



**Evaluación técnica informática en base de riesgos de la Coordinación Zonal 1 –
Salud, utilizando el marco de referencia COBIT 2019**

Félix Bolaños, Amada Leonor

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Gerencia de Sistemas

Trabajo de titulación, previo a la obtención del título de Magíster en Gerencia de
Sistemas

MsC. Ron Egas, Mario Bernabé

11 de abril del 2023

Revisado
Ing. Mario B. Ron Egas MSc.



Document Information

Analyzed document	TESIS LEONOR FELIX ABR2023.pdf (D163628934)
Submitted	4/11/2023 2:13:00 PM
Submitted by	Ramiro Delgado
Submitter email	pg.doccenterdr@uniandes.edu.ec
Similarity	8%
Analysis address	pg.doccenterdr.unia@analysis.orkund.com

Sources included in the report

SA	TESIS_TANIA_ANDRADE para urkund.docx Document TESIS_TANIA_ANDRADE para urkund.docx (D50331341)		3
SA	ANDERSON SANTIAGO MORAN ARELLANO TESIS BIEN 06-10-2021.pdf Document ANDERSON SANTIAGO MORAN ARELLANO TESIS BIEN 06-10-2021.pdf (D114460306)		1
SA	PLAN DE INVESTIGACIÓN COMPLETO VFINAL - BAUTISTA ANGULO JENNIFFER VERÓNICA.docx Document PLAN DE INVESTIGACIÓN COMPLETO VFINAL - BAUTISTA ANGULO JENNIFFER VERÓNICA.docx (D68707485)		2
SA	Tesis Maestria Eduardo Tusa.pdf Document Tesis Maestria Eduardo Tusa.pdf (D111093271)		7
SA	TESIS EVALUACION TECNICA ESPE SD FINAL biblioteca.docx Document TESIS EVALUACION TECNICA ESPE SD FINAL biblioteca.docx (D14556982)		13
SA	TesisFinalESPE_LlumiquingaSelena_TipánLeticia.docx Document TesisFinalESPE_LlumiquingaSelena_TipánLeticia.docx (D62374150)		26
SA	ET BanCodesarrollo.pdf Document ET BanCodesarrollo.pdf (D14305904)		7
SA	TESIS JOHANNA VERA 17-07-2019.docx Document TESIS JOHANNA VERA 17-07-2019.docx (D54559499)		3
SA	tesisPálizabril2017.docx Document tesisPálizabril2017.docx (D27079925)		2

Entire Document

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA CENTRO DE ESTUDIOS DE POSGRADO CIENCIAS DE LA COMPUTACIÓN MAESTRÍA EN GERENCIA DE SISTEMAS
TESIS DE GRADO DE MAESTRÍA



Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Certificación

Certifico que el trabajo de titulación, **“Evaluación técnica informática en base de riesgos de la Coordinación Zonal 1 – Salud, utilizando el marco de referencia COBIT 2019”** fue realizado por la señorita **Félix Bolaños Amada Leonor**, mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 13 de abril del 2021

Firma



.....

MsC. Mario Bernabé Ron Egas

C.C.: 1704229747

Director del Proyecto



Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Responsabilidad de Auditoría

Yo, **Félix Bolaños, Amada Leonor** con cédula de ciudadanía N° 0401710371 declaro que el contenido, ideas y criterios del trabajo de titulación: **“Evaluación técnica informática en base de riesgos de la Coordinación Zonal 1 – Salud, utilizando el marco de referencia COBIT 2019”**, es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 11 de abril del 2023

Firma

.....
Ing. Félix Bolaños Amada Leonor

C.C.: 0401710371



Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Autorización de Publicación

Yo, **Félix Bolaños, Amada Leonor** con cédula de ciudadanía N° 0401710371, autorizo a la Universidad de Fuerzas Armadas ESPE publicar el trabajo de titulación: **“Evaluación técnica informática en base de riesgos de la Coordinación Zonal 1 – Salud, utilizando el marco de referencia COBIT 2019”**, en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 11 de abril del 2023

Firma

Ing. Félix Bolaños Amada Leonor

C.C.: 0401710371

Dedicatoria

Dedico este proyecto a mis padres que son mi ejemplo y mi principal inspiración, a ellos que trabajan día a día inalcanzablemente por nuestra familia, a ellos que desde pequeña han inculcado en mi los valores y virtudes que me han permitido concluir esta etapa de vida.

Félix Bolaños Amada Leonor

Agradecimiento

A mis padres, Augusto Félix y Angelita Bolaños, por todo el apoyo brindado en mi etapa de maestrante y ser mi ejemplo en cada una de mis metas.

A la Coordinación Zonal 1 – Salud y sobre todo a la Dirección Zonal de Tecnologías de la Información, en donde, gracias a su apoyo pude realizar el trabajo presente.

A mi director de Tesis Mayor. Mario Ron, quien con su asesoramiento contribuyó para culminar con éxito este trabajo de titulación.

A los docentes de la maestría de Gerencia de Sistemas XVIII, quienes a lo largo de estos dos años supieron transmitir sus experiencias y conocimientos.

Agradezco a Dios por haberme dado la salud y vida, así como la sabiduría, paciencia, y sobre todo la constancia de trabajo y esfuerzo que he puesto a diario para alcanzar mis objetivos.

Félix Bolaños Amada Leonor

Índice de Contenidos

Dedicatoria	6
Agradecimiento	7
Resumen.....	14
Abstract	15
Capítulo 1: Introducción.....	16
Antecedentes.....	16
Planteamiento del Problema	17
Objetivos del Proyecto	18
<i>Objetivo General</i>	18
<i>Objetivos Específicos</i>	18
Justificación e Importancia.....	19
Alcance del Proyecto	20
Hipótesis de la Investigación.....	20
Capítulo 2: Fundamentación Teórica.....	21
Base Conceptual.....	21
<i>Tecnologías de la Información</i>	21
<i>Gestión Tecnológica</i>	21
<i>Riesgos Informáticos</i>	21
<i>Seguridad Informática</i>	21
<i>Auditoría</i>	22
<i>Auditoría Informática</i>	22
<i>Auditoría Basada en Riesgos</i>	22

<i>Funciones de Auditoría Basada en Riesgos</i>	23
COBIT 2019.....	24
<i>Principios de COBIT 2019</i>	25
<i>Descripción General de COBIT 2019</i>	26
<i>Los objetivos de Gobernanza y Gestión en COBIT 2019</i>	27
<i>Cascada de Metas COBIT 2019</i>	28
Normas de Control Interno	29
Definición de la Organización.....	30
<i>Coordinación Zonal 1 - Salud</i>	30
<i>Dirección Zonal de Tecnologías de la Información y Comunicación</i>	31
<i>Infraestructura de la Organización</i>	34
<i>Servicios Brindados</i>	38
Capítulo 3: Evaluación Técnica Informática en Base De Riesgos.....	41
Método de Investigación	41
Metodología.....	41
Categoría de la Investigación.....	41
Pasos de la Investigación	42
Técnicas de Investigación.....	42
Estrategias de Investigación	43
Objetivos de la Evaluación.....	43
<i>Objetivo General</i>	43
<i>Objetivos Específicos</i>	44
Ejecución de la Evaluación	44

	10
Selección de los Procesos Críticos a Evaluar	47
Plan de Investigación.....	63
Investigación de Campo.....	71
Investigación Documental	72
Evaluación de los Procesos Críticos Utilizando COBIT 2019	74
Hallazgos	80
Matriz de Riesgos	81
Capítulo 4: Informe De La Auditoría	86
Informe Ejecutivo	86
<i>Introducción</i>	86
Declaración de Propósito de Alto Nivel	87
Área de TI Auditada.....	88
<i>Resumen Ejecutivo</i>	88
<i>Objetivos de la Evaluación Técnica Informática</i>	91
<i>Metodología de la Evaluación Técnica Informática</i>	92
Planificación de la Evaluación Técnica Informática	92
Ejecución de la Evaluación Técnica Informática	93
<i>Resultados o Hallazgos de la Evaluación Técnica Informática</i>	93
Evaluar, Dirigir y Monitorear EDM.....	93
Alinear, Planificar y Organizar APO	95
Construir, Adquirir e Implementar BAI.....	112
Entregar, Dar Servicio y Soporte DSS	118
<i>Conclusiones de la Evaluación Técnica Informática</i>	119
<i>Apéndices</i>	123

Copia Completa de la Respuesta del Auditado	123
Capítulo 5: Conclusiones y Recomendaciones.....	124
Conclusiones	124
Recomendaciones	125
Bibliografía	127
Apéndices	130

Índice de tablas

Tabla 1 <i>Equipamiento activo de red</i>	34
Tabla 2 Servidores de la Dirección Zonal de Tecnologías de la Información.	35
Tabla 3 <i>Objetivos estratégicos y estrategias MSP</i>	49
Tabla 4 <i>Ponderaciones para la valoración en cascada de metas</i>	55
Tabla 5 <i>Metas corporativas de COBIT</i>	55
Tabla 6 <i>Metas corporativas de TI COBIT 2019</i>	57
Tabla 7 <i>Resultados evaluación procesos de COBIT</i>	60
Tabla 8 <i>Procesos Críticos - seleccionado para Evaluación Técnica Informática</i>	62
Tabla 9 <i>Plan de Investigación</i>	63
Tabla 10 Instrumentos de campo	71
Tabla 11 <i>Evaluación proceso EDM04</i>	76
Tabla 12 <i>Hallazgos de la ETI</i>	80
Tabla 13 <i>Probabilidad de ocurrencia</i>	81
Tabla 14 <i>Nivel de Impacto</i>	81
Tabla 15 <i>Nivel de riegos de hallazgos encontrados en la ETI</i>	82
Tabla 16 <i>Porcentaje de niveles de riesgo de los hallazgos</i>	84

Índice de figuras

Figura 1	<i>Principios de COBIT 2019</i>	25
Figura 2	<i>Visión general COBIT 2019</i>	26
Figura 3	<i>Modelo Core de COBIT 2019</i>	28
Figura 4	<i>Cascada de Metas</i>	29
Figura 5	<i>Estructura Orgánica de las Coordinaciones Zonales de Salud</i>	30
Figura 6	<i>Estructura Orgánica de la Dirección Zonal de Tecnologías de la Información</i>	33
Figura 7	<i>Topología de red</i>	37
Figura 8	<i>Topología física de rack de cada piso</i>	37
Figura 9	<i>Topología física datacenter</i>	38
Figura 10	<i>Pasos de la investigación cualitativa</i>	42
Figura 11	<i>Cascada para selección de procesos a evaluar</i>	48
Figura 12	<i>Mapeo 1 Estrategias MSP - Metas empresariales de COBIT 2019</i>	54
Figura 13	<i>Mapeo 2 Metas Corporativas de COBIT - Metas de TI COBIT 2019</i>	57
Figura 14	<i>Mapeo 3 Metas Corporativas de TI COBIT – Procesos de COBIT 2019</i>	59
Figura 15	<i>Cascada para selección de procesos a evaluar</i>	82
Figura 16	<i>Porcentajes de niveles de riesgo de hallazgos de ETI</i>	84

Resumen

El Ministerio de Salud Pública es el ente rector del Sistema Nacional de Salud, está conformado por nueve Coordinaciones Zonal distribuidas en todo el país. La Coordinación Zonal 1 corresponde a las provincias de Esmeraldas, Carchi, Imbabura y Sucumbíos, la sede zonal es una entidad administrativa que coordina, controla y planifica en la zona las acciones referentes a la salud pública.

La Coordinación Zonal 1 – Salud a través de la Dirección Zonal de Tecnologías de la Información y Comunicación DZTIC, aplica políticas, normas y procedimientos que efectivicen la gestión y administración de las tecnologías de la información y comunicaciones orientadas a la optimización de recursos, sistematización y automatización de los procesos del nivel zonal, para ello la DZTIC brinda varios servicios a los funcionarios de la sede zonal y funcionarios de las entidades operativas desconcentradas llamadas EODs.

A través de la presente investigación se realiza una evaluación técnica informática en base de riesgos de la Coordinación Zonal 1 – Salud, utilizando el Marco de Referencia COBIT 2019, que permita conocer la situación actual de las tecnologías de la información en la institución y emitir recomendaciones acertadas y oportunas, las mismas que posteriormente deberán ser implementadas para el beneficio la institución, que permita el cumplimiento de las normas vigentes para la Dirección Zonal de Tecnologías de la Información y Comunicación, como es las Normas de Control Interno de la Contraloría General del Estado y finalmente se evidencie en mejoras en los servicios brindados a través de las tecnologías de la información.

Palabras clave: evaluación técnica informática, COBIT 2019, riesgos, gobierno de TI.

Abstract

The Ministry of Public Health is the governing body of the National Health System, it is made up of nine Zonal Coordinations distributed throughout the country. Zonal 1 corresponds to the provinces of Esmeraldas, Carchi, Imbabura and Sucumbíos, is an administrative entity that coordinates, controls and plans actions related to public health in the area.

The Zonal Coordination 1 - Health through the Zonal Directorate of Information and Communication Technologies DZTIC, applies policies, standards and procedures that make the management and administration of information and communications technologies effective, aimed at optimizing resources, systematization and automation of the zonal level processes, for this the DZTIC provides various services to the officials of the zonal headquarters and officials of the decentralized operating entities called EODs.

Through this research, a risk-based computer technical evaluation of Zonal Coordination 1 - Health is carried out, using the COBIT 2019 Reference Framework, which allows knowing the current situation of information technologies in the institution and issuing recommendations correct and timely, which must later be implemented for the benefit of the institution, which allows compliance with the current regulations for the Zonal Directorate of Information and Communication Technologies, such as the Internal Control Standards of the State Comptroller General's Office and finally it is evidenced in improvements in the services provided through information technologies.

Key Word: IT technical assessment, COBIT 2019, risks, IT governance.

Capítulo 1: Introducción

Antecedentes

El Ministerio de Salud Pública fue creado el 16 de junio de 1967, cuya misión es *“Ejercer la rectoría, regulación, planificación, coordinación, control y gestión de la Salud Pública ecuatoriana a través de la gobernanza y vigilancia y control sanitario y garantizar el derecho a la Salud a través de la provisión de servicios de atención individual, prevención de enfermedades, promoción de la salud e igualdad, la gobernanza de salud, investigación y desarrollo de la ciencia y tecnología; articulación de los actores del sistema, con el fin de garantizar el derecho a la Salud”* (Pública, 2012).

La Coordinación Zonal 1 – Salud fue creada en el año 2012, cuya misión es “Coordinar, controlar y planificar en la zona las acciones referentes a vigilancia de la Salud pública, de la vigilancia y control sanitario, la provisión de servicios de atención individual, prevención de enfermedades, promoción de la salud e igualdad, la gobernanza de salud, y participación social, modelo de atención y, redes pública y complementaria de salud (de Gestión Organizacional).

La Dirección Zonal de Tecnologías de la Información y Comunicaciones DZTIC en base a lo establecido en el Estatuto Orgánico Sustitutivo de Gestión Organizacional por Procesos del Ministerio de Salud Pública, art.34 Tecnologías de la Información y Comunicaciones busca *“aplicar las políticas, normas y procedimientos que efectivicen la gestión y administración de las tecnologías de la información y comunicaciones orientadas a la optimización de recursos, sistematización y automatización de los procesos del nivel zonal”* (de Gestión Organizacional).

La Dirección Zonal de Tecnologías de la Información y Comunicación, brinda varios servicios como: Internet, telefonía IP, mesa de Ayuda OTRS, nube nextcloud, correo institucional zimbra, página web institucional, plataforma de capacitaciones Moodle, entre otros,

con el objetivo operativo de brindar a la institución integridad de la información, optimización de recursos y soporte tecnológico institucional.

Planteamiento del Problema

Las tecnologías de la información con el transcurso del tiempo han tenido una introducción acelerada en la sociedad, teniendo actualmente influencia directa en la industria, educación, turismo, salud, en fin, en todas las áreas, convirtiéndose en parte esencial en todas las organizaciones públicas o privadas. De la mano de ese crecimiento de las tecnologías de la información, han surgido a nivel mundial sin número de ataques que ponen en riesgo las tecnologías de la información.

En Ecuador, las tecnologías de la información no tienen un alto porcentaje de penetración en comparación a otros países más desarrollados, el plan nacional de tecnologías de la información y las comunicaciones vigente tiene entre uno de sus objetivos aumentar la penetración de servicios TIC en la población, no se considera aún como objetivo el tema de la seguridad en las tecnologías de la información. En lo que respecta al sistema de salud pública existen mejoras a nivel tecnológico respecto a décadas pasadas, en donde, por ejemplo, los registros de la atención en salud eran únicamente de forma manual, mediante papeles, historias clínicas en archivadores, sin embargo, no existe homologación respecto a las tecnologías de la información a nivel nacional, ya que cada zona actúa o realiza su gestión a nivel desconcentrado.

La sede de la Coordinación Zona 1 – Salud, cuenta con un Centro de Datos que aloja varios servicios que son brindados a los funcionarios de la sede zonal y funcionarios de las entidades operativas desconcentradas llamadas EODs. La infraestructura tecnológica existente tiene más de 10 años de vida útil, año tras año la asignación presupuestaría para la gestión en la Dirección Zonal de TIC es mínima, entre otras condiciones, no han permitido un avance

significativo de las tecnologías de la información en la institución, por lo tanto, los servicios brindados están expuestos continuamente a diferentes riesgos que pueden ocasionar hasta la paralización del servicio, al no tener una evaluación técnica informática oficial sobre dichos riesgos se dificulta evidenciar dichos inconvenientes a la gerencia general, en este caso a el Coordinador Zonal.

Objetivos del Proyecto

Objetivo General

Realizar una evaluación técnica informática en base de riesgos a la Dirección Zonal de Tecnologías de la Información y Comunicación de la Coordinación Zonal 1 – Salud utilizando el marco de referencia COBIT 2019, para determinar las medidas de control necesarias a nivel de TI que permitan mejorar los servicios brindados por la dirección y el cumplimiento de normas que permitan posteriormente la obtención de certificaciones.

Objetivos Específicos

- Detallar los fundamentos teóricos sobre el marco de referencia COBIT 2019 e información relacionada, para la aplicación de estos en la evaluación técnica informática.
- Realizar una evaluación técnica informática para recopilar información que evidencie la situación actual de la unidad de tecnologías de la información, que permita identificar los riesgos tecnológicos usando los procesos de TI del marco de referencia COBIT 2019.
- Elaborar un informe con los resultados de la evaluación técnica y las recomendaciones respectivas que ayuden a mitigar los riesgos detectados y permitan mejorar los servicios brindados por la dirección.

Justificación e Importancia

El Ministerio de Salud Pública dentro de sus actividades tiene como objetivo principal ejercer plenamente la gobernanza del sistema nacional de salud, con un modelo que priorice la promoción de la salud y la prevención de enfermedades, garantizando la salud integral y el acceso universal a la red de servicios. La salud es un derecho de todos los ciudadanos garantizado en la constitución de la república del Ecuador, en este contexto, las tecnológicas de la información están enfocadas a la optimización de recursos, sistematización y automatización de los procesos del nivel zonal que permitan evidenciar una mejor atención a la ciudadanía.

A nivel mundial los cambios tecnológicos avanzan a pasos agigantados, pero de la mano de dichos avances surgen ciertos riesgos que podrían poner en peligro el correcto funcionamiento de las infraestructuras de TI y por ende a las organizaciones. Cada día se involucra más a las tecnologías de la información en el desarrollo del negocio, por ello se evidencia la demanda de auditorías, evaluaciones técnicas informáticas.

Es necesario contar con una evaluación técnica informática que permita conocer la situación actual de las tecnologías de la información, conocer los riesgos y las posibilidades para afrontar dichos riesgos, además de garantizar el adecuado funcionamiento de TI y posteriormente se pueda realizar una auditoría de certificación. En muchas ocasiones la necesidad de una evaluación técnica informática surge para cumplir con parámetros de evaluación, certificación, acreditación, entre otros. Al ser la Coordinación Zonal 1 – Salud una entidad pública, contar con una evaluación técnica informática permitiría el cumplimiento de la normativa vigente como es Estatuto Orgánico Sustitutivo de Gestión Organizacional por Procesos del Ministerio de Salud Pública, Normas de Control Interno de la Contraloría General del Estado.

Al ser la Dirección Zonal de TIC una unidad de apoyo, su razón de ser es contribuir a alcanzar los objetivos estratégicos institucionales, para ello existen varios marcos de referencia y estándares internacionales que brindan buenas prácticas que permiten alinear los objetivos de TI con los de la organización, COBIT 2019 ofrece un marco integral con varios objetivos de control que orientan y ofrecen un modelo de referencia aplicable para la gestión de TI, es decir ayuda a las empresas a crear valor mediante un balance entre la obtención de beneficios y la optimización de los niveles del riesgo y el uso de recursos, además permite administrar de forma integral cubriendo todo el negocio de extremo a extremo teniendo en cuenta a los grupos de interés.

Alcance del Proyecto

La evaluación técnica se realizará en base al marco referencia COBIT 2019, aplicando un modelo en cascada para determinar los procesos críticos a ser evaluados, de estos procesos se escogerán las actividades más importantes, las que serán evaluadas en la presente evaluación técnica.

El proyecto concluye con la elaboración de un informe con los resultados de la evaluación técnica y las recomendaciones respectivas que ayuden a mitigar los riesgos detectados y permitan mejorar los servicios brindados por la dirección.

Hipótesis de la Investigación

Conocer información que refleje de forma oficial la situación actual de las tecnologías de la información en la Coordinación Zonal 1 – Salud en base el marco de referencia COBIT 2019 y emitir recomendaciones acertadas y oportunas a nivel de TI para el beneficio de la institución.

Capítulo 2: Fundamentación Teórica

Base Conceptual

Tecnologías de la Información

Las TIC se definen colectivamente como innovaciones en microelectrónica, computación (hardware y software), telecomunicaciones y optoelectrónico – microprocesadores, semiconductores, fibra óptica – que permiten el procesamiento y acumulación de enormes cantidades de información, además de una rápida distribución de la información a través de redes de comunicación (Romaní, 2009).

Gestión Tecnológica

Según Zorrilla (1997), la gestión tecnológica es la actividad organizacional mediante la cual se define e implanta la tecnología necesaria para lograr los objetivos y metas del negocio en términos de calidad, efectividad, adición de valor y competitividad.

Riesgos Informáticos

El riesgo es la probabilidad de que una amenaza determinada se materialice explotando las vulnerabilidades de un activo o grupo de activos y por lo tanto causar daño o pérdidas a la organización (Arévalo, Cedillo, & Moscoso, 2017).

Seguridad Informática

La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información (Fernández & Alonso, 2013).

Auditoría

Según Piattini and Peso (2000) la palabra auditoría viene de latin auditorius, y de ésta proviene la palabra auditor la misma que significa que tiene la virtud de oír. El auditor tiene la virtud de oír y revisar, pero debe estar encaminado a un objetivo específico que es evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de recursos alternativos de acción, se tome decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la actuación.

La auditoría es fundamental para garantizar que las organizaciones gestionan el negocio bajo un ambiente de control, los auditores han tenido que transformar la tradicional forma de hacer auditoría y esto representa retos y oportunidades.

Auditoría Informática

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos (Velthuis, 2008).

Auditoría Basada en Riesgos

Según Solano (2019) la auditoría basados en riesgos presenta algunas características que se detallan a continuación:

- Priorización de los riesgos relevantes.
- Enfocado en procesos
- Se especializa en el negocio
- Es integral
- Genera valor

Según Hernandez (2018) la auditoría basada en riesgos, ayuda a una organización a lograr sus objetivos al brindar un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de gestión de riesgos, control y gobierno, agrega valor a una organización de diferentes maneras:

- Enfoque centrado en el negocio que ayuda a la organización a lograr sus objetivos.
- Enfoque de auditoría inclusivo que facilita la gestión de la gerencia.
- Nivel óptimo de aseguramiento que respalda el logro de los objetivos del negocio.
- Mejor priorización de hallazgos y recomendaciones.
- Mejora de la mitigación de riesgos.
- Uso más efectivo de los recursos de auditoría.

Funciones de Auditoría Basada en Riesgos

Para Choy (2014), las funciones de auditoría basada en riesgos son:

- Incorporar al universo de los asuntos de auditoría la visión de riesgo que tiene la organización.
- Desarrollar procesos de auditoría basada en riesgos e incorporarlos en los planes anuales de la auditoría.
- Darle seguimiento al plan estratégico y ajustar el plan de la auditoría ante cambios en el primero.
- Utilizar técnicas y procedimientos de riesgo cuando se realiza la auditoría.
- Informar a los administradores y responsables de la organización los resultados de las auditorías con un lenguaje de riesgos y no de control interno.
- Identificar de manera conjunta los riesgos que pudieran afectar adversamente la continuidad de la organización para alcanzar sus objetivos.
- Ayudar a evaluar el Impacto que pudieran tener estos riesgos dentro de la organización.

- Sugerir el tratamiento y/o las acciones que deberán establecerse para disminuir la probabilidad de exposición a estos riesgos.
- Evaluar la suficiencia y efectividad de los controles internos actuales.
- Obtener planes de acción de los responsables para corregir las fallas de control identificadas.
- Dar a conocer los resultados a la Dirección General y a su Comité de Auditoría, mediante reporte de auditoría redactado adecuadamente, basado en los hallazgos de auditoría para una oportuna y adecuada toma de decisiones.

COBIT 2019

COBIT es un marco para el gobierno y la gestión de las tecnologías de la información de la empresa, dirigido a toda la empresa. La I&T empresarial significa toda la tecnología y procesamiento de la información que la empresa utiliza para lograr sus objetivos, independientemente de dónde ocurra dentro de la empresa. En otras palabras, la I&T empresarial no se limita al departamento de TI de una organización, aunque este está indudablemente incluido (ISACA, 2019).

El marco de referencia COBIT hace una distinción clara entre gobierno y gestión. Estas dos disciplinas abarcan distintos tipos de actividades, requieren distintas estructuras organizativas y sirven diferentes propósitos.

El gobierno asegura que:

- Las necesidades, condiciones y opciones de las partes interesadas se evalúan para determinar objetivos empresariales equilibrados y acordados.
- La dirección se establece a través de la priorización y la toma de decisiones.
- El desempeño y el cumplimiento se monitorean en relación con la dirección y los objetivos acordados.

En la mayoría de las empresas, el gobierno en general es responsabilidad del consejo de dirección bajo el liderazgo del presidente. Responsabilidades específicas de gobierno se pueden delegar a estructuras organizativas especiales a un nivel adecuado, en particular, en empresas más grandes y complejas.

La gerencia:

- Planifica, construye, ejecuta y monitorea actividades en línea con la dirección establecida por el órgano de gobierno para alcanzar los objetivos de la empresa.

COBIT 2019 se desarrolló en base a dos conjuntos de principios:

- Principios que describen los requisitos centrales de un sistema de gobernanza para la información y la tecnología empresarial.
- Principios para un marco de gobernanza que se puede utilizar para construir un sistema de gobernanza para la empresa.

Principios de COBIT 2019

- 1.- Proporcionar valor a las partes interesadas.
- 2.- Enfoque holístico.
- 3.- Sistema de gobierno dinámico.
- 4.- Separar el gobierno de la gestión.
- 5.- Adaptar a las necesidades de la empresa.
- 6.- Sistema de gobierno íntegro.

Figura 1

Principios de COBIT 2019

Los objetivos de Gobernanza y Gestión en COBIT 2019

Los objetivos de gobernanza y gestión en COBIT se agrupan en cinco dominios. Los dominios tienen nombres con verbos que expresan el propósito clave y las áreas de actividad del objetivo contenido en ellos:

Los objetivos de gobernanza se agrupan en el dominio evaluar, dirigir y supervisar (EDM). En este dominio, el cuerpo directivo evalúa las opciones estratégicas, dirige a la alta gerencia sobre las opciones estratégicas elegidas y monitorea el logro de la estrategia.

Los objetivos de gestión se agrupan en cuatro dominios:

1.- Alinear, planificar y organizar (APO) aborda la organización general, la estrategia y las actividades de apoyo para I&T.

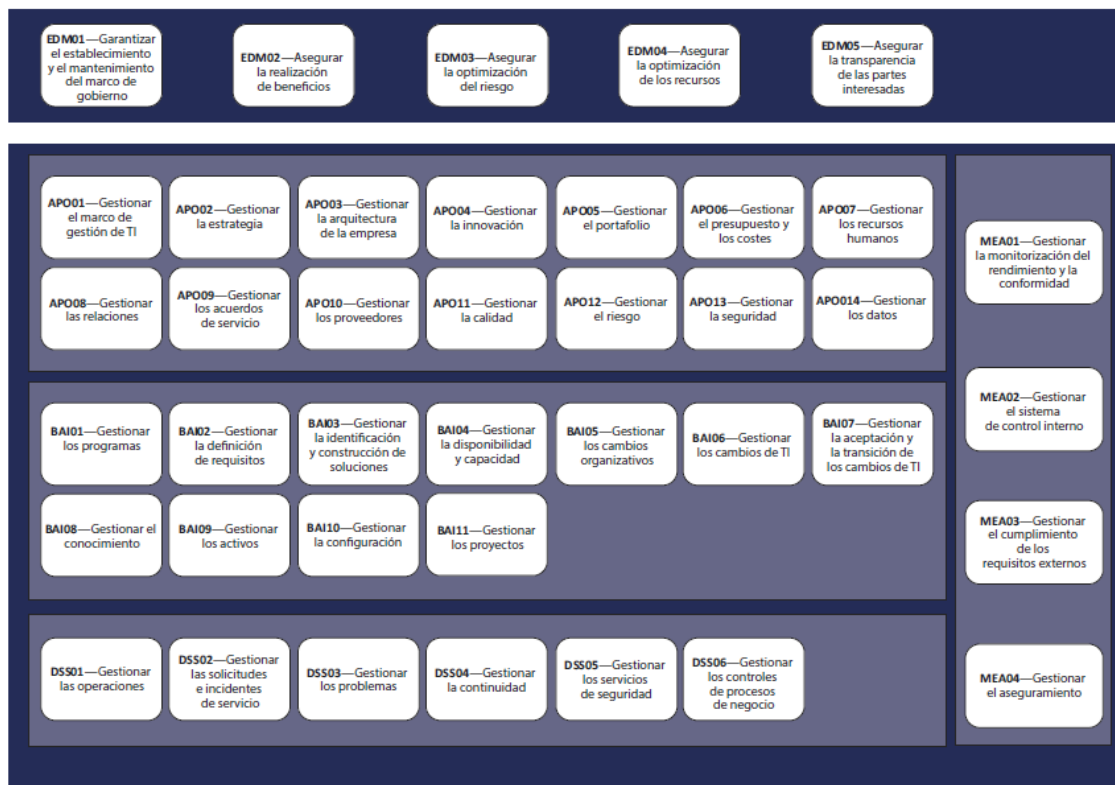
2.- Construir, adquirir e implementar (BAI) trata la definición, adquisición e implementación de soluciones de I&T y su integración en los procesos comerciales.

3.- Entregar, servicio y soporte (DSS) aborda la entrega operativa y el soporte de los servicios de I&T, incluida la seguridad.

4.- Monitorear, evaluar y evaluar (MEA) aborda el monitoreo del desempeño y la conformidad de I&T con los objetivos internos de desempeño, los objetivos de control interno y los requisitos externos.

Figura 3

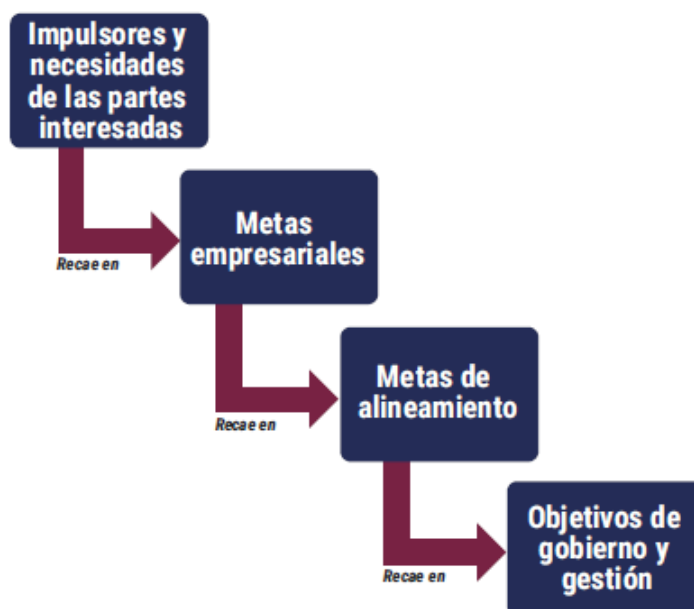
Modelo Core de COBIT 2019



Nota. Tomado de COBIT 2019 Framework Introducción y Metodología ISACA, (2019).

Cascada de Metas COBIT 2019

Las necesidades de las partes interesadas tienen que transformarse en una estrategia factible para la empresa. La cascada de metas soporta las metas empresariales, que es uno de los factores de diseño clave para un sistema de gobierno. Apoya la priorización de los objetivos de la dirección basada en la priorización de las metas empresariales.

Figura 4*Cascada de Metas*

Nota. Cascada de Metas COBIT 2019 ISACA, (2019).

La cascada de metas soporta además la conversión de las metas empresariales en prioridades para metas de alineamiento.

Normas de Control Interno

La Contraloría General del Estado es el organismo encargado del control de las instituciones públicas en el país, la cual en base a sus competencias emite las directrices y lineamientos que controla y regula estas instituciones, una de ellas es las NORMAS DE CONTROL INTERNO DE LA CONTRALORIA GENERAL DEL ESTADO, las mismas que son de cumplimiento obligatorio y en cuyo numeral 410 Tecnología de la Información establece las directrices que cada entidad debe cumplir respecto a las Tecnologías de la Información TI (Del Estado, DE, QUE, & PUBLICOS, 2009).

Definición de la Organización

Coordinación Zonal 1 - Salud

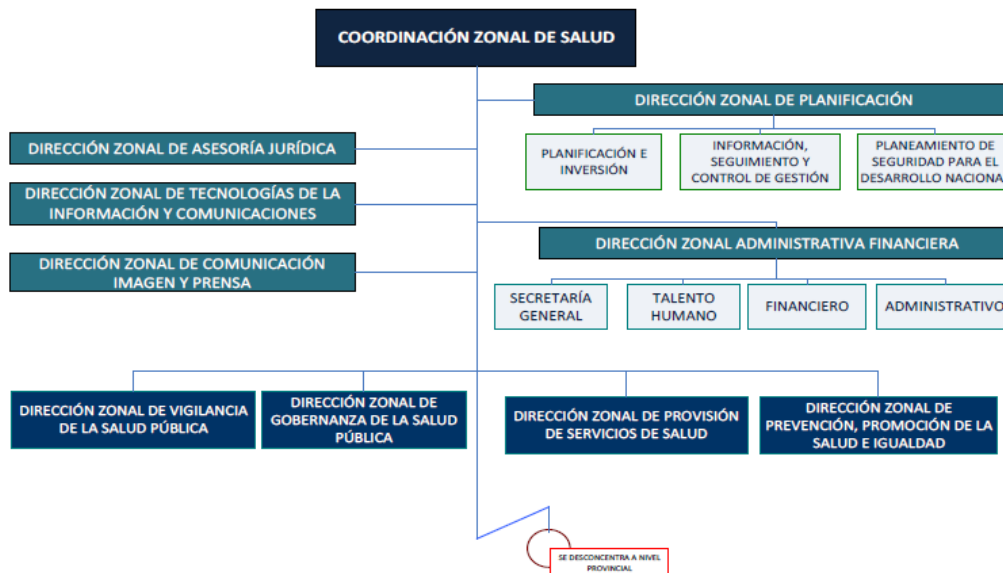
Tiene como función coordinar, controlar y planificar en la zona las acciones referentes a vigilancia de la Salud pública, de la vigilancia y control sanitario, la provisión de servicios de atención individual, prevención de enfermedades, promoción de la salud e igualdad, la gobernanza de salud, y participación social, modelo de atención y, redes pública y complementaria de salud.

Es parte del Ministerio de Salud Pública quien ejerce la gobernanza del Sistema Nacional de Salud, con un modelo referencial en latinoamérica que priorice la promoción de la salud y la prevención de enfermedades, con altos niveles de atención de calidad, con calidez, garantizando la salud integral de la población y el acceso universal a una red de servicios, con la participación coordinada de organizaciones públicas, privadas y de la comunidad (Espinosa, Acuña, De la Torre, & Tambini, 2017).

La estructura Orgánica de las Coordinaciones Zonales se presenta a continuación:

Figura 5

Estructura Orgánica de las Coordinaciones Zonales de Salud



Nota: Información extraída de la página oficial de la institución <http://www.saludzona1.gob.ec/>

Dirección Zonal de Tecnologías de la Información y Comunicación

La dirección aplica las políticas, normas y procedimientos que efectivicen la gestión y administración de las tecnologías de la información y comunicaciones orientadas a la optimización de recursos, sistematización y automatización de los procesos del nivel zonal.

Tiene como atribuciones y responsabilidades:

- a) Aplicar políticas y estándares para la sistematización de los procesos administrativos;
- b) Coordinar el crecimiento de redes y comunicaciones del nivel zonal y de unidades desconcentradas;
- c) Aplicar las políticas buenas prácticas de acceso y utilización de los recursos y servicios tecnológicos definidas en el nivel central;
- d) Aplicar y controlar los sistemas de información sobre la base de requerimientos del nivel zonal;
- e) Proporcionar soporte de mesa de ayuda en tecnología informática a nivel zonal;
- f) Proporcionar soporte en el seguimiento al cumplimiento de los procesos establecidos;

- g) Participar de ser requerido y de acuerdo al ámbito de su competencia en la sala situacional de la zona;
- h) Ejercer las funciones, representaciones y delegaciones que le asigne el/la Coordinador/a Zonal y otras asignadas desde la Coordinación General de Gestión Estratégica.

Sus productos son:

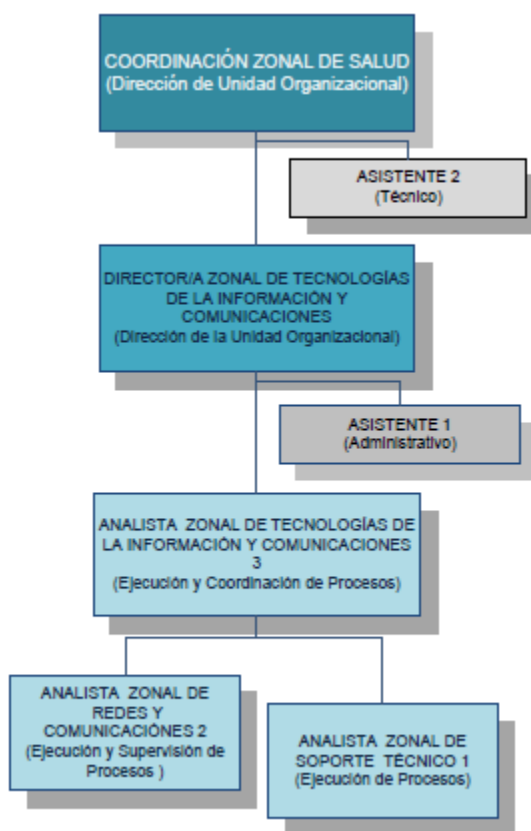
- a) Informes de aplicación de las especificaciones técnicas de los recursos tecnológicos a nivel zonal;
- b) Informe de implementación y control de gestión tecnológica a nivel zonal;
- c) Informes de aplicación de sistemas de información;
- d) Plan de crecimiento de redes y comunicaciones de la zona y sus niveles desconcentrados;
- e) Plan de implementación de buenas prácticas de acceso y utilización de los recursos y servicios tecnológicos en conformidad a la normativa vigente;
- f) Informes de desarrollo y funcionamiento de la infraestructura tecnológica de la zona;
- g) Informe de las vulnerabilidades existentes y brechas en los sistemas de comunicación de red de la institución a nivel zonal;
- h) Informes del avance y desempeño de los proyectos tecnológicos que están siendo implementados y de los proyectos a ejecutarse a nivel zonal y distrital;
- i) Informe de ejecución del soporte técnico brindado al usuario;
- j) Informe del inventario periódico de equipos a nivel zonal;
- k) Informe de entrega de equipamiento tecnológico a nivel zonal y distrital;
- l) Informe de ejecución del mantenimiento preventivo y correctivo de los equipos informáticos de hardware a nivel zonal;

- m) Informes de ejecución de planes de capacitaciones a usuarios sobre la utilización y manejo de aplicaciones a implementarse;
- n) Resguardo y soporte del mapa de procesos a nivel zonal y distrital.

La estructura orgánica de la dirección se presenta a continuación:

Figura 6

Estructura Orgánica de la Dirección Zonal de Tecnologías de la Información



Nota. Información extraída de la página oficial de la institución <http://www.saludzona1.gob.ec/>

Infraestructura de la Organización

La Dirección Zonal de Tecnologías de la Información y Comunicaciones, brinda varios servicios a los funcionarios de la Coordinación Zonal 1 - Salud, con el objetivo de ayudar a mejorar las tareas de los funcionarios y agilizar los procesos. Para brindar servicios de calidad a los funcionarios actualmente se cuenta con el siguiente equipamiento activo de red.

Tabla 1

Equipamiento activo de red

EQUIPO	MARCA	MODELO	SERIE	ESTADO
Switch	3COM	2824	3CBLUG24	OPERATIVO
	3COM	2928	6,41884E+11	OPERATIVO
	D-LINK	KVM-440	NA	OPERATIVO
	CISCO	SG 200-26P	DNI173605PU	OPERATIVO
	CISCO	SF 200-24P	DNI173800DV	OPERATIVO
	CISCO	SG 300-28P	DNI1637045Z	OPERATIVO
	CISCO	SG 200-26P	DNI163307PC	OPERATIVO
	CISCO	C2960S- 48LPD-L	FOC1529X58F	OPERATIVO
	CISCO	C2960S- 48LPD-L	FOC1521Y06Z	OPERATIVO
	CISCO	C2960S- 48LPD-L	FOC1519X1RV	OPERATIVO
	CISCO	C2960S- 24PD-L	FOC1526X307	OPERATIVO
	CISCO	SG200-08P	PSZ17421E2E	OPERATIVO
	AP Sede Zonal	CISCO	WAP4410N	SER131800WR
UNIFI UBIQUITI		UniFi AP-Pro	24A43CB0402B	OPERATIVO
UNIFI UBIQUITI		UniFi AP-Pro	24A43CB03F83	OPERATIVO

EQUIPO	MARCA	MODELO	SERIE	ESTADO
	UNIFI	UniFi AP-Pro	24A43CB03F7	OPERATIVO
	UBIQUITI			
	UNIFI	UniFi AP-Pro	24A43CB03EEF	OPERATIVO
	UBIQUITI			
	UNIFI	UniFi AP-Pro	24A43CB0456	OPERATIVO
	UBIQUITI			
	DLINK	DAP-2690	NA	OPERATIVO
	HP	MSM 430	NA	OPERATIVO
	HP	MSM 430	CNEBDWY0SK	OPERATIVO
	DLINK	DAP-1353	P42X186000471	OPERATIVO
	DLINK	DIR 635	F3TQ18A001507	OPERATIVO

Nota. Información proporcionada por la Dirección Zonal de Tecnologías de la Información.

Como servidores se cuenta con el equipamiento que se detalla en la Tabla 2.

Tabla 2

Servidores de la Dirección Zonal de Tecnologías de la Información.

SERVIDOR/ SERVICIO	MARCA	MODELO	SERIE	PROCESA DOR	DISCO DURO	ESTADO
Storage	HP	Proliant	MX24450	CPU	4TB	OPERATIV
Freenas		Microserv	03D	G2020T @		O
		er Gen8		2.50GHz		
Firewall	HP	Proliant	5C7319P0	AMD Turion	1 TB	OPERATIV
Pfsense		Microserv	ZJ	II Neo 2.2		O
LAN/WIFI		er Gen7		GHz		
Virtualizador	HP	Proliant	MX24450	CPU	1TB	OPERATIV
Proxmox 2		Microserv	03E	G2020T @		O
		er Gen8		2.50GHz		
Firewall	HP	ML 115	2UX83007	AMD	1TB	OPERATIV
Pfsense		G5	D2	Opteron		O
LAN/WIFI						

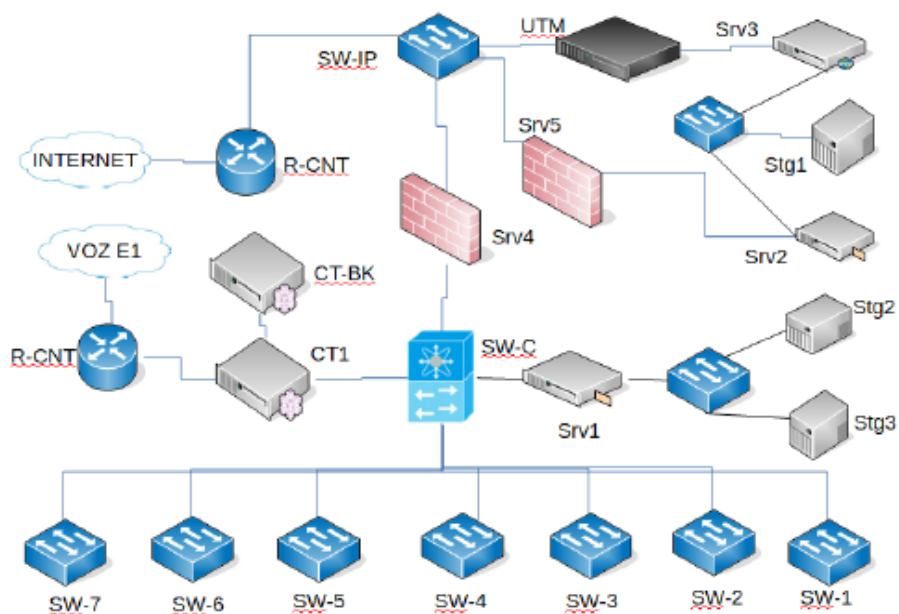
SERVIDOR/ SERVICIO	MARCA	MODELO	SERIE	PROCESA DOR	DISCO DURO	ESTADO
				QuadCore, 2.2 GHz		
UTM	EDGE BOX	Enterprise	M1224203 7	NA	450GB	OPERATIV O
Central Telefónica	MITEL	3300MXE	SAEEA05 40	NA	80GB	OPERATIV O
Central Telefónica/Ba ckup	MITEL	3300MXE	SAEEA05 47	NA	80GB	OPERATIV O
Firewall Pfsense DMZ	HP	Proliant Microserv er Gen7	5C7319P0 ZJ	AMD Turion II Neo 2.2 GHz	1 TB	OPERATIV O
Servidor Rack (Virtualizador Proxmox 1)	FUJITSU	RX200-S6	YL6S0117 47	NA	6x146G B	OPERATIV O
Storage Master	FUJITSU	ETO8L22 AU	43111138 82	NA	12x600 GB	DAÑADO
Storage Backup	FUJITSU	ETO8L22 AU	46601548	NA	6x600G B	DAÑADO
Virtualizador Proxmox 3	HURRICA NE	HURRICA NE	NA	CPU(s) 12 x Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz	3 TB	OPERATIV O

Nota. Información proporcionada por la Dirección Zonal de Tecnologías de la Información.

A continuación, se detalla la topología física y lógica de red.

Figura 7

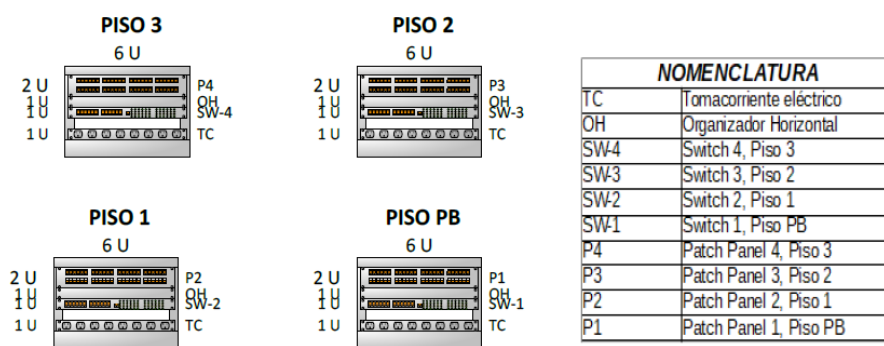
Topología de red



Nota. Información proporcionada por la Dirección Zonal de Tecnologías de la Información.

Figura 8

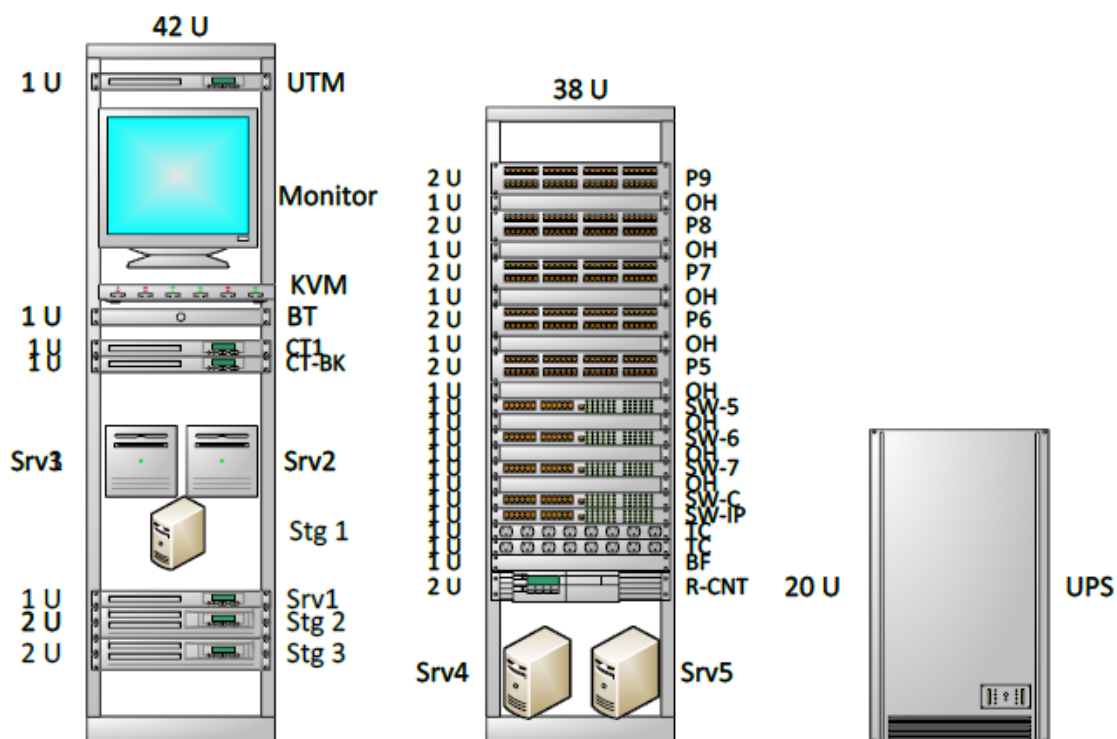
Topología física de rack de cada piso



Nota. Información proporcionada por la Dirección Zonal de Tecnologías de la Información.

Figura 9

Topología física datacenter



Nota: Información proporcionada por la dirección Zonal de Tecnologías de la Información.

Servicios Brindados

Los servicios que maneja la Dirección Zonal 1 de Tecnologías de la Información y Comunicaciones, son los siguientes de manera general:

- Seguridad Perimetral – Firewall Pfsense para la red de la Coordinación Zonal 1 (DNS interno, proxy cache, Dhcp, vlans).
- Seguridad Perimetral – Firewall Pfsense para la red DMZ de los servidores (DNS interno, proxy cache, Dhcp, vlans).

- Mesa de Ayuda OTRS: Servidor web Httpd, Base de datos Mysql, Sistema operativo Centos 7, firewalld, Sistema de detección y prevención de intrusos Fail2ban.
- Plataforma Cloud: Sistema operativo Ubuntu server 18.04, Base de datos Mysql, modulo Nextcloud 18.0.02, módulo de chat y videoconferencias Talk, módulo colaborativo ONLYOFFICE, firewalld, Sistema de detección y prevención de intrusos Fail2ban.
- Correo Institucional Zimbra Multidominio: Sistema operativo Centos 7, Zimbra 8.8.15_GA_3928, LDAP integrado con plataforma cloud, firewalld, Sistema de detección y prevención de intrusos Fail2ban. Actualmente aloja 10 dominios de los distritos de Imbabura, Sucumbios, Esmeraldas, actualmente se mantiene alrededor de 900 cuentas pertenecientes a funcionarios de la Coordinación Zonal 1, distritos, unidades operativas, Hospitales básicos, centros de salud tipo A, B y C.
- AntiSpam/ Antivirus (Mailscanner/Mailwatch) para correo institucional Zimbra: Sistema operativo Centos 7, Mailscanner 5.1.3, Mailwatch 1.2.12, ClamAV 0.102.2, SpamAssassin 3.4.0, Php 7.2.27, Base de Datos MariaDB, Postfix Version: 2.10.1
- Página web institucional: Sistema operativo Centos 7, plataforma de gestión de contenido joomla, servicio Httpd, firewalld, Sistema de detección y prevención de intrusos Fail2ban.
- Administrador central de seguridad ESET.
- Proxy Squid.
- Sistema VPN Ipsec, para conectarse de manera segura con firewall de seguridad perimetral del Centro de Especialidades de Rehabilitación Integral, y tener conectividad con la consola de Administrador central de seguridad ESET.
- Storage Freenas, para backups de las máquinas virtuales de todos los servicios y aplicaciones de la Coordinación Zonal 1.

- Storage Master y Backup Fujitsu.
- Plataforma de Aprendizaje Moodle: Sistema operativo Debian, container.
- Plataforma colaborativa Collabora Online – Nextcloud, módulo de chat y videoconferencias Talk.
- 3 Servidores instalados Virtualizador de servicios Proxmox para administrar todos los servicios y aplicaciones de la Zona1: sistema operativo Debian 10.
- Plataforma de videoconferencia Meetjitsi: Sistema operativo Ubuntu server 18.04, plataforma jitsi meet, módulo jicofo, módulo prosody, módulo jitsi-videobridge2, firewalld, Sistema de detección y prevención de intrusos Fail2ban.
- Plataforma de grabación videoconferencia Meetjitsi: Sistema operativo Ubuntu server 18.04, módulo jibri, firewalld, Sistema de detección y prevención de intrusos Fail2ban.
- Telefonía Ip con enlace E1.

Capítulo 3: Evaluación Técnica Informática en Base De Riesgos

En el capítulo se planifica y desarrolla la Evaluación Técnica Informática ETI mediante el marco de referencia COBIT 2019 de los procesos críticos de la organización determinados a través de la cascada de metas.

Método de Investigación

El método a utilizar en el presente proyecto es el inductivo (Abreu, 2014), ya que mediante este método se observa, estudia y conoce las características genéricas o comunes que se reflejan en un conjunto de realidades para elaborar una propuesta o ley científica de índole general.

Metodología

Se realiza inicialmente una revisión documental de fundamentos teóricos sobre el marco de referencia COBIT 2019 e información relacionada, posteriormente se procede con una investigación documental en la Dirección Zonal de Tecnologías de la Información y Comunicación, a partir de la cual se conduce una investigación de campo, con técnicas específicas de auditoría y evaluación in situ. Posteriormente se realiza un análisis de la información que comprende la evaluación técnica informática en base de buenas prácticas internacionales, en este caso de estudio mediante el marco de referencia COBIT 2019, para emitir los resultados obtenidos mediante un informe final de auditoría, concluyendo finalmente con un análisis de resultados mediante conclusiones y recomendaciones

Categoría de la Investigación.

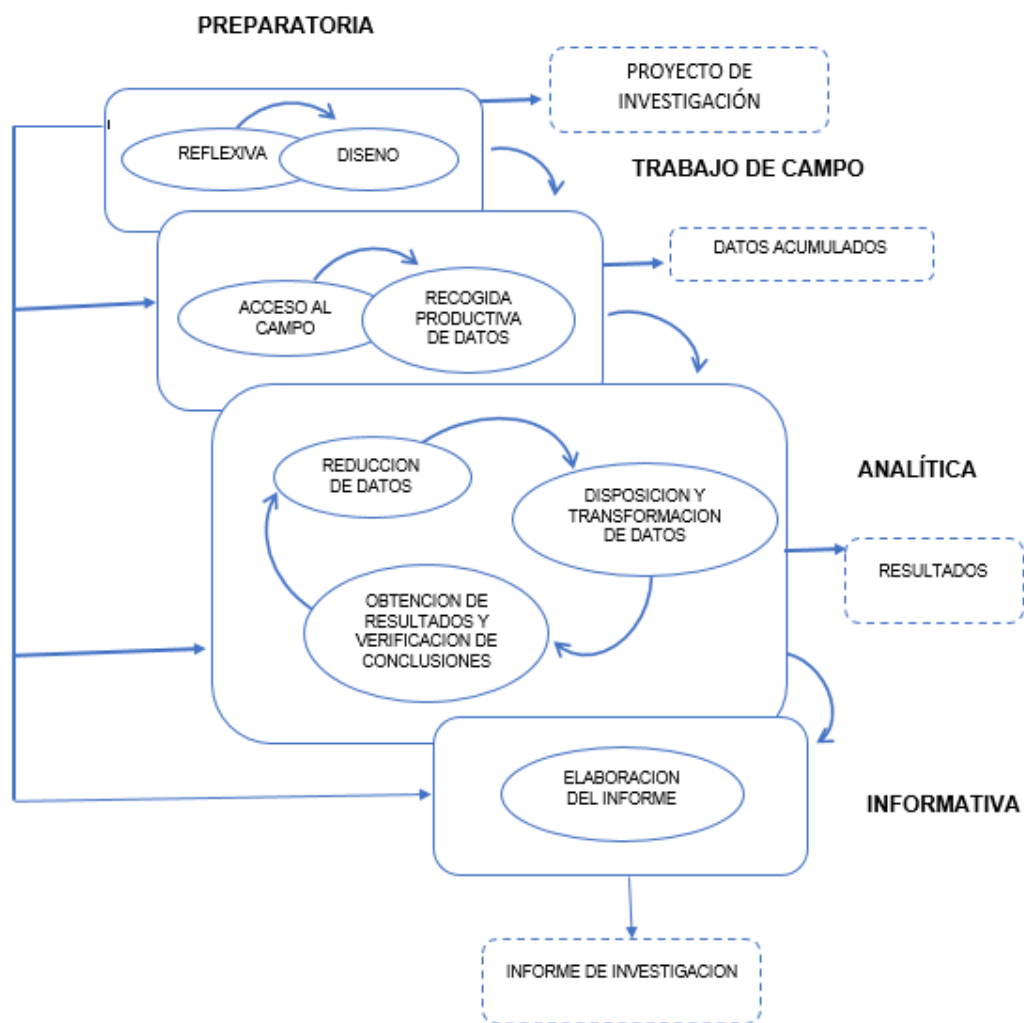
La categoría es cualitativa (Quecedo Lecanda & Castaño Garrido, 2002) ya que la investigación produce datos descriptivos, no es una investigación estadística, comienza con la recogida de datos, mediante la observación empírica o mediciones de alguna clase, y a continuación construye, a partir de las relaciones descubiertas, sus categorías y proposiciones teóricas.

Pasos de la Investigación

La investigación cualitativa presenta las siguientes fases y etapas.

Figura 10

Pasos de la investigación cualitativa



Nota. Extraído de Flores, Gómez, and Jiménez (1999).

Técnicas de Investigación

- Investigación documental. - Se analizará información registrada sobre el tema de objeto de estudio.

- Investigación de campo. - Se aplicará extrayendo datos e información directamente de la realidad a través del uso de técnicas de recolección como entrevistas o encuestas.

Estrategias de Investigación

- Revisión documental. – Revisar artículos científicos, libros, informes, reportes para la fundamentación teórica.
- Recepción de informes. – Recibir y revisar de Información técnica de la unidad de TIC.
- Observación. – Realizar visitas en situ a las instalaciones de TIC y conocer la infraestructura de TI.
- Registro de datos. – Obtener datos a partir de las técnicas de investigación de campo, datos útiles para la investigación, mediante entrevistas, encuestas, etc.
- Procesamiento de información y obtención de resultados. – Procesar, detallar la información obtenida para la evaluación técnica respectiva mediante COBIT 2019.
- Revisión de resultados. – Revisar los datos arrojados en la evaluación técnica para emitir el informe de auditoría con la evidencia pertinente.
- Comunicación de resultados. - En relación con el informe de auditoría, comunicar los resultados obtenidos en forma de conclusiones y recomendaciones.

Objetivos de la Evaluación

Objetivo General

Realizar una evaluación técnica informática en base de riesgos a la Dirección Zonal de Tecnologías de la Información y Comunicación de la Coordinación Zonal 1 – Salud utilizando el marco de referencia COBIT 2019.

Objetivos Específicos

Realizar una investigación documental en la Dirección Zonal de Tecnologías de la Información y Comunicación.

Ejecutar una investigación de campo, con técnicas específicas de auditoría y evaluación in situ.

Determinar los procesos a ser evaluados, mediante el método de cascada de COBIT 2019.

Realizar un análisis de la información recopilada, que comprende la evaluación técnica informática en base de buenas prácticas internacionales, en este caso de estudio mediante el marco de referencia COBIT 2019.

Realizar el informe de auditoría en donde se evidencie la situación actual de la unidad de tecnologías de la información.

Emitir las conclusiones y recomendaciones que ayuden a mitigar los riesgos detectados y permitan mejorar los servicios brindados por la dirección.

Ejecución de la Evaluación

Si bien como auditor se tiene el conocimiento pertinente de la institución debido a que laboré 4 años en la unidad de TI, para ejecutar la investigación de campo se realiza una entrevista preliminar a la Ing. Vanessa Alvear responsable de la Dirección Zonal de Tecnologías de la Información y Comunicación, para conocer datos relevantes de la institución de manera formal, comprender el modelo de negocio, para en base a dicho conocimiento posteriormente realizar una selección adecuada de los procesos a evaluar mediante la cascada de metas COBIT 2019, la entrevista preliminar con código de evidencia AF-ENT01-TIC consta de 53 preguntas detalladas a continuación:

- ¿La Coordinación Zonal 1- Salud tiene un área de Tecnología (TI)?
- ¿La organización ha definido claramente qué significa las TI para ella?
- ¿La unidad de TI es valorada en la organización?
- ¿Cuánto tiempo labora en la institución y en el puesto que actualmente se desempeña?
- ¿Tiene claro sus responsabilidades y autoridad como responsable de la unidad de TI?
- ¿Se han documentado las áreas de responsabilidad del responsable de TI (CIO, en inglés)? ¿En dónde?
- ¿Existe organigrama de la unidad de TI?
- ¿Existe manual de puestos de la unidad de TI?
- ¿Cuántas personas están en la unidad de TI?
- ¿Las personas que están en la unidad de TI son las necesarias?
- ¿Cuántas personas debería haber en la unidad de TI?
- ¿Con qué tipo de personal cuenta la unidad de TI?
- ¿Se emplean especialistas para las diversas tecnologías (por ejemplo, aplicaciones versus tecnologías de infraestructura)? ¿Si la respuesta es negativa, por qué no?
- ¿La Coordinación Zonal 1- Salud tiene un plan estratégico? En caso afirmativo.
¿Conoce el plan estratégico institucional?
- ¿Cuáles son los objetivos a largo plazo?
- ¿Cuáles son los objetivos a mediano plazo?
- ¿Cuáles son los objetivos corto plazo?
- ¿La Coordinación Zonal 1- Salud tiene un plan estratégico de TI? En caso negativo
¿Por qué no?
- ¿Existe una planificación anual de gestión?
- ¿Se realiza una planificación presupuestaria en la unidad de TI?

- ¿Se recibe la asignación presupuestaria de acuerdo con la planificación de la unidad de TI?
- ¿La asignación presupuestaria es suficiente?
- ¿Existen manuales de procedimientos?
- ¿Existen estructuras de control, políticas, normas de TI dentro de la organización? En caso afirmativo. ¿Cuáles?
- ¿Se evalúan anualmente los temas emergentes y los riesgos para determinar su relevancia dentro de la organización?
- ¿Cómo se identifican los temas emergentes dentro de la organización?
- ¿Existen planes de contingencia para el área informática? En el caso de tenerlo ¿cómo se las comunica a las demás áreas?
- ¿Se realiza continuas adquisiciones a nivel tecnológico?
- ¿Cómo se realiza la adquisición de la infraestructura tecnológica?
- ¿Actualmente existen proyectos que serán implementados en el área?
- ¿Con qué tipo de seguridad física se cuenta en las oficinas?
- ¿Con qué tipo de seguridades lógicas cuenta la información de la Coordinación Zonal 1-Salud?
- ¿Con qué tipo de seguridades físicas cuenta la información de la Coordinación Zonal 1-Salud?
- ¿Existe un plan de mantenimiento?
- ¿Cuántas veces al año recibe los equipos mantenimientos?
- ¿Se conservan registros de acciones de mantenimiento preventivo y correctivo realizados?
- ¿Se cuenta con metodología definida para llevar a cabo tareas de mantenimiento?
- ¿Existe un plan de capacitaciones?

- ¿Puede recuperar la información de los equipos de computación en caso de daños?
- ¿La red de datos está siempre disponible?
- ¿Las capacidades de las personas, procesos y tecnologías soportan los objetivos de la organización?
- ¿Cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI?
- ¿Qué actividades se desarrollan dentro de la institución que permitan optimizar las capacidades del personal?
- ¿Se relaciona los objetivos de la institución con los objetivos del área?
- ¿Qué área administra los proveedores de TI?
- ¿Cuándo surgen problemas o incidentes como se resuelve?
- ¿La infraestructura existente, es la necesaria? ¿Se encuentra identificada?

Selección de los Procesos Críticos a Evaluar

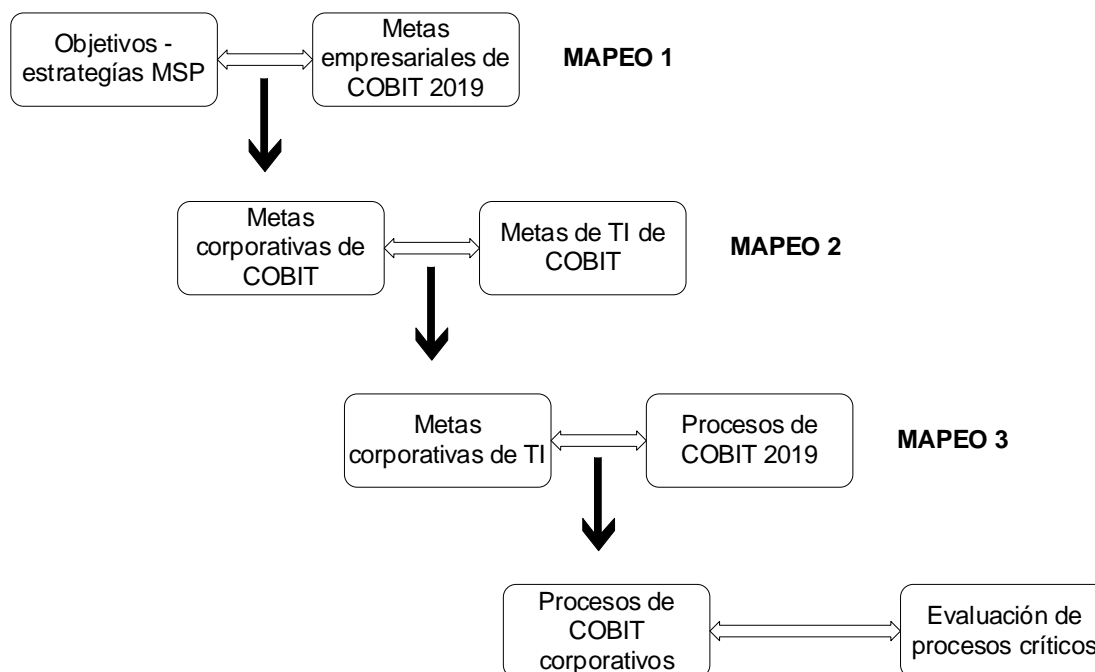
Para la selección de los procesos a ser evaluados se utiliza la cascada de metas de COBIT 2019, que relaciona las metas empresariales, metas de alineamiento de TI y los objetivos de gobierno y de gestión, como se visualiza en la figura 4.

Para lo cual es necesario contar con el Plan Estratégico Institucional, fuente principal que nos proporciona los objetivos estratégicos de la organización y las estrategias para cumplir dichos objetivos. La Coordinación Zonal 1 – Salud, no cuenta con un Plan Estratégico Institucional propio pues se maneja con el establecido por el Ministerio de Salud.

El modelo en cascada para la selección de los procesos críticos se realizará de la siguiente manera:

Figura 11

Cascada para selección de procesos a evaluar



Nota: Cascada de Metas COBIT 2019 ISACA, (2019).

Como podemos observar en la figura 11, se realiza 3 mapeos:

Mapeo 1.- Entre los objetivos – estrategias del MSP y las metas empresariales que plantea COBIT 2019 (13), de este mapeo se obtiene las **metas corporativas de COBIT**, es decir, aquellas metas del modelo COBIT 2019 que están estrechamente relacionadas con la institución.

Mapeo 2.- Las metas corporativas de COBIT previamente obtenidas se mapean con las metas de alineamiento de TI de COBIT 2019, de este mapeo se obtiene las **metas corporativas de TI COBIT**, es decir, aquellas metas TI del modelo COBIT 2019 que están estrechamente relacionadas con la institución.

Mapeo 3.- Las metas corporativas de TI COBIT previamente obtenidas se mapean con los procesos de COBIT 2019, de este mapeo se obtiene los **procesos de TI COBIT corporativos**, es decir, aquellos procesos del modelo COBIT 2019 que están estrechamente relacionadas con la institución.

Con este mapeo se realiza una selección idónea de los procesos críticos a ser evaluados ya que se filtra en 3 niveles: empresarial, de TI y de procesos, las directrices emitidas en el marco de referencia y se asocia a la realidad de la institución.

En la tabla siguiente se detalla los objetivos estratégicos del Ministerio de Salud Pública y las estrategias establecidas para su ejecución.

Tabla 3

Objetivos estratégicos y estrategias MSP.

OBJETIVOS ESTRATÉGICOS	ESTRATEGIAS
(OB1) Incrementar la Gobernanza en el Sistema Nacional de Salud.	<p>(OB1) Regular y controlar el Sistema Nacional de Salud con el desarrollo de políticas públicas y la aplicación de documentos normativos.</p> <p>(OB1) Promover la calidad en la gestión de la Red Pública Integral de Salud y Red Complementaria con base al Modelo de Atención Integral en Salud con enfoque en la atención primaria en salud.</p> <p>(OB1) Asegurar el acceso y uso racional a medicamentos y otras tecnologías sanitarias.</p> <p>(OB1) Planificar los requerimientos del talento humano en salud y la formación continua en coordinación con las instancias pertinentes de acuerdo a las necesidades del Sistema Nacional de Salud.</p>

OBJETIVOS ESTRATÉGICOS	ESTRATEGIAS
(OB2) Incrementar la calidad de la vigilancia y control sanitario en el Sistema Nacional de Salud.	<p>(OB2) Fortalecer las estrategias de salud pública para la prevención, control de enfermedades transmisibles y no transmisibles e inmunoprevenibles considerando el ciclo de vida, factores de riesgo y perfil epidemiológico nacional.</p> <p>(OB2) Fortalecer la capacidad de generar alertas de notificación oportuna frente a eventos epidemiológicos y origen natural, antrópico, ambiental, profesional y ocupacional.</p>
(OB3) Incrementar entornos y prácticas saludables con enfoque de derechos, de género, intercultural e intergeneracional a nivel nacional.	<p>(OB3) Promover el ejercicio de los derechos sexuales y los derechos reproductivos de la población.</p> <p>(OB3) Impulsar la participación comunitaria y de colectivos organizados en los procesos de información, planificación, implementación y seguimiento de las acciones de salud.</p> <p>(OB3) Generar lineamientos normativos que permitan a la población acceder a una atención de salud, sin discriminación, con enfoque intercultural y con derecho a decidir.</p>

OBJETIVOS ESTRATÉGICOS	ESTRATEGIAS
(OB4) Incrementar el acceso a servicios de salud de calidad, integrales integrados y continuos en el Ministerio de Salud Pública.	<p>(OB3) Promover la acción intersectorial para la generación de políticas públicas saludables que incidan en los determinantes de la salud y permita el mejoramiento de las condiciones de vida de la población.</p> <p>(OB4) Fortalecer la prestación integral de servicios de salud de calidad en coordinación con la RPIS y la Red Complementaria teniendo como puerta de entrada el primer nivel de atención.</p> <p>(OB4) Implementar las estrategias de salud pública priorizadas en los servicios de salud del MSP.</p> <p>(OB4) Fortalecer y generar mecanismos inclusivos garantizando la atención integral en salud a grupos vulnerables y de atención prioritaria.</p> <p>(OB4) Asegurar la disponibilidad oportuna, universal y con el adecuado manejo de medicamentos y otras tecnologías sanitarias, sangre, órganos y tejidos en los servicios de salud del MSP.</p>
(OB5) Incrementar la calidad y calidez de las prestaciones de servicios de salud en el	(OB5) Generar e implementar acciones de mejora continua de la calidad en los servicios de salud.

OBJETIVOS ESTRATÉGICOS	ESTRATEGIAS
(OB8) Incrementar la eficiencia institucional en el Ministerio de Salud Pública.	(OB7) Mejorar el acceso en tecnologías de la información y comunicaciones para el Ministerio de Salud Pública. (OB8) Coordinar acciones para la disponibilidad, buen uso, mantenimiento y aseguramiento de los bienes muebles e inmuebles del Ministerio de Salud Pública.
(OB9) Incrementar el desarrollo del talento humano en el Ministerio de Salud Pública.	(OB8) Fortalecer la institucionalidad de la gestión por procesos en el Ministerio de Salud Pública y unidades operativas. (OB9) Dotar y retener en el Ministerio de Salud Pública a servidores y/o trabajadores calificados y comprometidos con la institución.
(OB10) Incrementar el uso eficiente del presupuesto en el Ministerio de Salud Pública.	(OB9) Promover la identificación y satisfacción de las necesidades de los servidores y/o trabajadores del Ministerio de Salud Pública, conforme parámetros establecidos en la normativa legal vigente. (OB10) Planificar y asignar recursos en la redes de servicios de salud en los territorios de manera prospectiva y participativa.

Nota. Información proporcionada por el Coordinación Zonal 1 – Salud.

Para realizar la selección de procesos críticos a evaluar, se consideró dos criterios:

- Auditor, Amada Leonor Félix Bolaños quien trabajó en la institución 4 años, por ende, tiene conocimientos necesarios de la organización y los fundamentos de COBIT 2019.
- Personal de la Dirección Zonal de Tecnologías de la Información, quienes se encuentra laborando actualmente en la organización.

Para ello se realizó un trabajo en conjunto en las instalaciones de la Dirección Zonal de TI, en donde se realizó los 3 mapeos planteados.

MAPEO 1

El primer mapeo se realiza entre las 27 estrategias del MSP y las 13 METAS EMPRESARIALES DEL COBIT 2019, de la siguiente manera:

Figura 12

Mapeo 1 Estrategias MSP - Metas empresariales de COBIT 2019

	1	2	3	4	5	6
METAS CORPORATIVAS DE COBIT	Metas empresariales de COBIT					
	Financiera				Cliente	
Estrategias MSP	Portafolio de productos y servicios competitivos	Gestión de riesgo de negocio	Cumplimiento de leyes y regulaciones externas	Calidad de la información financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio del negocio
(OB1) Regular y controlar el Sistema Nacional de Salud con el desarrollo de políticas públicas y la aplicación de documentos normativos.	1	1	2	1	2	1
(OB1) Promover la calidad en la gestión de la Red Pública Integral de Salud y Red Complementaria con base al Modelo de Atención Integral en Salud con enfoque en la atención primaria en salud.	2	1	1	1	2	2

El mapeo completo se encuentra en el ANEXO 1, para ello se procedió a asignar un valor numérico de acuerdo con el nivel de alineamiento que tiene cada estrategia con las metas empresariales de COBIT 2019. Para la valoración se utilizó las siguientes ponderaciones:

Tabla 4

Ponderaciones para la valoración en cascada de metas

VALOR	DETALLE
0	No está alineada la estrategia del MSP con la meta empresarial de COBIT
1	Parcialmente alineada la estrategia del MSP con la meta empresarial de COBIT
2	Completamente alineada la estrategia del MSP con la meta empresarial de COBIT

Nota. Ponderaciones planeadas para la auditoría.

Adicional para marcar las metas seleccionadas se asigna letras de la siguiente manera:

S.- Procesos secundarios

P.- Procesos principales

A continuación, se detallan las metas empresariales de COBIT con su respectivo puntaje obtenido:

Tabla 5

Metas corporativas de COBIT

Metas empresariales de COBIT	Puntaje	Porcentaje	Metas seleccionadas
Portafolio de productos y servicios competitivos	48	91%	P
Gestión de riesgo de negocio	40	75%	P
Cumplimiento de leyes y regulaciones externas	30	57%	S
Calidad de la información financiera	39	74%	S

Metas empresariales de COBIT	Puntaje	Porcentaje	Metas seleccionadas
Cultura de servicio orientada al cliente	50	94%	P
Continuidad y disponibilidad del servicio del negocio	44	83%	P
Calidad de la información de gestión	50	94%	P
Optimización de la funcionalidad de procesos internos del negocio	46	87%	P
Optimización de costes de los procesos del negocio	45	85%	P
Habilidades, motivación y productividad del personal	51	96%	P
Cumplimiento con las políticas internas	53	100%	P
Gestión de programas de transformación digital	44	83%	P
Innovación de producto y negocio	44	83%	P

Del primer mapeo se obtiene las METAS CORPORATIVAS DE COBIT (11), que son aquellas con mayor puntaje, se ha seleccionado 11 de 13 metas empresariales de COBIT, que son las que superan el 75% del porcentaje.

MAPEO 2

Una vez obtenidas las METAS CORPORATIVAS DE COBIT (11) realizamos el mapeo con las METAS DE TI de COBIT 2019 (13), para obtener las METAS CORPORATIVAS DE TI que son aquellas metas del modelo que tienen más relevancia para la institución, de la siguiente manera:

Figura 13

Mapeo 2 Metas Corporativas de COBIT - Metas de TI COBIT 2019

	1	2	3	4
METAS CORPORATIVAS DE TI COBIT	Metas de alineamiento TI COBIT			
	Financiera			
Metas corporativas de COBIT	Cumplimiento y soporte de I&T para el cumplimiento empresarial con las leyes y regulaciones externas	Gestión de riesgo relacionado con I&T	Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T	Calidad de la información financiera relacionada con la tecnología
Portafolio de productos y servicios competitivos	1	3	3	3
Gestión de riesgo de negocio	3	3	3	3
Cultura de servicio orientada al cliente	1	3	3	1
Continuidad y disponibilidad del servicio del negocio	3	3	3	3

El mapeo completo se encuentra en el ANEXO 2. Para dicho mapeo se asignaron los valores 3 y 1 a las letras P y S, para obtener datos numéricos que nos permitan realizar la selección respectiva.

A continuación, se detallan las metas de alineamiento de TI COBIT con su respectivo puntaje obtenido:

Tabla 6

Metas corporativas de TI COBIT 2019

Metas de alineamiento TI COBIT	Puntaje	Porcentaje	Metas seleccionadas
Cumplimiento y soporte de I&T para el cumplimiento empresarial con las leyes y regulaciones externas	23	74%	S
Gestión de riesgo relacionado con I&T	31	100%	P

Metas de alineamiento TI COBIT	Puntaje	Porcentaje	Metas seleccionadas
Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T	25	81%	S
Calidad de la información financiera relacionada con la tecnología	27	87%	S
Prestación de servicios de I&T conforme a los requerimientos del negocio	31	100%	P
Agilidad para convertir los requerimientos del negocio en soluciones operativas	31	100%	P
Seguridad de la información, infraestructura y aplicaciones de procesamiento y privacidad	31	100%	P
Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología	31	100%	P
Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplen con los requisitos y estándares de calidad	31	100%	P
Calidad de la información sobre gestión de I&T	31	100%	P
Cumplimiento de I&T con las políticas internas	25	81%	S
Personal competente y motivado con un entendimiento mutuo de la tecnología y el negocio	31	100%	P
Conocimiento, experiencia e iniciativas para la innovación empresarial	31	100%	P

Se ha seleccionado 9 de las 13 metas de alineamiento de TI COBIT, es decir, aquellas que obtuvieron un porcentaje del 100%, las mismas que se encuentran marcadas con la letra P, es importante recalcar, que según la valoración realizada por el equipo evaluador se considera la mayoría de metas estrechamente relacionadas con la institución por ello se evidencia que 9 de 13 metas obtienen un porcentaje del 100%.

MAPEO 3

Una vez obtenidas las METAS CORPORATIVAS DE TI (9) realizamos el mapeo con los PROCESOS DE COBIT 2019 (40), para obtener las PROCESOS DE COBIT CORPORATIVOS, de la siguiente manera:

Figura 14

Mapeo 3 Metas Corporativas de TI COBIT – Procesos de COBIT 2019

	1	2	3
PROCESOS COBIT A SER AUDITADOS	PROCESOS DE COBIT		
	Evaluar, dirigir, monitorizar		
	EDM01	EDM02	EDM03
Metas corporativas de TI COBIT	Asegurar el establecimiento y el mantenimiento del marco de gobierno	Asegurar la entrega de beneficios.	Asegurar la optimización del riesgo
Gestión de riesgo relacionado con I&T	1	1	3
Prestación de servicios de I&T conforme a los requerimientos del negocio	1	3	1
Agilidad para convertir los requerimientos del negocio en soluciones operativas	1	3	1

El mapeo completo se encuentra en el ANEXO 3. En la siguiente tabla se muestra los 40 PROCESO DE COBIT 2019 con el respectivo puntaje obtenido:

Tabla 7*Resultados evaluación procesos de COBIT.*

Dominio	Proceso	Puntaje	Porcentaje	Metas seleccionadas
EDM01	Asegurar el establecimiento y el mantenimiento del marco de gobierno	11	41%	S
EDM02	Asegurar la entrega de beneficios.	21	78%	S
EDM03	Asegurar la optimización del riesgo	21	78%	S
EDM04	Asegurar la optimización de recursos	27	100%	P
EDM05	Asegurar la participación de las partes interesadas	17	63%	S
APO01	Gestionar el marco de gestión de I&T	13	48%	S
APO02	Gestionar la estrategia	15	56%	S
APO03	Gestionar la arquitectura empresarial	19	70%	S
APO04	Gestionar la innovación	27	100%	P
APO05	Gestionar el portafolio	17	63%	S
APO06	Gestionar el presupuesto y los costes	25	93%	P
APO07	Gestionar los recursos humanos	25	93%	P
APO08	Gestionar las relaciones	17	63%	S
APO09	Gestionar los acuerdos de servicio	25	93%	P
APO10	Gestionar los proveedores	9	33%	S
APO11	Gestionar la calidad	27	100%	P
APO12	Gestionar riesgos	27	100%	P

Dominio	Proceso	Puntaje	Porcentaje	Metas seleccionadas
APO13	Gestionar la seguridad	25	93%	P
APO14	Gestionar los datos	25	93%	P
BAI01	Gestionar los programas	19	70%	S
BAI02	Gestionar la definición de requerimientos	21	78%	S
BAI03	Gestionar la identificación y construcción de soluciones	27	100%	P
BAI04	Gestionar la disponibilidad y capacidad	19	70%	S
BAI05	Gestionar los cambios organizativos	21	78%	S
BAI06	Gestionar los cambios de TI	25	93%	P
BAI07	Gestionar la aceptación y la transición de los cambios de TI	23	85%	S
BAI08	Gestionar el conocimiento	19	70%	S
BAI09	Gestionar los activos	23	85%	S
BAI10	Gestionar la configuración	25	93%	P
BAI11	Gestionar los proyectos	27	100%	P
DSS01	Gestionar las operaciones	21	78%	S
DSS02	Gestionar las peticiones y los incidentes del servicio	23	85%	S
DSS03	Gestionar los problemas	21	78%	S
DSS04	Gestionar la continuidad	25	93%	P
DSS05	Gestionar los servicios de seguridad	21	78%	S
DSS06	Gestionar los controles de los procesos de negocio	11	41%	S
MEA01	Gestionar la monitorización del rendimiento y la conformidad	15	56%	S
MEA02	Gestionar el sistema de control interno	11	41%	S

Dominio	Proceso	Puntaje	Porcentaje	Metas seleccionadas
MEA03	Gestionar el cumplimiento de los requerimientos externos	23	85%	S
MEA04	Gestionar el aseguramiento	21	78%	S

De los cuales se ha seleccionado los 14 procesos con puntaje más alto para la presente evaluación técnica, es decir, se ha seleccionado los procesos que superaron el 90%, los mismos que se detallan en la tabla siguiente:

Tabla 8

Procesos Críticos - seleccionado para Evaluación Técnica Informática

Dominio	Proceso	Puntaje	Porcentaje
EDM04	Asegurar la optimización de recursos	27	100%
APO04	Gestionar la innovación	27	100%
APO06	Gestionar el presupuesto y los costes	25	93%
APO07	Gestionar los recursos humanos	25	93%
APO09	Gestionar los acuerdos de servicio	25	93%
APO11	Gestionar la calidad	27	100%
APO12	Gestionar riesgos	27	100%
APO13	Gestionar la seguridad	25	93%
APO14	Gestionar los datos	25	93%
BAI03	Gestionar la identificación y construcción de soluciones	27	100%
BAI06	Gestionar los cambios de TI	25	93%
BAI10	Gestionar la configuración	25	93%
BAI11	Gestionar los proyectos	27	100%
DSS04	Gestionar la continuidad	25	93%

Plan de Investigación

Previo a la ejecución de la Evaluación Técnica Informática ETI, se realizó la socialización del proyecto con los directivos de la Coordinación Zonal 1 - Salud con la finalidad de informar los beneficios de contar con una ETI en la institución, objetivos, metodología, cronogramas y actividades a realizarse.

Posteriormente, se elaboró el Plan de Investigación de Campo basado en los lineamientos que plantea COBIT, determinando los tipos de instrumentos a ser aplicados para las estrategias de investigación (cuestionarios, encuestas) y establecer los documentos a ser solicitados.

En la tabla siguiente se presenta el Plan de Investigación para el proceso EDM04, el Plan de Investigación de los 14 procesos a ser evaluados se encuentra en el **ANEXO 4**.

Tabla 9

Plan de Investigación.

PROCESO	OBJETIVO DE GOBIERNO	PRACTICA DE GESTION	ACTIVIDAD/ TEMA IMPORTANTE	PREGUNTA BÁSICA	DOCUMENTO REQUERIDO	INSTRUMENTO DE INV. DE CAMPO	FUENTE Evaluado	FECHA APLICACIÓN
EDM04	Asegurar la optimización de recursos	EDM04.01 Evaluar la gestión de recursos.	1. Partiendo de las estrategias actuales y futuras, examinar las posibles opciones para proporcionar recursos relacionados con I&T (recursos tecnológicos, financieros y humanos), y desarrollar capacidades para hacer frente a las necesidades actuales y futuras (incluidas opciones de abastecimiento).	¿Cómo se realiza la asignación de recursos para TI?	Documento de asignación presupuestaria a TI 2021	AF-CUE02-ADM	Responsable Zonal Administrativo Financiero	18/1/2021
			2. Definir los principios fundamentales de la asignación y gestión de recursos y capacidades, de forma que I&T puede satisfacer las necesidades de la empresa conforme a las prioridades acordadas y los	¿Cómo se evalúa si los recursos asignados a las TIC son o no suficientes?		AF-CUE02-ADM	Responsable Zonal Administrativo Financiero	18/1/2021

PRO CESO	OBJETIVO DE GOBIERNO	PRACTI CA DE GESTION	ACTIVIDAD/ TEMA IMPORTANTE	PREGUNTA BÁSICA	DOCUMEN TO REQUE RIDO	INSTRUMEN TO DE INV. DE CAMPO	FUENTE Evaluado	FECHA APLI CACIÓN
			límites presupuestarios. Por ejemplo, definir opciones preferidas de abastecimiento definidas para determinados servicios y los límites presupuestarios por opción de abastecimiento.					
			3. Revisar y aprobar las estrategias del plan de recursos y de la arquitectura empresarial para proporcionar valor y mitigar el riesgo con los recursos asignados.	¿La unidad de TI participa en la planificación de los recursos de la institución?	Convocatoria de reunión para la revisión de recursos de la institución	AF-CUE02-ADM	Respuesta Zonal Administrativo Financiero	18/1/2021
			4. Entender los requisitos para el alineamiento de la gestión de recursos de I&T con la planificación de recursos	¿Cómo se verifica el alineamiento de los	PEDI (Plan Estratégico de Desarrollo	AF-CUE02-ADM	Respuesta Zonal Administrativo	18/1/2021

PROCESO	OBJETIVO DE GOBIERNO	PRACTICA DE GESTION	ACTIVIDAD/ TEMA IMPORTANTE	PREGUNTA BÁSICA	DOCUMENTO REQUERIDO	INSTRUMENTO DE INV. DE CAMPO	FUENTE Evaluado	FECHA APLICACIÓN
			humanos (RR. HH.) y financieros de la empresa.	requerimientos de TI con la planificación de recursos de la institución?	Institucional)		tivo Financiero	
			5. Definir los principios para la gestión y el control de la arquitectura empresarial	¿Qué principios, directrices o políticas han sido emitidas por la alta dirección para el diseño de la Arquitectura de TI?		AF-CUE01-COO	Coordinador Zonal 1 - Salud	18/1/2021

PROCESO	OBJETIVO DE GOBIERNO	PRACTICA DE GESTION	ACTIVIDAD/ TEMA IMPORTANTE	PREGUNTA BÁSICA	DOCUMENTO REQUERIDO	INSTRUMENTO DE INV. DE CAMPO	FUENTE Evaluado	FECHA APLICACIÓN
		EDM04.02	1. Asignar responsabilidades para la ejecución de la gestión de recursos.	¿Quiénes han sido designado para la gestión de recursos de TI y qué responsabilidades tiene cada uno de ellos?		AF-CUE04-TIC	Responsable Zonal de Tecnologías de la Información y Comunicación	19/1/2021
			2. Establecer los principios relacionados con la protección de los recursos.	¿Qué principios, directrices o políticas han sido emitidas por la alta dirección para la		AF-CUE01-COO	Coordinador Zonal 1 - Salud	18/1/2021

PROCESO	OBJETIVO DE GOBIERNO	PRACTICA DE GESTION	ACTIVIDAD/ TEMA IMPORTANTE	PREGUNTA BÁSICA	DOCUMENTO REQUERIDO	INSTRUMENTO DE INV. DE CAMPO	FUENTE Evaluado	FECHA APLICACIÓN
				protección de la información?				
			3. Comunicar y dirigir la adopción de estrategias de gestión de recursos, principios y del plan de recursos y arquitectura empresarial acordados.	¿Existen estrategias de gestión de recursos?		AF-CUE03-PLA	Respuesta zonal de Planificación	18/1/2021
			4. Alinear la gestión de recursos con la planificación financiera y de RR. HH. de la empresa.	¿En la planificación financiera se toma en cuenta los recursos humanos?		AF-CUE03-PLA	Respuesta zonal de Planificación	18/1/2021
			5. Definir las metas, mediciones y métricas clave para la gestión de recursos.	¿Existen métricas definidas		AF-CUE03-PLA	Respuesta zonal de	18/1/2021

PROCESO	OBJETIVO DE GOBIERNO	PRACTICA DE GESTION	ACTIVIDAD/ TEMA IMPORTANTE	PREGUNTA BÁSICA	DOCUMENTO REQUERIDO	INSTRUMENTO DE INV. DE CAMPO	FUENTE Evaluado	FECHA APLICACIÓN
				para la gestión de recursos?			Planificación	
		EDM04.03 Monitorizar la gestión de recursos.	1. Supervisar la asignación y optimización de recursos conforme a los objetivos y prioridades de la empresa usando metas y métricas acordadas.	¿Cómo se supervisa la asignación y optimización de recursos de TI conforme a los objetivos y prioridades de la institución?		AF-CUE03-PLA	Respuesta zonal de Planificación	18/1/2021
			2. Supervisar las estrategias de abastecimiento de I&T, las estrategias de arquitectura empresarial y las capacidades y recursos empresariales y de	¿Cómo se evalúa las capacidades y recursos empresariales				

PROCESO	OBJETIVO DE GOBIERNO	PRACTICA DE GESTION	ACTIVIDAD/ TEMA IMPORTANTE	PREGUNTA BÁSICA	DOCUMENTO REQUERIDO	INSTRUMENTO DE INV. DE CAMPO	FUENTE Evaluado	FECHA APLICACIÓN
			TI para garantizar que se puedan satisfacer las necesidades y objetivos actuales y futuros de la empresa.	s y de TI para garantizar que se puedan satisfacer las necesidades y objetivos actuales y futuros de la empresa??				
			3. Monitorizar el rendimiento de los recursos en relación a los objetivos, analizar la causa de las posibles desviaciones, y poner en marcha las acciones remediales para solucionar las causas subyacentes.	¿Cómo se monitoriza el rendimiento de los recursos en relación a los objetivos?		AF-CUE03-PLA	Respuesta zonal de Planificación	18/1/2021

Investigación de Campo

En relación con las preguntas establecidas en el Plan de Investigación, se realizó varios cuestionarios, encuestas, para los directores zonales de la Coordinación Zonal 1 – Salud y personal de la institución, con el objetivo de recopilar información que permita conocer la realidad de las Tecnologías de la Información y de la institución, de acuerdo con el siguiente detalle:

Tabla 10

Instrumentos de campo

INSTRUMENTO DE INV. DE CAMPO	FUENTE (Evaluado)
AF-ENT01-TIC	Responsable Zonal de Tecnologías de la Información y Comunicación
AF-CUE01-COO	Coordinador Zonal 1 - Salud
AF-CUE02-ADM	Responsable Zonal Administrativo Financiero
AF-CUE03-PLA	Responsable zonal de Planificación
AF-CUE04-TIC	Responsable Zonal de Tecnologías de la Información y Comunicación
AF-CUE05-TH	Responsable Zonal de Talento Humano
AF-CUE06-PRO	Responsable Zonal de Provisión de los servicios
AF-ENC01-MAS	Personal Coordinación Zonal 1 – Salud

Entrevista (ENT): Se realizó una entrevista preliminar al responsable de la unidad de Tecnologías de la Información para conocer datos relevantes de la institución y de la unidad de TI, en el Anexo A1 se presenta la entrevista aplicada.

Cuestionarios (CUE): Se realizaron en base a las preguntas planteadas en el Plan de Investigación de Campo. En el Anexo B1, AnexoB2, Anexo B3, Anexo B4, Anexo B5 y Anexo B6 se presenta los cuestionarios aplicados a los responsables de las diferentes unidades de la institución.

Encuestas: Se realizó una encuesta a los todos los funcionarios de la Coordinación Zonal 1 – Salud que son los usuarios de los servicios que brinda la unidad de TI. En el Anexo C1 se presenta la encuesta aplicada.

Los documentos de sustento de la investigación de campo se encuentran debidamente firmados por cada uno de los entrevistados de tal manera que sustentan la veracidad de la información entregada, así como existen los audios de grabación del desarrollo de cada uno de las entrevistas, encuestas, grabaciones realizadas bajo el consentimiento de cada uno de los entrevistados. Información que ha sido entregada de manera formal en la institución como respaldo de la Evaluación Técnica Informática ETI realizada

Investigación Documental

Para realizar la investigación documental, se solicita a la máxima autoridad de la institución se facilite la documentación que respalde la información recabada, a continuación, se detalla algunos de los documentos solicitados, en el Anexo D1 se encuentra la solicitud formal de la documentación y en el Anexo D2 la respuesta sobre la disponibilidad de estos.

- Documento de asignación presupuestaria a TI 2020
- Convocatoria de reunión para revisión de recursos de la institución
- PEDI (Plan Estratégico de Desarrollo Institucional)
- Plan de innovación tecnológica de la Institución o su equivalente
- Plan de respaldo del personal
- Plan de capacitación para el personal de TI
- Brecha de Talento Humano de TI
- Catálogo de servicios de TI
- SLA (Acuerdo de nivel de servicio)
- SLA con proveedores externos

- Plan de acción de riesgos
- Registro de riesgos que se han materializado
- Informes externos de auditoría a TI
- Plan de tratamiento de riesgos de seguridad de la información
- PETI (Planificación Estratégica de la Tecnología de la Información)
- Certificado de capacitación en Gestión de Proyectos de TI
- Acta de reunión de socialización de un proyecto de TI
- Plan de gestión de la calidad de un proyecto
- Mapa de riesgos de un proyecto de TI
- Registro de Riesgos de un proyecto del área de TI
- Informe de recomendaciones de proyectos de TI
- Plan de continuidad del negocio
- Plan de respuesta ante desastres
- Plan de copias de seguridad de los sistemas, aplicaciones, datos y documentación
- Plan de continuidad de TI
- Plan de capacidad del área de Tecnologías de la Información o su equivalente
- Informe de análisis de la brecha digital existente de la institución o su equivalente
- Análisis de posibilidades de innovación tecnológica de la institución
- Plan de adquisiciones/desarrollo de alto nivel para proyectos del área de Tecnologías de la Información
- Plan de mantenimiento de servicios y/o productos del área de Tecnologías de la Información.
- Mapa de procesos de la Institución
- Manual de procesos de la Institución
- Plan de contingencia del negocio

- Plan de respuesta ante desastres
- Informe de análisis externo de la institución (PEST O PESTEL O FODA) o su equivalente
- Marco de Referencia de la Arquitectura Empresarial (TOGAF, DODAF, MODAF, FEA, GARTNER O ZACHMAN)
- Planificación de gestión de TI
- Inventario tecnológico actualizado equipos de cómputo
- Inventario tecnológico actualizado equipos de red
- Diagrama de cableado estructurado de datos y telefonía
- Políticas de TI

De los 61 documentos solicitados, la institución indica mediante oficio que se cuenta con 24 de ellos.

Evaluación de los Procesos Críticos Utilizando COBIT 2019

Para ejecutar la evaluación fue necesario desarrollar algunas actividades previas, recolección de información mediante: observación realizando visitas en situ a las instalaciones de TIC y conocer la infraestructura de TI; registro de datos a través de técnicas de investigación como encuestas y cuestionarios; recepción y análisis de documentación de respaldo, evaluando las actividades planteadas en cada proceso del marco de referencia COBIT 2019: Objetivos de gobierno y gestión.

Para la evaluación de los procesos, conforme al Plan de Investigación planteado, se realiza en base a las actividades que soportan el cumplimiento de cada proceso de COBIT seleccionado de acuerdo al marco de referencia, para ello se determina si dichas actividades se ejecutan, no se ejecutan o se ejecutan parcialmente, resultado que se sustenta por medio de alguna evidencia recopilada.

Una vez realizada la evaluación a cada uno de los procesos se obtienen las observaciones respectivas, es decir, los hallazgos de la Evaluación Técnica Informática ETI.

A continuación, se presenta la tabla de la evaluación al proceso EDM04, las evaluaciones realizadas de los 13 procesos restantes se encuentran en el ANEXO 5:

Tabla 11

Evaluación proceso EDM04

PROCESO:	EDM04 Asegurar la optimización de recursos		
DESCRIPCIÓN:	Asegurar que se dispone de recursos adecuados y suficientes relacionadas con I&T (personas, procesos y tecnología) y con el negocio para apoyar eficazmente los objetivos empresariales, a un coste óptimo.		
PROPÓSITO:	Asegurarse de que las necesidades de recursos de la empresa se satisfagan de manera óptima, que los costes de I&T se optimicen, y que exista una mayor probabilidad de obtener beneficios y disponibilidad para cambios futuros.		
N	ACTIVIDADES	RESPUESTA	EVIDENCIA / COMENTARIOS
1	1. Partiendo de las estrategias actuales y futuras, examinar las posibles opciones para proporcionar recursos relacionados con I&T (recursos tecnológicos, financieros y humanos), y desarrollar capacidades para hacer frente a las necesidades actuales y futuras (incluidas opciones de abastecimiento).	Si	La asignación de recursos para TI se realiza en base a la necesidad que levanta cada unidad en la proforma presupuestaria anual.
2	2. Definir los principios fundamentales de la asignación y gestión de recursos y capacidades, de forma que I&T puede satisfacer las necesidades de la empresa conforme a las prioridades acordadas y los límites presupuestarios. Por ejemplo, definir opciones preferidas de abastecimiento definidas para determinados servicios y los límites presupuestarios por opción de abastecimiento.	Si	Para evaluar si los recursos asignados a las TIC son suficientes, el indicador es la ejecución presupuestaria, depende si se ejecuta al 100% en un corto tiempo, significa que se requiere más recursos, sin embargo, si de lo asignado no hay un porcentaje alto

PROCESO:		EDM04 Asegurar la optimización de recursos	
			de ejecución significa que los recursos asignados han excedentes
3	3. Revisar y aprobar las estrategias del plan de recursos y de la arquitectura empresarial para proporcionar valor y mitigar el riesgo con los recursos asignados.	Si	Todas las direcciones zonales participan en la elaboración de la proforma presupuestaria.
4	4. Entender los requisitos para el alineamiento de la gestión de recursos de I&T con la planificación de recursos humanos (RR. HH.) y financieros de la empresa.	Si	El alineamiento de los requerimientos de TI con la planificación de recursos de la institución se verifica a través del POA, es decir, que los requerimientos de TI estén alineados con la Planificación Operativa Anual.
5	5. Definir los principios para la gestión y el control de la arquitectura empresarial	No	No se han emitido por parte de la Coordinación Zonal 1 – Salud, existen arquitecturas definidas desde nivel central del Ministerio de Salud, pero no se ejecutan por varias razones, entre ellas, presupuesto, apoyo político para implementar cambios, como por ejemplo telemedicina, historia clínica única en el país.

PROCESO:		EDM04 Asegurar la optimización de recursos	
6	1. Asignar responsabilidades para la ejecución de la gestión de recursos.	Si	El responsable zonal de Tecnologías de la Información y Comunicación es el designado para la gestión de los recursos de TI, las responsabilidades están establecidas en el Estatuto Orgánico por Procesos del Ministerio de Salud Pública. La gestión de los recursos de TI como la infraestructura existente está a cargo del Mgs. Gabriel Pavón.
7	2. Establecer los principios relacionados con la protección de los recursos.	No	No se han emitido por parte de la Coordinación Zonal 1 – Salud, las directrices se ha recibido desde nivel central, la Coordinación Zonal 1 – Salud es un reflejo de nivel central del Ministerio de Salud, no hay seguridad de la información al 100%, no habido inversión y existe actualmente personas que tienen mucho conocimiento que pueden poner en riesgo la seguridad.
8	3. Comunicar y dirigir la adopción de estrategias de gestión de recursos, principios y del plan de recursos y arquitectura empresarial acordados.	Si	Existen estrategias y proyectos de cómo se ejecutan los recursos.

PROCESO:		EDM04 Asegurar la optimización de recursos	
9	4. Alinear la gestión de recursos con la planificación financiera y de RR. HH. de la empresa.	Si	En la planificación financiera se toma en cuenta los recursos humanos, dependiendo de la necesidad que tiene cada área.
10	5. Definir las metas, mediciones y métricas clave para la gestión de recursos.	No	Desde el área de planificación no se han establecido métricas.
11	1. Supervisar la asignación y optimización de recursos conforme a los objetivos y prioridades de la empresa usando metas y métricas acordadas.	Si	Se supervisa a través de la matriz de cedula presupuestaria, la optimización de recursos se realiza desde cada proceso
12	3. Monitorizar el rendimiento de los recursos en relación a los objetivos, analizar la causa de las posibles desviaciones, y poner en marcha las acciones remediales para solucionar las causas subyacentes.	Parcialmente	No se monitoriza en relación a los objetivos, el administrador de contrato revisa la relación de acuerdo a los objetivos

Hallazgos

De la Evaluación Técnica Informática ETI se obtuvo 14 hallazgos, los cuales representan las carencias o deficiencias a nivel de TI, es decir, aquellas circunstancias que no se encuentran desarrollando adecuadamente en la unidad de TI, los mismos que se detallan en la tabla siguiente:

Tabla 12

Hallazgos de la ETI

Nro	HALLAZGOS
1	No se dispone de recursos adecuados y suficientes relacionadas con I&T (personas, procesos y tecnología)
2	No se dispone de un Plan de Innovación Tecnológica
3	El presupuesto asignado a TI es sumamente bajo y no existe una optimización de costes.
4	No existen planes formales de planificación y de desarrollo profesional para fomentar el desarrollo de competencias y las oportunidades para el avance personal
5	La monitorización de los productos y servicios de I&T no se encuentra correctamente documentada
6	No existe un sistema de gestión de la calidad
7	No se registran datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa
8	No existe un sistema de gestión de seguridad de la información (SGSI)
9	No existe una estrategia de gestión de los datos
10	No se realiza desarrollo a nivel zonal, solo se puede realizar desarrollo desde nivel central.
11	No están definidos los cambios de emergencia y no existe un procedimiento documentado sobre un cambio de emergencia.
12	No está establecido un modelo de la configuración y no existe un repositorio de configuración.
13	El personal que conforma el área de informática no cuenta con capacitación para la gestión de proyectos de TI.

Nro HALLAZGOS

14 No existe el Plan de Continuidad del Negocio

Matriz de Riesgos

Para determinar el nivel de riesgo de los hallazgos identificados en la Evaluación Técnica Informática, se realizó un análisis cualitativo (Sánchez, 2015) tomando en cuenta dos parámetros importantes: la probabilidad y el impacto, de acuerdo con las valoraciones establecidas en las tablas siguientes:

Tabla 13

Probabilidad de ocurrencia

Valoración	Descripción
Baja	La amenaza se materializa máximo una vez cada año
Media	La amenaza se materializa máximo una vez cada mes
Alta	La amenaza se materializa máximo una vez cada semana

Tabla 14

Nivel de Impacto

Valoración	Descripción
Bajo	El resultado de que se concrete la amenaza no tiene consecuencias relevantes para la organización
Medio	El resultado de que se concrete la amenaza tiene consecuencias tolerables para la organización.
Alto	El resultado de que se concrete la amenaza tiene consecuencias graves para la organización

Con base a las valoraciones detalladas anteriormente y en combinación de estas se determina el nivel de riesgo acorde a la imagen siguiente:

Figura 15

Cascada para selección de procesos a evaluar

		NIVEL DEL RIESGO			
P R O B A L I D A D	↑	ALTA	Medio	Alto	Muy alto
		MEDIA	Bajo	Medio	Alto
		BAJA	Muy bajo	Bajo	Medio
			BAJO	MEDIO	ALTO
			→ IMPACTO		

Nota. Sánchez (2015)

Para determinar el nivel de riesgo de los hallazgos se realiza un mapeo entre la probabilidad y el impacto, análisis realizado acorde a la tabla siguiente:

Tabla 15

Nivel de riesgos de hallazgos encontrados en la ETI.

Nro	HALLAZGOS	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
1	No se dispone de recursos adecuados y suficientes relacionadas con I&T (personas, procesos y tecnología)	Alta	Alto	Muy alto
2	No se dispone de un Plan de Innovación Tecnológica	Alta	Medio	Alto
3	El presupuesto asignado a TI es sumamente bajo y no existe una optimización de costes.	Alta	Alto	Muy alto

Nro	HALLAZGOS	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
4	No existen planes formales de planificación y de desarrollo profesional para fomentar el desarrollo de competencias y las oportunidades para el avance personal	Alta	Medio	Alto
5	La monitorización de los productos y servicios de I&T no se encuentra correctamente documentada	Alta	Medio	Alto
6	No existe un sistema de gestión de la calidad	Alta	Alto	Muy alto
7	No se registran datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa	Alta	Alto	Muy alto
8	No existe un sistema de gestión de seguridad de la información (SGSI)	Alta	Alto	Muy alto
9	No existe una estrategia de gestión de los datos	Alta	Alto	Muy alto
10	No se realiza desarrollo a nivel zonal, solo se puede realizar desarrollo desde nivel central.	Alta	Medio	Alto
11	No están definidos los cambios de emergencia y no existe un procedimiento documentado sobre un cambio de emergencia.	Alta	Bajo	Medio
12	No está establecido un modelo de la configuración y no existe	Alta	Bajo	Medio

Nro	HALLAZGOS	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
	un repositorio de configuración.			
13	El personal que conforma el área de informática no cuenta con capacitación para la gestión de proyectos de TI.	Alta	Medio	Alto
14	No existe el Plan de Continuidad del Negocio	Alta	Alto	Muy alto

De los 14 hallazgos encontrados, 7 tienen un nivel muy alto de riesgo, 5 un nivel alto y 2 de nivel de riesgo medio, con porcentajes que se presentan en la tabla siguiente:

Tabla 16

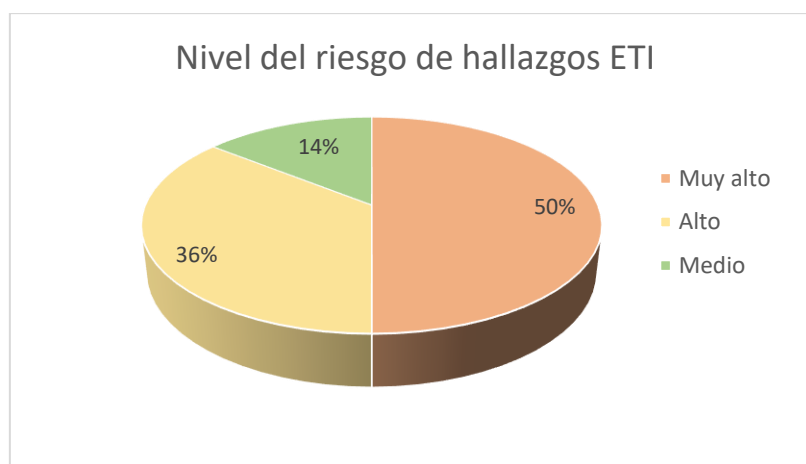
Porcentaje de niveles de riesgo de los hallazgos.

Nivel	Hallazgos	Porcentaje
Muy alto	7	50%
Alto	5	36%
Medio	2	14%

En la imagen siguiente se representa de forma gráfica los resultados obtenidos:

Figura 16

Porcentajes de niveles de riesgo de hallazgos de ETI



Nota: Autor

Como se puede observar el porcentaje de hallazgos que se encuentran en el nivel muy alto es del 50% lo que implica que el impacto en la institución es significativo, un 36% en alto y un 14% en medio.

Capítulo 4: Informe De La Auditoría

Informe Ejecutivo

Introducción

La Coordinación Zonal 1 – Salud fue creada en el año 2012, es una de las coordinaciones que conforman el Ministerio de Salud Pública, su misión es coordinar, controlar y planificar en la zona las acciones referentes a vigilancia de la Salud pública, de la vigilancia y control sanitario, la provisión de servicios de atención individual, prevención de enfermedades, promoción de la salud e igualdad, la gobernanza de salud, y participación social, modelo de atención y, redes pública y complementaria de salud (de Gestión Organizacional), está ubicada en la ciudad de Ibarra y corresponde la gestión de las provincias Imbabura, Carchi, Sucumbíos y Esmeraldas.

La Coordinación Zonal se encuentra constituida por distritos que son entidades administrativas y a su vez los distritos cuentan con unidades operativas que son los centros de salud, hospitales, etc. En la Coordinación Zonal 1 existen 9 direcciones zonales denominadas procesos, procesos agregadores de valor, procesos de apoyo y procesos de asesoría, las Direcciones son: Provisión y Calidad de los Servicios de Salud, Gobernanza de la Salud, Promoción de la Salud, Vigilancia de la Salud, Administrativo Financiero, Asesoría Jurídica, Comunicación, Planificación y Tecnologías de la Información, cada dirección o unidad cuenta con un responsable zonal de la unidad, dentro del Administrativo Financiero se encuentran las unidades de Talento Humano, Financiero y Administrativo.

La Coordinación Zonal 1 – Salud no cuenta con un Plan Estratégico Institucional PEI propio, ya que se basan a lo establecido desde nivel central del Ministerio de Salud Pública, en él se establecen los siguientes objetivos:

(OB1) Incrementar la Gobernanza en el Sistema Nacional de Salud.

(OB2) Incrementar la calidad de la vigilancia y control sanitario en el Sistema Nacional de Salud.

(OB3) Incrementar entornos y prácticas saludables con enfoque de derechos, de género, intercultural e intergeneracional a nivel nacional.

(OB4) Incrementar el acceso a servicios de salud de calidad, integrales integrados y continuos en el Ministerio de Salud Pública.

(OB5) Incrementar la calidad y calidez de las prestaciones de servicios de salud en el Ministerio de Salud Pública.

(OB6) Incrementar la investigación científica en salud.

(OB7) Incrementar la gestión oportuna y calidad de la información enfocada en las necesidades de la población para el Sistema Nacional de Salud sobre el desarrollo de las TICs.

(OB8) Incrementar la eficiencia institucional en el Ministerio de Salud Pública.

(OB9) Incrementar el desarrollo del talento humano en el Ministerio de Salud Pública.

(OB10) Incrementar el uso eficiente del presupuesto en el Ministerio de Salud Pública.

Declaración de Propósito de Alto Nivel

El trabajo desarrollado se concretó en la evaluación técnica informática en base al marco referencia COBIT 2019, aplicando un modelo en cascada para determinar los procesos críticos a ser evaluados, de estos procesos se selecciona las actividades más importantes, las que fueron analizadas en la presente evaluación técnica.

Área de TI Auditada

El área evaluada es la unidad de Tecnologías de la Información de la Coordinación Zonal 1 – Salud, su infraestructura, sus productos y servicios brindados.

Resumen Ejecutivo

El presente informe contiene alcance, los objetivos, la metodología y los resultados de la Evaluación técnica informática en base de riesgos de la Coordinación Zonal 1 – Salud, utilizando el Marco de Referencia COBIT 2019, con la intención de presentar finalmente un conjunto de recomendaciones pertinentes y relevantes para conseguir la mejora en la administración de las Tecnologías de la Información y Comunicación (TIC) de la Institución y lograr que éstas tecnologías aporten significativamente a la consecución de los objetivos institucionales en forma eficaz y efectiva.

Se ha tomado como criterio de referencia dos tipos de normas; la primera referida al ámbito internacional de la administración de las TIC, como es el caso de COBIT 2019 y una segunda fundamental en las instituciones públicas que es la normativa de la Contraloría General del Estado CGE.

El informe contiene los hallazgos de acuerdo con los dominios de COBIT previamente seleccionados respecto a: evaluar, dirigir y supervisar (EDM) que corresponde a los objetivos de gobernanza dirigidos a la alta gerencia; alinear, planificar y organizar (APO) que aborda la organización general, la estrategia y las actividades de apoyo para TI; construir, adquirir e implementar (BAI) que trata la definición, adquisición e implementación de soluciones de TI y su integración en los procesos comerciales; entregar, servicio y soporte (DSS) que aborda la entrega operativa y el soporte de los servicios de TI, incluida la seguridad.

Cada una de las observaciones encontradas contiene en primer lugar, el criterio de referencia normativo ya sea de la norma COBIT 2019 o de las Normas

Técnicas de la Contraloría (NTC), posteriormente se detalla las condiciones encontradas de la situación actual de la Unidad de Tecnologías de la Información, luego se establece la causa por la que se produce la condición actual y el efecto o impacto en la institución por la deficiencia encontrada. Finalmente se presentan las recomendaciones respectivas para que el proceso observado sea mejorado.

El objetivo de la Evaluación Técnica Informática es determinar de manera formal la situación actual de la unidad de Tecnologías de la Información, evidenciar los riesgos existentes en la unidad, demostrar el cumplimiento o no de las normativas vigentes que rigen a la institución y el apoyo brindado por la unidad de TI al cumplimiento de los objetivos y estrategias institucionales, para posteriormente emitir las recomendaciones respectivas para mitigar los hallazgos encontrados.

La Evaluación Técnica Informática ETI ha permitido determinar que respecto al dominio evaluar, dirigir y supervisar (EDM), cuyo objetivo de gobierno número 4 es asegurar la optimización de recursos, que no se dispone de recursos adecuados y suficientes relacionadas con TI (personas, procesos y tecnología), lo que impide desarrollar capacidades para hacer frente a las necesidades actuales y futuras de la institución.

Respecto al dominio alinear, planificar y organizar (APO), es importante contar en la institución con un modelo de gestión en donde se encuentre documentando principalmente el Plan Estratégico Institucional PEI, el Plan Estratégico de TI, el Plan Operativo de TI, seguidamente de un Plan de Innovación Tecnológica, planes formales de planificación y de desarrollo profesional, un sistema de gestión de seguridad de la información SGSI, proyectos de manera formal, entre otros, de esta manera gestionar adecuadamente el presupuesto de acuerdo con las posibilidades de la institución.

Al existir directrices desde nivel central del Ministerio de Salud que no permiten el desarrollo a nivel zonal, restringe un desarrollo íntegro del dominio construir, adquirir

e implementar (BAI), limita las posibilidades de la unidad de TI para solventar las necesidades de la institución y la optimización de procesos, a pesar de ello, acogiéndose a las normativas existentes la unidad de TI ha brindado varios servicios, sin embargo, es necesario contar con procedimientos y procesos documentados adecuadamente tanto en la construcción, adquisición e implementación.

La institución no cuenta con un Plan de Continuidad del Negocio y tampoco un Plan de Continuidad de TI, por lo que la institución no está preparada para protegerse ante posibles incidentes que puedan afectar la capacidad operativa, lo que restringe el cumplimiento del dominio DSS que corresponde la entrega de servicios y soporte.

La unidad de TI de la Coordinación Zonal 1 – Salud requiere una reestructuración técnica importante que debería ser apoyada desde nivel central al ser la institución parte del Ministerio de Salud Pública y estar bajo su dependencia, de tal forma que aporte de una manera más afectiva al cumplimiento de los objetivos institucionales. Aprovechar el proceso de reestructuración que debe cumplir el Ministerio de Salud por las fusiones realizadas, en este caso de la Coordinación Zonal 1 que era una entidad netamente administrativa con el distrito 10d01 que era una entidad operativa, así evidenciar las necesidades reales de la institución respecto a las Tecnologías de la Información, se establezcan las bases, políticas, directrices y lineamientos que permitan que la unidad de TI cumpla las prácticas de gestión de un estándar a nivel internacional como es COBIT, las Normas de Control Interno de la Contraloría y por ende apalanquen el cumplimiento de los objetivos institucionales.

Alcance de la Evaluación Técnica Informática

De acuerdo con el Oficio Nro. MSP-CZONAL1-2021-0039-O suscrito por el Espc. Rennzo Giovanni Vásquez Vaca COORDINADOR ZONAL 1 – SALUD que autoriza el desarrollo del proyecto de tesis "EVALUACIÓN TÉCNICA INFORMÁTICA

EN BASE DE RIESGOS DE LA COORDINACIÓN ZONAL 1 – SALUD, UTILIZANDO EL MARCO DE REFERENCIA COBIT 2019” se realizó una Evaluación Técnica Informática a la unidad de TI, desde el mes de enero del 2021 a febrero del 2021. La evaluación se orienta a la aplicación de la cascada de metas de COBIT2019 para determinar los procesos críticos a ser evaluados en la institución.

La Evaluación Técnica Informática se realizó de acuerdo con los Estándares de Auditoría y Aseguramiento de SI, los Lineamientos de Auditoría y Aseguramiento de SI emitidos por ISACA, COBIT 2019 y las Normas de Control Interno de la Contraloría General del Estado. Esas normas requieren que la auditoría se planifique y se ejecute para obtener evidencia suficiente, relevante y válida para proporcionar una base razonable para las conclusiones, opiniones y hallazgos.

La Evaluación Técnica Informática se limitó a la selección de los procesos a ser evaluados mediante la cascada de metas de COBIT, iniciando con un análisis entre las objetivos y estrategias de la institución y las metas empresariales de COBIT, de donde se obtiene las metas corporativas de COBIT, las mismas que se analizan con las metas de TI de COBIT, dando como resultado la Metas Corporativas de TI, estas últimas se analizan frente a los procesos de COBIT y se determina los Procesos Corporativos de COBIT, que son los procesos relevantes para la realidad de la institución, dando como resultado 14 de los 40 procesos establecidos en COBIT los mismos que fueron respectivamente evaluados.

Objetivos de la Evaluación Técnica Informática

Los objetivos de la Evaluación Técnica Informática son: seleccionar los procesos críticos de la institución para determinar el cumplimiento o no de las prácticas de gestión y actividades establecidas en el Marco de Referencia COBIT 2019, con ello identificar los posibles riesgos potenciales, determinar si se cumple con la normativa legal vigente que rige en el sector público, evaluar si se dispone de recursos adecuados y suficientes relacionadas con TI (personas, procesos y

tecnología), es decir, determinar la situación actual de la unidad de TI mediante los hallazgos encontrados y emitir las recomendaciones pertinentes que ayuden a mitigar los riesgos encontrados y permitan mejorar los servicios brindados por la dirección, así como la obtención posterior de posibles certificaciones

Metodología de la Evaluación Técnica Informática

Planificación de la Evaluación Técnica Informática

Para determinar el alcance y los objetivos de la evaluación, se realizaron algunos pasos previos (planificación de la auditoría), que incluyeron la obtención, el registro y comprensión de la misión de la Coordinación Zonal 1 - Salud, las operaciones relevantes y la tecnología de apoyo. Se identificaron los requisitos operativos, legales, reglamentarios y la infraestructura de TI de la organización auditada al revisar la documentación relevante, realizar cuestionarios y entrevistas con la administración auditada. Se realizaron visitas en situ, a las áreas operativas de TI y se realizó una evaluación de riesgos de alto nivel.

La planificación de auditoría incluyó:

- Obtención y revisión de políticas y procedimientos
- Obtención y revisión de contratos con terceros.
- Identificación de factores críticos de éxito para operaciones de TI de misión crítica.
- Identificación de criterios de auditoría, evaluación de la materialidad e idoneidad de los controles establecidos.

Se desarrollaron objetivos de la evaluación en relación con los objetivos operativos y de control identificados y se desarrolló la estrategia de la evaluación en relación con el alcance y los objetivos planteados.

Ejecución de la Evaluación Técnica Informática

La evaluación se realizó de acuerdo con los Estándares de Auditoría y Aseguramiento de SI y los Lineamientos de Auditoría y Aseguramiento de SI emitidos por ISACA y prácticas de la industria generalmente aceptadas. Los criterios de auditoría que se utilizaron en la evaluación incluyeron políticas y procedimientos de gestión, Normas de Control Interno de la Contraloría General del Estado, Ley Orgánica de Educación Intercultural, Reglamento General a la Ley Orgánica de Educación Intercultural, Ley Orgánica de Transparencia y acceso a la Información Pública y pautas de control de gestión, que se describen en COBIT®, emitido por ISACA.

Resultados o Hallazgos de la Evaluación Técnica Informática

El propósito de esta sección es proporcionar una explicación detallada de los resultados de la evaluación, recomendaciones y respuestas de la gerencia, agrupadas en base a los dominios de COBIT V 2019:

Evaluar, Dirigir y Monitorear EDM

Observación N° 1:

- No se dispone de recursos adecuados y suficientes relacionadas con I&T (personas, procesos y tecnología)

Criterio:

- COBIT V2019 EDM04 - Asegurar la optimización de recursos: “Partiendo de las estrategias actuales y futuras, examinar las posibles opciones para proporcionar recursos relacionados con I&T (recursos tecnológicos, financieros y humanos), y desarrollar capacidades para hacer frente a las necesidades actuales y futuras (incluidas opciones de abastecimiento).”

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad Administrativa Financiera menciona que: “Para conocer si los recursos asignados a las TI son suficientes, se lo realiza analizando el porcentaje de ejecución presupuestaria” (Evidencia Nro. AF-CUE02-ADM), es decir, únicamente se controla el porcentaje de ejecución más no si es lo necesario o no.
- En los cuestionarios realizados, el Coordinador Zonal menciona: “No se han emitido por parte de la Coordinación Zonal 1 – Salud directrices de arquitectura empresarial, existen arquitecturas definidas desde nivel central del Ministerio de Salud, pero no se ejecutan por varias razones, entre ellas, presupuesto, apoyo político para implementar cambios” (Evidencia Nro. AF-CUE01-COO).
- En los cuestionarios realizados, el responsable zonal de la unidad de Planificación menciona: “No existen métricas definidas para la gestión de recursos” (Evidencia Nro. AF-CUE03-PLA).
- En los cuestionarios realizados, el responsable zonal de la unidad de Talento Humano menciona que: “Si existe una brecha de recursos humanos en TI” (Evidencia Nro. AF-CUE05-TH).
- En los cuestionarios realizados, el responsable zonal de la unidad de Tecnologías de la Información menciona que: “Los recursos asignados no a TI no son suficientes” (Evidencia Nro. AF-CUE04-TIC).

Causa:

- Se realiza la proforma presupuestaria de TI en base a los techos presupuestarios y directrices de nivel central y no acorde a las necesidades reales de la unidad.
- Falta de apoyo político para implementar cambios.
- Falta de recursos para cubrir la brecha de TI existente.

Efecto:

- Impide desarrollar capacidades para hacer frente a las necesidades actuales y futuras de la institución.

Recomendación N° 1:

- A la unidad de TI, realizar un análisis detallado de los recursos necesarios en la unidad de TI (personas, procesos y tecnología) y comunicar al nivel directivo, en este caso al Coordinador Zonal.
- Al Coordinador Zonal, elevar los documentos generados por la unidad de TI respecto a los recursos faltantes en la unidad, hacia el nivel central, a fin de evidenciar las necesidades al MSP.

Alinear, Planificar y Organizar APO

Observación N° 2:

- No se dispone de un Plan de Innovación Tecnológica

Criterio:

- COBIT V5 2019 APO.04 - Crear un entorno favorable que conduzca a la innovación: “Crear un entorno favorable que conduzca a la innovación, señala: Crear un plan de innovación que incluya el apetito al riesgo, un presupuesto propuesto para iniciativas de innovación y objetivos de innovación.”

Condición:

- En los cuestionarios realizados, el Coordinador Zonal menciona que: “Es muy importante el desarrollo tecnológico, sería un gran apoyo para la institución. Si hay concienciación sobre el tema, se conoce y evidencia las maravillas tecnológicas y como aportan a la sociedad, sin embargo, la limitante es el presupuesto. No existe en la Coordinación Zonal 1 un comité de TI para investigación” (Evidencia Nro. AF-CUE01-COO)

- En los cuestionarios realizados, el responsable de la unidad de TI menciona que: “No existe un Plan de Innovación de TI. En la Coordinación Zonal no existe programas a los cuales presentar ideas innovadoras, pero si hay un proyecto a nivel central que se llama SISALUD. No existe un comité de Tecnología encargado de investigar las tendencias tecnológicas emergentes” (Evidencia Nro. AF-CUE04-TIC)
- En los cuestionarios realizados, el responsable zonal de la unidad Administrativa Financiera menciona que: “No existe un presupuesto asignado para el tema de innovación, el único presupuesto para proyectos se recibe de SISALUD” (Evidencia Nro. AF-CUE02-ADM)

Causa:

- Brecha de Talento Humano de TI como para tener suficiente personal para formar un comité para investigación.
- Presupuesto limitante para ejecución del plan de innovación.
- La asignación de varias funciones al personal de TI limita que se pueda realizar actividades enfocadas a la innovación tecnológica.
- No existe un presupuesto específico para innovación.

Efecto:

- La institución desconoce las acciones a tomar ante posibles cambios tecnológicos.
- Poca innovación tecnológica en la institución.
- No se satisface las necesidades institucionales conforme a los avances tecnológicos.
- No tiene ventaja competitiva ante otras instituciones.

Recomendación N° 2:

- A la unidad de TI, se recomienda crear el Plan de Innovación Tecnológica, para sustentar la toma de decisiones a nivel gerencial a favor de TI, gestionar los recursos necesarios que apoyen la ejecución del plan y así permitir que la institución se encuentre preparada para afrontar los cambios tecnológicos. Crear el comité de Tecnologías encargado de investigar las tendencias tecnológicas emergentes.
- A la Coordinación Zonal, solicitar a nivel central un presupuesto destinado para el tema de innovación.

Observación N° 3:

- El presupuesto asignado a TI es sumamente bajo y no existe una optimización de costes.

Criterio:

- COBIT V5 2019 APO06.02 - Gestionar el presupuesto y los costes: “Asignar recursos empresariales y de TI (incluidos proveedores de servicios externos) dentro de las asignaciones presupuestarias de alto nivel para programas, servicios y activos relacionados con I&T.”
- NTCI 402 Administración Financiera - PRESUPUESTO: “Las entidades del sector público delinearán procedimientos de control interno presupuestario para la programación, formulación, aprobación, ejecución, evaluación, clausura y liquidación del presupuesto institucional; se fijarán los objetivos generales y específicos en la programación de ingresos y gastos para su consecución en la ejecución presupuestaria y asegurar la disponibilidad presupuestaria de fondos en las asignaciones aprobadas”.

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad la unidad Administrativa Financiera señala: “El porcentaje de asignación presupuestaria

es de 0,5 % del valor total asignado de inversión a través del proyecto de nivel central SISALUD. No existe una clasificación para identificar todos los elementos de costes relacionados con la I&T. No hay una optimización de costes operativos recurrentes. No existe un estudio de costes de TI en los servicios” (Evidencia Nro. AF-CUE02-ADM).

- En los cuestionarios realizados, el responsable zonal de la unidad la unidad de Planificación señala: “Hay ciertos proyectos que por factores externos no se cumplen a cabalidad y se ajusta los presupuestos de acuerdo con la necesidad de la institución, se generan reformas presupuestarias desde el Financiero. Se monitoriza los montos ejecutados, más no la efectividad de todos los aspectos del presupuesto. Se presupuesta en base a historiales de años pasados, tiene mucha influencia los techos presupuestarios establecidos desde nivel central, lo que limita la planificación presupuestaria real. No existe un modelo documentado de asignación de costes, se realiza la asignación de acuerdo con el requerimiento del proceso. No existe un análisis del ROI ya que al ser una entidad pública se centra más en la calidad del servicio de salud” (Evidencia Nro. AF-CUE03-PLA).

Causa:

- Se prioriza la asignación presupuestaria para procesos que están directamente relacionados al tema de salud, como es la Dirección Zonal de Provisión y Calidad.
- No se ha evidenciado la necesidad de realizar un análisis de costes operativos recurrentes.
- Se establece techos presupuestarios desde nivel central, lo que limita la solicitud un presupuesto de acuerdo con las necesidades.
- Se presupuesta en base a historiales de años anteriores lo que limita una planificación presupuestaria acorde a las necesidades actuales.

- Se evalúa la gestión de los recursos únicamente respecto a la ejecutado, más no a lo efectividad de dichos recursos.

Efecto:

- No se realiza mejoras significativas a nivel tecnológico ya que la asignación presupuestaria no llega ni al 1%.
- No se plantea soluciones a nivel tecnológico que permitan la optimización en procesos recurrentes.
- Mejora desigualitaria entre las áreas de provisión con las áreas de TI.
- No se asigna el presupuesto real necesario por la unidad de TI, ya que desde la elaboración de la proforma presupuestaria se establece techos.
- No se evidencia el beneficio económico de inversiones de TI.

Recomendación N° 3:

- Se realice una asignación de recursos en un mayor porcentaje para la unidad de TI.
- Se realice un análisis de costes relacionados con TI.
- Se realice un presupuesto real de las necesidades de TI y no únicamente acorde a los techos presupuestarios establecidos desde nivel central.
- Se realice un análisis del ROI de los proyectos de TI ejecutados para evidenciar el impacto de TI en la institución.

Observación N° 4:

- No existen planes formales de planificación y de desarrollo profesional para fomentar el desarrollo de competencias y las oportunidades para el avance personal

Criterio:

- COBIT V5 2019 APO07.04 - Evaluar y reconocer/recompensar el rendimiento laboral de los empleados: “Proporcionar planes formales de planificación y de desarrollo profesional conforme a los resultados del proceso de evaluación para fomentar el desarrollo de competencias y las oportunidades para el avance personal y para reducir la dependencia de individuos clave. Proporcionar coaching a los empleados sobre el rendimiento y la conducta cuando sea apropiado.
- NTCI 200.03 - Políticas y prácticas de talento humano: “La administración del talento humano, constituye una parte importante del ambiente de control, cumple con el papel esencial de fomentar un ambiente ético desarrollando el profesionalismo y fortaleciendo la transparencia en las prácticas diarias. Esto se hace visible en la ejecución de los procesos de planificación, clasificación, reclutamiento y selección de personal, capacitación, evaluación del desempeño y promoción y en la aplicación de principios de justicia y equidad, así como el apego a la normativa y marco legal que regulan las relaciones laborales.”
- NTCI 200.06 - Competencia profesional: “Los directivos de la entidad, especificarán en los requerimientos de personal, el nivel de competencias necesario para los distintos puestos y tareas a desarrollarse en las áreas correspondientes. Así mismo, los programas de capacitación estarán dirigidos a mantener los niveles de competencia requeridos.”

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad de Talento Humano señala que: “No existen planes de planificación y desarrollo profesional y no se proporciona coaching a los empleados sobre el rendimiento y la conducta. Se tiene convenios de prácticas con institutos tecnológicos, pero no con otro tipo de instituciones públicas o privadas que apoyen las necesidades empresariales de TI. No existe un plan de respaldo de personal.

No se tiene identificado las brechas entre las habilidades requeridas y las disponibles del personal de TI. No se proporciona por parte de la institución acceso a los repositorios de conocimiento para respaldar el desarrollo de habilidades y competencias. No se tiene identificado las carencias del personal de TI y tampoco proporcionado las recomendaciones al nivel respectivo” (Evidencia Nro. AF-CUE05-TH).

Causa:

- La mayoría del personal corresponde a contratos son ocasionales, por lo tanto, no se prioriza elaborar planes de planificación y desarrollo profesional.
- Dificultad para ejecutar convenios con instituciones educativas de tercer nivel por burocracia en trámites.
- Escasos recursos para proporcionar acceso a repositorios de conocimiento para respaldar el desarrollo de habilidades y competencias.
- No se prioriza realizar evaluaciones habilidades y carencias del personal.

Efecto:

- No existe un desarrollo profesional del personal.
- Personal poco motivado en rendimiento y conducta.
- No existe apoyo externo de instituciones académicas especializadas o empresas privadas que aporten a las necesidades empresariales de TI.
- Inconveniente para la continuidad del negocio al no existir un plan de respaldo del personal.
- No se capacita de acuerdo con las carencias existentes.

Recomendación N° 4:

- La unidad de Talento Humano debe elaborar planes de planificación y desarrollo profesional.

- Proporcionar continuamente coaching a los empleados sobre el rendimiento y la conducta.
- Realizar convenios con instituciones que apoyen las necesidades empresariales de TI.
- Elaborar el plan de respaldo del personal.
- Identificar las brechas entre las habilidades requeridas y las disponibles del personal de TI

Observación N° 5:

- La monitorización de los productos y servicios de I&T no se encuentra correctamente documentada

Criterio:

- COBIT V5 2019 APO09.04 - Monitorizar y reportar los niveles de servicio: “Acordar planes de acción y remediaciones para cualquier problema de rendimiento o tendencias negativas.”
- NTCI 410-12 Administración de soporte de tecnología de información: “Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos.”
- NTCI 410-13 Monitoreo y evaluación de los procesos y servicios: “Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.”

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad de TI señala que: “Se tiene identificado las áreas de mejora de los servicios de TI existentes, pero no en un documento formal, se lo identifica y revisa en las reuniones

formales del área, pero tampoco existen actas de reunión. Se conoce la capacidad de los servicios, pero no se encuentra documentado, no se tiene estudios de la demanda futura, pero se conoce una aproximación estimada. Existe un listado de los servicios brindados, más no un catálogo como tal. No existe planes de acción y remediaciones para cualquier problema de rendimiento o tendencias negativas en los servicios” (Evidencia Nro. AF-CUE04-TIC)

Causa:

- La asignación de varias funciones al personal de TI limita que se pueda documentar adecuadamente todas actividades los productos y servicios.
- Se prioriza la elaboración de los documentos de respaldo de los productos del Estatuto de la unidad de TI.

Efecto:

- Se dificulta sustentar las áreas de mejoras de TI ya que no se tiene estudios de la demanda futura de los servicios.
- No se cuenta con un catálogo de servicios de TI.
- Respuesta ante tendencias negativas en los servicios no definida.

Recomendación N° 5:

- Identificar las áreas de mejora de los servicios de TI en un documento formal.
- Documentar la capacidad actual de los servicios de TI.
- Realizar estudios de la demanda futura de los servicios de TI.
- Elaborar el catálogo de servicios de TI.
- Elaborar un plan de acción y remediaciones para cualquier problema de rendimiento o tendencias negativas en los servicios

Observación N° 6:

- No existe un sistema de gestión de la calidad

Criterios:

- COBIT V2019 APO11.01 - Establecer un sistema de gestión de calidad (SGC):
“Asegurar que el marco de control de I&T y los procesos empresariales y de TI, incluyen una estrategia estándar, formal y continua con respecto a la gestión de la calidad que está alineada con los requisitos de la empresa. Dentro del marco de control de I&T y los procesos empresariales y de TI, identificar los requisitos y criterios de calidad (p. ej. conforme con los requisitos legales y los requisitos de los clientes).”
- NTCI 401-03 Supervisión: “La supervisión de los procesos y operaciones se los realizará constantemente para asegurar que se desarrollen de acuerdo con lo establecido en las políticas, regulaciones y procedimientos en concordancia con el ordenamiento jurídico; comprobar la calidad de sus productos y servicios y el cumplimiento de los objetivos de la institución”.

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad de Planificación menciona que: “No existe un sistema de gestión de la calidad documentado, pero todo se rige en bases a los reglamentos, políticas que implica ser una institución pública. No se realiza revisiones de calidad por procesos, la responsabilidad recae únicamente en el líder de cada unidad” (Evidencia Nro. AF-CUE03-PLA).
- En los cuestionarios realizados, el responsable zonal de la unidad de Provisión de los servicios menciona que: “No se obtiene opiniones de los clientes de forma periódica, se obtiene las opiniones a través de la ventanilla de las instituciones cuando los usuarios ingresan oficios de inconformidades. No se ha cuantificado los beneficios y costes de las certificaciones de calidad. No se

tiene identificado ejemplos de procesos de entrega de calidad excelente”

(Evidencia Nro. AF-CUE06-PRO)

- En los cuestionarios realizados, el responsable zonal de la unidad de TI menciona que: “No existe una plataforma para compartir buenas prácticas y captar información sobre los defectos y errores para permitir el aprendizaje a partir de ellos” (Evidencia Nro. AF-CUE04-TIC).

Causa:

- La gestión de la calidad está enfocada al área de Provisión de Servicios que es el proceso más importante de la institución y no se considera la gestión de la calidad en los demás procesos.
- No se visualiza la importancia cuantificar los beneficios y costes de las certificaciones de calidad y como aportan a la institución.
- Infraestructura de TI limitada para crear una plataforma para compartir buenas prácticas y captar información sobre los defectos y errores para permitir el aprendizaje a partir de ellos.
- No existe un análisis comparativo de los resultados de benchmarks de calidad con los datos históricos internos.

Efecto:

- Se crea una gestión de calidad enfocada únicamente al paciente y se maneja desde la unidad de Provisión, no existe una gestión de calidad integral como institución.
- No se establecen métricas la evaluación, gestión de la calidad en cada uno de los procesos de la institución como es: Gobernanza, Administrativo Financiero, Promoción, TI entre otros.
- No se enfoca la institución en la obtención de certificaciones de calidad y cuantificar los beneficios que ello implica.

Recomendación N° 6:

- Establecer un Sistema de Gestión de la Calidad SGC institucional y definir los roles y responsabilidades para su gestión en la estructura organizativa.
- Cuantificar los beneficios y costes de las certificaciones de calidad.
- Realizar continuas revisiones de la calidad por procesos en base a lo establecido en el SGC.
- Establecer plataformas de TI que permitan compartir buenas prácticas y captar información sobre los defectos y errores para permitir el aprendizaje a partir de ellos
- Identificar ejemplos de procesos de entrega de calidad.

Observación N° 7:

- No se registran datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa

Criterio:

- COBIT V2019 APO12.02 Analizar el riesgo: “Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa”.
- NTCI 410-11 Plan de contingencias: “Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento”.

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad de TI menciona: “No se registran datos relevantes y significativos relacionados con

los riesgos de I&T en el entorno operativo interno y externo de la empresa, que se elabora informes, pero no se cuenta con una bitácora o herramienta similar. Los datos de eventos de riesgo que han causado o podrían causar impacto en el negocio están documentados en informes, pero no se lleva un registro de ellos. No se realiza periódicamente análisis de eventos y factores de riesgo. No existe un Plan de acción de riesgos” (Evidencia Nro. AF-CUE04-TIC).

Causa:

- La asignación de varias funciones al personal de TI limita que se pueda documentar adecuadamente todas actividades sobre la gestión de riesgos, ya que se ejecuta varias actividades, pero no se encuentra documentado adecuadamente.
- Se prioriza la elaboración de los documentos de respaldo de los productos del Estatuto de la unidad de TI.
- No existe una concientización sobre la importancia de la gestión del riesgo.

Efecto:

- Las actividades de gestión del riesgo las realiza el funcionario asignado, únicamente en base a su criterio y no con una metodología y documentos de respaldo.
- Al no contar con un registro detallado de datos relevantes al riesgo de TI, se dificulta el sustento para la toma de decisiones de mejoras a nivel de TI y evitar posibles impactos de los riesgos existentes.
- Al surgir un evento fortuito y no existir un Plan de acción de riesgos se actúa bajo criterio del funcionario responsable.
- No se realiza de manera formal la gestión de los riesgos.

Recomendación N° 7:.

- A la unidad de TI: Llevar un registro de datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la institución.
- Definir los escenarios de riesgo y categorías de impacto y probabilidad.
- Registra datos de eventos de riesgo que han causado impacto en el negocio y analizar los datos históricos de riesgo de TI.
- Realizar un análisis periódico de eventos y factores de riesgo.
- Elaborar el Plan de acción de riesgos.
- Elaborar un conjunto de propuestas de proyectos para reducir el riesgo.

Observación N° 8:

- No existe un sistema de gestión de seguridad de la información (SGSI).

Criterio:

- COBIT V2019 APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI): “Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología. Incluir detalles y justificación de las exclusiones del alcance.
- NTCI 410-10 Seguridad de tecnología de información: “La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos”.

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad de TI menciona que: “No existe un sistema de gestión de seguridad de la información

(SGSI), no existe un Plan de tratamiento de riesgos de seguridad de la información y tampoco una propuesta” (Evidencia Nro. AF-CUE04-TIC).

- En los cuestionarios realizados, el responsable zonal de la unidad de Talento Humano menciona que: “No se realiza capacitaciones, programas de formación y concienciación sobre seguridad de la información y privacidad, pero se envía correos con recordatorios” (Evidencia Nro. AF-CUE05-TH).

Causas:

- La asignación de varias funciones al personal de TI limita que se pueda documentar adecuadamente todas actividades sobre la gestión de la seguridad, ya que se ejecuta varias actividades, pero no se encuentra documentado adecuadamente.
- Se prioriza la elaboración de los documentos de respaldo de los productos del Estatuto de la unidad de TI.
- No se ha evidenciado la necesidad de realizar capacitaciones continuas de formación sobre la seguridad de la información y privacidad.

Efectos:

- Las actividades de gestión de la seguridad las realiza el responsable asignado únicamente en base a su criterio y no con un documento de respaldo.
- No se realiza de manera formal un tratamiento de los riesgos de seguridad de la información.
- Personal de la institución con desconociendo y concienciación sobre la importancia de la seguridad de la información y privacidad.

Recomendación N° 8:

- A la unidad de TI: Establecer y mantener un sistema de gestión de seguridad de la información (SGSI). Establecer el Plan de tratamiento de riesgos de seguridad de la información.

- A la unidad de Talento Humano: Realiza capacitaciones, programas de formación y concienciación sobre seguridad de la información y privacidad.

Observación N° 9:

- No existe una estrategia de gestión de los datos.

Criterio:

- COBIT V2019 APO14.01 Gestionar los datos: “Asegurar que el negocio y la tecnología desarrollan de forma colaborativa la estrategia de gestión de datos de la organización. Asegurar que los objetivos, prioridades y alcance de la gestión de datos reflejen los objetivos empresariales, sean consistentes con las políticas y regulación de gestión de datos y cuenten con la aprobación de todas las partes interesadas”.
- NTCI 410-05 Modelo de información organizacional: “Se deberá generar un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad
- NTCI 410-12 Administración de soporte de tecnología de información: “La Unidad de Tecnología de Información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen”

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad de Planificación menciona que: “No existe una estrategia de gestión de datos, tampoco existe un glosario empresarial y que, si bien se valida la calidad de los datos no existe una estrategia documentada de calidad de los datos, no existe un plan de secuencial de mejora de la calidad de los datos, no existe una

política de depuración de datos y no existe un historial de cambio de datos”
(Evidencia Nro. AF-CUE03-PLA).

- En los cuestionarios realizados, el responsable zonal de la unidad de TI menciona que: “No existe un proceso de gestión de metadatos y no se dispone de un repositorio de data warehouse que proporcione acceso a datos históricos” (Evidencia Nro. AF-CUE04-TIC).

Causa:

- No se ha evidenciado la necesidad de contar con una estrategia de gestión de datos.
- No se ha definido roles y responsabilidad de la gestión de datos de la institución.
- No existe una infraestructura de TI establecida para la gestión de metadatos.

Efecto:

- No existe un repositorio de los datos de la institución, lo que dificulta el acceso oportuno a datos para la toma de decisiones a nivel directivo.
- Los datos de la institución se mantienen en los diferentes computadores de los funcionarios asignados a dichas actividades, lo que pone en riesgo los datos históricos generados.
- Cuando se requiere datos de la institución se debe solicitar indistintamente a cada unidad, es decir, no existe un repositorio donde se consolide los datos de la institución.

Recomendación N° 9:

- A la institución, definir y comunicar la estrategia y los roles y responsabilidades de la gestión de datos de la organización.
- A la unidad de TI, brindar a través de la unidad de TI apoyo tecnológico para la gestión de datos.

Construir, Adquirir e Implementar BAI

Observación N° 10:

- No se realiza desarrollo a nivel zonal, solo se puede realizar desarrollo desde nivel central.

Criterio:

- COBIT V2019 BAI03.12 - Diseñar soluciones conforme a la metodología de desarrollo definida: "Establecer la metodología de desarrollo adecuada y la estrategia organizativa que lleve a cabo la solución propuesta de forma eficaz y eficiente y que sea capaz de satisfacer los requisitos de la empresa, arquitectura y sistema. Adaptar los procesos a la estrategia elegida como corresponda".
- NTCI 410-07 Desarrollo y Adquisición de Software aplicativo: "La Unidad de Tecnología de Información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos"

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad de TI menciona que: "No se realiza desarrollo a nivel zonal, ya que existen directrices de nivel central del MSP que limitan esta actividad, todo lo que es desarrollo se realiza únicamente en la Dirección Nacional de Tecnologías de la Información DNTIC" (Evidencia Nro. AF-CUE04-TIC)

Causa:

- Restricciones de nivel central del MSP para desarrollo a nivel zonal.
- Brecha de personal de TI en la unidad de TI.
- No existe en perfil de desarrollador en la unidad de TI.

Efecto:

- Limita el soporte de TI para la organización.
- No se asegura que la unidad de TI satisfaga en su totalidad a las necesidades de los usuarios en base a los requerimientos planteados por los mismos.
- Limitada automatización de procesos.

Recomendación N° 10:

- A la unidad de TI, documentar mediante un estudio la necesidad de que exista desarrollo a nivel zonal y se plantee los requerimientos de recursos humanos, tecnológicos y económicos necesarios para realizar desarrollo a nivel zonal.

Observación N° 11:

- No están definidos los cambios de emergencia y no existe un procedimiento documentado sobre un cambio de emergencia.

Criterio:

- COBIT V2019 BAI06.02 Gestionar cambios de emergencia. “Definir lo que constituye un cambio de emergencia” y “Asegurar que existe un procedimiento documentado para declarar, evaluar, aprobar inicialmente, autorizar después del cambio y registrar un cambio de emergencia”.
- NTCI 410-11 Plan de contingencias: “Corresponde a la Unidad de Tecnología de Información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado”.

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad de TI menciona que: “Si bien se conoce los cambios de emergencia, no se encuentra

definido en un documento formal, que no existe un procedimiento documentado sobre un cambio de emergencia, que no se elabora informes de estado de los cambios con métricas de rendimiento” (Evidencia Nro. AF-CUE04-TIC).

Causa:

- La asignación de varias funciones al personal de TI limita que se pueda documentar adecuadamente todas actividades sobre los cambios de emergencia.
- No se ha identificado la necesidad de contar con un repositorio de configuración.

Efecto:

- Inconvenientes para ejecutar con eficacia los cambios de emergencia.
- No se garantiza la continuidad de TI en caso de encontrarse ausente la persona encargada de la gestión de cambios de emergencia.

Recomendación N° 11

- A la unidad de TI, realizar un documento formal en donde se defina los cambios de emergencia, documentar los procedimientos sobre los cambios de emergencia, elaborar informes con métricas de rendimiento sobre los cambios realizados.

Observación N° 12:

- No está establecido un modelo de la configuración y no existe un repositorio de configuración.

Criterio:

- COBIT V2019 BAI10.01 Establecer y mantener un modelo de la configuración:
“Definir y acordar el alcance y nivel de detalle sobre la gestión de la

configuración (es decir, qué elementos configurables de servicios, activos e infraestructura incluir)” y “Establecer y mantener un modelo lógico para la gestión de la configuración, incluida la información de los tipos de CI, atributos, tipos de relaciones, atributos de relaciones y códigos de estado”.

- NTCI 410-12 Administración de soporte de tecnología de información:
“Mantenimiento de un repositorio de diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción”.

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad de TI menciona que: “No se tiene definido el alcance y nivel de detalle sobre la gestión de la configuración, no se tiene un repositorio de configuraciones ya que esa información mantiene el responsable de dicha actividad, así como no se revisa formalmente las líneas de referencia de la configuración de un servicio, aplicación o infraestructura” (Evidencia Nro. AF-CUE04-TIC).

Causa:

- No se ha identificado la necesidad de contar con un modelo de configuración.
- La asignación de varias funciones al personal de TI limita que se pueda documentar adecuadamente todas actividades sobre la gestión de la configuración.
- No se ha identificado la necesidad de contar con un repositorio de configuración.

Efecto:

- Gestión de la configuración no homologada, es decir, los cambios se realizan a criterio personal de cada miembro de TI que intervenga.
- Configuraciones no entendibles o desconocidas.

- No se garantiza la continuidad de TI en caso de encontrarse ausente la persona encargada de la gestión de las configuraciones.
- Acceso limitado a los respaldos de configuración al no contar con un repositorio de acceso a todo el equipo de TI.

Recomendación N° 12:

- A la unidad de TI, definir el alcance y nivel de detalle sobre la gestión de la configuración
- Crear un repositorio de configuraciones a donde tenga acceso no solo una persona de la unidad de TI.
- Revisar formalmente las líneas de referencia de la configuración de un servicio, aplicación o infraestructura.

Observación N° 13:

- El personal que conforma el área de informática no cuenta con capacitación para la gestión de proyectos de TI.

Criterio:

- COBIT V2019 BAI11.01 Mantener un enfoque estándar en la gestión de proyectos: “Proporcionar una capacitación en gestión de proyectos adecuada y considerar la certificación para los gestores de proyecto”.
- NTCI 407-06 Capacitación y entrenamiento continuo: “Los directivos de la entidad promoverán en forma constante y progresiva la capacitación, entrenamiento y desarrollo profesional de las servidoras y servidores en todos los niveles de la entidad, a fin de actualizar sus conocimientos, obtener un mayor rendimiento y elevar la calidad de su trabajo”.

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad de TI menciona que: “Por parte de la institución no se ha brindado capacitación para la gestión de proyectos y la institución en la respuesta de documentos de respaldo indica que no se cuenta con certificados de capacitación en proyectos” (Evidencia Nro. AF-CUE05-TH).

Causa:

- No se ha identificado la necesidad de capacitar al personal sobre la gestión de proyectos de TI.
- Carecen de los recursos necesarios para la capacitación.
- Carencia de incentivos al personal por parte de la institución.
- Desconocimiento de los beneficios que aporta la capacitación sobre gestión de proyectos de TI, al desempeño laboral.

Efecto:

- No se incentiva a la creación de nuevos proyectos.
- No se garantiza la adecuada Gestión de los proyectos del área de informática
- No se tiene personal especializado para la gestión de los proyectos del área de informática.

Recomendación N° 13

- A la institución, se recomienda contemplar la asignación de recursos para capacitaciones específicas orientadas al área de tecnología.
- Se recomienda realizar un control de cumplimiento del Plan Anual de Capacitaciones, para verificar su cumplimiento de acuerdo a las necesidades de la unidad de TI.

Entregar, Dar Servicio y Soporte DSS

Observación N° 14:

- No existe el Plan de Continuidad del Negocio

Criterio:

- COBIT V2019 DSS04.03 Gestionar la continuidad: “Definir acciones y comunicaciones de respuesta a incidentes que se deban tomar en caso de interrupción. Definir roles y responsabilidades relacionados, incluida la rendición de cuentas para la política y la implementación”.

Condición:

- En los cuestionarios realizados, el responsable zonal de la unidad de TI menciona que: “No existe un Plan de Continuidad del Negocio y la institución en la respuesta de documentos de respaldo indica que no se cuenta con el Plan Continuidad del Negocio” (Evidencia Nro. AF-CUE04-TIC).

Causa:

- No se ha identificado la necesidad de crear un Plan de Continuidad del negocio.
- Desconocimiento de los beneficios que aporta el Plan de Continuidad del Negocio.
- Falta de planificación y tiempo disponible por parte del personal para elaborar el Plan de Continuidad de TI ya que se prioriza la ejecución de los productos establecidos es el Estatuto Orgánico por Procesos del MSP.

Efecto:

- La institución no está preparada para protegerse ante posibles incidentes que puedan afectar la capacidad operativa.

- La institución no está preparada para recuperar y restaurar las funciones críticas ya sea parcial o totalmente ante posibles eventualidades.
- No se mantenga la funcionalidad de la institución a un nivel aceptable durante una contingencia.

Recomendación N° 14

- A la institución, se recomienda implementar el Plan de Continuidad del Negocio, con el fin aumentar la probabilidad de continuidad de las funciones críticas de la institución ante posibles interrupciones en sus operaciones.

Conclusiones de la Evaluación Técnica Informática

El propósito de esta sección es proporcionar una conclusión general u opinión con respecto a los objetivos de auditoría del trabajo. Comprensiblemente, el trabajo se realizó como un examen con un nivel apropiado de pruebas de auditoría, de acuerdo con todos los estándares de auditoría relevantes y conclusiones basadas en evidencia suficiente, relevante y válida.

La auditoría incluyó políticas y procedimientos de gestión, Normas de Control Interno de la Contraloría General del Estado, Estatuto Orgánico por Procesos del Ministerio de Salud Pública, Ley Orgánica de Transparencia y acceso a la Información Pública y pautas de control de gestión que se describen en COBIT V2019, emitido por ISACA.

- Después de realizar la evaluación Técnica Informática ETI en la unidad de Tecnologías de la Información en la Coordinación Zonal 1 – Salud mediante COBIT 2019, se evidenció que la institución depende de directrices y financiamiento del Ministerio de Salud y Ministerio de Finanzas, por lo tanto, su gestión se encuentra limitada.
- Al evaluar el proceso EDM04 - Asegurar la optimización de recursos, se evidenció que en la unidad de TI no se dispone de recursos adecuados y

suficientes relacionadas con I&T (personas, procesos y tecnología), las limitaciones de recursos al establecer techos presupuestarios desde nivel central, las directrices del MSP, entre otros parámetros, no permiten realizar una asignación presupuestaria real a la unidad.

- Al evaluar el proceso APO04 - Gestionar la innovación, se evidenció que la unidad de TI no dispone del Plan de innovación tecnológica, que sustente la toma de decisiones a nivel gerencial en favor de la unidad, lo que ocasiona que la institución no se encuentra preparada para los avances tecnológicos.
- Al evaluar el proceso APO06 - Gestionar el presupuesto y los costes, se evidenció que el porcentaje asignado a TI es de 0,5% del total de inversión manejado desde el proyecto de nivel central SISALUD, mientras que de gasto corriente de la institución no se asignan para proyectos de TI, lo cual representa un porcentaje sumamente bajo, esto limita a que se realicen mejoras significativas a nivel tecnológico y no exista una optimización de recursos recurrentes.
- Al evaluar el proceso APO07 - Gestionar los recursos humanos, se evidenció que no existen planes formales de planificación y de desarrollo profesional para fomentar el desarrollo de competencias y las oportunidades para el avance personal, debido a que la mayoría del personal se encuentra bajo la modalidad de contrato, esto ocasiona que el personal no se encuentre completamente motivado y capacitado de acuerdo las carencias existentes.
- Al evaluar el proceso APO09 - Gestionar los acuerdos de servicio, se evidenció que la monitorización de los productos y servicios de TI no se encuentra correctamente documentada, esto dificulta la toma de decisiones respecto a las áreas de mejoras de TI y la respuesta ante tendencias negativas en los servicios no está definida.
- Al evaluar el proceso APO11 - Gestionar la calidad, se evidenció que en la institución no existe un sistema de gestión de la calidad integral, está enfocada

únicamente en el área de Provisión de Servicios que es el proceso más importante de la institución, no se establecen métricas la evaluación, gestión de la calidad en cada uno de los procesos de la institución como es: Gobernanza, Administrativo Financiero, Promoción, TI entre otros.

- Al evaluar el proceso APO12 - Gestionar riesgos, se evidenció que no se realiza una gestión documentada del riesgo, no están definidos de escenarios de riesgo y categorías de impacto y probabilidad, no se realiza un registro formal de datos relevantes y significativos relacionados con los riesgos de I&T por lo tanto no cuenta con una gestión formal aun cuando en la institución se realiza algunas actividades operativas para gestionar el riesgos, tampoco existe un Plan de acción de riesgos, lo que dificulta el sustento para la toma de decisiones de mejoras a nivel de TI y evitar posibles impactos de los riesgos existente.
- Al evaluar el proceso APO13 - Gestionar la seguridad, se evidenció que en la institución se cuenta con una persona designada como el Oficial de la Seguridad de la Información quien realiza varias actividades para la gestión de la seguridad, sin embargo, no existe un sistema de gestión de seguridad de la información (SGSI) y las actividades realizadas no se encuentran documentadas adecuadamente de tal manera que soporten las prácticas de gestión del proceso.
- Al evaluar el proceso APO14 - Gestionar los datos, se evidenció que no se realiza gestión de datos en la institución, partimos desde la no existencia de una estrategia de gestión de datos hasta no contar con estrategias de depuración, todos estas actividades si bien se realizan de alguna manera empírica no se encuentra normalizada ni documentada, no existe un repositorio que permita tener acceso a datos históricos ya que los mismos se encuentran en computadores indistintos de los funcionarios de la institución, todo esto

implica que no exista un acceso oportuno a información relevante para la toma de decisiones a nivel directivo.

- Al evaluar el proceso BAI03 - Gestionar la identificación y construcción de soluciones, se constató que en la institución no se realiza desarrollo ya que existen directrices desde nivel central del Ministerio de Salud que limitan dicha actividad, el desarrollo se realiza desde nivel central, esto limita el soporte de TI para la organización ya que no se asegura que la unidad de TI satisfaga en su totalidad a las necesidades de los usuarios en base a los requerimientos planteados por los mismos, además, se limita la automatización de procesos.
- Al evaluar el proceso BAI06 - Gestionar los cambios de TI, se evidenció que no se gestiona adecuadamente los cambios de emergencia, no están definidos los cambios de emergencia y no se encuentra documentado los procedimientos.
- Al evaluar el proceso BAI10 - Gestionar la configuración, se evidenció que en la institución no se cuenta con modelo de la configuración y no existe un repositorio de configuración, lo que implica que en caso de existir incidentes no se garantiza la continuidad de TI en caso de encontrarse ausente la persona encargada de la gestión de las configuraciones.
- Al evaluar el proceso BAI11 - Gestionar los proyectos, se evidenció que el personal de la unidad de TI no se encuentra capacitado en la gestión de proyectos de TI debido a la falta de iniciativa y recursos por parte de la institución en dichas capacitaciones, por lo cual no se puede garantizar una adecuada gestión de los proyectos del área de TI y limita la generación de nuevos proyectos.
- Al evaluar el proceso DSS04 - Gestionar la continuidad, se evidenció que la institución no dispone de un Plan de Continuidad del negocio, debido a la falta de planificación y tiempo disponible por parte del personal para elaborar el Plan de Continuidad de TI ya que se prioriza la ejecución de los productos

establecidos es el Estatuto Orgánico por Procesos del MSP, lo cual sitúa a la institución en un ambiente vulnerable ante posibles eventualidades.

Apéndices

Copia Completa de la Respuesta del Auditado

A continuación, se anexa los documentos de evidencia de acuerdo con el siguiente Índice:

1. Evidencia Nro. AF-CUE01-COO
Cuestionario aplicado al Coordinador Zonal 1 - Salud
2. Evidencia Nro. AF-CUE02-ADM
Cuestionario aplicado al Responsable Zonal Administrativo Financiero
3. Evidencia Nro. AF-CUE03-PLA
Cuestionario aplicado al Responsable Zonal de Planificación
4. Evidencia Nro. AF-CUE04-TIC
Cuestionario aplicado al Responsable Zonal de Tecnologías de la Información
5. Evidencia Nro. AF-CUE05-TH
Cuestionario aplicado al Responsable Zonal de Talento Humano
6. Evidencia Nro. AF-CUE06-PRO
Cuestionario aplicado al Responsable Zonal de Provisión y Calidad de los Servicios
7. Evidencia Nro. AF-ENT01-TIC
Entrevista aplicada al Responsable Zonal de Tecnologías de la Información
8. Evidencia Nro. AF-ENC01-MAS
Encuesta masiva aplicada al personal de la Coordinación Zonal 1 – Salud
9. Evidencia Nro. AF-IDC-01
Solicitud de documentos de respaldo
10. Evidencia Nro. AF-IDC-02
Respuesta de la institución con documentos de respaldo

Capítulo 5: Conclusiones y Recomendaciones

Conclusiones

- El desarrollo de la Evaluación Técnica Informática ETI mediante el Marco de Referencia COBIT 2019 permitió realizar una evaluación integral y sistémica del Gobierno y Gestión de la Coordinación Zonal 1 – Salud determinando que la unidad de TI no cuenta con un Gobierno Empresarial de Tecnologías de la Información GETI.
- Al realizar la Evaluación Técnica Informática ETI se obtiene hallazgos que ratifican lo establecido en el Estatuto Orgánico por Procesos del Ministerio de Salud, en donde se considera a la unidad de TI como un proceso habilitante de asesoría y no como un proceso agregador de valor, por ende, no permite la creación de valor para la empresa a través de las tecnologías de la información TI.
- Con la Evaluación Técnica Informática ETI se obtuvo un conocimiento amplio de la realidad y problemas existentes en la unidad de TI en la Coordinación Zonal 1 - Salud, observaciones o hallazgos sobre los procesos evaluados, que reflejan las carencias en la unidad de TI, entre ellos que no se dispone de recursos adecuados y suficientes relacionadas con I&T (personas, procesos y tecnología), no existe una estrategia de gestión de los datos y no existe un sistema de gestión de seguridad de la información (SGSI), así como los problemas operativos existentes que no han permitido realizar una correcta gestión en los servicios brindados y la poca automatización de procesos.
- Mediante la cascada de metas de COBIT se seleccionó los procesos del modelo más relevantes para la institución, es decir, los procesos críticos, al realizar 3 mapeos se garantiza que se los procesos seleccionados sean los más relacionados en el ámbito empresarial y de TI, sin embargo, en base a los resultados obtenidos en cada mapeo se observa que no existe mucha

diferencia porcentual entre las metas evaluadas determinando que las metas del marco de referencia COBIT están presentes en la institución.

- Los documentos de sustento de la investigación de campo se encuentran debidamente firmados por cada uno de los entrevistados de tal manera que sustentan la veracidad de la información entregada, así como existen los audios de grabación del desarrollo de cada una de las entrevistas, encuestas, grabaciones realizadas bajo el consentimiento de cada uno de los entrevistados, información que ha sido entregada de manera formal en la institución como respaldo de la Evaluación Técnica Informática ETI realizada

Recomendaciones

- En la institución se debe implementar un Gobierno Empresarial de Tecnologías de la Información GETI en la institución mediante un marco para el gobierno y gestión como es COBIT 2019, que permita la creación de valor a partir de la transformación digital y la mitigación del riesgo del negocio derivado de dicha transformación, obteniendo resultados como la obtención de beneficios, optimización de riesgo y optimización de recursos.
- Se recomienda a la unidad de TI realizar las gestiones pertinentes a fin de que se implemente las recomendaciones emitidas en el informe de la Evaluación Técnica Informática, como es realizar un análisis detallado de los recursos necesarios en la unidad de TI (personas, procesos y tecnología) y comunicar al nivel directivo para que se asigne los recursos necesarios.
- Finalizada la ETI recomienda se revise las Normas de Control Interno de la Contraloría General del Estado respecto a Tecnologías de la Información, a fin de que las mismas sean cumplidas a través de los servicios y productos brindados por la unidad de TI y cumplir la normativa vigente como institución pública.

- Realizar una ETI de los demás procesos establecidos en el marco de referencia COBIT 2019 (40) para de esta manera tener una evaluación integral a nivel de TI en la institución.
- La Coordinación Zonal 1 – Salud cuenta con 9 “procesos” que son las 9 direcciones zonal existentes, si bien son considerados como procesos dentro de la organización, es necesario establecer mapas de procesos reales dentro de cada dirección los mismos que establezca métricas que permitan cuantificar su efectividad y por ende se pueda evaluar de una manera más cuantificable, aún cuando se trate de una institución del estado y este enfocada sus servicios sin fines de lucro.

Bibliografía

- Abreu, J. L. (2014). El Método de la Investigación Research Method. *Daena: International Journal of Good Conscience*, 9(3), 195-204.
- Arévalo, F., Cedillo, I., & Moscoso, S. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos Agile Methodology for Computer Risk Management. *Revista Killkana Técnica. Vol, 1(2)*.
- Choy, S. (2014). AUDITORIA CON UN ENFOQUE BASADO EN RIESGOS.
- Correa, R. (2008). Decreto 1014 Software Libre Ecuador: Recuperado.
- de Gestión Organizacional, M. E. O. por Procesos. *Estatuto Orgánico de Gestión Organizacional por Procesos*.
- Del Estado, C. G., DE, S. P. Y. P. J., QUE, D. P., & PUBLICOS, D. D. R. (2009). Normas de Control Interno de la Contraloría General del Estado. *Registro Oficial Suplemento, 87*.
- Espinosa, V., Acuña, C., De la Torre, D., & Tambini, G. (2017). La reforma en salud del Ecuador. *Revista Panamericana de Salud Publica, 41*.
- Fernández, J., & Alonso, E. F. (2013). Seguridad en Informática. *Aprocal*. Obtenido de <http://www.aprocal.mx/files> Obtenido de <http://aprocal.mx/files/2200/03SeguridadenInfor/2200/03SeguridadenInformaticaV1.0.pdf>.
- Flores, J. G., Gómez, G. R., & Jiménez, E. G. (1999). Metodología de la investigación cualitativa. *Málaga: aljibe*.
- Guaranda Sornoza, V. F. (2018). Auditoría de gestión de servicios tecnológicos en la Universidad Estatal del Sur de Manabí, basado en el marco de referencia COBIT 5.
- Hernandez, C. (2018). Qué es la Auditoría basada en riesgos y cuáles son sus ventajas. incp.org.co.
- ISACA, C. (2019). Framework: Introduction & Methodology. USA: ISACA.

- Loja, C. E., & Guzmán, D. C. (2016). Guía de auditoría para la evaluación del control interno de seguridad de la información con enfoque COBIT 5: caso Universidad Católica de Cuenca (UCACUE). *Revista Científica y Tecnológica UPSE*, 3(3), 113-121.
- Loor, L. V., & Bernal, F. E. (2018). *GUÍA METODOLÓGICA PARA LA EVALUACIÓN TÉCNICA INFORMÁTICA DE LA IMPLEMENTACIÓN DE EDUCACION Y CAPACITACIÓN VIRTUAL-COBIT 5* (Vol. 40): 3Ciencias.
- Malo-Serrano, M., & Malo-Corral, N. (2014). Reforma de salud en Ecuador: nunca más el derecho a la salud como un privilegio. *Revista Peruana de Medicina Experimental y Salud Pública*, 31, 754-761.
- Mejía, J. N., & De La Cruz, L. EVALUACIÓN TÉCNICA INFORMÁTICA DEL COMIL 10 ABDÓN CALDERÓN, UTILIZANDO EL ESTÁNDAR INTERNACIONAL COBIT.
- Palacios-Bayas, A. R., Bosquez-Barcenas, V. A., Palacios-Bayas, J. M., & Camacho-Castillo, L. A. (2019). AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN, APLICANDO COBIT 5. *Revista de Investigación Talentos*, 6(2), 1-11.
- Piattini, M. G., & Peso, E. G. (2000). *Auditoría informática: un enfoque práctico*: Ra-ma.
- Pública, M. d. (2012). Manual del Modelo de Atención Integral del Sistema Nacional de Salud Familiar, Comunitario e Intercultural: Obtenido de <http://instituciones.msp.gob.ec/somossalud/images/documentos>
- Quecedo Lecanda, R., & Castaño Garrido, C. M. (2002). Introducción a la metodología de investigación cualitativa. *Revista de psicodidáctica*.
- Romaní, J. C. C. (2009). El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento. *Zer: Revista de estudios de comunicación*, 14(27).
- Sánchez, L. (2015). COSO ERM y la gestión de riesgos. *Quipukamayoc*, 23, 44.

SILVA, I. C. F. V. (2015). *VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA*. UNIVERSIDAD NACIONAL DE CHIMBORAZO.

Solano, M. (2019). Un Plan de auditoría basado en riesgos. *Deloitte*.

Vásconez, P. V., Játiva, J. N., & Chiriboga, E. G. EVALUACIÓN TÉCNICA A LOS PROCESOS DE ALTA CRITICIDAD EN LA DIRECCIÓN DE INFORMÁTICA DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR UTILIZANDO COBIT 5.

Velthuis, M. G. P. (2008). *Auditoría de Tecnologías y Sistemas de Información*: Grupo Editorial RA-MA.

Zorrilla, H. (1997). La gerencia del conocimiento y la gestión tecnológica. *Programa de Gestión tecnológica*. Recuperado el, 18.

Apéndices