UNIVERSIDAD NACIONAL DEL ALTIPLANO DE PUNO

FACULTAD DE INGENIERÍA ESTADÍSTICA E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA ESTADÍSTICA E INFORMÁTICA

AUDITORIA INFORMÁTICA DEL SISTEMA DE ADMINISTRACIÓN TRIBUTARIA DE LA MUNICIPALIDAD DISTRITAL DE PILCUYO

TESIS

PRESENTADA POR:

Bach. JOSE LUIS ARO MAQUERA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ESTADÍSTICO E INFORMÁTICO

PUNO – PERÚ

2021

DEDICATORIA

A mis padres:

Quiero dedicar esta tesis a mis padres Roberto y Lidia porque ellos han dado razón a mi vida. Por sus consejos, su apoyo incondicional y su paciencia, todo lo que hoy soy es gracias a ellos.

A mi esposa e hijo:

A mi esposa Luz y mi menor hijo Daniel por su afecto y tu cariño son los detonantes de mi felicidad, de mi esfuerzo, de mis ganas de buscar lo mejor para ustedes. Me han enseñado y me siguen enseñando muchas cosas de esta vida.

A toda mi familia que es lo mejor y más valioso que Dios me ha dado.

Muchas gracias.

Jose Luis Aro Maquera

AGRADECIMIENTOS

A mis padres:

Que gracias a sus consejos y palabras de aliento me han ayudado a crecer como persona y a luchar por lo que quiero, gracias por enseñarme valores que me han llevado a alcanzar una gran meta. Los quiero mucho.

A mi esposa e hijo:

Gracias por su apoyo, cariño y por estar en los momentos más importantes de mi vida. Este logro también es para ustedes.

A mi asesor:

Por el tiempo dedicación y paciencia en la elaboración de mi proyecto de tesis.

Jose Luis Aro Maquera

ÍNDICE GENERAL

CAPITULO III

MATERIALES Y MÉTODOS

CAPITULO IV

RESULTADOS Y DISCUSIÓN

Área : Informática
Tema : Auditoria Informática

FECHA DE SUSTENTACIÓN: 09 de marzo de 2021

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE ACRÓNIMOS

COBIT : Objetivo de Control para Tecnología de Información (Control Objetives Information Tecnologies)

T.I. : Tecnologías de información

ISACA : Information Systems Audit and Control Association

EDM : Evaluación, orientación y supervisión

APO : Alinear, Planificar y Organizar (Align, Plan and Organise)

BAI : Construir, Adquirir e Implementar (Build, Acquire and Implement)

DSS : Entregar, dar Servicio y Soporte (Deliver, Service and Support)

MEA : Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess)

RESUMEN

Mediante el modelo COBIT v.5 se realizó la auditoría informática del sistema de administración tributaria, cuyo objetivo fue realizar la auditoria informática usando las normas COBIT v.5 en la oficina de informática y tecnología de la Municipalidad Distrital de Pilcuyo. El diseño de investigación fue el diseño descriptivo. Las conclusiones a las que se llegaron fueron: En cuanto a la gestión de los sistemas de información se encontraron inconvenientes con la dotación de personal en la oficina de informática y tecnología puesto que solo hay un encargado de dicho área, así mismo no existe un proceso que permita mantener las habilidades y competencias del personal que debe laborar en el área; como también el Sistema de Administración Tributaria no cuenta con documentación pertinente la cual ayude entender su proceso en la actualidad; así mismo cuando se realizó la auditoria informática se encontró que a partir de las pruebas de dicha auditoria de la seguridad de información se encontró falencias en la base de datos, redes y comunicación, seguridad lógica y seguridad física, puesto que se verifico que no se planifican ni existen iniciativas que permitan diagnosticar el riesgo e identificar los procesos críticos del sistema de administración tributaria; por último se presentó un informe que involucra recomendaciones y planes de mejora. En tanto para salvaguardar la información en el sistema de administración tributaria se debe dar fortaleza a los tres principios de seguridad de la información: confidencialidad, integridad y disponibilidad, a través de políticas de seguridad.

Palabras Clave: Administración tributaria, auditoria, informática, sistemas de información, gestión y tecnología.

ABSTRACT

Using the COBIT v.5 model, a computer audit of the tax administration system was carried out, the objective of which was to perform a computer audit using the COBIT v.5 standards in the IT and technology office of the Pilcuyo District Municipality. The research design was descriptive. The conclusions reached were: Regarding the management of information systems, there were problems with the staffing of the IT and technology office since there is only one person in charge of this area, likewise there is no process to maintain the skills and competencies of the staff that should work in the area; as well as the Tax Administration System does not have relevant documentation which helps to understand its current process; Likewise, when the IT audit was carried out, it was found that from the tests of said information security audit, there were deficiencies in the database, networks and communication, logical security and physical security, since it was verified that there are no plans or initiatives to diagnose the risk and identify the critical processes of the tax administration system; finally, a report was presented that involves recommendations and improvement plans. In order to safeguard the information in the tax administration system, the three principles of information security must be strengthened: confidentiality, integrity and availability, through security policies.

Keywords: Tax administration, auditing, IT, information systems, management and technology.

CAPÍTULO I

INTRODUCCIÓN

En la actualidad debido al avance tecnológico de los sistemas, las telecomunicaciones que día a día han logrado posicionarse tanto en sectores públicos y privados de todo el mundo constituyéndose en una herramienta estratégica para el desarrollo institucional, dando paso a que los sistemas informáticos necesiten un adecuado control sujetos a lineamientos, normas y estándares que vayan acorde a la política institucional. Es decir, realizar una auditoria informática, para verificar el uso eficaz y eficiente de dichos sistemas para brindar al usuario un servicio óptimo y satisfactorio.

En base a ello, la presente investigación enfoca a realizar auditoría informática aplicando un único marco general para unificar procesos del COBIT 5, que permitirá comprender el gobierno y la gestión de las tecnologías de información, en este caso del sistema de administración tributaria que es gestionada directamente por la oficina de informática y tecnología de la Municipalidad en mención. La presente investigación está estructurada en los siguientes capítulos, que se detallan a continuación:

CAPITULO I: Introducción; encontramos el planteamiento del problema, formulación del problema, objetivo general y objetivos específicos que guiaron el trabajo de investigación.

CAPITULO II: Revisión de la Literatura; contiene los antecedentes de la investigación, el marco teórico que se utilizó como base para trabajar la presente investigación.

CAPITULO III: Materiales y Métodos; comprende tipo de investigación, método de investigación, diseño de investigación, ubicación y descripción de la población, técnicas

e instrumentos que permitieron la recolección de información, estadístico prueba de hipótesis.

CAPITULO IV: Resultados dando a conocer los resultados de la investigación.

CAPITULO V: Se presente las conclusiones, recomendaciones, referencias y los anexos donde se detalla el instrumento de recolección de datos.

1.1. PROBLEMA DE LA INVESTIGACIÓN

Debido a constante avance tecnológico en el mundo, donde los sistemas de información han logrado posicionarse en distintos sectores ya sean públicos o privados, dando paso a un adecuado control para el uso de estos sistemas. Como menciona RAMOS (2015). El avance tecnológico de los sistemas de información y telecomunicaciones han alcanzado gran evolución, junto con eso es la misma proporción avanzan los riesgos asociados a las mismas, y hoy en día para mucha empresa del Perú, sean privados o públicas, la seguridad de la información es un problema que posee en común, debido a que poca de estas empresas plantea medidas de contingencia para salvaguarda el activo más importante hoy considerado como lo es a información.

En tanto en el Perú, para salvaguardar la información y eficacia de las auditorias informáticas para el buen desempeño de los sistemas de información ya sea en organizaciones públicas como privadas, en su gran mayoría no se realizan por dos factores; primero el alto costo de este proceso y el segundo el desconocimiento de este proceso puesto que se piensa que es el método para evaluar al personal y por ende la destitución del cargo lo cual no es de agrado para los empleados de las distintas organizaciones.

La Municipalidad Distrital de Pilcuyo, es una institución encargado de la administración de los recursos a fin de satisfacer las necesidades y brindar servicios de calidad a la

población, por la que sería recomendable realizar Auditorías informáticas a todas sus oficinas con el fin de mejorar el desenvolvimiento de las mismas, pero lamentablemente en la práctica no se aplican puesto que no es un proceso muy conocido. Dicha municipalidad maneja un único sistema de administración tributaria que permite la gestión y administración tributaria, en dicho sistema se ha encontrado debilidades puesto que no cuenta con una gestión de sus procesos en cuanto a las estrategias de desarrollo, implementación y mantenimiento del sistemas de información y sobre todo en la seguridad de información, puesto que no existe un software que garantice la seguridad de la información lo que puede generar que haya un inminente peligro de pérdida de información de las diferentes áreas del municipio que tienen T.I.; así mismo no hay personal capacitado y no existe una área para que se pueda realizar los procesos de supervisión y evaluación del sistema, también se tienen una pobre documentación donde se detalle las actividades de los procesos del sistema, o simplemente no están debidamente formalizados y basados en buenas prácticas, generando que el personal de T.I. no tenga conocimiento de todos los problemas que existen, ni cómo está funcionando cada proceso del sistema.

Es así que la problemática mencionada puede crear insatisfacción del usuario ya que el municipio no brindara un servicio eficaz, eficiente y sobre todo de calidad. Es por ello que se requiere realizar auditoria informática en dicha municipalidad.

1.2. FORMULACIÓN DEL PROBLEMA

¿Será posible realizar la auditoría informática usando la metodología COBIT 5 al sistema de administración tributaria en la oficina de informática y tecnología de la Municipalidad Distrital de Pilcuyo?

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. Objetivo general

Realizar la auditoria informática usando la metodología COBIT 5 al sistema de administración tributaria en la oficina de informática y tecnología de la Municipalidad Distrital de Pilcuyo.

1.3.2. Objetivos específicos

- Evaluar la gestión del sistema de información de administración tributaria de la oficina de informática y tecnología de la Municipalidad Distrital de Pilcuyo.
- Realizar una auditoria informática aplicando la metodología COBIT 5 al sistema de administración tributaria de la oficina informática y tecnología de la Municipalidad del Distrito de Pilcuyo.
- Elaborar el informe de auditoría sobre la gestión del sistema de información de la oficina de informática y tecnología de la Municipalidad del Distrito de Pilcuyo.

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. Antecedente Internacional

Guadalupe (2017), en su investigación recomienda implementar en la corporación una metodología que permita administrar, supervisar, controlar y evaluar los procesos que realizan los Sistemas informáticos y las herramientas tecnológicas que se encuentran implementadas actualmente; establecer la aplicación de una Auditoria Informática orienta a evaluar las necesidades de la institución, así como el control interno, para alcanzar un manejo más eficiente de los recursos y reformar los trabajos que se realizan para de esa manera alcanzar las metas propuestas por los ejecutivos de la corporación; aplicar la metodología COBIT5 en los procesos diarios que realiza el Comercial "JAHER" agencia Babahoyo como mecanismo de mejora del funcionamiento y garantizar la transparencia de los mismos.

Jiménez (2016), en su investigación concluyo que los procesos de auditoría informática o evaluaciones técnicas en la actualidad son muy necesarios en las empresas, independientemente de su tamaño o entorno de negocio, esto permite que una empresa tenga un conocimiento de la condición y de cómo las Tecnologías de Información apoyan y fortalecen los procesos de negocio brindándoles grandes beneficios a costos de operación óptimos; COBIT 5 es un marco metodológico para el gobierno y gestión de las tecnologías de la Información y el negocio, provee un conocimiento amplio, gracias a que reúne la experiencia de varios profesionales de

todo el mundo en las diferentes áreas en las que las tecnologías de la información se encuentran involucradas, brindando un soporte consiste que puede ser aplicado a las organizaciones de todo tipo de entorno y de todo tamaño; COBIT 5 es un marco metodológico muy versátil, que logra adaptarse a las necesidades y expectativas de las organizaciones, sus guías y recomendaciones cubren por completo, brindando las pautas que pueden escoger las organizaciones para adaptar un gobierno tecnológico eficientemente gestionado.

Arreaga (2019), en su investigación aconsejo que la elaboración de un plan integral, que conjugue todas las unidades académicas y sea gestado en forma interdisciplinaria en especial por profesionales en la ingeniería de sistemas, contadores y auditores para gestar eficientemente la seguridad informática en toda la UTMACH, así como aprovechar al máximo sus potencialidades al ámbito académico.

Sánchez (2018), en su investigación llego a la conclusión que luego de haber hecho la evaluación el software de control de seguridad de la empresa Transvas S.A, el sistema informático tiene algunos problemas y nos muestra vulnerabilidades de aspecto riesgosos en el sistema operativo y perdida de información; el personal fue evaluado y se indicó que estaban capacitados en ciertos aspectos técnicos del sistema, pero requieren más conocimientos acerca de seguridad sistema informático; después de haber hecho la evolución llevaremos a cabo el desarrollo de un manual de Divulgación de información confidencial que puede causar problemas a las empresas, así como daños de reputación o poner en peligro relaciones ya que no se lleva un control y monitoreo del sistema; el manual de funciones que sirva como guía auditoria del control de seguridad a través de la norma COBIT 5.

2.1.2. Antecedente Nacional

Bugosen y Tejada (2015), en este proyecto se planteó una solución probada de modelo de Gobierno y Gestión de TI basado en COBIT5 enfocado en el dominio de gestión Entregar, Dar Servicio y Soporte. Así mismo se concluyó, que es plenamente necesario contar con un adecuado modelo de Gobierno de TI, para garantizar la correcta operación en la entrega de servicio de infraestructura y aplicación de TI apoyando en la mitigación de riegos y evitando los problemas expuestos

Rafael y Castillo (2017), en su investigación concluyó que aplicando encuestas, entrevistas y checklist, se pudo determinar cuál es la situación problemática del Hospital Regional Docente Las Mercedes de Chiclayo, encontrándose como principales problemas el no mantener la dotación de personal suficiente en el área, así mismo no existe un proceso que permita mantener las habilidades y competencias del personal TI; utilizando el estándar COBIT 5, se determinó que de los 37 objetivos de control que tiene COBIT, 19 aplican a nuestro proyecto, los cuales se detallaron a lo largo de la auditoría; se aplicó el estándar COBIT, mediante el cual se evaluó cada uno de los objetivos de control aplicados, de los cuales se encontraron 9 objetivos de control efectivos y 10 objetivos de control no efectivos.

Beingolea (2015), en su investigación concluyo que se identificaron 31 procesos habilitadores de COBIT 5 que permiten formar el gobierno de TI según las necesidades del negocio, de los cuales se escogieron 14 procesos habilitadores debido al enfoque de seguridad de la información; también se concluye que la empresa del caso de estudia cuenta con un nivel de madurez adecuado para el gobierno de TI con enfoque de seguridad según el nivel que se definió en un inicio, pues en la mayoría de los caso se alcanzó dicho nivel y en algunos se superó, pues lo recomendable seria cerrar las brechas que se tienen aun en algunos procesos que

no llegaron a alcanzar el objetivo establecido; si bien se cumple con el objetivo definido en la actualidad, se debe de estar revisan semestralmente que nuevas actividades se deben de añadir para fortalecer el proceso así como cuales estarían dejando de ser obsoletas con la finalidad de contar con procesos de gobierno actualizados a las tendencias y requerimientos actuales de seguridad la información.

2.1.3. Antecedentes locales

Puma (2017), de los resultados obtenidos se concluye que la implantación del proceso de Auditoría de Seguridad de Información basada en la norma ISO/IEC 27002, fue un éxito logrando reducir el costo de la auditoría de seguridad de información realizada en la Caja Los Andes, Puno-2016, gracias a que el proceso facilita al auditor interno tener herramientas, pautas técnicas, plan de pruebas, una estructura de custodia de papeles de trabajo, una ficha de control de tiempos, un informe y una estructura sistematizada para realizar la auditoria de seguridad de información; también del diagnóstico obtenido sobre el análisis situacional se puede concluir que al establecer un proceso hay que conocer cómo se venía trabajando y tomar en cuenta ese expertis que tienen los empleados para afianzar las actividades del proceso implantado.

2.2. MARCO TEÓRICO

2.2.1. Auditoria

La auditoría tiene un concepto amplio puesto que no solo se encargará de detectar los errores, si no realizara un examen crítico para determinar la eficiencia y eficacia de una organización.

La auditoría en sí es una actividad que consiste en emitir un juicio y opinión profesional sobre el objetivo o la materia analizada indicando si se están cumpliendo los requisitos que procedan en cada temática. Esta opinión deberá fundamentarse en una serie de procedimientos que justifiquen y sirvan de soporte al análisis realizado. (Tejada, 2015)

Según Brito *et al.* (2016) define la auditoria como el proceso metódico de obtener y valorar los registros patrimoniales de una empresa con el fin de probar su estado crediticio. Tiene como propósito demarcar la razonabilidad, moralidad y autenticidad de los estados financieros, expedientes y demás documentos administrativos contables presentados por la gerencia, así como revelar las deducciones o alusiones de la empresa. La ocupación del auditor es examinar la precisión y claridad de los registros mostrados por una compañía, a fin de rectificar errores, perversiones y engaños. Se basa en el funcionamiento de la contabilidad, sin embargo, los objetivos son más grandes: emitir una valoración sobre la marcha de la organización, tazar las metas, examinar su gestión e intérpretes, ejecutar un ojeo de influencias en la empresa.

2.2.1.1. Classification de la auditoria:

La auditoría por su ámbito y de acuerdo con la identidad del auditor, se clasifican como auditoría externa e interna.

Auditoría Interna

Es aquella que se hace dentro de una organización; sin contratar a personas de afuera. La auditoría interna es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. Las empleadas que realizan esta tarea son remuneradas económicamente.

Auditoría Externa

Conocida como auditoría independiente, la efectúan profesionales que no dependen de la empresa, ni económicamente ni bajo cualquier otro concepto. Se presume una mayor objetividad que en la auditoria interna, debido al mayor distanciamiento entre auditores y auditados.

2.2.1.2. Tipos de auditoria

Auditoría operacional, el cual se refieren a la inspección del proceder de una organización y juzga la eficacia de la misma.

Auditoría administrativa, los cuales se refieren a la ordenación y validez de la estructura de los trabajadores con la que dispone la institución y los procedimientos administrativos de dichos trabajadores.

Auditoría contable, es un proceso sistemático de revisión de las cuentas anuales de una persona jurídica con el fin de comprobar que estas reflejen la imagen fiel de la misma.

Tabla 1: Diferencia entre los tipos de auditorías.

	AUDITORIA ADMINISTRATIVA	AUDITORIA OPERACIONAL	AUDITORIA CONTABLE	AUDITORIA INFORMÁTICA
NATURALEZA	Técnica de control administrativo	Técnica de control administrativo	Técnica de control administrativo	Técnica de control administrativo
PROPÓSITO / OBJETIVO	Evaluar y mejorar la administración	Promover la eficiencia en las empresas	Dictamen a los estados financieros	Evaluar los recursos informáticos
ALCANCE	La eficiencia y productividad del proceso productivo	La eficiencia de las operaciones	El sistema contable	Todas las actividades informáticas
FUNDAMENTO	La ciencia administrativa y la normatividad de la empresa	La ciencia administrativa y la normatividad de la empresa	Principios de contabilidad y normas de auditoría	Normatividad institucional y legal
METODOLOGÍA	Apoyado en métodos científicos	Técnicas y procedimientos predeterminados	Técnicas y procedimientos predeterminados	Técnicas y procedimientos predeterminados
APLICACIÓN	A la empresa y sus funciones básicas	A las funciones de la empresa	A los estados financieros	A todas las áreas de la empresa
PROYECCIÓN	Hacia el futuro	Hacia el futuro	Hacia el pasado	Hacia el futuro
INFORME	Amplio	Amplio	Preciso	Amplio y preciso

Fuente: Universidad Nacional Autónoma de México (UNAM) (2018).

2.2.1.3. Etapas de la auditoria

Según Hernández y McGraw (2017), la auditoria tiene 5 etapas que cumplir, las que se detalla a continuación

Exploración

Es la etapa en la cual se desarrollan los estudios o reconocimientos previos al inicio de la auditoria con el deseo de conocer a detalle las características de la compañía a auditar para conseguir los elementos necesarios que permitan un

apropiado planeamiento del compromiso a hacer y dirigirlo hacia las cuestiones que resulten de máximo beneficio para los objetivos previstos para la auditoría.

Planeamiento

El compromiso esencial en esta etapa es el precisar la estrategia que se debe alcanzar en la auditoría a desarrollar, Lo antepuesto conlleva imaginar los temas que se deben ejecutar, de manera que aseguren la realización de una auditoría de alta calidad y que se logre con la economía, eficiencia, eficacia y prontitud merecidas.

Supervisión

El objetivo vital de la supervisión es aseverar el cumplimiento de los objetivos de la auditoria y la calidad justificable del trajín. Una orientación y un cuidado precisos de la auditoria son obligatorios en todas las fases y las etapas del trabajo, desde la investigación incluso la emisión del informe y su estudio con los factores de la entidad auditada. Asimismo, debe asegurar el cumplimiento de las pautas de auditoría y que el informe final refleje bien los resultados de las demostraciones, comprobaciones e indagaciones realizadas.

Ejecución

El efecto vital de esta fase es reunir las pruebas que sustenten las opiniones del auditor sobre el trabajo realizado, es la etapa, por decir de alguna forma, del trabajo de campo, esta depende ampliamente del grado de profundidad con que se hayan desarrollado las dos fases anteriores, en esta se elaboran los papeles del trajín y las hojas de nota, herramientas que respaldan excepcionalmente la opinión del auditor.

Informe

En esta fase el auditor se dedica a formalizar los resultados en un documento los cuales detallan el proceder de la auditoría ejecutada y demás comprobaciones vinculadas con el trabajo realizado. Comunicar los resultados al máximo nivel de dirección de la entidad auditada y otras instancias administrativas, así como a las autoridades que correspondan, cuando esto proceda. Elaborar del informe final de auditoría es una de las etapas más importante y compleja de este estudio, por lo que requiere de mucho cuidado en su elaboración.

Seguimiento

Como indica la palabra, los resultados de una auditoría, habitualmente una auditoría evaluada de manera deficiente o mal, se tiene que pasado un plazo aproximado de seis meses o un año se vuelve a realizar otra auditoría de modelo recurrente para asegurar el verdadero cumplimiento de las debilidades detectadas en la auditoría.

2.2.1.4. Auditoria en informática

Hernández y McGraw (2017) afirman que es el proceso que consiste en recoger, agrupar y evaluar evidencias para delimitar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

Se desarrolla en función de normas, procedimientos y técnicas definidas por institutos establecidos a nivel nacional e internacional; por ello, nada más señalarán algunos aspectos básicos para su entendimiento.

Así, la auditoría en informática es:

- Proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.
- Un proceso formal ejecutado por especialistas del área de auditoría y de informática; se orienta a la verificación y aseguramiento para que las políticas y procedimientos en la organización se realicen de una manera oportuna y eficiente.
- Las actividades ejecutadas por profesionales del área de informática y de auditoría encaminadas a evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección, etc.). Dicha evaluación deberá ser la pauta para la entrega del informe de auditoría en informática, el cual debe contener las observaciones, recomendaciones y áreas de oportunidad para el mejoramiento y optimización permanente de la tecnología de informática en el negocio.
- El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de que los recursos de informática operen en un ambiente de seguridad y control eficientes, con la finalidad de proporcionar a la alta dirección o niveles ejecutivos la certeza de que la información que circula por el área se maneja con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etcétera.
- Proceso metodológico que tiene el propósito principal de evaluar los recursos (humanos, materiales, financieros, tecnológicos, etc.) relacionados con la función de informática para garantizar al negocio que dicho conjunto opere

con un criterio de integración y desempeño de niveles altamente satisfactorios, para que a su vez apoyen la productividad y rentabilidad de la organización.

2.2.1.5. Importancia de la auditoria en informática

Según Kuna (2014), la auditoría de sistemas es fundamental para garantizar el correcto funcionamiento de los Sistemas de Información al proporcionar los controles necesarios que permiten garantizar la seguridad, integridad, disponibilidad y confiabilidad de los mismos. Un proceso de auditoría informática permite reconocer debilidades y amenazas a los procesos de negocio de una empresa que se encuentra vinculados a las TIC, permite además evaluar, si las políticas adoptadas en la institución están siendo acatadas y cumplidas, determinando a la vez un examen detallado a los mecanismos de control adoptados, valorando si los mismos son idóneos o no para el escenario en el cual son aplicados.

Analiza las posibles deficiencias o debilidades permitiendo a la dirección de la empresa tomar las medidas respectivas que disminuyan los impactos que provocan las amenazas. Es un estudio que presenta una visión amplia de la condición actual de las TIC, agregando sugerencias de mejora para garantizar la continuidad del negocio.

Según el autor, nos recalca que la tecnología de informática, traducida en hardware, software, sistemas de Información, investigación tecnológica, redes locales, base de datos, ingeniería de software, telecomunicaciones, servicios y organización de informática, permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos,

identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes

2.2.1.6. Objetivos de la auditoria en informática

- El análisis de la eficiencia de los sistemas de información.
- La verificación del cumplimiento de la normativa en este ámbito.
- La revisión de la eficaz gestión de los recursos informáticos

2.2.2. COBIT 5.

Es importante indicar que todas las empresas, actualmente manejan y gestionan datos e información y la tecnología viene desempeñando un papel importante en estas acciones. Toda empresa u organización necesita ser capaz de confiar en información de calidad para apoyar los procesos de toma de decisiones de calidad para así incrementar sus logros en cuanto a beneficios, a través del uso adecuado de sus recursos tecnológicos, esta acción les permite generar valor a su negocio y atraer oportunidades de inversión, logrando la excelencia operativa. A la vez deben de mantener a niveles aceptables y manejables los riesgos que implica las TI. Apuntando de la misma manera, a que sus clientes internos y externos experimenten satisfacción en los servicios ofertados.

Para lograr estos objetivos se requiere de un adecuado gobierno y gestión de la información y los activos tecnológicos. Y para este estudio se establecerá las normas COBIT V.5 que esta presentado por ISACA (Information Systems Audit and Control Association) como un marco de referencia amplio, que busca ayudar a las organizaciones a cumplir con el alcance de sus objetivos, agregando un valor significativo, mediante la implementación de una adecuada gobernabilidad y gestión de las TI.

Historia y Evolución de COBIT

El proyecto COBIT se emprendió por primera vez en el año 1995, con el fin de crear un mayor producto global que pudiese tener un impacto duradero sobre el campo de visión de los negocios, así como sobre los controles de los sistemas de información implantados.

La primera edición del COBIT, fue publicada en 1996 y fue vendida en 98 países de todo el mundo. La segunda edición (tema de estudio en este informe) publicada en Abril de 1998, desarrolla y mejora lo que poseía la anterior mediante la incorporación de un mayor número de documentos de referencia fundamentales, nuevos y revisados (de forma detallada) objetivos de control de alto nivel, intensificando las líneas maestras de auditoría, introduciendo un conjunto de herramientas de implementación, así como un CD-ROM completamente organizado el cual contiene la totalidad de los contenidos de esta segunda edición. (PEOPLECERT, 2019)

Una temprana suma significativa avizorada para la familia de productos COBIT, es la del desarrollo de las guías de gerencia que incluyen factores críticos de éxito, indicadores claves de desempeño y medidas comparativas. Los factores críticos de éxito, identificarán las acciones más relevantes para la administración y lograr obtener así, dichas acciones o contemplar los aspectos para conseguir dominio sobre los procesos de TI. Los indicadores clave de desempeño proporcionarán medidas de éxito que permitirán a la dirección observar si un proceso de TI está alcanzando los requerimientos del negocio. Las medidas comparativas establecerán niveles de madurez que pueden ser utilizadas por la dirección para: fijar el nivel vigente de madurez en la empresa; determinar los niveles de madurez

que se desea conseguir, como una ocupación de sus riesgos y objetivos; y suministrar una base de comparación de sus prácticas de inspección de TI hacia empresas similares o normas de la misma industria. (Martínez, 2017)

Actualmente el 9 de abril de 2012 fue publicado oficialmente por ISACA el marco de referencia COBIT 5, es la evolución de la familia COBIT, aprovechando las versiones anteriores y las practicas actuales; COBIT permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones. Enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de COBIT. (Chillida, 2013)

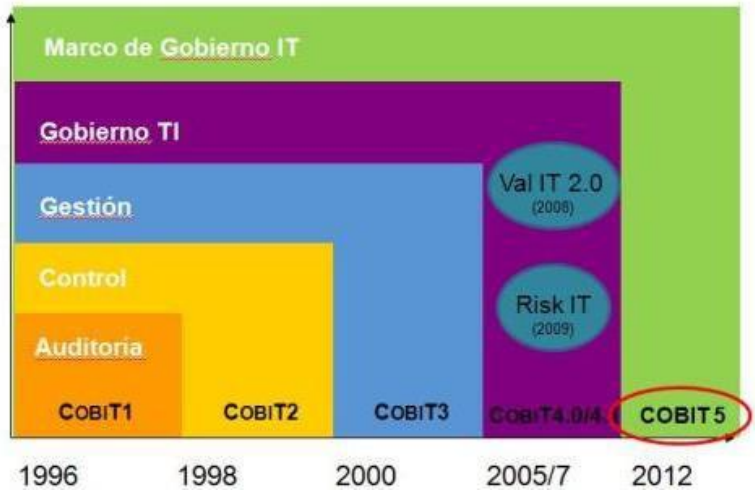

***Figura 1*:** Ámbito de evolución de Cobit.

Fuente: Arquitectura Empresarial (Martínez, 2017).

2.2.2.1. ¿Qué es COBIT?

COBIT posibilita que las TI sean gobernadas y gestionadas de forma holística para todo el organismo, tomando en consideración el negocio y las áreas funcionales de pico a pico, así como los interesados internos y externos. COBIT

permite aplicarse a todos los tamaños, tanto en el sector público y privado, así como en entidades que se desempeñan sin fines de lucro. (Soto, 2016)

2.2.2.2. ¿Para qué se utiliza COBIT?

Según López (2009) las normas COBIT se utiliza para:

- Planear, implementar, controlar y evaluar el gobierno sobre TI; incorporando objetivos de control, directivas de auditoria, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.
- Permite el desarrollo claro de políticas y la práctica buena para el control de TI en todas las partes de la organización.
- Es constantemente actualizado; el cual permite a las empresas aumentar su valor en TI y reduce los riesgos asociados a proyectos tecnológicos.
- Gracias a que COBIT se estructura a partir de parámetros generalmente aplicables y aceptados, para mejorar las prácticas de planeación, control y seguridad de las Tecnologías de Información.

2.2.2.3. Objetivos y beneficios COBIT

- Proveer un marco único reconocido a nivel mundial de las “mejores prácticas” de control y seguridad de TI.
- Consolidar y armonizar estándares originados en diferentes países desarrollados.
- Concientizar a la comunidad sobre importancia del control y la auditoría de TI.
- Enlaza los objetivos y estrategias de los negocios con la estructura de control de la TI, como factor crítico de éxito.

- Aplica a todo tipo de organizaciones independiente de sus plataformas de TI.
- Ratifica la importancia de la información, como uno de los recursos más valiosos de toda organización exitosa. (Ron, 2010)

2.2.2.4. ¿Quiénes utilizan COBIT?

Según Vega (2017), Cobit 5, es empleado en todo el mundo por personas quienes tienen como responsabilidad principal los procesos de negocio y la tecnología, son aquellos de quien depende de la tecnología y la información confiable, fiable y los que proveen calidad, confiabilidad y control de tecnología de información.

La Gerencia: Para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

Los Usuarios Finales: Quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

Los Auditores: Para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.

Los responsables de TI: Para identificar los controles que requieren en sus áreas. También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

2.2.2.5. Principios del COBIT 5

El marco de COBIT 5 según ISACA (2012), menciona 5 principios clave que incluyen una amplia guía para los facilitadores de gobierno y gestión de TI en la empresa. En la siguiente figura 3 se muestran estos 5 principios.

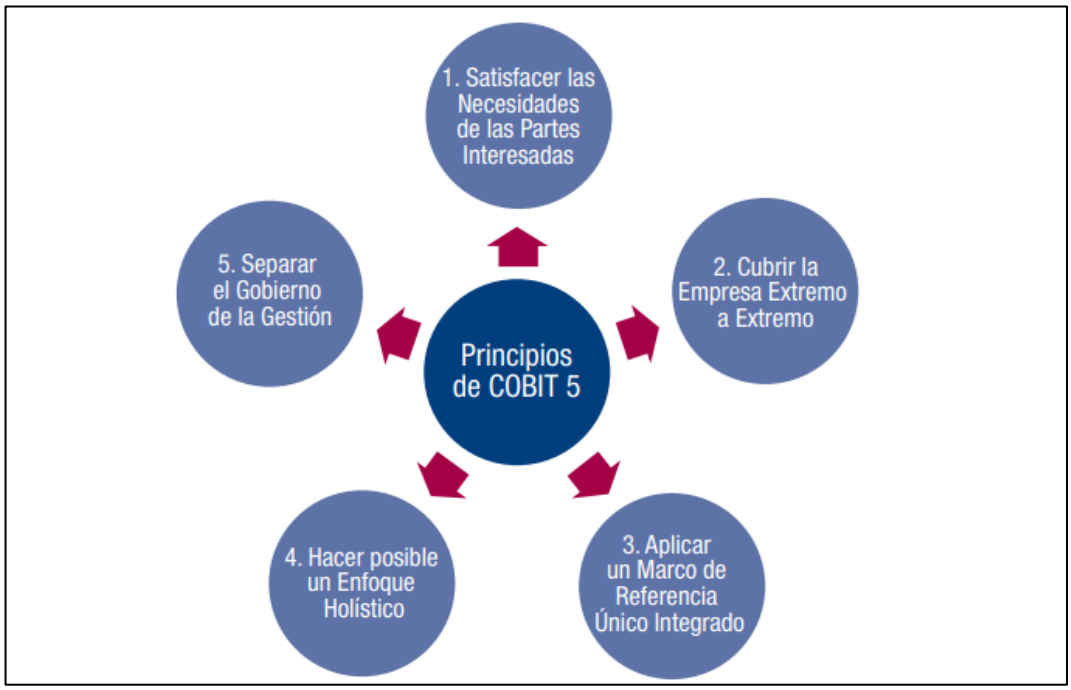

***Figura 2*:** Principios de COBIT 5

Fuente: COBIT 5 (ICASA, 2012)

Principio 1. Satisfacer las Necesidades de las Partes Interesadas

Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más

manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

Principio 2: Cubrir la Empresa Extremo-a-Extremo

COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo:

Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.

Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

Principio 3: Aplicar un Marco de Referencia único integrado

Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.

Principio 4: Hacer Posible un Enfoque Holístico

Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los

catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores:

- Principios, Políticas y Marcos de Trabajo
- Procesos
- Estructuras Organizativas
- Cultura, Ética y Comportamiento
- Información
- Servicios, Infraestructuras y Aplicaciones
- Personas, Habilidades y Competencias

Principio 5: Separar el Gobierno de la Gestión

El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:

Gobierno

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

Gestión

La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales. En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO).

Juntos, estos cinco principios habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas.

2.2.2.6. Estructura COBIT

Modelo de referencia de procesos COBIT 5

COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Dicho modelo representa todos los procesos que normalmente encontramos en una empresa relacionados con las actividades de TI, proporciona un modelo de referencia común entendible para las operaciones de TI y los responsables de negocio. El modelo de proceso propuesto es un modelo completo e integral, pero no constituye el único modelo de procesos posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular. (ISACA, 2012)

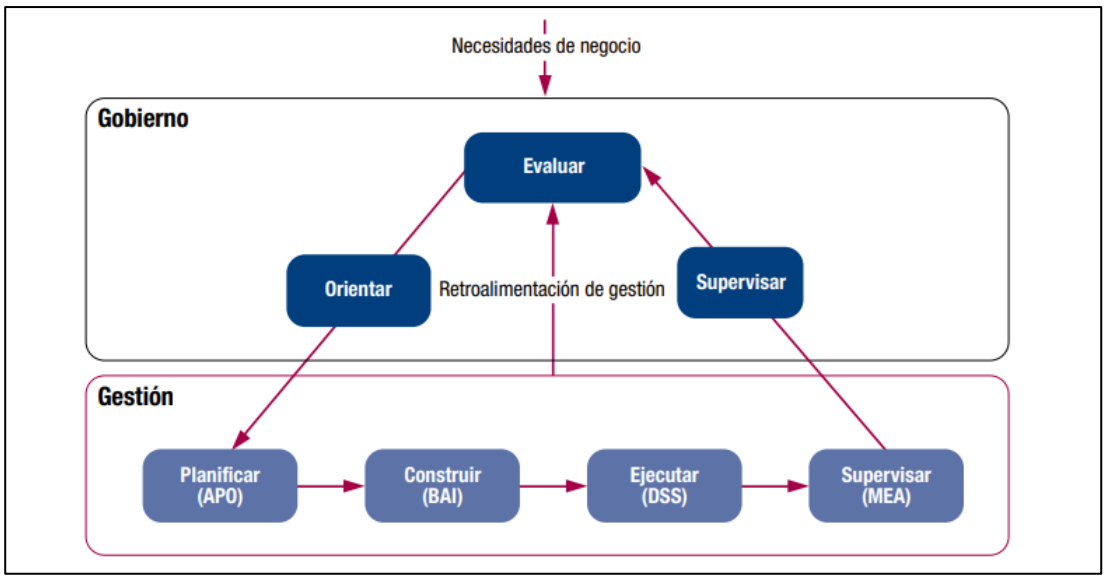

***Figura 3*:** Estructura COBIT 5

Fuente: COBIT 5 (ICASA, 2012)

El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

Gobierno: Contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM)

Gestión: Contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (Plan, Build, Run and Monitor - PBRM), y proporciona cobertura extremo a extremo de las TI. Estos dominios son una evolución de la estructura de procesos y dominios de COBIT 4.1. Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales, pero contienen más verbos para describirlos:

- Alinear, Planificar y Organizar (Align, Plan and Organise, APO)
- Construir, Adquirir e Implementar (Build, Acquire and Implement, BAI)
- Entregar, dar Servicio y Soporte (Deliver, Service and Support, DSS)

- Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, MEA)

Dominios y procesos de COBIT 5

Cada dominio contiene un número de procesos. A pesar de que, según hemos descrito antes, la mayoría de los procesos requieren de actividades de "planificación", "implementación", "ejecución" y "supervisión", bien en el propio proceso, o bien en la cuestión específica a resolver (como p. ej. calidad, seguridad), están situados en dominios de acuerdo con el área más relevante de actividad cuando se considera la TI a un nivel empresarial. (ISACA, 2012)

A continuación, se muestra el conjunto completo de los 5 dominios y 37 procesos de gobierno y gestión de COBIT 5.

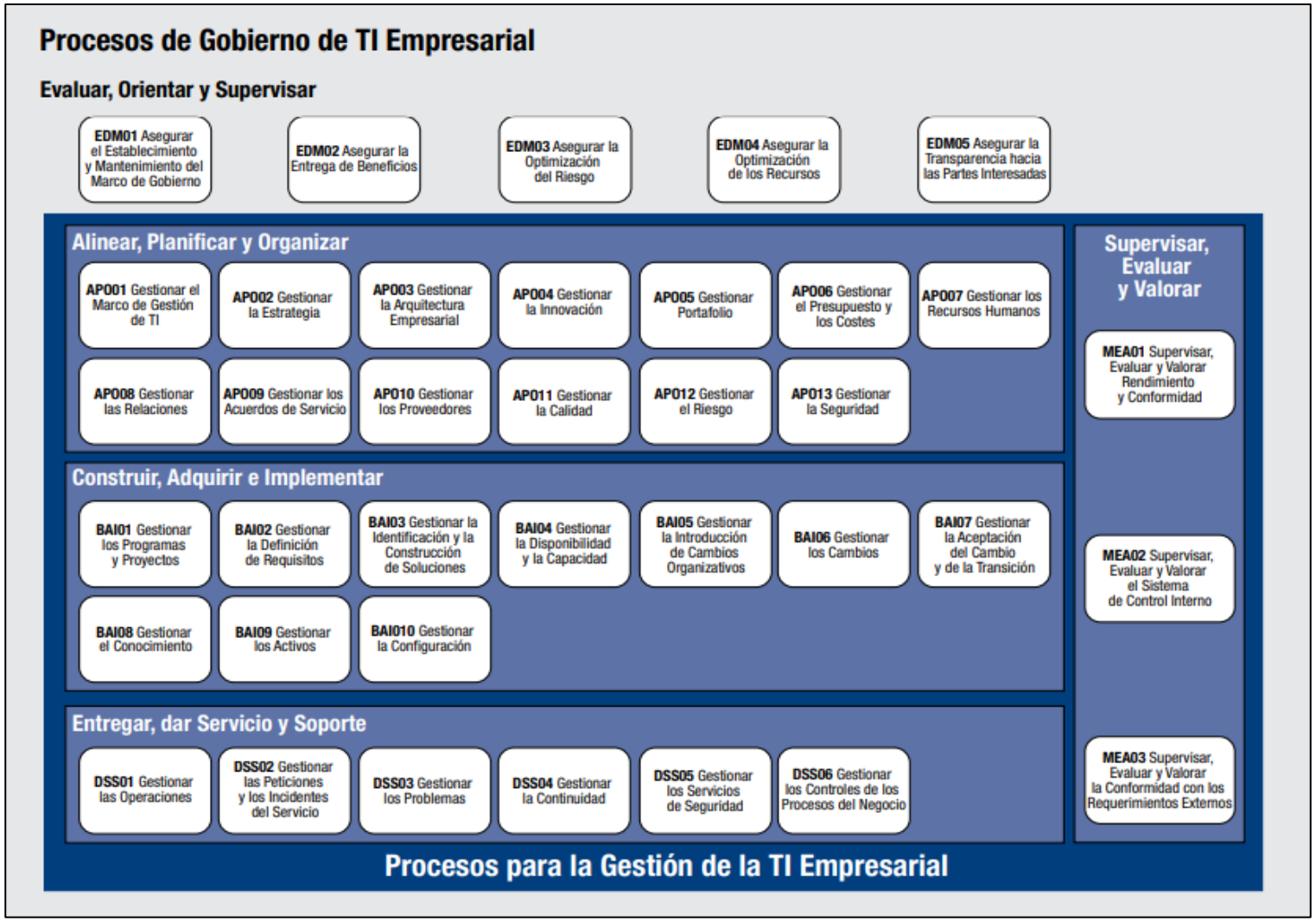

***Figura 4*:** Procesos COBIT 5

Fuente: COBIT 5 (ICASA, 2012)

CAPITULO III

MATERIALES Y MÉTODOS

3.1. TIPO DE INVESTIGACIÓN

Por las características de la muestra y el problema de investigación, es una investigación con paradigma cualitativo de tipo descriptivo, como menciona Hernández *et al.* (2014), tiene como propósito medir el nivel de seguridad del sistema académico considerando el problema en estudio y sus componentes.

3.2. POBLACION Y MUESTRA DE LA INVESTIGACION

3.2.1. Población:

La población de estudio está constituida por el encargado de la oficina de informática y tecnología de la Municipalidad Distrital de Pilcuyo.

3.2.2. Muestra

La muestra es no probabilística puesto que fue determinada por conveniencia debido a los objetivos y criterios del investigador como menciona Hernández – Sampieri, Fermandez . Collado *et al.* (2017) en las muestras no probabilísticas, la elección de los elementos no depende de la probabilidad, sino del proceso de toma de decisiones de una persona o de Grupo de persona; por lo tanto, no se aplicó muestreo alguno.

Entonces nuestra muestra de estudio corresponde al (01) encargado de la oficina de Informática y Tecnología, quien administra el sistema de información de administración tributaria.

3.3. ÁMBITO O LUGAR DE ESTUDIO

La investigación se realizó en la Oficina de Informática y Tecnología de la Municipalidad Distrital de Pilcuyo, que está ubicado en el Distrito de Pilcuyo, Provincia del Collao, Departamento de Puno.

***Figura 5*:** Ámbito o lugar de estudio.
Fuente: ProcesoReporteGrafPb

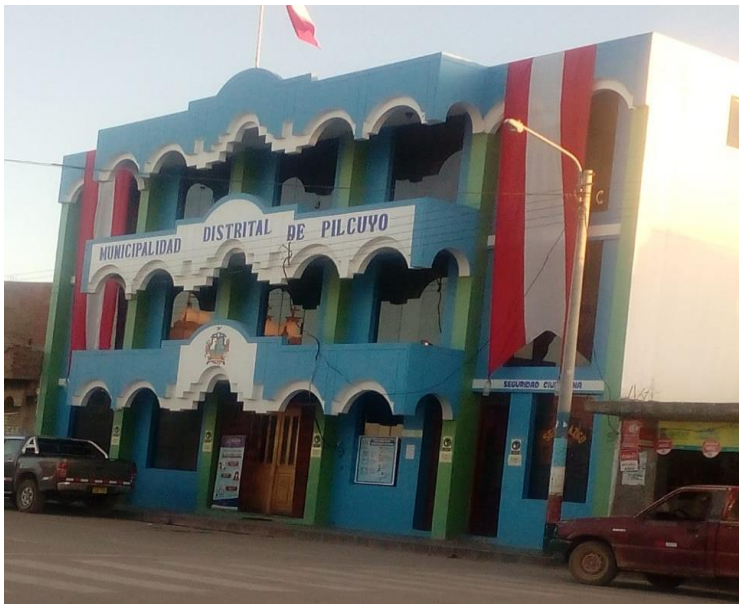

***Figura 6*:** Ámbito o lugar de estudio.
Fuente: Fotografía propia.

3.4. TÉCNICA E INSTRUMENTOS DE RECOPILACIÓN DE DATOS

Para el desarrollo de la auditoria utilizó distintas técnicas e instrumentos de acuerdo a los puntos a ser auditados tomando en cuenta el marco de trabajo para el gobierno y la gestión de las TI, basado en 5 dominios y 37 procesos que tiene COBIT 5.

3.4.1. Técnicas

- *Encuestas*: Nos fue de utilidad para recolectar los datos, esta fue empleada de manera personal y nos permitió conocer el entorno tal y como se presenta.

- *Entrevistas:* Permitieron la interrelación y el dialogo entre el entrevistador y el entrevistado aplicando una entrevista semiestructurada.

- *Análisis documental:* Esta técnica fue importante para la recolección de información, puesto que dio lugar a la obtención de documentos principales y secundarios para la elaboración de dicho informe.

3.4.2. Instrumentos

- *Cuestionario*: Esta fue aplicada a los trabajadores de dicha sub gerencia, teniendo una encuesta previamente diseña para conocer las perspectivas de dichos trabajadores.

- *Entrevista:* Esta se aplicó directamente al jefe de la Oficina de informática.

- *Notas de campo:* Estas se llevaron a cabo al momento del desarrollo de la investigación, con el que se tuvo apuntes de las observaciones, indagaciones y entrevistas con algunos trabajadores.

3.5. MÉTODO

Llevar a cabo una auditoría de sistemas computacionales requiere una serie ordenada de acciones y procedimientos específicos, los cuales deberán ser diseñados previamente de manera secuencial, cronológica y ordenada, de acuerdo a las etapas, eventos y actividades que se requieran para su ejecución, mismos que han sido establecidos conforme a las necesidades especiales de la institución. Además, estos procedimientos se adaptan de acuerdo al tipo de auditoría de sistemas que se realizar, y con estricto apego a las necesidades, técnicas y métodos de evaluación del área de sistemas de información. Muñoz. (2002).

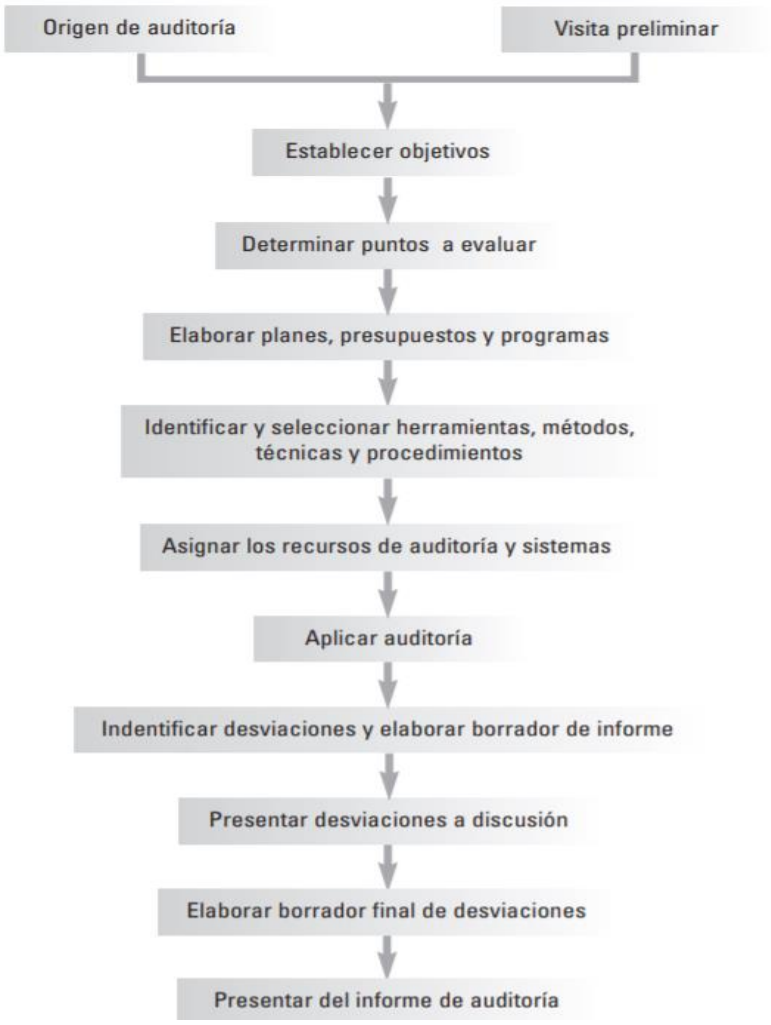

***Figura 7*:** Procesos de auditoria

Fuente: (Muñoz, 2002)

A partir de este proceso de auditoria se partirá considerando los puntos a ser auditados tomando en cuenta el marco de trabajo para el gobierno y la gestión de las TI, basado en 5 dominios y 37 procesos que tiene COBIT 5.

3.6. PROCESOS METODOLÓGICO

3.6.1. Puntos a auditar

a. Evaluación de los objetivos del centro de informática

b. Evaluación de la seguridad de los sistemas de información

c. Evaluación de la información, documentación y registros de los sistemas

d. Evaluación de los recursos humanos del área de sistemas

e. Evaluación del sistema de información

3.6.2. Selección de procesos COBIT V5

a. Evaluación de los objetivos del centro de informática

APO01 Gestionar el Marco de Gestión de TI

Descripción del Proceso de COBIT 5: Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.

b. Evaluación de la seguridad de los sistemas de información

MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno

Descripción del Proceso COBIT 5. Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar

y mantener normas para la evaluación del control interno y las actividades de aseguramiento.

c. Evaluación de la información, documentación y registros de los sistemas

BAI02 Gestionar la Definición de Requisitos

Descripción del Proceso COBIT 5: Identificar soluciones y analizar requisitos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocio, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requisitos y soluciones propuestas.

d. Evaluación de los recursos humanos del área de sistemas

APO07 Gestionar los Recursos Humanos

Descripción del Proceso de COBIT 5: Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada

e. Evaluación del sistema de información

MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad

Descripción de Proceso COBIT 5: Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están

realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.

3.6.3. Ponderación

Tabla 2: Ponderación de los puntos a auditar

Factores primarios que serán ponderados	Peso específico
Objetivos del centro de informática	10%
Seguridad de los sistemas de información	25%
Información, documentación y registros de los sistemas	20%
Recursos humanos del área de sistemas	20%
Sistema de información	25%
Peso total de la ponderación	100%

Fuente: Equipo de trabajo.

3.6.4. Técnicas de evaluación

Tabla 3: Técnicas de evaluación para la auditoria

Referencia	Actividad o función para evaluar	Técnica de Evaluación	Ponderación	Calificación
GA-01	Objetivos del centro de informática.	Revisión documental Acta testimonial Matriz de evaluación	10%	No cumple:1 Limitaciones:2 Completo:3
GA-02	Seguridad de los sistemas de información	Examen Inspección Confirmación Acta testimonial	25%	No cumple:1 Limitaciones:2 Completo:3
GA-03	Información, documentación y registros de los sistemas	Comparación Revisión documental Acta testimonial Matriz de evaluación	20%	No cumple:1 Limitaciones:2 Completo:3
GA-04	Recursos humanos del área de sistemas	Inspección Confirmación Revisión documental Acta testimonial	20%	No cumple:1 Limitaciones:2 Completo:3
GA-05	Sistema de información	Examen Inspección Confirmación Revisión documental	25%	No cumple:1 Limitaciones:2 Completo:3
TOTAL			**100%**	

Fuente: Equipo de trabajo.

3.6.5. Evaluación de acuerdo al gobierno y la gestión de las TI, basado en los procesos que tiene COBIT 5.

Tabla 4: Evaluación de los puntos a auditar en base a los procesos COBIT5

Referencia	Actividad o función para evaluar	Técnica de Evaluación	Instrumentos	Ponderación	Calificación	Observación
GA-01	Objetivos del centro de informática.	Revisión documental Acta testimonial Matriz de evaluación	Entrevistas Cuestionarios Encuestas Observación	10%	No cumple:1 Limitaciones:2 Completo:3	Se evaluará de acuerdo a los procesos COBIT 5: **APO01** Gestionar el Marco de Gestión de TI
GA-02	Seguridad de los sistemas de información	Examen Inspección Confirmación Acta testimonial	Cuestionarios Encuestas Observación Experimentación	15%	No cumple:1 Limitaciones:2 Completo:3	Se evaluará de acuerdo a los procesos COBIT 5: **MEA02** Supervisar, Evaluar y Valorar el Sistema de Control Interno
GA-03	Información, documentación y registros de los sistemas	Comparación Revisión documental Acta testimonial Matriz de evaluación	Observación Cuestionarios Experimentación	10%	No cumple:1 Limitaciones:2 Completo:3	Se evaluará de acuerdo a los procesos COBIT 5: **BAI02** Gestionar la Definición de Requisitos
GA-05	Recursos humanos del área de sistemas	Inspección Confirmación Revisión documental Acta testimonial	Entrevistas Cuestionarios Encuestas Observación	10%	No cumple:1 Limitaciones:2 Completo:3	Se evaluará de acuerdo a los procesos COBIT 5: **APO07** Gestionar los Recursos Humanos
GA-05	Sistema de información	Examen Inspección Confirmación Revisión documental	Cuestionarios Observación Experimentación	20%	No cumple:1 Limitaciones:2 Completo:3	Se evaluará de acuerdo a los procesos COBIT 5: MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad
TOTAL				100%		

Fuente: Equipo de trabajo.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

En la investigación, se ha desarrollado actividades de recolección de información para determinar la gestión de los sistemas informáticos y si estos cumplen con asegurar la integridad de la información de la Municipalidad; la calificación de los procesos de auditoría está delimitados mediante las vulnerabilidades de la entidad, en el cual establecemos algunos procesos con altas prioridades, la identificación de estos procesos del COBIT 5, se dio a partir de los objetivos planteados y los puntos a ser auditados. Todo el proceso desarrollado nos ayudará a plantear recomendaciones para que después sean tomados como referencia ante eventuales diligencias para mejorar los criterios de toma de decisiones por parte del encargado de la oficina de informática y tecnología, conjuntamente con las autoridades de la Municipalidad Distrital de Pilcuyo.

4.1. EVALUACIÓN DE LA GESTIÓN DEL SISTEMA INFORMACIÓN DE ADMINISTRACIÓN TRIBUTARIA DE LA OFICINA DE INFORMÁTICA Y TECNOLOGÍA DE LA MUNICIPALIDAD DISTRITAL DE PILCUYO.

4.1.1. Situación actual de la municipalidad distrital de Pilcuyo

La Municipalidad Distrital de Pilcuyo es una organización dedicada exclusivamente a administrar los recursos y garantizar la atención de las necesidades de la población con recurso humano competente, organizados y articulando diversos actores estratégicos. Su finalidad es promover el empleo, bienestar social y desarrollo de las necesidades de los ciudadanos que la conforma.

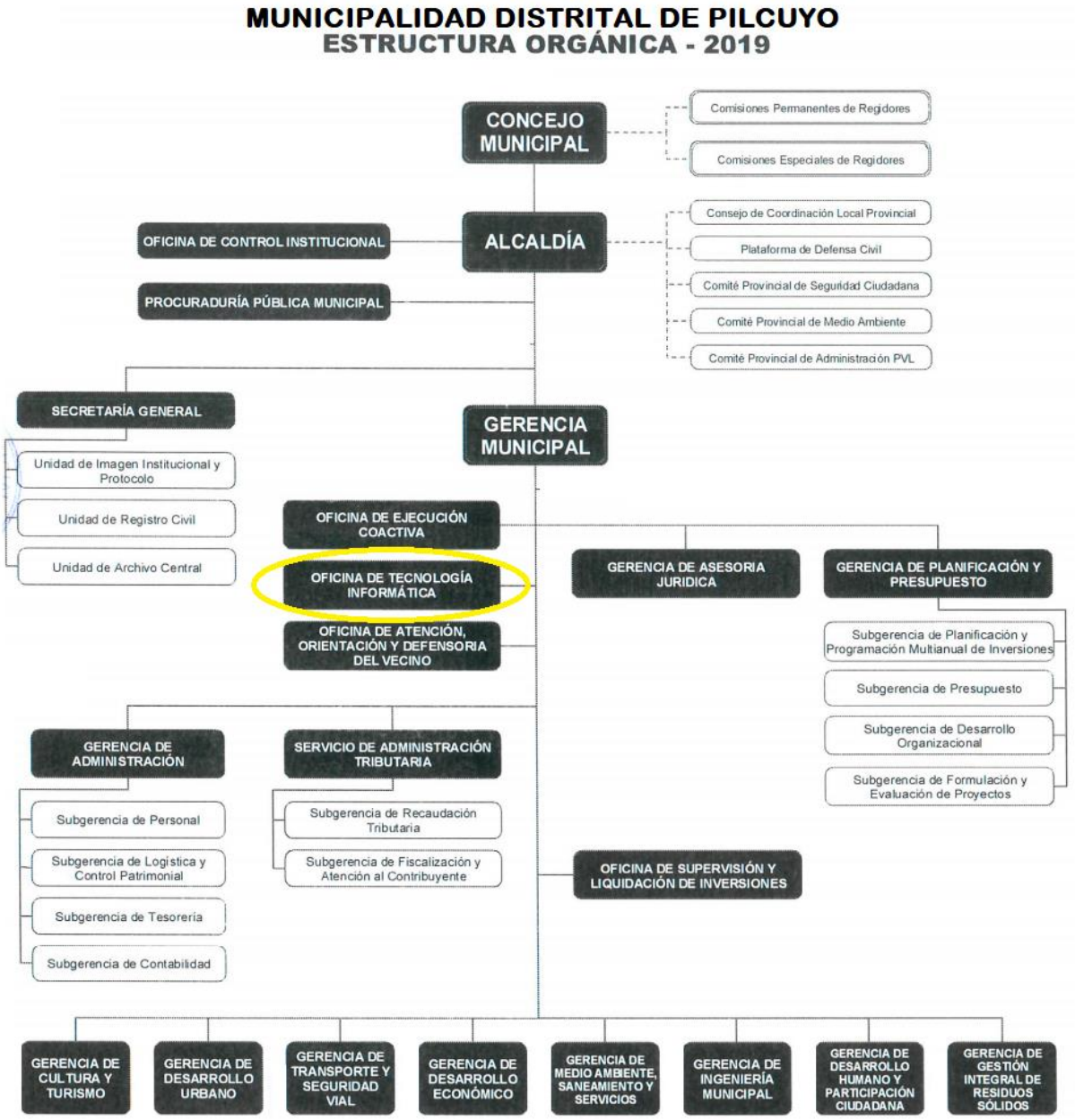

***Figura 8*:** Organigrama de la Municipalidad Distrital de Pilcuyo

Fuente: (Manual de organización y funciones de la Municipalidad Distrital de Pilcuyo, 2019)

4.1.2. Situación actual de oficina de informática y tecnología de la Municipalidad Distrital de Pilcuyo

Como se observa en la figura 7, cuenta con una oficina de informática y tecnología cuyo objetivo es mantener los sistemas informáticos óptimos y brindar soporte técnico a todos los demás órganos de la municipalidad, con especial énfasis en el mantenimiento de los sistemas de información, a través de la automatización de los procesos manuales, contribuyendo a la oportuna toma de decisiones y a la optimización de la gestión municipal para el cumplimiento de objetivos de este.

Objetivos de la oficina de informática y tecnología

- Incrementar el conocimiento del personal de la Municipalidad de distrital de Pilcuyo en los sistemas informáticos propios del municipio.
- Incrementar la eficacia del servicio de tecnología a usuarios mediante la utilización de conceptos y buenas prácticas para la gestión de servicios de Tecnología de la Información, así como la elaboración y difusión de políticas de uso de los recursos.
- Incrementar la eficacia y eficiencia en la gestión de infraestructura y servicios tecnológicos mediante la definición de procesos y la generación de nuevos servicios para los funcionarios de la Municipalidad de Pilcuyo.

Así mismo se realizó un breve diagnóstico, planteándose así un breve análisis de FODA de dicha oficina

Tabla 5: Análisis de fortalezas y debilidades de la oficina de tecnología e informática

FORTALEZAS	DEBILIDADES
- Buena comunicación en la institución - Personal con experiencia en las diferentes áreas - Reconocer que se debe mejorar internamente - Organización y cumplimiento de objetivos	- Espacio físico reducido - Escaso personal en las áreas - Escasa capacitación al personal del área - Escaso equipamiento y los sistemas están en proceso de modernización - Falta de planes y políticas a largo plazo en la sub gerencia

Fuente: Equipo de Trabajo.

Tabla 6: Análisis de oportunidades y amenazas de la oficina de tecnología e informática

OPORTUNIDADES	AMENAZAS
- Mejorar la imagen para con los ciudadanos. Aplicación de nuevas tecnologías. - Avances tecnológicos en software y hardware.	- Falta de colaboración y apoyo por parte de la gerencia municipal. - No existe una buena distribución de funciones - Incorrecta asignación de presupuestos. - No existe un software que permita tener la información segura

Fuente: Equipo de trabajo.

La Oficina de Informática y Tecnología, es quien está a cargo del único sistema de administración tributaria y es quien se debe de encargar de velar por la disponibilidad e integridad de los datos mediante copias de seguridad y replicación de datos, pero realizando los estudios pertinentes se observó que no hay un mecanismo para resguardar la seguridad de la información generada por el sistema. En cuanto a las tareas son controlados y ejecutados por el jefe y único trabajador del área de informática, quien a su vez es el encargado de dar mantenimiento y garantizar el

óptimo funcionamiento de los softwares y aplicaciones que se manejan en toda la municipalidad.

En la actualidad no se han realizado auditorias informáticas, pero cuentan con documentación de años anteriores, donde establecen sus funciones también cuentan con Planes de Contingencia para poder prevenir accidentes o fallos en aplicaciones informáticas, equipos tecnológicos y otros sistemas los que no fueron ejecutados.

4.1.3. Situación actual del sistema de administración tributaria de la Municipalidad Distrital de Pilcuyo

El sistema de administración tributaria tiene por objetivo recaudar impuestos en del distrito de Pilcuyo, fue implementado en el año 2018 según información brindara por el jefe de la oficina de informática y tecnología, con el lenguaje de programación Oracle Developers 6i, trabajando con la base de datos Oracle 12c, así mismo, la creación de ventanas se realizó con Forms builders y para generar los reportes se tuvo que utilizar Reports builders. Dicho sistema. En tanto actualmente el municipio enfrento un incremento de información, creando vulnerabilidad ante la inseguridad del sistema; a continuación, se muestra la entrevista realizada al jefe de la oficina de informática y tecnología de la municipalidad distrital de Pilcuyo.

Tabla 7: Entrevista al jefe de la oficina de informática y tecnología

ENTREVISTA REALIZADA AL JEFE DE LA OFICINA DE INFORMATICA Y TECNOLOGIA DE LA MUNICIPALIDAD DE PILCUYO		
Objetivo	Recolectar información de la situación actual del Sistema de administración tributaria y del departamento de Tecnologías de la Información en la municipalidad de Pilcuyo.	
Fecha:	28 de Julio del 2019	
Entrevistado:	Responsable de la Oficina.	
Cargo:	Jefe de la oficina de tecnología e informática	
N°	**Preguntas**	**Respuestas**
1	¿En la oficina de informática y tecnología cuentan con un plan de mejora del sistema?	Sí, tenemos un plan, para proveer un nuevo sistema de administración tributaria, puesto que para este área se necesita un sistema que cumpla con respaldo de seguridad, para manejar temas económicos.
2	¿Tienen algún plan para manejar la seguridad de la información que genera el sistema?	Actualmente no contamos con un plan de seguridad, en tanto se planteara un proceso de consultoría en seguridad de información a nivel de tecnologías puesto que el sistema es muy vulnerable.
3	¿Con cuántos sistemas cuenta la institución?	Solo existe un sistema y dentro de estos varios módulos que se comunican entre sí.
4	¿Sabe si alguna vez se realizó auditoria informática en la oficina de informática y tecnología?	No, porque la oficina se está implementando recientemente este último año..
5	¿Crees que es necesario realizar auditoria informática en la oficina de tecnología e informática?	A mi percepción si, para ver el estado actual en que se encuentra la oficina.
6	¿Crees que la información que maneja el municipio es importante?	Si, la información siempre será importante en todas las instituciones, pues hoy en día la información se ha convertido un activo fijo.
7	¿La oficina de informática y tecnología, alguna vez ha sufrido algún ataque informático?	Hasta el momento no se realizó pruebas de hacking ético en la oficina para demostrar encontrar en si las vulnerabilidades del sistema, en tanto no sabría decirle si existe vulnerabilidad o algún ataque informático.
8	¿Cuentan con documentación donde se establezca funciones de su área de trabajo?	Si, cada área cuenta con documentación donde se especifica las funciones que desarrollamos.
9	A su consideración, ¿Piensa que el personal que trabaja en el área está capacitado para desempeñar sus funciones?	Si está capacitado para manejar los módulos que ellos manejan, ya que las nuevas tecnologías nos exigen capacitación e investigación es los procesos que se va a conciliar con todos para llegar a una nivelación para todos.
10	Para cumplir las funciones del área, ¿Se requiere contratar a terceros?	Raras veces, para intercambiar información entre instituciones, siempre y cuando con los convenios que existan, más no para utilizar los módulos.
11	¿Alguna vez han existido problemas con los usuarios que manejan el sistema?	Por lo general, a nivel de roles ya que no se han definido correctamente que roles se les ha asignado.

12	¿El municipio tiene manuales de procedimientos actualizados y procesos que deben de realizarse?	Si se cuentan con manuelas de procedimiento y de cada proceso que se realiza se genera información, mediante el trabajo que se realiza.

ENTREVISTADOR: Bach. José Luis Aro Maquera

Fuente: Equipo de Trabajo

En tanto con respecto a la Tabla 1, según la entrevista realizada al jefe de la oficina de informática y tecnología, se logró entender que en la oficina no se realizó trabajos de Auditoria en el área de Informática, para poder determinar las situación actual en la que se encuentra dicha oficina, así mismo, se evidencio que no existe algún plan de mejora o estratégico que nos ayude a visualizar a saber qué sucedería en caso de pérdida de información que pueda presentar el Sistema de Administración Tributaria. También se pudo verificar que en la oficina existen inconvenientes críticos como la deficiente asignación de perfiles, en si con la creación de usuarios; por último, se verifico que no existen políticas que ayuden con el manejo adecuado de los procesos y de la información generada.

4.1.3.1. Documentación del Sistema de Administración Tributaria

Para realizar este proceso se solicitó al jefe de la oficina de informática y tecnología para que nos pueda brindar información, para verificar la documentación que existe; esta se presenta en la siguiente tabla.

Tabla 8: Documentación del Sistema de Administración Tributaria

Documentación	Validación	Observación
Plan de Contingencia.	No cumple.	No se cuenta con un plan de contingencia, para entender que procedimiento se debe de realizar en caso que el sistema pueda fallar o colapsar.
Plan estratégico.	No cumple.	No se cuenta con un plan estratégico que ayude con las mejoras al sistema de Administración Tributaria.
Levantamiento de requerimientos.	No cumple.	No existe documentación alguna, que pueda ayudar al levantamiento de requerimientos del proceso administración tributaria.
Diagramas de Flujo.	No cumple.	No existen ninguna documentación del diagrama de flujo que ayuden a comprender el manejo del sistema de administración tributaria.

Fuente: Equipo de trabajo

En tanto se pudo verificar que el Sistema de Administración Tributaria no existe documentación necesaria que ayude a comprender los proceso que realiza el sistema, así mismo, no existe información sobre el levantamiento de requerimientos, para poder entender cómo se ha estructurado en sistema.

4.1.3.2. Base de datos

La base de datos utilizada en la Municipalidad distrital de Pilcuyo es Oracle 12c, esta es manejada por el área de informática y tecnología.

Las características que presenta un DBMS son las siguientes:

- Seguridad e integridad en los datos.
- Cuenta con lenguajes para realizar consultas de manera interactiva.
- Introducción y edición de datos de manera interactiva.

Por lo general esta base de datos es utilizada a nivel mundial, puesto que su ventaja es la ejecución en cualquier plataforma; los respaldos se realizan todos los días a media noche, para poder resguardar la información generada en el día. Como también el inconveniente que tiene se da al momento de crear los usuarios, puesto que no se tiene definido el rol y perfil del usuario que se crea en la base de datos.

4.1.3.3. Redes y comunicaciones.

Las redes y comunicación son el conjunto de elementos que están conectados entre sí, es así que en la Municipalidad distrital de Pilcuyo, utilizan los Checkpoint y el firewall. Puesto que el checkpoint ayuda con el monitoreo del tráfico de red entrante y saliente mediante la generación de reglas, definiendo permisos de acceso a la red, de acuerdo al perfil de cada usuario del municipio. Así mismo, el Firewall permitirá evitar ataques que no sean deseados y sobre todo el manejo de páginas web. Por ultimo podemos mencionar que la conexión de los equipos de la Municipalidad distrital de Pilcuyo, se da mediante IP estáticas y DHCP que están unidos al domingo de la institución.

4.1.3.4. Seguridad lógica

La seguridad lógica que maneja el municipio debería estar controlada por la oficina de informática y tecnología, en tanto esta no cuenta con sistemas que protegen digitalmente la información de manera directa, se requiere que el área de informática implemente estos sistemas, puesto que la información que genera, está siendo vulnerable ante los ataques informáticos, por lo que se debería de manejar varios tipos de seguridad como:

- Control de accesos a la red, es decir se deben de utilizar nombre de usuarios y contraseñas y equipos específicos que pertenecen al entorno del municipio para

evitar ataques informáticos.

- Antivirus actualizados, que ayudaran detectar la entrada de virus a los equipos que se encuentran en óptimas condiciones.

- Cortafuegos(firewall), que nos ayuda que muchos dispositivos de software, de hardware que permiten, deniegan o restringen el acceso al sistema. Protege la integridad de la información

4.1.3.5. Seguridad física

En cuanto a la seguridad física, la municipalidad cuenta con colaboradores capacitados que controla ingresos de usuarios mediante un registro manual donde se especifica el motivo y área de ingreso, como también se decepciona el documento de identidad hasta su salida, en cuanto al personal que labora en la institución se cuenta con un sistema biométrico de control. Así mismo para el ingreso a la oficina de informática y tecnología donde se encuentra el datacenter, se permite solo el acceso al personal autorizado de la institución.

Entonces con el análisis y la documentación revisada, se pudo evidenciar las carencias del área de informática y tecnología de la municipalidad, que presentan en la Base de Datos, Redes y Comunicación, Seguridad Física y Seguridad Lógica, En tanto estas nos servirán para ser separadas en los diferentes principios de Cobit 5 dependiendo las características que cumplan.

4.2. AUDITORIA INFORMÁTICA APLICANDO LA METODOLOGÍA COBIT 5 AL SISTEMA DE ADMINISTRACIÓN TRIBUTARIA DE LA OFICINA INFORMÁTICA Y TECNOLOGÍA DE LA MUNICIPALIDAD DEL DISTRITO DE PILCUYO.

Para realizar el siguiente proceso se hizo uso de los cinco principios de la metodología COBIT 5, para realizar la clasificación de las distintas pruebas realizadas y separarlas de acuerdo a las características que estas cumplan.

Tabla 9: Pruebas realizadas divididas por Principios COBIT 5

PRINCIPIOS / PRUEBAS	**Principio 1:** Satisfacer las Necesidades de las Partes Interesadas	**Principio 2**: Cubrir la Empresa Extremo a Extremo	**Principio 3:** Aplicar un Marco de Referencia único integrado	**Principio 4:** Hacer Posible un Enfoque Holístico	**Principio 5**: Separar el Gobierno de la Gestión.
BASE DE DATOS					
P001: Acceso de los usuarios	X	X		X	
P002: Creación de usuarios y contraseñas.	X	X		X	
P003: Selección de personal de tecnologías de la información.	X	X		X	
P004: Documentación de procesos de base de datos entregada al personal.	X	X		X	
P005: Estabilidad de la base de datos en transacciones información (rollback)	X	X		X	
P006: Recuperación Información (backups)	X	X		X	
P007: Control de cambios en la estructura de la base de datos.	X	X		X	
P008: Control de duplicidad de información.	X	X		X	
P009: Estándares de nomenclatura al momento de creación de tablas.	X	X		X	

REDES Y COMUNICACIÓN			
P010: Comprobar la seguridad configurada en el software para acceso remoto al Sistema de Administración Tributaria.	X	X	X
P011: Acceso de las personas que ingresan a las instalaciones y que trabajos se disponen a realizar en los servidores.	X	X	X
P012: Integridad del cableado estructurado.	X	X	X
P013: Configuración del firewall por parte del proveedor.	X	X	X
P014: Protocolos con los que trabajan las aplicaciones.	X	X	X
P015: Seguridad del checkpoint.	X	X	X
P016: Encriptación de información.	X	X	X
SEGURIDAD LÓGICA			
P017: Logs de la base de datos.	X	X	X
P018: Software instalado en los equipos de cómputo.	X	X	X
P019: Licencias del software instalado en los equipos de cómputo cliente.	X	X	X
P020: Eliminación de archivos temporales y obsoletos.	X	X	X
P021: Creación de usuarios y contraseñas del Sistema de Administración Tributaria.	X	X	X
P022: Tipo de procedimiento de redundancia.	X	X	X
P023: Comprobación de los antivirus.	X	X	X

P024: Administración de los dispositivos de almacenamiento de los backups.	X	X	X
SEGURIDAD FÍSICA			
P025: Sistemas de vigilancia (Cámaras).	X	X	X
P026: Seguridad del sistema biométrico.	X	X	X
P027: Contratos de los empleados de seguridad	X	X	X
P028: Contraseñas de acceso a la BIOS.	X	X	X
P029: Verificación de los UPS.	X	X	X
P030: Acceso al data center.	X	X	X

Fuente: Equipo de trabajo.

X: Si Cumple.

Los resultados se presentarán de manera general, para tener una orientación clara del porque una prueba no cumple con alguno de los principios Cobit 5. Se tiene lo siguiente:

Principio 1. Satisfacer las Necesidades de las Partes Interesadas

Las pruebas realizadas en el primer principio cumplen con las necesidades de las partes extremas e internas, en tanto que lo externo se refiere a la sociedad en general, es decir clientes, auditores externos y con lo interno a la organización administrativa, es decir los responsables de los procesos de negocios y auditores internos.

Principio 2: Cubrir la Empresa Extremo-a-Extremo

Las pruebas realizadas en el segundo principio se cumplen, puesto que en este principio se verifica el control y manipulación de roles del negocio, y como estos serán utilizados y manejados por las distintas actividades, roles en relación a la tecnología de información.

Principio 3: Aplicar un Marco de Referencia único integrado

Las pruebas realizadas en el tercer principio no se cumplen, puesto que la oficina de informática y tecnología no ha generado pruebas que ayuden a seguir un adecuado proceso, para llegar a cumplir dicho principio se tendría que realizar pruebas las cuales se rijan a un estándar o norma.

Principio 4: Hacer Posible un Enfoque Holístico

Las pruebas realizadas en el cuarto principio se cumplen pero no en una totalidad en tanto que se tiene un comportamiento ético de los trabajadores y de la institución las que aportaran al cumplimiento de las leyes, políticas y procedimientos internos, los que ayudaran a proteger la información y por ende a los activos tecnológicos de información; en cuanto a los servicios infraestructura y aplicaciones de la institución permiten el proceso de información y servicios relacionados con el Sistema de Administración Tributaria. Por otro lado, los principios, políticas y marcos de referencia se necesitan para cumplir y registrar las operaciones relevantes para el uso del Sistema de Administración Tributaria, se tiene deficiencias en los procesos para gestionar las actividades del sistema de administración tributaria y con las estructuras organizativas se tiene debilidades en la asignación de los roles asociadas al sistema de Administración Tributaria.

Principio 5: Separar el Gobierno de la Gestión

El quinto principio 5 no se podrá cumplir a cabalidad, puesto que las pruebas que se realizaron cumplirán con los principios de Gobierno en tanto que se evaluará, orientara y supervisará dichas pruebas aplicando eficientemente los principios Cobit 5, por otro lado, no se logrará cumplir con el principio de gestión puesto que no hay un área encargada de planificar ni construir las políticas. En tanto no se podrá cumplir a cabalidad.

4.3. INFORME DE LA AUDITORÍA INFORMÁTICA SOBRE LA GESTIÓN DEL SISTEMA DE INFORMACIÓN DE LA OFICINA DE INFORMÁTICA Y TECNOLOGÍA DE LA MUNICIPALIDAD DISTRITAL DE PILCUYO.

4.3.1. Introducción

El presente informe realizado muestra la evaluación ejecutada al Sistema de Administración Tributaria el cual es el encargado de la recaudación de bienes en la ciudad de Pilcuyo, las áreas evaluadas fueron Base de Datos, Redes y Comunicación, Seguridad Lógica y Seguridad Física las cuales están vinculadas a dicho sistema de la Municipalidad distrital de Pilcuyo.

De acuerdo con la auditoría realizada se pudo concluir que la oficina de informática y tecnología, se encarga de la gestión de información, contribuyendo a la toma de decisiones del municipio y por ende de la oficina, considerando al Sistema de Administración Tributaria como un activo tecnológico de suma importancia; es tanto mediante la realización de la autoría informática se garantizara normativas y procesos para disminuir los riesgos en la información, estos basados en el Cobit 5.

4.3.2. Alcance de la auditoria

En la auditoría realizada se evaluaron sobre todo aspectos de seguridad lógica, procedimiento y alguna que otra documentación para la evaluación de controles a los procesos seleccionados mediante un análisis de riesgo, que permitan revelar la condición de seguridad de la información del sistema de información del municipio

4.3.3. Objetivo de la auditoria

El objetivo principal de esta auditoría fue realizar auditoria informática usando las normas COBIT v.5 en la oficina de informática y tecnología.

4.3.4. Periodo de ejecución

La auditoría comprende el periodo desde el 1 de junio del 2020 al 30 de setiembre del 2020, en donde se realizó una evaluación especial a la oficina de informática y

tecnología y al sistema de administración tributaria de la Municipalidad Distrital de Pilcuyo

4.3.5. Marco referencial

El marco de referencia utilizado para esta auditoría informática es COBIT 5, el cual está basado en procesos y objetivos de control de las tecnologías de la información y comunicación que pueden ser implementados para auditar, controlar y administrar una organización. Está basado en las mejores prácticas y sistemas de información de auditoría y control de los sistemas informáticos**.**

4.3.6. Hallazgos

Los hallazgos que se tuvieron en la auditoría realizada fueron los siguientes:

Base de Datos: Tomando en cuenta las pruebas de diseño y ejecución de auditoria informática se evidencio lo siguiente:

- No se encontró estándares de asignación de usuarios y contraseñas.
- No se encontró manuales para la asignación de perfiles y de contratación.
- No se evidencio ejecuciones de pruebas técnicas.
- No existe manejo de documentación ni estructuración para la base de datos.
- No cuenta con registros de proceso para la recuperación de información
- Existe escasos procesos de backups.

Redes y Comunicaciones: Tomando en cuentan el diseño y ejecución de pruebas de Auditoria Informática, se evidencio lo siguiente:

- No existe registro de equipos con acceso remoto por VNC.
- No existen planos de cableado estructurado usados en el municipio.

- No realizan configuraciones del firewall.
- No cuentan con registros de aplicaciones y páginas web utilizadas.
- No tienen un manual que para el uso de protocolos, ni registros de los protocolos utilizados.
- No existe un manual, registros del personal encargado, reglas empleadas ni registros sobre las configuraciones del checkpoint.

Seguridad Lógica: Tomando en cuenta cuentan el diseño y ejecución de pruebas de Auditoria Informática, se evidencio lo siguiente:

- No existe procesos para la creación de logs.
- No existe un registro de procesos a utilizar ni cada cuanto tiempo se utilizarán los logs.
- No existen manuales, licencias ni registros de los software adquiridos en el municipio.
- No se cuentan con registros de los procedimientos para liberar espacios ni eliminación de archivos temporales y obsoletos.
- Carencia de estándar para la asignación de usuario y contraseñas (Mayúsculas, minúsculas, caracteres especiales).
- No se encontró documentación de tipo de raid que es utilizada en el municipio.
- No se encontró registro sobre las licencias de antivirus.
- No existe registros de la utilización de medios magnéticos
- No existe registros de etiquetado ni etiquetas que definan el contenido y nivel de seguridad.

Seguridad Física: Tomando en cuenta cuentan el diseño y ejecución de pruebas de Auditoria Informática, se evidencio lo siguiente:

- No existen manuales de uso, planos de ubicación, ni registros de cámaras de vigilancia que fueron instaladas en el municipio.
- No existe registros del tiempo en que se elimina la información la información recopilada.
- No se encontró los manuales del sistema biométrico, manejado para el control de personal.
- No se encontró registros sobre las configuraciones de la Bios.
- No se encontró los manuales de uso de los UPS del municipio.
- No existe inventarios ni planos de ubicación de los UPS.

4.3.7. Recomendaciones y sugerencias.

Una vez determinada las falencias e incumpliendo de requisitos mínimos que debe tener una institución en cuanto a tecnología se recomienda lo siguiente:

En cuando a la base de datos se deberá generar y contar con la documentación necesaria en cuando a procesos, políticas y estándares que ayuden a la gestión de recursos de manera óptima; como también, se deberá tener documentación en cuando al firewall, protocolos de seguridad y checkpoint, que apoye a la comprensión de los procesos, políticas y estándares que se deben de efectuarse. Así mismo, se debe implementar documentación del software adquirido y registros de eliminación de información, adquisición de licencias de software y antivirus y medios magnéticos que son importantes para el municipio; por último, se debe se implementar documentación sobre la adquisición, registros de manejo, ubicación y características de las UPS, sistemas biométricos y cámaras de vigilancia.

4.3.8. Plan de mejores prácticas

En estos planes de mejora se recomendará y se aran sugerencias en cuanto a las áreas de base de datos, redes y comunicación, seguridad lógica y seguridad física,

con las cuales se podrá aumentar la eficacia y eficiencia del sistema de información, puesto que se tendrá integridad, confidencialidad y confiabilidad en cuanto a la seguridad.

Tabla 10: Plan de mejores prácticas para Base de Datos

Pruebas		**Prácticas de mejora**		
Objetivo	**Resultados**	**Tareas**	**Recursos**	**Tiempo**
P001: Acceso de los usuarios				
Verificar las políticas para el acceso de usuarios.	- No tienen registros de logs para comprobar el acceso de los usuarios que desean ingresar a la base de datos.	Registrar ingresos de los usuarios que accedan a la base de datos.	- Registro de usuarios - Verificar registros de los logs - Verificar el número de intentos de acceso a la base de datos.	10 días hábiles
P002: Creación de usuarios y contraseñas.				
Verificar las políticas de creación de usuarios y asignación de perfiles.	- No cuentan con un estándar ni procesos adecuados para la asignación de perfiles. - Las contraseñas asignadas no cuentan no se rigen a estándares adecuados.	Creación de usuarios de acuerdo a los perfiles y cargo que desempeña	- Registro de usuarios del área de desarrollo. - Estándares para la asignación de usuarios y contraseñas (Mayúsculas, minúsculas, caracteres especiales). - Asignación de perfiles.	28 días hábiles
P003: Selección de personal de tecnologías de la información.				
Validar el proceso de selección del personal de tecnología e informática de acuerdo al perfil solicitado	- No existe información necesaria, para validar la prueba	Justificar que procesos se deben de tomar en cuenta para la selección del personal.	- Manual de contratación para el personal de la oficina de informática y tecnología	15 días hábiles
P004: Documentación de procesos de base de datos entregada al personal.				
Verificar la documentación de procedimientos y manejo de BD entregada al personal	- No existe documentación para tener conocimiento sobre los procedimientos y manejo de base de datos.	Comprender la adecuada gestión de base de datos.	- Documentación de la base de datos. - Ejecución de la documentación.	15 días hábiles
P005: Estabilidad de la base de datos en transacciones información (rollback).				
Identificar el proceso para la recuperación de información de la base de datos	- No existe documentación para la recuperación de información ya sea por pérdida o eliminación	Tener adecuados procesos para recuperar información	- Registros de procedimientos para recuperación de información.	28 días hábiles
P006: Recuperación de Información (backups).				
Verificar procesos de recuperación de información de	- No existe un manual de procedimientos sobre los procesos a cuáles se	Mostrar los procesos de recuperación de	- Registros de proceso de creación de backups. - Registros del tiempo	28 días hábiles

la base de datos, cuando es eliminada accidentalmente.	pueden realizar backups. - No existe documentación donde indiquen el tiempo de realización de backups.	información en la base de datos.	para e realizar los backups. - Almacenamientos de los backups en condiciones óptimas. - Pruebas semestrales de los Backups	
P007: Control de cambios en la estructura de la base de datos.				
Verificar los procesos de los cambios establecidos para la base de datos.	- No existe un manual de procedimientos adecuados. - Se realizan cambios con solicitudes verbales los que no respaldan con documentación dichos cambios.	Manuales sobre el procedimiento para realizar cambios en la base de datos.	- Manual de procesos para generar cambios. - Registros de los cambios realizados.	15 días hábiles
P008: Control de duplicidad de información.				
Verificar los procesos para evitar la duplicidad de información.	- No se encontró documentación sobre las estructuras de la base de datos - Al no contar con la estructura de base de datos, no se tiene evidencias sobre el atributo que viene a ser la clave primaria en las tablas creadas.	Evitar la redundancia y por ende la duplicidad de información en la base de datos.	- Implementación de una estructura de la base de datos. - Creación de claves primarias.	10 días hábiles
P009: Estándares de nomenclatura.				
Verificar los procesos adecuados para crear tablas.	- No presentan un manual para la adecuada creación de tablas.	Determinar normas y procedimientos para la creación de tablas, usuarios o contraseñas.	- Manual de procedimiento para la creación de tablas.	10 días hábiles
El responsable de la ejecución de las prácticas de mejora la deberá realizar el Jefe de la oficina de informática y tecnología de la Municipalidad de Pilcuyo.				

Fuente: Equipo de trabajo.

Tabla 11: Plan de mejores prácticas para Redes y Comunicación

Pruebas		**Prácticas de mejora**		
P010: Comprobar la seguridad configurada en el software VNC para acceso remoto al Sistema de Administración Tributaria.				
Objetivo	**Resultados**	**Tareas**	**Recursos**	**Tiempo**

Validar la adecuada configuración sobre seguridad para el acceso remoto del VNC.	- Los equipos de la institución cuentan con el software VNC. - No se encuentran registros sobre la configuración del VNC.	Realizar controles de seguridad del VNC utilizado para la conexión al Sistema de Administración Tributaria.	- Registros de usuarios con acceso remoto por VNC. - Configuración de seguridad del VNC.	28días hábiles
P011: Acceso físico de las personas que ingresan a las instalaciones de servidores y que trabajos se disponen a realizar.				
Comprobar la seguridad para el acceso de usuarios a las instalaciones.	- Generalmente los permisos no son formales, otorgando permisos para el acceso a servidores de manera informal (verbal).	Realizar documentación sustentadora para el adecuado proceso de ingreso de terceros a las instalaciones.	- Registro de acceso de usuarios visitantes. - Registro de ambientes a los que se puede tener acceso.	15 días hábiles
P012: Integridad del cableado estructurado.				
Comprobar el cableado estructurado en las infraestructura instalada	- No cuentan con planos donde se evidencie la estructura del cableado realizado en la institución.	Implementar documentación sobre el cableado estructurado implementad.	- Documentación sobre los planos del cableado estructurado y normativas aplicadas para su implementación.	10 días hábiles
P013: Configuraciones del firewall por parte del proveedor.				
Verificar las configuraciones del firewall.	- No existe documentación para realizar configuraciones en el firewall. - No se evidencia registros para verificar las páginas restringidas	Revisar las configuraciones realizadas al firewall y las ventajas que esta tenga.	- Configuración del firewall. - Registro de los accesos a páginas web.	28 días hábiles
P014: Protocolos con los que trabajan las aplicaciones.				
Identificar los protocolos con los que trabajan las aplicaciones utilizadas en el municipio	- Identificar los protocolos con los que trabajan las aplicaciones utilizadas en el municipio	Manejar protocolos seguros para las aplicaciones de la institución.	- Listado de las aplicaciones. - Listado de protocolos utilizados. - Manual de utilización de protocolos.	15 días hábiles
P015: Seguridad del checkpoint.				
Comprobar la seguridad del checkpoint para	- No se puede obtener documentación del checkpoint.	Entender el manejo del checkpoint mediante reglas	- Políticas del checkpoint. - Registro de los	10 días hábiles

evitar ataques.	- No existe un listado en el cual se pueda ver las personas que tienen acceso al checkpoint. - No se puede obtener las reglas generadas en la institución por motivos de seguridad.	dadas por la institución.	usuarios encargados de los checkpoint. - Registros sobre reglas aplicadas en el checkpoint.	
P016: Encriptación de información.				
Comprobar la encriptación de la información	- No existe documentación para entender el manejo de la información. - Se desconoce el tipo de tipo de encriptación que utilizan.	Mediante la encriptación mantener la información segura	- Procedimientos para el manejo de información. - Tipo de encriptación utilizada	10 días hábiles
El responsable de la ejecución de las prácticas de mejora la deberá realizar el Jefe de la oficina de informática y tecnología de la Municipalidad de Pilcuyo.				

Fuente: Equipo de trabajo.

Tabla 12: Plan de mejores prácticas para Seguridad Lógica

Pruebas		**Prácticas de mejora**		
Objetivo	**Resultados**	**Tareas**	**Recursos**	**Tiempo**
P017: Logs de la base de datos.				
Verificar si los logs están realizando los backups en tiempos estipulados.	- No se encontró documentación para determinar los procesos adecuados de los logs. - No hay registros de los logs creados - No hay registros para observar cada cuanto tiempo se realizan los logs.	Realizar registros de los procesos que se realizan en la base de datos.	- Creaciones de logs. - Registro de los procesos a los que se realiza los logs. - Registro de evidencia de cada cuanto tiempo se ejecutan los logs.	10 días hábiles
P018: Software instalado en los equipos de cómputo				
Verificar las licencias de los software instalados	- No existen registros sobre la adquisición del software de la institución - La mayoría del software utilizado en la institución no cuenta con documentación pertinente.	Realizar registros del software instalados en los equipos	- Registros del software adquirido - Manual de uso del software. - Licencia para el funcionamiento del software.	56 días hábiles
P019: Licencias del software instalado en los equipos de cómputo cliente.				
Comprobar las licencias de los software instalado	- No se encontró registros sobre el tiempo de vigencia de las licencias - No se encontró registros sobre el número de licencias adquiridas	Verificar la vigencia de las licencias adquiridas	- Registro de las licencias adquiridas de cada software instalado. - Registro del número de licencias adquiridas de acuerdo a los equipos o al uso que le da el usuario - Registros del tiempo de vigencia de las licencias.	56 días hábiles
P020: Eliminación de archivos temporales y obsoletos.				
Comprobar el proceso para la liberación de espacio en los servidores.	- No cuentan con registros de creación de carpetas para el almacenamiento de información caducada u obsoleta.	Tener procesos adecuados para eliminar información ya obsoleta.	- Documentos sobre los procedimientos de liberación de espacio y eliminación de información obsoleta.	56 días hábiles
P021: Creación de usuarios y contraseñas del Sistema de Administración Tributaria.				
Verificar los procedimientos de	- Se tiene un estándar para la creación de usuarios,	Tener procesos formales para la creación de	- Registro de usuarios del área de desarrollo.	5 días hábiles

creación de usuarios.	pero no está formalmente documentada. - No se encontró estándares para la creación de contraseñas - No hay documentos que detallen la asignación de perfiles para los usuarios.	usuario y contraseña y la asignación específica de perfiles.	- Estándares para la asignación de usuario y contraseña - Determinaciones para la asignación de perfil.	
P022: Tipo de procedimiento de redundancia.				
Identificar el tipo de raid y cuál es el motivo por el que se utiliza	- No se encontró información sustentadora para identificar el tipo de raid utilizada - No se concedió acceso para la verificar el Raid.	Comprender la utilidad del tipo y las ventajas del Raid.	- Documentos formales del tipo de raid adquirido - Comprobar si la documentación pertenece al raid adquirido.	28 días hábiles
P023: Comprobación de los antivirus.				
Comprobar la actualización de los antivirus	- No se encuentran registro ni documentación para la verificación de la vigencia del antivirus.	Realizar mantenimientos óptimos de los antivirus.	- Documentos de adquisición de antivirus. - Licencia del antivirus.	56 días hábiles
P024: Administración de los dispositivos de almacenamiento de los backups.				
Verificar los dispositivos de almacenamiento.	- No existen registros de los dispositivos magnéticos utilizados - Por motivos de seguridad no se contrasto los etiquetados.	Inspeccionar los procesos de almacenamiento de información de la institución	- Registros de los dispositivos magnéticos utilizados. - Uso de etiquetas para definir contenido y nivel de seguridad. - Registro de etiquetado.	28 días hábiles
El responsable de la ejecución de las prácticas de mejora la deberá realizar el Jefe de la oficina de informática y tecnología de la Municipalidad de Pilcuyo.				

Fuente: Equipo de trabajo.

Tabla 13: Plan de mejores prácticas para Seguridad Física

Pruebas		**Prácticas de mejora**		
Objetivo	**Resultados**	**Tareas**	**Recursos**	**Tiempo**
P025: Sistemas de vigilancia (Cámaras).				

Revisar el funcionamiento adecuado de las cámaras de seguridad.	- Este sistema lo maneja el área de seguridad física por lo tanto no se puso acceder a la información	Implementar procedimientos óptimos de los sistemas de vigilancia, basados en la protección de datacenter.	- Manual de uso de las cámaras de vigilancia. - Inventariado de las cámaras de vigilancia implementadas - Ubicación de los sistemas de vigilancia (planos) - Registros del cuando se eliminara la información almacenada.	15 días hábiles
P026: Seguridad del sistema biométrico.				
Revisar las políticas del sistema biométrico	- Este sistema lo maneja el área de seguridad física por lo tanto no se puso acceder a la información	Implementar procedimientos para el buen uso de los sistemas biométricos, para evitar el acceso a terceras personas.	- Manual de uso para los sistemas biométricos. - Inventariado de los sistemas biométricos implementados - ubicación de los sistemas biométricos (planos) - Registros del cuando se eliminara la información almacenada.	15 días hábiles
P027: Contratos de los empleados de seguridad.				
Revisar los registros del personal del área de seguridad.	- No se pudo acceder a la información, para revisar documentación sobre el personal de seguridad	Verificar el proceso de selección de personal	- Registros del personal del área de seguridad. - Perfil del personal de seguridad - Contrato del personal de seguridad.	15 días hábiles
P028: Contraseñas de acceso a la BIOS.				
Comprobar si los equipos poseen contraseñas al momento de acceder a la BIOS.	- No existen registros ni documentos que ayuden con la asignación de contraseñas para acceder a la BIOS.	Determinar estrategias adicionales de seguridad, para evitar cambios del sistema operativo de los equipos.	- Inventariado de los equipos adquiridos - Documentación sobre las características de los equipos. - Registros de las configuraciones realizadas a la BIOS.	10 días hábiles
P029: Verificación de los UPS.				
Revisar el tiempo de adquirió de las UPS	- No existe documentación sustentable sobre los UPS. - No se tiene registros de inventariado de las adquisiciones de los UPS. - No existe planos para identificar la ubicación de los UPS.	Verificar las características y el funcionamiento de los UPS.	- Manual de uso de los UPS - Inventariado de los UPS adquiridos. - Ubicación de los UPS (planos)	15 días hábiles
P030: Acceso al datacenter.				

Verificar el acceso de los usuarios al datacenter.	- Se tiene con sistemas biométricos y cámaras, pero no existe documentos formales que sustenten las características de dichos sistemas. - No existe registros y documentos sobre el uso del programa Teamviwer O VPN.	Determinar procesos para el acceso al datacenter, el que será vigilado por cámaras de vigilancia y sistemas biométricos.	- Controles biométricos. - Monitoreo por cámaras de vigilancia - Acceso remoto mediante VPN. - Uso del Teamviwer.	5 días hábiles
El responsable de la ejecución de las prácticas de mejora la deberá realizar el Jefe de la oficina de informática y tecnología de la Municipalidad de Pilcuyo.				

Fuente: Equipo de trabajo.

Con la elaboración de los planes de mejores prácticas elaborados para las áreas de Base de Datos, Redes y Comunicación, Seguridad Lógica y Seguridad Física, de esta manera se contribuirá con la confidencialidad y confiabilidad en los procesos del Sistema de Administración Tributaria y de la oficina de informática y tecnología. Como se puede observar se ha cumplido todos los objetivos planteados, los cuales servirán para el beneficio del Sistema de Administración Tributaria y de la oficina de informática y tecnología de La Municipalidad distrital de Pilcuyo.

Discusión:

La auditoría informática permite identificar la metodología del uso de recursos de TI para la generación de información logrando el cumplimiento de los objetivos para los cuales fue establecido, además da a conocer vulnerabilidades e inconvenientes que obstaculizan el flujo de información. Jiménez (2016), en su investigación indica que los procesos de la auditoria sin necesarias en las organizaciones independientemente del tamaño o su entorno, puesto que permite que la organización tenga conocimiento de la condición y de cómo las tecnologías de información apoyan y fortalecen los procesos del negocio brindándoles grandes beneficios a costos de operación óptimos. En tanto se puede recalcar que realizar una autoría informática es necesaria en toda empresa, organización ya sea pública o privada, puesto que permitía optimizar los procesos del sistema de

información y a la vez permitirá conocer las vulnerabilidades a las que pueda estar propensa el sistema.

Por otro lado, el marco de referencia utilizado para esta auditoría informática Cobit 5, se encontró que esta es apropiada para evaluar la situación actual de la oficina de informática y tecnología de la municipalidad distrital de Pilcuyo, utilizando la metodología Cobit 5, principalmente basándonos en los principios de Cobit 5. Mediante la ejecución de pruebas a las diferentes áreas como son Base de Datos, Redes y Comunicaciones, Seguridad Física y Seguridad Lógica, las cuales nos ayudó a evidenciar las falencias existentes. Campos *et al.* (2019) en su estudio indica que la aplicación de Cobit en la auditoria informática optimiza la utilización de las TI, ya que permite armonizar los beneficios, el manejo de los recursos y los niveles de riesgo, mediante una gestión integral en la organización. Al respecto como ya se mencionó en el estudio con el Cobit 5 ayudo a identificar las distintas falencias y vulnerabilidades en las distintas áreas de estudio.

Al evaluar la gestión de los sistemas de información de la oficina de informática y tecnología de la Municipalidad distrital de Pilcuyo se verificó que se tiene inconvenientes con la dotación de personal en la oficina de informática y tecnología, puesto que no se cuenta con personal calificado y/o conocedores del área. Así mismo comparando los resultados con Rafael y Castillo (2017), que encontró que la situación problemática del Hospital Regional Docente Las Mercedes de Chiclayo, son el no mantener la dotación de personal suficiente en el área, así mismo no existe un proceso que permita mantener las habilidades y competencias del personal TI. Además de que no se tienen definidos esquemas de clasificación de incidentes y peticiones de servicio, los cuales permitan priorizarlos de manera que se les dé una eficaz y eficiente resolución. Tampoco se analiza, ni se informa sobre el rendimiento del área de CSI a la Gerencia de manera

constante. En tanto decimos que estas falencias en cuanto al persona y documentación no solo se puede encontrar en una municipalidad pequeña como la que estudiamos, si no en Hospitales grandes donde sus procesos ya deben de estar definidos y su personal debe ser mejor capacitado, por lo que podemos verificar que el tema de la auditoria informática en el Perú aun no es muy utilizado.

En el tema se seguridad de información se encontró falencias puesto que el Sistema de Administración tributaría no se tiene el levantamiento de análisis de requisitos para su implementación, en cuanto a la seguridad de información a partir de las pruebas de auditoria informática se encontró falencias en la Base de Datos, Redes y Comunicación, Seguridad Lógica, Seguridad Física, puesto que se verifico que no existen controles que permitan garantizar la seguridad de la información del sistema de Administración tributaria, tampoco existe documentación como los manuales y diccionario de la base de datos del sistema. También Sánchez (2018), en su investigación encontró que el sistema informático tiene algunos problemas y nos muestra vulnerabilidades de aspecto riesgosos en el sistema operativo y perdida de información; el personal fue evaluado y se indicó que estaban capacitados en ciertos aspectos técnicos del sistema, pero requieren más conocimientos acerca de seguridad sistema informático; después de haber hecho la evolución llevaremos a cabo el desarrollo de un manual de Divulgación de información confidencial que puede causar problemas a las empresas, así como daños de reputación o poner en peligro relaciones ya que no se lleva un control y monitoreo del sistema; el manual de funciones que sirva como guía auditoria del control de seguridad a través de la norma COBIT 5.

V. CONCLUSIONES

PRIMERA: Se realizó la auditoria informática usando la metodologias Cobit 5, mediante ello se encontró que esta es apropiada para evaluar la gestión del sistema de información y que permitieron tener un diagnóstico sobre la situación actual de la oficina de informática y tecnología de la Municipalidad distrital de Pilcuyo. En tanto se verificó que se tiene inconvenientes con la dotación de personal en la oficina de informática y tecnología, puesto que no se cuenta con personal calificado y/o conocedores del área, también se observó que no existe un proceso que permita la selección del personal adecuado que debe laborar en el área. Así mismo se verifico que la distribución de funciones y actividades del personal no es la adecuada para que estos cumplan dichas funciones de manera correcta.

SEGUNDA: Cobit 5 es un marco metodológico muy versátil para la evaluación de sistemas de información, se verificó que el sistema de administración tributaría no se tiene el levantamiento de análisis de requisitos para su implementación, en cuanto a la seguridad de información a partir de las pruebas de auditoria informática se encontró falencias en la:

- *Base de Datos*, puesto que no existen estándares para la asignación de usuarios y contraseñas, no existe la documentación de la base de datos, así mismo carecen de listado de procesos para recuperación de información y falta de procesos de creación de backups.
- *Redes y Comunicación*, puesto que no existen planos del cableado estructurado instalado en la institución, hay carencia en el listado de personas encargadas del manejo del checkpoint. no existe algún proceso de manejo de información y no manipulan configuración del firewall.

- *Seguridad Lógica,* puesto que no tienen un listado de software adquiridos en la institución, no existe licencias del software y antivirus, no existe documentación o un listado de la cantidad de licencias adquiridas con respecto a la cantidad de equipos o usuarios que hacen uso de este software.

- *Seguridad Física,* puesto que no existe un inventario de las cámaras de vigilancia implementados en la institución. Falta de manuales, inventarios y planos de la ubicación de los UPS de la institución.

Además, se verifico que no existen controles que permitan garantizar la seguridad de la información del sistema de administración tributaria, tampoco existe documentación como manuales y diccionario de la base de datos del sistema.

TERCERA: La auditoría realizada en la municipalidad distrital de Pilcuyo, estuvo orientado a la auditoría de la oficina de informática y tecnología y al sistema de administración tributaria, para los cuales se presentó un informe (tabla10, tabla11, tabla12 y tabla13), que involucra recomendaciones y planes de mejora para diseñar un Sistema de Gestión de la Seguridad de la Información adecuado que brinde los beneficios más útiles para la municipalidad distrital de Pilcuyo.

VI. RECOMENDACIONES

- Se sugiere implementar un sistema de Gobierno y Gestión Tecnológico en Base a las guías de COBIT 5, que permitirá mejorar la gestión de la oficina de informática y tecnología así mismo la gestión de seguridad del sistema de Administración Tributaría inherentes al ámbito de TI, que les permita centrar y orientar esfuerzos en los procesos adecuados de seguridad de información con eficiencia y eficacia.
- Se recomienda aplicar controles para la selección del Recurso humano, específicamente al personal designado a la oficina de informática y tecnología, el cual debe ser suficientemente capacitado y adecuado para poder cumplir con todas las funciones y actividades que se les asigne en la oficina de tecnología e informática.
- Se recomienda delimitar un área y/o oficina de seguridad y resguardo informático, con la finalidad de tener personal capacitado y prevenir debilidades con respecto a fuga o pérdida de información a causa del acceso no autorizado de personas extrañas a la institución.
- Se recomienda que la oficina de tecnología y informática, tenga más contacto con los usuarios finales(Clientes). Puesto que dicha oficina actualmente no lo realiza.
- Se recomienda mitigar las amenazas, para evitar que se vulnere la seguridad de la información, y se conviertan en riesgos existentes en la oficina de informática y tecnología, promoviendo estudios y capacitaciones de concientización acerca de los activos de la municipalidad, en base a los principios básicos de seguridad, integridad confidencialidad y disponibilidad de la información, y a la vez a través COBIT 5 que posee un conjunto de procesos que permiten garantizar seguridad tomar diferentes criterios para una correcta administración de la información, mitigando futuras amenazas.

VII. REFERENCIAS BIBLIOGRÁFICAS

Auquilla, L. (2014). *Auditoria informática de seguros del Pichincha S.A. compañía de seguros y reaseguros, aplicando COBIT 5* (tesis de grado). Universidad Tecnológica Israel, Ecuador. Recuperado de: http://repositorio.uisrael.edu.ec/handle/47000/929

Beingolea, J. (2015). *Diseño de un modelo de gobierno de ti utilizando el marco de trabajo de COBIT 5 con enfoque en seguridad de la información caso de estudio: una empresa privada administradora de fondo de pensiones* (tesis de grado). Pontificia Universidad Católica Del Perú, Perú. Recuperado de: http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/6390

Brito Ochoa, M. P., Alcívar Cedeño, F. M., & Guerrero Carrasco, M. J. (2016). Auditoría en las empresas. *Contribuciones a la Economía*, 14.

Caridad, S. (2006). *Auditoría Informática*, España. Recuperado de: http://www.scaridad.com/files/Apuntes%20de%20AI.pdf

Chillida, J. (2013). *Tecnología de la Información.*

Coltell, S. (2012). Auditoría de los Sistemas de Información. *Servicio de Publicaciones de la Universidad Politécnica de Valencia*, España.

Gardey, A., y Pérez Porto, J. (2012). *Definición de metodología.* Recuperado de: https://definicion.de/metodologia/

Guapulema, M. (2017). *Implementar el sistema COBIT5 en los procesos de auditoria informática en la corporación Jarrin Herrera Cía. LTDA. Agencia Babahoyo* (tesis de grado). Universidad Regional Autónoma De Los Andes, Ecuador. Recuperado de:

http://dspace.uniandes.edu.ec/bitstream/123456789/8396/1/TUBSIS005-2017.pdf

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6a ed.). México: McGraw

Hernández, R., y McGraw, H. (Junio de 2017). *EcuRed – Auditoria*. Recuperado de: https://www.ecured.cu/Auditor%C3%ADa

ISACA (2011). *COBIT 5 – Cambios de la nueva versión, 2011*. Recuperado de: http://www.isaca.org/Groups/Professional-English/cobit-5-use-it-effectively/Pages/ViewDiscussion.aspx?PostID=18

ISACA (2015). *COBIT 5 – 2015*. Recuperado de: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

Jiménez, A. (2016). *Auditoria Informática del sistema de información de la empresa cocinas internacionales utilizando COBIT V.5* (tesis de grado). Universidad de las Fuerzas Armadas, Ecuador. Recuperado de: https://repositorio.espe.edu.ec/bitstream/21000/12111/2/T-ESPE-053368-D.pdf

Jimenez, R. (2019). *Marco de Gobierno de COBIT*. Recuperado de: http://mgcrj.blogspot.com/p/3.html

Kuna, H. D. (2014). *Asistente para la Realización de Auditoras de Sistemas en Organismos Públicos o Privados*. Recuperado de http://www.researchgate.net/profile/Horacio_Kuna/publication/26519345_Asistente_para_la_Realizacin_de_Auditoras_de_Sistemas_en_Organismos_Pblicos_o_Privados/links/54203f6a0cf241a65a1beafb.pdf

López, R. (2009). *Generalidades de la Auditoría.*

Martínez, C. (2017). *Arquitectura Empresarial*. Recuperado de: https://chae201421700812550.wordpress.com/2014/09/17/historia-y-evolucion-de-cobit/

Piattini, M. G. y Del Peso, E. (2003). *Auditoria Informática: Un Enfoque Práctico.*. España: RAMA

Puma, M. (2017). *Implantación de un proceso de auditoría de seguridad de información bajo la norma ISO/IEC 27002 en una entidad financiera de Puno – 2016* (tesis de grado). Universidad Nacional Del Altiplano, Perú. Recuperado de: http://repositorio.unap.edu.pe/bitstream/handle/UNAP/6629/Puma_Arosquipa_Max_Yonel.pdf?sequence=1&isAllowed=y

Quintuña, V. (2012). *Auditoría Informática a la Superintendencia de Telecomunicaciones*. Universidad de Cuenca. Ecuador.

Rafael, G. y Castillo, E. (2017). *Auditoría informática usando las normas COBIT en el centro de sistemas de información del Hospital Regional Docente las Mercedes De Chiclayo – 2016* (tesis de grado). Universidad Nacional "Pedro Ruiz Gallo", Peru. Recuperado de: http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/1221/BC-TES-5923.pdf?sequence=1&isAllowed=y

Ron, M. (2010). *Auditoría*.

Sanchez, J. (2018). *Evaluación de softwares de control de seguridad de bases de datos relacionales aplicando la norma COBIT 5* (tesis de grado). Universidad de Guayaquil, Ecuador. Recuperado de: http://repositorio.ug.edu.ec/bitstream/redug/36910/1/TESIS%20FINAL%2010-09-2018N.pdf

Soto, D. (2016). *¿Qué es COBIT y para qué sirve?*. Recuperado de:

https://nextech.pe/que-es-cobit-y-para-que-sirve/

Tejada, E. (2015). *Auditoría de Seguridad Informática. IFCT0109.* Málaga: IC Editorial.

Vega (2017). Sistema de Cobit en os procesos de auditoria de los sistemas informáticos:

https://doi.org/10.26910/issn.2528-8083vol2iss8.2017pp65-68

ANEXOS

Anexo 1. Encuesta

ENCUESTA

LA ENCUESTA ES APLICADA CON EL OBJETIVO DE EVALUAR, SI EXISTE POLITICAS DE SEGURIDAD INFORMATICA, EN LA OFICINA DE INFORMATICA Y TECNOLOGIA DE LA MUNICIPALIDAD DISTRITAL DE PILCUYO

DATOS GENERALES

FECHA DE AUDITORIA: DIA…… MES……..AÑO……

NOMBRE:

_____

CARGO: _____ FIRMA: _____

PREGUNTAS	SI	NO
1. ¿Existen políticas de seguridad de la información?		
2. ¿Conoce Ud. La norma ISO/IEC 27001:2014 NTP?		
3. ¿Existen lineamientos de seguridad de la información?		
4. ¿Existe un área de seguridad de la información?		
5. ¿Alguna vez sea divulgado información personal o privada?		
6. ¿Existe un procedimiento o manual que ayude al manejo de información privada o restringida?		
7. Cuando está ausente en su puesto de trabajo, ¿Es de fácil acceso a personal no autorizado a su ordenador a cargo?		
8. ¿Es monitoreado constantemente la información que manipula o modifica el usuario final (alumnos y estudiantes)?		
9. ¿Realiza respaldos de la información al terminar sus labores diarias?		
10. ¿Ha llevado archivos digitales para terminar en su casa por falta de tiempo?		
11. ¿Constantemente actualiza los mecanismos de seguridad de la información?		
12. ¿Los ordenadores a su cargo, tienen contraseñas?		
13. ¿Realiza periódicamente cambio de contraseñas a los ordenadores, servidores, etc.?		
14. ¿Utiliza mecanismo de cifrado para su memoria USB?		
15. ¿Existe algún registro de fallas o ataques a través de la red?		
16. ¿La infraestructura de gobierno electrónico está acorde a las normas o estándares establecidos por La secretaria de gobierno digital?		
17. ¿La información que se transmite a través del área, tiene los 3 principios básicos de la seguridad de la información? – Confidencial – Integro – Disponible.		
18. ¿Ha tenido alguna capacitación para mejorar la seguridad informática?		
19. ¿Se hace teletrabajo?		
20. ¿El usuario final conoce las normas o reglas existentes? - No alterando los tres principios de la seguridad. - No Alterando la fiabilidad y veracidad de la información consultada, modificada por cualquier medio informático.		

Anexo 2. Guía de entrevista

ENTREVISTA PARA EL DIRECTOR DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA MUNICIPALIDAD DE PILCUYO

La entrevista se realizó con la finalidad de recolectar información de la situación actual del Sistema de administración tributaria y del departamento de Tecnologías de la Información en la municipalidad de Pilcuyo.

FECHA:

_____

ENTREVISTADO:

_____

PREGUNTAS:

1. ¿Conoce Ud. si el departamento de TI cuanta con un plan estratégico para la mejora del sistema?

   _____
   _____
   _____

2. ¿Existen algún plan para la seguridad de la información de la institución?

   _____
   _____
   _____

3. ¿Conoce con cuántos sistemas cuenta la institución y cual son sus funciones?

   _____
   _____
   _____

4. ¿Conoce Ud. si se ha realizado una Auditoria Informática en el departamento de TI?

   _____
   _____
   _____

5. ¿Cree necesaria la elaboración de una auditoria informática en el departamento de TI?

   _____
   _____
   _____

6. ¿Ha considerado la importancia que tiene la información que se maneja en la institución?

_____

_____

_____

7. ¿La oficina de TI ha sufrido algún ataque mediante la red?

_____

_____

_____

8. ¿El área de tecnologías de la información cuenta con documentación donde establezca sus funciones?

_____

_____

_____

9. ¿Considera que el personal del área está capacitado para realizar las tareas que desempeñan?

_____

_____

_____

10. ¿Se requiere de servicios de terceros para cumplir con las funciones del área?

_____

_____

_____

11. ¿Conoce Ud. si han existido problemas con los usuarios del sistema?

_____

_____

_____

12. ¿La empresa posee manuales actualizados de procedimientos y procesos que se deben realizar?

_____

_____

_____