el inventario?		**X**			0,33	0,66
5	**11**	¿La programación de trabajo está organizado de manera más eficiente para cumplir los requerimientos de la institución?		**X**			0,33	
5	**12**	¿Son adecuados los procedimientos para garantizar el mantenimiento oportuno de la infraestructura de TI?			**X**		0,66	1,32
5	**13**	¿Los resguardos físicos sobre los activos de TI tales como impresoras o dispositivos de seguridad etc. son adecuados?		**X**			0,33	

Tabla 72: Cuestionario PO
Elaborado por: Acurio, Y. (2020)

PROCESO: DS13 Administración de Operaciones					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	1.32	2	0.66	0.20	0
1	0.99	2	0.50	0.15	0.15
2	0.66	2	0.50	0.15	0.30
3	1.32	2	0.66	0.20	0.60
4	0.66	2	0.50	0.15	0.60
5	1.32	3	0.44	0.15	0.75
TOTAL	6.27	13	3.26	1	2.4

Tabla 73: Nivel de madurez proceso Administración de Operaciones
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.4**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso DS13: Administración de Operaciones podemos decir que en la institución se han establecido políticas y procedimientos de operación para protección de datos de salida, sin embargo no hay un programa de monitoreo de infraestructura y mantenimiento preventivo de hardware razón por la que el mantenimiento de la infraestructura de TI no se realiza oportunamente teniendo como consecuencia que las computadoras, sistemas y aplicaciones que soportan los procesos de la institución con frecuencia no están disponibles, se interrumpen o retrasan.

4.1.1.4) Dominio 4: Monitorear y Evaluar (ME)

NV	N°	ME1 Monitorear y Evaluar el Desempeño de TI	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	1	¿El área de TI no desarrolla independientemente un monitoreo de proyectos o procesos?		**X**			0,33	0,66
0	2	¿No se reconoce la necesidad de objetivos de procesos claramente entendibles?		**X**			0,33	
1	3	¿Se implementa el monitoreo para los procesos de TI y para los servicios de información de otros departamentos?		**X**			0,33	0,33
1	4	¿La definición del proceso y el monitoreo se ajustan a las necesidades de los servicios de información?	**X**				0	
2	5	¿están aprobados los objetivos de desempeño de cada uno de los procesos de TI por la gerencia y otros interesados relevantes?				**X**	1	1,66
2	6	¿Se establecen procesos para recolectar información oportuna			**X**		0,66	

		para reportar el avance contra las metas?						
3	7	¿Se identifican e inician medidas correctivas basados en el monitoreo del desempeño?		**X**			0,33	0,66
3	8	¿Durante la revisión de los reportes se identifica cualquier desviación respecto al desempeño esperado?		**X**			0,33	
4	9	¿Se establece un marco de trabajo de monitoreo general que definan el alcance, la metodología y el proceso a seguir para medir la solución y la entrega de servicios de TI?		**X**			0,33	0,99
4	10	¿Se monitorea la contribución de TI a la institución?		**X**			0,33	
4	11	¿Se garantiza la implantación de un método en el proceso de monitoreo de TI?		**X**			0,33	
5	12	¿Se mejora el proceso para actualizar el monitoreo de estándares, políticas y mejoras prácticas en la institución?		**X**			0,33	0,66
5	13	¿Todos los procesos de monitoreo son optimizados y soportan objetivos globales de la institución?		**X**			0,33	

Tabla 74: Cuestionario ME1
Elaborado por: Acurio, Y. (2020)

PROCESO: ME1 MONITOREAR Y REALIZAR LA EVALUACIÓN DEL DESEMPEÑO DE TI					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.66	2	0.33	0.14	0
1	0.33	2	0.17	0.08	0.08
2	1.66	2	0.83	0.36	0.72
3	0.66	2	0.33	0.14	0.42
4	0.99	3	0.33	0.14	0.56
5	0.66	2	0.33	0.14	0.70
TOTAL	4.96	13	2.32	1	2.48

Tabla 75: Nivel de madurez proceso Monitorear y Evaluar el Desempeño de TI
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.48**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas

siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso ME1: Monitorear y Evaluar el Desempeño de TI podemos decir que en la institución no hay un monitoreo programado para los procesos de TI y para los servicios de información como tampoco se realizan periódicamente reportes del su desempeño a pesar de que, si se han definido indicadores, lo que hace complicado detectar errores y tomar acciones correctivas a tiempo y así lograr el cumplimiento y mejoramiento de los objetivos de TI.

NV	**N°**	ME2 Monitorear y Evaluar el Control Interno	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	1	¿La institución posee procedimientos para monitorear la efectividad de los controles internos?		**X**			0,33	0,66
0	2	¿Hay una ausencia general de conciencia de la seguridad operativa?		**X**			0,33	
1	3	¿Existe compromiso de parte de la administración para la seguridad operativa?			**X**		0,66	0,66
1	4	¿La administración de TI ha asigno formalmente la responsabilidad de monitorear la efectividad de los controles interno?	**X**				0	
2	5	¿La organización tiene mayor conciencia del monitoreo del control interno para TI?	**X**				0	0,66
2	6	¿Se confirman que los proveedores de servicios externos cumplan con las obligaciones contractuales?			**X**		0,66	
3	7	¿Se evalúa el estado de los controles internos sobre los proveedores de TI de servicios externos?		**X**			0,33	0,66
3	8	¿Se evalúa la completitud y efectividad de los controles de gerencia sobre los procesos de TI por medio de un programa de autoevaluación?		**X**			0,33	
4	9	¿Se monitorea el ambiente de control de TI y el marco de trabajo de control de TI para satisfacer los objetivos institucionales?		**X**			0,33	1,32
4	10	¿Se monitorea la eficiencia y efectividad de los controles internos de revisión de la gerencia de TI?		**X**			0,33	

4	11	¿Se establecen acciones correctivas en caso de controles ineficientes?			X		0,66	
5	12	¿Se obtiene un aseguramiento adicional de la efectividad de los controles internos por medio de la revisión de terceros?				X	1	2
5	13	¿Se identifican acciones correctivas derivadas de los controles de evaluación y los informes?				X	1	

Tabla 76: Cuestionario ME2
Elaborado por: Acurio, Y. (2020)

PROCESO: ME2 Monitorear y Evaluar el Control Interno					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.99	2	0.50	0.15	0
1	0.99	2	0.50	0.15	0.15
2	0.99	2	0.50	0.15	0.30
3	0.66	2	0.33	0.10	0.30
4	1.32	3	0.44	0.13	0.52
5	2	2	1	0.30	1.5
TOTAL	6.95	13	3.27		2.77

Tabla 77: Nivel de madurez proceso Monitorear y Evaluar el Control Interno
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.77**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso ME2: Monitorear y Evaluar el Control Interno podemos decir que a pesar de que existe un marco legal de

referencia como son las normas de control interno de la Contraloría General del Estado en la institución no hay la suficiente conciencia de lo importante que es monitorear el control interno para TI razón por la que no se realiza continuamente evaluaciones que permita identificar que las operaciones son llevadas a cabo de forma eficiente y en cumplimiento de leyes y reglamentos, es así que todas las evaluaciones de control interno forman parte de las auditorías financieras de la institución creando una desviación en cuanto a las necesidades del área.

NV	**N°**	ME3 Garantizar el Cumplimiento con Requerimientos Externos	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	1	¿Para la institución no es importante revisar y ajustar las políticas, estándares, procedimientos y metodologías de TI?		**X**			0,33	0,66
0	2	¿La gerencia tiene implantado un marco de trabajo para el monitoreo del control interno de TI?		**X**			0,33	
1	3	¿Existe conciencia respecto a los requerimientos externos que afectan a TI?			**X**		0,66	1,66
1	4	¿El departamento de TI tiene presente requerimientos legales dentro de su plan estratégico?				**X**	1	
2	5	¿La institución utiliza reportes de control informales para comenzar iniciativas de acción correctiva?			**X**		0,66	0,99
2	6	¿Los administradores de TI reciben capacitación sobre leyes locales e internacionales, regulaciones, y otros requerimientos externos que se deben de cumplir?		**X**			0,33	
3	7	¿Se verifica el cumplimiento de los procedimientos de TI con los requerimientos legales y regulatorios?		**X**			0,33	0,99
3	8	¿Se verifica el cumplimiento de políticas de TI con los requerimientos legales Y regulatorios?			**X**		0,66	
4	9	¿Con frecuencia se revisan nuevos reglamentos o estándares que deben ser adoptados por el departamento de TI?	**X**				0	0,66
4	10	¿Se toman acciones correctivas para garantizar el cumplimiento de las políticas internas o requerimientos legales externos?			**X**		0,66	
5	11	¿Se identifican sobre una base las leyes locales e internacionales que se deben cumplir para incorporar en las políticas, estándares, procedimientos y metodologías de TI de la institución?		**X**			0,33	0,66

5	12	¿Se resuelve cualquier brecha de cumplimiento por el responsable del proceso de forma oportuna?		**X**			0,33	

Tabla 78: Cuestionario ME3
Elaborado por: Acurio, Y. (2020)

PROCESO: ME3 Garantizar el Cumplimiento con Requerimientos Externos					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**
0	0.66	2	0.33	0.12	0
1	1.66	2	0.83	0.28	0.28
2	0.99	2	0.50	0.18	0.36
3	0.99	2	0.50	0.18	0.54
4	0.66	2	0.33	0.12	0.48
5	0.66	2	0.33	0.12	0.60
TOTAL	5.62	12	2.82	1.01	2.26

Tabla 79: Nivel de madurez proceso Garantizar el Cumplimiento con Requerimientos Externos
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.26**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso ME3: Garantizar el Cumplimiento con Requerimientos Externos podemos decir que el departamento de TI

si toma en consideración los requerimientos legales dentro de su plan estratégico, sin embargo, consideran que hace falta más capacitaciones sobre todas las leyes que rigen dentro y fuera del país así como reglamentos externos que se deben cumplir y así revisar nuevos reglamentos o estándares que deben ser adoptados por el departamento de TI y de ser el caso tomar acciones correctivas para garantizar su cumplimiento.

NV	N°	ME4 Proporcionar Gobierno de TI	De ningún modo	Un poco	Bastante	Completamente	calificación	Total
0	**1**	¿En la institución existe conciencia de la necesidad de definir el marco de gobierno de TI con la visión completa del entorno de control de la institución?		**X**			0,33	0,66
0	**2**	¿Se fomenta la corresponsabilidad entre la institución y TI en la toma de decisiones?		**X**			0,33	
1	**3**	¿Se alinea el marco de gobierno de TI con la visión completa del entorno de control de la institución?		**X**			0,33	0,99
1	**4**	¿Se brinda una orientación estratégica a la dirección respecto a TI?			**X**		0,66	
2	**5**	¿Se informa del estado y cuestiones de gobierno de TI?		**X**			0,33	0,99
2	**6**	¿Se da a conocer al consejo directivo sobre temas estratégicos de TI?			**X**		0,66	
3	**7**	¿Se aseguran de que el marco de gobierno de TI está cumpliendo con las leyes y regulaciones?			**X**		0,66	1,32
3	**8**	¿El departamento de TI garantiza la optimización de los costos por la prestación de servicios?			**X**		0,66	
4	**9**	¿Se informa a la alta dirección sobre el desempeño de TI?		**X**			0,33	0,66
4	**10**	¿Se implementa un enfoque disciplinado de la administración de TI?		**X**			0,33	
5	**11**	¿Se garantiza que la contribución potencial de TI cumple con las estrategias de la institución?		**X**			0,33	0,66
5	**12**	¿El departamento de informática garantiza las capacidades de TI para el funcionamiento de las operaciones de la institución?		**X**			0,33	

Tabla 80: Cuestionario ME4
Elaborado por: Acurio, Y. (2020)

PROCESO: ME4 Proporcionar Gobierno de TI					
Cómputo de los valores de cumplimiento del nivel de madurez					
A	**B**	**C**	**D**	**E**	**F**
Nivel de Madurez	**Suma de valores de cumplimiento**	**Número de declaraciones**	**Valor de cumplimiento (B/C)**	**Normalización del vector de cumplimiento (D/∑D)**	**Nivel de madurez (A*E)**

0	0.66	2	0.33	0.10	0
1	0.99	2	0.50	0.17	0.17
2	0.99	2	0.50	0.17	0.34
3	1.32	2	0.66	0.22	0.66
4	0.99	2	0.50	0.17	0.68
5	0.99	2	0.50	0.17	0.85
TOTAL	5.94	12	2.99	1	2.7

Tabla 81: Nivel de madurez proceso Proporcionar Gobierno de TI
Elaborado por: Acurio, Y. (2020)

Nivel de Madurez =	**2.7**

Análisis

El nivel de madurez para este proceso calculado por la herramienta de evaluación es de dos (nivel de madurez 2 o repetible); lo que en la escala del modelo de madurez de cobit indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

Interpretación

A partir del nivel de madurez obtenido en análisis del proceso ME4: Proporcionar Gobierno de TI podemos decir que a pesar de que el departamento de TI brinda una orientación a la dirección respecto a la contribución potencial de TI para el funcionamiento de las operaciones de la institución no se le da la debida importancia ya que muy poco se fomenta la corresponsabilidad entre la institución y TI en la toma de decisiones y no se ha logrado alinear el marco de gobierno de TI con el visón completa del entorno de control de la institución.

4.1.2 Análisis e interpretación de la Variable Dependiente

La segunda metodología a utilizar será el marco de referencia COSO ERM que tiene como objetivo evaluar el monitoreo de riesgos para lo cual se identificara riesgos de control utilizado los 5 componentes y en base a los 20 principios.

En primer lugar, se realizará una matriz de identificación de riesgos para lo cual se planteará enunciados en forma de pregunta por cada uno de los 20 principios que demanda el marco de referencia COSO ERM 2017 y el director administrativo de la institución identificar los riesgos de control del área financiera en relación a la seguridad de la información.

Gobierno y Cultura

Principio 1: La organización ejerce la supervisión de riesgos a través del consejo de administración	SI	NO
¿Existe conciencia sobre la responsabilidad de supervisar los riesgos en el manejo de información confidencial que genera el departamento financiero?	**X**	
¿Se han establecido políticas para la gestión de riesgos sobre la seguridad de información en el departamento financiero?	**X**	
¿La Dirección administrativa del hospital tiene conocimiento sobre los riesgos identificados que afecten a la información del departamento financiero?	**X**	
¿La Dirección administrativa realiza un monitoreo de los riesgos identificados en el Departamento Financiero?		**X**
¿La Dirección administrativa del hospital establece planes para supervisar los riesgos nuevos y emergentes sobre la seguridad de información del departamento financiero?		**X**
Principio 2: La Organización establece la estructura operativa para la búsqueda de los objetivos estratégicos y de negocio.	SI	NO
¿La Institución establece una estructura operativa para el cumplimiento de los objetivos del departamento financiero?	**X**	
¿La Dirección administrativa del hospital planifica y organiza las estrategias y objetivos en función de la misión, visión y valores de la entidad?	**X**	
¿La administración especifica los niveles de aprobación para las transacciones que se realizan en la Jefatura financiera?	**X**	
¿El departamento Financiero considera los riesgos nuevos y emergentes como parte de la toma de decisiones?	**X**	
¿La Dirección administrativa evalúa regularmente la estructura operativa de la Jefatura financiera?		**X**
Principio 3: La Organización establece la cultura deseada.	SI	NO
¿La Dirección administrativa del hospital establece una cultura de riesgos?	**X**	
¿La Dirección administrativa del hospital explica claramente sobre el manejo de los riesgos?		**X**

¿La Dirección administrativa del hospital muestra interés por el manejo de los riesgos del departamento financiero?	**X**	
¿La Dirección administrativa del hospital discute ampliamente sobre los riesgos identificados del departamento financiero?		**X**
¿La Dirección administrativa del hospital explica claramente los niveles de apetito al riesgo?		**X**
Principio 4: Demuestra compromiso con los valores fundamentales.	SI	NO
¿La Dirección administrativa del hospital predica con el ejemplo haciendo énfasis en la integridad y el comportamiento ético?	**X**	
¿Ha ocurrido hechos de abuso de autoridad en el departamento financiero?		**X**
¿La Dirección administrativa del hospital crea conciencia de manera permanente sobre la importancia de los riesgos financieros?		**X**
¿La Dirección administrativa del hospital alienta al personal del área financiera a participar en la toma de decisiones y a discutir riesgos los riesgos para identificar estrategias?	**X**	
¿La Dirección administrativa del hospital aborda el riesgo de forma consistente al tomar decisiones claves, lo que incluye debatir y revisar los escenarios de riesgo que pueden ayudar a todos a entender la interrelación y los impactos de los riesgos antes de tomar decisiones?	**X**	
¿La dirección demuestra comunicación abierta proporcionando una variedad de canales para que el personal informen sus preocupaciones sobre la toma de riesgos, la conducta comercial o el comportamiento potencialmente inapropiados o excesivos sin temor a represalias o intimidación?		**X**
¿La Dirección administrativa del hospital envía un mensaje claro de lo que es un comportamiento aceptable e inaceptable cada vez que se conocen las desviaciones y dichas desviaciones de los estándares de conducta se abordan de manera oportuna y constante?	**X**	
Principio 5: Atrae, desarrolla y retiene personal capacitado.	SI	NO
¿La Dirección administrativa del hospital evalúa el desempeño del Jefe financiero, quien a su vez evalúa a su equipo?	**X**	
¿Existen políticas de administración del recurso humano (atraer, capacitar, evaluar y retener)?	**X**	
¿Cualquier comportamiento que no sea coherente con los estándares de conducta, las políticas, las expectativas de desempeño y las responsabilidades de gestión del riesgo empresarial se identifica, evalúa y corrige de manera oportuna?	**X**	
¿La función de recursos humanos ayuda a promover la competencia asistiendo a la administración en el desarrollo de descripciones de funciones y responsabilidades, facilitando la capacitación y evaluando el desempeño individual para la gestión del riesgo?	**X**	
¿El departamento de talento humano tiene planes para capacitar a los nuevos integrantes del departamento Financiero?		**X**

Tabla 82: Cuestionario Gobierno y Cultura
Elaborado por: Acurio, Y. (2020)

Estrategia y objetivos

Principio 6. Analiza el Contexto del Negocio.	SI	NO
¿El departamento Financiero identifica su entorno interno (capital, personas, proceso y tecnología) y las partes interesadas que pueden afectar su capacidad para lograr la presentación de informes a tiempo?	**X**	
¿El departamento Financiero identifica su entorno externo y las partes interesadas que puedan interferir al momento de generar la información y el alcance para anticiparse y adaptarse al cambio.? El entorno externo comprende varios factores como son: político, económico, social, tecnológico, legal y ambiental.	**X**	
Principio 7. Definición de Apetito al Riesgo.	SI	NO

¿El apetito de riesgo es comunicado y difundido en todo el departamento financiero de tal forma que todos los que toman las decisiones comprendan el apetito de riesgo con el que deben operar para generar la información?	**X**	
¿Se supervisa continuamente el apetito por el riesgo en todos los niveles del departamento Financiero y se adapta al cambio cuando es necesario?	**X**	
¿La Dirección administrativa del hospital crea una cultura que enfatiza la importancia del apetito por el riesgo y establece a los responsables de implementar la gestión del riesgo dentro de los parámetros de apetito por el riesgo?		**X**
¿Conoce la definición del apetito al riesgo?		**X**
¿El apetito al riesgo está alineado a las estrategias y a la gestión de riesgos de la institución?		**X**
Principio 8. Evalúa estrategias alternativas.	SI	NO
¿El departamento Financiero alinea sus estrategias para generar información correcta y eficiente con la misión, visión, valores y apetito de riesgo de la entidad?	**X**	
¿Se evalúa periódicamente las estrategias seleccionadas para mitigar los riesgos en la seguridad de la información?	**X**	
¿Al evaluar las estrategias la entidad se identifica y comprenden los posibles riesgos y oportunidades de cada estrategia que se está considerando?	**X**	
¿Existe un registro de los riesgos identificados en la seguridad de la información y sus estrategias para mitigarlos?		**X**
Principio 9. Formula Objetivos de Negocio.	SI	NO
¿El Departamento Financiera establece objetivos que son específicos, medibles, alcanzables y relevantes sobre la seguridad de la información?	**X**	
¿Las estrategias del área financiera se alinean con el objetivo de mantener un aseguramiento de información lo que permita a la entidad respaldar el logro de la misión y visión?	**X**	
¿La Dirección administrativa del hospital establece una medida para monitorear el desempeño del departamento financiero y respaldar que la información que se genera es correcta y apoya al cumplimiento de los objetivos?		**X**

Tabla 83: Cuestionario Estrategias y objetivos
Elaborado por: Acurio, Y. (2020)

Desempeño

Principio 10: Identifica Riesgos.	SI	NO
¿El departamento financiero identifica los riesgos, incluyendo nuevos, cambiantes y riesgos emergentes que pueden impactar en la información generada?	**X**	
¿El departamento financiero considera como los cambios pueden crear riesgos nuevos o emergentes que afecten a la información?	**X**	
¿Al identificar los riesgos se describe con precisión el riesgo, como las causas del riesgo, los posibles impactos del riesgo o el efecto del riesgo??		**X**
¿Existen mecanismos establecidos para identificar los riesgos que afecten directamente a la información que genera el departamento financiero?		**X**
¿Se establecen responsables para la identificación de riesgos en la generación de información del departamento financiero?		**X**
Principio 11: Evalua Severidad de Riesgo.	SI	NO

¿Los riesgos identificados e incluidos en el inventario de riesgos se evalúan a fin de comprender la gravedad de cada uno para el logro de la presentación de información del departamento financiero??		**X**
¿La severidad de un riesgo se evalúa en múltiples niveles (a través de divisiones, funciones y unidades operativas) de acuerdo con los objetivos del departamento financiero que pueden afectar?		**X**
¿El departamento financiero selecciona medidas para evaluar la gravedad del riesgo y el impacto en la información que genera?	**X**	
¿Como parte de la evaluación de riesgos, la colorimetría del mapa se alinea con un resultado de severidad particular y refleja el apetito de riesgo de la entidad?		**X**
Principio 12: Prioriza los Riesgos.	SI	NO
¿El departamento financiero prioriza los riesgos, de acuerdo a su severidad e impacto en la seguridad de su información y se alineada a su apetito para dar respuestas a los mismos?	**X**	
¿Se realiza un mapa de riesgos para identificar los riesgos altos, moderados y bajos?		**X**
¿Se actualiza periódicamente el mapa de riesgos para priorizarlos?		**X**
Principio 13: Implementa respuesta al riesgo.	SI	NO
¿Para todos los riesgos identificados, el departamento financiero selecciona y despliega una respuesta de riesgo, considerando la severidad y el impacto en la seguridad de la información?	**X**	
¿Una vez que se selecciona una respuesta de riesgo, se realizan actividades de control para garantizar que esas respuestas de riesgo se lleven a cabo según lo previsto?		**X**
¿Existe un documento formal sobre los riesgos identificados en el departamento financiero y cuál es la respuesta a los mismos?		**X**
¿Se establece los responsables de implementar la respuesta al riesgo seleccionadas?		**X**
Principio 14: Implementa respuesta al riesgo.	SI	NO
¿Existe un plan autorizado por la dirección para implementar la respuesta a los riesgos que afectan a la seguridad de la información en el área financiera?		**X**
¿Se evalúa periódicamente las acciones para implementar la respuesta a los riesgos que afectan a la seguridad de la información en el área financiera?	**X**	
¿El departamento informático apoya en el plan para dar respuesta a los riesgos en la seguridad de la información?	**X**	
¿En caso de desviaciones en la implementación de acciones para prevenir los riesgos en la seguridad de la información se corrigen?	**X**	

Tabla 84: Cuestionario Desempeño
Elaborado por: Acurio, Y. (2020)

Evaluación y revisión

Principio 15: Evalúa cambios sustanciales.	SI	NO
¿Se ha ocasionado perdida de información por los constantes cambios de tecnológicos y actualizaciones de los diferentes sistemas que maneja el departamento financiero?		**X**
¿Se identifica y evalúa los cambios tecnológicos que pueden afectar sustancialmente a la información que genera el departamento financiero?	**X**	
¿Como producto de los cambios en la infraestructura tecnológica el departamento financiero evalúa los riesgos de modificación en la información generada y realiza las correcciones?	**X**	

¿Cómo producto de cambios o actualizaciones en los sistemas, el departamento informático realiza copias de seguridad de la información que permita recuperar información?	**X**	
¿El departamento informático realiza capacitaciones después de realizar algún cambio o actualización de los sistemas informáticos?	**X**	
Principio 16: Revisa Riesgo y Desempeño	SI	NO
¿La Jefatura Financiera revisa los riesgos tecnológicos que afecten a la generación de la información?	**X**	
¿La Jefatura Financiera evalúa los niveles de desempeño de los sistemas para generar la información?	**X**	
¿La Jefatura Financiera revisa los riesgos que afecten a la integridad de la información?	**X**	
¿La Jefatura Financiera monitorea sus riesgos para lograr un aseguramiento de información?		**X**
Principio 17: Busca la mejora en la Gestión de Riesgos Empresarial.	SI	NO
¿La Jefatura Financiera busca mejorar la gestionar riesgos sobre la seguridad de la información?		**X**
¿La Jefatura Financiera se prepara constantemente a los posibles riesgos que afecten a la seguridad de la información?		**X**

Tabla 85: Cuestionario Evaluación y revisión
Elaborado por: Acurio, Y. (2020)

Información, comunicación y reporte

Principio 18: Apalanca información y tecnología.	SI	NO
¿El departamento financiero aprovecha los sistemas de información y tecnología de la entidad para respaldar la gestión de riesgos empresariales, poniendo información relevante para ayudar de una forma mas ágil en la toma de decisiones?	**X**	
¿El departamento financiero considera la información que es recogida desde otras fuentes para categorizar o evaluar sus riesgos, como Auditoría Interna, gestión de la información, áreas de peticiones, quejas y reclamos, reguladores, etc. y esta información sirve de base para el desarrollo de informe y respuestas de riesgos?		**X**
¿Se tienen controles para asegurar la calidad y confiabilidad de los datos y así proporcionar información correcta para respaldar las decisiones conscientes de los riesgos?		**X**
¿El departamento financiero evalúa que tecnología implementar de acuerdo a los objetivos de la organización, las necesidades, los costos y beneficios asociados, para equilibrar beneficios de obtener y administrar información con los costos de seleccionar o desarrollar tecnología de soporte?		**X**
¿Se realiza una revisión de los cambios internos, externos de las tecnologías de la información y si estos están aportando al aseguramiento de la información que se genera en el departamento financiero?		**X**
¿El departamento Financiero clasifica la información para posibilitar o restringir el acceso a la misma?	**X**	
Principio 19: Comunica información de riesgo.	SI	NO
¿Se cuenta con canales de comunicación abiertos donde se pueda recibir información de partes interesadas externas, con el propósito de generar información real? Por ejemplo, clientes o proveedores?		**X**
¿La Jefatura Financiera proporcionar supervisión y garantizar que se implementen las medidas adecuadas para asegurar la información que se maneja ?	**X**	
¿La Jefatura Financiera garantizar que se cumplan con los criterios de seguridad de la información y se comunique en caso de identificar riesgos?		**X**

Principio 20: Informe sobre riesgo, cultura y rendimiento.	SI	NO
¿La Jefatura Financiera informa sobre el riesgo, la cultura y el rendimiento, identificando los usuarios de los informes y sus funciones para así mismo generar el tipo de detalle en el informe?		**X**
¿La Jefatura Financiera informa sobre el riesgo, la cultura y el rendimiento de las tecnologías de información?		**X**

Tabla 86: Cuestionario información, comunicación y reporte
Elaborado por: Acurio, Y. (2020)

Una vez identificados los posibles riesgos se evaluarán mediante la ponderación del impacto y probabilidad de ocurrencia utilizando los parámetros del COSO ERM (Contraloria General del Estado , 2002) (Sulca & Becerra, 2017)

La probabilidad de ocurrencia se medirá de acuerdo con la escala de medición indicada en la siguiente tabla:

Probabilidad	**Estado**	**Valor**	**Descripción**
Improbable	Bajo	1	No se presenta en ningún escenario
Probable	Medio	2	Se daría bajo ciertas condiciones y frecuencia
Muy probable	Alto	3	Se presentaría frecuentemente afectando a las operaciones

Tabla 87: Probabilidad
Elaborado por: Acurio, Y. (2020)

IMPACTO	**ESTADO**	**VALOR**	**DESCRIPCIÓN**
Severo	Alto	4-5	Las consecuencias amenazarían las operaciones en el área financiera. Puede existir daño a la confianza o imagen de la institución

Moderado	Media	2-3	Afecta parcialmente a los procesos del área financiera
No significativo	Baja	1	Las consecuencias se manejan con procedimientos de rutina

Tabla 88: Impacto
Elaborado por: Acurio, Y. (2020)

Una vez generada la matriz de riesgos en base al impacto y la probabilidad se los representará gráficamente mediante un plano cartesiano con las siguientes condiciones:

- El eje X identificará la probabilidad de ocurrencia del factor de riesgo
- El eje Y identificará el impacto que este factor tiene

Finalmente, se obtendrá una matriz con los riesgos clasificados de tres categorías bajo, medio y alto.

RIESGOS	Calificación del Riesgo				
	Probabilidad		Impacto		Criticidad
	Nivel	Valor	Nivel	Valor	
1.-La Dirección administrativa del hospital no estable políticas para la gestión de riesgos sobre la seguridad de información en el departamento financiero	Probable	2	Severo	5	ALTO
2.-La Dirección administrativa del hospital no establece planes para supervisar los riesgos nuevos y emergentes de TI del departamento financiero	Muy probable	3	Severo	5	ALTO
3.- La Dirección administrativa no evalúa regularmente la estructura operativa de la Jefatura financiera	Probable	2	Medio	3	MEDIO
4.-La Dirección administrativa del hospital no explica claramente sobre el manejo de los riesgos en la tecnología de información	Muy Probable	3	Medio	2	MEDIO
5.-La Dirección administrativa del hospital no discute ampliamente sobre los riesgos identificados en las tecnologías de la información del departamento financiero	Probable	2	Medio	2	BAJO
6.- La Dirección administrativa del hospital no explica claramente los niveles de apetito al riesgo en TI	Probable	2	Medio	3	MEDIO
7.-La Dirección administrativa del hospital no crea conciencia de manera permanente sobre la importancia de los riesgos de TI en el departamento financieros	Probable	2	Severo	4	MEDIO
8.-La dirección no demuestra comunicación abierta proporcionando una variedad de canales para que el personal informen sus preocupaciones sobre la toma de riesgos, la conducta comercial o el comportamiento potencialmente inapropiados o excesivos sin temor a represalias o intimidación	Probable	2	Medio	2	BAJO

Tabla 89: Matriz de riesgos 1
Elaborado por: Acurio, Y. (2020)

RIESGOS	Calificación del Riesgo				
	Probabilidad		Impacto		Criticidad
	Nivel	Valor	Nivel	Valor	
9.-El departamento de talento humano no tiene planes para capacitar a los nuevos integrantes de los diferentes departamentos	Probable	2	Severo	3	MEDIO
10.-La Dirección administrativa del hospital no crea una cultura que enfatiza la importancia del apetito por los riesgos de TI y establece a los responsables de implementar la gestión del riesgo dentro de los parámetros de apetito por el riesgo	Muy Probable	3	Severo	4	ALTO
11.- Conoce la definición del apetito al riesgo	Improbable	1	Medio	2	BAJO
12.- El apetito al riesgo no está alineado a las estrategias y a la gestión de riesgos de la institución	Probable	2	Severo	3	MEDIO
13.-No existe un registro de los riesgos identificados en la seguridad de la información y sus estrategias para mitigarlos	Probable	2	Severo	5	ALTO
14.-La Dirección administrativa del hospital no establece una medida para monitorear el desempeño de TI en departamento financiero y respaldar que la información que se genera es correcta y apoya al cumplimiento de los objetivos	Improbable	1	Medio	2	BAJO
15.-El departamento financiero no identifica los riesgos de TI, incluyendo nuevos, cambiantes y riesgos emergentes que pueden impactar en la información generada	Muy probable	3	Severo	5	ALTO

Tabla 90: Matriz de riesgos 2
Elaborado por: Acurio, Y. (2020)

RIESGOS	Calificación del Riesgo				
	Probabilidad		Impacto		Criticidad
	Nivel	Valor	Nivel	Valor	
16.-No existen mecanismos establecidos para identificar los riesgos que afecten directamente a la información que genera el departamento financiero	Muy Probable	3	Severo	4	ALTO
17.- No se establecen responsables para la identificación de riesgos en la generación de información del departamento financiero	Muy Probable	3	Severo	4	ALTO
18.- La severidad de un riesgo no se evalúa en múltiples niveles (a través de divisiones, funciones y unidades operativas) de acuerdo con los objetivos del departamento financiero que pueden afectar	Probable	2	Severo	4	MEDIO
19.-Como parte de la evaluación de riesgos, la colorimetría del mapa no se alinea con un resultado de severidad particular y refleja el apetito de riesgo de la entidad	Muy Probable	3	Bajo	1	BAJO
20.-No se realiza un mapa de riesgos para identificar los riesgos altos, moderados y bajos	Muy Probable	3	Severo	4	ALTO
21.-No se actualiza periódicamente el mapa de riesgos para priorizarlos	Muy Probable	3	Severo	5	ALTO
22.- Una vez que se selecciona una respuesta de riesgo, no se realizan actividades de control para garantizar que esas respuestas de riesgo se lleven a cabo según lo previsto	Probable	2	Severo	4	MEDIO
23.- No existe un documento formal sobre los riesgos identificados en el departamento financiero y cuál es la respuesta a los mismos	Probable	2	Medio	2	BAJO

Tabla 91: Matriz de riesgos 3
Elaborado por: Acurio, Y. (2020)

RIESGOS	Calificación del Riesgo				
	Probabilidad		Impacto		Criticidad
	Nivel	Valor	Nivel	Valor	
24.- No se establece los responsables de implementar la respuesta al riesgo seleccionadas	Muy Probable	3	Medio	2	MEDIO
25.-No existe un plan autorizado por la dirección para implementar la respuesta a los riesgos que afectan a la seguridad de la información en el área financiera	Improbable	1	Baja	1	BAJO
26.-La Jefatura Financiera no monitorea sus riesgos para lograr un aseguramiento de información	Probable	2	Severo	5	ALTO
27.- La Jefatura Financiera no busca mejorar la gestionar riesgos sobre la seguridad de la información	Probable	2	Severo	5	ALTO
28.- La Jefatura Financiera no se prepara constantemente a los posibles riesgos que afecten a la seguridad de la información	Muy Probable	3	Medio	2	MEDIO
29.- El departamento financiero no considera la información que es recogida desde otras fuentes para categorizar o evaluar sus riesgos, como Auditoría Interna, gestión de la información, áreas de peticiones, quejas y reclamos, reguladores, etc. y esta información sirve de base para el desarrollo de informe y respuestas de riesgos	Probable	2	Medio	3	MEDIO
30.- Se tienen controles para asegurar la calidad y confiabilidad de los datos y así proporcionar información correcta para respaldar las decisiones conscientes de los riesgos	Probable	2	Severo	5	ALTO

Tabla 92: Matriz de riesgos 4
Elaborado por: Acurio, Y. (2020)

RIESGOS	Calificación del Riesgo				
	Probabilidad		Impacto		Criticidad
	Nivel	Valor	Nivel	Valor	
31.- El departamento financiero no evalúa que tecnología implementar de acuerdo a los objetivos de la organización, las necesidades, los costos y beneficios asociados, para equilibrar beneficios de obtener y administrar información con los costos de seleccionar o desarrollar tecnología de soporte	Probable	2	Severo	5	ALTO
32.- No se realiza una revisión de los cambios internos, externos de las tecnologías de la información y si estos están aportando al aseguramiento de la información que se genera en el departamento financiero	Muy Probable	3	Severo	5	ALTO
33.- No se cuenta con canales de comunicación abiertos donde se pueda recibir información de partes interesadas externas, con el propósito de generar información real. Por ejemplo, clientes o proveedores	Probable	2	Medio	3	MEDIO
34.- La Jefatura Financiera no garantiza que se cumplan con los criterios de seguridad de la información y se comunique en caso de identificar riesgos	Muy Probable	3	Severo	5	ALTO
35.- La Jefatura Financiera no informa sobre el riesgo, la cultura y el rendimiento, identificando los usuarios de los informes y sus funciones para así mismo generar el tipo de detalle en el informe	Improbable	1	Medio	2	BAJO
36.- La Jefatura Financiera no informa sobre el riesgo, la cultura y el rendimiento de las tecnologías de información	Probable	2	Medio	3	MEDIO

Tabla 93: Matriz de riesgos 5
Elaborado por: Acurio, Y. (2020)

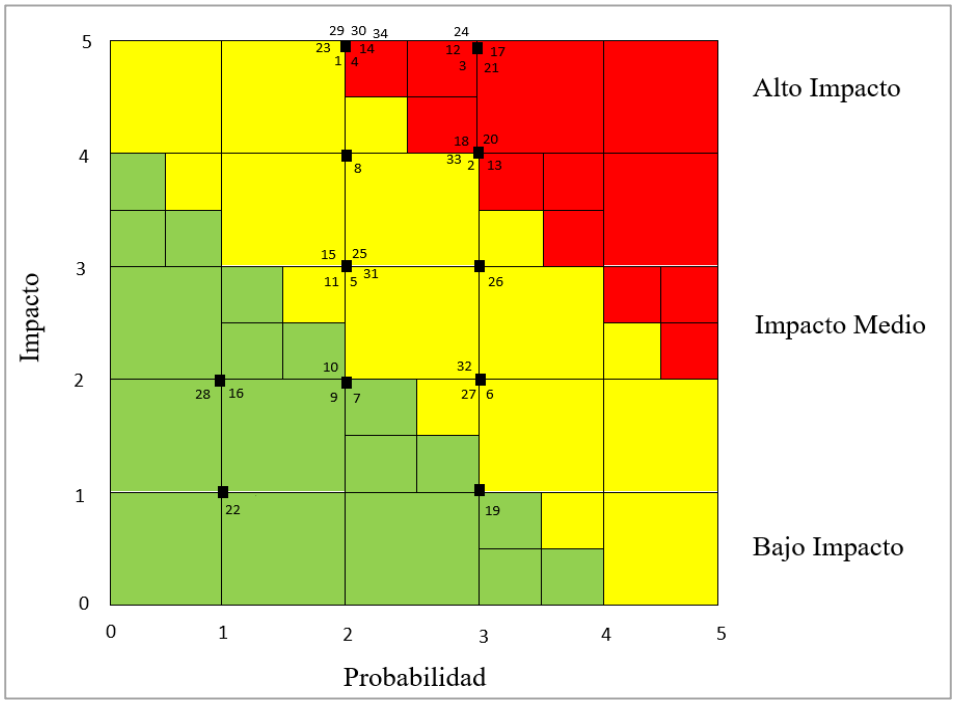


Figura 18: Plano Cartesiano de riesgos
Elaborado por: Acurio, Y. (2021)

Análisis

Los riesgos con criticidad alta están ubicados en la zona roja del plano cartesiano de la figura son:

- R1: La Dirección administrativa del hospital no estable políticas para la gestión de riesgos sobre la seguridad de información en el departamento financiero.
- R2: La Dirección administrativa del hospital no establece planes para supervisar los riesgos nuevos y emergentes de TI del departamento financiero.
- R10: La Dirección administrativa del hospital no crea una cultura que enfatiza la importancia del apetito por los riesgos de TI y establece a los responsables de implementar la gestión del riesgo dentro de los parámetros de apetito por el riesgo.

- R13: No existe un registro de los riesgos identificados en la seguridad de la información y sus estrategias para mitigarlos
- R15: El departamento financiero no identifica los riesgos de TI, incluyendo nuevos, cambiantes y riesgos emergentes que pueden impactar en la información generada
- R16: No existen mecanismos establecidos para identificar los riesgos que afecten directamente a la información que genera el departamento financiero
- R17: No se establecen responsables para la identificación de riesgos en la generación de información del departamento financiero
- R20: No se realiza un mapa de riesgos para identificar los riesgos altos, moderados y bajos
- R21: No se actualiza periódicamente el mapa de riesgos para priorizarlos
- R26: La Jefatura Financiera no monitorea sus riesgos para lograr un aseguramiento de información.
- R27: La Jefatura Financiera no busca mejorar la gestionar riesgos sobre la seguridad de la información.
- R30: Se tienen controles para asegurar la calidad y confiabilidad de los datos y así proporcionar información correcta para respaldar las decisiones conscientes de los riesgos.
- R31: El departamento financiero no evalúa que tecnología implementar de acuerdo a los objetivos de la organización, las necesidades, los costos y beneficios asociados, para equilibrar beneficios de obtener y administrar información con los costos de seleccionar o desarrollar tecnología de soporte

- R32: No se realiza una revisión de los cambios internos, externos de las Tecnologías de la información y si estos están aportando al aseguramiento de la información que se genera en el departamento financiero
- R34: La Jefatura Financiera no garantiza que se cumplan con los criterios de seguridad de la información y se comunique en caso de identificar riesgos.

Los riesgos con criticidad media están ubicados en la zona amarilla del plano cartesiano de la figura son:

- R3: La Dirección administrativa no evalúa regularmente la estructura operativa de la Jefatura financiera
- R4: La Dirección administrativa del hospital no explica claramente sobre el manejo de los riesgos en la tecnología de información
- R6: La Dirección administrativa del hospital no explica claramente los niveles de apetito al riesgo en TI
- R7: La Dirección administrativa del hospital no crea conciencia de manera permanente sobre la importancia de los riesgos de TI en el departamento financieros
- R9: El departamento de talento humano no tiene planes para capacitar a los nuevos integrantes de los diferentes departamentos
- R12: El apetito al riesgos no está alineado a las estrategias y a la gestión de riesgos de la institución
- R18: La severidad de un riesgo no se evalúa en múltiples niveles (a través de divisiones, funciones y unidades operativas) de acuerdo con los objetivos del departamento financiero que pueden afectar

- R22: Una vez que se selecciona una respuesta de riesgo, no se realizan actividades de control para garantizar que esas respuestas de riesgo se lleven a cabo según lo previsto
- R24 No se establece los responsables de implementar la respuesta al riesgo seleccionadas
- R28: La Jefatura Financiera no se prepara constantemente a los posibles riesgos que afecten a la seguridad de la información
- R29: El departamento financiero no considera la información que es recogida desde otras fuentes para categorizar o evaluar sus riesgos, como Auditoria Interna, gestión de la información, áreas de peticiones, quejas y reclamos, reguladores, etc y esta información sirve de base para el desarrollo de informe y respuestas de riesgos
- R33: No se cuenta con canales de comunicación abiertos donde se pueda recibir información de partes interesadas externas, con el propósito de generar información real. Por ejemplo, clientes o proveedores
- R36: La Jefatura Financiera no informa sobre el riesgo, la cultura y el rendimiento de las tecnologías de información

Los riesgos con criticidad baja están ubicados en la zona verde del plano cartesiano de la figura son:

- R5: La Dirección administrativa del hospital no discute ampliamente sobre los riesgos identificados en las tecnologías de la información del departamento financiero
- R8: La dirección no demuestra comunicación abierta proporcionando una variedad de canales para que el personal informen sus preocupaciones sobre la

toma de riesgos, la conducta comercial o el comportamiento potencialmente inapropiados o excesivos sin temor a represalias o intimidación

- R11: Conoce la definicion del apetito al riesgo
- R14: La Dirección administrativa del hospital no establece una medida para monitorear el desempeño de TI en departamento financiero y respaldar que la información que se genera es correcta y apoya al cumplimiento de los objetivos
- R19: Como parte de la evaluación de riesgos, la colorimetría del mapa no se alinea con un resultado de severidad particular y refleja el apetito de riesgo de la entidad
- R23: No existe un documento formal sobre los riesgos identificados en el departamento financiero y cual es la respuesta a los mismos
- R25: No existe un plan autorizado por la dirección para implementar la respuesta a los riesgos que afectan a la seguridad de la información en el área financiera

Interpretación

A partir de los resultados obtenidos en el análisis se puede decir que hace falta integrar políticas internas e impulsar una cultura para la gestión de riesgos en las tecnologías informáticas que garanticen la seguridad de la información que se genera y maneja en el departamento financiero, es evidente la necesidad de tomar conciencia e incorporar un efectivo gobierno de TI y así establecer mecanismos para identificar los riesgos que afecten directamente a la información que genera el departamento financiero y así establecer estrategias para mitigar y monitorear sus riesgos para lograr un aseguramiento de información.

4.2 Contraste entre la metodología COBIT y el marco de regencia COSO ERM

Uno de los principales fines del presente estudio es determinar la relación existente entre el aseguramiento de la información en el área de informática y el monitoreo de riesgo en el subgerencia financiera del Hospital Básico del IESS de Latacunga. Así, en vista de que se han aplicado las dos metodologías (COBIT y COSO ERM) de forma independiente, tomando como unidad de análisis la institución de salud, a priori no es posible realizar un contraste entre los valores obtenidos por estos instrumentos. Por este motivo, es necesario construir una nueva estructura de datos, con una unidad de análisis diferente, que no se aleje de la noción del problema inicial y que permita asignar un valor proveniente de la metodología COSO ERM.

En este sentido, se procedió a tomar como la nueva unidad de análisis a los procesos diagnosticados en la metodología COBIT, que como ya se conoce, se encuentra determinado por un total de 34 procesos que se agrupan en 6 dominios. Para cada uno de estos procesos se han identificado uno o varios riesgos del departamento financiero que caracterizan a dicho proceso, y el valor asignado corresponde al promedio de los o puntajes de probabilidad e impacto entre estos riesgos para el proceso en cuestión. En este apartado se discute la distribución de riesgos, y el promedio obtenido para cada proceso. Los resultados se analizan por dominios:

4.2.1 Dominio 1: Planear y Organizar (PO)

Proceso	Riesgos asociados	Madurez	Impacto	Probabilidad
PO1	R12	3,35	2,0	3,0
PO2	R3	2,19	2,0	3,0
PO3	R17	3,01	3,0	4,0
PO4	R4	2,31	3,0	2,0
PO5	R27	2,69	2,0	5,0
PO6	R5	2,19	2,0	2,0
PO7	R9	3,04	2,0	3,0
PO8	R30	1,60	2,0	5,0
PO9	R2	2,49	3,0	5,0
PO10	R8	2,70	2,0	2,0

Tabla 94: Contraste entre el aseguramiento de la información y el monitoreo de riesgo del dominio planear y organizar
Elaborado por: Acurio, Y. (2020)

La naturaleza de los procesos que integran el dominio planear y organizar han permitido que se le asocie una puntuación relacionada al monitoreo de riesgos por medio del promedio del riesgo o grupo de riesgos; y se ha atribuido a este valor como el identificador del impacto y la probabilidad de riesgo asociado a cada uno de los procesos.

En este sentido, para el proceso PO1: Definir un Plan Estratégico de TI, se han asociado los riesgos que se refieren que no están alineado a las estrategias y a la gestión de riesgos de la institución. Para el caso de los procesos PO2: La Dirección administrativa no evalúa regularmente la estructura operativa de la Jefatura financiera; y PO3: No se establecen responsables para la identificación de riesgos en la generación de información del departamento financiero, los valores de probabilidad y madurez correspondiente a los riesgos R3.

Ahora, para el caso del proceso PO4: Definir los Procesos, Organización y Relaciones de TI, además el riesgo asociado a la dirección administrativa del hospital no explica claramente sobre el manejo de los riesgos en la tecnología de información (R4), en el

caso del proceso PO5: Administrar la Inversión en TI, se han considerado afinidad con la Jefatura Financiera no busca mejorar la gestionar riesgos sobre la seguridad de la información (R27).

El proceso PO6: Comunicar las Aspiraciones y la Dirección de la Gerencia; tiene que ver con la Dirección administrativa del hospital no discute ampliamente sobre los riesgos identificados en las tecnologías de la información del departamento financiero (R5).

En el proceso PO7: Administrar Recursos Humanos de TI; se han identificado el riesgo asociado: El departamento de talento humano no tiene planes para capacitar a los nuevos integrantes de los diferentes departamentos (R9). En el caso del proceso PO8: Administrar la Calidad, en realidad muestra una relación con muchos riesgos, pero se ha identificado que el que más se aproxima es no se tienen controles para asegurar la calidad y confiabilidad de los datos y asi proporcionar información correcta para respaldar las decisiones conscientes de los riesgos (R30).

Se puede ver que el proceso PO9: Evaluar y Administrar los Riesgos de TI, se encuentra asociado al riesgo: La Dirección administrativa del hospital no establece planes para supervisar los riesgos nuevos y emergentes de TI del departamento financiero (R2); Finalmente, al proceso P10: Administrar Proyectos, le concierne a que la dirección no demuestra comunicación abierta proporcionando una variedad de canales para que el personal informen sus preocupaciones sobre la toma de riesgos, la conducta comercial o el comportamiento potencialmente inapropiados o excesivos sin temor a represalias o intimidación (R8)

4.2.2 Dominio 2: Adquirir e Implementar (AI)

Proceso	Riesgos asociados	Madurez	Impacto	Probabilidad
AI1	R31	2,29	2,0	5,0
AI2	R32	2,45	3,0	5,0
AI3	R7	2,36	2,0	4,0
AI4	R6	3,27	2,0	3,0
AI5	R25	3,38	1,0	1,0
AI6	R24	2,44	3,0	2,0
AI7	R22	2,80	2,0	4,0

Tabla 95: Contraste entre el aseguramiento de la información y el monitoreo de riesgo del dominio adquirir e implementar
Elaborado por: Acurio, Y. (2020)

Ahora, se puede mencionar que la naturaleza de los procesos que integran el dominio adquirir e implementar han permitido que se le asocie una puntuación relacionada al monitoreo de riesgos por medio del promedio del riesgo o grupo de riesgos; y se ha atribuido a este valor como el identificador del impacto y la probabilidad de riesgo asociado a cada uno de los procesos.

Para el proceso AI1: Identificar soluciones automatizadas, se han asociado al riesgo que se refieren a que el departamento financiero no evalua que tecnologia implementar de acuerdo a los obejtivos de la organización, las necesidades, los costos y beneficios asociados, para equilibrar beneficios de obtener y administrar información con los costos de seleccionar o desarrollar tecnologia de soporte (R31). En el caso del proceso AI2: Adquirir y Mantener Software Aplicativo; este se relaciona con que no se realiza una revisión de los cambios internos, externos de las Tecnologias de la informacion y si estos estan aportando al aseguramiento de la informacion que se genera en el deparatamento financiero (R32).

En el proceso AI3: Adquirir y Mantener Infraestructura Tecnológica, ha encontrado afinidad con el riesgo: La Dirección administrativa del hospital no crea conciencia de

manera permanente sobre la importancia de los riesgos de TI en el departamento financieros (R7). Para el caso del proceso AI4: Facilitar la Operación y el Uso, se asocia con el riesgo referente a que la dirección administrativa del hospital no explica claramente los niveles de apetito al riesgo en TI (R6). En el caso del proceso AI5: Adquirir Recursos de TI, se han considerado afinidad a que no existe un plan autorizado por la dirección para implementar la respuesta a los riesgos que afectan a la seguridad de la información en el área financiera (R25).

El proceso AI6: Administrar Cambios; tiene que ver con el que no se establece los responsables de implentar la respuesta al riesgo seleccionadas (R24).

Finalmente, en el proceso AI7: Instalar y Acreditar Soluciones y Cambios; se ha identificado el riesgo asociado: Una vez que se selecciona una respuesta de riesgo, no se realizan actividades de control para garantizar que esas respuestas de riesgo se lleven a cabo según lo previsto (R22).

4.2.3 Dominio 3: Entregar y Dar Soporte (DS)

Proceso	Riesgos asociados	Madurez	Impacto	Probabilidad
DS1	R1	2,22	2,0	5,0
DS2	R29	3,03	2,0	3,0
DS3	R28	2,61	3,0	2,0
DS4	R26	2,79	2,0	5,0
DS5	R34	2,32	3,0	5,0
DS6	R16	2,54	3,0	4,0
DS7	R33	2,65	2,0	3,0
DS8	R35	1,80	1,0	2,0
DS9	R36	2,54	2,0	3,0
DS10	R21	2,70	3,0	5,0
DS11	R18	2,59	2,0	4,0
DS12	R10	2,04	3,0	4,0
DS13	R13	2,40	2,0	5,0

Tabla 96: Contraste entre el aseguramiento de la información y el monitoreo de riesgo del dominio entregar y dar soporte
Elaborado por: Acurio, Y. (2020)

Asimismo, por medio de la naturaleza de los procesos que integran el entregar y dar soporte se ha podido asociar una puntuación de monitoreo de riesgos tomado como un promedio de los riesgos asociados; y se ha atribuido a este valor como el identificador del impacto y la probabilidad de riesgo asociado a cada uno de los procesos.

El proceso DS1: Definir y administrar los niveles de servicio, se han asociado el riesgo, la Dirección administrativa del hospital no estable políticas para la gestión de riesgos sobre la seguridad de información en el departamento financiero (R1). En el caso del proceso DS2: Administrar los Servicios de Terceros; este se relaciona con que el departamento financiero no considera la información que es recogida desde otras fuentes para categorizar o evaluar sus riesgos, como Auditoria Interna, gestión de la información, areas de peticiones, quejas y reclamos, reguladores, etc y esta información sirve de base para el desarrollo de informe y respuestas de riesgos (R29). El proceso DS3: Administrar el Desempeño y la Capacidad, ha encontrado afinidad con el riesgo: La Jefatura Financiera no se prepara constantemente a los posibles riesgos que afecten a la seguridad de la información (R28).

Para el caso del proceso DS4: Garantizar la Continuidad del Servicio, se asocia con el riesgo referente a la Jefatura Financiera no monitorea sus riesgos para lograr un aseguramiento de información (R26). En el caso del proceso DS5: Garantizar la Seguridad de los Sistemas, se han considerado su afinidad con que la Jefatura Financiera no garantiza que se cumplan con los criterios de seguridad de la información y se comunique en caso de identificar riesgos (R34).

El proceso DS6: Identificar y Asignar Costos; tiene que ver con que no existen mecanismos establecidos para identificar los riesgos que afecten directamente a la

información que genera el departamento financiero (R16). En el proceso DS7: Educar y Entrenar a los Usuarios; se han relacionado con que no se cuenta con canales de comunicación abiertos donde se pueda recibir información de partes interesadas externas, con el proposito de generar informacion real. Por ejemplo, clientes o proveedores (R33).

Al proceso DS8: Administrar la Mesa de Servicio y los Incidentes, se le ha asociado el riesgo que se refiere a que la Jefatura Financiera no informa sobre el riesgo, la cultura y el rendimiento, identificando los usuarios de los informes y sus funciones para asi mismo generar el tipo de detalle en el informe (R35). En el caso del proceso DS9: Administrar la Configuración; este se relaciona con que la Jefatura Financiera no informa sobre el riesgo, la cultura y el rendimiento de las tecnologias de información (R36). El proceso DS10: Administración de Problemas, ha encontrado afinidad con que no se actualiza periódicamente el mapa de riesgos para priorizarlos (R21).

Para el caso del proceso DS11: Administración de Datos, se asocia con el riesgo la severidad de un riesgo no se evalúa en múltiples niveles (a través de divisiones, funciones y unidades operativas) de acuerdo con los objetivos del deparatamento financiero que pueden afectar (R18). En el caso del proceso DS12: Administración del Ambiente Físico, se han considerado su afinidad con la que la Dirección administrativa del hospital no crea una cultura que enfatiza la importancia del apetito por los riesgos de TI y establece a los responsables de implementar la gestión del riesgo dentro de los parámetros de apetito por el riesgo (R10). Finalmente, el proceso DS13: Administración de Operaciones; tiene que ver con que no existe un registro de los riesgos identificados en la seguridad de la información y sus estrategias para mitigarlos (R13).

4.2.4 Dominio 4: Monitorear y Evaluar (ME)

Proceso	Riesgos asociados	Madurez	Impacto	Probabilidad
ME1	R14	2,48	1,0	2,0
ME2	R15	2,77	3,0	5,0
ME3	R19	2,26	3,0	1,0
ME4	R23	2,70	2,0	2,0

Tabla 97: Contraste entre el aseguramiento de la información y el monitoreo de riesgo del dominio monitoreas y evaluar
Elaborado por: Acurio, Y. (2020)

Como punto final, por medio de la naturaleza de los procesos que integran el monitorear y evaluar se ha podido asociar una puntuación de monitoreo de riesgos tomado como un promedio de los riesgos asociados; y se ha atribuido a este valor como el identificador del impacto y la probabilidad de riesgo asociado a cada uno de los procesos.

El proceso ME1: Monitorear y Evaluar el Desempeño de TI, se ha asociado con el riesgo que se refieren a: La Dirección administrativa del hospital no establece una medida para monitorear el desempeño de TI en departamento financiero y respaldar que la información que se genera es correcta y apoya al cumplimiento de los objetivos (R14).

En el caso del proceso ME2: ME2 Monitorear y Evaluar el Control Interno; este se relaciona con que el departamento financiero no identifica los riesgos de TI, incluyendo nuevos, cambiantes y riesgos emergentes que pueden impactar en la información generada (R15).

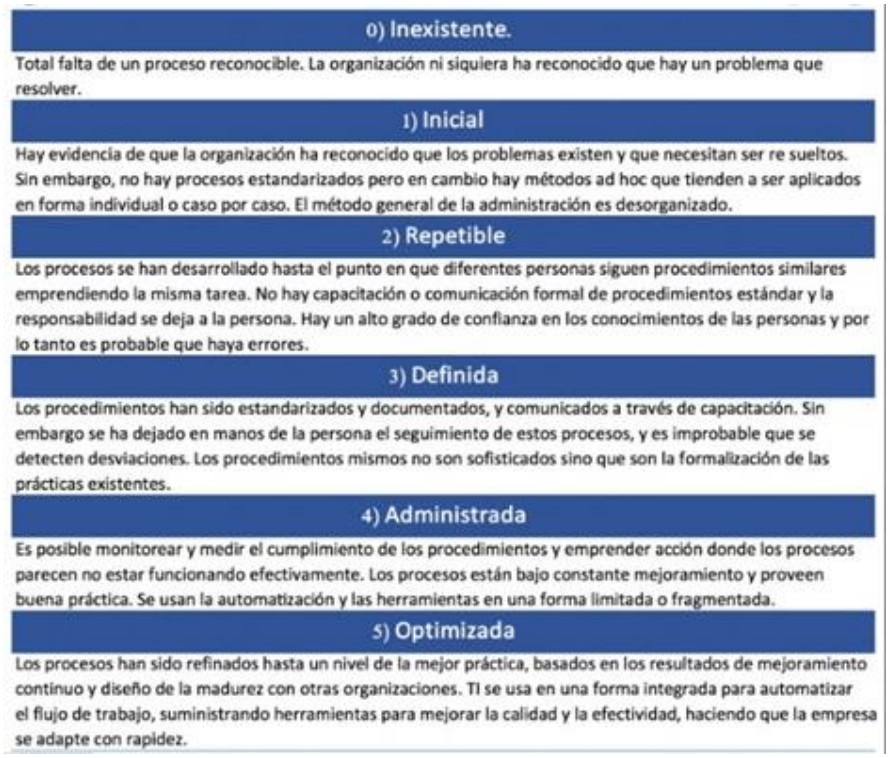
El proceso ME3: Garantizar el Cumplimiento con Requerimientos Externos, ha encontrado afinidad con que como parte de la evaluación de riesgos, la colorimetría del mapa no se alinea con un resultado de severidad particular y refleja el apetito de riesgo de la entidad (R19). Para el caso del proceso ME4: Proporcionar Gobierno de TI, se

asocia con el riesgo referente a No existe un documento formal sobre los riesgos identificados en el departamento financiero y cual es la respuesta a los mismos (R23).

4.2 Respuestas a las preguntas de investigación

¿Cuál es el nivel de aseguramiento de la información en los procesos de TI en el Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga?

El Instituto de Gestión de las Tecnologías de la Información (ITGI, por sus siglas en inglés) presenta a COBIT: Gestión, control y auditoría para la información y tecnología relacionada, como modelo de madurez para el marco de trabajo Objetivos de Control para Información y Tecnologías Relacionadas (COBIT: Control Objectives for Information and Related Technology). En sentido general cada modelo abarca 5 niveles de madurez que van desde un nivel 0 donde se defi ne que no existe la arquitectura empresarial hasta un nivel 5 de arquitectura empresarial optimizada, donde se percibe una comunicación directa entre las necesidades del negocio y la tecnología (Martinez, Robaina, & Stuart, 2015).



Dominio		**Madurez**	**Promedio Madurez**
Planificar y Organizar	PO1	3,35	2,56
	PO2	2,19	
	PO3	3,01	
	PO4	2,31	
	PO5	2,69	
	PO6	2,19	
	PO7	3,04	
	PO8	1,60	
	PO9	2,49	
	PO10	2,70	
Adquirir e implementar	AI1	2,29	2,71
	AI2	2,45	
	AI3	2,36	
	AI4	3,27	
	AI5	3,38	
	AI6	2,44	
	AI7	2,80	
Entregar y Dar Soporte	DS1	2,22	2,48
	DS2	3,03	
	DS3	2,61	

	DS4	2,79	
	DS5	2,32	
	DS6	2,54	
	DS7	2,65	
	DS8	1,80	
	DS9	2,54	
	DS10	2,70	
	DS11	2,59	
	DS12	2,04	
	DS13	2,40	
Monitorear y Evaluar	ME1	2,48	2,55
	ME2	2,77	
	ME3	2,26	
	ME4	2,70	

Tabla 98: Nivel de madurez de los dominios del Aseguramiento de la Información
Elaborado por: Acurio, Y. (2020)

Entre los dominios de Aseguramiento de Información se puede ver que el Adquirir e Implementar tiene un promedio general más elevado (2,71); seguido del planificar y organizar (2,56); luego el monitorear y evaluar; y por último el estregar y dar soporte (2,48).

El nivel de madurez promedio para todos los dominios se encuentra cercano a 2 o es repetible lo cual indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal de los procesos estándar.

¿Cuál es el nivel de riesgo en los procesos del área financiera en Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga?

La metodología COSO ERM fue diseñada para identificar eventos potenciales que afectasen a una entidad, evaluar y responder a los riesgos detectados, para que estén

dentro de los límites de nivel aceptables como parte de una buena administración. La aplicación de esta metodología, ha permitido identificar los riesgos existentes en la empresa y evaluar la eficiencia y eficacia de los controles establecidos, a fin de que la entidad logre los objetivos trazados. Las conclusiones de la investigación demostraron que la metodología COSO ERM identificó y administró riesgos a nivel de la entidad; alineó el nivel de riesgo aceptado con la estrategia de la empresa; mejoró las decisiones de respuesta al riesgo; minimizó sorpresas y pérdidas operativas; proveyó respuestas integradas a riesgos múltiples y sobre todo, aprovechó oportunidades (Sanchez, 2017).

Para establecer el nivel de riesgo en base a los compones del COSO ERM en la institución se obtuvieron los siguientes resultados:

COMPONENTE	TOTAL DE RIESGOS ENCONTRADOS	TOTAL ITEMS
GOBIERNO Y CULTURA	7	27
ESTRATEGIAS Y OBJETIVOS	5	14
DESEMPEÑO	12	20
EVALUACIÓN Y REVISIÓN	4	11
INFORMACIÓN, COMUNICACIÓN Y REPORTE	8	11

Tabla 99: Resultados de COSO ERM
Elaborado por: Acurio, Y. (2020)

Al realizar ponderación de los riesgos encontratos en relación en el total de ítems tenemos un porcentaje de riesgo por componente obteniendo los siguientes resultados:

COMPONENTE	NIVEL DE RIESGO
GOBIERNO Y CULTURA	25,93%
ESTRATEGIAS Y OBJETIVOS	35,71%
DESEMPEÑO	60,00%
EVALUACIÓN Y REVISIÓN	36,36%
INFORMACIÓN, COMUNICACIÓN Y REPORTE	72,73%
TOTAL DE LA INSTITUCION	43,37%

Tabla 100: Porcentaje
Elaborado por: Acurio, Y. (2020)

Como solución a la pregunta de investigación planteada se establece que el nivel de riesgo en los procesos del área financiera en Hospital Básico del Instituto Ecuatoriano de Seguridad Social de Latacunga es de 43,47%

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- De manera general, el nivel de madurez promedio para todos los dominios del aseguramiento de la información se caracterizan por ser repetible lo cual indica que los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares realizando la misma tarea, lo que hace evidente una falta de comunicación formal mediante documentos oficiales como manuales, guías o planes y oficios para que esta comunicación tenga un registro y un seguimiento, de los procesos estándar que se realizan en el Hospital Básico del IESS de Latacunga. Entre estos dominios se destaca el adquirir e implementar; y el planificar y organizar.
- El monitoreo de riesgos pone en evidencia falta de integración en políticas internas, así como la escaza promoción de una cultura para la gestión de riesgos en las tecnologías informáticas que garanticen la seguridad de la información que se genera y maneja en el departamento financiero del Hospital Básico del IESS de Latacunga.
- La presente investigación estimó una correlación inversa aproximada de 0,5 entre el aseguramiento de la información y el impacto - probabilidad de riesgo lo que indica que, un alto nivel de madurez del aseguramiento puede reducir los niveles de impacto y probabilidad de que se presenten riesgos sobre la seguridad de la información.

5.2 Recomendaciones

- Una vez que se ha realizado una apreciación general de los procesos que definen los dominios del aseguramiento de la información, resulta imperante señalar que hay muchos aspectos por mejorar. En este sentido, se sugiere prestar especial atención a aquellos procesos con un nivel de madurez por debajo de 2, como punto de partida para un plan de acción que busque asegurar que se cuenta con un nivel de madurez consolidado.
- De igual manera, resulta evidente la necesidad de tomar conciencia e incorporar un efectivo gobierno de TI y así establecer mecanismos para identificar los riesgos que afecten directamente a la información que genera el departamento financiero y así establecer estrategias para mitigar y monitorear sus riesgos para lograr un aseguramiento de información.
- Los resultados de la asociación entre el aseguramiento de la información y el monitoreo de riesgo, en este caso, resultaron a favor de Hospital Básico del IESS de Latacunga, ya que se encontró una una influencia positiva del aseguramiento de la información hacia el impacto o probabilidad de riesgo. En este caso se podría inferir que el aseguramiento de la información reduce en un 50% el impacto y probabilidad de riesgos; por lo cual, se recomienda minimizar el impacto del riesgo en el tratamiento de la información del departamento financiero.

BIBLIOGRAFÍA

AUDITOOL. (23 de ENERO de 2019). Obtenido de https://www.auditool.org/blog/sector-gobierno/6355-coso-en-entidades-del-sector-gobierno-y-privado

Gonzales, A., & Pando, M. (2016). Obtenido de https://www.nodo50.org/cubasigloXXI/economia/gcueto_311206.pdf

Asamblea Nacional del Ecuador . (20 de Octubre de 2008). *Constitucion de la República de Ecuador*. Obtenido de Constitucion de la República de Ecuador: http://www.inocar.mil.ec/web/images/lotaip/2015/literal_a/base_legal/A._Constitucion_republica_ecuador_2008constitucion.pdf

La Contraloria General del Estado . (2009). *Normas de control interno.* Obtenido de https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

Contraloría General del Estado . (2002). Obtenido de https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_23_ley_org_cge.pdf

Contraloria General del Estado . (2002). *LEY ORGANICA DE LA CONTRALORIA GENERAL DEL ESTADO*. Obtenido de https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_23_ley_org_cge.pdf

Contraloria General del Estado. (22 de Noviembre de 2001). *Manual de Auditoría de Gestión Para la Contraloria General del Estado y entidades y organismos del sector publico sometisdos a su control.*

Soler, R., Varela, P., Oñate, A., & Naranjo, E. (2018). *La gestión de riesgos: el ausente recurrente de la administracion de empresas* .

Martínez, E., & García, J. (Diciembre de 2011). *Gobierno de TI de Cobit.*

Baena, G., Mendoza, R., & Coronado, E. (2019). *IMPORTANCIA DE LA NORMA ISO/EIC 27000 EN LA IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN.* Obtenido de https://www.hacienda.go.cr/Sidovih/uploads//Archivos/Articulo/La%20importancia%20de%20la%20norma-ISO-eic.pdf

Velásquez, L. (2014). *METODOLOGÍA PARA MONITOREAR RIESGOS ESTRATÉGICOS PROVENIENTES DEL ENTORNO EXTERNO.* Obtenido de https://repository.eafit.edu.co/bitstream/handle/10784/2954/LuisFernando_VelasquezFranco_2014.pdf?sequence=1#:~:text=Identificaci%C3%B3n%20de%20riesgos%20estrat%C3%A9gicos%3A%20para,%2C%20J.%2C%202010).

Mejía, R., & Villanueva, E. (10 de Diciembre de 2014). *METODOLOGÍA PARA MONITOREAR RIESGOS ESTRATÉGICOS.* Obtenido de https://silo.tips/download/metodologia-para-monitorear-riesgos-estrategicos

Graterol, R. (2013). *Investigación de campo.* Obtenido de http://www.uovirtual.com.mx/moodle/lecturas/metoprot/10.pdf

Terán, B. (2015). *Tipod de investigación.* Obtenido de http://www.tiposdeinvestigacion.com/investigacion-exploratoria/

Miró, J. (12 de septiembre de 2006). *La investigación descriptiva.* Obtenido de http://noemagico.blogia.com/2006/091301-la-investigacion-descriptiva.php

Espinoza, E. (2019). *LAS VARIABLES Y SU OPERACIONALIZACIÓN EN LA INVESTIGACIÓN EDUCATIVA.* . Obtenido de http://scielo.sld.cu/pdf/rc/v15n69/1990-8644-rc-15-69-171.pdf

Moreno, A., & Gallardo, Y. (1999). *APRENDER A INVESTIGAR.* Obtenido de https://academia.utp.edu.co/grupobasicoclinicayaplicadas/files/2013/06/3.-Recolecci%C3%B3n-de-la-Informaci%C3%B3n-APRENDER-A-INVESTIGAR-ICFES.pdf

Neill, D., & Cortez, L. (2018). *PROCESOS Y FUNDAMENTOS DE LA INVESTIGACION CIENTIFICA* . Obtenido de http://repositorio.utmachala.edu.ec/bitstream/48000/12498/1/Procesos-y-FundamentosDeLainvestiagcionCientifica.pdf

Instituto Nacional de Estadística y Geografía. (2012). *PROCESAMIENETO DE LA INFORMACION* . Obtenido de https://www.snieg.mx/documentacionportal/normatividad/vigente/doctos_genbasica/procesamiento_informacion.pdf

Pederiva, A. (2003). *The COBIT Maturity Model in a Vendor Evaluation Case.* Obtenido de

file:///C:/Users/yese_/OneDrive/Escritorio/The_COBIT_Maturity_Model_in_a_Vendor_Eva%20(1).pdf

Espinoza, E. (2018). *La hipotesis en la investigacion* . Obtenido de http://scielo.sld.cu/pdf/men/v16n1/1815-7696-men-16-01-122.pdf

Sulca, G., & Becerra, E. (2017). *Control interno. Matriz de riesgo: Aplicación metodología COSO II.* Obtenido de file:///C:/Users/yese_/Downloads/686-Texto%20del%20art%C3%ADculo-2721-1-10-20170915.pdf

Tarazona, C. (2007). Amenazas informáticas y seguridad de la información. *Informática y Derecho Penal, 28*(84), 137 - 146.

Celi, E. (2014). La gestión de riesgos de TI y la efectividad de los sistemas de seguridad de la información: Caso procesos críticos en las pequeñas entidades financieras de Lambayeque, Perú. *3° Workshop de Tecnologías de Información.* Perú: 11° Congreso Internacional de Ingeniería de Software y Sistemas de Información Universidad Privada Antenor Orrego de Trujillo.

MINTIC. (2016). *Seguridad y privacidad de la información.* Colombia: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

García, J. (2011). Gobierno de TI a través de COBIT 4.1 y cambios esperados en COBIT 5.0. *ECORFAN, 2*(5), 109 - 131.

Escobar, M. (2020). *Investigaciones penales por corrupción en el sector salud están estancadas Para hacer uso de este contenido cite la fuente y haga un enlace a la nota original en Primicias.ec: https://www.primicias.ec/noticias/sociedad/investigaciones-penales-corrupcion-*. Recuperado el 2021, de Primicas: https://www.primicias.ec/noticias/sociedad/investigaciones-penales-corrupcion-sector-salud/

Código de gobierno corporativo del instituto ecuatoriano de seguridad social. (2012). Código de gobierno corporativo del instituto ecuatoriano de seguridad social. *NSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL*.

Código de ética del instituto ecuatoriano de seguridad social. (2012). NSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL.

Ministerio de Salud Pública. (2019). *Ministerio de Salud Pública*. Obtenido de Dirección Nacional de Tecnologías de la Información y Comunicaciones:

https://www.salud.gob.ec/direccion-nacional-de-tecnologias-de-la-informacion-y-comunicaciones/

La Contraloría General del Estado del Ecuador. (2009). INFORME DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES (DTIC).

Constitución de la republica del Ecuador. (2012). Constitución de la republica del Ecuador.

IESS. (2020). *Resolucion No. C. D. 612.* Quito: Instituto Ecuatoriano De Seguridad Social.

Sanchez, L. (2017). COSO ERM Y LA GESTIÓN DE RIESGOS. *QUIPUKAMAYOC Revista de la Facultad de Ciencias Contables, 23*(44), 43 - 50.

Martinez, A., Robaina, D., & Stuart, M. (2015). Una aproximación hacia la evaluación del nivel de madurez de la arquitectura empresarial. *Revista Cubana de Ingeniería*, *6*(3), 33 - 42.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2018). *DESARROLLO DE GOBIERNO ELECTRÓNICO EN LA ADMINISTRACIÓN PÚBLICA DE ECUADOR.* Recuperado el Abril de 2021, de Ministerio de Telecomunicaciones y de la Sociedad de la Información.: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/10/Desarrollo-de-Gobierno-Electr%C3%B3nico-en-la-Administraci%C3%B3n-P%C3%BAblica-de-Ecuador-1.pdf

Cedeño, R., & Morell, L. (2018). La gestión de riesgos en Ecuador: una aproximación evolutiva desde el control interno. *Cofín, 12*(2), 306 - 318. Obtenido de http://scielo.sld.cu/pdf/cofin/v12n2/cofin22218.pdf

Armijos, V., Enderica, O., Palomeque, E., & Berme, J. (2018). Los Sistemas de Información en el Sector Público en el Ecuador: Estudio de Caso la Autoridad Portuaria de Puerto Bolívar. *Revista Ciencia Unem, 11*(26), 25 - 37. Obtenido de https://www.redalyc.org/jatsRepo/5826/582661257003/582661257003.pdf

Contraloria General del Estado. (14 de diciembre de 2009). *Normas de Control Interno de la Contraloria General del Estado.* Recuperado el Abril de 2021, de https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

Ministerio de telecomunicaciones y de la sociedad de la información. (2026). *Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2016-2021.* Ministerio de telecomunicaciones y de la sociedad de la información. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/08/Plan-de-Telecomunicaciones-y-TI..pdf

Conejero, E. (2 de Enero de 2013). MIDIENDO EL RIESGO EN LAS ADMINISTRACIONES PÚBLICAS. *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*(9), 95 - 113. Obtenido de https://revistasocialesyjuridicas.files.wordpress.com/2013/04/09-tl-02.pdf

Mantilla, S. (Abril de 2015). *Estándares/Normas Internacionales de Aseguramiento de la Información Financiera (ISA/NIA).* Colombia: Ecoe ediciones. Obtenido de https://www.ecoeediciones.com/wp-content/uploads/2015/07/Est%C3%A1ndares-Normas-Internacionales-de-Aseguramiento-de-la-informaci%C3%B3n-financiera-ISA-NIA-1ra-Edici%C3%B3n.pdf

Avellaneda, A. (Noviembre de 2010). *Aseguramiento de la información con COBIT*. Recuperado el 2021, de Control Objectives for Information and related Technology: http://cobitsosw.blogspot.com/2010/11/aseguramiento-de-la-informacion-con.html

Mora, J., Joffre, L., Huilcapi, M., & Escobar, D. (2017). EL MODELO COBIT 5 PARA AUDITORÍA Y EL CONTROL DE LOS SISTEMAS DE INFORMACIÓN. *RRAAE*. Obtenido de http://rraae.org.ec/Record/PUCESA_2ebd828dc4cb245bc3c0e0e9cfdc7da1

Sanchez, L. (Octubre de 2015). COSO ERM Y LA GESTIÓN DE RIESGOS. *QUIPUKAMAYOCRevista de la Facultad de Ciencias Contables, 23*(44), 43 - 50. Obtenido de https://revistasinvestigacion.unmsm.edu.pe/index.php/quipu/article/view/11625/10435

Quiroz, S., & Macías, D. (2017). Seguridad en informática: consideraciones. *Revista dominio de las ciencias, 3*(5), 676 - 688. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

Rivera, J., Herrera, V., Naranjo, X., & Narváez, C. (2019). Gestión de Riesgos de TIC en hospitales públicos. *Revista Ibérica de Sistemas e Tecnologias de Información RISTI, 20*(5), 280 - 291. Obtenido de https://search.proquest.com/openview/2e45495973142cf41bb3814cfecea9bc/1?pq-origsite=gscholar&cbl=1006393

Arévalo, F., Cedillo, I., & Moscoso, S. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Revista Killkana Técnica, 1*(2), 31 - 42. Obtenido de https://pdfs.semanticscholar.org/2c12/90d64fd3d3f1a7bb9483754e1c4931dd7014.pdf

Tejena, M. (2018). Análisis de riesgos en seguridad de la información. *Polo del conocimiento, 3*(4), 230 - 244. Obtenido de https://polodelconocimiento.com/ojs/index.php/es/article/view/809/1026

Vargas, M., & Sabogal, M. (2017). Investigación crítico-propositiva, sistémico-transdisciplinar: pertinencia, diseño y modelado. *Red Científica Del Campo Unificado de la Educación*, 1 - 24. Obtenido de http://www.redcicue.com/attachments/article/80/SOBRE%20INVESTIG.%20Y%20MODELOS.pdf

Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social. (2019). *Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social.* Quito: Instituto Ecuatoriano de Seguridad Social. Obtenido de http://www.silec.com.ec/Webtools/LexisFinder/DocumentVisualizer/DocumentVisualizer.aspx?id=LABORAL-POLITICAS_QUE_REGULAN_USO_DE_TECNOLOGIAS_DE_LA_INFORMACION&query=tecnologia%20de%20la%20informaci%C3%B3n#I_DXDataRow0

Políticas Que Regulan Uso De Tecnologías De La Información Del IESS. (2020). *RESOLUCIÓN SUSTITUTIVA DE LAS POLÍTICAS QUE REGULAN LAS ACTIVIDADES RELACIONADAS CON EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.* Quito: Instituto Ecuatoriano de Seguridad Social. Obtenido de http://www.silec.com.ec/Webtools/LexisFinder/DocumentVisualizer/FullDocu

mentVisualizerPDF.aspx?id=LABORAL-POLITICAS_QUE_REGULAN_USO_DE_TECNOLOGIAS_DE_LA_INFORMACION

Dextre, J. (2016). Revista Lidera. *Aportes de Docentes y Profesionales*, 34 - 38. Obtenido de http://revistas.pucp.edu.pe/index.php/revistalidera/article/view/16896/17201

Contraloria General del Estado. (6 de Junio de 2003). *Manual de auditoria Gubernamental.* Obtenido de https://www.contraloria.gob.ec/WFDescarga.aspx?id=5&tipo=nor

Ministerio de Finanzas del Ecuador. (2017). METODOLOGÍA PARA LA GESTIÓN INTEGRAL DE RIESGOS. *Coordinación General de Planificación*, 1 - 26. Obtenido de https://www.finanzas.gob.ec/wp-content/uploads/downloads/2017/04/Metodolog%C3%ADa-para-la-Gesti%C3%B3n-de-Riesgos-30-03-17.pdf

Instituto Nacional de ciberseguridad. (2018). *Protección de la información.* España: Gobierno de España. Obtenido de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

Santacruz, J., Vega, C., Pinos, L., & Cárdenas, O. (2017). Sistema cobit en los procesos de auditorías de los sistemas informáticos. *JOURNAL OF SCIENCE AND RESEARCH: REVISTA CIENCIA E INVESTIGACIÓN, 2*(8), 65 - 68. Obtenido de https://revistas.utb.edu.ec/index.php/sr/article/view/342/264

Cestari, F., Cesar, A., & Dimmit, J. (2017). *Gerencia de Servicios de TI.* Bogota, Colombia: Red Nacional de Tecnología Avanzada - RENATA. Obtenido de https://cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI3.pdf

Oltra, R. (2016). *Itil (Information Technology Infrastructure Library).* Universitat Politècnica de València. Obtenido de https://riunet.upv.es/bitstream/handle/10251/68323/Oltra%20-%20ITIL%C2%AE%20(Information%20Technology%20Infrastructure%20Library)%20Qu%C3%A9%20es%20y%20Breve%20Historia.pdf?sequence=1

Mendoza, A. (Mayo de 2017). Importancia de la gestión administrativa para la innovación de las medianas empresa comerciales en la ciudad de Manta.

Dominio de las ciencias, 3(2), 947 - 964. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6325898

Brito, D. (Enero de 2018). El Riesgo Empresarial. *Universidad y Sociedad, 10*(1), 269 - 277. Obtenido de http://scielo.sld.cu/pdf/rus/v10n1/2218-3620-rus-10-01-269.pdf

Lizarzaburo, E., Barriga, G., Noriega, L., Lopez, L., & Mejía, P. (5 de septiembre de 2017). Gestión de Riesgos Empresariales:Marco de Revisión ISO 31000. *Revista espacios, 38*(59), 8. Obtenido de https://www.revistaespacios.com/a17v38n59/a17v38n59p08.pdf

Instituto de Auditores internos. (junio de 2017). *Gestión del Riesgo Empresarial Integrando Estrategia y Desempeño Gestión del riesgo empresarial integrando estratégia y desempeño.* Obtenido de COSO: https://auditoresinternos.es/uploads/media_items/coso-2018-esp.original.pdf

Galvazine. (Agosto de 2020). *Reporte y monitoreo del riesgo*. (ACL services) Recuperado el 2021, de High Bond: https://help.highbond.com/helpdocs/riskbond/es/Content/global_topics/get_started/solution_guides/enterprise_risk_management/reporting_and_monitoring_risk.htm

Dharma Consulting. (2013). *Monitorear y Controlar los riesgos*. Obtenido de Capacitacion virtual y soluciones de negocios: https://www.dharmacon.net/informacion-y-herramientas-gratuitas/gestion-de-proyectos/gpy_formatos/

Fernández, J. (2018). *El monitoreo de riesgos en Dirección de Proyectos*. Recuperado el 2021, de EALDE Business school: https://www.ealde.es/monitoreo-de-riesgos-direccion-de-proyectos/

Villanueva, E. (Diciembre de 2014). Metodología para monitorear riesgos estrategicos. *Revista de Investigaciones - Universidad del Quindío, 26*(1), 124 - 134.

ANDER-EGG, E. (2011). *APRENDER A INVESTIGAR.* Córdoba, Argentina: Editorial Brujas. Obtenido de https://abacoenred.com/wp-content/uploads/2017/05/Aprender-a-investigar-nociones-basicas-Ander-Egg-Ezequiel-2011.pdf.pdf

Hernandez, R., Collado, C., & Lucio, P. (2003). *Metodología de la investigación.* México: McGraw - Hill. Obtenido de http://metodos-comunicacion.sociales.uba.ar/wp-content/uploads/sites/219/2014/04/Hernandez-Sampieri-Cap-1.pdf

Arias, F. (2006). *El proyecto de investigación*. Recuperado el 2021, de Enfermería basada en la evidencia: https://ebevidencia.com/wp-content/uploads/2014/12/EL-PROYECTO-DE-INVESTIGACI%C3%93N-6ta-Ed.-FIDIAS-G.-ARIAS.pdf

Baena, G. (2014). *METODOLOGÍA DE LA INVESTIGACIÓN.* México D. F.: Grupo Editorial Patria. Obtenido de https://editorialpatria.com.mx/pdffiles/9786074384093.pdf

Tamayo, M. (1999). *APRENDER A INVESTIGAR* (Tercera edición ed.). Santa Fe de Bogotá, Colombia: ICFES. Obtenido de https://academia.utp.edu.co/grupobasicoclinicayaplicadas/files/2013/06/2.-La-Investigaci%c3%b3n-APRENDER-A-INVESTIGAR-ICFES.pdf

Hernández, R., Fernandez, C., & Pilar, B. (2014). *METODOLOGIA DE LA INVESTIGACIÓN.* México D. F.: McGraw - Hill. Obtenido de https://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf

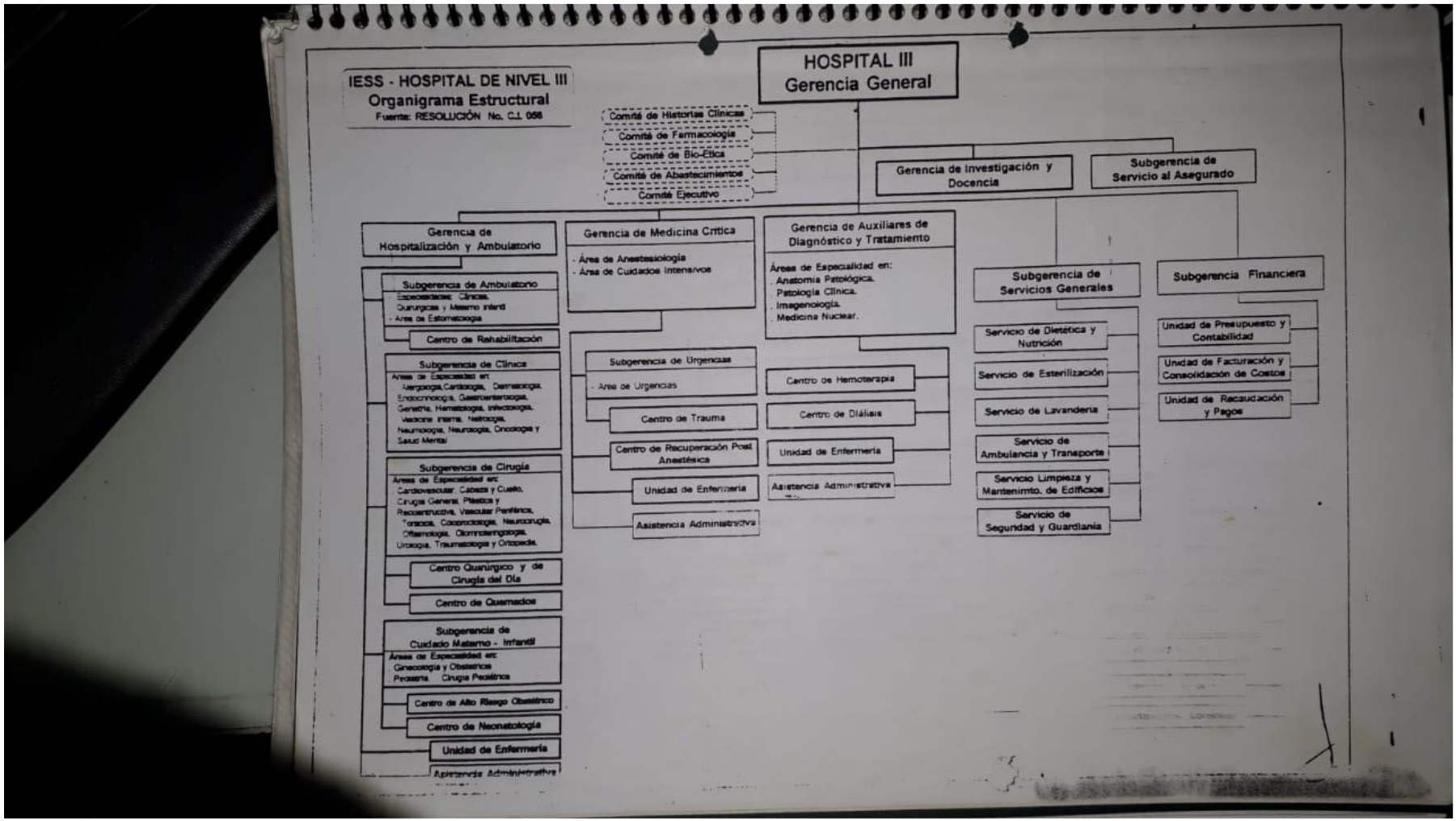
Arias, J., Villasís, M., & Miranda, M. (2016). El protocolo de investigación III: la población de estudio. *Revista Alergia México, 63*(2), 201 - 206. Obtenido de https://www.redalyc.org/pdf/4867/486755023011.pdf

Gonzáles, R., & Salazar, F. (2008). ASPECTOS BÁSICOS DEL ESTUDIO DE MUESTRA Y POBLACIÓN PARA LA ELABORACIÓN DE LOS PROYECTOS DE INVESTIGACIÓN. *Trabajo de Curso Especial de Grado presentado como requisito parcial Para optar al título de Licenciado en Administración* . UNIVERSIDAD DE ORIENTE NÚCLEO DE SUCRE . Obtenido de http://recursos.salonesvirtuales.com/assets/bloques/Raisirys-Gonz%C3%A1lez.pdf

Lopez, P. (2004). POBLACIÓN, MUESTRA Y MUESTREO. *Punto Cero*, 69 - 74. Obtenido de http://www.scielo.org.bo/pdf/rpc/v09n08/v09n08a12.pdf

Betancur, S. (2000). *Operacionalización de variables.* Recuperado el 2021, de http://fcaenlinea.unam.mx/anexos/1349/1349_u2_Act2.pdf

ANEXOS


IESS - HOSPITAL DE NIVEL III
Organigrama Estructural
Fuente: RESOLUCIÓN No. C.I. 056
HOSPITAL III
Gerencia General
Comité de Historias Clínicas
Comité de Farmacología
Comité de Bio-Ética
Comité de Abastecimientos
Comité Ejecutivo
Gerencia de Investigación y Docencia
Subgerencia de Servicio al Asegurado
Gerencia de Hospitalización y Ambulatorio
Subgerencia de Ambulatorio
Centro de Rehabilitación
Subgerencia de Clínica
Subgerencia de Cirugía
Centro Quirúrgico y de Cirugía del Día
Centro de Quemados
Subgerencia de Cuidado Materno - Infantil
Centro de Alto Riesgo Obstétrico
Centro de Neonatología
Unidad de Enfermería
Gerencia de Medicina Crítica
- Área de Anestesiología
- Área de Cuidados Intensivos
Subgerencia de Urgencias
- Área de Urgencias
Centro de Trauma
Centro de Recuperación Post Anestésica
Unidad de Enfermería
Asistencia Administrativa
Gerencia de Auxiliares de Diagnóstico y Tratamiento
Áreas de Especialidad en:
. Anatomía Patológica.
. Patología Clínica.
. Imagenología.
. Medicina Nuclear.
Centro de Hemoterapia
Centro de Diálisis
Unidad de Enfermería
Asistencia Administrativa
Subgerencia de Servicios Generales
Servicio de Dietética y Nutrición
Servicio de Esterilización
Servicio de Lavandería
Servicio de Ambulancia y Transporte
Servicio Limpieza y Mantenimto. de Edificios
Servicio de Seguridad y Guardianía
Subgerencia Financiera
Unidad de Presupuesto y Contabilidad
Unidad de Facturación y Consolidación de Costos
Unidad de Recaudación y Pagos