UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

CARRERA DE CONTABILIDAD Y AUDITORÍA

Proyecto Integrador, previo a la obtención del Título de Licenciado en Contabilidad y Auditoría C.P.A.

Tema:

"Auditoría al sistema de información del centro de procesamiento de datos en el Gobierno Autónomo Descentralizado Municipalidad de Ambato"

Autor: García Altamirano, Daniel Alexis

Tutora: Dra. Jiménez Estrella, Patricia Paola

Ambato-Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Dra. Patricia Paola Jiménez Estrella con cédula de identidad No. 180293423-0, en mi calidad de Tutora del proyecto integrador sobre el tema: **"AUDITORÍA AL SISTEMA DE INFORMACIÓN DEL CENTRO DE PROCESAMIENTO DE DATOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO"**, desarrollado por Daniel Alexis García Altamirano, de la Carrera de Contabilidad y Auditoría, modalidad presencial, considero que dicho informe investigativo reúne los requisitos, tanto técnicos como científicos y corresponde a las normas establecidas en el Reglamento de Graduación de Pregrado, de la Universidad Técnica de Ambato y en el normativo para presentación de Trabajos de Graduación de la Facultad de Contabilidad y Auditoría.

Por lo tanto, autorizo la presentación del mismo ante el organismo pertinente, para que sea sometido a evaluación por los profesores calificadores designados por el H. Consejo Directivo de la Facultad.

Ambato, Agosto 2022

TUTORA

.....

Dra. Patricia Paola Jiménez Estrella

C.I. 180293423-0

DECLARACIÓN DE AUTORÍA

Yo, Daniel Alexis García Altamirano con cédula de identidad No. 180439220-5, tengo a bien indicar que los criterios emitidos en el proyecto integrador, bajo el tema: **"AUDITORÍA AL SISTEMA DE INFORMACIÓN DEL CENTRO DE PROCESAMIENTO DE DATOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO"**, así como también los contenidos presentados, ideas, análisis, síntesis de datos, conclusiones, son de exclusiva responsabilidad de mi persona, como autor de este Proyecto Integrador.

Ambato, Agosto 2022

AUTOR

.....

Daniel Alexis García Altamirano

C.I. 180439220-5

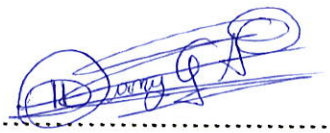
CESIÓN DE DERECHOS

Autorizo a la Universidad Técnica de Ambato, para que haga de este proyecto integrador, un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los derechos en línea patrimoniales de mi proyecto integrador, con fines de difusión pública; además apruebo la reproducción de este proyecto integrador, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial; y se realice respetando mis derechos de autor.

Ambato, Agosto 2022

AUTOR



.....

Daniel Alexis García Altamirano

C.I. 180439220-5

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el proyecto integrador, sobre el tema: **"AUDITORÍA AL SISTEMA DE INFORMACIÓN DEL CENTRO DE PROCESAMIENTO DE DATOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO"**, elaborado por Daniel Alexis García Altamirano, estudiante de la Carrera de Contabilidad y Auditoría, el mismo que guarda conformidad con las disposiciones reglamentarias emitidas por la Facultad de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

Ambato, Agosto 2022

Dra. Mg. Tatiana Valle
PRESIDENTE

Dra. Cecilia Toscano
MIEMBRO CALIFICADOR

Dra. Rocío Cando
MIEMBRO CALIFICADOR

DEDICATORIA

El presente proyecto integrador se la dedico a Dios porque él es dueño de mi vida y de mi corazón, quien ha estado presente incondicionalmente sobre todas las cosas.

A mis padres por el apoyo moral y monetario en el transcurso de mi carrera, además de sus palabras de aliento e incentivarme la constancia y dedicación.

A toda mi familia quienes creyeron convincentemente en mí para forjar buenas nuevas y romper cadenas limitaciones que se han ido arrastrando durante mucho tiempo.

Daniel Alexis García Altamirano

AGRADECIMIENTO

Agradecido primeramente con Dios quien ha sido el que me ha permitido llegar hasta aquí, siendo el que me otorga la sabiduría y la inteligencia para avanzar en mi educación y formación culta.

Agradezco a mi madre por todo el sacrificio, motivación y el dinero invertido en mí para poder cumplir mis sueños pese a todos los obstáculos que se ha presentado hemos salido ilesos juntos.

A mi tutora, la doctora Patricia Paola Jiménez Estrella por ser mi consejera y guía en la etapa final, además de todo esto una amiga sincera en quien se puede confiar.

Daniel Alexis García Altamirano

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORÍA
CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA: "AUDITORÍA AL SISTEMA DE INFORMACIÓN DEL CENTRO DE PROCESAMIENTO DE DATOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO"

AUTOR: Daniel Alexis García Altamirano
TUTORA: Dra. Patricia Paola Jiménez Estrella
FECHA: Agosto 2022

RESUMEN EJECUTIVO

El presente proyecto integrador tiene como objetivo realizar una auditoría al sistema de información del centro de procesamiento de datos en el GADMA. En el tratamiento de la información, su seguridad, sus posibles riesgos y como evitarlos utilizando los marcos de referencias COSO ERM 2017 Y COBIT. Los Marcos de Referencias son claves para mejorar la infraestructura tecnológica dentro del Departamento de Tecnologías de Información del municipio. Se obtuvieron resultados donde el GADMA tiene múltiples procesos informales, no estandarizados pero sirven para el manejo de sus actividades de prácticas de gobierno teniendo un modelo moderado en el manejo del sistema de información del centro de procesamiento de datos y buen cumplimiento del control interno institucional, pese a lo mencionado anteriormente la institución tiene algunas falencias en identificar y evaluar las eventualidades que traigan consigo posibles riesgos y amenazas concluyendo en que no existe una cultura en riesgos y además de que hay imprecisión en gestionar la seguridad.

PALABRAS DESCRIPTORAS: AUDITORÍA, MARCO DE REFERENCIA COSO ERM 2017, MARCO DE REFERENCIA COBIT, TECNOLOGÍA DE INFORMACIÓN.

TECHNICAL UNIVERSITY OF AMBATO

FACULTY OF ACCOUNTING AND AUDITING

ACCOUNTING AND AUDITING CAREER

TOPIC: "AUDIT TO THE INFORMATION SYSTEM OF THE DATA PROCESSING CENTER IN THE DECENTRALIZED AUTONOMOUS GOVERNMENT OF THE MUNICIPALITY OF AMBATO**"**

AUTHOR: Daniel Alexis García Altamirano

TUTOR: Dra. Patricia Paola Jiménez Estrella

DATE: August 2022

ABSTRACT

The objective of this integrative project is to carry out an audit of the information system of the data processing center in GADMA. In the treatment of information, its security, its possible risks and how to avoid them using the COSO ERM 2017 and COBIT reference frameworks. The Reference Frameworks are key to improving the technological infrastructure within the municipality's Information Technology Department. Results were obtained where the GADMA has multiple informal processes, not standardized but they serve to manage their activities of government practices, having a moderate model in the management of the information system of the data processing center and good compliance with internal institutional control. Despite the aforementioned, the institution has some shortcomings in identifying and evaluating the eventualities that bring with them possible risks and threats, concluding that there is no risk culture and that there is also inaccuracy in managing security.

KEYWORDS: AUDIT, FRAME OF REFERENCE COSO ERM 2017, FRAME OF REFERENCE COBIT, INFORMATION TECHNOLOGY.

ÍNDICE GENERAL

CONTENIDO **PÁGINA**

ÍNDICE DE TABLAS

CONTENIDO **PÁGINA**

ÍNDICE DE GRÁFICOS

CONTENIDO PÁGINA

CAPÍTULO I

MARCO TEÓRICO

1.1 Introducción

1.1.1 Antecedentes del proyecto Integrador

1.1.1.1 Historia de la empresa

A continuación, se presenta la historia del Gobierno Autónomo Descentralizado Municipalidad de Ambato, (2022):

Ambato declara su independencia el 12 de noviembre de 1820. Ambato pertenecía a la provincia de Chimborazo, pero por medio del decreto realizado el 6 de noviembre de 1831 agregó que Ambato pertenecía a la provincia de Pichincha.

Ambato adquiere su categoría de provincia el 21 de mayo de 1861 mediante el decreto de la Convención Nacional.

El municipio de Ambato se creó con el afán de lidiar con problemas de sus habitantes en base a mejoras, progreso, reconstrucciones. Se necesitaba de personas con fuerte civismo y moralidad política para los cargos necesitados.

Don Tomás Sevilla fue el primer Comisario Municipal de Ambato denominado como el primer alcalde en la inauguración de la calle Bolívar. La Décima Quinta Asamblea Nacional Constituyente nombró como primer alcalde al Sr. Alfredo Coloma por un periodo de 2 años, a partir de ese año por elecciones populares se contaba con alcaldes en el cantón.

El Gobierno Autónomo Descentralizado Municipalidad de Ambato o GAD Municipalidad de Ambato aparece en el año 2011 dejando a un lado el antiguo nombre de Gobierno Cantonal de Ambato.

1.1.1.2 Detalles estratégicos

Misión de la Municipalidad de Ambato

A continuación, se presenta la misión del Gobierno Autónomo Descentralizado Municipalidad de Ambato, (2022):

El GAD Municipalidad de Ambato es una institución que promueve el desarrollo sostenible del cantón, a través de la prestación de servicios accesibles, óptimos y oportunos, la implementación de políticas públicas incluyentes, la mejora continua e innovación de sus procesos y servicios, el uso de tecnologías, y el fomento de la participación ciudadana, para mejorar la calidad de vida de sus ciudadanos.

Visión de Futuro

A continuación, se presenta la visión del Gobierno Autónomo Descentralizado Municipalidad de Ambato, (2022):

Al 2023 El GAD Municipalidad de Ambato será la institución formuladora y ejecutora de acciones que permitan hacer de Ambato un cantón seguro, digital, resiliente, inclusivo, sostenible, y saludable, con servicios de calidad; generadora de políticas que posicionen al cantón a nivel nacional como polo de desarrollo comercial y productivo, fundamentada en el capital intelectual y en el uso eficiente y transparente de sus recursos.

Objetivos institucionales

A continuación, se presenta los objetivos institucionales del Gobierno Autónomo Descentralizado Municipalidad de Ambato, (2022):

1. Promover el desarrollo social e intercultural fortaleciendo la salud, bienestar, igualdad de género, deporte y recreación; la conservación del patrimonio cultural, identidad, apropiación de tradiciones y costumbres de Ambato.

2. Promover el desarrollo urbano sostenible, mediante la transformación cultural, participación ciudadana, educación, capacitación, control mitigación, restauración de la transgresión ambiental, aplicando principios de movilidad sostenible,

jerarquización de residuos, cuidado del agua, cuidado animal, cuidado ambiental, para el beneficio del cantón.

3. Impulsar el desarrollo productivo del cantón, mediante la optimización de sus diferentes sistemas formales de comercialización, en pro de su beneficio económico.

4. Optimizar las fuentes de financiamiento del presupuesto institucional, a través de recaudaciones propias, recursos fiscales, líneas de crédito y cooperación, para financiar la gestión municipal.

5. Garantizar la dotación de servicios públicos e infraestructura, mediante procesos sostenibles, para el beneficio de los habitantes del cantón.

6. Impulsar la innovación y competitividad del cantón, a través de la digitalización de servicios municipales, para el fortalecimiento de la gestión integral de la calidad institucional y la óptima interacción con los actores de interés y ciudadanía en general.

7. Fortalecer la administración interna institucional, a través de un modelo de gestión apropiado, la mejora continua e innovación de sus procesos y el uso de las tecnologías de información y comunicación, con el fin de alcanzar la excelencia del servicio.

8. Impulsar el desarrollo integral de Ambato, mediante normas que generen incentivos tributarios, un adecuado régimen de uso del suelo y un crecimiento urbano que sea ordenado, seguro, turístico, cultural, patrimonial, gastronómico, natural, inclusivo y sostenible, a fin de promover la inversión privada.

9. Fomentar la actualización y el cumplimiento de las ordenanzas y resoluciones de las competencias municipales acordes con las leyes y normas nacionales vigentes.

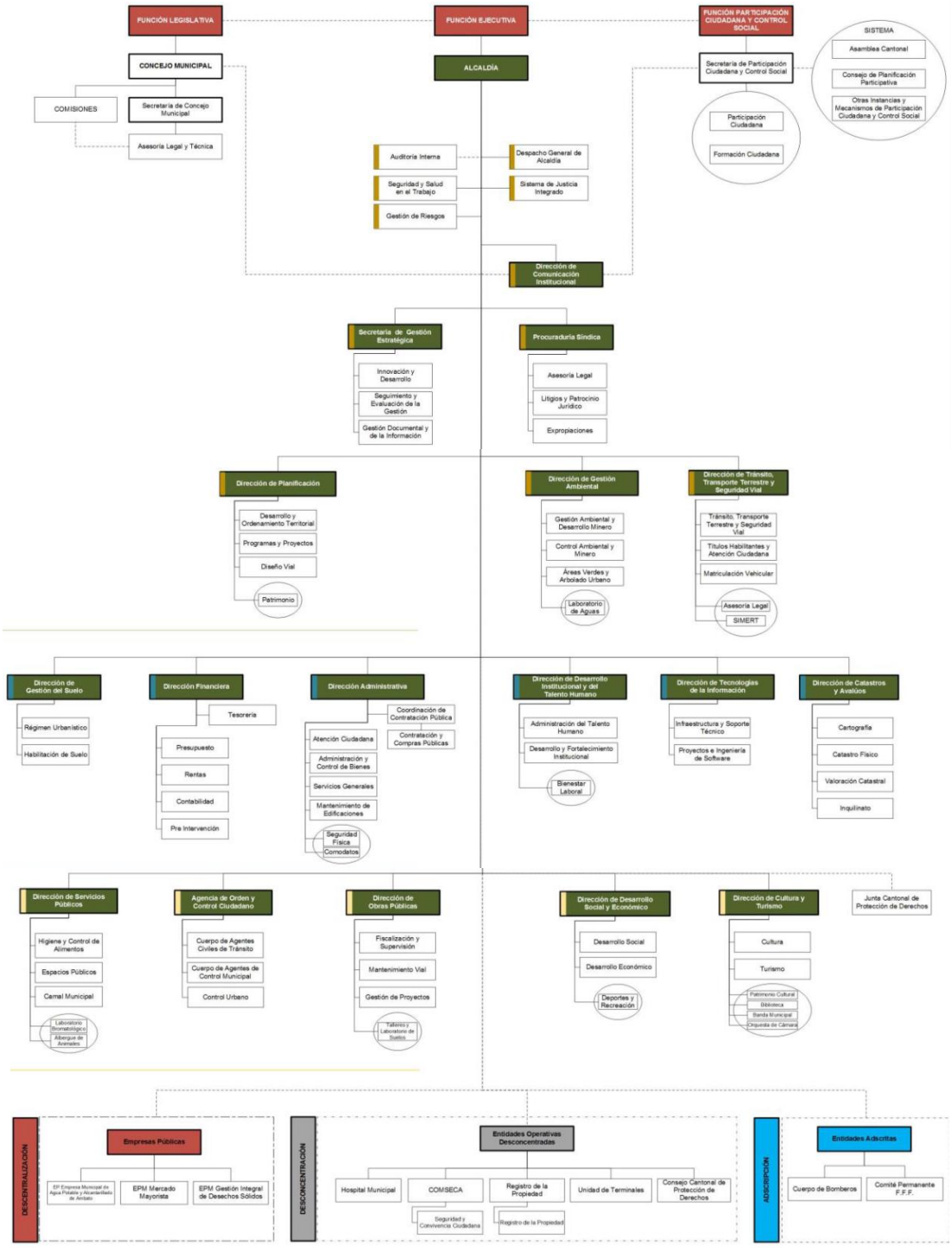
Valores institucionales

A continuación, se detalla los valores institucionales del Gobierno Autónomo Descentralizado Municipalidad de Ambato, (2022):

- Compromiso
- Honestidad
- Diálogo participativo
- Justicia
- Solidaridad
- Respeto
- Responsabilidad.

1.1.1.3 Estructura organizacional (organigrama estructural o funcional)

Gráfico 1. ***Organigrama del GAD Municipalidad de Ambato***



Fuente: GAD Municipalidad de Ambato (2022)

1.1.1.4 Detalles de operación

El GAD Municipalidad de Ambato, (2022) brinda los siguientes servicios:

Tabla 1. ***Servicios del GADMA***

Nª	Denominación del servicio	Descripción del servicio
1	Servicios en línea	• Rodaje • Renovación y cierre patente • Traspasos de dominio • Turnos trámites presenciales • Turnos matriculación • Pagos con tarjeta de crédito
2	Emprendo Ambato	• Sistema de reporte ciudadano
3	Registro de la Propiedad	• Consulta estado de trámite • Costo de trámites • Calcule el valor a pagar Valide su certificado
4	Trámites, Dependencias y Formularios	• Trámites/Requisitos • Dependencias municipales • Formularios municipales • Formatos títulos habilitantes
5	Quejas y Sugerencias	• Ingreso • Consultas
6	GEOPORTAL	• Edificios municipales • Puntos de recaudación • Edificios patrimoniales • Monumentos de la ciudad • Información catastral • Planificación y gestión territorial • Gestión ambiental • Tránsito transporte y movilidad
7	Intranet	• GADMAPPS • Sistema de permisos y vacaciones • Control horas extras • Consulta de horarios

Fuente: GAD Municipalidad de Ambato (2022)
Elaborado por: García (2022)

1.1.1.5 Detalles legales

El GAD Municipalidad de Ambato, (2022) cumple la siguiente normativa:

Tabla 2. ***Base Legal***

Art. 7 de la Ley Orgánica de Transparencia y Acceso a la Información Pública – LOTAIP Literal a2) Base legal que la rige	
Tipo de la Norma	Norma Jurídica
Carta Suprema	Constitución de la República del Ecuador
Norma internacional	Tratados y convenios internacionales
Códigos	Código Orgánico de Coordinación Territorial, Descentralización y Autonomía – COOTAD Código del Trabajo Código Orgánico Administrativo Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público
Leyes Orgánicas	Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP) Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (LOGJCC) Ley Orgánica de Servicio Público (LOSEP) Ley Orgánica de la Contraloría General del Estado Ley de Seguridad Pública y del Estado
Reglamentos de Leyes	Reglamento General a la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) Reglamento General a la Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP) Reglamento a la Ley Orgánica de Servicio Público (LOSEP)
Decretos Ejecutivos	Los Decretos Ejecutivos relacionados con la institución se re direccionarán al sitio web donde se encuentran alojados
Ordenanzas Municipales	Ordenanza de competencias territoriales

Fuente: GAD Municipalidad de Ambato (2022)

1.1.1.6 Marcas y logos

Gráfico 2. ***Marcas y Logos***

Fuente: GAD Municipalidad de Ambato (2022)

1.1.1.7 Ubicación

Avenida Atahualpa y Río Cutuchi.

1.1.2 Descripción del entorno

1.1.2.1- Auditorías informáticas y su impacto en las organizaciones

La Auditoría Informática es primordial para todo tipo de organización porque permite alcanzar múltiples estándares internacionales utilizando de manera correcta y efectiva las tecnologías de información (Arcentales & Caycedo, 2017). Por lo que, la auditoría informática puede aportar en gran medida a garantizar que una institución cubra la mayor de sus necesidades por medio de la informática abarcando el uso de sistemas de información y al uso de las tecnologías de información (Ramos, 2015). Así que, hoy en día la tecnología es indispensable porque agiliza todos los campos que comprenden las organizaciones facilitando las actividades cotidianas empresariales.

La Auditoría a los Sistemas de Información tiene como objetivo contribuir a mejorar y fortalecer los proyectos empresariales, institucionales y organizacionales con herramientas que sean eficientes, afianzadas a las buenas prácticas aplicando modelos tales sean COSO o COBIT transformándolos en una estrategia exitosa que impulsa a la adaptación en un entorno cambiante (Díaz, 2020). Además, los sistemas de Información en organizaciones modernas da lugar a la productividad, capacidad comercial, control y toma de decisiones (Negrín, 2017). En definitiva, la auditoría a los sistemas de información impulsa a las organizaciones a mejorar progresivamente sus actividades para alcanzar un fin en común que es el éxito convirtiéndoles en entes de alta competitividad en el mercado actual.

La auditoría informática sirve perfectamente para prevenir, descubrir y probar movimientos o acciones fraudulentas que nos generen consecuencias a tal grado de llegar al delito informático por lo que da lugar a la importancia de que los sistemas de información sean fiables y que sus datos precisen la realidad (Del Peso, 1994). De tal modo que, la información es considerada de suma importancia para las organizaciones porque en el campo de la informática permite tener una etapa de transición de mejora en iniciativas de control (Solano, 2004). Finalmente, debe existir una combinación legal y transparente entre la información que mantiene la empresa y la informática que procesa los datos para evitar fraudes de cualquier índole.

1.1.2.2- Auditorías al sistema de información del centro de procesamiento de datos en Gobiernos Autónomos Descentralizados

De acuerdo a lo que manifiesta Villalobos (2008) sobre que hay que diseñar varios registros de auditorías, no solo limitarnos a uno solo. Entonces, podemos compartir los resultados de Sabillón & Cano (2019) de que las auditorías de ciberseguridad pueden ser muy efectivas para evaluar controles y responder ante las amenazas cibernéticas. Por lo tanto, es factible ampliar las ramas de auditoría de sistemas para llegar a demostrar resultados más efectivos y que contribuyan al desarrollo de las organizaciones.

Según el aporte de Dávalos (2008), en la actualidad radica la importancia de administrar la seguridad de la información protegiendo los activos de información para evitar anomalías de carácter informático. Adicionalmente, Álvarez (2005) afirma que las organizaciones modernas a través del internet necesitan mejorar sus sistemas de infraestructuras informáticas en las medidas de protección para garantizar el desarrollo y la sostenibilidad de sus actividades. Así que, toda organización debe mantener la seguridad de su información para solventar las posibles vulnerabilidades que puedan existir.

La auditoría informática identifica la gestión de procesos informáticos y tecnológicos que no se están desarrollando eficazmente siendo necesario que se empleen medidas que favorezcan su crecimiento (Bailon, 2019). Acotando lo anterior, la auditoría debe actualizar los procesos aplicados en la evaluación y gestión de riesgos (Chuquimarca, 2020). Para finalizar, no se puede menospreciar la aparición de auditorías con fines informáticos y tecnológicos, por lo que es fundamental que la empresa esté aplicando la auditoría informática.

1.1.2.3- Contextualización del problema

El GAD Municipalidad de Ambato permitió observar cómo está organizada la empresa, su estructura organizacional, detalles estratégicos, operativos y base legal. Adicionalmente la auditoría aplicada en conocimiento al manejo de deberes y obligaciones. Entonces el GADMA tiene el control del libre ejercicio de sus actividades, utilización y distribución de recursos públicos.

La Contraloría General del Estado es la encargada de realizar las respectivas auditorías para verificar, examinar y evaluar las funciones de las instituciones públicas incluido el GAD Municipalidad de Ambato. Sin embargo, las Auditorías de Gestión son las únicas aplicadas dando lugar a la necesidad de realizar otros tipos de auditorías para ampliar conocimientos y tener más control sobre las diversas áreas existentes. Por lo tanto se señala que existe la ausencia de aplicación de una auditoría de sistemas informáticos.

La Auditoría de sistemas comprende la administración y control de los sistemas de información relacionados a los lineamientos y políticas establecidas en el GAD Municipalidad de Ambato. Para finalizar, la institución potenciará en la parte informática su gestión empresarial.

1.1.3 Justificación:

En el mundo actual predominan las tecnologías de información y las comunicaciones. Existe la necesidad de tener una seguridad sobre los recursos de información ya sean datos, tecnologías, aplicaciones, infraestructura y el activo humano así como el cumplimiento de objetivos, además de ser precisa y confiable (Negrín, 2017). Así mismo, en un mundo cambiante, el éxito de una institución se ha vinculado estrechamente con la importancia de las auditorías informáticas que radica en determinar las fortalezas, debilidades, riesgos y amenazas del sistema de información (Arcentales & Caycedo, 2017). Por lo que hoy en día la tecnología es la base primordial de todo tipo de profesión de modo que debemos profundizar más sobre esta herramienta para facilitar nuestras actividades para desempeñarnos mejor los sistemas de información.

El ejercicio profesional de la auditoría de sistemas de información, con el objetivo de minimizar riesgos inherentes y de control, mediante pruebas de control y programas de auditoría (Solano, 2004). Por otro lado, Del Peso Navarro (1994) expresa: "En los últimos años el uso de las nuevas tecnologías de la información en las empresas y en las distintas Administraciones ha experimentado un desarrollo espectacular". Así que, el empresario o gestor de estos días debe dominar la información que se actualiza prolongadamente para poder tomar decisiones más rápidas y con menor riesgo.

Las organizaciones tratan de proteger los activos cibernéticos e implementar medidas y programas de ciberseguridad, pero a pesar de este esfuerzo continuo, es inevitable que se presenten las violaciones de la ciberseguridad y se materialicen ataques cibernéticos (Sabillón & Cano, 2019). En definitiva, un auditor debe conocer sobre el procesamiento de datos electrónicos, sistemas de información, salvaguarda de activos informáticos, uso de TI.

1.1.4 Objetivos

1.1.4.1 Objetivo General:

Aplicar la auditoría al sistema de información del centro de procesamiento de datos en el GADMA para un mejor manejo y control informático.

1.1.4.2 Objetivos específicos:

- Utilizar herramientas, técnicas y procedimientos para la fase de planificación.
- Elaborar los papeles de trabajo relacionados a la auditoría de sistemas para la recolección de datos en su fase de ejecución.
- Dictaminar el informe final para una mayor comprensión de todas las evidencias y procesos efectuados como fase de comunicación de resultados.

1.2 Revisión de la literatura

1.2.1 Introducción a la informática

1.2.1.1 Definición

"La informática es el conjunto de conocimientos que actualmente tenemos respecto a un artilugio tecnológico al que llamamos ordenador" (Marco, 2012). En este sentido, Los aparatos tecnológicos tienen una conexión muy fuerte con la informática, siendo un complemento vital dentro de las organizaciones.

1.2.1.2 El auditor informático

"El auditor informático necesita de una larga experiencia tutelada y una gran información tanto auditora como informática" (Plattini, del Peso, & del Peso, 2015). Inclusive, El auditor debe tener presente la ética y el ejercicio profesional en su profesión para evitar fraudes y problemas legales.

1.2.1.3 La tecnología informática

"La tecnología informática engloba a todos aquellos conocimientos que permiten el diseño y la construcción de sistemas informáticos" (Marco, 2012).

Gráfico 3. ***Hardware y software***

Elaborado por: García (2022)
Fuente: Marco (2012)

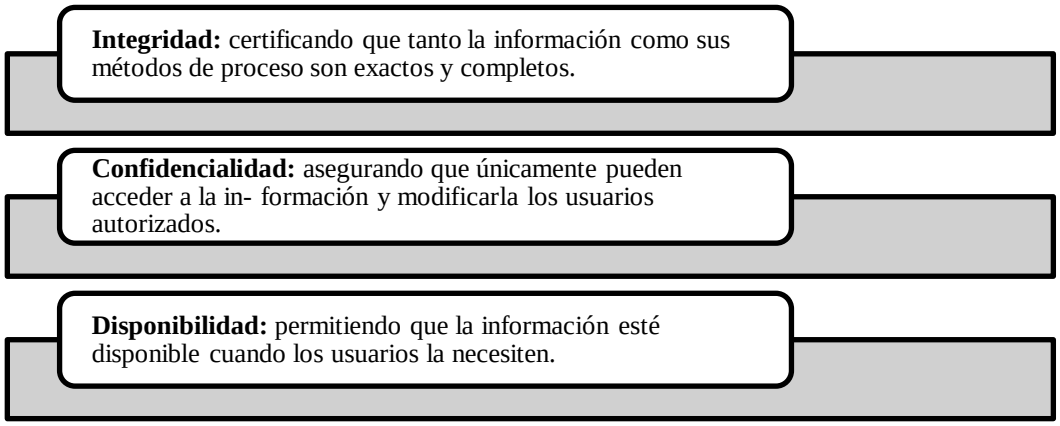
1.2.2 Sistemas de información

"Los sistemas de información son sistemas implicados en la recogida, tratamiento, distribución y uso de la información. Los sistemas de información prestan apoyo a los sistemas de actividad humana" (Davies, 2014). En definitiva, los sistemas de información permiten el uso y procesamiento de datos dando lugar a la información disponible y accesible para los miembros de la organización.

1.2.3 Seguridad de la información

"La seguridad de la información es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información" (Escrivá, Romero, Ramada, & Onrubia, 2013).

Gráfico 4. ***Valores***



Elaborado por: García (2022)
Fuente: Escrivá et al., (2013)

1.2.3.1 Seguridad informática

"La seguridad informática, por su parte, es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida" (Escrivá et al., 2013). Es decir, La seguridad de la información debe ser gestionada, supervisada y controlada para mitigar los riesgos, vulnerabilidades y amenazas.

1.2.4 Teoría de sistemas y la auditoría de sistemas de información

"La tecnología ha acabado pensando no ya en términos de máquinas sueltas sino de «sistemas»." (Bertalanffy, 1976). Puesto que. La pirámide de toda organización en la actualidad es la tecnología monitoreados por ordenadores.

"La auditoría de sistemas tiene como principal objetivo validar la integridad de la información y datos almacenados en las bases de datos de los sistemas de información y su procesamiento" (Blanco, 2008). Así que, la auditoría de sistemas se encarga de evaluar todos los procedimientos que la empresa utiliza para proteger la información, su integridad y confidencialidad de la misma.

1.2.5 Tipos y clases de auditorías de sistemas

1.2.5.1 Auditoría a sistema informatizado de explotación

El objetivo de una auditoría a un sistema informático que esté en explotación es el mismo que a un sistema informativo manual o mecanizado (Blanco, 2008). En síntesis, su trabajo, tendrá un enfoque más anticipativo, más proactivo, para resolver problemas potenciales antes que se manifiesten y produzcan efectos negativos.

1.2.5.2 Auditoría de la información

"La auditoría de la información es una herramienta de gestión de la información y de gestión estratégica, a la vez que una fase o un proceso dentro de la cadena de valor de la información" (Soy i Aumatell, 2013). Por lo que, La auditoría de la información verifica y regula los datos obtenidos para procesarlos en la gestión empresarial utilizadas con el fin de ser mucho más eficientes y eficaces.

1.2.5.3 Auditoría a la función informática

"La Auditoría a la función informática es la atención al sistema de dirección y control de la entidad, algo de lo cual no se puede prescindir en los momentos actuales, donde la adecuada administración, sobre bases informativas sólidas, representa la diferencia entre el éxito y el fracaso de una organización" (Blanco, 2008). Cabe resaltar, que la informática es la razón principal por la cual el auditor en su ámbito de trabajo debe dominarla a la perfección.

1.2.5.4 Auditoría a las áreas de procesamiento de datos

"La auditoría a la base de datos examina controles de accesos, de actualización, de integridad y calidad de los datos" (Blanco, 2008). En definitiva, El auditor debe controlar la aplicación adecuada de las políticas en el manejo de datos.

CAPÍTULO II

METODOLOGÍA

2.1 Descripción de la metodología

2.1.1 Unidad de análisis

La auditoría de sistemas consiste en verificar controles en el procesamiento de la información e instalación de sistemas, así como verificar, juzgar objetivamente la información, examinar y evaluar los procesos en cuanto a la informatización y tratamiento de los datos, su eficiencia y eficacia. Debe contar con controles robustos tales como copias de seguridad, planes de recuperación de desastres, gestión de incidentes, entre otros.

La auditoría contribuyó en la identificación de problemas relacionados a la gestión de cambios en el GAD Municipalidad de Ambato en el Departamento de Tecnologías de Información. Por consiguiente, se tomó a consideración Las Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos, en particular la 410-10 Seguridad de tecnología de información.

Se utilizó el Marco de Referencia COSO ERM 2017 (The Committee of Sponsoring Organizations of the Treadway Commission in Enterprise Risk Management) y el Marco de Referencia COBIT (Control Objectives for Information and Related Technologies) para dar respuesta en la aplicación de un adecuado manejo y control de la exposición del riesgo.

Todo esto Incluía la identificación de las estrategias y actividades para responder a cada uno de los posibles riesgos. Cuando se seleccionó una respuesta para un riesgo específico, se tuvo que valorar dicho riesgo nuevamente y decidir si está listo para ser aceptado o si tenía que requerir la aplicación de una nueva respuesta o un cambio en la estrategia.

En el Marco de Referencia COSO ERM 2017 se realizaron análisis de controles a todas las políticas, procedimientos, prácticas, estructura, organizacional implementados con la finalidad de conocer su nivel de confianza y su nivel de riesgo.

Tabla 3. ***Ponderación Nivel de Confianza y Nivel de Riesgo***

NIVEL DE CONFIANZA		
BAJO	**MODERADO**	**ALTO**
5% - 50%	51% - 75%	76% - 95%
95% - 50%	49% - 25%	24% - 5%
ALTO	**MODERADO**	**BAJO**
NIVEL DE RIESGO		

Fuente: Adaptado de COSO ERM 2017 (2017)
Elaborado por: García (2022)

El Marco de Referencia COBIT sirvió como guía para mejorar las prácticas de gobierno dirigida al control y supervisión de la tecnología de la información para la gestión del riesgo de la infraestructura de TI.

Tabla 4. ***Niveles de capacidad***

Niveles de capacidad COBIT	**Nivel observado**
Nivel 0 inexistente	No existen procesos de ninguna índole, por lo tanto la institución no es capaz de reconocer un problema y por consecuente no resolverlo.
Nivel 1 inicial o ejecutado	La institución es capaz de reconocer los problemas existentes y resolverlos por medio de métodos aplicados pero no existen procedimientos estandarizados.
Nivel 2 Repetibles-Administrado	Los procesos siguen igual a lo anterior con la inexistencia de procedimientos estandarizados, así que la responsabilidad se deja a la o las personas quienes dominan las situaciones y se tiene alto grado de confianza en los conocimientos.
Nivel 3 Establecido o definido	Los procesos son documentados y comunicados a través de capacitaciones, sin embargo se ha dejado en manos de las personas el seguimiento de este proceso.
Nivel 4 Predecible o administrado	Los procesos están bajo constante mejoramiento y proveen buena práctica por medio de la tecnología, se usa la automatización y las herramientas informáticas.
Nivel 5 Optimizado	Los procesos han sido estandarizados hasta un nivel de mejoramiento continuo y diseño de la madurez.

Fuente: Adaptado de COBIT (2012)
Elaborado por: García (2022)

Para la evaluación de los procesos según las Normas ISO 15504 se tomaron los siguientes rangos:

Tabla 5. ***Niveles de capacidad de procesos***

Nivel de capacidad de procesos NORMA ISO 15504			
Sigla	**Descripción**	**Valoración**	**%**
F	Proceso está completamente alcanzado	>85<=100	%
L	Proceso está alcanzado en gran manera	>50<=85	%
P	Proceso parcialmente alcanzado	>15<=50	%
N	Proceso no se cumple (no alcanzado)	0<=15	%

Fuente: Adaptado de COBIT (2012)
Elaborado por: García (2022)

2.1.2 Fuentes y técnicas de recolección de información

Fuentes de información primaria.- La información se extrajo del GAD Municipalidad de Ambato específicamente en el Departamento de Tecnologías de Información por una persona quien fue pieza clave en el esclarecimiento del tema planteado.

Encuesta.- Se aplicaron al final del mes de junio, utilizando la encuesta de forma presencial aplicando cuestionarios de los marcos de referencias para conocer el control interno informático.

Cuestionario.- En la presente investigación para el Marco de Referencia COSO ERM 2017 se utilizaron preguntas de Sí y No y para el Marco de Referencia COBIT se utilizó la tabulación del 0 al 5 según sus niveles de capacidad.

Tabla 6. ***Personas encuestadas o entrevistadas***

Nombres	**Cargo**	**Departamento**
Ricardo Fiallos	Ingeniero del Departamento	Tecnologías de la Información

Elaborado por: García (2022)

Tabla 7. ***Preguntas del cuestionario COSO ERM 2017***

GAD MUNICIPALIDAD DE AMBATO PERÍODO 2022 CUESTIONARIO DE CONTROL INTERNO SEGÚN MÉTODO COSO ERM 2017				
Componente	**Principios**	**Práctica**	**SÍ**	**NO**
GOBIERNO Y CULTURA	**1. La Junta Directiva ejerce supervisión sobre los riesgos**	¿Se realizan reuniones con el personal del departamento de TI para actualizar las prácticas de gestión de riesgos?		
		¿Se revisan y actualizan periódicamente las decisiones y objetivos estratégicos de la entidad en el resguardo de la información?		
		¿Existe la asignación de responsabilidad para el manejo, supervisión y control continuo de los procesos dentro del departamento de TI?		
		Al tomar una decisión sobre el uso o aplicación de las TI ¿existe un responsable que notifique mediante los procesos pertinentes?		
	2. Establece estructuras operativas	¿El departamento de TI maneja buenas prácticas para la gestión de riesgos?		
		¿Se tienen acciones correctivas en caso de presentarse eventualidades con el fin de establecer la forma de actuar?		
		¿El software que se utiliza soporta el proceso institucional?		
		¿Se realizan actividades de supervisión continuas sobre el riesgo existente?		
	3. Define la cultura deseada	¿Se tiene en cuenta competencias, habilidades y conocimientos necesarios para cada función relacionada con las TI?		
		¿Se han cumplido con los objetivos planteados en la entidad sobre el uso de TI?		
		¿Fomenta una cultura de inteligencia en riesgos?		
		¿El departamento de TI conoce los objetivos planteados a cumplirse?		
		¿Existe compromiso por parte del personal de TI en no manipular los datos del departamento?		

Fuente: Adaptado de COSO ERM (2017)
Elaborado por: García (2022)

Tabla 8. ***Actividades de las prácticas de gobierno COBIT***

ACTIVIDADES	NIVEL DE CAPACIDAD
1. Desarrollar procesos de negocio, servicios de soporte, aplicaciones e infraestructura y repositorios de información basados en las especificaciones acordadas y requerimientos técnicos, funcionales y de negocio. 2. Cuando proveedores terceros estén involucrados en el desarrollo de la solución, asegurar que el mantenimiento, soporte, estándares y licenciamiento están contempladas en las obligaciones contractuales 3. Registrar las peticiones de cambio y revisar el diseño, rendimiento y calidad, asegurando una participación activa de las partes interesadas afectadas 4. Documentar todos los componentes de la solución acorde a los estándares definidos y mantener el control de la versión sobre los mismos y la documentación asociada. 5. Evaluar el impacto de la personalización de la solución y la configuración en el rendimiento y eficiencia de las soluciones adquiridas y en su interoperabilidad con las aplicaciones, sistemas operativos y otra infraestructura existentes. Adaptar los procesos de negocio como se requiera para aprovechar las capacidades de la aplicación. 6. Asegurar que las responsabilidades por usar una alta seguridad o acceso restringido a los componentes de la infraestructura están claramente definidas y son comprendidas por todos aquellos que desarrollan e integran los componentes de la infraestructura. Su uso debería ser supervisado y evaluado.	

Fuente: Adaptado de COBIT (2012)
Elaborado por: García (2022)

2.1.3 Fases del desarrollo

Tabla 9. ***Fases de auditoría***

Fases	Evidencia	Resultado
Fase I Planificación	• Encuesta • Información estratégica de la empresa • Establecimiento del alcance de la auditoría • Guía de visita previa • Memorando de planificación (archivo permanente) • Programa de Auditoría	Metodología de la Auditoría al sistema de información (Archivo Permanente)
Fase II Ejecución	• Identificación de vulnerabilidades ,amenazas y • riesgos • Marco de referencia COSO ERM 2017 • Marco de referencia COBIT	Validación de los descubrimientos (hallazgos)
Fase III Comunicación	• Emisión del informe de auditoría al sistema de información	Comunicación de resultados

Elaborado por: García (2022)

Fase I de Planificación

Para la Planificación se revisó la información estratégica y legal del GAD además de las tecnologías y el control interno sobre los elementos que están constituidos del sistema de información.

En el departamento de las TI se estableció el alcance en base a la identificación de hardware y software, específicamente de sistemas y aplicaciones de información como parte de la revisión.

En la auditoría al sistema de información se planeó los recursos en base a la evaluación de riesgos para detectar las áreas y activos más vulnerables con el fin de evitarlos y mejorar la organización tecnológica.

El Programa de Auditoría se elaboró para delimitar la auditoría al sistema de información al centro de procesamiento de datos. Por último se realizó una guía de visita previa con la finalidad de conocer más a fondo la entidad y sus componentes para obtener información que nos ayudará en el proceso de realizar la Auditoría.

Fase II de Ejecución

Los controles fueron de ayuda para observar si existieron daños físicos o destrucción de los activos. Además sirvió para prevenir pérdidas por fraude o errores cometidos por el personal, extravío de documentos fuente, inaccesibilidad de los datos, archivos e in formes, robos o mal uso de dispositivos y medios de almacenamiento. Así que el riesgo comprendió en evitar la interrupción de las operaciones del negocio por fallas del sistema, pérdida de integridad de los datos e ineficiencia de operaciones.

Para la auditoría al sistema de información se elaboraron matrices para las posibles amenazas, vulnerabilidades y riesgos que se pueden presentar utilizando técnicas como los Marcos de Referencias COSO ERM 2017 Y COBIT. Todos estos fueron aplicados por los principios relacionados con el GADMA mediante procesos en la gestión de las TI, evaluación de riesgos y la seguridad de la información.

Fase III de Comunicación

En el informe final de Auditoría se detalló todos los resultados obtenidos producto de la auditoría al sistema de información, el cual fue dirigido al Jefe del departamento de las TI una vez obtenidas y analizadas las respuestas de los componentes objeto de estudio de sistemas de información, concluyendo y recomendando controles claves direccionados al mejoramiento de la gestión del as TI en sus sistema de información.

CAPÍTULO III

DESARROLLO

El proyecto integrador se basó en la Auditoría al sistema de información del centro de procesamiento de datos en el GAD Municipalidad de Ambato aplicando las 3 fases correspondientes.

En la Fase I Planificación se recabó de manera adecuada la información más relevante del GAD Municipalidad de Ambato del período 2022 para proceder con un análisis, integrando los conocimientos obtenidos en la aplicación de una auditoría y así, poder plantear soluciones a los problemas y a las necesidades encontradas en la institución.

En la Fase II Ejecución se aplicó el Marco de Referencia COSO ERM 2017 y el Marco de Referencia COBIT en donde los datos extraídos del Departamento de TI del GADMA. Donde fueron aplicados en la búsqueda de vulnerabilidades y amenazas que den lugar a riesgos inminentes así que se evaluó, califico e interpreto los resultados obtenidos.

En la Fase III Comunicación se procedió a delimitar los problemas encontrados definiéndolos como hallazgos para buscar soluciones y recomendar cambio y mejores en las prácticas de Gobierno y Control interno del Departamento de TI.

Fase I Planificación

Guía de visita previa

Tabla 10. ***Información general***

GVP

1. INFORMACIÓN GENERAL	
1.1. Nombre de la entidad a Auditar	GAD Municipalidad de Ambato
1.2. Número de Ruc	1860000210001
1.3. Dirección	Av. Atahualpa y Río Cutchi
1.4. Correo electrónico de la empresa	salcaldia@ambato.gob.ec
1.5. Fecha de la visita	27 de mayo del 2022
1.6. Responsable de contestar la entrevista	Ing. Ricardo Fiallos
1.7. Entrevistador: Nombre y Cargo	Daniel García

Elaborado por: García (2022)

Tabla 11. ***Información secundaria***

2. INFORMACIÓN DEL DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN	
	La Dirección de Tecnologías de la Información se encarga de dirigir y gestionar servicios relacionados con tecnologías de la información; proveer servicios de diseño y desarrollo de software; y, realizar el monitoreo y mantenimiento continuo de la infraestructura de telecomunicaciones.

Elaborado por: García (2022)

Tabla 12. ***Información de la institución***

AP

INFORMACIÓN DE LA Institución	
Nombre de la Empresa:	GAD Municipalidad de Ambato
Tipo de Auditoría:	Auditoría de Sistemas
Período Auditado:	Año 2022

Elaborado por: García (2022)

Tabla 13. ***Información de la institución***

A.P.1	ORGANIZACIÓN DE LA ENTIDAD	
A.P.1.1	Breve historia de la entidad auditada	**Véase Capítulo I, pág. 1**
A.P.1.2	Certificado del RUC	**Véase Anexos , pág. 81**
A.P.1.3	Base Legal de la Entidad	**Véase Capítulo I, pág. 7**
A.P.1.4	Lista de máximas autoridades	**Véase Capítulo III, pág. 29**
A.P.1.5	Organización general de la entidad	**Véase Capítulo I, pág. 5**
A.P.1.6	Reglamentos, instructivos y otra normatividad interna o especifica	**Véase Capítulo III, pág.30**

A.P.2	VISIÓN ESTRATÉGICA DE LA INSTITUCIÓN	
A.P.2.1	Visión, misión, objetivos y valores institucionales	**Véase Capítulo I, pág. 2**
A.P.2.2	Principales actividades institucionales y descripción de bienes o servicios	**Véase Capítulo I, pág. 6**
A.P.2.3	Detalle de las Fortalezas, Oportunidades, Debilidades y Amenazas de la entidad	**Véase Capítulo III, pág.31**
A.P.2.4	Marcas y Logos de la Entidad	**Véase Capítulo I, pág. 8**
A.P.2.5	Ubicación de la Entidad	**Véase Capítulo I, pág. 8**

Elaborado por: García (2022

Máximas Autoridades

A.P.29.4

Tabla 14. ***Máximas autoridades***

CARGO	NOMBRE Y APELLIDO
Alcalde Cantonal	Dr. Javier Francisco Altamirano Sánchez
Secretaria de Gestión Estratégica	Ing. Mgs. María Elena Calle Naranjo
Secretario de Concejo Municipal	Abg. Adrián Andrade López
Procurador Síndico Municipal	Abg. Javier Aguinaga Bósquez
Directora Financiera	Ing. Priscila Fernández Naranjo
Director de Servicios Públicos	Ing. Álvaro Mantilla
Director de Gestión de Suelo	Arq. Trajano Sánchez Rizzo
Director de Avalúos y Catastros	Arq. Manuel Guzmán
Directora de Cultura y Turismo	Diana Mariela Freire Muñoz
Director de Planificación	Arq. Julio Rodríguez
Director de Comunicación Institucional	Mgs. Lcdo. Miguel Cabrera
Director de Desarrollo Social y Económico	Ing. William Roberto Yambay
Director de Obras Públicas	Ing. Klever Padrón
Director de Gestión Ambiental	Blgo. Mauricio Vargas
Director de Tecnologías de la Información	Ing. Xavier Francisco López
Secretaria de Participación Ciudadana	Sra. Neida Vásconez
Despacho General de Alcaldía	Sra. Mercedes Soria
Agencia de Orden y Control Ciudadano	Crnel. (SP) Fernando Torres

Fuente: GAD Municipalidad de Ambato (2022)

Reglamentos, instructivos y otra normatividad interna o específica

A.P.30.6

Tabla 15. ***Reglamentos y normativas***

Art. 7 de la Ley Orgánica de Transparencia y Acceso a la Información Pública – LOTAIP		
LOTAIP Literal a3) Regulaciones y procedimientos internos aplicables a la entidad		
Regulación o procedimiento que expide	**No. del documento**	**Fecha de la regulación o del procedimiento**
Resolución de la aprobación reglamento interno del GADMA	DA-14-030	05-feb-14
Reglamento interno del GADMA	DA-14-0156	05-feb-14
Resolución de reforma a la estructura orgánica del gobierno autónomodescentralizado municipalidad de Ambato – GADMA	DA-20-096	17-ago-20
Acto normativo interno regula la aplicación de faltas leves dentrodel régimen disciplinario LOSEP	DA-20-023	17-sep-20
Reformar la resolución administrativa da-20-096, en su artículo 6 inciso sexto, mediante la cual se reforma la estructura orgánica	DA-20-156	18-nov-20
Estatuto orgánico de gestión organizacional por procesos del gobierno autónomo descentralizado municipalidad de Ambato	DA-20-0169	24-dic-20
Acto normativo de carácter administrativo de aplicación el régimendisciplinario sujeto	DA-21-028	06-ago-21

Fuente: GAD Municipalidad de Ambato (2022)

Detalle de las fortalezas, oportunidades, debilidades y amenazas de la entidad

Tabla 16. ***FODA***

A.P.2.3

	FORTALEZAS	OPORTUNIDADES
ANÁLISIS FODA	✚ Asume las competencias legales establecidas siendo pioneros a nivel regional por la institucionalidad y manejo de su gestión ✚ Se considera el servicio al usuario como parte prioritaria dentro de la institución ✚ Constantes fuentes de ingresos por recaudaciones, y capacidad de endeudamiento ✚ Impulso de proyectos con gestión transparente y participativa ✚ La cultura y tradición de Ambato es reconocida a nivel internacional ✚ Modelo de gestión y desarrollo de proyectos basada en los Objetivos de Desarrollo Sostenible (ODS) de la ONU ✚ Predisposición de la máxima autoridad para la implementación de objetivos que promuevan la conformación de ciudad inteligente	✚ Iniciativas para fomentar infraestructura pública y privada sostenibles ✚ Impulso de comercio exterior a través de polos de desarrollo ✚ Interés de usuarios y contribuyentes en conocer los productos y servicios que presta la institución ✚ Mecanismos para mejorar la calidad del agua en la cuenca Alta del Río Pastaza ✚ Integración a la IOTS (Internet de las cosas) ✚ Prestación de servicios en línea y automatización de procesos ✚ Conciencia medioambiental en las nuevas generaciones ✚ Alianzas público-privadas para impulsar proyecto
	DEBILIDADES	**AMENAZAS**
	✚ Desarticulación de gestión entre los directores departamentales provocaría no cumplir el plan de trabajo del Sr. Alcalde. ✚ Instrumentos de planificación territorial local desactualizados ✚ Instrumentos normativos desactualizados ✚ Liderazgo comunicacional poco efectivo ✚ Falta de capacitación y continuidad en los funcionarios públicos ✚ Concentración en la cobertura de servicios ✚ Recursos tecnológicos desactualizados para ejercicio de las funciones.	✚ Pago de impuestos, transferencias de recursos por parte del gobierno central que afecten el auto sustento de la municipalidad ✚ Susceptibilidad a riesgos naturales y/o pandemia ✚ Ingresos por recesión económica que incrementa el no pago de impuestos ✚ Reducción de empleo ✚ Incremento de niveles de delincuencia ✚ Desconfianza en la gestión municipal ✚ Escasez de agua en el cantón ✚ Inestabilidad política

Fuente: GAD Municipalidad de Ambato (2022)

Gráfico 5. ***Memorando***

"YIN-YANG"
FIRMA DE AUDITORÍA

MM

MEMORANDO DE PLANIFICACIÓN
PERIODO DEL AÑO 2022

Entidad : **GAD MUNICIPALIDAD DE AMBATO**

Auditoría al Sistema de Información del Centro de Procesamientos de datos en el GADMA

Periodo: 2022

1. REQUERIMIENTO DE LA AUDITORIA

2. FECHA DE INTERVENCION	**Fecha estimada**
Cronograma	
Marco de Referencia COSO ERM 2017	01/06/2022
Marco de Referencia COBIT	08/06/2022

3. EQUIPO MULTIDISCIPLINARIO

NOMBRE	**INICIALES**
Daniel Alexis García Altamirano	DAGA

4. RECURSOS

PROFESIONALES

Para la realización del presente proyecto integrador se desarrollo por el grupo de trabajo conformado por la Doctora Patricia Paola Jimenez Estrella en calidad de tutora y yo, Daniel Alexis García Altamirano estudiante de la Facultad de Contabilidad y Auditoría, Carrera de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

MATERIALES

Hardware y Software	$ 500,0,00
Gastos de transporte	$ 200,0,00
Oficios	$ 50,0,00
Impresiones y copias	$ 100,0,00
	$ 850,0,00

5. ENFOQUE DE LA AUDITORIA

5.1 Información general de la entidad auditada

-Misión

El GAD Municipalidad de Ambato es una institución que promueve el desarrollo sostenible del cantón, a través de la prestación de servicios accesibles, óptimos y oportunos, la implementación de políticas públicas incluyentes, la mejora continua e innovación de sus procesos y servicios, el uso de tecnologías, y el fomento de la participación ciudadana, para mejorar la calidad de vida de sus ciudadanos.

-Visión

Al 2023 El GAD Municipalidad de Ambato será la institución formuladora y ejecutora de acciones que permitan hacer de Ambato un cantón seguro, digital, resiliente, inclusivo, sostenible, y saludable, con servicios de calidad; generadora de políticas que posicionen al cantón a nivel nacional como polo de desarrollo comercial y productivo, fundamentada en el capital intelectual y en el uso eficiente y transparente de sus recursos.

-Objetivos

1. Promover el desarrollo social e intercultural fortaleciendo la salud, bienestar, igualdad de género, deporte y recreación; la conservación del patrimonio cultural, identidad, apropiación de tradiciones y costumbres de Ambato.

2. Promover el desarrollo urbano sostenible, mediante la transformación cultural, participación ciudadana, educación, capacitación, control mitigación, restauración de la transgresión ambiental, aplicando principios de movilidad sostenible, jerarquización de residuos, cuidado del agua, cuidado animal, cuidado ambiental, para el beneficio del cantón.

3. Impulsar el desarrollo productivo del cantón, mediante la optimización de sus diferentes sistemas formales de comercialización, en pro de su beneficio económico.

4. Optimizar las fuentes de financiamiento del presupuesto institucional, a través de recaudaciones propias, recursos fiscales, líneas de crédito y cooperación, para financiar la gestión municipal.

5. Garantizar la dotación de servicios públicos e infraestructura, mediante procesos sostenibles, para el beneficio de los habitantes del cantón.

6. Impulsar la innovación y competitividad del cantón, a través de la digitalización de servicios municipales, para el fortalecimiento de la gestión integral de la calidad institucional y la óptima interacción con los actores de interés y ciudadanía en general.

7. Fortalecer la administración interna institucional, a través de un modelo de gestión apropiado, la mejora continua e innovación de sus procesos y el uso de las tecnologías de información y comunicación, con el fin de alcanzar la excelencia del servicio.

8. Impulsar el desarrollo integral de Ambato, mediante normas que generen incentivos tributarios, un adecuado régimen de uso del suelo y un crecimiento urbano que sea ordenado, seguro, turístico, cultural, patrimonial, gastronómico, natural, inclusivo y sostenible, a fin de promover la inversión privada.

9. Fomentar la actualización y el cumplimiento de las ordenanzas y resoluciones de las competencias municipales acordes con las leyes y normas nacionales vigentes.

-Actividades Principales

N°	Denominación del servicio
1	Servicios en línea
2	Emprendo Ambato
3	Registro de la Propiedad
4	Trámites, Dependencias y Formularios
5	Quejas y Sugerencias
6	GEOPORTAL

- Base Legal	
Art. 7 de la Ley Orgánica de Transparencia y Acceso a la Información Pública - LOTAIP Literal a2) Base legal que la rige	
Tipo de la Norma	Norma Jurídica
Carta Suprema	Constitución de la República del Ecuador
Norma internacional	Tratados y convenios internacionales
Códigos	Código Orgánico de Coordinación Territorial, Descentralización y Autonomía - COOTAD
	Código del Trabajo
	Código Orgánico Administrativo
	Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público
Leyes Orgánicas	Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)
	Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP)
	Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (LOGJCC)
	Ley Orgánica de Servicio Público (LOSEP)
	Ley Orgánica de la Contraloría General del Estado
	Ley Orgánica de la Contraloría General del Estado
	Ley de Seguridad Pública y del Estado
Reglamentos de Leyes	Reglamento General a la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)
	Reglamento General a la Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP)
	Reglamento a la Ley Orgánica de Servicio Público (LOSEP)
Decretos Ejecutivos	Los Decretos Ejecutivos relacionados con la institución se re direccionarán al sitio web donde se encuentran alojados
Ordenanzas Municipales	Ordenanza de competencias territoriales

5.2 Motivo de la auditoría

La auditoria de sistemas es dirigida al sistema de información del Centro de procesamiento de datos en el GAD Municipalidad de Ambato para recoger, agrupar y evaluar la seguridad razonable de la infraestructura tecnológica en el recogimiento, almacenamiento, procesamiento y disposición de la información siendo este un recurso para la toma de decisiones.

5.3 Enfoque a:

AUDITORIA DE SISTEMAS AL SISTEMA DE INFORMACIÓN DEL CENTRO DE PROCESAMIENTO DE DATOS

5.4. Objetivos

Objetivo General

Aplicar la auditoría al sistema de información del centro de procesamiento de datos en el GADMA para un mejor manejo y control informático.

Objetivos Específicos

Utilizar herramientas, técnicas y procedimientos para la elaboración de la planificación requerida
Elaborar los papeles de trabajo relacionados a la auditoría de sistemas para la recolección de datos en su ejecución.
Dictaminar el informe final para una mayor comprensión de todas las evidencias y procesos efectuados

5.5. Alcance

La Contraloría General del Estado es la encargada de realizar las respectivas auditorías para verificar, examinar y evaluar las funciones de las instituciones públicas incluido el GAD Municipalidad de Ambato. Sin embargo, las Auditorías de Gestión y Financieras son las únicas aplicadas dando lugar a la necesidad de realizar otros tipos de auditorías para ampliar conocimientos y tener más control sobre las diversas áreas existentes. Por lo tanto existe la necesidad de aplicación de una auditoría de sistemas informáticos. La Auditoría al Sistema de Información del Centro de procesamiento de datos tendrá un rol funadamental en el análisis de los activos frente a los posibles riesgos dentro del departamento de TI por ello surge la necesidad de una implementación de controles internos informáticos para asegurar que el procesamiento de información tenga una seguridad razonable .

5.6. Resumen de los Resultados de la Evaluación del Control Interno.

VALORACIÓN			
Calificación Total	(C.T.)=	44	
Ponderación Total	(P.T.)=	72	
Nivel de Confianza	NC= CT/PT x 100	61,11%	
Nivel de Riesgo Inherente / De control	RI-RC= 100% - NC%	38,89%	ENFOQUE DE AUDITORIA
	MODERADO		*MIXTO-DOBLE PROPÓSITO*

El Marco de Referencia COSO ERM 2017 en base a la gestión de riesgos empresariales fue desarrollado con la necesidad de evaluar los 5 componentes con los 20 principios, abordando preguntas de interés para conocer el estado actual del departamento de TI en el GADMA. Se realizaron preguntas con opciones de respuesta de sí (1) o no(0) para caliificar y poder conocer el nivel de riesgo y confianza ,mostrándonos un nivel de confianza de 61,11% y un nivel de riesgo de 38,89% sinedo este en un rango moderado.

5.7. Grado de Confianza y controles claves

En el Componente Gobierno y Cultura se obtuvo un nivel de confianza del 90% con un riesgo mínimo del 10% por lo tanto su resultado final es bajo, con un enfoque de auditoría mixto- doble propósito es decir realizar pruebas de cumplimiento y sustantivas siendo este el componente con más cumplimiento dentro del Departamento de TI.

En el Componente Estrategia y Objetivos se obtuvo un nivel de confianza del 43,75% con un riesgo mínimo del 56,26% por lo tanto su resultado final es un riesgo alto, por ello su enfoque de auditoría es pruebas sustantivas.

En el Componente Desempeño se obtuvo un nivel de confianza del 44,44% con un riesgo mínimo del 55,56% por lo tanto su resultado final es un riesgo alto, por ello su enfoque de auditoría es pruebas sustantivas.

En el Componente Revisión se obtuvo un nivel de confianza del 63,64% con un riesgo mínimo del 36,36% por lo tanto su resultado final es moderado, con un enfoque de auditoría mixto- doble propósito es decir realizar pruebas de cumplimiento y sustantivas.

En el Componente Información, comunicación y reporte se obtuvo un nivel de confianza del 58,33% con un riesgo mínimo del 41,67% por lo tanto su resultado final es moderado, con un enfoque de auditoría mixto- doble propósito es decir realizar pruebas de cumplimiento y sustantivas.

6 TRABAJO A REALIZAR EN LA FASE DE EJECUCIÓN

6.1 TRABAJO A REALIZAR POR LOS AUDITORES EN LA FASE DE EJECUCIÓN

- Verificación de controles verificar con lo de los programas y objetivos especificos de la tesis
- Análisis de riesgos, vulnerabilidades y amenazas
- Marco de referencia COSO ERM 2017
- Marco de referencia COBIT

7. COLABORACIÓN DE LA ENTIDAD AUDITADA

7.1 Ingenieros internos

Ing. Ricardo Fiallos

7.2 Otros profesionales

Ing. Patricio Mayorga
Ing. Galo Castillo

8. OTROS ASPECTOS

La Auditoría al Sistema de Información del Centro de Procesamiento de datos en el GAD Municipalidad de Ambato se lo realiza por primera vez siendo esta, una apertura de mejora en el departamento de las TI máximimando su eficiencia y eficacia.

Fuente: GAD Municipalidad de Ambato (2022)
Elaborado por: García (2022)

OBJETIVOS

1.- Evaluar los métodos y procedimientos del uso de aplicaciones y sistemas de información en la entidad.

2.-Identificar los niveles de riesgos que pueden presentar los activos de información

3.-Verificar los niveles de capacidad de los procesos informatizados en el software de aplicación para el manejo de los datos

4.-Aplicar los marcos de referencia COBIT y COSO ERM 2017 al sistema de información de la entidad.

Tabla 17. ***Programa de auditoría***

N.	PROCEDIMIENTOS	PRUEBA (TIPO DE PROCEDIMIENTOS)	TECNICA	ELABORADO POR	FECHA
1	Evaluar el control interno	Pruebas de cumplimiento	Cuestionario	DAGA	07/06/22
2	Identificar los niveles de riesgos que pueden presentar los activos de información	Pruebas sustantivas	Observación Matriz de evaluación	DAGA	07/06/22
3	Verificar los niveles de capacidad de los procesos informatizados	Pruebas de cumplimiento	Matriz de evaluación	DAGA	07/06/22
4	Aplicar los marcos de referencia COBIT y COSO ERM 2017 al sistema de información de la entidad	Pruebas sustantivas	Matriz de evaluación	DAGA	07/06/22

Elaborado por: García (2022)

Fase II Ejecución

En la Ejecución se aplicó los dos Marcos de Referencias para la evaluación y gestión de riesgos en el Departamento de TI del GAD Municipalidad de Ambato.

Los datos fueron extraídos y ejecutados a la realidad del departamento en base al sistema de información del centro de procesamiento de datos, con la finalidad de conocer el marco de TI, sus estrategias, control interno y seguridad de la información.

A continuación se presenta los marcos de referencias:

Marco de referencia COSO ERM 2017

EL COSO ERM 2017 en la Gestión de Riesgos Empresariales abordó sobre los riesgos y el cumplimiento de control interno para conocer las vulnerabilidades y amenazas que den lugar a los posibles riesgos.

Tiene 5 componentes que son: Gobierno y cultura, Estrategias y objetivos, Desempeño, Revisión, Información, comunicación y reporte y sus 20 principios relacionados a cada componente. Todo esto fue elaborado con preguntas relacionadas a cada componente para cuantificar y medir el nivel de riesgo y el nivel de confianza acorde a la **Tabla 3.** ***Ponderación nivel de confianza y nivel de riesgo.***

Las preguntas con la metodología ERM ayudó a conocer en qué porcentaje el departamento gestiona los riesgos y a proponer soluciones a las anomalías o hallazgos encontrados en el transcurso de su elaboración.

Gráfico 6. ***Marco de referencia COSO ERM 2017***

COMPONENTE	N.	PREGUNTA	C		C.T
			SI	NO	
Gobierno y cultura	1	¿Se realizan reuniones con el personal del departamento de TI con el fin de actualizar las prácticas de gestión de riesgos?	1		**1**
	2	¿Se revisan y actualizan periódicamente las decisiones y objetivos estratégicos de la entidad en el resguardo de la información?	1		**1**
	3	¿Existe la asignación de responsabilidad para el manejo, supervisión y control continuo de los procesos dentro del departamento de TI?		0	**0**
	4	Al tomar una decisión sobre el uso o aplicación de las TI ¿existe un responsable que notifique mediante los procesos pertinentes?		0	**0**
	5	¿El departamento de TI maneja buenas prácticas para la gestión de riesgos?	1		**1**
	6	¿Se tienen acciones correctivas en caso de presentarse eventualidades con el fin de establecer la forma de actuar?		0	**0**
	7	¿El software que se utiliza soporta el proceso institucional?	1		**1**
	8	¿Se realizan actividades de supervisión continuas sobre el riesgo existente?	1		**1**
	9	¿Se tiene en cuenta competencias, habilidades y conocimientos necesarios para cada función relacionada con las TI?	1		**1**
	10	¿Se han cumplido con los objetivos planteados en la entidad sobre el uso de TI?	1		**1**
	11	¿Fomenta una cultura de inteligencia en riesgos?		0	**0**
	12	¿El departamento de TI conoce los objetivos planteados a cumplirse?	1		**1**
	13	¿El departamento de TI no divulga la información de confidencialidad?	1		**1**
	14	¿Existe compromiso por parte del personal de TI en no manipular los datos del departamento?	1		**1**
	15	¿El personal está consciente de las consecuencias que trae un acto de corrupción en ciberseguridad?	1		**1**
	16	¿La gestión de riesgos está integrada en la transparencia y los subcomponentes de los valores éticos?	1		**1**
	17	¿Clarifica la responsabilidad en todo el departamento de TI?	1		**1**
	18	¿Se tiene claro la segregación de funciones del personal en la gestión de riesgos?		0	**0**
	19	¿Se realizan capacitaciones al personal en base a la gestión de riesgos?	1		**1**
	20	¿El departamento fomenta el desarrollo de conocimientos e incentiva al personal por el mejoramiento de sus actividades?	1		**1**

Estrategia y objetivos	21	¿El departamento cumple con las leyes, normas y estatutos de control interno institucional y seguridad de la información?	1		**1**
	22	¿El departamento conoce y aplica el marco de referencia COSO ERM 2017 ante los riesgos?		0	**0**
	23	¿Los objetivos institucionales están relacionados a la productividad y gestión en el departamento de TI?			**0**
	24	¿Existen escalas de medición numérica para evaluar los riesgos?		0	**0**
	25	¿Se detecta rápidamente la aparición de los riesgos informáticos?	1		**1**
	26	¿Se conoce la gravedad que puede ocasionar la aparición de riesgos en los sistemas de información?	1		**1**
	27	¿El departamento cuenta con políticas de control interno para la gestión de riesgos informáticos?	1		**1**
	28	¿El jefe responsable del departamento de TI es conocedor de los planes estratégicos para la toma de decisiones?			**0**
	29	¿Existe personal capacitado en la elaboración de estrategias alternativas contra riesgos de los sistemas de información?	1		**1**
	30	¿El departamento de TI cuenta con estrategias suficientes ante la aparición de posibles riesgos?		0	**0**
	31	¿En el departamento se han medido el nivel de credibilidad en las estrategias planteadas ante riesgos?		0	**0**
	32	¿Se han añadido nuevos objetivos empresariales en el departamento de TI para prevenir los riesgos?		0	**0**
	33	¿Se tomaron en cuenta los riesgos ocasionados anteriormente para la nueva toma de decisiones institucionales?	1		**1**
	34	¿Existe un plan de mitigación ante posibles riesgos?	1		**1**
	35	¿Los objetivos institucionales están relacionados a la gestión de riesgos?			**0**
Desempeño	36	¿Se encuentran debidamente identificados los riesgos en cumplimiento de los controles internos informáticos?		0	**0**
	37	¿Los diferentes riesgos legales y administrativos relacionados a las actividades del departamento de TI?	1		**1**
	38	¿El departamento cuenta con un procedimiento para identificar riesgos potenciales en las actividades que desarrollan?		0	**0**
	39	¿El riesgo de fraude es evaluado en el departamento de TI?		0	**0**
	40	¿Existen procedimientos establecidos que aseguren el cumplimiento de las leyes en el manejo de los activos de información?	1		**1**
	41	¿Se orientan a detectar y prevenir los abusos y el fraude en los procesos establecidos por el departamento de TI?	1		**1**
	42	¿El departamento de TI conoce los riesgos por no cumplir con las regulaciones y leyes aplicables en su operación?	1		**1**
	43	¿Para establecer el riesgo potencial y la probabilidad de ocurrencia existen criterios definidos?		0	**0**
	44	¿El departamento de TI ha preparado un plan de riesgos en el que se identifica su probabilidad de ocurrencia e impacto potencial?		0	**0**
	45	¿Los riesgos han sido clasificados como tolerantes o que requieran las adopciones de medidas?		0	**0**
	46	¿El departamento de TI toma acciones para identificar factores críticos de riesgos potenciales en las actividades?		0	**0**
	47	¿El departamento de TI implementa medidas de mitigación en respuesta al riesgo observado?	1		**1**
	48	¿Se promueve el establecimiento de una cultura de gestión de riesgo mediante la provisión de capacidades al personal para el desarrollo de los mismos?	1		**1**
	49	¿Se ha definido sobre la base del mapa de riesgos la respuesta al mismo?	1		**1**
	50	¿El departamento de TI cuenta con procedimientos para erradicar riesgos identificados como fraude?	1		**1**

Revisión	51	¿El departamento identifica los cambios sustanciales que se deben efectuar?	1		**1**
	52	¿El departamento evalúa los cambios sustanciales que se hayan realizado en el período?	1		**1**
	53	¿El departamento verifica el funcionamiento de la gestión de los riesgos informáticos?		0	**0**
	54	¿Son verificados con frecuencia los riesgos y el desempeño en sus períodos de gestión?	1		**1**
	55	¿Tienen claro conocimiento de las revisiones que deben realizar en el departamento?	1		**1**
	56	¿El departamento plantea adecuadamente las revisiones necesarias a realizar?			**0**
	57	¿Plantean mejoras en las gestiones de riesgos informáticos identificados?	1		**1**
	58	¿Propone mejoras en la gestión de riesgos informáticos a través de controles e indicadores?	1		**1**
	59	¿Dentro de las mejoras a aplicar en el departamento, se toma en cuenta el dinamismo profesional?		0	**0**
	60	¿Las propuestas de mejora en la gestión de riesgos al sistema de información son planteadas oportunamente?	1		**1**
Información, comunicación y reporte	61	¿Se hace uso de tecnología para los intereses departamentales?	1		**1**
	62	¿Tienen base de datos con información que soporta la toma de decisiones?	1		**1**
	63	¿Existe seguridad de la información de la entidad?	1		**1**
	64	¿Cuenta con Firewalls para evitar intrusos o usuarios de carácter malicioso?	1		**1**
	65	¿Se comparte información necesaria, de fuentes internas y externas a través de todo el departamento de TI?		0	**0**
	66	¿Se define las estrategias de acuerdo a los riesgos informáticos identificados?	1		**1**
	67	¿Se revisa los posibles impactos de los riesgos en las estrategias ya definidas?		0	**0**
	68	¿Se toma en cuenta el riesgo para estrategia y desempeño departamental?	1		**1**
	69	¿Se coordina de mejor manera las expectativas de gobierno y supervisión de TI?		0	**0**
	70	¿Se ha definido una filosofía de gestión de riesgos de sistemas de información?	1		**1**
	71	¿Las actividades de gestión de riesgo en el departamento de TI están implementadas consistentemente?		0	**0**
	72	¿El departamento de TI existe una Alineación entre desempeño y gestión de riesgos?		0	**0**
		PONDERACIÓN TOTAL			**72**
		CALIFICACIÓN TOTAL			**44**

Fuente: Adaptado de COSO ERM 2017 (2017)
Elaborado por: García (2022)

Gráfico 7. ***Resultados COSO ERM 2017***

VALORACIÓN		
Calificación Total	44	
Ponderación Total	72	
Nivel de Confianza	61,11%	
Nivel de Riesgo Inherente / De control	38,89%	**ENFOQUE DE AUDITORIA**
	MODERADO	***MIXTO-DOBLE PROPÓSITO***

Gobierno y cultura		
Calificación Total	18	
Ponderación Total	20	
Nivel de Confianza	90,00%	
Nivel de Riesgo Inherente / De control	10,00%	**ENFOQUE DE AUDITORIA**
	BAJO	***CUMPLIMIENTO***

Estrategia yobjetivos		
Calificación Total	7	
Ponderación Total	16	
Nivel de Confianza	43,75%	
Nivel de Riesgo Inherente / De control	56,25%	**ENFOQUE DE AUDITORIA**
	ALTO	***SUSTANTIVO***

Desempeño		
Calificación Total	8	
Ponderación Total	18	
Nivel de Confianza	44,44%	
Nivel de Riesgo Inherente / De control	55,56%	**ENFOQUE DE AUDITORIA**
	ALTO	***SUSTANTIVO***

Revisión		
Calificación Total	7	
Ponderación Total	11	
Nivel de Confianza	63,64%	
Nivel de Riesgo Inherente / De control	36,36%	**ENFOQUE DE AUDITORIA**
	MODERADO	***MIXTO-DOBLE PROPÓSITO***

Información, comunicación y reporte		
Calificación Total	7	
Ponderación Total	12	
Nivel de Confianza	58,33%	
Nivel de Riesgo Inherente / De control	41,67%	**ENFOQUE DE AUDITORIA**
	MODERADO	***MIXTO-DOBLE PROPÓSITO***

Fuente: Adaptado de COSO ERM 2017 (2017)
Elaborado por: García (2022)

Marco de referencia COBIT

En esta sección se aplicó el Marco de Referencia COBIT en donde se desarrollaron 5 Dominios con sus 7 procesos que son: EDM04 Asegurar la optimización de recursos, APO 01 Gestionar el marco de gestión de TI, APO 12 Gestionar el riesgo, APO 13 Gestionar la seguridad, BAI09 Gestionar los activos, DSS05 Gestionar servicios de seguridad y finalmente MEA02 Supervisar, evaluar y valorar el sistema de control interno.

El dominio BAI (Construir, Adquirir e Implementar), con uno de sus procesos BAI 09 (Gestionar los activos) y todas sus prácticas de gestión se presenta como el más alcanzado en el Gobierno Corporativo de TI dentro del departamento.

Los niveles de capacidad actual de cada actividad definió las actividades de las prácticas de gobierno, adicionalmente se calificó el porcentaje de cumplimiento de las mismas, definiendo el promedio de esos porcentajes clasificándolos entre las escalas según la norma ISO 15504 que establece según el detalle de la **Tabla 5.** ***Niveles de Capacidad de Procesos***.

Finalmente se define el nivel objetivo meta de cumplimiento como el nivel “F”, dando a conocer si la actividad cumple o no con dicho objetivo.

A continuación se presenta como muestra de ejemplo la aplicación del Marco de Referencia COBIT con el proceso BAI 09 analizando sus prácticas de gestión y cada una de sus actividades:

Gráfico 8. ***Gestionar los activos***

BAI09 Gestionar los Activos	**Área:** Administración **Dominio:** Construir, Adquirir e Implementar
Descripción del Proceso Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia. **Declaración del Propósito del Proceso** Contabilización de todos los activos de TI y optimización del valor proporcionado por estos activos.	
El proceso apoya la consecución de un conjunto de objetivos primarios relacionados con las TI:	
Metas TI	**Métricas Relacionadas**
06 Transparencia de los costes, beneficios y riesgo de las TI	• Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados. • Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI.
11 Optimización de activos, recursos y capacidades de TI	• Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes • Tendencia de los resultados de las evaluaciones • Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades TI
Objetivos y Métricas del Proceso:	
Meta del Proceso	**Métricas Relacionadas**
1. Las licencias cumplen y están alineadas con las necesidades del negocio.	• Porcentaje de licencias usadas respecto a licencias pagadas
2. Los activos se mantienen en condiciones óptimas.	• Número de activos no utilizados • Comparativa de costes • Número de activos obsoletos

MATRIZ RACI																									
Matriz RACI BAI01																									
Práctica Clave de Gobierno	**Consejo de Administración**	**Director General Ejecutivo (CEO)**	**Director General Financiero (CFO)**	**Director de Operaciones (COO)**	**Ejecutivos de negocio**	**Propietarios de los Procesos de Negocio**	**Comité Ejecutivo Estratégico**	**Comité Estratégico (Desarrollo/Proyectos)**	**Oficina de Gestión de Proyectos**	**Oficina de Gestión del Valor**	**Director de Riesgos (CRO)**	**Director de Seguridad de la Información (CISO)**	**Consejo de Arquitectura de la Empresa**	**Comité de Riesgos Corporativos**	**Jefe de Recursos Humanos**	**Cumplimiento Normativo (Compliance)**	**Auditoría**	**Director de Informática/Sistemas (CIO)**	**Jefe de Arquitectura del Negocio**	**Jefe de Desarrollo**	**Jefe de Operaciones TI**	**Jefe de Administración TI**	**Gestor de Servicio (Service Manager)**	**Gestor de Seguridad de la Información**	**Gestor de Continuidad de Negocio**	**Gestor de Privacidad de la información**
BAI09.03 Gestionar el ciclo de vida de los activos.						C													C	C	A	R	R			
BAI09.04 Optimizar el coste de los activos.			R		I	C												A	R	R	R	R	R			
BAI09.05 Administrar licencias.					I	C										C	R	A		R	R	R	C			

PRÁCTICA DE GESTIÓN
BAI09.03 Gestionar el ciclo de vida de los activos.
Gestionar los activos desde su adquisición hasta su eliminación para asegurar que se utilizan tan eficaz y eficientemente como sea posible y son contabilizados y protegidos físicamente.

				76%		NIVEL DE CUMPLIMIENTO	NIVEL DE CAPACIDAD OBJETIVA	
		NIVEL DE CAPACIDAD DE PROCESOS						
ACTIVIDADES	NIVEL DE CAPACIDAD	N	P	L	F	VALOR	META	OBSERVACION
1. Adquirir todos los activos basándose en solicitudes aprobadas y de acuerdo con las políticas y las prácticas de adquisición de la empresa.	4			80%		80%	F	NO SE CUMPLE
2. Identificar el origen, recibir, verificar, probar y registrar todos los activos de una manera controlada, incluyendo el etiquetado físico, si fuera necesario.	3		50%			50%	F	NO SE CUMPLE
3. Aprobar los pagos y completar el proceso con proveedores según las condiciones acordadas por contrato.	4			80%		80%	F	NO SE CUMPLE
4. Desplegar los activos siguiendo el ciclo de vida de implementación estándar, incluyendo la gestión de cambios y pruebas de aceptación.	4			80%		80%	F	NO SE CUMPLE
5. Asignar activos a los usuarios, con aceptación y firma de responsabilidades, según corresponda.	4			80%		80%	F	NO SE CUMPLE
6. Reasignar los activos siempre que sea posible cuando ya no sean necesarios debido a un cambio de función de rol del usuario, redundancia dentro de un servicio o finalización de un servicio.	5				100%	100%	F	SE CUMPLE
7. Eliminar los activos cuando no sirvan a ningún propósito útil debido a la finalización de todos los servicios relacionados, tecnología obsoleta o falta de usuarios.	4			80%		80%	F	NO SE CUMPLE
8. Eliminar los activos de forma segura, teniendo en cuenta, por ejemplo, la eliminación permanente de los datos registrados en dispositivos y posibles daños al medio ambiente.	4			80%		80%	F	NO SE CUMPLE
9. Planificar, autorizar y realizar las actividades relacionadas con la finalización de uso, manteniendo los registros apropiados para satisfacer las necesidades regulatorias y cambiantes del negocio.	3		50%			50%	F	NO SE CUMPLE

PRÁCTICA DE GESTIÓN
BAI09.04 Optimizar el coste de los activos.
Revisar periódicamente la base global de activos para identificar maneras de optimizar los costes y mantener el alineamiento con las necesidades del negocio.

			55%				
		NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO	NIVEL DE CAPACIDAD OBJETIVA
ACTIVIDADES	NIVEL DE CAPACIDAD	N	P	L	F	VALOR	META / OBSERVACION
1. Revisar la base general de activos de forma regular, teniendo en cuenta si está alineada con los requerimientos del negocio.	3		50%			50%	F / NO SE CUMPLE
2. Evaluar los costes de mantenimiento, considerar si son razonables e identificar opciones de menor coste, incluyendo, cuando sea necesario, el reemplazo con nuevas alternativas.	4			80%		80%	F / NO SE CUMPLE
3. Revisar las garantías y considerar la relación calidad-precio y estrategias de reemplazo para determinar opciones de menor coste.	4			80%		80%	F / NO SE CUMPLE
4. Revisar la base general para identificar oportunidades de normalización, abastecimiento único y otras estrategias que pueden disminuir los costes de adquisición, soporte y mantenimiento.	3		50%			50%	F / NO SE CUMPLE
5. Usar estadísticas de capacidad y utilización para identificar activos infrautilizados o redundantes que pudieran ser considerados para su eliminación o sustitución por otro con menores costes.	2		20%			20%	F / NO SE CUMPLE
6. Revisar el estado general para identificar las oportunidades para aprovechar tecnologías emergentes o estrategias de aprovisionamiento alternativas para reducir los costes o incrementar el valor del dinero.	3		50%			50%	F / NO SE CUMPLE

PRÁCTICA DE GESTIÓN
BAI09.04 Optimizar el coste de los activos.
Administrar las licencias de software de forma que se mantenga el número óptimo de licencias para soportar los requerimientos de negocio y el número de licencias en propiedad sea suficiente para cubrir el software instalado y en uso.

				55%		NIVEL DE CUMPLIMIENTO	NIVEL DE CAPACIDAD OBJETIVA	
		NIVEL DE CAPACIDAD DE PROCESOS						
ACTIVIDADES	NIVEL DE CAPACIDAD	N	P	L	F	VALOR	META	OBSERVACION
1. Mantener un registro de todas las licencias de software adquiridas y sus acuerdos de licencia asociados.	4			80%		80%	F	NO SE CUMPLE
2. De forma regular, llevar a cabo una auditoría para identificar a todos las copias de software instalado con licencia.	3		50%			50%	F	NO SE CUMPLE
3. Comparar el número de copias de software instalado con el número de licencias en propiedad.	3		50%			50%	F	NO SE CUMPLE
4. Cuando las copias sean inferiores al número en propiedad, decidir si existe una necesidad de mantener o cancelar licencias, considerando el potencial de ahorrar en mantenimiento innecesario, formación y otros gastos.	3		50%			50%	F	NO SE CUMPLE
5 Cuando las copias sean superiores al número en propiedad, considerar primero la posibilidad de desinstalar copias que no sean ya necesarias o no estén justificadas, y después, si es necesario, adquirir licencias adicionales para cumplir con los acuerdos de licencia.	3		50%			50%	F	NO SE CUMPLE
6. De forma regular, considerar si se puede obtenerse un mejor valor mediante la actualización de productos y licencias asociadas.	3		50%			50%	F	NO SE CUMPLE

Fuente: Adaptado de COBIT (2012)
Elaborado por: García (2022)

En la tabla resumen se presenta los porcentajes de los niveles de capacidad de los procesos establecidos que tiene el Departamento de TI del GADMA.

Tabla 19. ***Cuadro resumen COBIT***

DOMINIO	PROCESO	PRÁCTICA CLAVE DE GOBIERNO	N	P	L	F
Evaluar, Orientar y Supervisar (EDM)	**EDM04 Asegurar la Optimización de Recursos**	EDM04.01 Evaluar la gestión de recursos.		50%		
		EDM04.02 Orientar la gestión de recursos.			54%	
		EDM04.03 Supervisar la gestión de recursos.			60%	
Alinear, Planificar y Organizar (APO)	**APO01 Gestionar el Marco de Gestión de TI**	APO01.01 Definir la estructura organizativa.		17%		
	APO12 Gestionar el Riesgo	APO12.01 Recopilar datos.		33%		
		APO12.02 Analizar el riesgo.	10%			
		APO12.03 Mantener un perfil de riesgo.	3%			
		APO12.06 Responder al riesgo.	4%			
Construir, Adquirir e Implementar (BAI)	**BAI09 Gestionar los Activos**	BAI09.03 Gestionar el ciclo de vida de los activos.			76%	
		BAI09.04 Optimizar el coste de los activos.			55%	
		BAI09.05 Administrar Licencias			55%	
Supervisar, Evaluar y Valorar (MEA)	**MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno**	MEA02.01 Supervisar el control interno.		31%		
		MEA02.02 Revisar la efectividad de los controles.	14%			
		MEA02.03 Realizar autoevaluaciones de control.		41%		
		MEA02.04 Identificar y comunicar las deficiencias.		35%		
		MEA02.05 Garantizar que los proveedores.		33%		
		MEA02.06 Planificar iniciativas de aseguramiento.		23%		
		MEA02.07 Estudiar las iniciativas de aseguramiento.		26%		
		MEA02.08 Ejecutar las iniciativas de aseguramiento.		39%		

Fuente: Adaptado de COBIT (2012)
Elaborado por: García (2022)

El Departamento de TI no tiene procesos estandarizados pero tiene procesos informales que son aplicados en las actividades y prácticas de gobierno en la gestión de riesgos y control de la información en relación con la tecnología.

El gráfico Radial consiste en que mientras más alejados estén los procesos del punto de origen son los que más se cumplen en llegar al nivel de capacidad objetiva y mientras más cerca estén del punto de origen menos efectivos son en alcanzar la capacidad deseada.

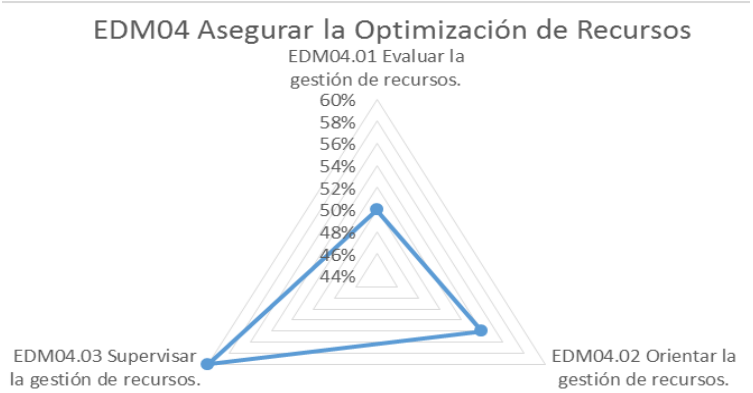
A continuación, se presenta el análisis respectivo de cada proceso definido con gráficos Radiales:

Evaluar, orientar y supervisar (EDM)

EDM 04 Asegurar la optimización de recursos

Los procesos han sido alcanzados en gran manera con un promedio del 55% en un nivel óptimo debido a que existe una relación adecuada entre el personal, los procesos aplicados y la tecnología, además de que las actividades son monitoreadas adecuadamente, las necesidades de recursos del departamento son cubiertos en gran medida y las capacidades de las TI van mejorando de forma continua. Los 3 procesos están siendo alcanzados en gran manera, de los cuales el proceso EDM04.03 es el que más sobresale en base a supervisar la gestión de recursos.

Gráfico 9. ***Radial EDM04***



Fuente: Adaptado de COBIT (2012)
Elaborado por: García (2022)

Alinear, planificar y organizar (APO)

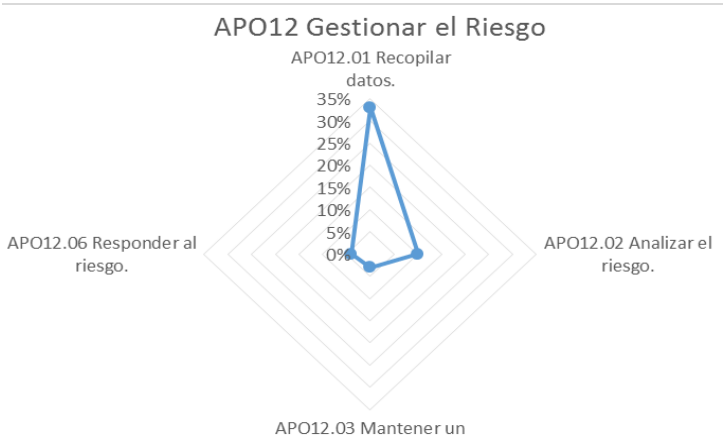
APO01 Gestionar el marco de gestión de TI

Los procesos no se han cumplido o no se han alcanzado con un valor del 17% porque no hay procesos aplicados en la mayoría de las actividades, en cambio hay métodos que tienden a ser aplicados según sea el caso pero no hay una alineación entre la gestión de TI y el gobierno corporativo porque no hay actividades fiables y existe carencia de métodos. Existen procesos del dominio APO01 que no aplica, por lo tanto, existe el proceso APO01.01 en gestionar el marco de TI que no es alcanzado y por lo tanto no es fiable.

APO12 Gestionar el riesgo

Los procesos no se han cumplido o no se han alcanzado con un promedio del 12% porque no hay procesos estandarizados, en cambio hay métodos que tienden a ser aplicados según sea el caso pero no existe una cultura de riesgos relacionadas con las TI y también por la ausencia de la aplicación de marcos de referencia como el ERM y COBIT, dentro del cual la práctica clave de gobierno que más se acerca al cumplimiento del objetivo meta del proceso es APO12.01 referente a recolectar datos, cumpliendo sus actividades de forma parcial.

Gráfico 10 ***Radial APO12***



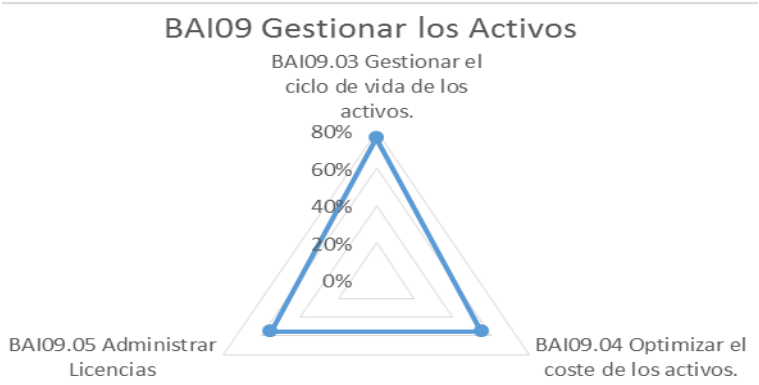
Fuente: Adaptado de COBIT (2012)
Elaborado por: García (2022)

Construir, Adquirir e implementar (BAI)

BAI09 Gestionar los activos

Los procesos del dominio BAI 09 han sido alcanzados en gran manera con un promedio del 62% en un nivel óptimo debido a que los activos de TI son gestionados, protegidos y optimizados en costes con beneficio así que se mantienen y se despliegan eficientemente en relación a las actividades del departamento y cuenta con software de licencia capaces de soportar el proceso institucional.

Gráfico 11. ***Radial BAI09***



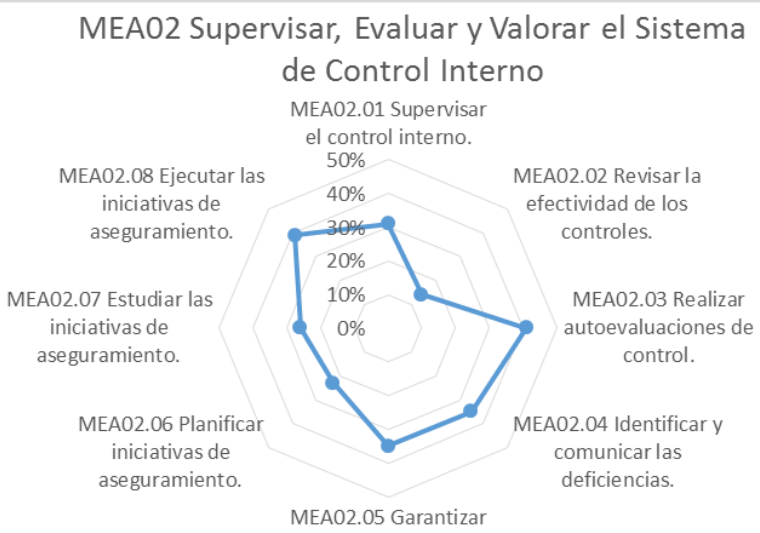
Fuente: Adaptado de COBIT (2012)
Elaborado por: García (2022)

Supervisar, evaluar y valorar (MEA)

MEA02 Supervisar, evaluar y valorar el sistema de control interno

Los procesos fueron parcialmente alcanzados con un promedio de 30% en un nivel regular mostrando que el control interno del departamento tiene deficiencias e ineficiencias en las acciones de mejora pese a que existen políticas y normas establecidas no cuentan con la medición de riesgos de negocio y ni un marco de control de las TI. Así que, el control interno tienes procesos parcialmente alcanzando mostrando solidez en el proceso MEA02.03 que consiste en realizar autoevaluaciones de control.

Gráfico 12. ***Radial MEA02***



Fuente: Adaptado de COBIT (2012)
Elaborado por: García (2022)

Fase III Comunicación

A continuación, se presenta todos los resultados obtenidos con sus respectivos hallazgos en la evaluación de riesgos aplicados los Marcos de Referencias.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO

INFORME GENERAL

AUDITORIA AL SISTEMA DE INFORMACIÓN DEL CENTRO DE PROCESAMIENTO DE DATOS EN EL GAD MUNICPALIDAD DE AMBATO POR EL PERÍODO 2022

SIGLAS Y/O ABREVIATURAS UTILIZADAS

Tabla 20. ***Cuadro resumen COBIT***

Siglas y/o abreviaturas	Significado
COSO ERM	Committee of Sponsoring Organizations of the Tradeway Commission
COBIT	Control Objectives for Information and Related Technologies
TI	Tecnología de Información
EDM	Evaluar, Orientar y Supervisar
APO	Alinear, Planificar y Organizar
BAI	Construir, Adquirir e Implementar
DSS	Entrega, Servicio y Soporte
MEA	Supervisar, Evaluar y Valorar

Fuente: Adaptado de COBIT (2012)
Elaborado por: García (2022)

Ambato, 31 de enero de 2022

Dr. Javier Francisco Altamirano Sánchez

Alcalde Cantonal

Presente. -

De mi consideración:

Hemos efectuado la evaluación de elementos importantes en la auditoría de sistemas al Gobierno Autónomo Descentralizado Municipalidad de Ambato por el período comprendido del año 2022.

El examen se efectúo de acuerdo con los marcos de referencias COSO ERM 2017 y COBIT. Se ha considerado diversos factores informáticos que pueden estar influyendo en las operaciones de la institución, igual que las actividades que se hayan ejecutado de conformidad con las disposiciones legales y reglamentarias vigentes, políticas y demás normas aplicables, a fin de brindar recomendaciones a las posibles soluciones que garanticen un óptimo resultado en cuanto al gobierno y gestión de TI, así como el cumplimiento de controles y procedimientos adecuados.

El objetivo de la Auditoría se enmarca al correcto funcionamiento de Departamento de TI, considerando como alcance la evaluación de áreas vulnerables, el nivel de confianza en cuanto al control interno informático, verificación de los activos de información, respuesta a riesgos relevantes, evaluación de niveles de capacidad a los procesos y los elementos inmersos en la ejecución del SI y herramientas de sistemas tanto física como lógica.

Los resultados se encuentran expresados en los criterios, conclusiones y recomendaciones que constan en el presente informe.

Atentamente

Estudiante Daniel Alexis García Altamirano

RESULTADOS DEL EXAMEN

3.3.1. Marco de referencia COSO ERM 2017

1.1 Estrategias y objetivos

Comentario

El departamento desconoce sobre los marcos de referencias, uno de ellos siendo el COSO ERM 2017 ante los riesgos.

Conclusión

La ausencia de marcos de referencias puede provocar un grado de exposición de que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Adaptar el marco de referencia COSO ERM 2017 para gestionar los riesgos estratégicos y emergentes. Conocer el Marco de referencia COSO ERM 2017 a profundidad, sus componentes y sus principios para relacionarlos y aplicarlos dentro del departamento.

Hallazgo

Comentario

Los objetivos institucionales no están relacionados a la productividad y gestión por la ausencia de métodos de aplicación en el tratamiento de riesgos en de TI.

Conclusión

Existe la desalineación entre estrategia y desempeño, es decir no hay una coordinación entre las metas de la institución con procesos estandarizados que erradiquen y gestionen los riesgos, por lo tanto se incumplen las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Establecer objetivos institucionales de medición de la cultura de riesgo para definir una filosofía de gestión en el proceso de planeación estratégica. Estudiar y profundizar el marco de referencia y las guías de apoyo de forma que se entienda claramente y se aplique las metas de TI objetivos de los procesos.

Hallazgo

Comentario

No existen escalas de medición numérica para la evaluación de riesgos por la ausencia de métodos de aplicación en el tratamiento de riesgos en el Departamento de TI.

Conclusión

La ausencia de herramientas basadas en técnicas y procedimientos para medir, cuantificar e identificar los riesgos puede provocar un grado de exposición de que

una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Diseñar matrices para detectar los riesgos, medirlos y calificarlos acorde a los activos del departamento ya sea de información, recursos, personas y aparatos que existan con la finalidad de conocer y controlar más el departamento. Supervisar los activos de información constantemente para saber y priorizar los que estén expuestos a los posibles riesgos ya sea ambiental, informático o eléctrico.

Hallazgo

Comentario

El jefe responsable del departamento de TI no es conocedor de los planes estratégicos para la toma de decisiones debido a la inobservancia de los planes estratégicos.

Conclusión

Existe la desalineación entre estrategia y desempeño, es decir no hay una coordinación entre las metas de la institución con procesos estandarizados que erradiquen y gestionen los riesgos, por lo tanto se incumplen las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Realizar una lista de todos los planes estratégicos para aplicarlos en la toma de decisiones dentro del departamento. Abordar el plan estratégico del GADMA para alinearlos y complementarlos con la toma de decisiones que se realicen en el departamento para que vayan de la mano con los demás departamentos y así impulsar conjuntamente la institución.

Hallazgo

Comentario

El departamento de TI no cuenta con estrategias suficientes ante la aparición de posibles riesgos por la ausencia de métodos de aplicación en el tratamiento de riesgos.

Conclusión

La ausencia de herramientas basadas en técnicas y procedimientos para medir, cuantificar e identificar los riesgos puede provocar un grado de exposición de que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Adaptar marcos de referencias ya sea COBIT o COSO ERM para gestionar los riesgos que probablemente aparecerán en un futuro y poder mitigarlos sin que dañen los activos de información. Reconocer las actividades institucionales del departamento para aplicar los marcos de referencia contra riesgos que más se afinen con el GADMA.

Hallazgo

Comentario

En el departamento no se han medido el nivel de credibilidad en las estrategias planteadas ante riesgos por la ausencia de métodos de aplicación en el tratamiento de riesgos.

Conclusión

La ausencia de herramientas basadas en técnicas y procedimientos para medir, cuantificar e identificar los riesgos puede provocar un grado de exposición de que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Diseñar matrices para detectar los riesgos, medirlos y calificarlos acorde a los activos del departamento ya sea de información, recursos, personas y aparatos que existan con la finalidad de conocer y controlar más el departamento. Verificar el plan estratégico del GADMA para alinearlos y complementarlos con la toma de decisiones que se realicen en el departamento para que vayan de la mano con los demás departamentos y así impulsar conjuntamente la institución.

Hallazgo

Comentario

No se han añadido nuevos objetivos empresariales en el departamento de TI para prevenir los riesgos debido a que los objetivos institucionales no engloban la productividad y gestión de los departamentos de manera individual.

Conclusión

Existe la desalineación entre estrategia y desempeño, es decir no hay una coordinación entre las metas de la institución con procesos estandarizados que erradiquen y gestionen los riesgos, por lo tanto se incumplen las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Preparar o actualizar nuevos objetivos institucionales de acuerdo a los riesgos que han aparecido en el pasado para definir procesos y controlarlos en su máximo nivel. Fomentar una cultura en riesgos para plantear los objetivos institucionales, es decir el riesgo debe ser gestionado en su totalidad, no sólo debe ser mitigado, aceptado o evitado.

Hallazgo

Comentario

Los objetivos institucionales no están relacionados a la gestión de riesgos debido a que no engloban la productividad y gestión de los departamentos de manera individual.

Conclusión

Existe la desalineación entre estrategia y desempeño, es decir no hay una coordinación entre las metas de la institución con procesos estandarizados que erradiquen y gestionen los riesgos, por lo tanto se incumplen las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Establecer objetivos institucionales de medición de la cultura de riesgo para definir una filosofía de gestión en el proceso de planeación estratégica. Estudiar y profundizar el marco de referencia y las guías de apoyo de forma que se entienda claramente y se aplique las metas de TI objetivos de los procesos.

1.2 Desempeño

Hallazgo

Comentario

No se encuentran debidamente identificados los riesgos en cumplimiento de los controles internos informáticos por la ausencia de métodos de aplicación en el tratamiento de riesgos en el Departamento de TI.

Conclusión

La ausencia de herramientas basadas en técnicas y procedimientos para medir, cuantificar e identificar los riesgos puede provocar un grado de exposición de que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Diseñar matrices para detectar los riesgos, medirlos y calificarlos acorde a los activos del departamento ya sea de información, recursos, personas y aparatos que existan con la finalidad de conocer y controlar más el departamento. Fomentar una cultura en riesgos para plantear los objetivos institucionales, es decir el riesgo debe ser gestionado en su totalidad, no sólo debe ser mitigado, aceptado o evitado.

Hallazgo

Comentario

El departamento no cuenta con un procedimiento para identificar riesgos potenciales en las actividades que desarrollan porque los procedimientos son informales no estandarizados para controlar los riesgos.

Conclusión

La ausencia de herramientas basadas en técnicas y procedimientos para medir, cuantificar e identificar los riesgos puede provocar un grado de exposición de que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Diseñar un manual de procesos que contenga políticas establecidas y definidas de los procesos de la gestión de riesgos para el Departamento de TI. Dominar a fondo las actividades del departamento de TI para anticiparse a los riesgos que puedan perjudicar, retrasar o limitar la operación institucional.

Hallazgo

Comentario

El riesgo de fraude no es evaluado en el departamento de TI por la ausencia de métodos de aplicación en el tratamiento de riesgos en el Departamento de TI.

Conclusión

La ausencia de herramientas basadas en técnicas y procedimientos para medir, cuantificar e identificar los riesgos puede provocar un grado de exposición de que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Utilizar métricas, herramientas y programas para reportar, medir y monitorear el riesgo para detectar las eventualidades con la finalidad de indicar soluciones para poder actuar y resolverlos. Fomentar una cultura en riesgos para plantear los objetivos institucionales, es decir el riesgo debe ser gestionado en su totalidad, no sólo debe ser mitigado, aceptado o evitado.

Hallazgo

Comentario

Para establecer el riesgo potencial y la probabilidad de ocurrencia no existen criterios definidos porque los procedimientos son informales no estandarizados para controlar los riesgos.

Conclusión

La ausencia de herramientas basadas en técnicas y procedimientos para medir, cuantificar e identificar los riesgos puede provocar un grado de exposición de que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Diseñar un manual de procesos que contenga políticas establecidas y definidas de los procesos de la gestión de riesgos para el Departamento de TI. Fomentar una cultura en riesgos para plantear los

objetivos institucionales es decir los riesgos deben gestionarse, no sólo ser mitigados o evitados.

Hallazgo

Comentario

El departamento de TI no ha preparado un plan de riesgos en el que se identifica su probabilidad de ocurrencia e impacto potencial por la ausencia de métodos de aplicación en el tratamiento de riesgos.

Conclusión

La ausencia de herramientas basadas en técnicas y procedimientos para medir, cuantificar e identificar los riesgos puede provocar un grado de exposición de que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Diseñar un manual de procesos que contenga políticas establecidas y definidas de los procesos de la gestión de riesgos para el Departamento de TI. Fomentar una cultura en riesgos para plantear los objetivos institucionales, es decir el riesgo debe ser gestionado en su totalidad, no sólo debe ser mitigado, aceptado o evitado.

1.2.6 Hallazgo

Comentario

Los riesgos no han sido clasificados como tolerantes o que requieran las adopciones de medidas por la ausencia de métodos de aplicación en el tratamiento de riesgos en el Departamento de TI.

Conclusión

La ausencia de herramientas basadas en técnicas y procedimientos para medir, cuantificar e identificar los riesgos puede provocar un grado de exposición de que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Diseñar matrices para detectar los riesgos, medirlos y calificarlos acorde a los activos del departamento ya sea de información, recursos, personas y aparatos que existan con la finalidad de conocer y controlar más el departamento. Fomentar una cultura en riesgos para plantear los objetivos institucionales, es decir el riesgo debe ser gestionado en su totalidad, no sólo debe ser mitigado, aceptado o evitado.

Hallazgo

Comentario

El departamento de TI no toma acciones para identificar factores críticos de riesgos potenciales en las actividades por la ausencia de métodos de aplicación en el tratamiento de riesgos.

Conclusión

La ausencia de herramientas basadas en técnicas y procedimientos para medir, cuantificar e identificar los riesgos puede provocar un grado de exposición de que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Diseñar un manual de procesos que contenga políticas establecidas y definidas de los procesos de la gestión de riesgos para el Departamento de TI. Designar a la persona que está a cargo de la supervisión y control de los activos que realice una constatación física y electrónica periódicamente para evitar los riesgos potenciales de los activos del departamento de TI.

2. Marco de Referencia COBIT

2.1 APO Alinear, planificar y organizar

APO01 Gestionar el marco de gestión de TI

Comentario

No se cumplen las prácticas de gobierno del proceso APO 01 debido a que no se aplica algunas actividades porque no existe una mejora continua de los procesos ni catalizadores de control de TI.

Conclusión

La infraestructura de TI no tiene mejoras continuas en base a roles, funciones y decisiones por lo que no se llega a gestionar las necesidades del departamento por lo tanto esto provoca una desalineación de la organización relativa a TI con los modelos organizativos de arquitectura corporativa, incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

ISO/IEC 15504 Calidad y Gestión

Evaluar, establece y mejora la capacidad o la madurez de los procesos de la empresa.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Establecer un enfoque de gestión para cumplir con las prácticas de gobierno, gestión de riesgo, infraestructura tecnológica, segregación de funciones, actitudes, aptitudes, habilidades y competencias.

APO12 Gestionar el riesgo

Comentario

No se cumplen las prácticas de gobierno del proceso APO 12 debido a que no se aplica algunas actividades porque no existe una gestión en la seguridad de la información.

Conclusión

No se ha delimitado una cultura en riesgos en la identificación y notificación de la información de datos en el departamento de TI todo esto provoca un número de incidentes significativos relacionados con las TI en la evaluación de riesgos, incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

ISO/IEC 15504 Calidad y Gestión

Evaluar, establece y mejora la capacidad o la madurez de los procesos de la empresa.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Incorporar una gestión de riesgos empresariales relacionados con el departamento de TI como el Marco de Referencia COSO ERM.

APO12 Gestionar la seguridad

Comentario

No se cumplen las prácticas de gobierno del proceso APO 13 debido a que no se aplica algunas actividades porque no se aplica el proceso APO13 de la gestión de la seguridad.

Conclusión

La falta de un enfoque formal, estandarizado y continuo en el sistema de gestión de la seguridad de la información provoca la ausencia global de un plan de seguridad de la infoirmación significativos relacionados con las TI en la evaluación de riesgos, incumpliendo las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

ISO/IEC 15504 Calidad y Gestión

Evaluar, establece y mejora la capacidad o la madurez de los procesos de la empresa.

Todo esto provoca un número de incidentes significativos relacionados con las TI en la evaluación de riesgos.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Custodiar el impacto y la probabilidad de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.

2.2 DSS ENTREGA, SERVICIO Y SOPORTE

DSS05 Gestionar Servicios de Seguridad

Comentario

No se cumplen las prácticas de gobierno del proceso DSS05 en su totalidad porque no se aplica el proceso DSS05 de la gestión de servicios de seguridad.

Conclusión

No hay protección sólida en la seguridad de la información provocando incidentes cooperativos relacionados con las TI en la evaluación de riesgos, se incumplen las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

ISO/IEC 15504 Calidad y Gestión

Evaluar, establece y mejora la capacidad o la madurez de los procesos de la empresa.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Minimizar el impacto de las vulnerabilidades e incidentes operativos de seguridad en la información en el departamento de TI.

2.3 MEA Supervisar, Evaluar y Valorar

MEA02 Supervisar, evaluar y valorare el sistema de control interno

Comentario

No se cumplen las prácticas de gobierno del proceso MEA 12 debido a que no se aplica algunas actividades porque no se evalúa de forma continua el control interno.

Conclusión

A l no aplicar un manual de políticas de control interno, más a fondo en gestionar los riesgos provoca deficiencias e ineficiencias en el control del marco corporativo de TI, por lo tanto se incumplen las normas:

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

ISO/IEC 27001 Sistemas de Gestión la Seguridad de la Información

Estándar de requerimientos SGSI que maneja la seguridad y confidencialidad.

ISO/IEC 27002 Proteger los sistemas de información

Mejores prácticas en la gestión de la seguridad de la información en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 31000 Sistemas de Gestión de Riesgos

Las organizaciones deben desarrollar, implantar y mejorar continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

ISO/IEC 15504 Calidad y Gestión

Evaluar, establece y mejora la capacidad o la madurez de los procesos de la empresa.

Recomendaciones

Dirigido al Jefe de Departamento de TI: Mantener la transparencia en las partes interesadas claves respecto a la adecuación del sistema de control interno para generar confianza y un entendimiento adecuado del riesgo en el departamento de TI y el logro de los objetivos del GADMA.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

La Auditoría y sus fases son de gran importancia en la aplicación del proyecto integrador para evaluar el sistema de información del centro de procesamiento de datos en el GADMA porque permitió conocer a fondo el tratamiento de la información del Departamento de TI por medio de la utilización de la tecnología.

En la planificación consta toda la información interna de la institución pública y las bases legales, siendo esta cumplida en su totalidad debido a que los lineamientos van de la mano con los objetivos estratégicos establecidos, permitiendo armar el archivo permanente con la información general esta fase.

El Marco de Referencia COSO ERM 2017 identifica las actividades y procedimientos en base a la gestión de riesgos empresariales, permitiendo evaluar las vulnerabilidades, amenazas y riesgos identificando en el control interno ciertas falencias en los componentes de desempeño, estrategia y objetivos donde el principal problema radica en que no existe una cultura en riesgos, es decir no hay escalas de medición ante posibles riesgos por la falta de aplicación de marcos de referencias.

Las políticas que si cumplieron estando en una medida moderada fueron aquellas que fortalecían al gobierno corporativo como la coordinación, protección y uso adecuado de los activos de información con procesos informales

.

El Marco de Referencia COBIT se aplicó en los objetivos de control de información y tecnología buscando mejores prácticas de gobierno y gestión, sin embargo en el departamento de TI algunos procesos si se cumplieron moderadamente tales como: EDM04, BAI09, APO12 Y MEA02 que se refieren a la gestión del gobierno corporativo TI, Optimización de Recursos y el Control interno, pero existen algunos procesos no aplicados en su totalidad como APO13 Y DSS05 que abordan la gestión la seguridad, reiterando que no hay una cultura en riesgos.

La comunicación de resultados a través del informe de auditoría presenta los hallazgos encontrados con la aplicación de los marcos de referencia para la evaluación de los riesgos determinando 20 hallazgos dentro de los procesos tanto de control interno como gobierno y gestión de las TI lo que le permite a la institución tener una clara visión del estado actual de dichos procesos.

4.2 Recomendaciones

- Continuar con el eficiente cumplimiento de las normas y reglamentos internos que permiten el normal desenvolvimiento de las actividades dentro del GADMA, adicionalmente considerar dentro de su Planificación los posibles riesgos de tecnologías que puedan presentarse para tomar medidas preventivas de control.
- Aplicar marcos de referencia que permitan el manejo adecuado de un marco integral de trabajo orientado a la mejora continua y buenas prácticas en la utilización de tecnologías de la información.
- Realizar un seguimiento y monitoreo del cumplimiento de las recomendaciones a los procesos evaluados en la presente auditoría.

Recomendación hoja de hallazgos	Frecuencia	Responsable	Acciones a realizar	Cumplimiento SÍ/NO	Resultado obtenido
Aplicar el marco de referencia COSO ERM 2017 para gestionar los riesgos estratégicos y emergentes.	Semestral	Jefe del Departamento de TI	Conocer el Marco de referencia COSO ERM 2017 a profundidad, sus componentes y sus principios para relacionarlos y aplicarlos dentro del departamento.	Llenar el responsable	Llenar el responsable
Establecer objetivos institucionales de medición de la cultura de riesgo para definir una filosofía de gestión en el proceso de planeación estratégica.	Anual	Jefe del Departamento de TI	Estudiar y profundizar el marco de referencia y las guías de apoyo de forma que se entienda claramente y se aplique las metas de TI objetivos de los procesos.	Llenar el responsable	Llenar el responsable
Diseñar matrices para detectar los riesgos, medirlos y calificarlos acorde a los activos del departamento ya sea de información, recursos, personas y aparatos que existan con la finalidad de conocer y controlar más el departamento.	Mensual	Jefe del Departamento de TI	Supervisar los activos de información constantemente para saber y priorizar los que estén expuestos a los posibles riesgos ya sea ambiental, informático o eléctrico.	Llenar el responsable	Llenar el responsable
Realizar una lista de todos los planes estratégicos para aplicarlos en la toma de decisiones dentro del departamento.	Anual	Jefe del Departamento de TI	Abordar el plan estratégico del GADMA para alinearlos y complementarlos con la toma de decisiones que se realicen en el	Llenar el responsable	Llenar el responsable

			departamento para que vayan de la mano con los demás departamentos y así impulsar conjuntamente la institución.		
Aplicar marcos de referencias ya sea COBIT o COSO ERM para gestionar los riesgos que probablemente aparecerán en un futuro y poder mitigarlos sin que dañen los activos de información.	Semestral	Jefe del Departamento de TI	Reconocer las actividades institucionales del departamento para aplicar los marcos de referencia contra riesgos que más se afinen con el GADMA.	Llenar el responsable	Llenar el responsable
Diseñar matrices para detectar los riesgos, medirlos y calificarlos acorde a los activos del departamento ya sea de información, recursos, personas y aparatos que existan con la finalidad de conocer y controlar más el departamento.	Semestral	Jefe del Departamento de TI	Verificar el plan estratégico del GADMA para alinearlos y complementarlos con la toma de decisiones que se realicen en el departamento para que vayan de la mano con los demás departamentos y así impulsar conjuntamente la institución.	Llenar el responsable	Llenar el responsable
Preparar o actualizar nuevos objetivos institucionales de acuerdo a los riesgos que han aparecido en el pasado para definir procesos y controlarlos en su máximo nivel.	Anual	Jefe del Departamento de TI	Fomentar una cultura en riesgos para plantear los objetivos institucionales es decir los riesgos deben gestionarse, no sólo ser mitigados o evitados.	Llenar el responsable	Llenar el responsable
Establecer objetivos institucionales de	Anual	Jefe del Departamento de TI	Estudiar y profundizar el marco	Llenar el responsable	Llenar el responsable

medición de la cultura de riesgo para definir una filosofía de gestión en el proceso de planeación estratégica.			de referencia y las guías de apoyo de forma que se entienda claramente y se aplique las metas de TI objetivos de los procesos.		
Diseñar matrices para detectar los riesgos, medirlos y calificarlos acorde a los activos del departamento ya sea de información, recursos, personas y aparatos que existan con la finalidad de conocer y controlar más el departamento.	Semestral	Jefe del Departamento de TI	Fomentar una cultura en riesgos para plantear los objetivos institucionales es decir los riesgos deben gestionarse, no sólo ser mitigados o evitados.	Llenar el responsable	Llenar el responsable
Diseñar un manual de procesos que contenga políticas establecidas y definidas de los procesos de la gestión de riesgos para el Departamento de TI.	Trimestral	Jefe del Departamento de TI	Dominar a fondo las actividades del departamento de TI para anticiparse a los riesgos que puedan perjudicar, retrasar o limitar la operación institucional.	Llenar el responsable	Llenar el responsable
Utilizar métricas, herramientas y programas para reportar, medir y monitorear el riesgo para detectar las eventualidades con la finalidad de indicar soluciones para poder actuar y resolverlos.	Mensual	Jefe del Departamento de TI	Fomentar una cultura en riesgos para plantear los objetivos institucionales es decir los riesgos deben gestionarse, no sólo ser mitigados o evitados.	Llenar el responsable	Llenar el responsable

Diseñar un manual de procesos que contenga políticas establecidas y definidas de los procesos de la gestión de riesgos para el Departamento de TI.	Trimestral	Jefe del Departamento de TI	Designar a la persona que está a cargo de la supervisión y control de los activos que realice una constatación física y electrónica periódicamente para evitar los riesgos potenciales de los activos del departamento de TI.	Llenar el responsable	Llenar el responsable
Establecer un enfoque de gestión para cumplir con las prácticas de gobierno, gestión de riesgo, infraestructura tecnológica, segregación de funciones, actitudes, aptitudes, habilidades y competencias.	Cuatrimestral	Jefe del Departamento de TI	Designar en el control interno del Departamento de TI las responsabilidades a cargo de supervisar y controlar que los procesos se cumplan acorde al manual.	Llenar el responsable	Llenar el responsable
Incorporar una gestión de riesgos empresariales relacionados con el departamento de TI como el Marco de Referencia COSO ERM.	Semestral	Jefe del Departamento de TI	Elaborar un plan de acciones correctivas según las eventualidades que se vayan presentando.	Llenar el responsable	Llenar el responsable
Custodiar el impacto y la probabilidad de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.	Mensual	Jefe del Departamento de TI	Considerar riesgos para el posicionamiento estratégico, ejecución estratégica y la gestión de riesgos emergentes.	Llenar el responsable	Llenar el responsable
Minimizar el impacto de las vulnerabilidades e incidentes operativos de seguridad en la	Mensual	Jefe del Departamento de TI	Integrar la gestión de riesgos en la toma de decisiones del departamento en función del	Llenar el responsable	Llenar el responsable

información en el departamento de TI.			gobierno y cultura del GADMA.		
Mantener la transparencia en las partes interesadas claves respecto a la adecuación del sistema de control interno para generar confianza y un entendimiento adecuado del riesgo en el departamento de TI y el logro de los objetivos del GADMA.	Semanal	Jefe del Departamento de TI	Incluir la gestión de riesgos empresariales que requiera un proceso continuo para obtener y compartir información necesaria.	Llenar el responsable	Llenar el responsable

REFERENCIAS BIBLIOGRÁFICAS

Alvarez, L. (2005). Seguridad informática. *(Tesis de Licenciatura).* Universidad Iberoamérica, Pueblo.

Arcentales, D., & Caycedo, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las ciencias, 3*, 157-173.

Arcentales, D., & Caycedo, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las ciencias, 3*, 157-173. doi:http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.157-173

Bailon, W. (2019). Auditoría informática al control y mantenimiento de una infraestructura tecnológica. *Cienciamatria, 5*(1), 73-87. Obtenido de https://creativecommons.org/licenses/by-nc-sa/4.0/

Bertalanffy, L. (1976). Teoría general de los sustemas. *Fondo de Cultura Económica*, 1-9.

Blanco, L. (2008). *Auditoría y sistemas de información.* La habana: Félix Varela.

Chicano, E. (2014). *Auditoría de la seguridad informática.* Andalucía: IC editorial.

Chuquimarca, M. (2020). El futuro de la auditoría y las innovaciones tecnológicas. *Dominio de las ciencias, 6*(1), 316-339. doi:http://dx.doi.org/10.23857/dc.v6i1.1149

Dávalos, Á. (2008). Auditoria de seguridad de información. *Fides er ratio*, 19-30.

Davies, P. (2014). *Sistemas de información: introducción a la informática en las organizaciones.* Barcelona: Reverté.

Del Peso, N. (1994). Prevención versus fraude: la auditoría. *Dialnet*, 466-471.

Deloitte. (2017). *COSO ERM 2017 y la generación de valor.* Recuperado el 12 de Mayo de 2022, de COSO ERM 2017 y la generación de valor:

https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Presentaci%C3%B3n%20COSO%20ERM%202017%20(Oct%2024).pdf

Díaz, G. (2020). La Auditoría a los sistemas de información como aporte a la actividad gerencial. *Dialnet, 5*(3), 236-268.

Escrivá, G., Romero, R., Ramada, J., & Onrubia, R. (2013). *Seguridad informática.* Macmillan.

GAD Municipalidad de ambato. (2022). *GAD Municipalidad de Ambato*. Recuperado el 23 de 04 de 2022, de GAD Municipalidad de Ambato: https://ambato.gob.ec/

ISACA. (2012). *COBIT.* E.E.U.U: ISACA.

Marco, M. (2012). *Escaneando la informática.* Barcelona: UOC.

Negrín, E. (2017). Propuesta a un programa de auditoría a los sistemas de información. *Dialnet, 8*(2), 131-143.

Plattini, M., del Peso, E., & del Peso, M. (2015). *Auditoría de tecnologías y sistemas de información.* Madrid: Ra-Ma.

Ramos, M. (2015). La Auditoría Informática. *Dialnet*, 983-991.

Sabillón, R., & Cano, J. (2019). Auditorías en ciberseguridad: un modelo de aplicación general para empresas y naciones. *risti*(32), 33-48. doi:DOI: 10.17013/risti.32.33–48

Solano, Ó. (2004). La auditoría de sistemas de información como elemento de control. *Dialnet, 31,* 123-167.

Soy i Aumatell, C. (2013). *Auditoría de la información.* Barcelona: UOC.

Villalobos, J. (2008). Auditanto en las bases de datos. *Uniciencia,* 135-140.

ANEXOS

Gráfico 13. ***RUC***

SRi

Certificado
Registro Único de Contribuyentes

Razón Social
GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO

Número RUC
1860000210001

Representante legal
- ALTAMIRANO SANCHEZ JAVIER FRANCISCO

Estado	Régimen	
ACTIVO	REGIMEN GENERAL	
Fecha de registro	**Fecha de actualización**	**Inicio de actividades**
08/02/1922	28/10/2021	20/09/1756
Fecha de constitución	**Reinicio de actividades**	**Cese de actividades**
20/09/1756	No registra	No registra
Jurisdicción		**Obligado a llevar contabilidad**
ZONA 3 / TUNGURAHUA / AMBATO		SI
Tipo	**Agente de retención**	**Contribuyente especial**
SOCIEDADES	SI	SI

Domicilio tributario

Ubicación geográfica

Provincia: TUNGURAHUA **Cantón:** AMBATO **Parroquia:** HUACHI CHICO

Dirección

Calle: AV. ATAHUALPA **Número:** S/N **Intersección:** RIO CUTUCHI **Referencia:** A UNA CUADRA DEL MALL DE LOS ANDES

Medios de contacto

Teléfono trabajo: 032997800 **Email:** salcaldia@ambato.gob.ec **Celular:** 0984254123

Actividades económicas

- O84110101 - DESEMPEÑO DE LAS FUNCIONES EJECUTIVAS Y LEGISLATIVAS DE LOS ÓRGANOS Y ORGANISMOS CENTRALES, REGIONALES Y LOCALES.
- L68200202 - ACTIVIDADES DE ALQUILER DE BIENES INMUEBLES A CAMBIO DE UNA RETRIBUCIÓN O POR CONTRATO (LOCALES COMERCIALES).
- Q87200101 - SERVICIOS DE ATENCIÓN EN INSTALACIONES PARA EL TRATAMIENTO DEL ALCOHOLISMO Y LA DROGODEPENDENCIA.
- A01620901 - ACTIVIDADES DE ALBERGUE Y CUIDADES DE ANIMALES DE GRANJA
- O84122005 - CONSERVACION Y CUSTODIA DE REGISTROS Y ARCHIVOS PUBLICOS DE LA PROPIEDAD.
- L68100404 - VENTA DE LOTES DE CEMENTERIOS.
- R93290101 - ACTIVIDADES DE PARQUES RECREATIVOS Y PLAYAS, INCLUIDO EL ALQUILER DE CASETAS, CASILLEROS, SILLAS, HAMACAS; LA GESTIÓN DE INSTALACIONES DE TRANSPORTE RECREATIVO; POR EJEMPLO, PUERTOS DEPORTIVOS, Y EL ALQUILER DE EQUIPO DE ESPARCIMIENTO Y RECREO COMO PARTE INTEGRAL DE LOS SERVICIOS DE ESPARCIMIENTO, BANANAS, LANCHAS, ETCÉTERA.

1/2

www.sri.gob.ec

Fuente: GAD Municipalidad de Ambato (2022)
Elaborado por: García (2022)