UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE INGENIERÍA EN INFORMÁTICA

Tema: "Plan de mitigación de riesgos tecnológicos basado en auditoría informática a la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán"

Trabajo de titulación previa la obtención del título de Ingeniera en Informática

AUTORA: Pantoja Miño Yuly Estefania

TUTOR: Guano Cárdenas Carlitos Alberto, MSc.

Tulcán, 2020

CERTIFICADO JURADO EXAMINADOR

Certificamos que la estudiante Pantoja Miño Yuly Estefanía con el número de cédula 0401916713 ha elaborado el trabajo de titulación: "Plan de mitigación de riesgos tecnológicos basado en auditoría informática a la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán"

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de Titulación, Sustentación e Incorporación de la UPEC, por lo tanto, autorizamos la presentación de la sustentación para la calificación respectiva.

f.....

Guano Cárdenas Carlitos Alberto, MSc.

TUTOR

f.....

Arcos Ponce Georgina Guadalupe, MSc

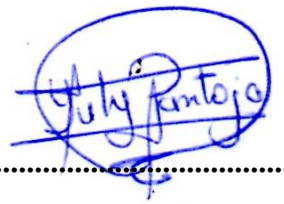
LECTORA

Tulcán, febrero de 2020

AUTORÍA DE TRABAJO

El presente trabajo de titulación constituye requisito previo para la obtención del título de **Ingeniera** en la Carrera de Ingeniería en Informática de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Yo, Pantoja Miño Yuly Estefania con cédula de identidad número 0401916713 declaro: que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.



f.....

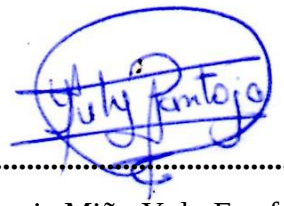
Pantoja Miño Yuly Estefanía

AUTORA

Tulcán, febrero de 2020

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

Yo, Pantoja Miño Yuly Estefania declaro ser autor/a de los criterios emitidos en el trabajo de investigación: "Plan de mitigación de riesgos tecnológicos basado en auditoría informática a la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán" y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.



f.....

Pantoja Miño Yuly Estefania

AUTORA

Tulcán, febrero de 2020

AGRADECIMIENTO

A la Universidad Politécnica Estatal del Carchi, por ser el pilar fundamental de la formación académica de la juventud ecuatoriana.

A la Carrera de Ingeniería en Informática, por guiar a los estudiantes en el proceso de formación profesional. A sus docentes que comparten diariamente los conocimientos, con paciencia y acompañamiento constante.

A la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán, de manera especial al Ing. Alejandro Obando, MSc. Jackson Obando e Ing Andrea Chávez, servidores públicos de la empresa, por su apertura y colaboración en la realización del presente proyecto de titulación.

Agradecimiento total al MSc. Carlitos Guano, tutor del proyecto, y a la MSc. Georgina Arcos, lectora del trabajo, por el apoyo constante y la orientación adecuada para el cumplimiento de esta meta.

DEDICATORIA

A Dios dueño de todo lo creado, por brindarme las fuerzas necesarias en cada paso de mi vida.

A mis padres Iván y Teresa por el apoyo incondicional, por ser las personas que han forjado mi disciplina a base de amor y esfuerzo constante, motivo suficiente para continuar y no desfallecer.

A mis hermanos Jefferson y Maricela fuente de inspiración y alegría, los mejores amigos que forman parte de los momentos más maravillosos de mi existencia.

A mis compañeros, Andrés A, Oscar, Steven, Jonathan C, Dixon, Patricio, Johana, Reynaldo, Javier, Michael, Francisco, Jonathan R, Andrés T, Adair, Ricardo y Cristian que han compartido cinco años de experiencias y amistad, por convertirse en mi segunda familia.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto evaluó la situación de los procesos tecnológicos que se llevan a cabo en la a la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán (EPMAPA-T), mediante la aplicación de una auditoría informática basada en la metodología de Objetivos de Control para Tecnologías de la Información y Tecnologías relacionadas 5 (COBIT® 5) hacia el Departamento de Supervisión Informática (DSI). Las fases de auditoría realizadas fueron: planeación, ejecución y dictamen. El objetivo de la investigación fue emitir un plan de mitigación de riesgos tecnológicos tomando como base los hallazgos de auditoría. Para lograr el objetivo se tomó en cuenta una metodología con enfoque cuali – cuantitativa, que permitió el análisis de la documentación legal y constitutiva de la empresa, la verificación de cumplimiento de requisitos COBIT® 5 y la fundamentación teórica en la metodología. Adicional a ello se obtuvo información mediante la aplicación de entrevistas a los actores de auditoría y una encuesta hacia los servidores públicos y lectores en un total de 46 informantes, con fines de conocer la gestión del área actualmente. Se elaboró fichas de proceso que permitió documentar los procesos institucionales y del área de tecnología. Finalmente, se emitió un documento de resultados de auditoría, con el nivel de cumplimiento actual de los procesos de tecnología correspondiente a 1 de 5 que indica que el proceso se encuentra ejecutado con base a los requerimientos COBIT® 5. Posteriormente, la matriz de riesgos por procesos fue elaborada y con base en ella se emitió estrategias y documentación a desarrollar para llevar el cumplimiento hacia los niveles aceptables iguales o superiores a 3 que indica que los procesos se encuentran establecidos, predecibles y optimizados. El presente estudio constituye una propuesta dirigida hacia el área de tecnología que al ponerla en práctica permitirá cumplir los procesos de manera óptima y con bajos niveles de riesgo.

Palabras clave: Auditoría informática, mitigación de riesgos tecnológicos, metodología COBIT® 5, tecnología de información (TI)

ABSTRACT

This project evaluated the state of technological processes which are carried out at Municipal Public Company Drinking Water and Sewerage in Tulcán (EPMAPAT), by implementing a computer audit based on the Control Objectives for Information Technologies and Related Technologies methodology (COBIT® 5) to Computer Oversight Department (DSI). The audit phases carried out were: planning, execution and opinion. The objective of the investigation was to issue a mitigating plan technological risks based on the audit findings. To achieve the objective, qualitative-quantitative approach was taken into account, this allowed the analysis of the legal and constituent documentation of the company, COBIT® 5 compliance verification and theoretical rationale on the methodology. In addition, information was obtained through interviews with audit actors and a survey to public servants and readers in a total of 46 informants, to know about the area management currently. Process sheets were developed to document the institutional and IT processes. Finally, an audit results document was issued, detailing the current level of compliance with technology processes, corresponding to 1 out of 5 indicating that the process is running based on COBIT® 5 requirements. Subsequently, the process risk matrix was developed and based on the matrix, strategies and documentation were issued to be developed to bring compliance to acceptable levels equal to or greater than 3 indicating that processes are set, predictable and optimized. This study is a proposal aimed at the area of technology, that by implementing it will allow to meet the processes optimally and with low levels of risk.

Keywords: Computer audit, mitigating technological risks, COBIT® 5 methodology. information technology (IT)

INTRODUCCIÓN

La Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán, objeto de estudio es una institución pública que brinda servicios relacionados a la distribución de agua potable y administración del alcantarillado de la ciudad, inició sus labores en el año 2005 y está ubicada en las Av. Juan Ramón Arellano y Bolívar en la ciudad de Tulcán.

Dentro de la estructura orgánica funcional de la EPMAPA-T cuenta con el Departamento de Supervisión Informática con tareas referentes a la gestión y administración tecnológica, cuya finalidad principal del área es contribuir con tecnología al cumplimiento de los procesos institucionales. Sin embargo, este no es suficiente comparado con el crecimiento de información que necesita ser asegurada y por lo tanto es necesario una intervención de los procesos en los cuáles se encuentra involucrada.

El presente proyecto tuvo como finalidad la generación de un plan de mitigación de riesgos tecnológicos, mediante los hallazgos de auditoría informática basada en la metodología COBIT® 5, que pretende mitigar o por lo menos reducir el impacto de los riesgos tecnológicos que puedan ocasionar en los procesos institucionales, por lo que primera instancia se indagó acerca de la metodología y de esta manera se desarrolló la planificación de auditoría. La etapa de ejecución constituyó uno de los objetivos estratégicos con fines de evaluación, los resultados fueron expuestos en un informe y tomados como base para la etapa de dictamen que fue complementada con la determinación de riesgos en la matriz, estableciendo de esta manera la probabilidad de ocurrencia y el impacto negativo para las situaciones identificadas, por último, se emitió las estrategias de mitigación para cada riesgo.

Al adoptar la propuesta de mitigación de riesgos, se pretende reducir el impacto negativo generado por los conflictos de TI en la institución, de esta manera constituye un apoyo para el logro de los objetivos planteados por TI y contribuye a la toma de decisiones.

El informe investigativo fue desarrollado en cinco capítulos que se describen a continuación.

El capítulo uno expone la problemática de estudio, justificación de la investigación, objetivos establecidos y preguntas de investigación. El capítulo dos trata acerca de la fundamentación teórica, donde se describen antecedentes de investigaciones similares, por su parte en la sección de marco teórico se define terminología exclusiva de la presente investigación, tales como: auditoría, riesgos tecnológicos y metodología COBIT. El tercer capítulo describe el enfoque

metodológico utilizado, los tipos de investigación en las cuáles se fundamentó, idea a defender, operacionalización de variables de estudio y métodos necesarios para la recolección de información. El capítulo cuatro describe los resultados de la investigación y la discusión, para ello se da a conocer datos informativos de la empresa, el proceso de auditoría informática en todas sus fases, informe de resultados y el plan de mitigación de riesgos tecnológicos. El capítulo quinto expone las conclusiones y recomendaciones a las que se ha llegado en la finalización del proyecto. Los capítulos sexto y séptimo describen las referencias bibliográficas y anexos respectivamente.

I. PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, la tecnología e información constituyen el pilar fundamental de la sociedad, la misma crece a pasos agigantados, y con ello crece la necesidad de prevenir los riesgos informáticos que se pueden ocasionar sin previo aviso.

Según el informe denominado "Incidentes de Ciberseguridad Industrial en Servicios Esenciales en España" y que fue desarrollado por el Centro de Ciberseguridad Industrial y Check Point (2019) menciona que:

> Durante 2018, se han registrado más de 33.000 incidentes de ciberseguridad en entidades del sector público y empresas de interés estratégico para España, una cuarta parte más que el año anterior, según el Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia (CNI). De dichos ataques, alrededor de 1.600 han sido calificados de peligrosidad muy alta. (p.7)

Es decir, se conoce que los ataques en empresas españolas se incrementaron en un 25% durante el 2018 en relación al año 2017, de esta manera es posible deducir que dichas empresas no cuentan con estudios que permitan asegurar la integridad institucional ante siniestros de ciberseguridad.

De esta manera nace la necesidad de identificar ataques complejos, donde las organizaciones deben analizar la coincidencia de patrones para lograr un verdadero análisis y modelo basados en riesgos. Con la integración de estándares que regulen el cumplimiento de los procesos informáticos, y garanticen una correcta administración de tecnologías de información acorde a los requerimientos de la empresa, y por ende brindar servicios de calidad a la sociedad.

En el Ecuador las organizaciones crecen aceleradamente, y demandan controles más eficientes y que vayan de acuerdo con el grupo de trabajo y al giro del negocio. El diario el Telégrafo en Redacción Justicia (2016) "…indica que el 85% de los ataques a los sistemas informáticos son causados por errores de los consumidores, quienes no toman precauciones al acceder a las redes sociales, utilizar el correo electrónico, y en el uso de usuario y contraseña.", es decir en el país aún no se pone en práctica una cultura de seguridad y se refleja, ya sea en pérdidas económicas o el daño a la integridad y confiabilidad de la información de las organizaciones. Por lo tanto, la preocupación principal de las entidades públicas es protegerse ante cualquier situación en la

cual se vea amenazada, es por ello que las instituciones ven en la auditoria informática, la oportunidad de mejorar y crecer como empresa, aplicando una evaluación a los distintos recursos tecnológicos que posea la organización, así como también al personal que interactúe en los procesos.

Al garantizar una efectiva administración de riesgos y realizar un control minucioso para prevenir, detectar y corregir los errores potenciales que se llevan a cabo en los procesos en los que interviene la información, se define la importancia de monitorear de manera continua las operaciones soportadas por las tecnologías de información, con lo cual la auditoría informática puede proporcionar las herramientas necesarias para lograr los objetivos de la organización e idear un plan que beneficie a la misma.

La Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán, es una empresa pública de servicio a la comunidad, que administra y controla la distribución del líquido vital en la ciudad de Tulcán, misma que dispone de un crecimiento de información debido a la cantidad de usuarios que se encuentran registrados, sumado a la generación de reportes mensuales de consumo de agua potable, por lo que la información se encuentra en situación de riesgo inherente.

La principal problemática radica en que la EPMAPA-T cuenta con insuficientes mecanismos para protegerse ante riesgos tecnológicos, debido a que en los procedimientos internos de la empresa no se estipula una normativa de control interno informático, cumpliendo parcialmente con los requerimientos de manera empírica, sumado a una inadecuada evaluación de procesos dentro de la organización.

La Norma de Control Interno de la Contraloría General del Estado Ecuatoriano (2014) menciona que:

> Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional. (p.68)

Al analizar el punto 410-01 de Organización Informática de la Norma de Control Interno, surge una inquietud; debido a que por un lado existen altas exigencias para asegurar la transparencia y control en los procesos de tecnología de información y por otro la EPMAPA-T cuenta con una inadecuada evaluación de dichos procesos.

1.2. FORMULACIÓN DEL PROBLEMA

La falta de una normativa interna regulatoria sumado a los insuficientes mecanismos de protección como el plan de mitigación de riesgos tecnológicos en los procedimientos internos, genera el cumplimiento parcial empírico de los requerimientos de control interno informático de la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán.

1.3. JUSTIFICACIÓN

La investigación se ajusta al perfil de egreso del Ingeniero Informático de la Universidad Politécnica Estatal del Carchi (UPEC) que en el inciso 1.2 de las políticas y lineamientos pertinentes al sector de las TIC menciona el siguiente enunciado: "Mejorar continuamente los procesos, la gestión estratégica y la aplicación de tecnologías de información y comunicación, para optimizar los servicios prestados", el mismo que se logra con un plan de mitigación de riesgos tecnológicos, cabe recalcar que existe suficiente sustentación teórica y práctica desarrollada por diferentes autores, y los recursos tecnológicos necesarios para llevar a buen término el resultado de esta investigación.

Con la aplicación de una auditoría informática se buscó evaluar el estado de los procesos y buen uso del equipo tecnológico de la EPMAPA-T, con la finalidad de prevenir, aceptar, mitigar y transferir los riesgos que se pueden ocasionar, detectando falencias que permitan tomar medidas correctivas.

Los beneficiarios directos son los miembros de la EPMAPA-T, debido a que los directivos de la empresa podrán tomar decisiones a partir de los resultados de la auditoría informática, y de esta manera cumplir los objetivos institucionales. Los beneficiarios indirectos son los usuarios de la ciudad de Tulcán, quienes hacen uso de los servicios que la empresa brinda mensualmente en los procesos de recolección de lecturas y facturación de las planillas de consumo del agua potable.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General.

Elaborar un plan de mitigación de riesgos tecnológicos basado en una auditoría informática a la EPMAPA-T, reduciendo los riesgos tecnológicos en los procedimientos internos implementando medidas de control para estos.

1.4.2. Objetivos Específicos

1. Recopilar información bibliográfica en medios virtuales y físicos que sustente teóricamente la investigación.

2. Diagnosticar los procesos tecnológicos de la EPMAPA-T, mediante la metodología COBIT® 5, efectuando la planeación de la auditoría informática.

3. Aplicar la auditoria informática, bajo la metodología COBIT® 5 al Departamento de Supervisión Informática, determinando los riesgos tecnológicos que se enfrenta la institución

4. Generar una matriz de riesgos tecnológicos basado en los hallazgos de auditoría informática, priorizando los puntos críticos que afectan a los procesos tecnológicos que se llevan a cabo en la EPMAPA-T.

1.4.3. Preguntas de Investigación

- ¿La recopilación de información bibliográfica en medios virtuales y físicos es de gran aporte para una mejor sustentación teórica de la investigación?

- ¿El diagnóstico de procesos tecnológicos de la EPMAPA-T, mediante la metodología COBIT® 5 permite tener información disponible para una adecuada planeación de auditoría informática?

- ¿La aplicación de la metodología COBIT® 5 en la auditoría informática del Departamento de Supervisión Informática, permite tomar decisiones para prevenir riesgos tecnológicos institucionales?

- ¿La generación de una matriz de riesgos tecnológicos, le permite a la institución anticiparse ante eventuales problemas, en puntos críticos que afectan a los procesos tecnológicos la EPMAPA-T?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES INVESTIGATIVOS

Tomando en cuenta investigaciones realizadas por otros autores, se recopila la siguiente información. Ulloa (2017) con su investigación denominada "Auditoría informática aplicando la metodología COBIT en el Gobierno Autónomo Descentralizado Municipal de San Cristóbal de Patate", donde uno de los objetivos específicos, fue "Analizar de la planeación, organización y situación actual del GAD de Patate, enfocándose en estrategias e infraestructura tecnológica de información." (p.4), indica que se obtuvieron los siguientes resultados "…la información importante manejada diariamente en los procesos en el GAD Municipal de Patate, es entregada de forma oportuna, veras y consistente en un 32,4%, teniendo un 67,6% de ineficiencia en el proceso." (p.89), de esta manera se logra evidenciar que la entidad auditada, aún no cuenta con medidas de protección ante riesgos en contra de la seguridad de la información.

De la misma manera Samillan y Castillo (2017) con la investigación denominada "Auditoría Informática usando las normas COBIT en el centro de sistemas de información del Hospital Regional Docente Las Mercedes de Chiclayo-2016", en la cual se describe el siguiente objetivo específico "Describir la situación actual del área del Centro de Sistemas de Información del Hospital Regional Docente Las Mercedes de Chiclayo, respecto a los procesos de Tecnologías de Información que se ejecutan en esta área."(p.24), se obtuvieron los siguientes resultados:

> Aplicando encuestas, entrevistas y checklist, se pudo determinar cuál es la situación problemática del Hospital Regional Docente Las Mercedes de Chiclayo, encontrándose como principales problemas el no mantener la dotación de personal suficiente en el área, así mismo no existe un proceso que permita mantener las habilidades y competencias del personal TI. Además de que no se tienen definidos esquemas de clasificación de incidentes y peticiones de servicio, los cuales permitan priorizarlos de manera que se les dé una eficaz y eficiente resolución. Tampoco se analiza, ni se informa sobre el rendimiento del área de CSI a la Gerencia de manera constante. Por otro lado, no se planifican ni estudian iniciativas de aseguramiento que permitan diagnosticar el riesgo e identificar los procesos críticos de TI. (p.151)

Es decir, la entidad auditada no cuenta con medidas que permitan la gestión de riesgos de TI implementadas en el Centro de Sistemas de Información.

Por último, se tiene la investigación de Molina (2015) cuyo tema fue "Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral", donde menciona que uno de los objetivos específicos fue "Identificar las principales amenazas que afectan a los activos anteriormente considerados, pudiendo afectar la integridad, disponibilidad y confiabilidad de la información que estos almacenan o transfieren" (p.4), el informe consta de una evaluación de los activos, la identificación de amenazas y finalmente las salvaguardas para cada uno de los riesgos. Se evidencia que uno de los activos más importantes es el servidor, de este equipo informático depende el software, los sistemas informáticos, el almacenamiento de datos y la virtualización, tal como indica el diagrama de dependencia de activos. La valoración del activo servidor es la siguiente:

Tabla 1. Valoración de amenazas por activos

Activos	Amenaza	Degradación	Frecuencia	Riesgo
Servidor	Incendio	MA	MB	Medio
	Terremoto	MA	MB	Medio
	Robo	A	B	Medio
	Acceso no autorizado	A	M	Alto
	Falla de generador eléctrico	A	B	Medio

Fuente: Molina (2015) *Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral*.

La información descrita anteriormente, forma parte de la tabla de valoración de amenazas por activo, en este caso se ha considerado solamente el activo servidor, debido a su importancia para el cumplimiento de los procesos en la Escuela Superior Politécnica del Litoral.

2.2. MARCO TEÓRICO

2.2.1 Auditoría.

La Asociación de Auditoría y Control de Sistemas de Información (ISACA®, 2015) menciona que auditoría es la "Inspección formal y verificación para comprobar si se está siguiendo un estándar o un conjunto de directrices, registros precisos, eficiencia o eficacia y si los objetivos se están cumpliendo." (p.6)

Por su parte Yubero (como se citó en Ulloa, 2017) menciona que auditoría es un: "Proceso de revisión, por un profesional suficientemente cualificado, determinado procedimiento, actividad, informe, proceso, entre otros, con intención de obtener un alto grado de garantía de la correcta elaboración o desarrollo de los mismos." (p.7), es decir, independientemente del tipo de auditoría, todas buscan el análisis con base en evaluación que permite detectar puntos críticos que se deben corregir.

2.2.2. Auditoría Informática

La auditoría informática es un proceso de evaluación, donde la tarea principal es identificar hallazgos y de esta manera establecer oportunidades de mejora en los procesos institucionales que se realizan. Encalada y Cordero (2016) manifiestan que su ayuda radica en: "la revisión y la evaluación de los controles y procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información." (p.114), por medio de la evaluación se logra información más eficiente y segura, que servirá para una correcta toma de decisiones.

De Pablos et al. (como se citó en Arcentales y Caycedo, 2017) señala que:

> Auditoría informática es la revisión, verificación y evaluación con un conjunto de métodos, técnicas y herramientas de los sistemas de información de una organización, de forma continua y a petición de su Dirección y con el fin de mejorar su rentabilidad, seguridad y eficacia. (p.162).

Por lo expuesto, se conoce que la finalidad de una auditoría informática es establecer procesos de mejora relacionado a rentabilidad, seguridad y eficacia en los procesos tecnológicos que se realizan en las empresas.

2.2.2.1 Auditoría informática de explotación.

El proceso de auditoría se fundamentó principalmente en la auditoria informática de explotación, Chicano (2014) señala que:

> La auditoría informática de explotación se encarga de analizar resultados informáticos de todo tipo: listados impresos, ordenes automatizadas de procesos, etc. El análisis consistirá sobre todo en someter los resultados obtenidos a controles de calidad y en analizar si su distribución posterior (al cliente, a otros empleados, a superiores, etc.) se realiza mediante un proceso adecuado.

En este caso, se realizó un análisis de los procesos tecnológicos que se llevan a cabo en la EPMAPAT, que permitió recolectar información de todo tipo relacionado al cumplimiento de los requerimientos COBIT® 5.

2.2.3 Riesgos Tecnológicos

ISACA® (2015) señala que el riesgo de TI es:" El riesgo comercial asociado con el uso, propiedad, operación, participación, influencia y adopción de TI de una empresa." (p.39)

De igual manera, Castillo (2016) menciona que los riesgos tecnológicos son: "La contingencia de que la interrupción, alteración, o falla de la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, provoque pérdidas financieras a la institución." (p.4)

2.2.3.1. Gestión de Riesgos Tecnológicos

El término ha sido definido en la publicación denominada "COBIT® 5 para la seguridad de la información" por ISACA® (2012) de la siguiente manera:

> Uno de los objetivos de gobierno. Requiere reconocer un riesgo; evaluar su impacto y probabilidad; y desarrollar estrategias, como, por ejemplo, evitar el riesgo, reduciendo el efecto negativo de riesgo y/o transfiriendo el riesgo, para gestionarlo en el contexto del apetito de riesgo de una empresa. (p.218)

Las decisiones que se toman en las organizaciones conllevan un riesgo inherente o asociado. El riesgo de dic2has decisiones se debe identificar, valorar y aprender a controlarlo. La superintendencia de Bancos de Guatemala en el Programa de Capacitación sobre Gestión de Riesgos con enfoque en seguros, presenta la siguiente figura que indica el proceso a llevar a cabo para una adecuada gestión de riesgos.

Figura 1. Gestión de Riesgos

Fuente: Superintendencia de Bancos de Guatemala (2017) *Gestión de riesgos con enfoque en seguros.*

Para el presente trabajo de investigación se eligió el tipo de gestión que se denomina mitigación, el mismo que de acuerdo con el análisis de riesgos, indica que se debe mitigar los riesgos con mayor nivel de prioridad.

2.2.4. Plan de mitigación de riesgos tecnológicos.

2.2.4.1. Definición

Benavides (2017) menciona que:

> Se denomina Plan de Mitigación a las estrategias definidas por la empresa que tratan de reducir la probabilidad de ocurrencia del riesgo o reducir el impacto que pueda causar.
>
> Es importante entender que el objetivo de mitigación de riesgos es reducir la exposición al riesgo con la intención de llevarlo a los límites de los umbrales aceptables para cada organización. La exposición al riesgo es la función de la probabilidad de ocurrencia del riesgo y el impacto de este riesgo en el proyecto.
>
> La estrategia de mitigación está referida a todas las acciones que se toman por adelantado o acciones proactivas. La probabilidad de ocurrencia del riesgo y su impacto se identifica

y se calcula en una fase temprana a fin de evitar el daño previsto en el proyecto. Esta estrategia de respuesta se documenta en el registro de riesgo.

2.2.4.2. Características.

Para describir las características de un plan de mitigación de riesgos tecnológicos se toma en cuenta lo expuesto en la Metodología para la gestión de riesgos del Ministerio de Finanzas del Ecuador (2017):

> En el plan de mitigación de riesgos se desarrollará una estrategia de gestión, que incluya su proceso e implementación. Se definirán objetivos y metas, asignando responsabilidades para áreas específicas, identificando conocimientos técnicos, describiendo el proceso de evaluación de riesgos y las áreas a considerar, detallando indicadores de riesgos, delineando procedimientos para las estrategias del manejo, estableciendo lineamientos para el monitoreo y definiendo los reportes, documentos y las comunicaciones necesarias. (p.6)

2.2.4.3. Cuando se lo ejecuta

"El Plan de Mitigación es conveniente hacerlo al principio del proyecto durante la planificación y continuarlo durante toda la ejecución del mismo. Se puede presentar como un informe, estudio, lista de acciones, etc." (Benavides, 2017)

2.2.5. COBIT® (Objetivos de Control para Tecnologías de la Información y Tecnologías relacionadas)

Coronel (como se citó en Carcelén, 2015) menciona el siguiente enunciado acerca de la metodología:

> COBIT propone un marco de referencia para la dirección de TI, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio. COBIT permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones. Enfatiza el cumplimiento normativo, ayuda a las organizaciones a

aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de COBIT. (p.11)

Por su parte ISACA® (2012) menciona que la metodología COBIT® 5 a comparación de la versión anterior, ha integrado las áreas Gobierno y Gestión en la metodología, de esta manera contribuye a las empresas para que mantengan un equilibrio entre los beneficios y la gestión de los niveles de riesgo en los procesos institucionales y la adecuada optimización de recursos dentro del área.

2.2.5.1. COBIT® y su relación con otras metodologías.

La metodología COBIT® 5 fue realizada con la finalidad de alinearse e integrarse con otras metodologías, mismas que aportan en la construcción de los procesos COBIT® y que se detallan a continuación:

Tabla 2. COBIT® y su relación con otras metodologías.

	Metodología	**Versión o Serie.**
ITIL®	*(Information Technology Infrastructure Library)*	ITIL® v3
TOGAF®	*(The Open Group Architecture Framework)*	TOGAF® 9
PMBOK®	*(Project Management Body of Knowledg.)*	PMBOK2®
PRINCE2®	*(Projects IN Controlled Environments 2)*	
COSO	*(Committee of Sponsoring Organizations of the Treadway Commission)*	
CMMI®	*(Capability Maturity Model Integration)*	
ISO	*International Organization for Standardization*	ISO/IEC 9000 ISO/IEC 20000 ISO/IEC 31000 ISO/IEC 27000 ISO/IEC 38500

Fuente: ISACA® (2012) *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*.

La metodología COBIT® 5 se constituye de un determinado número de metodologías y se cubren de la siguiente manera:

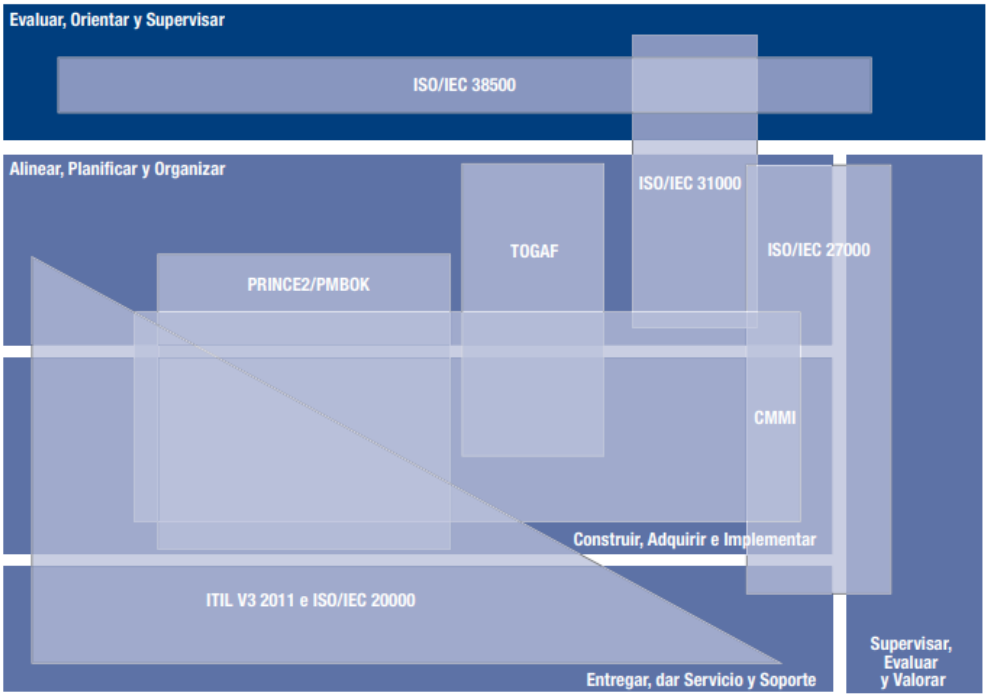


Figura 2. Cobertura de COBIT® 5 de otras metodologías.

Fuente: ISACA® (2012) *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*.

2.2.5.2. Principios de *COBIT® 5*

Los principios de COBIT® 5 son útiles para empresas de cualquier tamaño y dedicadas a cualquier actividad comercial, ya sean públicas o privadas, y se exponen a continuación:

Figura 3. Principios de COBIT® 5

Fuente: ISACA® (2012) *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*.

A continuación, una breve descripción de cada uno de los principios COBIT® 5, tal como lo realiza ISACA® (2012), en su publicación "COBIT® 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa".

Principio 1. Satisfacer las Necesidades de las Partes Interesadas

Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.

COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

Principio 2: Cubrir la Empresa Extremo-a-Extremo

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

- Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.
- Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos internos y externos, los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

Principio 3: Aplicar un Marco de Referencia único integrado

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

Principio 4: Hacer Posible un Enfoque Holístico

Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (*enablers*) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores:

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

Principio 5: Separar el Gobierno de la Gestión

El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. (p.14)

2.2.5.3. Procesos catalizadores de COBIT® 5

El modelo de referencia de procesos de COBIT® 5 subdivide las actividades y prácticas de la organización relacionadas con la TI en dos áreas principales:
Gobierno (1 dominio de procesos)

- Evaluar, Orientar y Supervisar – EDM.

Gestión (4 dominios de procesos)

- Alinear, Planificar y Organizar – APO.
- Construir, Adquirir e Implementar – BAI.
- Entregar, dar Servicio y Soporte – DSS.
- Supervisar, Evaluar y Valorar – MEA.

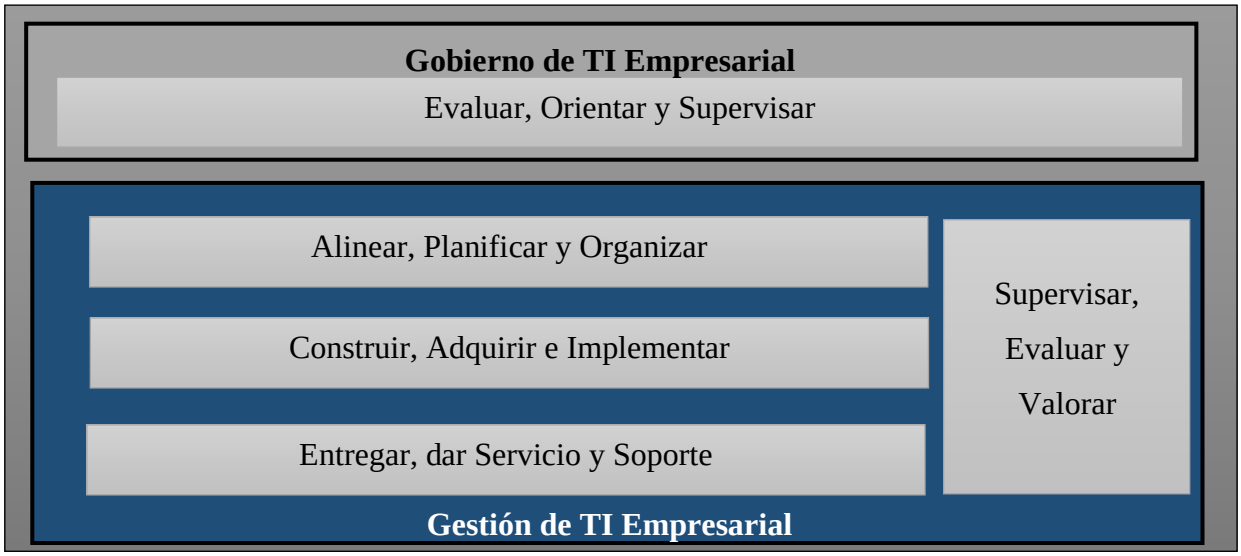


Figura 4. Modelo de referencia de procesos de COBIT® 5

Fuente: ISACA® (2012) *COBIT® 5, Procesos Catalizadores.*

A continuación, se describe el marco de trabajo completo de COBIT® 5, detallando el área, dominios, procesos habilitadores y objetivos de control, descritos en la publicación "COBIT® 5, Procesos Catalizadores" desarrollado por ISACA® (2012).

Tabla 3. Marco de trabajo del área de Gobierno

ÁREA. GOBIERNO		
Dominio	**Procesos**	**Objetivos de control**
Evaluar, Orientar y Supervisar – EDM	EDM01. Asegurar el establecimiento y mantenimiento del marco de gobierno.	EDM01.01. Evaluar el sistema de gobierno. EDM01.02. Orientar el sistema de gobierno. EDM01.03. Supervisar el sistema de gobierno.
	EDM02. Asegurar la entrega de beneficios.	EDM02.01. Evaluar la optimización de valor EDM02.02. Orientar la optimización de valor EDM02.03. Supervisar la optimización de valor
	EDM03. Asegurar la optimización del riesgo.	EDM03.01. Evaluar la gestión de riesgos. EDM03.02. Orientar la gestión de riesgos. EDM03.03. Supervisar la gestión de riesgos.
	EDM04. Asegurar la optimización de los recursos	EDM04.01. Evaluar la gestión de recursos. EDM04.02. Orientar la gestión de recursos. EDM04.03. Supervisar la gestión de recursos.
	EDM05. Asegurar la transparencia hacia las partes interesadas.	EDM05.01. Evaluar los requisitos de elaboración de informes de las partes interesadas. EDM05.02. Orientar la comunicación con las partes interesadas y la de elaboración de informes. EDM05.03. Supervisar la comunicación con las partes interesadas.

Fuente: ISACA® (2012) *COBIT® 5, Procesos Catalizadores.*

Tabla 4. Marco de trabajo del área de Gestión

ÁREA. GESTIÓN		
Dominio	**Procesos**	**Objetivos de control**
Alinear, Planificar y Organizar – APO	APO01. Gestionar el marco de gestión de TI.	APO01.01. Definir la estructura organizativa. APO01.02. Establecer roles y responsabilidades APO01.03. Mantener los elementos catalizadores del sistema de gestión. APO01.04. Comunicar los objetivos y la dirección de gestión. APO01.05. Optimizar la ubicación de la función de TI. APO01.06. Definir la propiedad de la información (datos) y del sistema. APO01.07. Gestionar la mejora continua de los procesos. APO01.08. Mantener el cumplimiento de las políticas y procedimientos.
	APO02. Gestionar la estrategia.	APO02.01. Comprender la dirección de la empresa. APO02.02. Evaluar el entorno, capacidades y rendimiento actuales. APO02.03. Definir el objetivo de las capacidades de TI. APO02.04. Realizar un análisis de diferencias. APO02.05. Definir el plan estratégico y la hoja de ruta. APO02.06. Comunicar la estrategia y dirección de TI
	APO03. Gestionar la arquitectura empresarial.	APO03.01. Desarrollar la visión de arquitectura de la empresa. APO03.02. Definir la arquitectura de referencia. APO03.03. Seleccionar las oportunidades y soluciones.

		APO03.04. Definir la implantación de la arquitectura. APO03.05. Proveer los servicios de arquitectura empresarial.
	APO04. Gestionar la innovación.	APO04.01 Crear un entorno favorable para la innovación. APO04.02. Mantener un entendimiento del entorno de la empresa. APO04.03. Supervisar y explorar el entorno tecnológico. APO04.04. Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras. APO04.05. Recomendar iniciativas apropiadas adicionales. APO04.06. Supervisar la implementación y el uso de la innovación.
	APO05. Gestionar el portafolio.	APO05.01. Establecer la mezcla del objetivo de inversión. APO05.02. Determinar la disponibilidad y las fuentes de fondos. APO05.03. Evaluar y seleccionar los programas a financiar. APO05.04. Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones. APO05.05. Mantener los portafolios APO05.06. Gestionar la consecución de beneficios.
	APO06. Gestionar el presupuesto y los costes.	APO06.01. Gestionar las finanzas y la contabilidad APO06.02. Priorizar la asignación de recursos. APO06.03. Crear y mantener presupuestos. APO06.04. Modelar y asignar costes. APO06.05. Gestionar costes.

	APO07. Gestionar los recursos humanos.	APO07.01. Mantener la dotación de personal suficiente y adecuada. APO07.02. Identificar personal clave de TI APO07.03. Mantener las habilidades y competencias del personal. APO07.04. Evaluar el desempeño laboral de los empleados. APO07.05. Planificar y realizar un seguimiento del uso de los recursos humanos de TI y del negocio. APO07.06. Gestionar el personal contratado.
	APO08. Gestionar las relaciones	APO08.01. Entender las expectativas del negocio. APO08.02. Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio. APO08.03. Gestionar las relaciones con el negocio. APO08.04. Coordinar y comunicar. APO08.05. Proveer datos de entrada para la mejora continua de los servicios.
	APO09. Gestionar los acuerdos de servicio.	APO09.01. Identificar servicios de TI. APO09.02. Catalogar servicios basados en TI. APO09.03. Definir y preparar acuerdos de servicio. APO09.04. Supervisar e informar de los niveles de servicio. APO09.05. Revisar acuerdos de servicio y contratos.
	APO10. Gestionar los proveedores.	APO10.01. Identificar y evaluar las relaciones y contratos con proveedores. APO10.02. Seleccionar proveedores. APO10.03. Gestionar contratos y relaciones con proveedores. APO10.04. Gestionar el riesgo en el suministro. APO10.05. Supervisar el cumplimiento y rendimiento del proveedor.
	APO11. Gestionar la calidad.	APO11.01. Establecer un sistema de gestión de calidad.

		APO11.02. Definir y gestionar los estándares, procesos y prácticas de calidad. APO11.03. Enfocar la gestión de calidad en los clientes. APO11.04. Supervisar y hacer controles y revisiones de calidad. APO11.05. Integrar la gestión de calidad en la implementación de soluciones y la entrega de servicios. APO11.06. Mantener una mejora continua.
	APO12. Gestionar el riesgo.	APO12.01. Recopilar datos. APO12.02. Analizar el riesgo. APO12.03. Mantener un perfil de riesgo. APO12.04. Expresar el riesgo. APO12.05. Definir un portafolio de acciones para la gestión de riesgos. APO12.06. Responder al riesgo.
	APO13. Gestionar la seguridad.	APO13.01. Establecer y mantener un SGSI. APO13.02. Definir y gestionar un plan de tratamiento del riesgo de la seguridad de información. APO13.03. Supervisar y revisar el SGSI.
Construir, Adquirir e Implementar – BAI	BAI01. Gestionar los programas y proyectos.	BAI01.01. Mantener un enfoque estándar para la gestión de programas y proyectos. BAI01.02. Iniciar un programa. BAI01.03. Gestionar el compromiso de las partes interesadas. BAI01.04. Desarrollar y mantener el plan del programa. BAI01.05. Lanzar y ejecutar el programa. BAI01.06. Supervisar controlar e informar de los resultados del programa.

	BAI01.07. Lanzar e iniciar proyectos dentro de un programa. BAI01.08. Planificar proyectos. BAI01.09. Gestionar la calidad de los programas y proyectos. BAI01.10. Gestionar el riesgo de programas y proyectos. BAI01.11. Supervisar y controlar proyectos BAI01.12. Gestionar los recursos y los paquetes de trabajo del proyecto. BAI01.13. Crear un proyecto o iteración. BAI01.14. Cerrar un programa.
BAI02. Gestionar la definición de requisitos.	BAI02.01. Definir y mantener los requerimientos técnicos y funcionales de negocio. BAI02.02. Realizar un estudio de vialidad y proponer soluciones alternativas. BAI02.03. Gestionar los riesgos de los requerimientos. BAI02.04. Obtener la aprobación de los requerimientos y soluciones.
BAI03. Gestionar la identificación y la construcción de soluciones.	BAI03.01. Diseñar soluciones de alto nivel BAI03.02. Diseñar los componentes detallados de la solución BAI03.03. Desarrollar los componentes de la solución. BAI03.04. Obtener los componentes de la solución. BAI03.05. Construir soluciones. BAI03.06. Realizar controles de calidad BAI03.07. Preparar pruebas de solución. BAI03.08. Ejecutar pruebas de solución. BAI03.09. Gestionar cambios a los requerimientos. BAI03.10. Mantener soluciones.

		BAI03.11. Definir los servicios de TI y mantener el catálogo de servicios.
	BAI04. Gestionar la disponibilidad y la capacidad.	BAI04.01. Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia. BAI04.02. Evaluar el impacto en el negocio. BAI04.03. Planificar requisitos de servicio nuevos o modificados BAI04.04. Supervisar y revisar la disponibilidad y capacidad. BAI04.05. Investigar y abordar cuestiones de disponibilidad rendimiento y capacidad.
	BAI05. Gestionar la introducción de cambios organizativos.	BAI05.01. Establecer el deseo de cambiar. BAI05.02. Formar un equipo de implementación efectivo. BAI05.03. Comunicar la visión deseada. BAI05.04. Facultar a los que juegan algún papel e identificar ganancias en el corto plazo. BAI05.05. Facilitar la operación y el uso. BAI05.06. Integrar nuevos enfoques. BAI05.07. Mantener los cambios.
	BAI06. Gestionar los cambios.	BAI06.01. Evaluar, priorizar y autorizar peticiones de cambio. BAI06.02. Gestionar cambios de emergencia. BAI06.03. Hacer seguimiento e informar de cambios de estado. BAI06.04. Cerrar y documentar cambios.
	BAI07. Gestionar la aceptación del cambio y de la transición	BAI07.01. Establecer un plan de implementación. BAI07.02. Planificar la conversión de procesos de negocio, sistemas y datos. BAI07.03. Planificar pruebas de aceptación. BAI07.04. Establecer un entorno de pruebas. BAI07.05. Ejecutar pruebas de aceptación.

	BAI07.06. Pasar a producción y gestionar los lanzamientos. BAI07.07 Proporcionar soporte en producción desde el primer momento. BAI07.08. Ejecutar una revisión post-implantación
BAI08. Gestionar el conocimiento.	BAI08.01. Cultivar y facilitar una cultura de intercambio de conocimientos. BAI08.02. Identificar y clasificar las fuentes de información. BAI08.03. Organizar y contextualizar la información, transformándola en conocimiento. BAI08.04. Utilizar y compartir el conocimiento. BAI08.05. Evaluar y retirar la información.
BAI09. Gestionar los activos.	BAI09.01. Identificar y registrar activos actuales. BAI09.02. Gestionar los activos críticos. BAI09.03. Gestionar el ciclo de vida de los activos BAI09.04. Optimizar el coste de los activos. BAI09.05. Administrar licencias.
BAI10. Gestionar la configuración	BAI10.01. Establecer y mantener un modelo de configuración. BAI10.02. Establecer y mantener un repositorio de configuración y una base de referencia. BAI10.03. Mantener y controlar los elementos de configuración. BAI10.04. Generar informes de estado y configuración. BAI10.05. Verificar y revisar la integridad del repositorio de configuración.

Entregar, dar Servicio y Soporte – DSS	DSS01. Gestionar las operaciones	DSS01.01. Ejecutar procedimientos operativos. DSS01.02. Gestionar servicios externalizados de TI. DSS01.03. Supervisar la infraestructura de TI DSS01.04. Gestionar el entorno DSS01.05. Gestionar las instalaciones.
	DSS02. Gestionar las peticiones e incidentes del servicio.	DSS02.01. Definir esquemas de clasificación de incidentes y peticiones de servicio. DSS02.02. Registrar, clasificar y priorizar peticiones e incidentes. DSS02.03. Verificar, aprobar y resolver peticiones de servicio. DSS02.04. Investigar, diagnosticar y localizar incidentes. DSS02.05. Resolver y recuperarse de incidentes DSS02.06. Cerrar peticiones de servicio e incidente DSS02.07. Seguir el estado y emitir informes.
	DSS03. Gestionar los problemas.	DSS03.01. Identificar y clasificar problemas. DSS03.02. Investigar y diagnosticar problemas. DSS03.03. Levantar errores conocidos. DSS03.04. Resolver y cerrar problemas DSS03.05. Realizar una gestión de problemas proactiva.
	DSS04. Gestionar la continuidad.	DSS04.01. Definir la política de continuidad de negocio, objetivos y alcance. DSS04.02. Mantener una estrategia de continuidad. DSS04.03. Desarrollar e implementar una respuesta a la continuidad de negocio. DSS04.04. Ejecutar, probar y revisar el plan de continuidad. DSS04.05 Revisar, mantener y mejorar el plan de continuidad DSS04.06. Proporcionar formación en el plan de continuidad.

		DSS04.07. Gestionar acuerdos de respaldo. DSS04.08. Ejecutar revisiones post- reanudación.
	DSS05. Gestionar los servicios de seguridad.	DSS05.01. Proteger contra software malicioso DSS05.02. Gestionar la seguridad de la red y las conexiones. DSS05.03. Gestionar la seguridad de los puestos de usuario final. DSS05.04. Gestionar la identidad del usuario y el acceso lógico DSS05.05. Gestionar el acceso físico a los activos de TI DSS05.06. Gestionar documentos sensibles y dispositivos de salida DSS05.07. Supervisar la infraestructura para detectar eventos relacionados con la seguridad.
	DSS06. Gestionar los controles de los procesos de negocio.	DSS06.01. Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos. DSS06.02. Controlar el procesamiento de información. DSS06.03. Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización. DSS06.04. Gestionar errores y excepciones. DSS06.05. Asegurar la trazabilidad de los eventos y responsabilidades de información DSS06.06. Asegurar los activos de información.
Supervisar, Evaluar y Valorar – MEA	MEA01. Supervisar, Evaluar y Valorar rendimiento y conformidad.	MEA01.01. Establecer un enfoque de la supervisión MEA01.02. Establecer los objetivos de cumplimiento y rendimiento MEA01.03. Recopilar y procesar los datos de cumplimiento y rendimiento. MEA01.04. Analizar e informar sobre el rendimiento.

		MEA01.05. Asegurar la implantación de medidas correctivas.
	MEA02. Supervisar, Evaluar y Valorar el sistema de Control Interno.	MEA02.01. Supervisar el control interno MEA02.02. Revisar la efectividad de los controles sobre los procesos de negocio. MEA02.03. Realizar autoevaluaciones de control. MEA02.04. Identificar y comunicar las deficiencias de control. MEA02.05. Garantizar que los proveedores de aseguramiento son independientes y están cualificados. MEA02.06. Planificar iniciativas de aseguramiento MEA02.07. Estudiar iniciativas de aseguramiento MEA02.08. Ejecutar iniciativas de aseguramiento.
	MEA03. Supervisar, Evaluar y Valorar la conformidad con los requerimientos externos.	MEA03.01. Identificar requisitos externos de cumplimiento. MEA03.02. Optimizar la respuesta a requisitos externos. MEA03.03. Confirmar el cumplimiento de requisitos externos. MEA03.04. Obtener garantía de cumplimiento de requisitos externos.

Fuente: ISACA® (2012) *COBIT® 5, Procesos Catalizadores.*

2.2.5.4. Modelo de Capacidad de Procesos

La publicación denominada "COBIT® 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa" indica la existencia de seis niveles de capacidad que se pueden alcanzar por un proceso, por lo que ISACA® (2012) menciona la valoración de la siguiente manera:

• **0 Proceso incompleto**. El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.

• **1 Proceso ejecutado (un atributo).** El proceso implementado alcanza su propósito.

• **2 Proceso gestionado (dos atributos).** El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.

• **3 Proceso establecido (dos atributos).** El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.

• **4 Proceso predecible (dos atributos).** El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.

• **5 Proceso optimizado (dos atributos).** El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con los metas empresariales presentes y futuros. (p.42)

En la siguiente figura se evidencia los seis niveles de capacidad de proceso, y los atributos a considerar por cada nivel, los atributos contribuyen a la escala de evaluación en el cumplimiento de determinado proceso a auditar, se considera que, si es mayor la capacidad del proceso, menor es el riesgo.

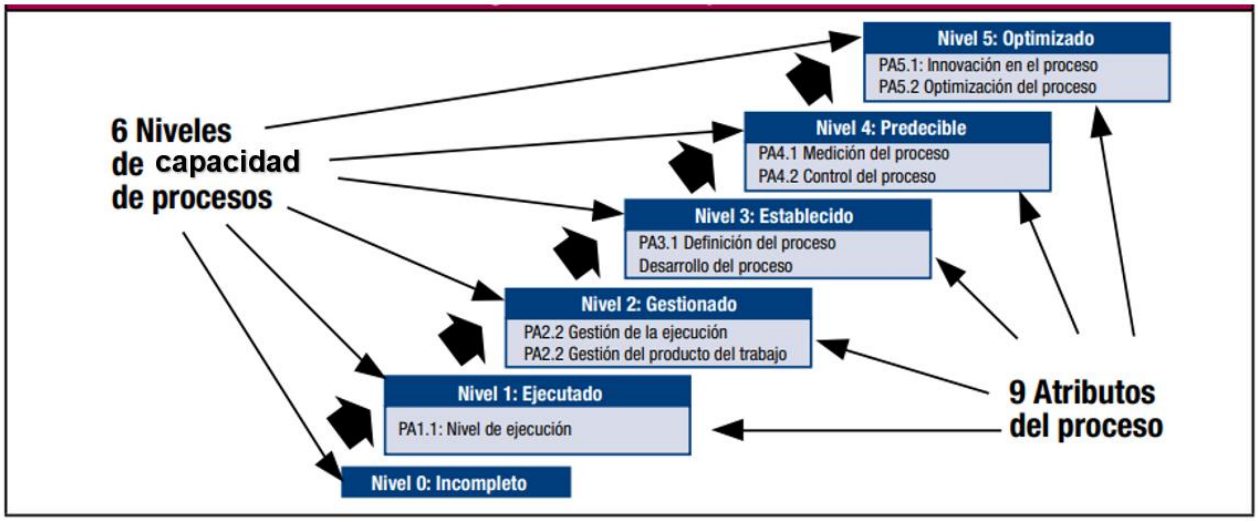


Figura 5. Modelo de capacidad de proceso

Fuente: ISACA® (2013) *Guía de Auto-Evaluación: Usando* COBIT® 5

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

La presente investigación tuvo un enfoque cuali-cuantitativo, Según Hernández, Fernández y Baptista (2014) "los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos" (p.7), es así que el proceso cualitativo contiene una serie de fases que se fundamentan en la revisión de la literatura denominado marco de referencia en este caso es la metodología COBIT® 5, de la misma manera los autores mencionan que "el enfoque cuantitativo es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos "brincar" o eludir pasos." (p.4), enunciado que se ajusta a los requerimientos de la investigación debido a que la auditoría informática se construyó con tres fases fundamentales que son: planeación, ejecución y dictamen, mismas que fueron planificadas y ejecutadas a la terminación de la etapa anterior.

3.1.2. Tipo de Investigación

Se describen los tipos de investigación que se tomaron en cuenta para la realización del presente proyecto de titulación, y son las siguientes:

- **Investigación Descriptiva.**

Esta investigación tuvo influencia sobre el estudio de los procesos institucionales y de TI por ello se describió: características, grupo de personas y actividades, concluyendo con análisis de riesgos.

- **Investigación- Acción.**

Se estableció un nivel de cumplimiento a cada proceso COBIT® 5 auditado en la EPMAPA-T, mismo que ha generado el plan de mitigación de riesgos tecnológicos que se enfoca a mejorar los procesos institucionales a base de estrategias de mitigación, con la finalidad de aportar información que guíe a la toma de decisiones referente a procesos, tecnología y personas que conforman la empresa.

- **Investigación Bibliográfica.**

Se consideró una investigación bibliográfica, debido a que se utilizaron libros, artículos, folletos, revistas y la metodología COBIT® 5. Además, apoyó al cumplimiento del primer objetivo planteado en la presente investigación.

- **Investigación de campo.**

Esta investigación permitió extraer información, utilizando diferentes técnicas de recolección desde el ambiente de estudio en este caso la EPMAPA-T.

3.2. IDEA A DEFENDER

El plan de mitigación de riesgos tecnológicos contribuye a minimizar el impacto generado por los riesgos tecnológicos en la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE VARIABLES

Tabla 5. Variable independiente-Auditoria informática basada en la metodología COBIT® 5

Definición	Dimensión	Indicadores	Técnicas	Instrumentos
Auditoria Informática. Es un examen que se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas del negocio. (Universidad Autónoma del Estado de Hidalgo, 2011, p.6)	Eficacia	• Cumplimiento de las funciones del DSI.	• Entrevista al supervisor informático • Observación regulada	• Revisión bibliográfica • Cuestionario estructurado • Fichas de proceso • Observación simple
	Eficiencia	• Manual de procesos. • Planificación POA para el DSI.	• Entrevista con personal que realiza el proceso • Entrevista al supervisor informático del departamento • Verificación de documentación.	• Revisión bibliográfica. • Cuestionario estructurado • Fichas de cumplimiento • Revisión documental
	Gestión Informática	• Documentación legal • Normativa vigente. • Cumplimiento de los objetivos institucionales y de TI	• Entrevista al supervisor informático del departamento • Verificación de documentación • Observación regulada • Encuesta a usuarios internos	• Revisión bibliográfica • Cuestionario estructurado • Fichas de proceso • Observación simple

Tabla 6. Variable independiente- Normativa interna regulatoria de riesgos tecnológicos

Definición	Dimensión	Indicadores	Técnicas	Instrumentos
Normas de control interno "El control interno es un proceso integral aplicado por la máxima autoridad regulatoria, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos" (Contraloría General del Estado Ecuatoriano, 2014, p.3)	Control interno institucional	• Normativa vigente. • Reglamentos vigentes.	• Entrevista al Director de Gestión Administrativa. • Verificación de documentación.	• Revisión documental • Cuestionario estructurado • Observación simple

Tabla 7. Variable Dependiente - Plan de mitigación de riesgos tecnológicos

Definición	Dimensión	Indicadores	Técnicas	Instrumentos
Se denomina Plan de Mitigación de riesgos a las estrategias definidas por la empresa que tratan de reducir la probabilidad de ocurrencia del riesgo o reducir el impacto que pueda causar. (Benavides, 2017).	Riesgos Identificados	• Interpretación • Cuantificación • Priorización • Evaluación	• Informe preliminar • Informe final	• Revisión bibliográfica • Documentación
	Estrategias para llevar a cabo	• Estrategias en base a los hallazgos.	• Plan de mitigación de riesgos tecnológicos	• Revisión bibliográfica • Documentación

3.4. MÉTODOS UTILIZADOS

En la presente investigación, se tomó en cuenta dos métodos que permitieron cumplir con el proceso investigativo de una manera eficiente.

Método científico

El autor Asensi y Parra (como se citó en De Hoyos, 2020), en la publicación denominada "El método científico y la filosofía como herramientas para generar conocimiento" mencionó el siguiente enunciado:

> El método científico está compuesto de unos pasos secuenciales para llevarse a cabo. La primera etapa tiene que ver con identificar el problema a abordar; este problema puede darse por la ausencia de conocimiento, por una pregunta que necesita una respuesta o por la necesidad de explicar datos preexistentes. En la segunda etapa, se propone una hipótesis con el objetivo de buscar una solución provisional al problema que se plantea. En la tercera etapa se recurre a la experimentación u observación para comprobar las hipótesis planteadas; en esta etapa se realiza la recogida, análisis e interpretación de los datos. (p.238)

En este caso se empezó por la revisión bibliográfica de la metodología COBIT® 5 y con ello se interpretó las métricas aplicables al caso de estudio, seguido se aplicó las técnicas para recolectar información y finalmente se interpretó los hallazgos del proceso de investigación.

Diseño No Experimental.

Según Hernández, Fernández y Baptista (2014) los diseños no experimentales son: "Estudios que se realizan sin la manipulación deliberada de variables y en los que sólo se observan los fenómenos en su ambiente natural para analizarlos." (p.152). En este proyecto se realizó una descripción de la situación tecnológica de la EPMAPA-T, sin necesidad de alterar el ambiente normal de la empresa.

3.4.1. Técnicas e instrumentos

Para la recolección y procesamiento de datos, se han utilizado las siguientes técnicas e instrumentos.

- *Entrevista estructurada.* La entrevista ha sido aplicada con fines de recolección de información que se complementa con otras técnicas y permitió conocer datos de notable importancia y que han sido incluidos en los cuestionarios.
- *Entrevista no estructurada*. Este tipo de técnica permitió obtener información de una manera más profunda, con la finalidad de indagar ciertos temas que se pasaron por alto en los cuestionarios realizados.
- *Observación simple no regulada*. Esta técnica permitió obtener información a partir de la observación del comportamiento y situaciones reales en el cumplimiento de los procesos institucionales y de TI.
- *Documentos y registros*. La revisión de documentos institucionales, fue una actividad permanente con la finalidad de demostrar evidencias de los hallazgos en el proceso de auditoría.
- *Validación de instrumentos.* Se llevó a cabo la validación de instrumentos de recolección de información, por parte de expertos en el tema previa a aplicación de los mismos en el entorno a auditar.

3.4.2. Población y muestra

En esta investigación no fue necesaria la aplicación de un método estadístico para el cálculo de la muestra, debido a que se obtuvo la información de una serie de técnicas e instrumentos, donde fue necesaria la intervención de diferentes actores dependiendo de los requerimientos de la investigación, mismos que se detallan a continuación:

Tabla 8. Población que interviene en la investigación

Fase	Instrumentos	Técnica	Actores
Estudio Inicial	Cuestionario estructurado	Entrevista	• Supervisor Informático • Analista de Sistemas • Director de Gestión Administrativa
	Cuestionario estructurado	Encuesta	• 40 servidores públicos y 6 lectores
Planeación de Auditoría	Fichas de proceso de TI	Entrevista	• Equipo del área de TI
	Fichas de proceso institucional	Entrevista Observación simple no regulada	• Director de Gestión de Comercialización. • Supervisor Informático • Secretaría General
Aplicación de Auditoría	Check list Matriz de verificación	Entrevista Documentos registros	• Supervisor Informático • Analistas de Sistemas • Dirección de Gestión Administrativa • Asistente de Talento Humano • Asesor Legal
	Revisión evidencias	Documentos registros	• Supervisor Informático • Director de Gestión Comercial • Director de Gestión Administrativa
Plan de mitigación de riesgos tecnológicos	Documento de estrategias de mitigación	Documentos	• Supervisor Informático. • Gerente General

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

4.1.1. Datos Informativos

Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán- EPMAPA-T

4.1.1.1. Logotipo

Figura 6. Logotipo EPMAPA-T
Fuente: EPMAPA (2019) *Sitio web.*

4.1.1.2. Ubicación

Av. Juan Ramón Arellano y Bolívar, S. Terminal

Tulcán – Carchi – Ecuador.

4.1.1.3. Descripción

La Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán es una empresa que se encarga la captación, conducción, tratamiento, almacenamiento, distribución y comercialización de agua potable en condiciones sanitarias apropiadas, de la misma manera el alcantarillado y tratamiento de las aguas residuales.

4.1.1.4. Misión

> La Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán, tiene como objeto suministrar servicios públicos de agua potable y alcantarillado a la ciudadanía de Tulcán, así como la prestación de productos y servicios de calidad y el asesoramiento a sus parroquias rurales, garantizando calidad, eficiencia, responsabilidad social, sostenibilidad económica y ambiental. (EPMAPA-T, 2019)

4.1.1.5. Visión

"La EPMAPA-T para el año 2030, proyecta ser una empresa líder en gestión sustentable, sostenible e innovadora en la administración del agua y alcantarillado logrando una valoración ciudadana de ecosistemas naturales productores de las fuentes hídricas." (EPMAPA-T, 2019)

4.1.1.6. Objetivo General

"Brindar servicios de óptima calidad de agua potable y alcantarillado, a través de procesos amigables con el medio ambiente, centrados siempre en una atención profesional, eficiente, personalizada y amable, en el fiel cumplimiento de las expectativas internas y externas." (EPMAPA-T, 2019)

4.1.1.7. Objetivos Estratégicos Institucionales

1. Garantizar a la población de Tulcán la prestación de los servicios de Agua Potable y Alcantarillado y el tratamiento de aguas residuales en condiciones óptimas.
2. Motivar el sentido de pertenencia de los ciudadanos a través del reconocimiento y valoración de la empresa.
3. Optimizar el sistema comercial para beneficio institucional y de los ciudadanos.
4. Garantizar la rentabilidad social en sus inversiones.
5. Conservar, mejorar y preservar de forma sustentables las fuentes de aprovechamiento de agua; la producción y distribución del agua potable de manera continua y de calidad contribuyendo a la preservación del medio ambiente y a la salud de la población.
6. Mantener costos y gastos controlados los mismos que se vean reflejados en tarifas justas que aseguren la autosostenibilidad financiera.
7. Apoyar tecnológicamente a los procesos internos para conseguir satisfacción en los clientes.
8. Desarrollar una gestión ambiental responsable que minimice los impactos sobre el ambiente.
9. Desarrollar una política de recursos humanos que, además de mejorar la eficiencia laboral, promueva el desarrollo de competencias profesionales. (EPMAPA-T, 2019)

4.1.1.8. Estructura Orgánica Funcional

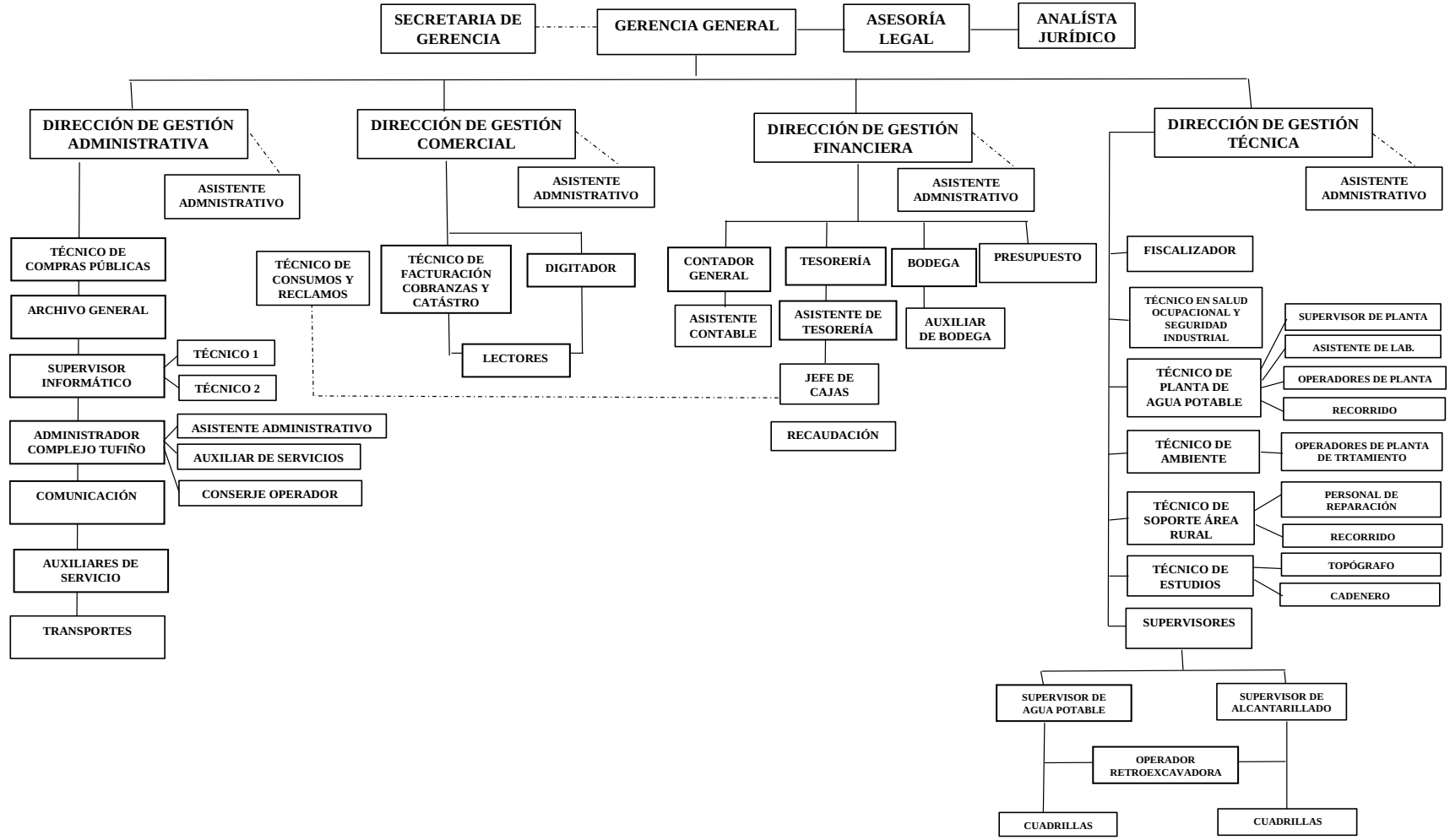


Figura 7. Estructura Orgánica Funcional
Fuente: EPMAPA-T (2018) *Transparencia EPMAPA-T 2018*

4.1.2. Auditoría Informática

4.1.2.1. Objetivo de auditoría

Desarrollar una evaluación informática a los procesos internos de la EPMAPA-T, con la finalidad de identificar riesgos tecnológicos que afecten el cumplimiento de los objetivos institucionales y/o tecnológicos.

4.1.2.2 Alcance de la Auditoría Informática

El alcance de la presente auditoría se determinó por el marco referencial de COBIT® 5, el mismo que está enfocado al cumplimiento de los objetivos de la institución, con una evaluación minuciosa que se fundamenta en las áreas o aspectos principales que son: Gobierno de TI y Gestión de TI.

La investigación se fundamentó principalmente en las áreas que la metodología COBIT® 5 lo solicitó, siendo las siguientes: (Gobierno de TI, Control Interno, Talento Humano, Dirección de TI, Operativo de TI), adicional a ello se realizó un diagnóstico de procesos institucionales y tecnológicos con la finalidad de identificar puntos críticos que afecten al cumplimiento de los objetivos institucionales y tecnológicos de la empresa.

4.1.2.3. Justificación

La auditoría informática es un proceso de evaluación que permite detectar falencias a nivel tecnológico, y de esta manera proyectarse a la mejora de los servicios que presta el área de tecnología en la EPMAPA-T

4.1.2.4. Equipo auditor

Auditor	Yuly Pantoja
Asesor	Ing. Carlitos Guano, MSc.

4.1.3. Estudio Inicial

4.1.3.1. Análisis de la situación actual de la EPMAPA-T

La Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán, es una entidad que se dedica a todo lo referente a la prestación de servicios de agua potable y alcantarillado, dentro del Cantón Tulcán, específicamente en la cabecera Cantonal.

La EPMAPA-T fue constituida inicialmente con la denominación de Empresa Municipal de Agua Potable y Alcantarillado de Tulcán, publicada en el Registro Oficial Nro. 71 del 25 de julio del 2005. Sin embargo, mediante registro oficial de fecha 16 de octubre del 2009, Nro. 48 se publicó la nueva Ley Orgánica de Empresas Públicas, por lo que el Concejo Municipal de Tulcán, mediante sesiones de 14 y 15 de abril de 2010, resolvió; aprobar la "ORDENANZA DE CONSTITUCIÓN DE LA EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE TULCÁN EPMAPA-T", publicado en el Registro Oficial No. 243 del lunes 16 de Julio del 2011; la empresa goza de personería jurídica de derecho público y autonomía orgánica, funcional y presupuestaria. (EPMAPA-T,2010, p.1)

Esta institución está regida por los cuatro niveles administrativos, que son los siguientes: Nivel Legislativo, Nivel Ejecutivo, Nivel Asesor y Nivel Operativo.

La EPMAPA-T cuenta con un Departamento de Supervisión Informática, el mismo que forma parte de la Dirección de Gestión Administrativa, que debe cumplir con las funciones estipuladas en el Reglamento Orgánico Funcional de la Empresa, las cuales son:

1. Implementación y desarrollo de tecnologías de la información
2. Diseño e implementación de redes cableadas e inalámbricas
3. Mantener las seguridades LAN y WAN
4. Administración e implementación de servidores
5. Administración y políticas de seguridad y usuarios
6. Diseño y mantenimiento de sitios web
7. Mantenimiento de equipos informáticos

8. Brindar soporte técnico
9. Labores de mantenimiento preventivo y limpieza del equipo informático
10. Programación, desarrollo y mantenimiento de los sistemas hechos en la EPMAPA-T
11. Colaborar en la elaboración de nuevos sistemas para mejorar la atención al público y la gestión
12. Soporte en los procesos de contratación pública;
13. Las demás responsabilidades inherentes al cargo, que le fueren encomendadas por sus superiores. (EPMAPA-T, 2010, p.9)

Las funciones han sido cumplidas de acuerdo a las posibilidades del DSI, sin embargo, existen varias situaciones que pueden derivar en posibles situaciones de riesgos que afecten a la institución.

4.1.3.2. Estructura Organizacional

La Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán, está conformada por los siguientes niveles Administrativos.

- Nivel Legislativo
- Nivel Ejecutivo
- Nivel Asesor; y,
- Nivel Operativo

Los niveles se encuentran distribuidos de la siguiente manera;

Tabla 9. Estructura Organizacional

Nivel Legislativo	
Responsable	**Integrantes**
Directorio	• Alcalde o su delegado • Concejal- presidente de obras públicas • Director de obras públicas del GAD Tulcán • Delegado de los clientes urbanos EPMAPA-T • Delegado de los GAD Parroquiales de Tulcán • Gerente General de la EPMAPA-T será el secretario del Directorio.
Nivel Ejecutivo	
Responsable	**Integrantes**
Gerente General	• Gerente General de la EPMAPA-T • Secretaría de Gerencia
Nivel Asesor	
Responsable	**Integrantes**
Comisiones Internas	**Permanentes** • Funcionarios de carácter Técnico y Finanzas. **Especiales** • Dos miembros del Directorio • Empleados de la EPMAPA-T • Otras Dependencias Municipales • Expertos en la materia cuestionada
Asesoría Legal	• Asesor Legal – Asistente Administrativo
Nivel Operativo	
Responsable	**Integrantes**
Dirección de Gestión Administrativa	• Director de Gestión Administrativa • Técnico en Sistemas (DSI) • Técnico en Compras Publicas • Comunicación Corporativa • Asistente Administrativo • Chofer Mensajero

Dirección de Gestión Financiera	• Director de Gestión Financiera • Tesorero - Pagador • Contador • Ayudante de Contabilidad • Bodeguero • Asistente Administrativo
Dirección de Gestión Comercial	• Director de Gestión Comercial • Técnico en Facturación, Cobranza y Catastro • Técnico en Consumo y Reclamos. • Digitador • Recaudador • Lector – Notificador • Asistente Administrativo.
Dirección de Gestión Técnica	• Director de Gestión Técnica. PLANIFICACION Y PROYECTOS • Técnico en proyectos • Técnico en fiscalización • Técnico en medio ambiente • Asistente Técnico. MANTENIMIENTO OPERACIONAL • Jefe de Planta • Asistente de laboratorio • Supervisor de planta • Operador de planta de agua potable • Operador de planta de aguas residuales • Guardián operador • Inspector • Plomero • Trabajadores en Alcantarillado

Fuente: EPMAPA-T (2010) *Reglamento Orgánico Funcional*

Para cada nivel administrativo, se cuenta con un número determinado de puestos de trabajo, de la siguiente manera:

Tabla 10. Puestos de trabajo por nivel

Nivel Administrativos	Puestos de trabajo
Nivel Legislativo	
Directorio	----------
Nivel Ejecutivo	
Gerente General	3
Nivel Asesor	
Comisiones Internas	----------
Asesoría Legal	2
Nivel Operativo	
Dirección de Gestión Administrativa	18
Dirección de Gestión Financiera	17
Dirección de Gestión Comercial	11
Dirección de Gestión Técnica	77
Total	**128**

Fuente: EPMAPA-T (2018) *Distributivo del personal 2018*

4.1.3.3. Técnicas para el levantamiento de información

Para llevar a cabo la fase de estudio inicial, se ha utilizado las siguientes técnicas:

Tabla 11. Técnicas para levantar información

Técnica	Personal de trabajo	Objetivo
Encuesta	Servidores públicos y lectores	Conocer el cumplimiento de funciones y actividades del DSI en la EPMAPA-T.
Entrevistas	Director de Gestión Administrativa. Personal del DSI	Conocer acerca de la temática de TI, y su vinculación con la EPMAPA-T, tanto en cumplimiento, gestión y documentación.

Observación	Toda la institución	Evidenciar el cumplimiento de las actividades, y el manejo de la información de la empresa.

4.1.3.4. Resultados obtenidos.

Resultados encuesta a los usuarios internos

La encuesta fue realizada a la totalidad de servidores públicos, debido a que son las personas que están en contacto con los equipos informáticos institucionales, siendo un total de cuarenta personas. Adicional a ello, se ha tomado en cuenta seis lectores debido a que son las personas que se dedican a la recolección de lecturas de consumo de agua potable, proceso que se lleva a cabo mediante una aplicación instalada en dispositivos móviles institucionales, dando un total de cuarenta y seis personas. El modelo de encuesta se encuentra en el Anexo 6.

EQUIPO INFORMÁTICO

1. ¿Para desarrollar las funciones y actividades dentro de la EPMAPA-¿T, utiliza un equipo informático? Si su respuesta es SI continúe con la encuesta, de lo contrario, la misma finaliza.

Tabla 12. Uso del equipo informático

	Cantidad	Porcentaje
Si	46	100%
No	0	0%
Total	46	100%

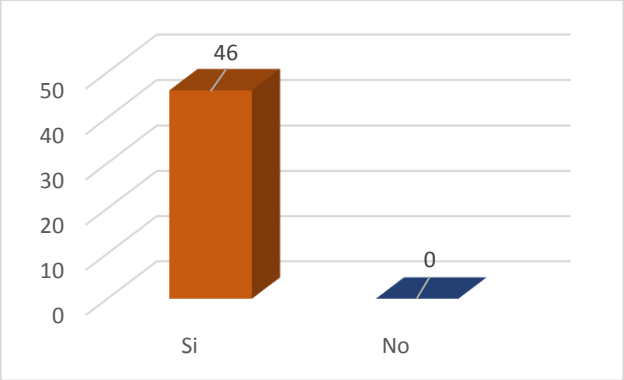


Figura 8. Uso del equipo informático

Análisis e Interpretación. El 100% del total de encuestados ha manifestado que usa un equipo informático para el cumplimiento de sus funciones y actividades. Tomando en cuenta que los

seis lectores hacen uso de teléfonos celulares institucionales, que disponen de un aplicativo móvil de lectura.

2. ¿El equipo informático que se encuentra a su disposición es?

Tabla 13. Pertenencia del equipo informático.

	Cantidad	Porcentaje
Personal	2	4%
Institucional	44	96%
Desconoce	0	0%
Total	46	100%

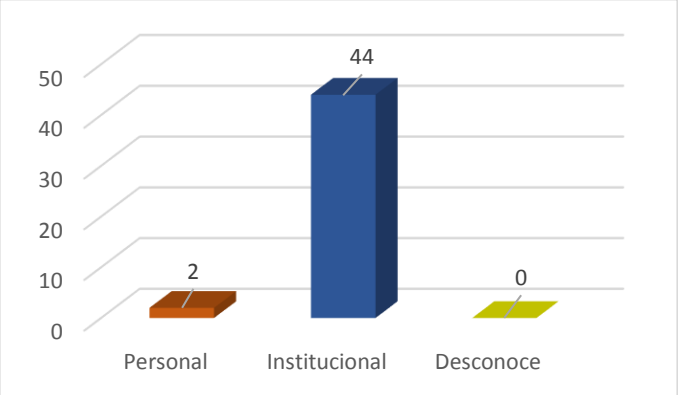


Figura 9. Pertenencia del equipo informático.

Análisis e Interpretación. El 96% del total de encuestados usa un equipo institucional, y el 4% usa un equipo personal para el desarrollo de sus funciones, el DSI ha manifestado que el 4 % de los encuestados que no usa equipo institucional se debe a que el equipo se encuentra en reparaciones por lo que en este caso el usuario interno debe usar un equipo personal.

3. ¿Conoce usted si al equipo que ocupa se le ha realizado mantenimiento preventivo y/o correctivo P/C por el DSI.?

Tabla 14. Conocimiento sobre el mantenimiento P/C

	Cantidad	Porcentaje
Si	17	37%
No	29	63%
Total	46	100%

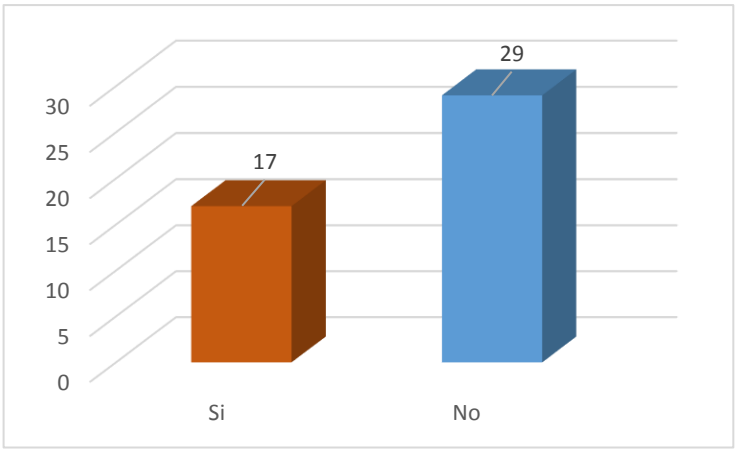


Figura 10. Conocimiento sobre el mantenimiento P/C

Análisis e Interpretación. El 37% ha manifestado respuesta afirmativa acerca del conocimiento sobre los mantenimientos preventivo y /o correctivo del equipo informático que usa, mientras el 63% ha manifestado que no tiene conocimiento de este procedimiento sobre sus equipos.

3.1. ¿Con que frecuencia se le ha realizado mantenimiento preventivo y/o correctivo al equipo que se encuentra a su disposición?

Tabla 15. Frecuencia del mantenimiento P/C

	Cantidad	Porcentaje
Bimestral	2	4%
Trimestral	7	15%
Semestral	7	15%
Anual	7	15%
Nunca	17	37%
Cuando se solicita	6	13%
Total	46	100%

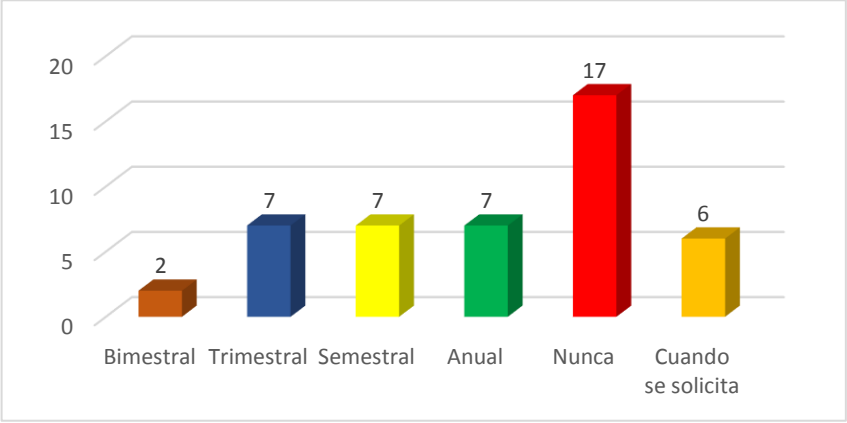


Figura 11. Frecuencia del mantenimiento P/C

Análisis e Interpretación. El 4% ha manifestado que se ha realizado el mantenimiento de equipos con una frecuencia bimestral, el 15% mencionó que se ha realizado con una frecuencia trimestral, el 15% con una frecuencia semestral, el 15% manifestó que se realiza con una frecuencia anual, el 37% mencionó que nunca se ha realizado este procedimiento y finalmente el 13% manifestó que el mantenimiento es realizado cuando el usuario interno lo solicita.

4. ¿Ha sido informado con anterioridad acerca de los mantenimientos preventivo y/o correctivo en el equipo que ocupa?

Tabla 16. Información sobre mantenimiento P/C

	Cantidad	Porcentaje
Sí	8	17%
No	38	83%
Total	46	100%

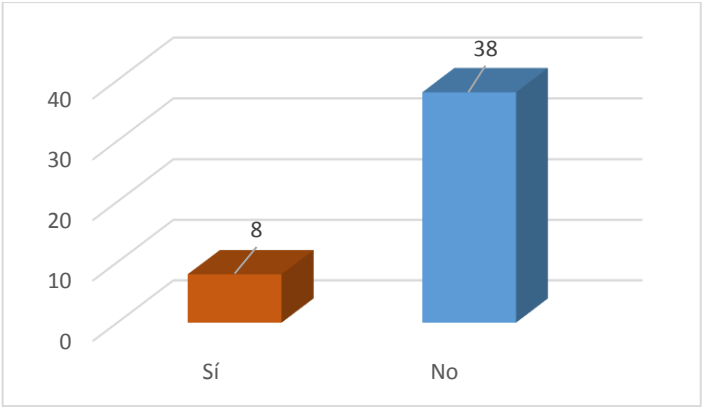


Figura 12. Información sobre mantenimiento P/C

Análisis e Interpretación. El 17% de los encuestados manifestó que, si han sido informados acerca de los mantenimientos realizados, mientras el 83% manifestó que no han sido informados sobre este hecho, es decir no se informa con anterioridad sobre los mantenimientos preventivos y/o correctivos los equipos institucionales.

4.1 ¿Conoce usted si se lleva un registro de las acciones realizadas en el mantenimiento sobre el equipo informático que utiliza?

Tabla 17. Bitácora de mantenimiento P/C

	Cantidad	Porcentaje
Sí	3	7%
No	43	93%
Total	46	100%

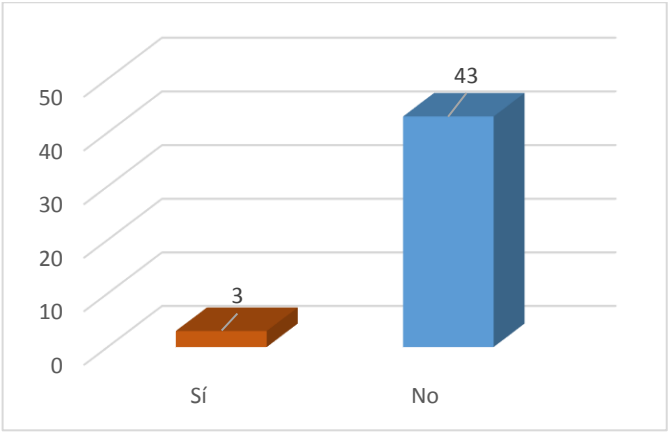


Figura 13. Bitácora de mantenimiento P/C

Análisis e Interpretación. El 7% de los encuestados manifestó que si conoce sobre el registró de acciones en los mantenimientos realizados, mientras el 93% mencionó que no tiene conocimiento sobre este procedimiento, es decir los usuarios internos desconocen sobre el registro de acciones en los diferentes tipos de mantenimientos que se realizan.

SERVICIO DE INTERNET

5. ¿Para el cumplimiento de sus funciones, necesita de servicio de Internet?

Tabla 18. Uso del servicio de internet

	Cantidad	Porcentaje
Sí	46	100%
No	0	0%
Total	46	100%

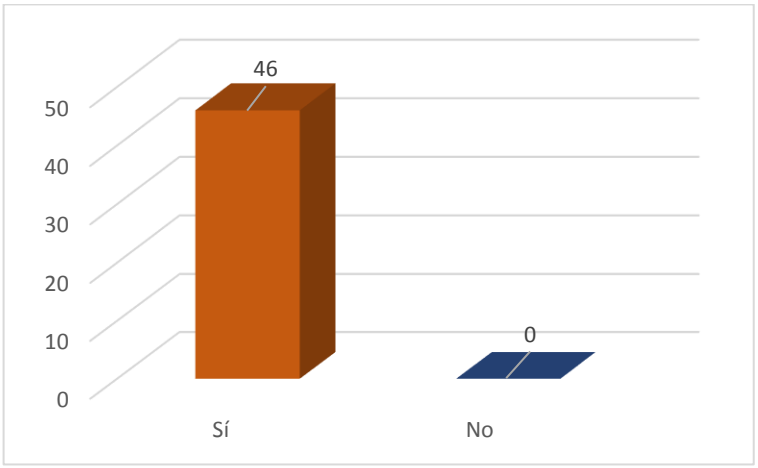


Figura 14. Uso del servicio de internet

Análisis e Interpretación. El 100% de los encuestados, ha manifestado que necesita del servicio de internet, para el desarrollo de funciones y actividades

5.1 ¿Cómo califica usted el servicio de internet?

Tabla 19. Calificación del servicio de internet.

	Cantidad	Porcentaje
Excelente	0	0%
Muy Bueno	14	30%
Bueno	23	50%
Regular	8	17%
Malo	1	2%
Total	46	100%

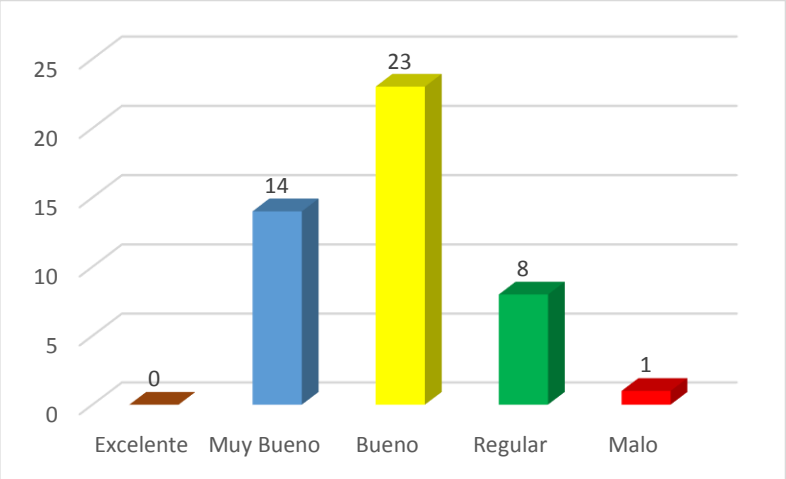


Figura 15. Calificación del servicio de internet.

Análisis e Interpretación. El 30% del total de encuestados calificó el servicio de internet como muy bueno, el 50% como bueno, el 17% calificó el servicio como regular y el 2% calificó al servicio de internet como malo, los usuarios internos consideran que el servicio de internet cumple con las características necesarias para el desarrollo de funciones y actividades.

6. ¿Conoce usted si el servicio de internet tiene políticas de restricción institucionales?

Tabla 20. Políticas de restricción institucional.

	Cantidad	Porcentaje
Sí	4	9%
No	42	91%
Total	46	100%

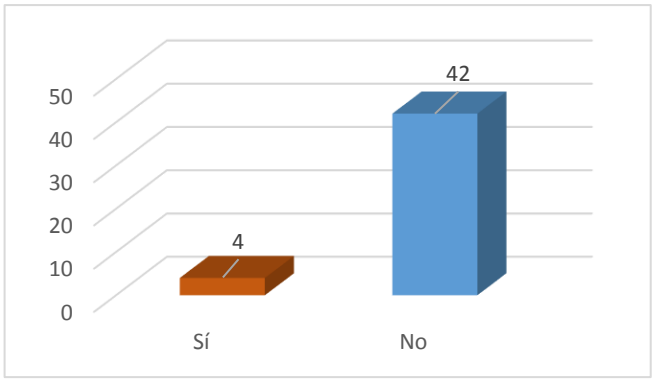


Figura 16. Políticas de restricción institucional.

Análisis e Interpretación. El 9 % de los encuestados conocía sobre políticas de restricción en el servicio de internet, mientras el 91% manifestó que no tiene conocimiento sobre este hecho. Mediante entrevistas, el Supervisor Informático manifestó que anteriormente se había implementado políticas de restricción de acceso a internet. Sin embargo, en la actualidad existen un acceso libre para todos los usuarios internos.

6.1 Marque las restricciones que usted ha identificado

Tabla 21. Restricciones identificadas.

	Cantidad	Porcentaje
Facebook	3	7%
Twiter	0	0%
Youtube	3	7%
Horas	1	2%
Otras	0	0%

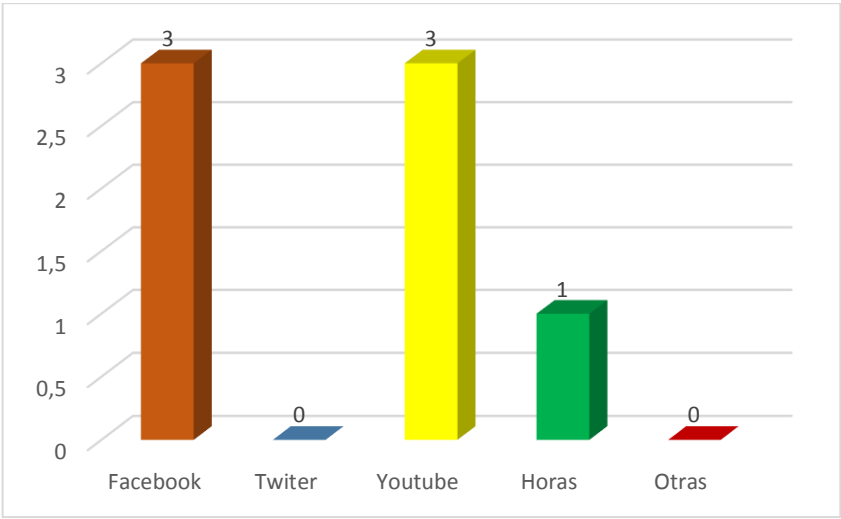


Figura 17. Restricciones identificadas.

Análisis e Interpretación. El 7% de los encuestados ha identificado que existe restricción de acceso a la red social Facebook, el 7% ha identificado restricción de acceso a la plataforma Youtube, mientras el 2% identificó que existe restricción de acceso en horas definidas.

SISTEMA INFORMÁTICO

7. Para el desarrollo de sus funciones y actividades. ¿Usted hace uso de un sistema y/o aplicativo informático?

Tabla 22. Uso del sistema informático

	Cantidad	Porcentaje
Sí	46	100%
No	0	0%
Total	46	100%

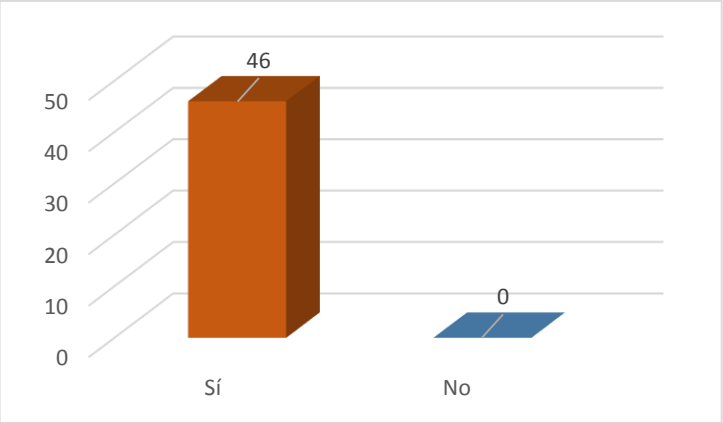


Figura 18. Uso del sistema informático.

Análisis e Interpretación. El 100% de la totalidad de encuestados, ha manifestado que usan un sistema y /o aplicativo informático, para el desarrollo de sus actividades.

7.1 ¿Cuál o cuáles sistemas y/o aplicativos utiliza?

Tabla 23. Sistemas y/o aplicativos utilizados

	Cantidad	Porcentaje
SIIM	17	37%
MEGAN	7	15%
App de Lectura	11	24%
Microsoft Office	34	74%
AUTOCAD	8	17%
PROEXCEL	7	15%
QGIS	2	4%
LEXIS	1	2%

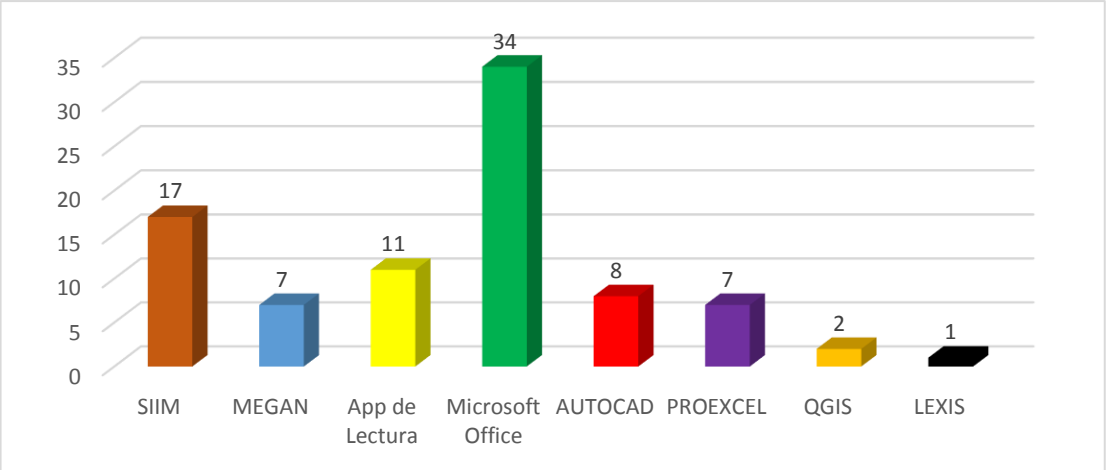


Figura 19. Sistemas y/o aplicativos utilizados

Análisis e Interpretación. El 37% de los encuestados usa el sistema informático SIIM, el 15% manifestó que utiliza el Sistema MEGAN, el 24% usa el aplicativo móvil de lectura, el 74% mencionó que usan el aplicativo ofimático Microsoft Office, el 17% usa el aplicativo AUTOCAD, el 15% utiliza el aplicativo PROEXCEL, el 4% usa el aplicativo de georreferenciación denominado QGIS y finalmente el 2% utiliza el aplicativo en línea denominado LEXIS enfocado a tareas de documentación legal.

7.2 ¿Dentro del proceso de inducción al cargo, ha recibido capacitación para el uso de los sistemas informáticos que utiliza?

Tabla 24. Capacitación para los sistemas y/o aplicativos

	Cantidad	Porcentaje
Sí	17	37%
No	29	63%
Total	46	100%

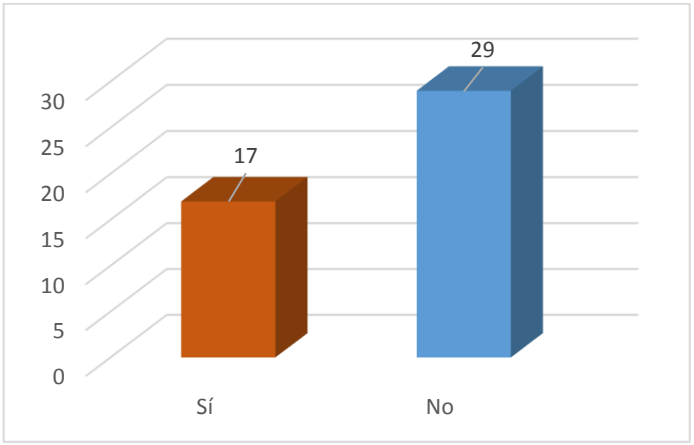


Figura 20. Capacitación para los sistemas y/o aplicativos

Análisis e Interpretación. El 37% de los encuestados mencionó que, si ha recibido inducción, mientras el 63% ha manifestado que no ha participado en procesos de inducción, es decir no se ha capacitado a los usuarios internos para el manejo de los sistemas y/o aplicativos que usan en la EPMAPA-T

7.3 ¿Cuáles sistemas y/o aplicativos ha recibido inducción?

Tabla 25. Sistemas y/o aplicativos con capacitación

	Cantidad	Porcentaje
SIIM	4	9%
MEGAN	3	7%
App de Lectura	4	9%
Microsoft Office	6	13%
AUTOCAD	3	7%
PROEXCEL	3	7%
QGIS	1	2%
LEXIS	0	0%

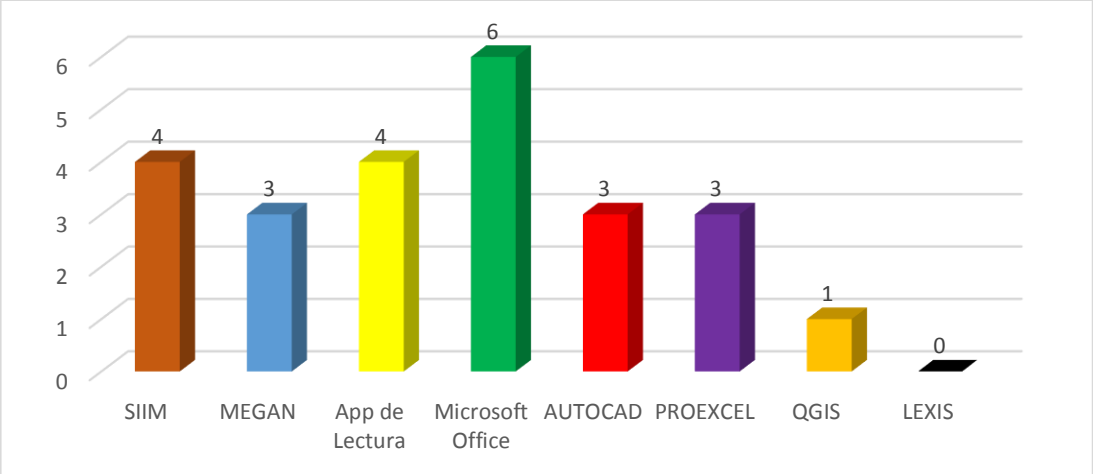


Figura 21. Sistemas y/o aplicativos con capacitación

Análisis e Interpretación. El 9% del total de encuestados ha manifestado que ha recibido inducción para el uso del Sistema SIIM, el 7% manifestó que ha recibido inducción para el sistema MEGAN, el 9% mencionó que se ha recibido inducción para el uso del aplicativo móvil de lectura, el 13% mencionó que ha recibido inducción para el uso del aplicativo ofimático Microsoft Office, el 7 % ha recibido inducción para el uso del aplicativo AUTOCAD, el 9% ha recibido inducción para el uso del Aplicativo PROEXCEL, finalmente el 2% ha recibido inducción para el uso del aplicativo QGIS.

7.4 ¿El o los sistemas han presentado fallas?

Tabla 26. Fallas en los sistemas y/o aplicativos

	Cantidad	Porcentaje
Sí	21	46%
No	25	54%
Total	46	100%

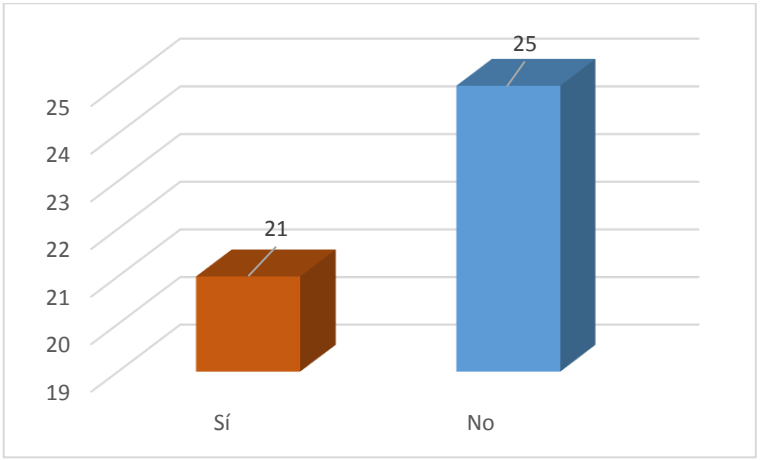


Figura 22. Fallas en los sistemas y/o aplicativos

Análisis e Interpretación. El 46% de los encuestados manifestó que, si se presenta fallas, mientras el 54% mencionó negativa ante este hecho, se puede evidenciar que las fallas en los sistemas y/o aplicativos son comunes en ciertos casos.

7.4.1 ¿Qué tipo de fallas?

Tabla 27. Fallas identificadas.

Fallas	Sistema	N° de veces
Cuadre cartera vencida	SIIM	1
Datos inconsistentes	SIIM	3
Duplicidad de procesos	SIIM	1
Inicio lento	Microsoft Office	2
Lentitud al enviar los datos	App móvil	2
Módulo de convenios con errores	SIIM	1
No se abren los archivos	Microsoft Office	2
Problemas en los reportes	SIIM	4
Programa con errores	AUTOCAD, Microsoft Office	1
Reinicios inesperados	Microsoft Office	1
Reportes inconsistentes	SIIM	2
Sistema es lento	SIIM, AUTOCAD	1
Total		21

Análisis e Interpretación. El sistema con mayor cantidad de fallas fue el Sistema SIIM, mismo que se utiliza en los Direcciones de Gestión Financiera y Comercialización, y presenta diversas fallas. Por otra parte, el aplicativo con mayor cantidad de fallas fue el aplicativo ofimático de Microsoft Office con inconvenientes en el proceso de funcionamiento.

7.4.2 ¿Con que frecuencia se presentan las fallas?

Tabla 28. Frecuencia de las fallas.

	Cantidad	Porcentaje
Diario	3	7%
Semanal	4	9%
Mensual	13	28%
Anual	1	2%
Nunca	0	0%
Total	21	46%

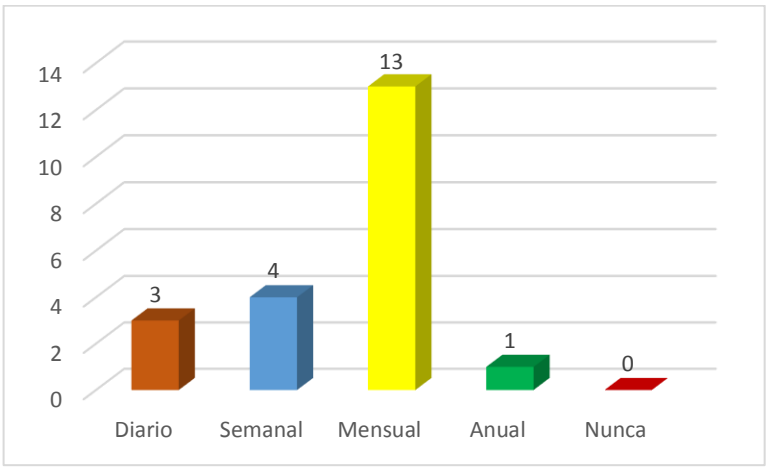


Figura 23. Frecuencia de fallas

Análisis e Interpretación. El 7% de los encuestados, indicó que las fallas se presentan a diario, el 9% indicó que se presentan de manera semanal, el 28% indicó que se presentan con una frecuencia mensual, finalmente el 2% manifestó que las fallas se presentan con una frecuencia anual.

SEGURIDAD Y CONTRASEÑAS

8. ¿Usted utiliza contraseñas para el acceso a los sistemas y/o servicios informáticos de la EPMAPA-T?

Tabla 29. Uso de las contraseñas para acceder a sistemas y/o servicios

	Cantidad	Porcentaje
Sí	37	80%
No	9	20%
Total	46	100%

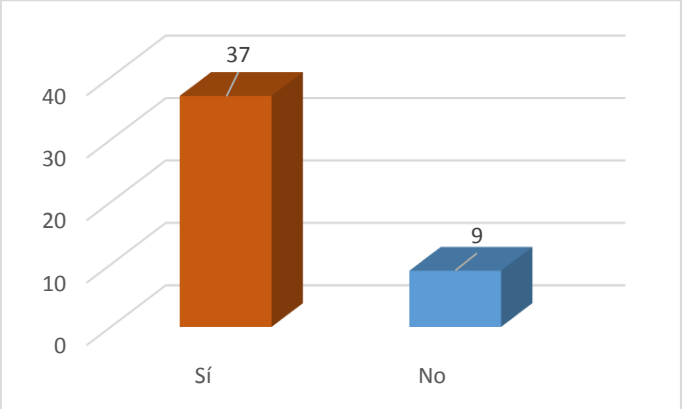


Figura 24. Uso de las contraseñas para acceder a sistemas y/o servicios

Análisis e Interpretación. El 80% de los encuestados mencionó que utiliza contraseñas de acceso, y el 20% manifestó que no usa contraseñas, es decir la mayoría de usuarios internos usan una contraseña para acceder a los sistemas y/o servicios informáticos de la EPMAPA-T.

8.1 ¿Para cuáles sistemas y /o servicios informáticos usa contraseñas?

Tabla 30. Sistemas y/o servicios informáticos.

Servicios	N°	Porcentaje
App móvil	5	11%
Archivos con contraseña	1	2%
Contraloría	2	4%
Correo Electrónico	8	17%
MEGAN	5	11%
Páginas de Ministerio	1	2%
SIIM	14	30%
Banco Central	1	2%
Total	37	80%

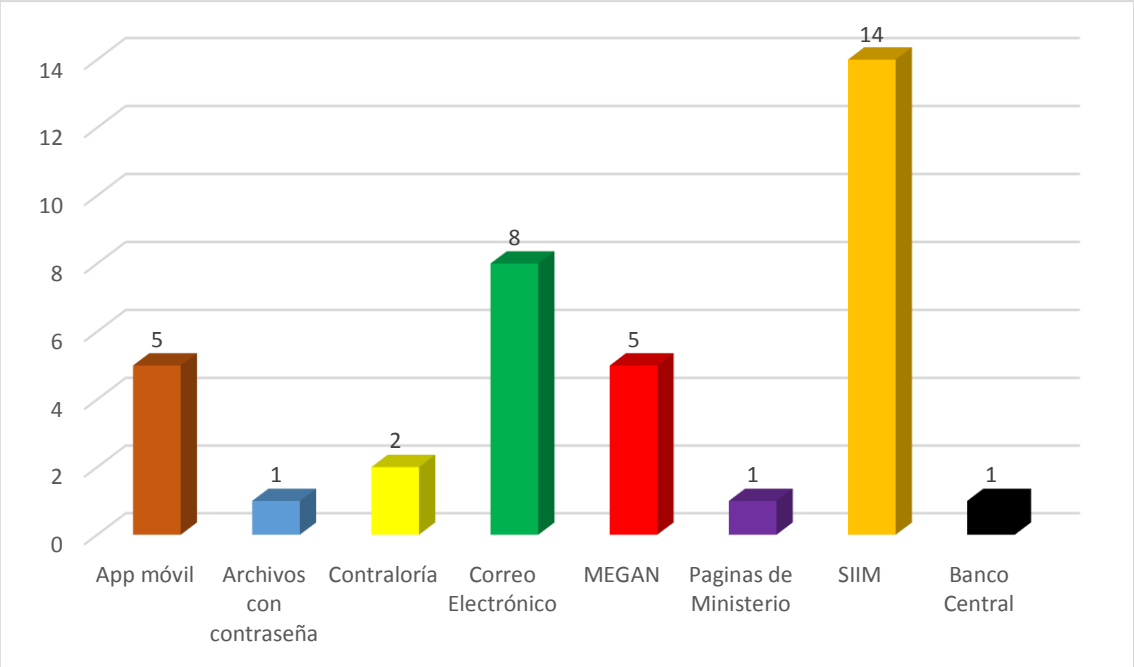


Figura 25. Sistemas y/o servicios informáticos.

Análisis e Interpretación. El 11% de encuestados manifestó que usa contraseñas para acceder al aplicativo móvil de lectura, el 2% usa contraseñas para proteger archivos, el 4% usa contraseñas de acceso a sistema de Contraloría, el 17 % usa contraseñas de acceso al Correo electrónico institucional, el 11% usa contraseñas para acceso al Sistema MEGAN, el 2% para acceder a páginas del ministerio y Banco Central, y finalmente el 30% que usa contraseñas para acceder al Sistema SIIM.

8.2 ¿Con que frecuencia se realiza el cambio de contraseñas, en los sistemas y /o servicios informáticos?

Tabla 31. Frecuencia de cambio de contraseñas

	Cantidad	**Porcentaje**
Trimestral	7	15%
Semestral	5	11%
Anual	9	20%
Nunca	16	35%
Total	37	80%

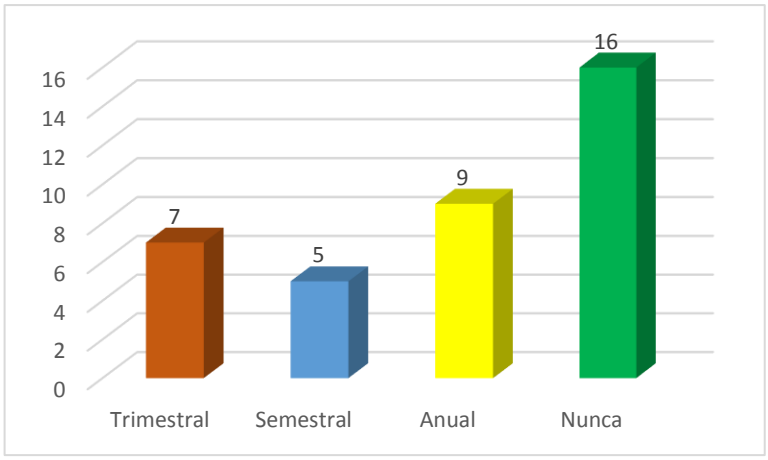


Figura 26. Frecuencia de cambio de contraseñas

Análisis e Interpretación. El 15% de los encuestados, realiza el cambio de contraseñas con una frecuencia trimestral, el 11% con una frecuencia semestral, el 20% con una frecuencia anual y finalmente el 35% nunca realiza cambio de contraseñas en los sistemas y/o servicios informáticos institucionales.

8.3 El cambio de contraseña se realiza por:

Tabla 32. Motivo del cambio de contraseñas

	Cantidad	Porcentaje
Decisión Personal	30	65%
Por solicitud del sistema	2	4%
Por política de seguridad	5	11%
Total	37	80%

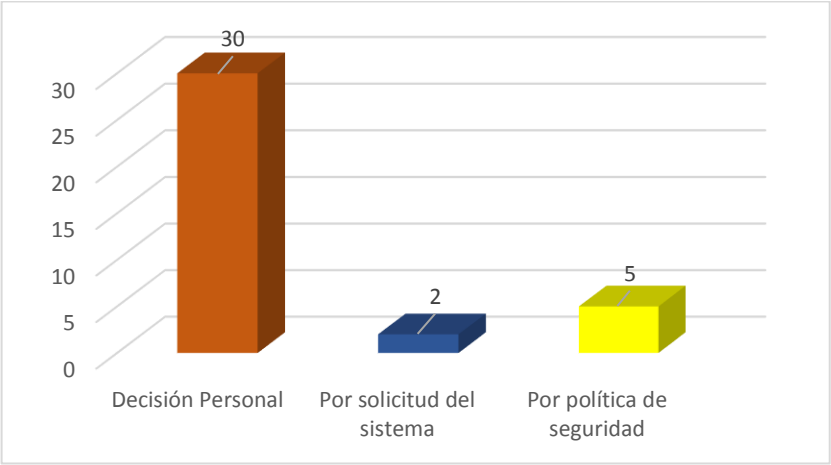


Figura 27. Motivo del cambio de contraseñas

Análisis e Interpretación. El 65% indicó que cambia sus contraseñas por decisión personal, el 4% cambia sus contraseñas por solicitud del sistema y el 11% cambia sus contraseñas por

políticas de seguridad. Los usuarios internos generalmente cambian sus contraseñas por decisión personal, lo que permite identificar que no se han establecido políticas que rijan este procedimiento.

9. ¿Usted utiliza contraseñas para el acceso al equipo informático qué usa?

Tabla 33. Uso de contraseñas para acceder al equipo

	Cantidad	Porcentaje
Sí	34	74%
No	12	26%
Total	46	100%

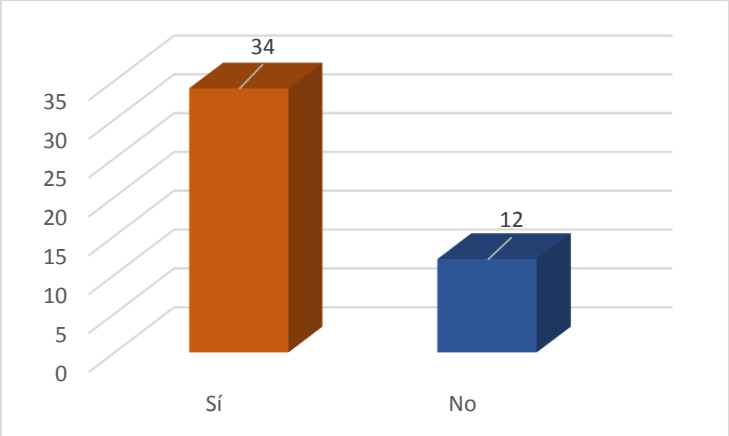


Figura 28. Uso de contraseñas para acceder al equipo

Análisis e Interpretación. El 74% manifestó que usa contraseñas para el acceso al equipo informático, mientras el 26% mencionó que no usa contraseñas de acceso, es decir la mayoría de usuarios internos han establecido una contraseña de acceso al equipo, generando un mayor nivel de seguridad a la información.

9.1 ¿Con que frecuencia se realiza el cambio de contraseñas, para acceso al equipo informático?

Tabla 34. Frecuencia de cambia de contraseñas para el equipo.

	Cantidad	Porcentaje
Trimestral	5	11%
Semestral	6	13%
Anual	11	24%
Nunca	12	26%
Total	34	74%

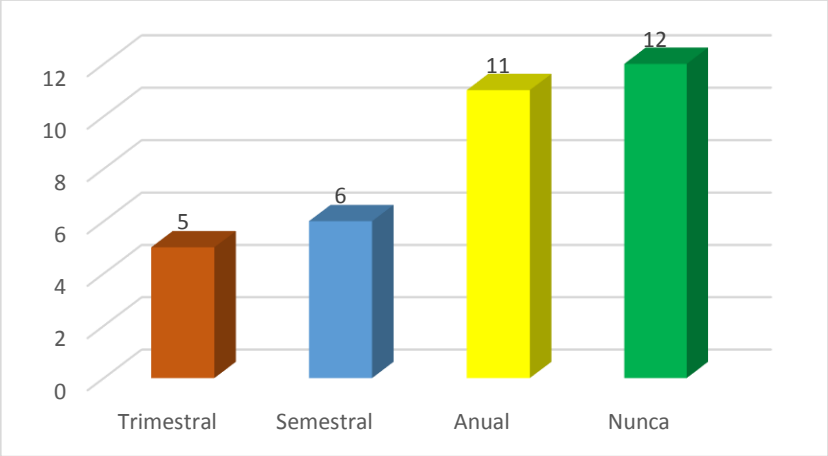


Figura 29. Frecuencia de cambia de contraseñas para el equipo.

Análisis e Interpretación. El 11% de los encuestados indicó que realiza un cambio de contraseñas con una frecuencia trimestral, el 13% de manera semestral, el 24% con una frecuencia anual, y el 26% nunca cambia su contraseña de acceso al equipo informático.

9.2 El cambio de contraseña se realiza por:

Tabla 35. Motivo de cambio de contraseña

	Cantidad	Porcentaje
Decisión Personal	27	59%
Por solicitud del equipo	0	0%
Por política de seguridad	7	15%
Total	34	74%

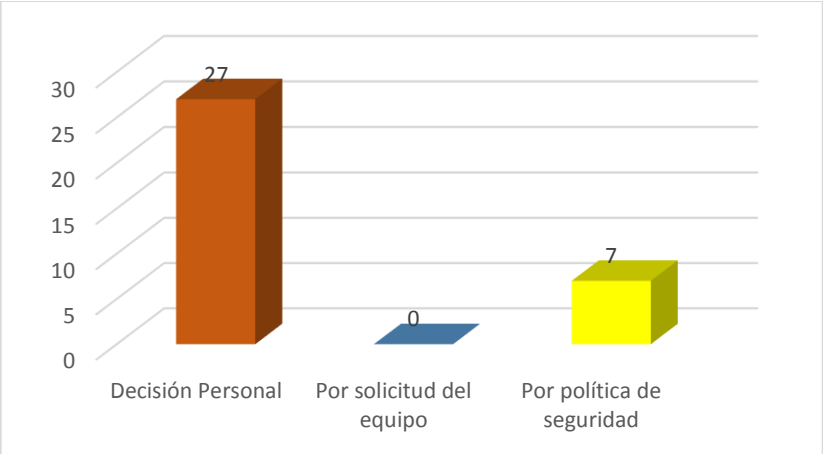


Figura 30. Motivo de cambio de contraseña

Análisis e Interpretación. El 59% mencionó que cambia su contraseña de acceso al equipo informático por decisión personal, y el 15% realiza el cambio debido a políticas de seguridad, es decir el DSI no se estipula una política que indique la frecuencia de cambia de contraseñas de acceso a equipos institucionales, delegando dicha responsabilidad al usuario interno.

10. ¿Cuál es la manera en la usted protege las contraseñas, para los equipos o Sistemas que dispone la EPMAPA-T?

Tabla 36. Protección de las contraseñas

	Cantidad	Porcentaje
Memoriza	33	72%
Notas personales	12	26%
Otro	1	2%
Total	46	100%

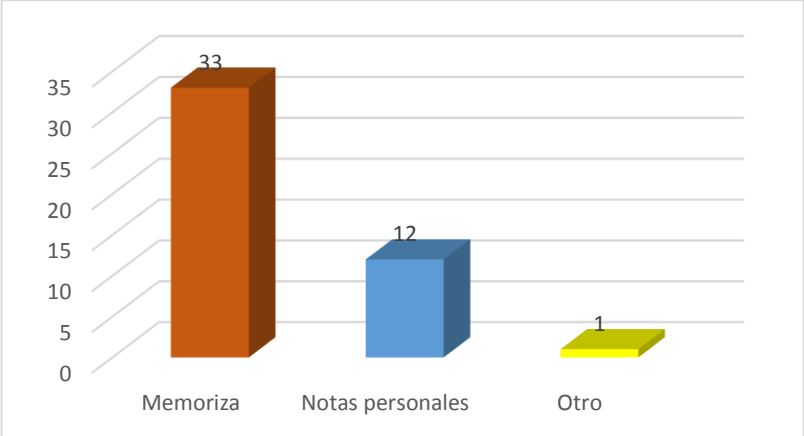


Figura 31. Protección de las contraseñas

Análisis e Interpretación. El 72% de la muestra manifestó que memoriza sus contraseñas, el 26% indicó que las protege escritas en notas personales, el 2% manifestó que disponía de un llave o código para acceso. Al memorizar las contraseñas existen mayor nivel de seguridad, de esta manera el acceso a las claves es restringido.

11. De las siguientes opciones, cuál o cuáles cumplen con la política de contraseñas establecida por la institución: (*varias opciones en caso que aplique*)

Tabla 37. Parámetros de contraseñas

	Cantidad	Porcentaje
Mayúsculas	19/46	41%
Minúsculas	36/46	78%
Números	27/46	59%
Caracteres Especiales	4/46	9%
Mínimo ocho caracteres	16/46	35%

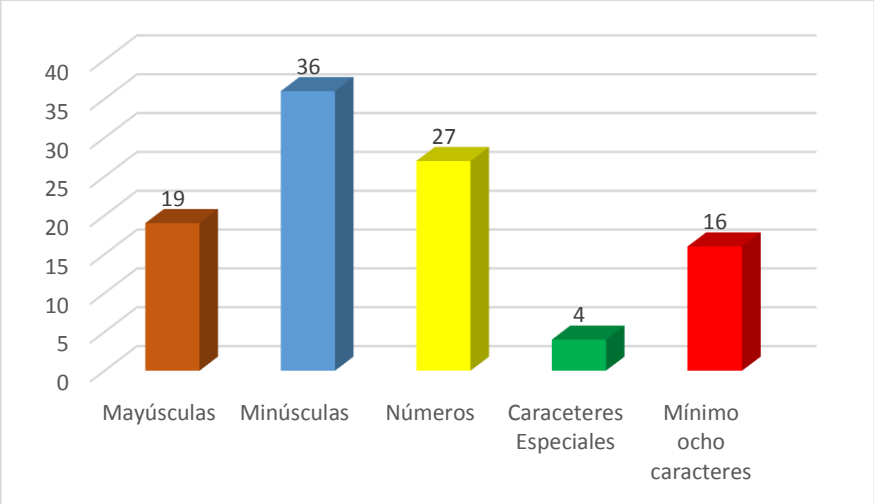


Figura 32. Parámetros de contraseñas

Análisis e Interpretación. De 46 encuestados 19 mencionó que usa mayúsculas en su contraseña, 36/46 usa minúsculas en sus contraseñas, 27/46 tiene una contraseña que contiene números, 4/46 tiene contraseñas con caracteres especiales, finalmente 16/46 de la muestra cumple con mínimo ocho caracteres en sus contraseñas.

CALIFICACIÓN DEL SERVICIO

12. ¿Con qué frecuencia solicita soporte al DSI de la EPMAPA-T?

Tabla 38. Frecuencia de solicitud de soporte.

	Cantidad	Porcentaje
1 a 5 días	6	13%
6 a 15 días	3	7%
16 a 30 días	5	11%
Mayor a un mes	24	52%
Nunca	8	17%
Total	46	100%

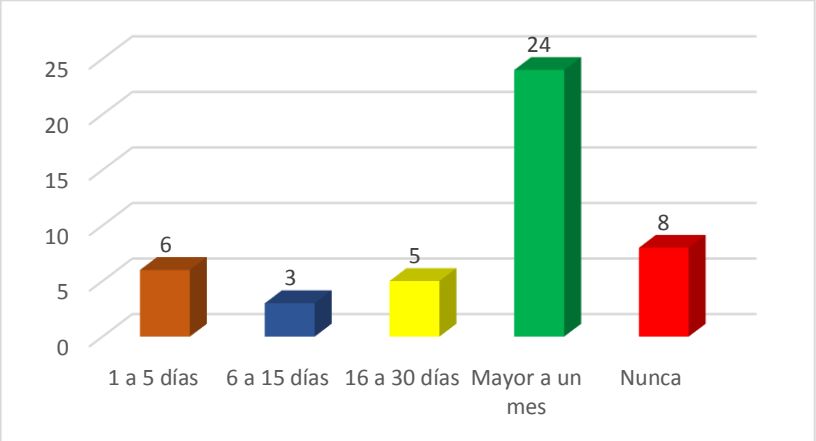


Figura 33. Frecuencia de solicitud de soporte

Análisis e Interpretación. El 13% indicó que solicita soporte al DSI con una frecuencia de 1 a 5 días, el 7% con una frecuencia de 6 a 15 días, el 11% con una frecuencia de 16 a 30 días, el 52% solicita soporte con una frecuencia mayor a un mes, mientras el 17% manifestó que nunca ha solicitado soporte. Se puede evidenciar que existe un porcentaje mayor al 50% que ha solicitado servicios al DSI con una frecuencia mayor a un mes, lo que indica que no ha sido necesaria la intervención de los técnicos en los equipos institucionales por lapsos prolongados de tiempo.

13. ¿El DSI, le ha informado a usted acerca de los tiempos de respuesta a una solución en caso de los siguientes problemas?

Tabla 39. Información problemas.

	Cantidad	Porcentaje
Problemas críticos	10	22%
Problemas altos	5	11%
Problemas medios	12	26%
Problemas bajos	13	28%

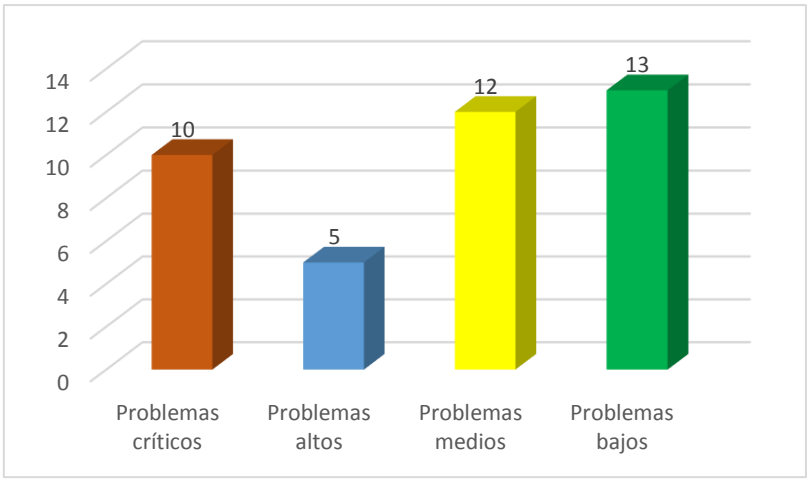


Figura 34. Información problemas**.**

Análisis e Interpretación. El 22% de los encuestados ha sido informado sobre los tiempos de respuesta en problemas críticos, el 11% en el caso de problemas altos, el 26% en problemas medios y el 28% el caso de problemas bajos.

13.1 ¿El DSI ha cumplido con los tiempos de solución estipulados?

Tabla 40. Cumplimiento de tiempos de solución

	Cantidad	Porcentaje
Si	19	41%
No	8	17%
Total	27	59%

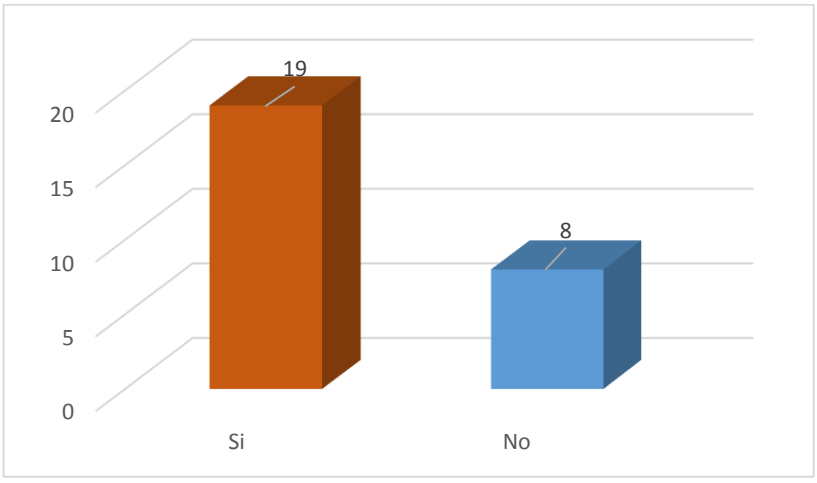


Figura 35. Cumplimiento de tiempos de solución

Análisis e Interpretación. El 41% del total de encuestados, manifestó que el DSI, ha cumplido con tiempos de solución estipulados en los problemas de determinado tipo y criticidad, mientras en el 17% ha manifestado que no se ha cumplido con los tiempos estipulados. El DSI ha cumplido con los tiempos de respuesta indicados al usuario interno.

13.2 En caso de que se supere los tiempos de solución. ¿Cuáles son las acciones que toma el DSI?

Tabla 41. Acciones que lleva a cabo el DSI

Acciones	N°
Llevar el equipo a lugares externos	3
Poner a punto con los respaldos	1
Se retrasan los tiempos de entrega	1
Sugiere usar el equipo personal	3
Intercambian el equipo	2

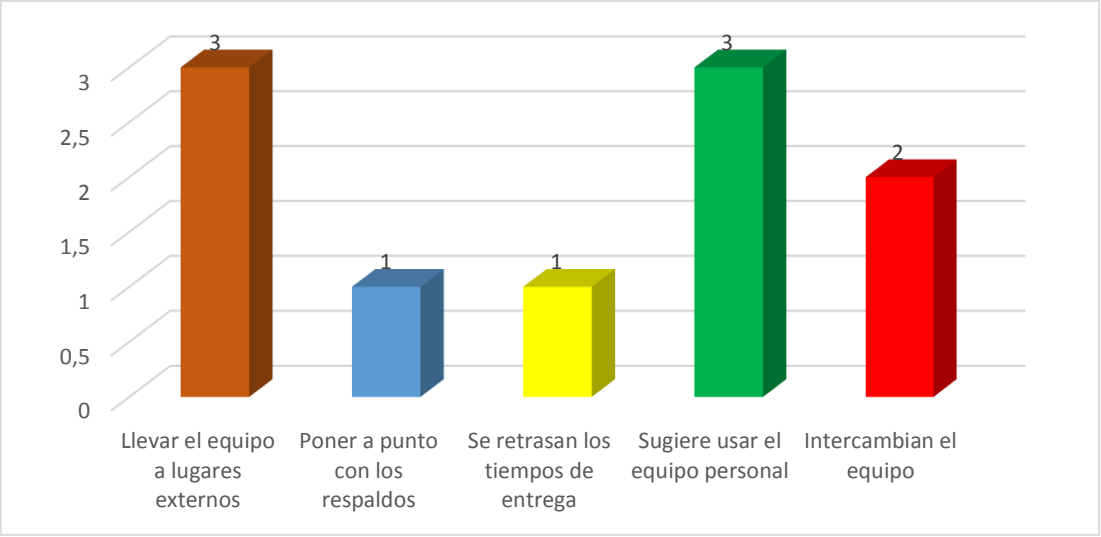


Figura 36. Acciones que lleva a cabo el DSI

Análisis e Interpretación. Dentro de las acciones que toma el DSI, el usuario mencionó que ha identificado que en ocasiones se lleva el equipo a lugares externos, en ocasiones la falla supera el tiempo de respuesta por lo que se sugiere trabajar un equipo personal temporalmente, en cambio para los usuarios internos que se dedican a tareas de recaudación el equipo con falla es reemplazado, tomando en cuenta que este procedimiento nunca debe ser paralizado.

13.3 ¿Cuál ha sido el tiempo máximo de respuesta del DSI a la solicitud de atención técnica, en relación a la criticidad del problema?

Tabla 42. Tiempos de solución

	Problemas críticos	Problemas altos	Problemas medios	Problemas bajos
1 a 15 min	1	1	3	7
16 a 30 min		1	4	6
31 a 45 min	1		1	2
46 a 60 min		1	6	
Mas de 60 min	17	12	5	3
Total	19	15	19	18

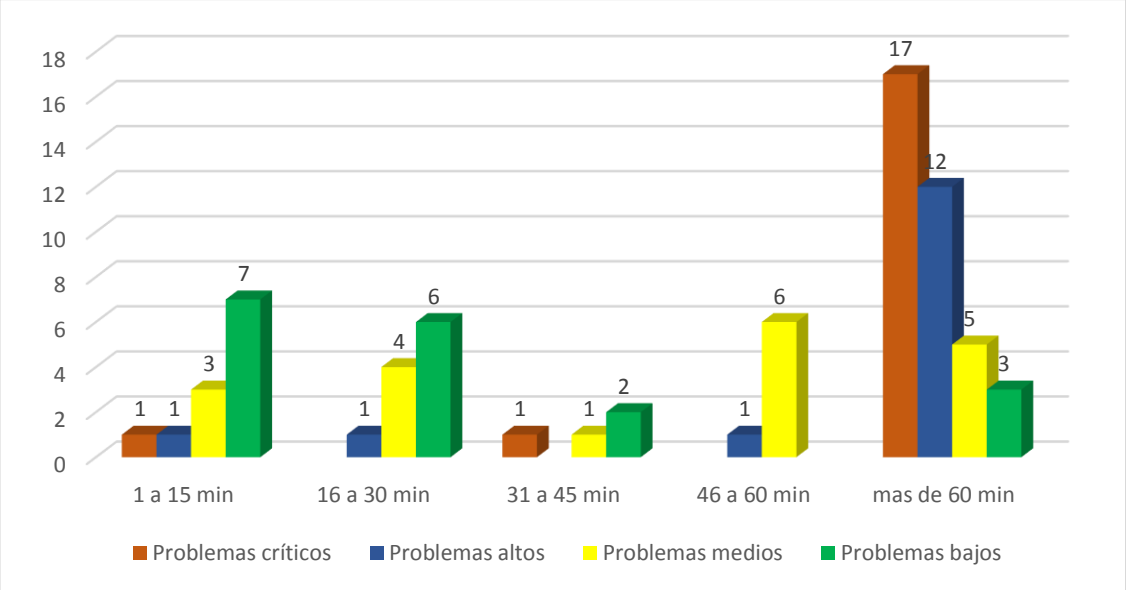


Figura 37. Tiempos de solución

Análisis e Interpretación. Los problemas críticos y altos generalmente superan un tiempo de respuesta mayor a 60 minutos, los problemas de carácter medio son resueltos en un tiempo de 46 a 60 minutos, y los problemas de carácter bajo generalmente son resueltos de 1 a 15 minutos.

14. ¿Existe un método para medir la calidad del servicio prestado por el DSI?

Tabla 43. Calidad del servicio prestado por el DSI

	Cantidad	Porcentaje
Si	3	7%
No	43	93%
Total	46	100%

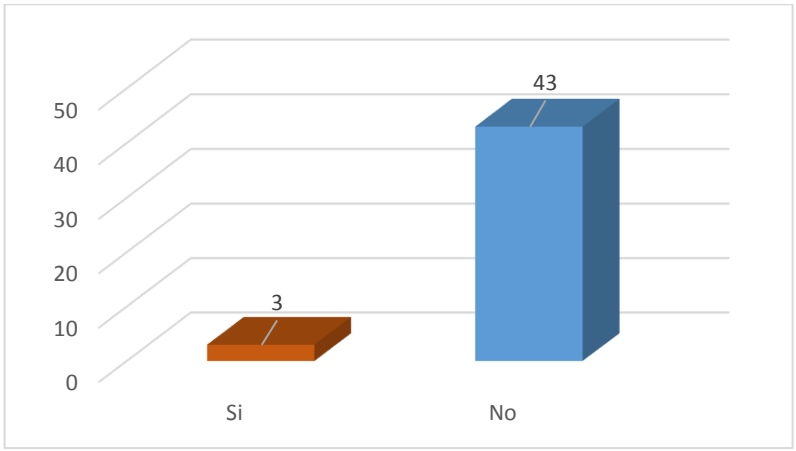


Figura 38. Calidad del servicio prestado por el DSI

Análisis e Interpretación. El 7% de los encuestados indicó que sí existe un método para medir la calidad del servicio prestado, mientras el 93% manifestó que no, es decir aún no se ha trabajo en niveles de servicio al usuario interno.

15. ¿Cómo califica el servicio brindado por el DSI de la EPMAPA-T?

Tabla 44. Calificación del servicio brindado por el DSI

	Cantidad	Porcentaje
Excelente	1	2%
Muy Bueno	9	20%
Bueno	25	54%
Regular	9	20%
Malo	2	4%
Total	46	100%

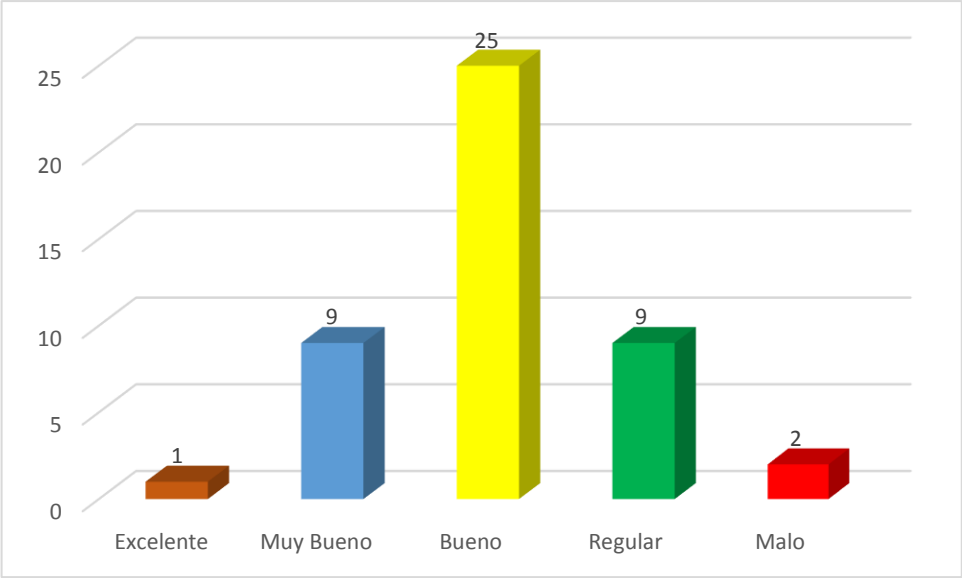


Figura 39. Calificación del servicio brindado por el DSI

Análisis e Interpretación. El 2% calificó como excelente el servicio brindado, el 20% calificó como muy bueno, el 54% calificó como bueno, el 20% calificó como regular y el 4% calificó como malo. Se considera que el servicio prestado por el DSI, generalmente es bueno y cumple con lo estipulado en las funciones y atribuciones del departamento.

Resultado Entrevistas

Las entrevistas fueron realizadas a los responsables de las Áreas de Gestión y Gobierno de TI, tal como lo indica el marco referencial de COBIT® 5, las mismas que se detallan a continuación:

Área de Gestión de TI: corresponde al personal del Departamento de Supervisión Informática, conformado por: Supervisor Informático y Analista de Sistemas. Los resultados de entrevista completa se encuentran en Anexo 2 y Anexo 4 respectivamente.

Área de Gobierno de TI: corresponde al Director de Gestión Administrativa.

Se ha realizado un cuadro resumen con los hallazgos relevantes, las entrevistas completas se encuentran en la sección de Anexo 3.

Entrevista al Supervisor Informático

Tabla 45. Resultados de entrevista al Supervisor Informático EPMAPA-T

Entrevista correspondiente al área de Gestión de TI			
Entrevistado	MSc. Jackson Obando		
Cargo	Supervisor Informático EPMAPA-T		
Hallazgo	**Si**	**No**	**Observaciones**
Planes de Continuidad de Negocio en el marco de TI		X	EPMAPA-T no ha generado un plan de continuidad de negocio enmarcado en el área de TI.
Planes de Disponibilidad de Negocio en el marco de TI		X	EPMAPA-T no ha desarrollado planes de disponibilidad de negocio.
Planes de mejora TI en el DSI EPMAPA-T		X	Exclusivamente se ha trabajado en planes de mejora del activo de TI, enfocado a renovar computadores que cumplieron su vida útil.
Planes de aseguramiento de TI en el DSI		X	EPMAPA-T no ha generado planes que permitan el aseguramiento de TI.
Marco de referencia implementado en el DSI que regule los procesos y recursos de TI		X	Regularmente el DSI, se somete a una auditoría general por cambio de autoridades, y se considera que debe cumplir con las leyes que rigen a las empresas públicas. Sin embargo, el área de TI no se alinea a una metodología específica.
Estudio de riesgos vinculados a TI		X	EPMAPA-T no ha trabajado, en gestión de riesgos de TI de ningún tipo.

Manual de procesos internos y externos en DSI	X	El Supervisor Informático ha manifestado que el manual de procesos institucional se encuentra a cargo de una consultora externa, por lo que aún no se cuenta con este documento.
Objetivos para alcanzar la mejora de los procesos de TI	X	El DSI no ha trabajado en objetivos de mejora debido a la inexistencia del manual de procesos.
Políticas de seguimiento al cumplimiento de los procesos de TI.	X	El DSI no ha establecido políticas de verificación, debido a la inexistencia de manual de procesos.
Políticas de servicio al usuario interno en la EPMAPA-T de acuerdo con las TI.	X	El DSI no ha establecido políticas de servicio al usuario interno.
Políticas de control interno informático.	X	EPMAPA-T no ha establecido políticas de control interno informático.
Catálogo de servicios internos y externos de TI.	X	Existe un catálogo único de servicio institucionales,

Entrevista al Analista de Sistemas

Tabla 46. Resultados de entrevista al Analista de Sistemas EPMAPA-T

Entrevista correspondiente al área de Gestión de TI	
Entrevistado	Ing. Alexis Sánchez
Cargo	Analista de Sistemas EPMAPA-T
Hallazgos	**Observaciones**
Talento humano y la difusión de políticas y normas de ética – comportamiento hacia el DSI	El Analista de sistemas conoce las normas de ética - comportamiento mediante una revisión del documento respectivo.
En caso de inasistencia a la Empresa. ¿Quién asume sus funciones?	Se ha manifestado que el Supervisor Informático, es quién asume las funciones y actividades, debido a que una plaza de Analista de Sistemas no ha sido cubierta. Sin embargo, el entrevistado considera el equipo de trabajo puede cumplir con las funciones adecuadamente

Dirección de Gestión Administrativa ha definido los procesos exclusivos para el área de TI	El profesional entrevistado desconoce el trabajo de la Dirección de Gestión Administrativa en los procesos del área de TI.
Dirección de Gestión Administrativa ha trabajado en procedimientos, vinculados a la Gestión de riesgos de TI.	El profesional entrevistado desconoce el trabajo en gestión de riesgos de TI, por Dirección de Gestión Administrativa.
Presupuesto y frecuencia de asignación	Existe una asignación presupuestaria, la misma que se contempla con una frecuencia de asignación anual, registrada en el Plan Operativo Anual (POA) 2019.
Áreas que se deben fortalecer con la asignación presupuestaria en el DSI.	El entrevistado considera que el área con mayor nivel de prioridad es Seguridad Informática.
Participación en proyectos de mejora vinculado a soluciones tecnológicas en la EPMAPA-T	El entrevistado ha manifestado que no se ha trabajado hasta el momento en proyectos de mejora de ningún tipo
Mantenimiento de equipos	Se ha manifestado, que se brinda mantenimiento correctivo y preventivo con una frecuencia trimestral, y se lleva un registro mediante informe que se entrega a Dirección de Gestión Administrativa.
Procedimiento para la atención al usuario interno	Hasta el momento no se ha trabajado en el procedimiento de atención al usuario interno.
Control Interno y seguimiento.	El control interno del DSI, se realiza mediante actas que se entregan al bodeguero, el mismo que realiza un control de materiales entregados.
Auditoría Informática en el DSI.	El DSI, se ha sometido a auditorías en ocasiones anteriores. Sin embargo, no se cuenta con la información acerca de hallazgos y recomendaciones efectuadas debido a que ellas son de conocimiento exclusivo del Supervisor Informático.

Entrevista al Director de Gestión Administrativa

Tabla 47. Resultados entrevista al Director de Gestión Administrativa EPMAPA-T

Entrevista correspondiente al área de Gobierno de TI			
Entrevistado	Ing. Andrés Velasco		
Cargo	Director de Gestión Administrativa EPMAPA-T		
Hallazgo	**Cumple**	**No cumple**	**Observaciones**
Manual de procesos internos y externos de negocio		X	El manual de procesos institucional se encuentra a cargo de una consultora externa, por lo que aún no se cuenta este documento.
Marco de referencia implementado en la EPMAPA-T que regule los procesos y recursos de TI		X	El entrevistado desconoce del tema, debido a que el DSI, en encarga de su propia regulación.
Seguridad de Información		X	En la presente administración, no se ha trabajado en aspectos relacionados con seguridad de la información.
Gestión de TI en la EPMAPA-T		X	EPMAPA-T no ha realizado, una evaluación de la gestión de los servicios prestados por el DSI.
Gestión de Planes, Proyectos y Programas relacionados con TI.	X		La Dirección Gestión Administrativa ha trabajado en capacitaciones al personal del DSI.
Gestión de Riesgos en el DSI	X		El entrevistado ha manifestado que, si se ha trabajado en gestión de riesgos de TI, sin embargo, no se ha documentado, el proceso y los resultados obtenidos.

Finalizado el Estudio Inicial, basado en la aplicación de técnicas de recolección de información tales como entrevistas y encuestas, se concluye que:

- Los usuarios internos no han recibido inducción para el uso de los sistemas y/o aplicativos informáticos, los conocimientos han sido adquiridos por medio de la revisión de manuales e instructivos disponibles.
- El DSI no ha establecido políticas para el uso y manejo de contraseñas, delegando responsabilidades de cambio de contraseñas y custodia a los usuarios internos.
- La mayoría de usuarios internos desconocen los procesos de mantenimiento preventivo y/o correctivo, mencionando que el DSI no ha informado con anterioridad sobre este procedimiento.
- La EPMAPA-T, cumple con sus procesos diarios sin la documentación respectiva, debido a la inexistencia del Manual de Procesos que regule el cumplimiento de las actividades y funciones encomendadas.
- La EPMAPA-T, no dispone de un Plan de Gestión de riesgos de TI, delegando toda la responsabilidad al DSI.
- La Estructura Orgánica Funcional de la EPMAPA-T, contempla dentro de su distribución para el DSI un Supervisor Informático y dos Analistas de Sistemas, por el momento el equipo de trabajo se encuentra incompleto, debido a que uno de los puestos de Analista de Sistemas no ha sido cubierto.
- Existe asignación presupuestaria anual, misma que se detalla en el POA 2019, pero a pesar de ejecutar todo el presupuesto existen temas y procesos del departamento sin atender, en especial los que surgen después de la planificación.
- No se ha realizado una evaluación de la Gestión del DSI y los servicios prestados a los usuarios internos en la EPMAPA-T.
- El control interno dentro del DSI, no se lleva a cabo, por parte de un área especializada, por el momento se trabaja mediante actas que se entregan al bodeguero, el mismo que realiza un control básico de materiales e instrumentos entregados.

4.1.4. Plan de Auditoría

4.1.4.1. Selección de procesos institucionales.

La selección de procesos se ha llevado a cabo mediante la técnica de observación directa y entrevista, los principales parámetros a tomar en cuenta fueron:

- Procesos que se vinculen al servicio prestado al usuario externo.
- Procesos que se vinculen con el área de TI.

Es por ello que del total de doce procesos que se vinculan al usuario final, cuatro se vinculan al área de TI, mismos que se detallan a continuación.

Tabla 48. Selección de procesos institucionales

Procesos vinculados al usuario externo	**Procesos vinculados a TI**
Concesión de nuevo servicio	X
Emisión	X
Refacturación	X
Reparaciones/Limpieza de sumideros	
Recolección de lecturas	X
Inspecciones Líneas de fabrica	
Operación y mantenimiento de la planta de tratamiento de agua potable	
Operación y mantenimiento de plantas de tratamiento de aguas residuales	
Operación y mantenimiento de colectores	
Soporte técnico al usuario externo	
Diseños y presupuestos hidráulicos y de saneamiento	
Levantamientos topográficos	

Una vez seleccionado los procesos institucionales, se expone la ficha de cada proceso que contiene: descripción, responsables, procesos relacionados, documentación de referencia, diagrama del proceso.

Tabla 49. Ficha Concesión de nuevo servicio.

FICHA DE PROCESO			
Proceso	Concesión de nuevo servicio.	**N°**	1
Descripción	Registrar un nuevo abonado, por concesión de agua potable y/o alcantarillado, para que el servicio sea instalado por el equipo técnico		
Responsables	• Departamento de Comercialización • Plomero • Recaudación		
Procesos relacionados	• Conexión e instalación de cometidas • Conexión de alcantarillado • Inspecciones líneas de fábrica.		
Documentación de referencia	• Reglamento de prestación de servicios EPMAPA-T 2015.		
Diagrama de proceso			

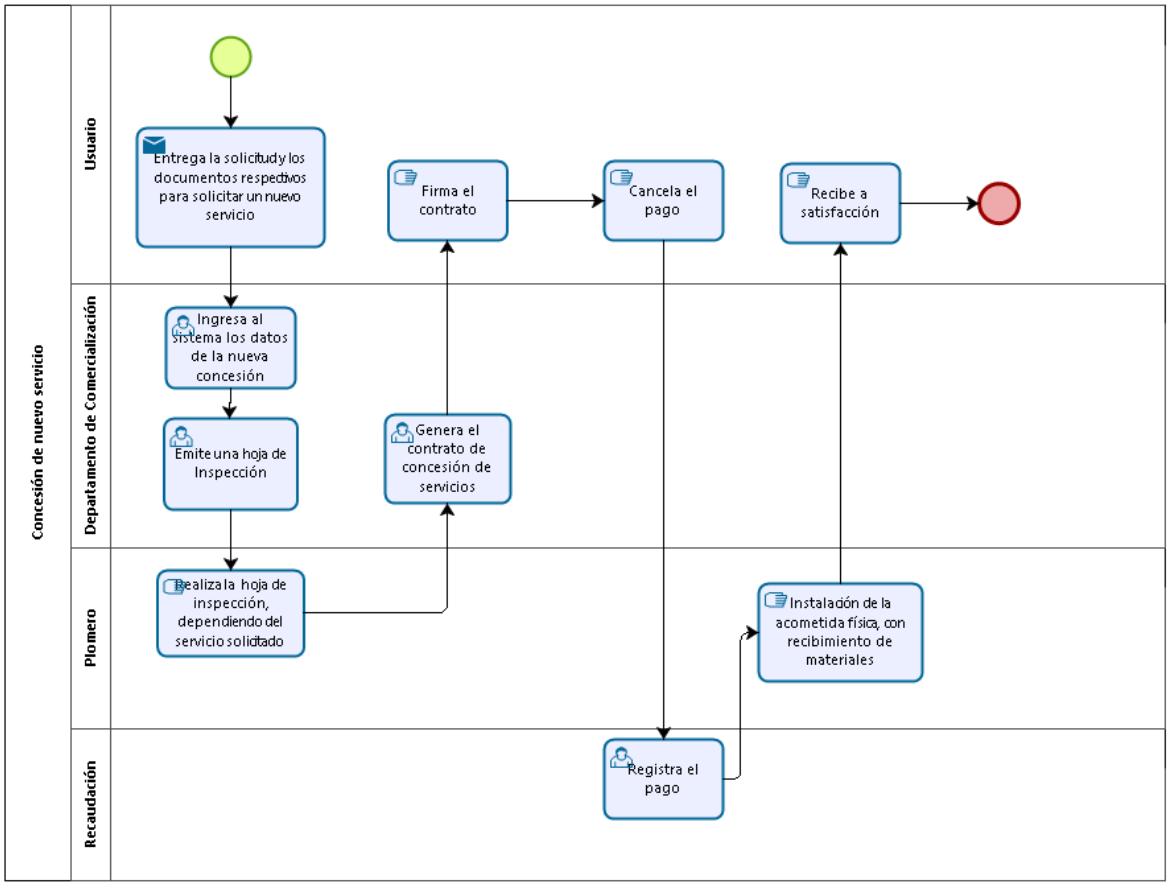


Figura 40. Diagrama de proceso - Concesión de un nuevo servicio.

Revisado por: Supervisor Informático.

Tabla 50. Ficha Emisión

FICHA DE PROCESO			
Proceso	Emisión	**N°**	2
Descripción	Generación del comprobante de pago por los servicios prestados por concepto de agua potable y/o alcantarillado, el abonado debe presentarse a cancelar el rubro a cualquiera de las oficinas de Recaudación.		
Responsables	• Recaudación		
Procesos relacionados	• Recolección de lecturas • Refacturación		
Documentación de referencia	• Reglamento de prestación de servicios EPMAPA-T 2015.		
Diagrama de proceso			

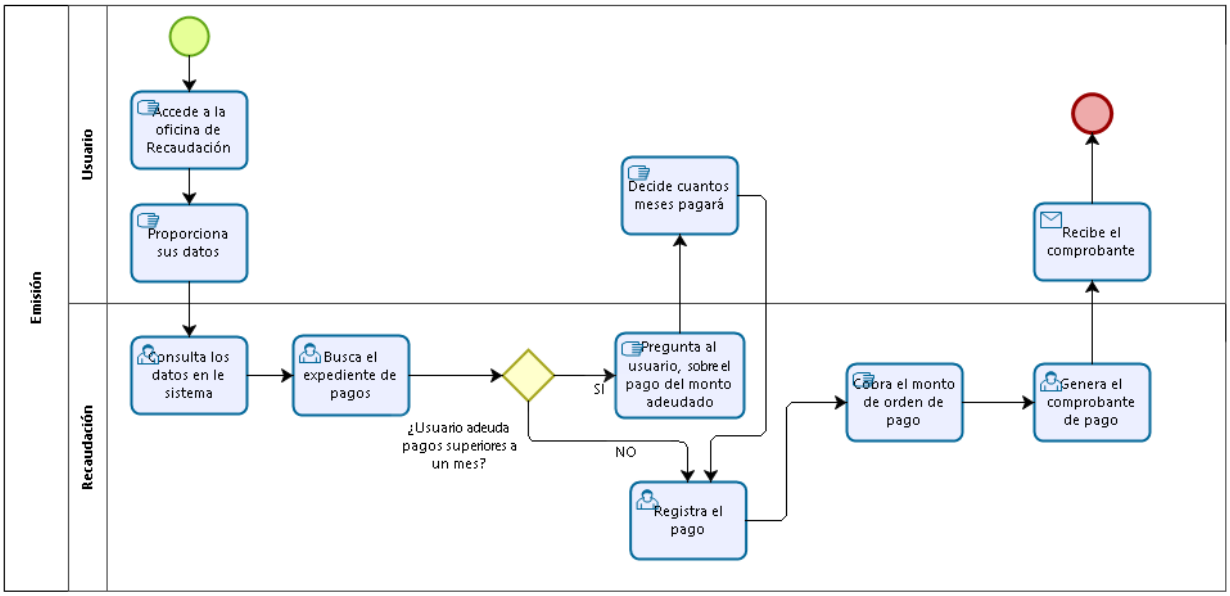


Figura 41. Diagrama de proceso – Emisión.

Revisado por: Supervisor Informático

Recaudador

Tabla 51. Ficha Refacturación

FICHA DE PROCESO			
Proceso	Refacturación	**N°**	3
Descripción	Revisión y corrección de errores que se hayan presentado en el proceso de emisión por servicios que presta la EPMAPA-T.		
Responsables	• Comisión de refacturación • Dirección de Gestión Comercial		
Procesos relacionados	• Emisión		
Documentación de referencia	• Reglamento de prestación de servicios EPMAPA-T 2015.		
Diagrama de proceso			

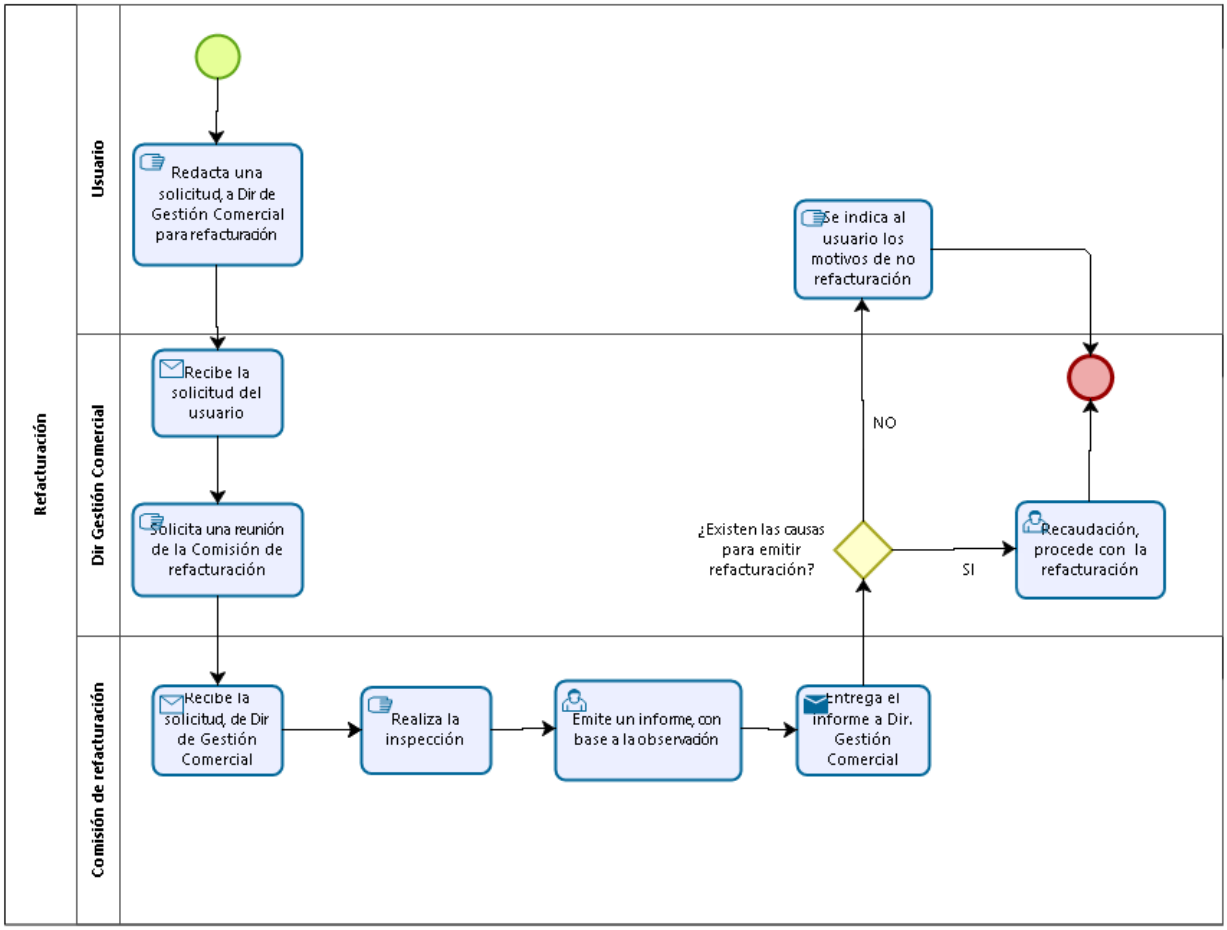


Figura 42. Diagrama de proceso – Refacturación

Revisado por: Técnica de Refacturación

Tabla 52. Ficha Recolección de lecturas

FICHA DE PROCESO			
Proceso	Recolección de lecturas	**N°**	4
Descripción	Registro de lecturas de consumo de agua potable de los abonados de la ciudad de Tulcán, mediante el uso del sistema aplicativo móvil.		
Responsables	• Dirección de Gestión Comercial • Lectores • Recaudación		
Procesos relacionados	• Emisión • Refacturación • Asignación de sectores y rutas.		
Diagrama de proceso			

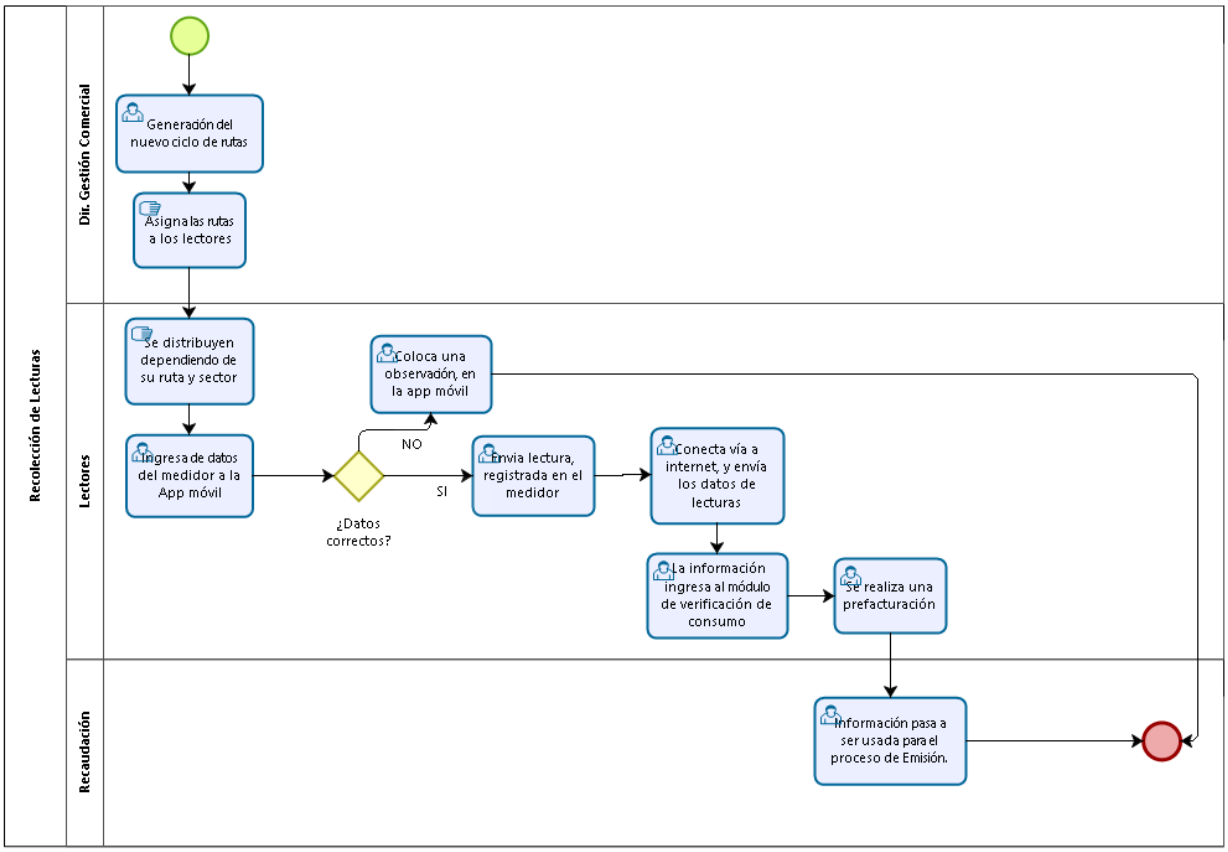


Figura 43. Diagrama de proceso – Recolección de lecturas

Revisado por: Supervisor Informático.

A continuación, se determinó la prioridad para los riesgos identificados en los procesos, dicha valoración se realizó mediante evaluación de impacto y probabilidad de ocurrencia de cada uno. La probabilidad de ocurrencia se realizó con base a la siguiente métrica.

Tabla 53. Probabilidad de ocurrencia

Probabilidad	Escala	Descripción
Poco probable	1	Anual
Posible	2	Mensual
Probable	3	Semestral
Muy probable	4	Diario

Fuente: Ulloa (2017) *Auditoría informática aplicando la metodología COBIT en el Gobierno Autónomo Descentralizado Municipal de San Cristóbal de Patate*

Y el impacto se realizó con base a la siguiente escala.

Tabla 54. Impacto en el cumplimiento de procesos

Impacto	Escala	Descripción
Bajo	1	Intervención mínima en el cumplimiento de objetivos.
Moderado bajo	2	Intervención media en el cumplimiento de objetivos
Moderado alto	3	Intervención considerable en el cumplimiento de objetivos
Alto	4	Intervención total en el cumplimiento de objetivos.

Con los valores expuestos, se procede a la priorización que se detalla a continuación.

Tabla 55. Priorización de procesos institucionales

Cod.	Procesos seleccionados	Probabilidad de ocurrencia	Impacto	Prioridad
PI.1	**Concesión de nuevo servicio**			
PI.2	**Emisión**			
E.1	Equipo de recaudación con daño.	2	2	4
E.2	Falla en el módulo verificación de errores.	1	3	3
PI.3	**Refacturación**			

PI.4	**Recolección de Lecturas**			
R.1	Base de datos con errores.	1	3	3
R.2	Zonas de falla del aplicativo	3	2	6
R.3	Actualizaciones defectuosas del aplicativo	3	3	9

Los riesgos identificados para cada proceso fueron valorados bajo criterios de prioridad y se emiten estrategias en plan de mitigación de riesgos tecnológicos.

4.1.4.2. Selección de procesos de TI.

Los procesos desarrollados en el DSI, fueron seleccionados tomando en cuenta las funciones que desempeña el equipo de trabajo, y se agrupan de la siguiente manera:

- Soporte técnico a usuarios internos.
- Mantenimiento de equipos
- Administración de sistemas informáticos
- Administración de base de datos.
- Administración de redes
- Administración del sitio web.

A continuación, se expone la ficha de cada proceso seleccionado, cada ficha contiene las siguientes especificaciones:

- Descripción
- Responsables
- Hallazgos frecuentes en el proceso
- Documentación y,
- Diagrama del proceso.

Tabla 56. Ficha de Soporte técnico a usuarios internos

FICHA DE PROCESOS TI			
Proceso	Soporte técnico a usuarios internos	**N°**	1
Descripción	Atender las solicitudes de soporte de los usuarios internos de la EPMAPA-T		
Responsables	P. Analista de Sistemas S. Supervisor Informático		
Hallazgos frecuentes	• Problemas de conexión a la red. • Problemas para ingresar a equipos y/o acceder a las impresoras. • Problemas de inicio a sistemas y/o aplicativos		
Frecuencia del proceso	Diario		
Documentación	Registro de soporte técnico		
Diagrama de proceso			

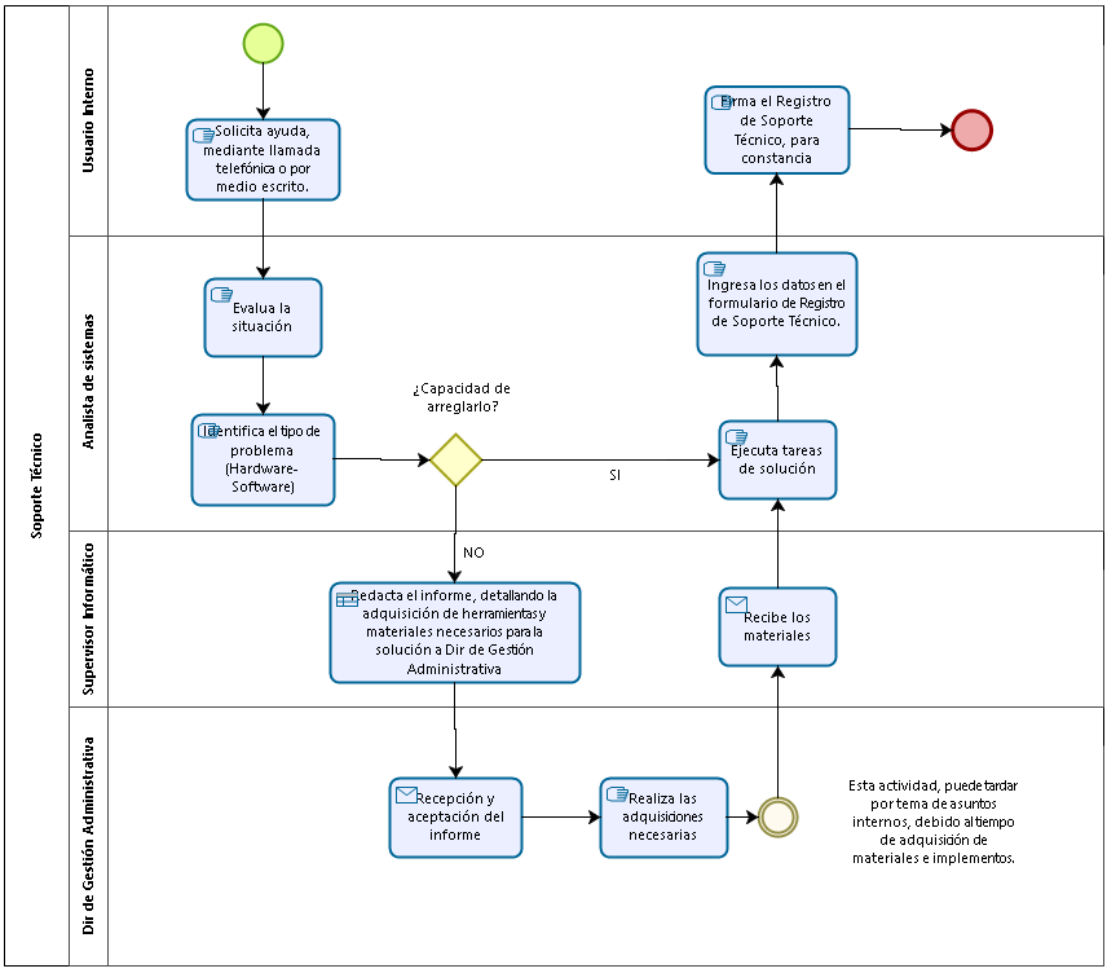


Figura 44. Diagrama de proceso – Soporte técnico a usuarios internos.

Revisado por: Supervisor Informático

Tabla 57. Ficha de mantenimiento de equipos

FICHA DE PROCESOS TI			
Proceso	Mantenimiento de equipos	**N°**	2
Descripción	Realizar tareas de mantenimiento preventivo y/o correctivo de equipos de acuerdo con una planificación establecida.		
Responsables	P. Supervisor Informático S. Analista de Sistemas		
Hallazgos frecuentes	• Daño o desgaste interno de equipos.		
Frecuencia del proceso	Trimestral		
Documentación	Planificación de mantenimiento de equipos. Informe de mantenimiento de equipos		
Diagrama de proceso			

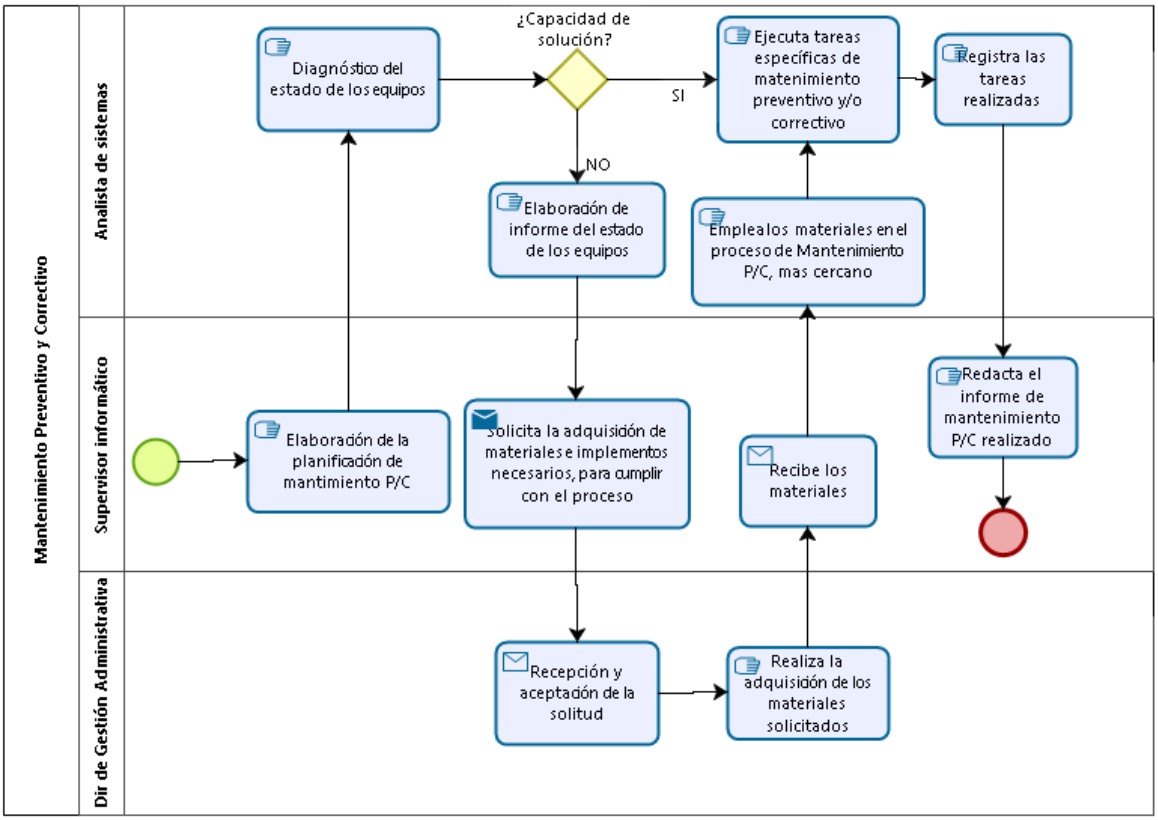


Figura 45. Diagrama de proceso – Mantenimiento de equipos

Revisado por: Supervisor Informático

Tabla 58. Ficha de Administración de redes

FICHA DE PROCESOS TI			
Proceso	Administración de redes	**N°**	3
Descripción	Realizar tareas de verificación de funcionamiento de la red e inventariar elementos		
Responsables	P. Supervisor Informático S. Analista de Sistemas		
Hallazgos frecuentes	• Elementos de red con falla.		
Frecuencia del proceso	Mensual		
Documentación	Inventario de elementos de la red.		
Diagrama de proceso			

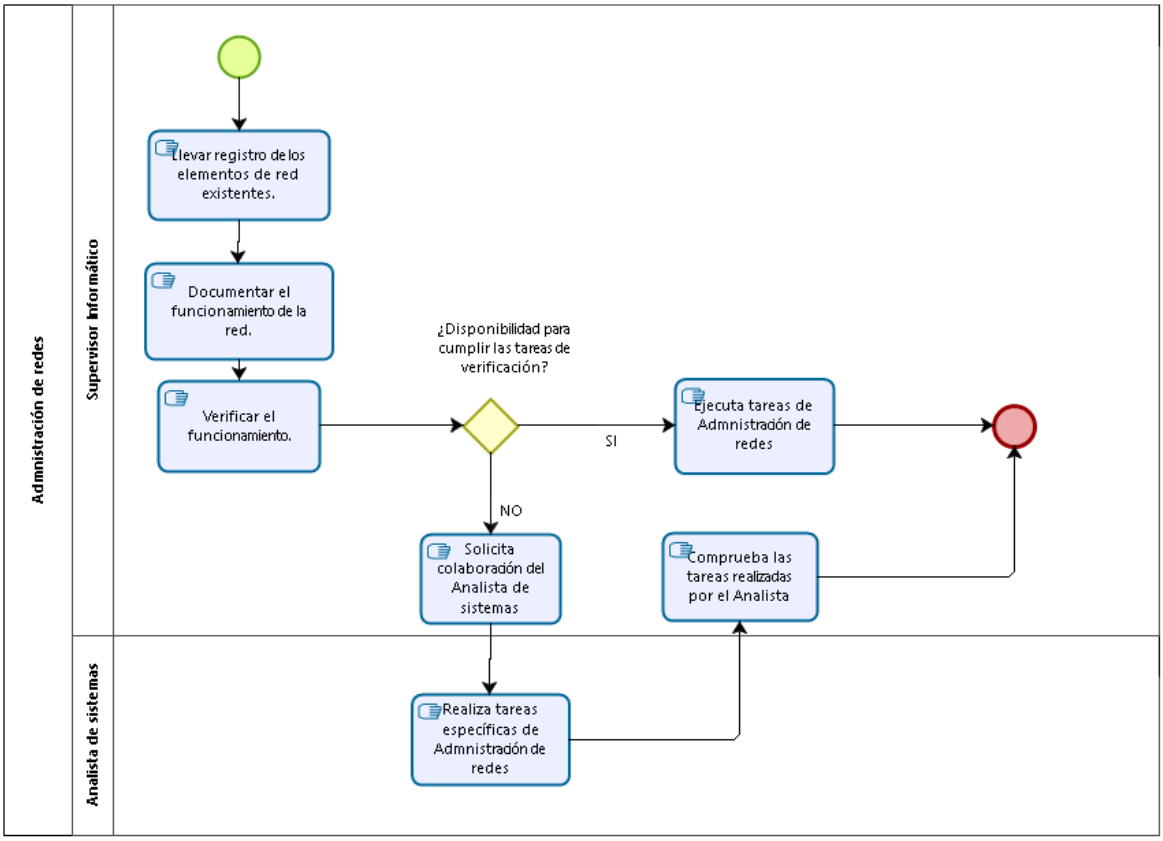


Figura 46. Diagrama de proceso – Administración de redes

Revisado por: Supervisor Informático

Tabla 59. Ficha de Administración de sistemas informáticos

FICHA DE PROCESOS TI			
Proceso	Administración de sistemas informáticos	**N°**	4
Descripción	Realizar tareas de administración de sistemas informáticos, de acuerdo con evaluación de fallas, y en los hallazgos del proceso de soporte técnico		
Responsables	P. Supervisor Informático S. Analista de Sistemas		
Hallazgos frecuentes	• Fallas en el Sistema SIIM • Reportes con fallas		
Frecuencia del proceso	Mensual		
Documentación	Manuales de usuario y técnico de los sistemas informáticos		
Diagrama de proceso			

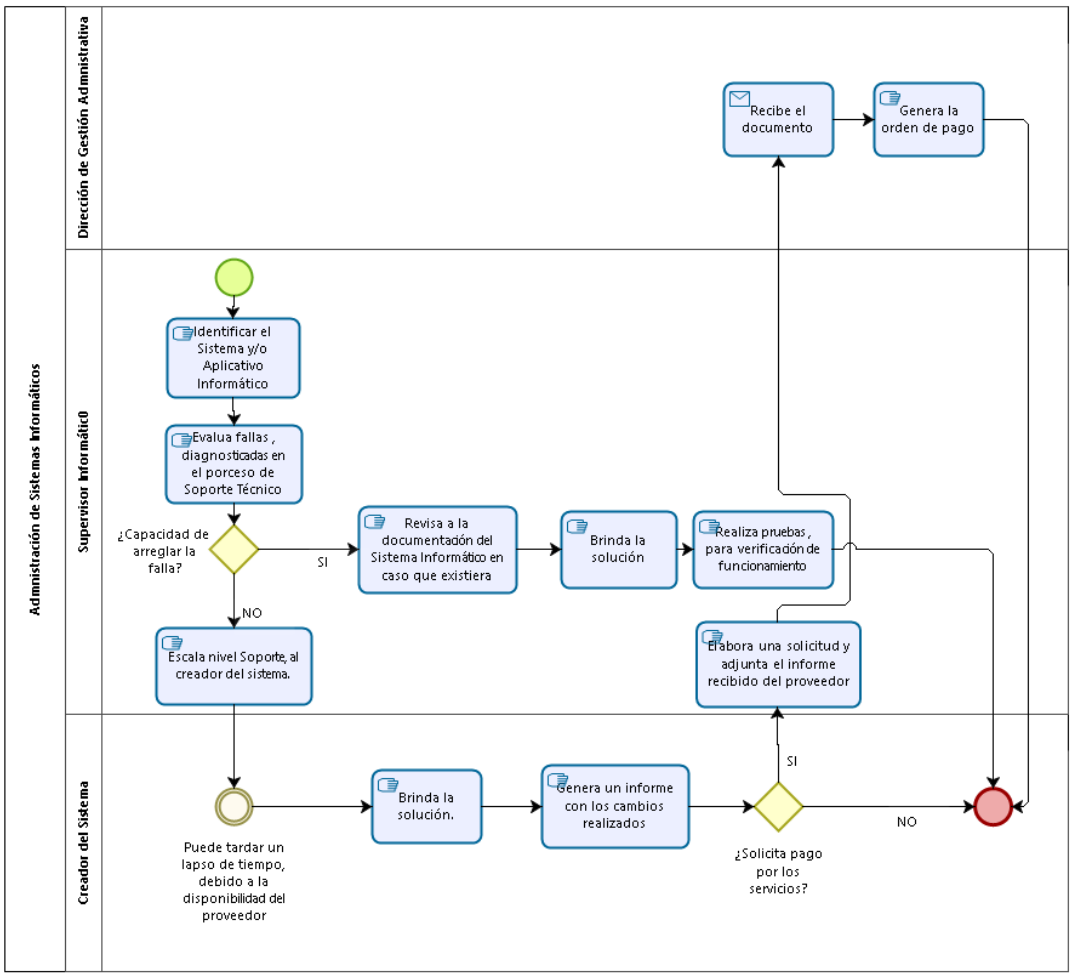


Figura 47. Diagrama de proceso – Administración de sistemas informáticos.

Revisado por: Supervisor Informático

Tabla 60. Ficha de Administración de base de datos.

FICHA DE PROCESOS TI			
Proceso	Administración de base de datos	**N°**	5
Descripción	Tareas de administración de base de datos, de acuerdo con evaluación de fallas.		
Responsables	P. Supervisor Informático S. Analista de Sistemas		
Hallazgos frecuentes	• Campos de la base de datos redundantes		
Frecuencia del proceso	Mensual		
Documentación	Inventario de tablas de la base de datos.		
Diagrama de proceso			

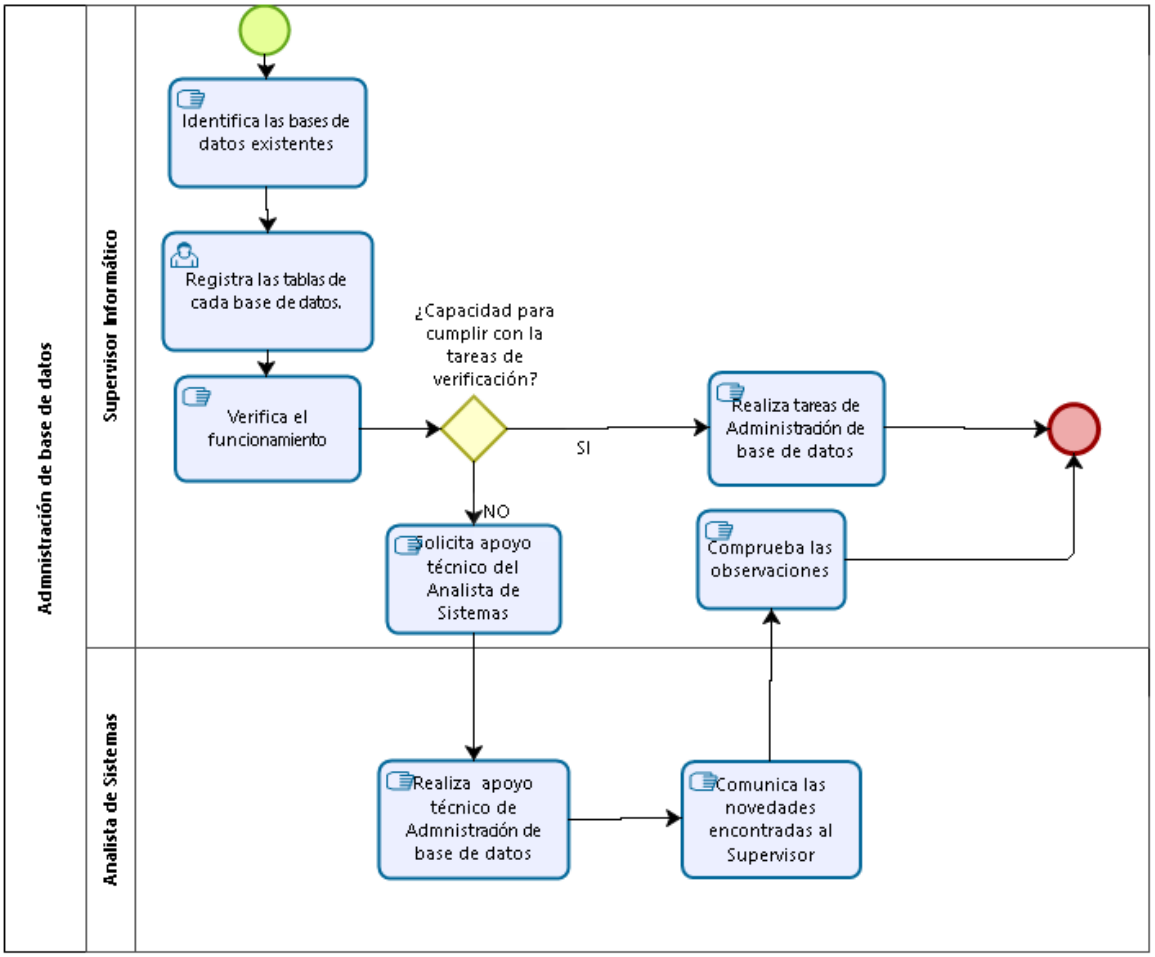


Figura 48. Diagrama de proceso – Administración de base de datos.

Revisado por: Supervisor Informático

Tabla 61. Ficha de Administración del sitio web

FICHA DE PROCESOS TI			
Proceso	Administración del sitio web	**N°**	6
Descripción	Publicación de información en el sitio web institucional, por solicitud de la comisión encargada.		
Responsables	P. Analista de sistemas S. Supervisor Informático		
Hallazgos frecuentes	• Sitio de participación ciudadana, riguroso.		
Frecuencia del proceso	Anual		
Documentación	Certificado de participación ciudadana.		
Diagrama de proceso			

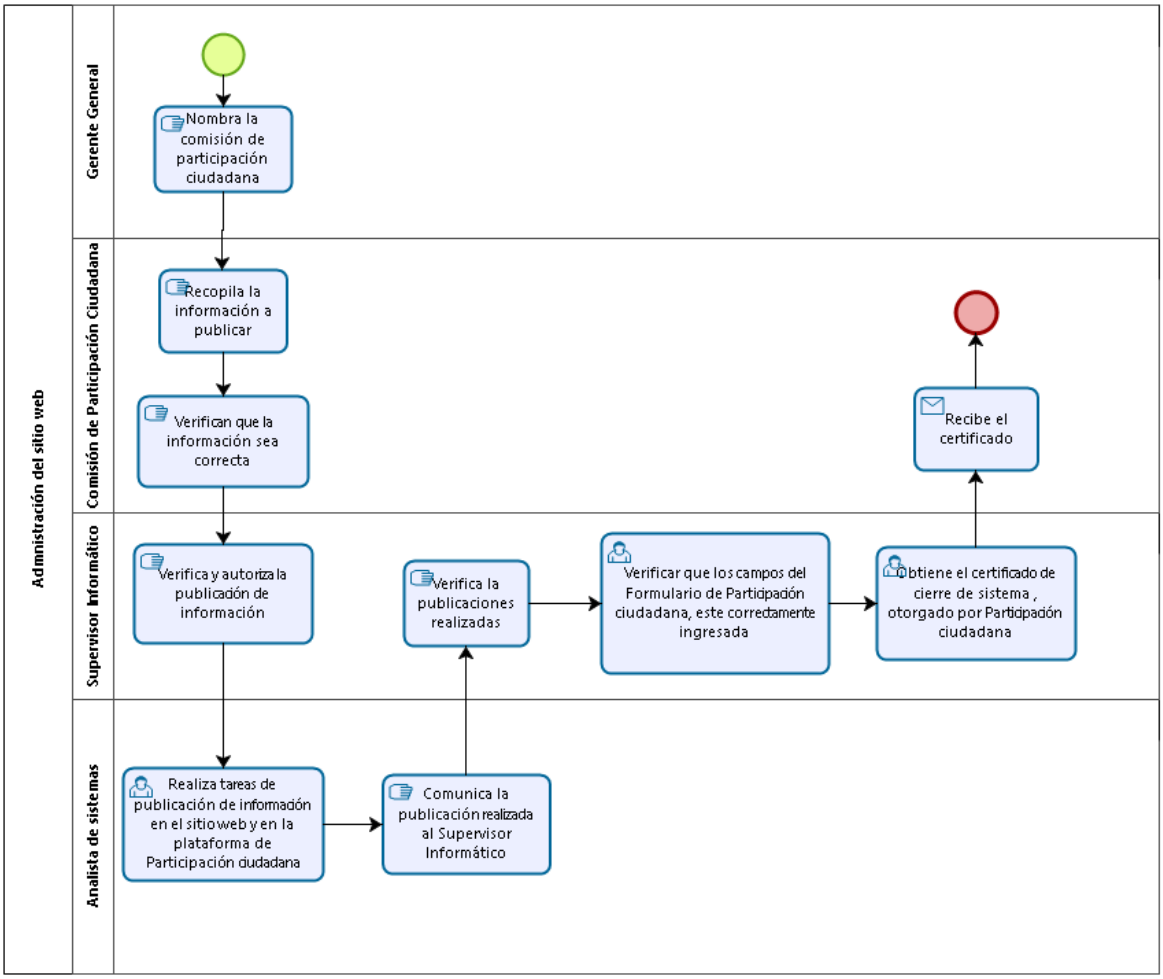


Figura 49. Diagrama de proceso - Administración del sitio.

Revisado por: Supervisor Informático

Después de conocer cada uno de los procesos que se llevan a cabo en el DSI, se procede a identificar las situaciones de riesgo y valorarlas con base a la escala presentada anteriormente.

Tabla 62. Priorización de procesos de TI

N°	Procesos seleccionados	Probabilidad de ocurrencia	Impacto	Prioridad
PTI.1	**Soporte técnico a UI**			
ST.1	Problemas críticos en soporte	3	3	9
ST.2	Inexistencia de materiales y herramientas en el DSI	4	2	8
ST.3	Excesivas solicitudes de soporte	2	2	4
PTI.2	**Mantenimiento de equipos**			
PTI.3	**Administración de sistemas informáticos.**			
ASI.1	Módulos de los sistemas informáticos con errores	3	3	9
ASI.2	Lentitud en los sistemas informáticos.	3	2	6
PTI.4	**Administración de base de datos.**			
ABD.1	Campos de la base de datos redundantes.	2	2	4
ABD.2	Inadecuado respaldo de información	1	3	3
PTI.5	**Administración de redes**			
AR.1	Elementos de red con deterioro.	3	3	9
AR.2	Dispositivos de red con errores.	2	3	6
AR.3	Inadecuada distribución de elementos de red	2	2	4
PTI.6	Administración del sitio web.			

Con la valoración de los riesgos tecnológicos identificados se procede a emitir estrategias el plan de mitigación de riesgos tecnológicos.

4.1.4.3. Procesos COBIT® 5

Los procesos COBIT® 5 permiten monitorear y gestionar las actividades de TI, enfocándose en la mejora continua de los procesos desarrollados en el área. Se determinó los procesos a auditar con base al estudio inicial de la empresa, señalando el cumplimiento de cada uno y de esta manera determinar los procesos aplicables al caso de estudio.

La matriz contiene los siguientes factores de cumplimiento:

- *Cumple parcialmente*. Para aquellos procesos, que tienen en cumplimiento por lo menos un objetivo de control.
- *No cumple*. Para aquellos procesos que no cumplen con ningún objetivo de control
- *No aplica.* Para aquellos procesos, que no se ajustan a los requerimientos de la empresa a evaluar.

Con base a lo expuesto anteriormente, se listan la totalidad de los procesos COBIT® 5 a continuación:

Tabla 63. Procesos COBIT® 5 – Área de Gobierno

Dominio	Proceso	Cumple parcialmente	No cumple	No aplica
Evaluar, Orientar y Supervisar – EDM	EDM01. Asegurar el establecimiento y mantenimiento del marco de gobierno.	X	X	
	EDM02. Asegurar la entrega de beneficios.	X		
	EDM03. Asegurar la optimización del riesgo.			
	EDM04. Asegurar la optimización de los recursos.	X		
	EDM05. Asegurar la transparencia hacia las partes interesadas.	X		

Tabla 64. Procesos COBIT® 5 – Área de Gestión

Dominio	Proceso	Cumple parcialmente	No cumple	No aplica
Alinear, Planificar y Organizar – APO	APO01. Gestionar el marco de gestión de TI.	X		
	APO02. Gestionar la estrategia.	X		
	APO03. Gestionar la arquitectura empresarial.	X		
	APO04. Gestionar la innovación.			X
	APO05. Gestionar el portafolio.		X	
	APO06. Gestionar el presupuesto y los costes.	X		
	APO07. Gestionar los recursos humanos.	X		
	APO08. Gestionar las relaciones	X		
	APO09. Gestionar los acuerdos de servicio.	X		
	APO10. Gestionar los proveedores.		X	
	APO11. Gestionar la calidad.		X	
	APO12. Gestionar el riesgo.		X	
	APO13. Gestionar la seguridad.		X	
Construir, Adquirir e Implementar – BAI	BAI01. Gestionar los programas y proyectos.	X		
	BAI02. Gestionar la definición de requisitos.		X	
	BAI03. Gestionar la identificación y la construcción de soluciones.	X		
	BAI04. Gestionar la disponibilidad y la capacidad.	X		

	BAI05. Gestionar la introducción de cambios organizativos.	X		
	BAI06. Gestionar los cambios.			X
	BAI07. Gestionar la aceptación del cambio y de la transición.			X
	BAI08. Gestionar el conocimiento.		X	
	BAI09. Gestionar los activos.	X		
	BAI10. Gestionar la configuración	X		
Entregar, dar Servicio y Soporte – DSS	DSS01. Gestionar las operaciones	X		
	DSS02. Gestionar las peticiones e incidentes del servicio.		X	
	DSS03. Gestionar los problemas.	X		
	DSS04. Gestionar la continuidad.	X		
	DSS05. Gestionar los servicios de seguridad.	X		
	DSS06. Gestionar los controles de los procesos de negocio.	X		
Supervisar, Evaluar y Valorar – MEA	MEA01. Supervisar, Evaluar y Valorar rendimiento y conformidad.	X		
	MEA02. Supervisar, Evaluar y Valorar el sistema de control interno.			X
	MEA03. Supervisar, Evaluar y Valorar la conformidad con los requerimientos externos.	X		

Procesos COBIT® 5 no aplicables.

Los siguientes procesos no se toman en cuenta para el proceso de auditoría, debido a que la naturaleza institucional no se ajusta no se ajusta a los requerimientos.

- **APO04. Gestionar la innovación**.

La EPMAPA-T es una empresa que cumple con los objetivos planteados en todas sus áreas, sin embargo, hasta el momento no se ha proyectado a cambios de innovación tecnológica, se considera que el presupuesto asignado al DSI no es suficiente.

- **BAI06. Gestionar los cambios**.

Los cambios realizados en el DSI no han sido controlados y su seguimiento no ha cumplido con un proceso estándar, es por ello que este proceso no aplica en evaluación.

- **BAI07. Gestionar la aceptación del cambio y de la transición**.

No existe gestión de cambios en el DSI hasta el momento.

- **MEA02. Supervisar, Evaluar y Valorar el sistema de control interno.**

La EPMAPA-T no cuenta con una unidad especializada que se dedique al control interno institucional, las actividades de supervisión son realizadas por la Dirección de Gestión Administrativa.

Procesos COBIT® 5 que la EPMAPA-T no cumple.

Los siguientes procesos han sido identificados, mediante el análisis del estudio inicial. A continuación, las observaciones por cada proceso COBIT® 5.

- **EDM03. Asegurar la optimización del riesgo.**

La EPMAPA-T no cuenta con registros de gestión de riesgos de TI.

- **APO05. Gestionar el portafolio.**

El DSI no ha establecido estrategias y medidas de inversión en el área, tampoco existen registros de evaluación de cambios financieros.

- **APO10. Gestionar los proveedores.**

El DSI no ha realizado un análisis de cumplimiento de obligaciones vinculadas a los proveedores de servicios de tecnología, así como también minimizar la inversión realizada en dichos servicios.

- **APO11. Gestionar la calidad.**

El DSI no cumple con requisitos de calidad en los procesos de TI, no existe registro sobre la monitorización y el uso de estándares en el área.

- **APO12. Gestionar el riesgo.**

En el área de TI no se ha gestionado riesgos asociados a tecnología, similar al proceso EDM03.

- **APO13. Gestionar la seguridad.**

No se ha implementado un sistema de gestión de seguridad de la información para la EPMAPA-T.

- **BAI02. Gestionar la definición de requisitos.**

El DSI no cuenta con registros sobre gestión de los requisitos previa la adquisición o creación de una solución tecnológica.

- **BAI08. Gestionar el conocimiento.**

El DSI no cuenta con procesos documentados que permitan soportar las actividades del equipo de trabajo, con la finalidad de mejorar en la toma decisiones y la productividad.

- **DSS02. Gestionar las peticiones e incidentes del servicio.**

El DSI no ha trabajado en gestión de peticiones e incidentes de servicio mediante planificación, priorización y soluciones.

Procesos COBIT® 5 aplicables

Después de realizar un análisis del estudio inicial se toma en cuenta los siguientes procesos con los objetivos de control que se cumplen, para realizar el proceso de evaluación.

Tabla 65. Procesos COBIT® 5 aplicables a auditoría

GOBIERNO		
Dominio	**Proceso**	**Objetivo de control**
Evaluar, Orientar y Supervisar – EDM	EDM01. Asegurar el establecimiento y mantenimiento del marco de gobierno.	EDM01.01. Evaluar el sistema de gobierno. EDM01.02. Orientar el sistema de gobierno.
	EDM02. Asegurar la entrega de beneficios.	EDM02.01. Evaluar la optimización de valor. EDM02.02. Orientar la optimización de valor
	EDM04. Asegurar la optimización de los recursos	EDM04.01. Evaluar la gestión de recursos.
	EDM05. Asegurar la transparencia hacia las partes interesadas.	EDM05.01. Evaluar los requisitos de elaboración de informes de las partes interesadas. EDM05.02. Orientar la comunicación con las partes interesadas y la de elaboración de informes.
GESTIÓN		
Alinear, Planificar y Organizar – APO	APO01. Gestionar el marco de gestión de TI.	APO01.01. Definir la estructura organizativa. APO01.02. Establecer roles y responsabilidades APO01.03. Mantener los elementos catalizadores del sistema de gestión. APO01.05. Optimizar la ubicación de la función de TI.
	APO02. Gestionar la estrategia.	APO02.01. Comprender la dirección de la empresa.
	APO03. Gestionar la arquitectura empresarial**.**	APO03.01. Desarrollar la visión de arquitectura de la empresa. APO03.02. Definir la arquitectura de referencia.

	APO06. Gestionar el presupuesto y los costes.	APO06.02. Priorizar la asignación de recursos APO06.03. Crear y mantener presupuestos.
	APO07. Gestionar los recursos humanos.	APO07.01. Mantener la dotación de personal suficiente y adecuada. APO07.02. Identificar personal clave de TI APO07.03. Mantener las habilidades y competencias del personal.
	APO08. Gestionar las relaciones	APO08.01. Entender las expectativas del negocio. APO08.04. Coordinar y comunicar.
	APO09. Gestionar los acuerdos de servicio.	APO09.01. Identificar servicios de TI. APO09.02. Catalogar servicios basados en TI.
Construir, Adquirir e Implementar – BAI	BAI01. Gestionar los programas y proyectos.	BAI01.01. Mantener un enfoque estándar para la gestión de programas y proyectos. BAI01.02. Iniciar un programa. BAI01.03. Gestionar el compromiso de las partes interesadas. BAI01.04. Desarrollar y mantener el plan del programa.
	BAI03. Gestionar la identificación y la construcción de soluciones.	BAI03.01. Diseñar soluciones de alto nivel BAI03.02. Diseñar los componentes detallados de la solución BAI03.03. Desarrollar los componentes de la solución. BAI03.10. Mantener soluciones. BAI03.11. Definir los servicios de TI y mantener el catálogo de servicios.

	BAI04. Gestionar la disponibilidad y la capacidad.	BAI04.01. Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.
	BAI05. Gestionar la introducción de cambios organizativos.	BAI05.01. Establecer el deseo de cambiar.
	BAI09. Gestionar los activos.	BAI09.01. Identificar y registrar activos actuales. BAI09.02. Gestionar los activos críticos. BAI09.03. Gestionar el ciclo de vida de los activos BAI09.05. Administrar licencias.
	BAI10. Gestionar la configuración	BAI10.02. Establecer y mantener un repositorio de configuración y una base de referencia. BAI10.04. Generar informes de estado y configuración.
Entregar, dar Servicio y Soporte – DSS	DSS01. Gestionar las operaciones.	DSS01.01. Ejecutar procedimientos operativos. DSS01.05. Gestionar las instalaciones.
	DSS03. Gestionar los problemas.	DSS03.01. Identificar y clasificar problemas. DSS03.05. Realizar una gestión de problemas proactiva.
	DSS04. Gestionar la continuidad.	DSS04.02. Mantener una estrategia de continuidad. DSS04.07. Gestionar acuerdos de respaldo. DSS04.08. Ejecutar revisiones post-reanudación.
	DSS05. Gestionar los servicios de seguridad.	DSS05.01. Proteger contra software malicioso

		DSS05.02. Gestionar la seguridad de la red y las conexiones. DSS05.04. Gestionar la identidad del usuario y el acceso lógico
	DSS06. Gestionar los controles de los procesos de negocio.	DSS06.03. Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.
Supervisar, Evaluar y Valorar – MEA	MEA01. Supervisar, Evaluar y Valorar rendimiento y conformidad.	MEA01.01. Establecer un enfoque de la supervisión MEA01.04. Analizar e informar sobre el rendimiento.
	MEA03. Supervisar, Evaluar y Valorar la conformidad con los requerimientos externos.	MEA03.01. Identificar requisitos externos de cumplimiento. MEA03.04. Obtener garantía de cumplimiento de requisitos externos.

Con la selección de procesos COBIT® 5, se procede a la elaboración de las hojas de trabajo aplicables a los diferentes actores en el proceso de auditoría.

Las hojas de trabajo se encuentran en la sección de la siguiente manera:

- Anexo 8: Hoja de trabajo Dirección Administrativa
- Anexo 9: Hoja de trabajo Control Interno
- Anexo 10: Hoja de trabajo Talento Humano
- Anexo 11: Hoja de trabajo Supervisor Informático
- Anexo 12: Hoja de trabajo Analista de Sistemas.

4.1.5. Resultados de Auditoría

A continuación, se elaboran las matrices de verificación de cumplimiento, con base a los procesos COBIT® 5 seleccionados.

4.1.5.1. Verificación de cumplimiento.

En las siguientes matrices se puede observar la siguiente información:

- ***Área***. Hace referencia al área COBIT® 5 (*Gobierno – Gestión*)
- ***Dominio.*** Hace referencia a los dominios COBIT® 5
- ***Proceso.*** Hace referencia al proceso seleccionado.
- ***Objetivos de control.*** Se lista la totalidad de los objetivos de control correspondientes al proceso seleccionado, donde se indica con color azul los objetivos de control evaluados. Los objetivos de control en color blanco fueron identificados con no cumplimiento con base al estudio inicial.
- ***Revisión a través de.*** Aspectos a evaluar.
- ***Descripción de la prueba.*** Hallazgos del proceso de auditoría correspondiente al proceso seleccionado.
- ***Evaluación.*** Dictamen final de cada proceso donde *EFECTIVO* será la respuesta cuando los requerimientos COBIT® 5 se cumplan y *NO EFECTIVO* cuando no se cumplan.
- ***Documentos de soporte.*** Documentos en los cuales se basa la evaluación.

Tabla 66. Verificación de cumplimiento EDM01

ÁREA	Gobierno			**DOMINIO**	Evaluar, Orientar y Supervisar – EDM	
PROCESO	EDM01. Asegurar el establecimiento y mantenimiento del marco de gobierno.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
EDM01.01. Evaluar el sistema de gobierno.	X		Evaluación interna empresarial, donde incluya el área de TI. Procedimientos de evaluación al DSI.	La existencia de un informe del estado de los equipos informáticos de la EPMAPA-T, demuestra que se ha realizado una evaluación de hardware de la empresa, que permite tomar medidas correctivas con la finalidad que las actividades se desarrollen con normalidad.	NO EFECTIVO	• Reglamento Orgánico Funcional • Informe estado de los equipos EPMAPA-T • Hoja de trabajo Dirección de Gestión Administrativa (Ver Anexo 8)
EDM01.02. Orientar el sistema de gobierno.		X				
EDM01.03. Supervisar el sistema de gobierno.		X				

Tabla 67. Verificación de cumplimiento EDM02

ÁREA	Gobierno			**DOMINIO**	Evaluar, Orientar y Supervisar – EDM	
PROCESO	EDM02. Asegurar la entrega de beneficios.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
EDM02.01. Evaluar la optimización de valor		X	Cumplimiento de objetivos institucionales basados en TI. Catálogo de servicios de TI	La EPMAPA-T considera al DSI un departamento de apoyo, por lo tanto, no se toma en cuenta para la verificación de cumplimiento de objetivos institucionales Se ha comprobado la inexistencia un catálogo de servicios de TI.	NO EFECTIVO	• Hoja de trabajo Dirección de Gestión Administrativa (Ver Anexo 8) • Hoja de trabajo Control Interno (Ver Anexo 9) • Hoja de trabajo Supervisor Informático (Ver Anexo 11)
EDM02.02. Orientar la optimización de valor		X				
EDM02.03. Supervisar la optimización de valor		X				

Tabla 68. Verificación de cumplimiento EDM04

ÁREA	Gobierno			**DOMINIO**	Evaluar, Orientar y Supervisar – EDM	
PROCESO	EDM04. Asegurar la optimización de los recursos					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
EDM04.01. Evaluar la gestión de recursos.		X	Seguimiento a los recursos asignados al DSI	Se realiza un reporte básico de materiales e implementos el bodeguero. Sin embargo, este control no se considera suficiente.	NO EFECTIVO	• Hoja de trabajo Control Interno (Ver Anexo 9)
EDM04.02. Orientar la gestión de recursos.		X				
EDM04.03. Supervisar la gestión de recursos		X				

Tabla 69. Verificación de cumplimiento EDM05

ÁREA	Gobierno			**DOMINIO**	Evaluar, Orientar y Supervisar – EDM	
PROCESO	EDM05. Asegurar la transparencia hacia las partes interesadas.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
EDM05.01. Evaluar los requisitos de elaboración de informes de las partes interesadas.	X		Informes de cumplimiento de funciones. Formatos de informes de cumplimiento	Se realiza un reporte de cumplimiento por el DSI. El formato del reporte es similar para toda la dirección.	EFECTIVO	• Reporte de cumplimiento de funciones mensual. • Hoja de trabajo Control Interno (Ver Anexo 9)
EDM05.02. Orientar la comunicación con las partes interesadas y la de elaboración de informes.	X					
EDM05.03. Supervisar la comunicación con las partes interesadas.		X				

Tabla 70. Verificación de cumplimiento APO1

ÁREA	Gestión			**DOMINIO**	Alinear, Planificar y Organizar – APO	
PROCESO	APO01. Gestionar el marco de gestión de TI.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
APO01.01. Definir la estructura organizativa.	X		Objetivos de TI. Cumplimiento de funciones por el DSI Comunicación de las funciones y responsabilidades al personal. TI en la conformación de comités institucionales.	El DSI, forma parte del comité de participación ciudadana, de esta manera se conoce que sus funciones aportan en otras áreas. Se han establecido objetivos de TI. Sin embargo, no se han alineado a los objetivos institucionales. Las funciones y responsabilidades han sido comunicadas mediante el contrato y el Manual de Descripción, Valoración y Clasificación de puestos.	EFECTIVO	• Manual de Descripción, Valoración y Clasificación de puestos • Hoja de trabajo Dirección de Gestión Administrativa (Ver Anexo 8) • Hoja de trabajo Control Interno (Ver Anexo 9) • Hoja de trabajo Talento Humano (Ver Anexo 10) • Hoja de trabajo Supervisor Informático (Ver Anexo 11)
APO01.02. Establecer roles y responsabilidades	X					
APO01.03. Mantener los elementos catalizadores del sistema de gestión.	X					
APO01.04. Comunicar los objetivos y la dirección de gestión.		X				
APO01.05. Optimizar la ubicación de la función de TI.	X					
APO01.06. Definir la propiedad de la información (datos) y del sistema.		X				
APO01.07. Gestionar la mejora continua de los procesos.		X				
APO01.08. Mantener el cumplimiento de las políticas y procedimientos		X				

Tabla 71. Verificación de cumplimiento APO02.

ÁREA	Gestión			**DOMINIO**	Alinear, Planificar y Organizar – APO	
PROCESO	APO02. Gestionar la estrategia.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
APO02.01. Comprender la dirección de la empresa.		X	Plan estratégico de TI 2010.	Existe un plan estratégico que hasta la fecha sigue operando en el DSI. Sin embargo, se encuentra desactualizado debido a que fue desarrollado para el periodo 2010-2014	NO EFECTIVO	• Plan estratégico de TI 2010. • Hoja de trabajo Supervisor Informático (Ver Anexo 11)
APO02.02. Evaluar el entorno, capacidades y rendimiento actuales.		X				
APO02.03. Definir el objetivo de las capacidades de TI.		X				
APO02.04. Realizar un análisis de diferencias.		X				
APO02.05. Definir el plan estratégico y la hoja de ruta.		X				
APO02.06. Comunicar la estrategia y dirección de TI		X				

Tabla 72. Verificación de cumplimiento APO03

ÁREA	Gestión			**DOMINIO**	Alinear, Planificar y Organizar – APO	
PROCESO	APO03. Gestionar la arquitectura empresarial.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
APO03.01. Desarrollar la visión de arquitectura de la empresa.	X		Distribución de la Estructura orgánica funcional. Funciones del personal del DSI	La distribución de la estructura orgánica funcional del DSI cuenta con un Supervisor y dos Analistas de sistemas. Las funciones del DSI, se encuentran en los contratos y en el manual de descripción y valoración de puestos.	NO EFECTIVO	• Manual de Descripción, Valoración y Clasificación de puestos • Contrato del Analista de Sistemas. • Estructura orgánica funcional. • Reglamento orgánico funcional. • Hoja de trabajo Talento Humano (Ver Anexo 10)
APO03.02. Definir la arquitectura de referencia.	X					
APO03.03. Seleccionar las oportunidades y soluciones.		X				
APO03.04. Definir la implantación de la arquitectura.		X				
APO03.05. Proveer los servicios de arquitectura empresarial.		X				

Tabla 73. Verificación de cumplimiento APO06

ÁREA	Gestión			**DOMINIO**	Alinear, Planificar y Organizar – APO	
PROCESO	APO06. Gestionar el presupuesto y los costes.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
APO06.01. Gestionar las finanzas y la contabilidad		X	Asignación Plan operativo anual-POA. Planificación de asignación POA 2020. Plan presupuestario del DSI	El DSI ha realizado un informe, detallando el presupuesto necesario para la asignación POA 2020. Se contempla una asignación para la adquisición de nuevos equipos y el nuevo software que integrará varias áreas en la Institución	NO EFECTIVO	• Plan operativo anual. • Informe previo la asignación del POA • Plan presupuestario para adquisición de software y hardware. • Hoja de trabajo Dirección de Gestión Administrativa (Ver Anexo 8) • Hoja de trabajo Supervisor Informático (Ver Anexo 11)
APO06.02. Priorizar la asignación de recursos.	X					
APO06.03. Crear y mantener presupuestos.	X					
APO06.04. Modelar y asignar costes.		X				
APO06.05. Gestionar costes.		X				

Tabla 74. Verificación de cumplimiento APO07

ÁREA	Gestión			**DOMINIO**	Alinear, Planificar y Organizar – APO	
PROCESO	APO07. Gestionar los recursos humanos.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
APO07.01. Mantener la dotación de personal suficiente y adecuada.	X		Contratación del personal DSI. Designación de responsabilidades dentro del DSI. Evaluación de habilidades y destrezas del personal del DSI.	El proceso de contratación institucional, con base al PAC. En el proceso de contratación del personal del DSI, se toma como base el perfil descrito en el manual de Descripción y valoración de puestos. No existe registro de evaluación de habilidades y destrezas del personal.	NO EFECTIVO	• Manual de Descripción, Valoración y Clasificación de puestos • Plan anual de contratación - PAC • Hoja de trabajo Talento humano (Ver Anexo 10) • Hoja de trabajo Supervisor Informático (Ver Anexo 11)
APO07.02. Identificar personal clave de TI	X					
APO07.03. Mantener las habilidades y competencias del personal.		X				
APO07.04. Evaluar el desempeño laboral de los empleados.		X				
APO07.05. Planificar y realizar un seguimiento del uso de los recursos humanos de TI y del negocio.		X				
APO07.06. Gestionar el personal contratado		X				

Tabla 75. Verificación de cumplimiento APO08

ÁREA	Gestión			**DOMINIO**	Alinear, Planificar y Organizar – APO	
PROCESO	APO08. Gestionar las relaciones					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
APO08.01. Entender las expectativas del negocio.		X	Gestión de incidentes que alteren los objetivos institucionales. Caso de situaciones de emergencia en TI	El DSI no ha implementado un procedimiento de gestión de incidentes basado en TI. No se ha focalizado situaciones emergentes de TI.	NO EFECTIVO	• Hoja de trabajo Supervisor Informático (Ver Anexo 11)
APO08.02. Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio.		X				
APO08.03. Gestionar las relaciones con el negocio.		X				
APO08.04. Coordinar y comunicar.		X				
APO08.05. Proveer datos de entrada para la mejora continua de los servicios.		X				

Tabla 76. Verificación de cumplimiento APO09

ÁREA	Gestión			**DOMINIO**	Alinear, Planificar y Organizar – APO	
PROCESO	APO09. Gestionar los acuerdos de servicio.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
APO09.01. Identificar servicios de TI.		X	Catálogo de servicios de TI. Niveles de servicio de TI.	El DSI contempla el cumplimiento de funciones y actividades, no ha desarrollado un catálogo exclusivo de TI. No se ha establecido niveles de servicio de TI.	NO EFECTIVO	• Reglamento de prestación de servicios EPMAPA-T. • Hoja de trabajo Supervisor Informático (Ver Anexo 11)
APO09.02. Catalogar servicios basados en TI.		X				
APO09.03. Definir y preparar acuerdos de servicio.		X				
APO09.04. Supervisar e informar de los niveles de servicio.		X				
APO09.05. Revisar acuerdos de servicio y contratos.		X				

Tabla 77. Verificación de cumplimiento BAI01

ÁREA	Gestión			**DOMINIO**	Construir, Adquirir e Implementar – BAI	
PROCESO	BAI01. Gestionar los programas y proyectos.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
BAI01.01. Mantener un enfoque estándar para la gestión de programas y proyectos.		X	Planes, proyectos y programas actuales Compromiso del DSI en la ejecución del proyecto	Se lleva a cabo el plan de adquisición del nuevo software. El DSI ejecuta actualmente el plan de renovación del paquete informático. Las funciones se designan verbalmente por el Supervisor Informático.	NO EFECTIVO	• Plan de adquisición de hardware y software • Hoja de trabajo Supervisor Informático (Ver Anexo 11) • Hoja de trabajo Analista de sistemas (Ver Anexo 12)
BAI01.02. Iniciar un programa.	X					
BAI01.03. Gestionar el compromiso de las partes interesadas.	X					
BAI01.04. Desarrollar y mantener el plan del programa.		X				
BAI01.05. Lanzar y ejecutar el programa.		X				
BAI01.06. Supervisar controlar e informar de los resultados del programa.		X				
BAI01.07. Lanzar e iniciar proyectos dentro de un programa.		X				
BAI01.08. Planificar proyectos.		X				
BAI01.09. Gestionar la calidad de los programas y proyectos.		X				
BAI01.10. Gestionar el riesgo de programas y proyectos.		X				
BAI01.11. Supervisar y controlar proyectos		X				
BAI01.12. Gestionar los recursos y los paquetes de trabajo del proyecto.		X				
BAI01.13. Crear un proyecto o iteración.		X				
BAI01.14. Cerrar un programa		X				

Tabla 78. Verificación de cumplimiento BAI03

ÁREA	Gestión			**DOMINIO**	Construir, Adquirir e Implementar – BAI	
PROCESO	BAI03. Gestionar la identificación y la construcción de soluciones.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
BAI03.01. Diseñar soluciones de alto nivel	X		Identificar soluciones a implementar para mejora de la EPMAPA-T. Soluciones tecnológicas creadas en el DSI	Se han identificado soluciones tecnológicas que contribuyan a la mejora de los procesos institucionales. El sistema ERP del sitio web, es la única solución tecnológica creada en el DSI	NO EFECTIVO	• Proyecto nuevo software /ERP • Hoja de trabajo Supervisor Informático (Ver Anexo 11) • Hoja de trabajo Analista de sistemas (Ver Anexo 12)
BAI03.02. Diseñar los componentes detallados de la solución	X					
BAI03.03. Desarrollar los componentes de la solución.	X					
BAI03.04. Obtener los componentes de la solución.		X				
BAI03.05. Construir soluciones.		X				
BAI03.06. Realizar controles de calidad		X				
BAI03.07. Preparar pruebas de solución.		X				
BAI03.08. Ejecutar pruebas de solución.		X				
BAI03.09. Gestionar cambios a los requerimientos.		X				
BAI03.10. Mantener soluciones.		X				
BAI03.11. Definir los servicios de TI y mantener el catálogo de servicios		X				

Tabla 79. Verificación de cumplimiento BAI04

ÁREA	Gestión			**DOMINIO**	Construir, Adquirir e Implementar – BAI	
PROCESO	BAI04. Gestionar la disponibilidad y la capacidad.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
BAI04.01. Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.	X		Recursos invertidos para el desarrollo de funciones	El DSI realiza el control de recursos con base a la partida presupuestaria del departamento. Se realizan actas que se dirigen al bodeguero, para registrar los materiales recibidos.	NO EFECTIVO	• Certificado de partida presupuestaria. • Hoja de trabajo Supervisor Informático (Ver Anexo 11)
BAI04.02. Evaluar el impacto en el negocio.		X				
BAI04.03. Planificar requisitos de servicio nuevos o modificados		X				
BAI04.04. Supervisar y revisar la disponibilidad y capacidad.		X				
BAI04.05. Investigar y abordar cuestiones de disponibilidad rendimiento y capacidad.		X				

Tabla 80. Verificación de cumplimiento BAI05

ÁREA	Gestión			**DOMINIO**	Construir, Adquirir e Implementar – BAI	
PROCESO	BAI05. Gestionar la introducción de cambios organizativos.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
BAI05.01. Establecer el deseo de cambiar.	X		Entrevista Dirección Gestión Administrativa	La Dirección de Gestión Administrativa ha manifestado que la EPMAPA-T, estará en periodo de cambios para la planificación 2020, debido a la nueva administración de la empresa.	NO EFECTIVO	• Hoja de trabajo Dirección de Gestión Administrativa (Ver Anexo 8) • Hoja de trabajo Supervisor Informático (Ver Anexo 11)
BAI05.02. Formar un equipo de implementación efectivo.		X				
BAI05.03. Comunicar la visión deseada.		X				
BAI05.04. Facultar a los que juegan algún papel e identificar ganancias en el corto plazo.		X				
BAI05.05. Facilitar la operación y el uso.		X				
BAI05.06. Integrar nuevos enfoques.		X				
BAI05.07. Mantener los cambios.		X				

Tabla 81. Verificación de cumplimiento BAI09

ÁREA	Gestión			**DOMINIO**	Construir, Adquirir e Implementar – BAI	
PROCESO	BAI09. Gestionar los activos.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
BAI09.01. Identificar y registrar activos actuales.	X		Inventario de activos (categorización, priorización y ciclo de vida) Licencias de aplicativos utilizados	El DSI dispone de un inventario de activos informáticos de la EPMAPA-T, sin categorizar ni priorizar. El ciclo de vida de los equipos fue establecido en el informe presentado a Dirección de Gestión Administrativa, con la finalidad de adquirir nuevo hardware. Los paquetes informáticos que cuentan con licencia son el antivirus y el sistema ERP.	NO EFECTIVO	• Inventario de activos • Informe estado de los equipos EPMAPA-T. • Hoja de trabajo Supervisor Informático (Ver Anexo 11)
BAI09.02. Gestionar los activos críticos.		X				
BAI09.03. Gestionar el ciclo de vida de los activos	X					
BAI09.04. Optimizar el coste de los activos.		X				
BAI09.05. Administrar licencias.		X				

Tabla 82. Verificación de cumplimiento BAI10

ÁREA	Gestión			**DOMINIO**	Construir, Adquirir e Implementar – BAI	
PROCESO	BAI10. Gestionar la configuración					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
BAI10.01. Establecer y mantener un modelo de configuración.		X	Relación de recursos y cumplimiento de funciones. Estado de los recursos y registro de configuración	Se ha logrado conocer el estado de los equipos mediante el informe realizado para la adquisición de nuevo hardware para la EPMAPA-T	NO EFECTIVO	• Informe estado de los equipos EPMAPA-T. • Hoja de trabajo Supervisor Informático (Ver Anexo 11)
BAI10.02. Establecer y mantener un repositorio de configuración y una base de referencia.		X				
BAI10.03. Mantener y controlar los elementos de configuración.		X				
BAI10.04. Generar informes de estado y configuración.	X					
BAI10.05. Verificar y revisar la integridad del repositorio de configuración		X				

Tabla 83. Verificación de cumplimiento DSS01

ÁREA	Gestión			**DOMINIO**	Entregar, dar Servicio y Soporte – DSS	
PROCESO	DSS01. Gestionar las operaciones					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
DSS01.01. Ejecutar procedimientos operativos.	X		Proceso de soporte técnico. Infraestructura tecnológica	Las actividades de soporte técnico son registradas, para el reporte de cumplimiento. Las instalaciones eléctricas no son aprobadas por técnicos especializados.	NO EFECTIVO	• Registro de soporte técnico. • Hoja de trabajo Supervisor Informático (Ver Anexo 11) • Hoja de trabajo Analista de sistemas (Ver Anexo 12)
DSS01.02. Gestionar servicios externalizados de TI.		X				
DSS01.03. Supervisar la infraestructura de TI		X				
DSS01.04. Gestionar el entorno.		X				
DSS01.05. Gestionar las instalaciones.		X				

Tabla 84. Verificación de cumplimiento DSS03

ÁREA	Gestión			**DOMINIO**	Entregar, dar Servicio y Soporte – DSS	
PROCESO	DSS03. Gestionar los problemas.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
DSS03.01. Identificar y clasificar problemas.		X	Clasificación de problemas. Gestión de problemas	En el proceso de soporte técnico el Analista de sistemas registra los incidentes, pero aún no se ha categorizado ni gestionado.	NO EFECTIVO	• Hoja de trabajo Analista de sistemas (Ver Anexo 12)
DSS03.02. Investigar y diagnosticar problemas.		X				
DSS03.03. Levantar errores conocidos.		X				
DSS03.04. Resolver y cerrar problemas		X				
DSS03.05. Realizar una gestión de problemas proactiva.		X				

Tabla 85. Verificación de cumplimiento DSS04

ÁREA	Gestión			**DOMINIO**	Entregar, dar Servicio y Soporte – DSS	
PROCESO	DSS04. Gestionar la continuidad.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
DSS04.01. Definir la política de continuidad de negocio, objetivos y alcance.		X	Plan de continuidad. Plan de respaldos de información y post-reanudación	El DSI no ha desarrollado un plan de continuidad frente a incidentes de TI. Se respalda la información del servidor mediante un aplicativo con una frecuencia diaria. El respaldo ya ha sido utilizado en una ocasión, después de un inconveniente donde se perdió información de la base de datos.	NO EFECTIVO	• Plan de respaldos de información-servidor. • Hoja de trabajo Supervisor Informático (Ver Anexo 11) • Hoja de trabajo Analista de sistemas (Ver Anexo 12)
DSS04.02. Mantener una estrategia de continuidad.		X				
DSS04.03. Desarrollar e implementar una respuesta a la continuidad de negocio.		X				
DSS04.04. Ejecutar, probar y revisar el plan de continuidad.		X				
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.		X				
DSS04.06. Proporcionar formación en el plan de continuidad.		X				
DSS04.07. Gestionar acuerdos de respaldo.	X					
DSS04.08. Ejecutar revisiones post- reanudación	X					

Tabla 86. Verificación de cumplimiento DSS05

ÁREA	Gestión			**DOMINIO**	Entregar, dar Servicio y Soporte – DSS	
PROCESO	DSS05. Gestionar los servicios de seguridad.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
DSS05.01. Proteger contra software malicioso	X		Antivirus en los equipos Seguridad de la red. Designación de privilegios, roles y permisos	Todos los equipos de la EPMAPA-T, cuentan con paquete de antivirus. La administración de la red institucional, se ha realizado en base a la categoría de la red. Se registra la totalidad de las direcciones en el diagrama topológico.	NO EFECTIVO	• Paquete de antivirus Kaspersky • Diagrama topológico • Hoja de trabajo Supervisor Informático (Ver Anexo 11) • Hoja de trabajo Analista de sistemas (Ver Anexo 12)
DSS05.02. Gestionar la seguridad de la red y las conexiones.		X				
DSS05.03. Gestionar la seguridad de los puestos de usuario final.		X				
DSS05.04. Gestionar la identidad del usuario y el acceso lógico	X					
DSS05.05. Gestionar el acceso físico a los activos de TI		X				
DSS05.06. Gestionar documentos sensibles y dispositivos de salida		X				
DSS05.07. Supervisar la infraestructura para detectar eventos relacionados con la seguridad.		X				

Tabla 87. Verificación de cumplimiento DSS06

ÁREA	Gestión			**DOMINIO**	Entregar, dar Servicio y Soporte – DSS	
PROCESO	DSS06. Gestionar los controles de los procesos de negocio.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
DSS06.01. Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos.		X	Designación de privilegios, roles y permisos	No se ha definido bajo registro los privilegios, roles y permisos de acceso a la red. La única verificación es que las direcciones se mantengan conforme al registro. En el sistema SIIM, se ingresa mediante autentificación de usuario y contraseña, para el cumplimiento de funciones en el Sistema Informático.	NO EFECTIVO	• Hoja de trabajo Supervisor Informático (Ver Anexo 11) • Hoja de trabajo Analista de sistemas (Ver Anexo 12)
DSS06.02. Controlar el procesamiento de información.		X				
DSS06.03. Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.		X				
DSS06.04. Gestionar errores y excepciones.		X				
DSS06.05. Asegurar la trazabilidad de los eventos y responsabilidades de información		X				
DSS06.06. Asegurar los activos de información.		X				

Tabla 88. Verificación de cumplimiento MEA01

ÁREA	Gestión			**DOMINIO**	Supervisar, Evaluar y Valorar – MEA	
PROCESO	MEA01. Supervisar, Evaluar y Valorar rendimiento y conformidad.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
MEA01.01. Establecer un enfoque de la supervisión		X	Evaluación de riesgos para el DSI, por parte del Sistema de control interno. Proceso de supervisión para el DSI	No se ha implementado sistema de control interno. La EPMAPA-T, no ha establecido procesos de supervisión para el DSI.	NO EFECTIVO	• Hoja de trabajo Control Interno (Ver Anexo 9)
MEA01.02. Establecer los objetivos de cumplimiento y rendimiento		X				
MEA01.03. Recopilar y procesar los datos de cumplimiento y rendimiento.		X				
MEA01.04. Analizar e informar sobre el rendimiento.		X				
MEA01.05. Asegurar la implantación de medidas correctivas.		X				

Tabla 89. Verificación de cumplimiento MEA03.

ÁREA	Gestión			**DOMINIO**	Supervisar, Evaluar y Valorar – MEA	
PROCESO	MEA03. Supervisar, Evaluar y Valorar la conformidad con los requerimientos externos.					
OBJETIVOS DE CONTROL	**CUMPLE**	**NO CUMPLE**	**REVISIÓN A TRAVÉS DE:**	**DESCRIPCIÓN DE LA PRUEBA**	**EVALUACIÓN**	**DOCUMENTOS DE SOPORTE**
MEA03.01. Identificar requisitos externos de cumplimiento.		X	Ítems de cumplimiento solicitados por ente gubernamental. TI, en informes de rendición de cuentas	Los requerimientos gubernamentales son específicos de las direcciones, por lo que el DSI no se toma en cuenta para el proceso de rendición de cuentas.	NO EFECTIVO	• Hoja de trabajo Control Interno (Ver Anexo 9)
MEA03.02. Optimizar la respuesta a requisitos externos. de requisitos externos.		X				
MEA03.03. Confirmar el cumplimiento de requisitos externos.		X				
MEA03.04. Obtener garantía de cumplimiento		X				

4.1.6. Informe final de Auditoría

10 enero de 2020

4.1.6.1. Tema del Proyecto de Titulación

Plan de mitigación de riesgos tecnológicos basado en auditoría informática a la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán.

4.1.6.2. Institución auditada

Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán (EPMAPA-T)

El proceso de auditoría informática se llevó a cabo bajo la metodología COBIT® 5, y evaluó principalmente el desarrollo de los procesos tecnológicos del Departamento de Supervisión Informática de la EPMAPA-T, que tuvo inicio en enero 2019 y finalizó en diciembre 2019.

El proceso fue desarrollado por Yuly Pantoja, estudiante de la Carrera de Ingeniería en Informática de la Universidad Politécnica Estatal del Carchi, bajo el asesoramiento del Ing Carlitos Guano docente de la misma Carrera.

Se realizó con apoyo de los siguientes interlocutores, el Ing Alejandro Obando y el MSc Jackson Obando miembros del DSI institucional, y en el área de Gobernanza la Ing Andrea Chávez Directora de Gestión Administrativa

La evaluación de auditoría comprendió los puntos, que se detallan a continuación:

- Desarrollo de procesos institucionales vinculados a TI.
- Desarrollo de procesos de tecnología en el DSI.
- Revisión de documentación institucional.
- Revisión de documentación del área de tecnología
- Gestión de riesgos institucional y de TI
- Determinar falencias de TI, a nivel físico y documental.

4.1.6.3. Procesos COBIT® 5 aplicables

Se determinó los procesos a evaluar con base al estudio inicial de la auditoría. Del total de 37 procesos COBIT® 5, 4 no fueron aplicables a evaluación y son los siguientes:

- APO04. Gestionar la innovación.
- BAI06. Gestionar los cambios.
- BAI07. Gestionar la aceptación del cambio y de la transición.
- MEA02. Supervisar, Evaluar y Valorar el sistema de control interno.

4.1.6.4. Capacidad del proceso auditados.

Se estableció la capacidad de procesos COBIT® 5 a 33 procesos aplicables.
Los procesos COBIT® 5, ha sido agrupados por cada dominio y se estableció la capacidad del proceso, de la siguiente manera:

- **0 Proceso incompleto**. El proceso no está implementado
- **1 Proceso ejecutado.** El proceso implementado alcanza el propósito.
- **2 Proceso gestionado.** El proceso implementado ya está planificado, supervisado y ajustado.
- **3 Proceso establecido**. El proceso implementado es capaz de alcanzar resultados
- **4 Proceso predecible**. El proceso implementado se ejecuta dentro límites para alcanzar resultados.
- **5 Proceso optimizado**. El proceso implementado es mejorado de forma continua para alcanzar metas presentes y futuras.

La valoración fue realizada con base a la siguiente fórmula:

$$\frac{N°\ objetivos\ de\ control\ con\ cumplimiento\ *\ Nivel\ más\ alto(5)}{N°\ de\ objetivos\ de\ control\ total} > 3$$

Esta valoración se realiza con base a la matriz de verificación, y para ello se toma en cuenta cada uno de los 33 procesos COBIT® 5 aplicables, se ha establecido que el valor óptimo de los procesos debe ser 3 ***(proceso establecido),*** considerando que los procesos evaluados deben ser gestionados, implementados y que sean capaces de alcanzar resultados.
Aquellos procesos que lleguen al valor óptimo o superen el mismo se consideran procesos ***efectivos***. De esta manera, los procesos que obtengan un nivel menor a tres se consideran ***no efectivos.*** En la siguiente matriz se detalla el nivel alcanzado actualmente por los procesos en la EPMAPA-T ***(color rojo)*** y el nivel óptimo al cuál se considera aceptable ***(color verde).***

Tabla 90. Análisis de cumplimiento - Evaluar, Orientar y Supervisar

GOBIERNO						
Dominio	**Proceso**	**Capacidad de proceso**			**Evaluación**	
		Obtenida	**Total**	**Óptima**	**Efectivo**	**No efectivo**
Evaluar, Orientar y Supervisar – EDM	EDM01. Asegurar el establecimiento y mantenimiento del marco de gobierno.	1.67	2	3		X
	EDM02. Asegurar la entrega de beneficios.	0	0	3		X
	EDM03. Asegurar la optimización del riesgo.	0	0	3		X
	EDM04. Asegurar la optimización de los recursos.	0	0	3		X
	EDM05. Asegurar la transparencia hacia las partes interesadas.	3.33	3	3	X	

Tabla 91. Análisis de cumplimiento - Alinear, Planificar y Organizar

GESTIÓN						
Dominio	**Proceso**	**Capacidad de proceso**			**Evaluación**	
		Obtenida	**Total**	**Óptima**	**Efectivo**	**No efectivo**
Alinear, Planificar y Organizar – APO	APO01. Gestionar el marco de gestión de TI.	2.5	3	3	X	
	APO02. Gestionar la estrategia.	0	0	3		X
	APO03. Gestionar la arquitectura empresarial.	2	2	3		X
	APO05. Gestionar el portafolio.	0	0	3		X
	APO06. Gestionar el presupuesto y los costes.	2	2	3		X
	APO07. Gestionar los recursos humanos.	1.67	2	3		X
	APO08. Gestionar las relaciones	0	0	3		X
	APO09. Gestionar los acuerdos de servicio.	0	0	3		X
	APO10. Gestionar los proveedores.	0	0	3		X
	APO11. Gestionar la calidad.	0	0	3		X
	APO12. Gestionar el riesgo.	0	0	3		X
	APO13. Gestionar la seguridad.	0	0	3		X

Tabla 92. Análisis de cumplimiento - Construir, Adquirir e Implementar

GESTIÓN						
Dominio	**Proceso**	**Capacidad de proceso**			**Evaluación**	
		Obtenida	**Total**	**Óptima**	**Efectivo**	**No efectivo**
Construir, Adquirir e Implementar – BAI	BAI01. Gestionar los programas y proyectos.	0.71	1	3		X
	BAI02. Gestionar la definición de requisitos.	0	0	3		X
	BAI03. Gestionar la identificación y la construcción de soluciones.	1.36	1	3		X
	BAI04. Gestionar la disponibilidad y la capacidad.	1	1	3		X
	BAI05. Gestionar la introducción de cambios organizativos.	0.71	1	3		X
	BAI08. Gestionar el conocimiento.	0	0	3		X
	BAI09. Gestionar los activos.	2	2	3		X
	BAI10. Gestionar la configuración	1	1	3		X

Tabla 93. Análisis de cumplimiento - Entregar, dar Servicio y Soporte

GESTIÓN						
Dominio	**Proceso**	**Capacidad de proceso**			**Evaluación**	
		Obtenida	**Total**	**Óptima**	**Efectivo**	**No efectivo**
Entregar, dar Servicio y Soporte – DSS	DSS01. Gestionar las operaciones	1	1	3		X
	DSS02. Gestionar las peticiones e incidentes del servicio.	0	0	3		X
	DSS03. Gestionar los problemas.	0	0	3		X
	DSS04. Gestionar la continuidad.	1.25	1	3		X
	DSS05. Gestionar los servicios de seguridad.	1.43	1	3		X
	DSS06. Gestionar los controles de los procesos de negocio.	0	0	3		X

Tabla 94. Análisis de cumplimiento - Supervisar, Evaluar y Valorar

GESTIÓN						
Dominio	**Proceso**	**Capacidad de proceso**			**Evaluación**	
		Obtenida	**Total**	**Óptima**	**Efectivo**	**No efectivo**
Supervisar, Evaluar y Valorar – MEA	MEA01. Supervisar, Evaluar y Valorar rendimiento y conformidad.	0	0	3		X
	MEA03. Supervisar, Evaluar y Valorar la conformidad con los requerimientos externos.	0	0	3		X

A continuación, se realiza una matriz resumen de la valoración por cada dominio COBIT®5.

Tabla 95. Valoración total de la evaluación

Área	Dominios COBIT® 5	Capacidad de proceso	
		Obtenida	**Total**
Gobierno	Evaluar, Orientar y Supervisar – EDM	1	1
Gestión	Alinear, Planificar y Organizar – APO	0,75	1
	Construir, Adquirir e Implementar – BAI	0,87	1
	Entregar, dar Servicio y Soporte – DSS	0,5	1
	Supervisar, Evaluar y Valorar – MEA	0	0
	Valoración total	**0,62**	**1**

EL Departamento de Supervisión Informática de la EPMAPA-T, obtiene el nivel de capacidad de proceso correspondiente a 1 ***(proceso ejecutado),*** que significa que la gran mayoría de los procesos implementados cumplen su propósito. Sin embargo, no han sido gestionados, implementados adecuadamente, no son capaces de generar resultados, no son predecibles y no se encuentran optimizados.

De 37 procesos COBIT® 5, 4 no fueron aplicables al proceso, por lo que la evaluación fue realizada a 33.

- Dos procesos efectivos.
- Treinta y uno no efectivos.

Los procesos efectivos o que se encuentran en niveles aceptables son:

- **EDM05. Asegurar la transparencia hacia las partes interesadas.**

El DSI emite reportes de cumplimiento de funciones dirigidos hacia Dirección de Gestión Administrativa. El formato es estándar para toda la dirección, de esta manera se da cumplimiento a dos objetivos de control correspondiente a un nivel 3.33 de 5, por ello se considera que EDM05 se encuentra como ***proceso establecido (nivel 3),*** por lo tanto, se considera ***efectivo.***

- **APO01. Gestionar el marco de gestión de TI.**

El área de tecnología tiene posición en la Estructura Orgánica Funcional, se han designado funciones por cada puesto del DSI, y se las ha comunicado mediante el contrato y revisión del *Manual de Descripción, Valoración y Clasificación de puestos*. Se han establecido objetivos de TI. Sin embargo, no han sido alineados a los objetivos institucionales, de manera documental. De esta manera se da cumplimiento a cuatro objetivos de control correspondiente al nivel 2.5 de 5, por ello se considera que APO01 se encuentre como ***proceso establecido (nivel 3),*** por lo tanto, se considera ***efectivo.***

4.1.6.5. Hallazgos por procesos no efectivo

Se realizó un proceso de auditoría al DSI, con base a los procesos COBIT® 5 siendo 37 en total, para ello se determinó que 4 de no eran aplicables.

El proceso de auditoría se realizó sobre 33 procesos COBIT® 5, donde se encontró dos procesos efectivos o que cumplen con los requerimientos de la metodología y son:

- EDM05. Asegurar la transparencia hacia las partes interesadas.
- APO01. Gestionar el marco de gestión de TI.

Por lo tanto, se procede a la determinación de hallazgos de auditoría correspondiente a 31 procesos COBIT® 5 no efectivos, mismos que se listan a continuación

Tabla 96. Procesos COBIT® 5 no efectivos.

Dominio	Procesos no efectivos	Hallazgos de auditoría
	GOBIERNO	
Evaluar, Orientar y Supervisar – EDM	EDM01. Asegurar el establecimiento y mantenimiento del marco de gobierno.	• Inexistente evaluación de eficacia y rendimiento de gobernanza, sobre TI
	EDM02. Asegurar la entrega de beneficios.	• Inexistente verificación de cumplimiento de objetivos de TI
	EDM03. Asegurar la optimización del riesgo.	• Inexistente gestión de riesgos

	EDM04. Asegurar la optimización de los recursos.	• Inadecuado seguimiento de recursos.
	GESTIÓN	
Alinear, Planificar y Organizar – APO	APO02. Gestionar la estrategia.	• Plan estratégico de TI desactualizado.
	APO03. Gestionar la arquitectura empresarial.	• Inexistencia de arquitectura de procesos de TI.
	APO05. Gestionar el portafolio.	• El DSI no ha considerado medidas de inversión en el área
	APO06. Gestionar el presupuesto y los costes.	• Inadecuada gestión de presupuesto.
	APO07. Gestionar los recursos humanos.	• Inexistente capacitación de tecnología hacia el personal DSI. • Falta de personal
	APO08. Gestionar las relaciones	• Inexistencia de procedimientos que permitan focalizar las situaciones emergentes del área.
	APO09. Gestionar los acuerdos de servicio.	• No se ha establecido un catálogo de servicios de TI. • No se han establecido procesos mejora continua, enfocada al de servicios.
	APO10. Gestionar los proveedores.	• Inexistente gestión proveedores de servicios de la empresa. • Inexistente evaluación de la minimización de coste para adquirir los servicios.
	APO11. Gestionar la calidad.	• Inexistente gestión de calidad enfocada a TI.
	APO12. Gestionar el riesgo.	• Inexistente Gestión de riesgos de TI
	APO13. Gestionar la seguridad.	• Inexistencia de sistema de seguridad de la información

Construir, Adquirir e Implementar – BAI	BAI01. Gestionar los programas y proyectos.	• Inadecuada gestión de planes, proyectos y programas en el DSI.
	BAI02. Gestionar la definición de requisitos.	• Inexistente análisis de requisitos previa la adquisición o desarrollo de una solución informática.
	BAI03. Gestionar la identificación y la construcción de soluciones.	• Soluciones tecnológicas adquiridas presentan fallas.
	BAI04. Gestionar la disponibilidad y la capacidad.	• Inexistente evaluación del rendimiento de los recursos de TI.
	BAI05. Gestionar la introducción de cambios organizativos.	• Falta de comunicación sobre los cambios a realizarse en la empresa.
	BAI08. Gestionar el conocimiento.	• Inexistencia de procesos documentadas para el área de TI
	BAI09. Gestionar los activos.	• Inventario de activos, sin categorizar. • Inventario de activos sin establecer prioridad y ciclo de vida. • Paquetes informáticos sin licencia.
	BAI10. Gestionar la configuración	• Inexistencia de un modelo de servicios, activos e infraestructura.
Entregar, dar Servicio y Soporte – DSS	DSS01. Gestionar las operaciones	• Inexistencia de un procedimiento que regule las actividades de soporte. • Instalaciones eléctricas sin evaluar por un técnico.
	DSS02. Gestionar las peticiones e incidentes del servicio.	• No contar con un plan de gestión de incidentes.
	DSS03. Gestionar los problemas.	• Existe una identificación de problemas, sin categorizar.
	DSS04. Gestionar la continuidad.	• No dispone de plan de continuidad frente a incidentes de TI.

	DSS05. Gestionar los servicios de seguridad.	• Acceso físico a la institución sin restricción. • No se han establecido medidas de seguridad en la red.
	DSS06. Gestionar los controles de los procesos de negocio.	• No se han establecido privilegios, roles y permisos para el usuario interno en la red. • No plantear procesos de mejora.
Supervisar, Evaluar y Valorar – MEA	MEA01. Supervisar, Evaluar y Valorar rendimiento y conformidad.	• Falta de eficiencia y optimización de recursos en los procesos realizados por el DSI • Inadecuado seguimiento de cumplimiento de funciones y actividades.
	MEA03. Supervisar, Evaluar y Valorar la conformidad con los requerimientos externos.	• Inadecuada evaluación al DSI, debido a que no se basan en normas externas (estándar). • Procesos institucionales y de TI, sin iniciativas de mejora.

En el plan de mitigación de riesgos tecnológicos, se emiten estrategias para llevar a cada uno de los procesos COBIT® 5 hacia niveles de 3 o superiores mismos que se consideran aceptables o efectivos.

4.1.7. Plan de mitigación de riesgos tecnológicos

PLAN DE MITIGACIÓN DE RIESGOS TECNOLÓGICOS

Objetivo.

Mitigar los riesgos identificados en el proceso de auditoría basada en la metodología COBIT® 5, con la finalidad de disminuir el impacto provocado por los incidentes de tecnología en la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán-EPMAPA-T

Periodo de auditoría. Enero 2019 – Diciembre 2019

Equipo de auditor.

Auditor Yuly Estefanía Pantoja Miño

Asesor Ing. Carlitos Alberto Guano Cárdenas, MSc.

La matriz de riesgos se realiza con base a la siguiente escala.

Tabla 97. Matriz de riesgos.

Impacto / Probabilidad		Bajo	Moderado bajo	Moderado medio	Alto
		1	2	3	4
Muy Probable	4	**RIESGO MEDIO** alta probabilidad – bajo impacto		**RIESGO ALTO** alta probabilidad – alto impacto	
Probable	3				
Posible	2	**RIESGO BAJO** baja probabilidad – bajo impacto		**RIESGO MEDIO** baja probabilidad -alto impacto	
Poco probable	1				

Fuente: Calderón y Ocaña (2014) *Auditoria informática basada en el análisis de riesgos a la empresa Tecniseguros S.A.*

Procesos institucionales

Los procesos institucionales han sido seleccionados, tomado en cuenta la priorización realizada en la planificación de auditoría, y son los siguientes.

- PI.2. Emisión
- PI.4. Recolección de lecturas.

A continuación, se expone las situaciones de riesgo identificadas para su respectivo análisis.

Tabla 98. Priorización de situaciones de riesgo - Emisión

PI.2 Emisión				
Cod.	**Situación de riesgo**	**Probabilidad**	**Impacto**	**Prioridad**
E.1	Equipo de recaudación con daño.	2	2	4
E.2	Falla en el módulo verificación de errores.	1	3	3

E.1. Equipo de recaudación con daño

El sistema informático SIIM, es un sistema que se encuentra en la red de la EPMAPA-T, por lo que se tiene acceso desde cualquier equipo informático que se encuentre dentro de la red institucional.

E.2. Falla en el módulo de verificación de errores.

El módulo de verificación es muy confiable, realiza la depuración de lecturas indicando los valores con observación y de esta manera el usuario interno realiza la respectiva corrección.

Tabla 99. Priorización de situaciones de riesgo – Recolección de lecturas

PI.4 Recolección de lecturas				
Cod.	**Situación de riesgo**	**Probabilidad**	**Impacto**	**Prioridad**
R.1	Base de datos con errores.	1	3	3
R.2	Zonas de falla del aplicativo	3	2	6
R.3	Actualizaciones defectuosas del aplicativo	3	3	9

R.1. Base de datos con errores.

En el caso que un código de abonado se haya ingresado de manera errónea, será casi imposible que lector encuentre al usuario externo.

R.2. Zonas de falla del aplicativo

En ocasiones el medidor se encuentra en zonas subterráneas de edificios de la ciudad, por lo que se dificulta la toma de lecturas, debido a que el aplicativo funciona con servicio de internet.

R.3. Actualizaciones defectuosas del aplicativo.

La aplicación móvil de lectura ha sido actualizada de su versión original, por lo que ha presentado fallas. Ha sido necesario contactar al creador para la inmediata solución, de lo contrario retrasa el proceso de recolección de lecturas.

Tabla 100. Matriz de riesgos- Procesos institucionales

Impacto / Probabilidad		Bajo	Moderado bajo	Moderado medio	Alto
		1	2	3	4
Muy Probable	**4**				
Probable	**3**		R2	R3	
Posible	**2**		E1		
Poco probable	**1**			E2, R1	

Con la valoración generada por la matriz, se procede a listar los riesgos desde los más altos hasta los bajos. Con fines de emitir las estrategias de mitigación.

Tabla 101. Estrategias de mitigación – Procesos institucionales.

Cod.	Situación de riesgo	Prioridad	Riesgo	Estrategias de mitigación
E.1	Equipo de recaudación con daño	4	Bajo	• Colocar a disposición del recaudador otro equipo de emergencia, con la finalidad que no sea necesario ocupar un equipo destinado a otras actividades.
E.2	Falla en el módulo de verificación de errores.	3	Medio	• La verificación de errores es un módulo implementado en el sistema SIIM, al ser un sistema creado externamente se debe considerar un acuerdo, donde el creador se comprometa a brindar soporte en caso que el sistema presente fallas.
R.1	Base de datos con errores	3	Medio	• Realizar una comprobación de los códigos de nuevos abonados ingresados con una frecuencia trimestral, con la finalidad de evitar que existan errores en la toma de lecturas.
R.2	Zonas de falla del aplicativo.	6	Medio	• Realizar la observación al creador, para que en futuras versiones sea posible ingresar los datos temporalmente de manera local, sin necesitar servicio de internet.
R.3	Actualizaciones defectuosas del aplicativo.	9	Alto	• Al ser un sistema creado por ente externo, es recomendable poner a prueba durante una semana para evaluar el funcionamiento del aplicativo, después de cada actualización. • Soporte en etapa de estabilización del Sistema • Realizar el proceso de pruebas de release con los involucrados, antes de pasar a producción.

Procesos del área de TI

Los procesos del área de TI han sido seleccionados mediante la priorización realizada en la planificación de auditoría, y son los siguientes.

- PTI.1. Soporte técnico a usuarios internos.
- PTI.3. Administración de sistemas informáticos
- PTI.4. Administración de base de datos y,
- PTI.5. Administración de redes

Para ello a continuación se exponen las situaciones de riesgo identificadas para cada proceso, con la finalidad de realizar su análisis.

Tabla 102. Priorización de riesgo – Soporte técnico a usuarios internos

PTI.1. Soporte técnico a usuarios internos.				
Cod.	**Situación de riesgo**	**Probabilidad**	**Impacto**	**Prioridad**
ST.1	Problemas críticos en soporte	3	3	9
ST.2	Inexistencia de materiales y herramientas en el DSI	4	2	8
ST.3	Excesivas solicitudes de soporte	2	2	4

ST.1. Problemas críticos en soporte.

El equipo de trabajo del DSI se ha enfrentado a situaciones donde el problema con el equipo informático es muy crítico, por lo que solicitan los implementos necesarios para lograr la solución. Este procedimiento lleva tiempo por lo que la solución se tarda.

ST.2. Inexistencia de materiales y herramientas en el DSI.

El DSI no cuenta con un stock de materiales y herramientas, las solicitudes son variadas y es necesario recurrir a implementos que no se disponen en la EPMAPA-T.

ST.3. Excesivas solicitudes de soporte.

Esta situación escasamente se ha dado, debido a que la empresa es pequeña. Existen inconvenientes cuando las oficinas periféricas de recaudación requieren soporte técnico debido a la movilización del personal encargado.

Tabla 103. Priorización de riesgo – Administración de sistemas informáticos

PTI3. Administración de sistemas informáticos				
Cod.	**Situación de riesgo**	**Probabilidad**	**Impacto**	**Prioridad**
ASI.1	Módulos de los sistemas informáticos con errores	3	3	9
ASI.2	Lentitud en los sistemas informáticos.	3	2	6

ASI.1 Módulos del sistema con errores

Mediante el estudio inicial se ha logrado identificar que algunos de los sistemas informáticos presentan errores, interrumpiendo el desarrollo de actividades de los usuarios internos.

ASI.2 Lentitud en los sistemas

Los usuarios internos han manifestado que existen situaciones que el sistema se vuelve lento, por lo que se retrasan las actividades del usuario interno.

Tabla 104. Priorización de riesgo – Administración de base de datos

PTI.4. Administración de base de datos				
Cod.	**Situación de riesgo**	**Probabilidad**	**Impacto**	**Prioridad**
ABD.1	Campos de la base de datos redundantes.	2	2	4
ABD.2	Inadecuado respaldo de información	1	3	3

ABD.1. Campos de la base de datos redundantes.

Se ha manifestado que la base de datos tiene campos redundantes, de esta manera se consume recursos innecesarios.

ABD.2. Inadecuado respaldo de información

El respaldo de información se realiza mediante una aplicativo que genera respaldos con frecuencia diaria, de los datos almacenados en el servidor. Sin embargo, se considera una situación de riesgo en el caso que el aplicativo deje de funcionar.

Tabla 105. Priorización de riesgo – Administración de redes

PTI.5. Administración de redes				
Cod.	**Situación de riesgo**	**Probabilidad**	**Impacto**	**Prioridad**
AR.1	Elementos de red con deterioro.	3	3	9
AR.2	Dispositivos de red con errores.	2	3	6
AR.3	Inadecuada distribución de elementos de red	2	2	4

AR.1. Elementos de red con deterioro.

Se ha presentado el caso en que los elementos de red presentan fallas debido a que han cumplido con su vida útil.

AR.2. Dispositivos de red con errores.

Se ha presentado el caso que dispositivos nuevos instalados presentan fallas de fábrica, generando inconvenientes en el desempeño de funciones.

AR.3. Inadecuada distribución de elementos de red

Esta situación no se ha presentado actualmente. Sin embargo, se considera una situación de riesgo debido a las iniciativas de cambio que se llevan a cabo en la EPMAPA-T.

Tabla 106. Matriz de riesgos – Procesos del área de TI

Impacto / **Probabilidad**		**Bajo**	**Moderado bajo**	**Moderado medio**	**Alto**
		1	**2**	**3**	**4**
Muy Probable	**4**		ST.2		
Probable	**3**		ASI.2	ST.1, ASI.1 AR.1	
Posible	**2**		ST.3, ABD.1 AR.3	AR.2	
Poco probable	**1**			ABD.2	

Tabla 107. Estrategias de mitigación – Procesos del área de TI.

Cod.	Situación de riesgo	Prioridad	Riesgo	Estrategias de mitigación
ST.1	Problemas críticos en soporte	9	Alto	• Disponer de un Plan de Gestión de Incidentes de TI, que permita direccionar las actividades para cada tipo de problema.
ST.2	Inexistencia de materiales y herramientas en el DSI	8	Medio	• Determinar los implementos y materiales más comunes para lograr el cumplimiento de una solicitud de ayuda, con la finalidad de incluir en el plan de adquisiciones para el DSI.
ST.3	Excesivas solicitudes de soporte	4	Bajo	• Establecer una mesa de servicio para el usuario interno • Designar las solicitudes a solucionar para cada uno de los miembros del personal del DSI. • Determinar el tiempo estimado a invertir en la solución, para aquellas solicitudes ubicadas en oficinas de recaudación periféricas.
ASI.1	Módulos del sistema con errores	9	Alto	La totalidad de los sistemas informáticos, han sido adquiridos por lo tanto no se tiene control sobre el funcionamiento de los mismos. • Establecer acuerdos de servicios con el proveedor, con la finalidad de obtener apoyo técnico en el caso que fallo de alguno de ellos. • Desarrollar de sistemas informáticos propios.
ASI.2	Lentitud en los sistemas	6	Medio	• Realizar pruebas de hardware. • Realizar pruebas de estrés al software en colaboración con el proveedor. • Escaneo de vulnerabilidades.

				• Control de tráfico y navegación web • Monitoreo de red.
ABD.1	Campos de la base de datos redundantes.	4	Bajo	• Proceso de mantenimiento a la base de datos. • Utilizar un aplicativo que aplique la forma normal de base de datos. • Monitoreo del funcionamiento de la base de datos con una frecuencia mensual.
ABD.2	Inadecuado respaldo de información	3	Medio	• Realizar batch diario de la totalidad de información. • Almacenar el respaldo en una oficina alterna, con fines de aseguramiento.
AR.1	Elementos de red con deterioro.	9	Alto	• Establecer ciclo de vida de cada elemento de red, de manera que, si uno llegará a fallar el cambio sea inmediato basado en un diagnóstico preventivo. • Test de velocidad en el funcionamiento de los elementos de red.
AR.2	Dispositivos de red con errores.	6	Medio	• Monitoreo de la red.
AR.3	Inadecuada distribución de elementos de red	4	Bajo	• Disponer de un stock de dispositivos comunes, con la finalidad que el cambio sea inmediato. • Ejecutar tareas de distribución de la red, con el apoyo de un técnico experto. • Realizar cableado estructurado.

Procesos COBIT® 5

Metodología COBIT® 5

COBIT® 5 es una metodología enfocada al desarrollo de políticas y prácticas de control para el área de TI en las organizaciones. La finalidad principal es cumplimiento de los objetivos institucionales.

Para el presente proyecto se tomó en cuenta como la metodología base de estudio y permitió realizar una evaluación a la situación tecnológica de la EPMAPA-T, obteniendo como resultado el PLAN DE MTIGACIÓN DE RIESGOS TECNOLÓGICOS, que permitirá reducir el riesgo de TI.

La EPMAPA-T, es una empresa pública que provee de servicio de agua potable y alcantarillado a la ciudad de Tulcán, cuenta con un Departamento de Supervisión Informática, que cumple con funciones enfocadas a la administración tecnológica de la institución.

Determinación de riesgos

Los riesgos son situaciones conflictivas que se encuentran presente en el cumplimiento de los procesos, para este análisis se han divido en dos grupos y son los siguientes:

- ***Riesgos externos.*** Aquellos riesgos que se encuentran presente todo el tiempo o se encuentran asociados a situaciones ajenas a la institución.
- ***Riesgos internos.*** Aquellos riesgos que se pueden controlar desde una unidad especializada, para el normal desempeño de las actividades institucionales.

Riesgos externos

Existen situaciones de riesgo externo que pueden afectar con alto impacto a la empresa y al área de TI, por ello se ha recopilado un listado de situaciones de riesgo, tomando en cuenta la realidad de la zona y las amenazas que se puedan presentar, siendo las siguientes:

- Terremoto
- Erupción Volcánica
- Incendio
- Robo de equipos informáticos
- Daño a las instalaciones.
- Corte de suministro eléctrico indefinidamente

A continuación, se procede a la priorización de este tipo de amenazas, para su respectivo análisis

Tabla 108. Priorización riesgos externos.

Riesgos externos.				
Cod.	**Situación de riesgo**	**Probabilidad**	**Impacto**	**Prioridad**
R.E.01	Terremoto	1	4	4
R.E.02	Erupción Volcánica	1	3	3
R.E.03	Incendio	2	4	8
R.E.04	Robo de equipos informáticos	2	4	8
R.E.05	Daño a las instalaciones.	2	4	8
R.E..06	Corte de suministro eléctrico indefinidamente	3	4	12

Se ha establecido que el riesgo es inherente e incierto, se desconoce el momento que se darán los hechos, lo único seguro es que cada uno de ellos tendrá un impacto fuerte.

La obligación del DSI es realizar los estudios necesarios para minimizar el porcentaje de consecuencias graves para la EPMAPA-T. A continuación, se realiza el análisis y posteriormente se emitirán las estrategias de mitigación.

Tabla 109. Matriz de riesgos externos

Impacto / Probabilidad		Bajo	Moderado bajo	Moderado medio	Alto
		1	2	3	4
Muy Probable	**4**				
Probable	**3**				R.E.06
Posible	**2**				R.E.03 R.E.04 R.E.05
Poco probable	**1**			R.E.02	R.E.01

Estrategias de mitigación riesgos externos.

Tabla 110. Estrategias de mitigación riesgos externos.

TERREMOTO					
Cod.	R.E.01	**Prioridad**	4	**Tipo de riesgo**	Medio baja probabilidad – alto impacto
DESCRIPCIÓN					
Es un riesgo que se ubica entre las catástrofes naturales con mayores consecuencias negativas. Se registran indicios de este riesgo en años atrás, en la actualidad se registran sismos de menor magnitud que no han generado gran impacto. Sin embargo, hay que tomar en cuenta la ubicación geográfica del Ecuador, que se encuentra en peligro de colisión de placas tectónicas.					
ESTRATEGIAS DE MITIGACIÓN					
• Realizar simulacros de evacuación con una frecuencia semestral. • Almacenar el respaldo de información en otra oficina, de preferencia fuera de la ciudad. • Incluir especificaciones técnicas sobre este riesgo en el plan de continuidad de TI, frente a desastres. • Detallar un comité de emergencias.					

ERUPCIÓN VOLCÁNICA					
Cod.	R.E.02	**Prioridad**	3	**Tipo de riesgo**	Medio baja probabilidad – alto impacto

DESCRIPCIÓN

Es un riesgo de menor impacto que los anteriores, debido a que en la localidad no existe aproximación de volcanes. Sin embargo, al estar ubicados en la cordillera de los andes, las erupciones volcánicas de otros afectan en magnitud proporcional a la distancia.

ESTRATEGIAS DE MITIGACIÓN

- Almacenar el respaldo de información en una oficina alterna, de preferencia fuera de la ciudad.
- Incluir las consideraciones a seguir dependiendo del tipo de alerta emitida para la localidad por el organismo encargado para el efecto (Gestión de riesgos, ECU911, etc)
- Incluir especificaciones técnicas sobre este riesgo en el Plan de continuidad de TI, frente a desastres.

INCENDIO					
Cod.	R.E.03	**Prioridad**	8	**Tipo de riesgo**	Medio baja probabilidad – alto impacto

DESCRIPCIÓN

El incendio es un riesgo que se puede provocar por diversos factores internos de esta manera la responsabilidad sería propia, como también puede darse el caso de que un incendio estructural de edificios aledaños, causen este riesgo a la infraestructura de la empresa.

ESTRATEGIAS DE MITIGACIÓN

- Evaluación de las conexiones eléctricas de la institución.
- Instalación sistemas contra incendio.
- Instalación de alarmas contra incendio.
- Dar mantenimiento periódico a los extintores de la institución.
- Almacenar respaldo de información en otro lugar, de preferencia en oficinas fuera de la ciudad.
- Incluir especificaciones técnicas sobre este riesgo en el Plan de continuidad de TI, frente a desastres.

ROBO DE EQUIPOS INFORMÁTICOS					
Cod.	R.E.04	**Prioridad**	8	**Tipo de riesgo**	Medio baja probabilidad – alto impacto

DESCRIPCIÓN

Es un riesgo que puede comprometer la seguridad de la información de la empresa, debido a que existe información interna que no se respalda de los equipos informáticos y que representa una prioridad de la institución.

ESTRATEGIAS DE MITIGACIÓN

- Reforzar la seguridad física de la institución.
- Contratación de seguridad privada.
- Restringir el acceso físico en horas no laborables.
- Instalación de cámaras de seguridad.
- Generar un plan de respaldos básico para información interna de la institución.
- Clasificar información en privada, pública y confidencial.
- Establecer NASS en red para archivos críticos.

DAÑO A LAS INSTALACIONES					
Cod.	R.E.05	**Prioridad**	8	**Tipo de riesgo**	Medio baja probabilidad – alto impacto

DESCRIPCIÓN

Es un riesgo que provocaría un daño físico a la infraestructura, y dependiendo del impacto puede dañar de manera irreparable equipos informáticos e instalaciones de gran importancia.

ESTRATEGIAS DE MITIGACIÓN

- Instalación de cámaras de seguridad.
- Almacenar respaldo de información en otro lugar, de preferencia en oficinas fuera de la ciudad.
- Incluir especificaciones técnicas sobre este riesgo en el Plan de continuidad de TI, frente a desastres.
- Contar con una oficia alterna, que permita reanudar las actividades de momento.

CORTE DE SUMINISTRO ELÉCTRICO INDEFINIDAMENTE					
Cod.	R.E.06	**Prioridad**	12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto
DESCRIPCIÓN					
Interrupción de actividades debido a la falta de suministro eléctrico en la EPMAPA-T, riesgo de alto impacto para el funcionamiento del servidor.					
ESTRATEGIAS DE MITIGACIÓN					
• Verificación del funcionamiento del generador eléctrico. • Mantenimiento preventivo del generador eléctrico. • Evaluación del tiempo de suministro eléctrico de respaldo, es suficiente o es necesario ampliar. • Incluir especificaciones técnicas sobre este riesgo en el Plan de continuidad de TI, frente a desastres. • Contar con UPS y líneas protegidas.					

Riesgos internos.

Los riesgos internos son aquellos que dependen de la gestión de la empresa cuyos impactos o consecuencias influyen tanto en nivel general o en cada una de sus Direcciones y/o áreas. Se pueden mitigar o minimizar el impacto gracias una correcta gestión de los mismos.

Para este caso se ha tomado en cuenta un total de 26 riesgos que se encontraron mediante los hallazgos de auditoría informática aplica al DSI de la EPMAPA-T con base a la metodología COBIT® 5, para ello se procede a agrupar los riesgos por cada proceso afectado.

Tabla 111. Riesgos internos basados en hallazgos de auditoría

Cod.	Situación de riesgo	Proceso COBIT® 5 afectados
R.I.01	Incumplimiento de objetivos TI	EDM.01, EDM.02
R.I.02	Riesgos de TI, sin gestionar	EDM.03, APO.12
R.I.03	Inadecuada gestión de recursos	EDM.04, BAI.04
R.I.04	Estrategias de TI, desactualizadas	APO.02
R.I.05	Procesos de TI, sin documentar	APO.03, BAI.08, DSS.06
R.I.06	Presupuesto, costes e inversión de TI. gestionados inadecuadamente	APO.05, APO.06
R.I.07	Insuficiente capacitación al personal	APO.07
R.I.08	Personal de TI insuficiente	APO.07
R.I.09	Servicios de TI, sin identificar	EDM.01, APO.09, BAI.10
R.I.10	Inadecuada gestión de proveedores de servicio	APO.10
R.I.11	Procesos sin métricas de calidad	APO.03, APO.11, BAI.08
R.I.12	Información, sin asegurar adecuadamente	APO.13
R.I.13	Planes, proyectos y programas relacionados con TI, sin gestionar adecuadamente	BAI.01
R.I.14	Soluciones informáticas que no cumplen con las expectativas	BAI.02
R.I.15	Soluciones informáticas, presentan fallas	BAI.03
R.I.16	Activos de TI, sin gestionar adecuadamente	BAI.09
R.I.17	Paquetes informáticos sin licencia	APO.13, BAI.09
R.I.18	Soporte técnico, sin regular bajo procedimiento	DSS.01
R.I.19	Instalaciones e Infraestructura de TI, sin evaluación externa.	APO.13, DSS.01, DSS.05
R.I.20	Incapacidad de corregir incidentes frecuentes	DSS.02

R.I.21	Problemas de TI, sin categorizar	DSS.03
R.I.22	Inexistencia de plan de continuidad de TI frente a desastres.	EDM.03, DSS.04
R.I.23	Acceso físico a la institución sin restricción.	DSS.05
R.I.24	Inadecuada gestión de acceso lógico de los usuarios a la red	DSS.05, DSS.06
R.I.25	Inadecuado proceso de supervisión hacia el DSI	EDM.01, EDM.02, MEA.01
R.I.26	Inexistencia de una unidad de control interno institucional	MEA.01, MEA.03

A continuación, se procede a realizar la valoración del riesgo con base a la escala de probabilidad e impacto, para su respetivo análisis.

Tabla 112. Priorización riesgos internos.

Riesgos internos.				
Cod.	**Situación de riesgo**	**Probabilidad**	**Impacto**	**Prioridad**
R.I.01	Incumplimiento de objetivos TI	3	3	9
R.I.02	Riesgos de TI, sin gestionar	3	4	12
R.I.03	Inadecuada gestión de recursos	2	3	6
R.I.04	Estrategias de TI, desactualizadas	2	3	6
R.I.05	Procesos de TI, sin documentar	4	3	12
R.I.06	Presupuesto, costes e inversión de TI. gestionados inadecuadamente	2	3	6
R.I.07	Insuficiente capacitación al personal	1	3	3
R.I.08	Personal de TI insuficiente	3	4	12
R.I.09	Servicios de TI, sin identificar	3	4	12
R.I.10	Inadecuada gestión de proveedores de servicio	2	4	8
R.I.11	Procesos sin métricas de calidad	3	3	9

R.I.12	Información, sin asegurar adecuadamente	4	4	16
R.I.13	Planes, proyectos y programas relacionados con TI, sin gestionar adecuadamente	2	4	8
R.I.14	Soluciones informáticas que no cumplen con las expectativas	1	3	3
R.I.15	Soluciones informáticas, presentan fallas	2	3	6
R.I.16	Activos de TI, sin gestionar adecuadamente	2	3	6
R.I.17	Paquetes informáticos sin licencia	3	2	6
R.I.18	Soporte técnico, sin regular bajo procedimiento	4	3	12
R.I.19	Instalaciones e infraestructura de TI, sin evaluación externa.	2	4	8
R.I.20	Incapacidad de corregir incidentes frecuentes	2	3	6
R.I.21	Problemas de TI, sin categorizar	2	4	8
R.I.22	Inexistencia de plan de continuidad de TI frente a desastres.	3	4	12
R.I.23	Acceso físico a la institución sin restricción.	3	4	12
R.I.24	Inadecuada gestión de acceso lógico de los usuarios a la red	4	4	16
R.I.25	Inadecuado proceso de supervisión hacia el DSI	3	4	12
R.I.26	Inexistencia de una unidad de control interno institucional	3	4	12

Una vez realizado la priorización, correspondiente a riesgos internos, basado en COBIT® 5, se procede a colocar en la matriz de riesgos.

Tabla 113. Matriz de riesgos internos

Impacto / Probabilidad		Bajo	Moderado bajo	Moderado medio	Alto
		1	2	3	4
Muy Probable	**4**			R.I.18	R.I.12 R.I.24
Probable	**3**		R.I.17	R.I..01 R.I.11	R.I.02 R.I.05 R.I.08 R.I.09 R.I.22 R.I.23 R.I.25 R.I.26
Posible	**2**			R.I.03 R.I.04 R.I.06 R.I.15 R.I.16 R.I.20	R.I.10 R.I.13 R.I.19 R.I.21
Poco probable	**1**			R.I.07 R.I.14	

Estrategias de mitigación riesgos internos

Las estrategias de mitigación consisten en pautas y creación de documentación que contribuirá a lograr los objetivos planteados en el área de TI.

Tabla 114. Estrategias de mitigación riesgos internos

INCUMPLIMIENTO DE OBJETIVOS TI					
Cod.	R.I.01	**Prioridad**	9	**Tipo de riesgo**	Alto alta probabilidad – alto impacto
Descripción					
Este riesgo se presenta debido a que no existe una correcta evaluación hacia los objetivos de TI. Tampoco se ha realizado la alineación hacia los objetivos institucionales, por lo que el personal del DSI asumen que se cumplen efectivamente.					
Estrategias de mitigación					**Responsables**
• Plan de evaluación de objetivos de TI, basado en los reportes de cumplimiento de funciones. • Matriz de alineamiento tecnológico con los objetivos estratégicos institucionales.					• Dirección de Gestión Administrativa.

RIESGOS DE TI, SIN GESTIONAR					
Cod.	R.I.02	**Prioridad**	12	**Tipo de riesgo**	Alto alta probabilidad – alto impacto
Descripción					
La EPMAPA-T no ha identificado riesgos de TI bajo estándares, por lo que no se ha realizado gestión de los mismos hasta la fecha.					
Estrategias de mitigación					**Responsables**
• Identificar riesgos. • Plan de mitigación de riesgos tecnológicos. • Plan de gestión de riesgos.					• Auditora • DSI

INADECUADA GESTIÓN DE RECURSOS					
Cod.	R.I.03	**Prioridad**	6	**Tipo de riesgo**	Medio baja probabilidad – alto impacto
Descripción					
Se ha identificado que no existe una optimización de recursos en el área de TI.					
Estrategias de mitigación					**Responsables**
• Plan de recursos. (administración, responsable, procesos)					• DSI

ESTRATEGIAS DE TI, DESACTUALIZADAS					
Cod.	R.I.04	**Prioridad**	6	**Tipo de riesgo**	Medio baja probabilidad – alto impacto
Descripción					
El DSI opera bajo un plan estratégico de TI desactualizado.					
Estrategias de mitigación					**Responsables**
• Actualizar el plan estratégico de TI, a la planificación 2020.					• DSI

PROCESOS DE TI, SIN DOCUMENTAR					
Cod.	R.I.05	**Prioridad**	12	**Tipo de riesgo**	Alto alta probabilidad – alto impacto
Descripción					
El DSI, cumple con los procesos de manera empírica, debido a que no cuenta con un manual de procesos y procedimientos exclusivo del área de TI					
Estrategias de mitigación					**Responsables**
• Manual de procesos y procedimientos de TI					• DSI

PRESUPUESTO, COSTES E INVERSIÓN DE TI. GESTIONADOS INADECUADAMENTE					
Cod.	R.I.06	**Prioridad**	6	**Tipo de riesgo**	Medio baja probabilidad – alto impacto
Descripción					
El DSI trabaja bajo la asignación anual detallada en el Plan Operativo Anual – POA. Sin embargo, la gestión de recursos no se ha realizado adecuadamente.					
Estrategias de mitigación					**Responsables**
• Plan de recursos. (administración, responsable, procesos) • Plan presupuestario para el DSI.					• DSI

INSUFICIENTE CAPACITACIÓN AL PERSONAL					
Cod.	R.I.07	**Prioridad**	3	**Tipo de riesgo**	Medio baja probabilidad – alto impacto
Descripción					
El DSI, ha participado de jornadas de capacitación, pero ninguna vinculada a la actualización de conocimientos del área de TI.					
Estrategias de mitigación					**Responsables**
• Plan de capacitación para el DSI. • Evaluación de habilidades y destrezas del personal DSI, con la finalidad de identificar el personal idóneo para formar parte del equipo de trabajo DSI.					• Talento Humano

PERSONAL DE TI INSUFICIENTE					
Cod.	R.I.08	**Prioridad**	12	**Tipo de riesgo**	Alto alta probabilidad – alto impacto

Descripción
La distribución de la Estructura Orgánica Funcional de la EPMAPA-T detalla que el DSI se conforma de un Supervisor Informático y dos técnicos (Analistas de sistema), por lo que el equipo de trabajo está incompleto.

Estrategias de mitigación	**Responsables**
• Incluir en el Plan Anual de Contratación - PAC, al Analista de sistemas faltante. • Asignar funciones al Analista contratado.	• Talento Humano

SERVICIOS DE TI, SIN IDENTIFICAR					
Cod.	R.I.09	**Prioridad**	12	**Tipo de riesgo**	Alto alta probabilidad – alto impacto

Descripción
La EPMAPA-T ha desarrollado un *REGLAMENTO DE PRESTACIÓN DE SERVICIOS* dirigido al usuario externo. Sin embargo, no se ha tomado en cuenta la incidencia de tecnología para el cumplimiento de dichos servicios, es necesario identificarlos y documentarlos para un mejor cumplimiento

Estrategias de mitigación	**Responsables**
• Creación del catálogo de servicios de TI, enfocado al cumplimiento de objetivos Ti e institucionales de la EPMAPA-T. • Implementar proceso de mejora enfocada a servicios de tecnología • Establecer niveles de servicio de TI	• DSI

INADECUADA GESTIÓN DE PROVEEDORES DE SERVICIO					
Cod.	R.I.10	**Prioridad**	8	**Tipo de riesgo**	Medio baja probabilidad – alto impacto

Descripción

No se ha realizado una gestión de proveedores que ofrecen servicios tecnológicos hacia la EPMAPA-T

Estrategias de mitigación	Responsables
• Elaborar acuerdos de servicio con los proveedores en caso de falla. • Establecer una matriz de servicios tecnológicos indispensables y comparar los beneficios con el coste. • Identificar los proveedores mas frecuentes y establecer el nivel de cumplimiento de los acuerdos.	• DSI • Proveedores de servicios tecnológicos.

PROCESOS SIN MÉTRICAS DE CALIDAD					
Cod.	R.I.11	**Prioridad**	9	**Tipo de riesgo**	Alto alta probabilidad – alto impacto

Descripción

Actualmente, los procesos tecnológicos se llevan a cabo de manera empírica, sin seguir normas o procedimientos definidos, por lo que es necesario principalmente documentarlos y luego implementar métricas que permitan generar eficiencia y optimización de recursos.

Estrategias de mitigación	Responsables
• Manual de procesos y procedimientos de TI • Establecer políticas de calidad basados en ISO 9001 en el manual, referente al cumplimiento de procesos y procedimientos.	• DSI

INFORMACIÓN, SIN ASEGURAR ADECUADAMENTE					
Cod.	R.I.12	**Prioridad**	16	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto
Descripción					
Se ha identificado que la EPMAPA-T no cuenta con un sistema de seguridad de la información, que permita asegurar la integridad, disponibilidad y confidencialidad. Es por ello que se considera uno de los riesgos más importantes a mitigar					
Estrategias de mitigación					**Responsables**
• Plan de seguridad de la información, que incluya áreas, procedimientos, respaldo de información, y restricción de acceso. • Desarrollar el manual de seguridad de la información. • Socializar el manual de seguridad de la información hacia quienes conforman la EPMAPAT.					• DSI • Dirección de Gestión Administrativa

PLANES, PROYECTOS Y PROGRAMAS RELACIONADOS CON TI, SIN GESTIONAR ADECUADAMENTE					
Cod.	R.I.13	**Prioridad**	8	**Tipo de riesgo**	Medio baja probabilidad – alto impacto
Descripción					
Se ha identificado que la ejecución de planes, proyectos y programas no se han documentado. La designación de funciones se realiza de manera verbal y el método de evaluación durante la ejecución del plan, proyecto y/o programa no se realiza conforme a métricas o estándares.					
Estrategias de mitigación					**Responsables**
• Creación de procedimiento regulatorio que permita gestionar los planes, proyectos y programas. • Incluir los planes, proyectos y programas en los informes previo la asignación del POA • Evaluar bajo estándares, que permitan generar calidad de ejecución en el proceso.					• DSI

SOLUCIONES INFORMÁTICAS QUE NO CUMPLEN CON LAS EXPECTATIVAS					
Cod.	R.I.14	**Prioridad**	3	**Tipo de riesgo**	Medio baja probabilidad – alto impacto
Descripción					
Es muy importante realizar un análisis de requerimientos previo la adquisición o desarrollo de una solución tecnológica, para que no existen inconvenientes en la fase de implementación.					
Estrategias de mitigación					**Responsables**
• Adecuado análisis de requerimientos, previa adquisición o desarrollo de una solución tecnológica. • Incluir a la totalidad de interesados, para que el análisis sea completo.					• DSI • Creador de la solución

SOLUCIONES INFORMÁTICAS, PRESENTAN FALLAS					
Cod.	R.I.15	**Prioridad**	6	**Tipo de riesgo**	Medio baja probabilidad – alto impacto
Descripción					
Existe el inconveniente que varias de las soluciones informáticas adquiridas, presentan fallas lo que altera el desarrollo de funciones por parte de los usuarios internos que hacen uso de los sistemas.					
Estrategias de mitigación					**Responsables**
• Acuerdo o compromiso firmado, donde el creador se comprometa a brindar soporte inmediato en caso que el sistema presente fallas.					• DSI • Creador de la solución

ACTIVOS DE TI, SIN GESTIONAR ADECUADAMENTE					
Cod.	R.I.16	**Prioridad**	6	**Tipo de riesgo**	Medio baja probabilidad – alto impacto

Descripción
El DSI ha generado un inventario de activos de tecnología, donde no se ha establecido la importancia de cada uno de ellos, ni se les ha categorizado. Existe un informe que detalla el estado de los equipos, pero estas observaciones no se han incluido en el inventario.

Estrategias de mitigación	**Responsables**
• Inventario de activos completo (importancia, categorías, ciclo de vida)	• DSI

PAQUETES INFORMÁTICOS SIN LICENCIA					
Cod.	R.I.17	**Prioridad**	6	**Tipo de riesgo**	Medio alta probabilidad – bajo impacto

Descripción
Se ha manifestado que los paquetes que poseen licencia son sistema ERP y el paquete de antivirus Kaspersky. Por el contrario, aplicativos ofimáticos (Microsoft Office), sistema operativo (Windows), AUTOCAD y otros aplicativos no cuentan con licencia de funcionamiento.

Estrategias de mitigación	**Responsables**
• Adquirir las licencias. • Gestionar licencias existentes, tener en cuenta la fecha de caducidad, para su renovación • Utilizar paquetes informáticos de licencia gratuita.	• DSI • Dirección de Gestión Administrativa.

SOPORTE TÉCNICO, SIN REGULAR BAJO PROCEDIMIENTO					
Cod.	R.I.18	**Prioridad**	12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto
Descripción					
El proceso de soporte técnico ha presentado mejoras, debido al registro que se lleva a cabo por el equipo de trabajo del DSI. Sin embargo, el proceso no ha sido documentado.					
Estrategias de mitigación				**Responsables**	
• Incluir al proceso de soporte técnico, en el manual de procesos y procedimientos de TI.				• DSI	

INSTALACIONES E INFRAESTRUCTURA DE TI, SIN EVALUACIÓN EXTERNA.					
Cod.	R.I.19	**Prioridad**	8	**Tipo de riesgo**	Medio baja probabilidad – alto impacto
Descripción					
Se ha manifestado mediante entrevista que las instalaciones eléctricas no han sido verificadas por un técnico experto, así como también la distribución de los elementos de red no se han realizado con base en una norma o estándar.					
Estrategias de mitigación				**Responsables**	
• Verificar que la distribución de los elementos de red, se realicen con base a un estándar que brinde seguridad. • Evaluar el estado de la conexión eléctrica de la empresa con fines de asegurar la integridad de la institución.				• DSI • Técnico en conexiones eléctricas • Dirección de Gestión Administrativa	

INCAPACIDAD DE CORREGIR INCIDENTES FRECUENTES					
Cod.	R.I.20	**Prioridad**	6	**Tipo de riesgo**	Medio baja probabilidad – alto impacto
Descripción					
Se ha identificado que no se dispone de una categorización, priorización y métodos de solución para incidentes frecuentes debidamente documentados.					
Estrategias de mitigación				**Responsables**	
• Desarrollo del plan de gestión de incidentes, basado en el registro de soporte técnico • Emitir soluciones para incidentes frecuentes.				• DSI	

PROBLEMAS DE TI, SIN CATEGORIZAR					
Cod.	R.I.21	**Prioridad**	8	**Tipo de riesgo**	Medio baja probabilidad – alto impacto
Descripción					
El DSI no ha identificado y clasificado los problemas de TI, es de vital importancia categorizar errores conocidos, tiempo de respuesta y métodos de solución.					
Estrategias de mitigación				**Responsables**	
• Establecer el plan de Gestión de incidentes y categorizar por tipo de problemas. • Establecer niveles de servicio de TI				• DSI	

INEXISTENCIA DE PLAN DE CONTINUIDAD DE TI FRENTE A DESASTRES.					
Cod.	R.I.22	**Prioridad**	12	**Tipo de riesgo**	Alto alta probabilidad – alto impacto
Descripción					
El DSI no dispone de un plan de continuidad frente a desastres, su importancia radica en que mediante este documento se tiene el procedimiento a seguir para superar una situación adversa.					
Estrategias de mitigación				**Responsables**	
• Generar un plan de continuidad de TI, frente a desastres. • Incluir los riesgos externos identificados en este documento				• DSI • Dirección de Gestión Administrativa	

ACCESO FÍSICO A LA INSTITUCIÓN SIN RESTRICCIÓN.					
Cod.	R.I.23	**Prioridad**	12	**Tipo de riesgo**	Alto alta probabilidad – alto impacto
Descripción					
El acceso físico de la institución no se encuentra controlado por un experto de seguridad privada. En las funciones del conserje del edificio señala vigilar el acceso, mismo que no se considera suficiente, tomando en cuenta el nivel de crecimiento de la empresa en los últimos años.					
Estrategias de mitigación				**Responsables**	
• Instalar cámaras de vigilancia • Contratación de seguridad privada. • Restringir el acceso físico en horas no laborables.				• Dirección de Gestión Administrativa.	

INADECUADA GESTIÓN DE ACCESO LÓGICO DE LOS USUARIOS A LA RED					
Cod.	R.I.24	**Prioridad**	16	**Tipo de riesgo**	Alto alta probabilidad – alto impacto

Descripción

Se ha mencionado mediante entrevista que el DSI no ha realizado la asignación de privilegios, roles y permisos de red hacia los usuarios internos. Se considera un riesgo grave debido a la manipulación de documentos confidenciales que afecten la integridad de la información

Estrategias de mitigación	Responsables
• Implementar medidas de seguridad en la red. • Restringir el acceso de los usuarios en la red. • Elaborar un diagrama topológico, que registre todos usuarios internos y especifique sus roles, privilegios y restricciones de acuerdo a sus funciones. • Escaneo de vulnerabilidades. • Ethical Hacking.	• DSI

INADECUADO PROCESO DE SUPERVISIÓN HACIA EL DSI					
Cod.	R.I.25	**Prioridad**	12	**Tipo de riesgo**	Alto alta probabilidad – alto impacto

Descripción

La Dirección de Gestión Administrativa no ha establecido un proceso de supervisión hacia el DSI, se realiza control básico de cumplimiento de actividades mediante reporte.

Estrategias de mitigación	Responsables
• Generar un procedimiento de supervisión hacia el área. • Verificar el cumplimiento de los objetivos de TI. • Establecer criterios de evaluación de acuerdo a estándares y buenas prácticas. • Evaluaciones periódicas	• Dirección de Gestión Administrativa

INEXISTENCIA DE UNA UNIDAD DE CONTROL INTERNO INSTITUCIONAL					
Cod.	R.I.26	**Prioridad**	12	**Tipo de riesgo**	Alto alta probabilidad – alto impacto
Descripción					
La EPMAPA-T no registra en la estructura orgánica funcional, una unidad especializada en la supervisión institucional.					
Estrategias de mitigación				**Responsables**	
• Creación de la unidad de Control Interno Institucional.				• Directorio • Dirección de Gestión Administrativa	

4.2. DISCUSIÓN

El presente estudio tuvo como finalidad principal elaborar un plan de mitigación de riesgos tecnológicos basado en la aplicación de una auditoría informática a la EPMAPA-T tomando como base la metodología COBIT® 5 desarrollada por la Asociación de Auditoría y Control de Sistemas de Información – ISACA®, el proyecto de investigación se fundamentó en la indagación bibliográfica de la metodología.

El proceso de auditoría se llevó a cabo mediante la ejecución de cuatro etapas que fueron: estado inicial, planeación, ejecución y dictamen. La etapa de dictamen fue complementada con el análisis de riesgos, generando un documento de estrategias para cada riesgo identificado.

El presente proyecto es la primera evaluación basada en riesgos de tecnología que presenta la EPMAPA-T, generando un alto nivel de expectativa. La participación activa para colaborar con los procesos de mejora de los servicios prestados hacia el usuario externo, es una de las principales finalidades de quienes conforman la empresa.

Del total de 26 riesgos internos identificados, 13 que corresponde al 50% poseen un nivel alto de prioridad, es decir son riesgos que afectarían en gran impacto a la EPMAPA-T. A continuación, se listan los riesgos de carácter alto identificados.

Tabla 115. Riesgo con alto nivel de prioridad

Cod.	Situación de riesgo	Prioridad	Observación
R.I.12	Información, sin asegurar adecuadamente	16	La EPMAPA-T, no dispone de un sistema de seguridad de la información, que detalle los procesos y procedimientos, responsables y fases de aseguramiento.
R.I.24	Inadecuada gestión de acceso lógico de los usuarios a la red.	16	No se ha realizado una adecuada gestión de usuarios a la red, no se ha dispuesto niveles de acceso, roles o privilegios, que permitan restringir el acceso.
R.I.02	Riesgos de TI, sin gestionar	12	No se ha trabajado en gestión de riesgos de TI hasta el momento, este hecho va ligado al sistema de seguridad de la información, que en las organizaciones se considera el activo más importante.
R.I.05	Procesos de TI, sin documentar	12	El DSI, no dispone del manual de procesos y procedimientos del área.
R.I.08	Personal de TI insuficiente	12	El personal del DSI actualmente está incompleto, se considera un supervisor y dos técnicos analistas y por el momento un puesto de analista no ha sido cubierto.
R.I.09	Servicios de TI, sin identificar	12	No se ha establecido un catálogo de servicios de TI, tampoco se ha identificado como los procesos de tecnología apoyan al cumplimiento de servicios institucionales.
R.I.22	Inexistencia de plan de continuidad de TI frente a desastres.	12	No se ha desarrollado un plan de continuidad frente a desastres hasta el momento en la institución.
R.I.23	Acceso físico a la institución sin restricción.	12	La EPMAPA-T, no dispone de restricción de acceso controlada por seguridad privada.

R.I.25	Inadecuado proceso de supervisión hacia el DSI	12	No se ha establecido procesos de supervisión hacia el DSI, se reporta el cumplimiento de funciones y actividades de manera básica.
R.I.26	Inexistencia de una unidad de control interno institucional	12	La EPMAPA-T no dispone de una unidad de control interno, que se encargue de los procesos de supervisión hacia todas las direcciones.
R.I.18	Soporte técnico, sin regular bajo procedimiento	12	Este proceso de TI, se realiza con frecuencia diaria, por lo que es muy importante que sea normado de manera adecuada.
R.I..01	Incumplimiento de objetivos TI	9	Al no verificar la alineación de objetivos de TI, con objetivos institucionales se corre el riesgo de incumplir las metas trazadas.
R.I.11	Procesos sin métricas de calidad	9	En la EPMAPA-T no se trabaja con procesos estandarizados o con métricas de calidad.

Las situaciones de riesgo expuestas fueron valoradas en el plan de mitigación de riesgos tecnológicos para la EPMAPA-T. Se emitieron las estrategias y responsables de cumplimiento, para llevar a niveles de aceptación los riesgos identificados.

El producto de investigación fue revisado por el Supervisor Informático institucional, donde se ha manifestado la aceptación del documento. Tomando en cuenta que la empresa se proyecta a cambios para la nueva planificación 2020, debido a la nueva administración.

La entrega del Plan de mitigación de riesgos tecnológicos se llevó a cabo el día 10 enero del 2020, se dirigió al Gerente General de la EPMAPA-T, y en el consta la firma de responsabilidad del Supervisor Informático, debido a que el producto fue revisado previamente.

- Anexo 13: Documento entrega del Plan de mitigación de riesgos tecnológicos.
- Anexo 14: Certificación otorgada por el Gerente General EPMAPA-T

Análisis de la idea a defender

El documento sugiere en gran mayoría el desarrollo de documentación para el área de tecnología institucional. Se considera que la EPMAPA-T, obtendrá un menor impacto ante riesgos tecnológicos, al adoptar las estrategias expuestas en el documento de mitigación entregado. A continuación, se detalla los posibles beneficios al adoptar las recomendaciones sugeridas en el plan.

- Cumplimiento de objetivos institucionales y del área de TI.
- Área de TI como eje fundamental para el cumplimiento de objetivos institucionales.
- Desarrollo de procesos de TI documentados y controlados.
- Procesos institucionales y del área de TI con bajos niveles de riesgo.
- Apoyo en la toma de decisiones.
- Optimización de recursos tecnológicos.
- Mejora continua en los procesos institucionales más eficientes y optimizados.
- Iniciativa de creación de la unidad de Control Interno institucional.

Los niveles de capacidad de proceso que se estima alcanzar, al aplicar las estrategias expuestas en el plan de mitigación de riesgos tecnológicos, se describen a continuación:

Tabla 116. Niveles de capacidad de proceso a alcanzar.

Porcentaje de cumplimiento de estrategias presentadas.	Nivel	Valoración
81 - 100% de estrategias	4	Proceso predecible.
51 - 80% de estrategias	3	Proceso establecido.
21 - 50% de estrategias	2	Proceso gestionado.
1- 20% de estrategias	1	Proceso ejecutado.

De esta manera se justifica el cumplimiento de la idea a defender que fue propuesta en la presente investigación, donde se afirma que al aplicar el plan de mitigación de riesgos tecnológicos contribuye a a minimizar el impacto generado por los mismos en la EPMAPAT.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Se obtuvo cumplimiento del objetivo general referente a la elaboración un plan de mitigación de riesgos tecnológicos basado en auditoría informática aplicando la metodología COBIT® 5 a la EPMAPA-T, en cuanto a las situaciones de riesgo para procesos institucionales y de TI, se determinó los riesgos externos e internos basados en los hallazgos de auditoría, para la emitir las estrategias de mitigación correspondientes.

Se recopiló información mediante libros, revistas y medios virtuales incluido la metodología COBIT® 5 que permitió ajustar los requerimientos tecnológicos con los requerimientos de investigación y de esta manera establecer el proceso de auditoria informática que permitió evaluar la situación actual de los procesos que se llevan a cabo en la EPMAPA-T

Se realizó un estudio inicial de la empresa, mediante la aplicación de técnicas de verificación constituidas por entrevistas hacia el personal del DSI y Dirección de Gestión Administrativa. Adicional a ello, se evaluó la gestión informática del DSI en la EPMAPA-T, mediante una encuesta hacia los usuarios internos y lectores en un total de 46 informantes, tomando en cuenta que son ellos quienes hacen uso de un equipo informático institucional.

Se ejecutó el proceso auditoría informática en las siguientes fases:

- Fase de planeación de auditoría informática, mediante el diagnóstico de procesos institucionales y de TI, sumado a ello se determinó con base al estudio inicial que del total de 37 procesos COBIT® 5, 4 no era aplicables a la investigación, 9 procesos no obtuvieron cumplimiento y 24 cumplían parcialmente con los requerimientos, de esta manera se elaboró hojas de trabajo de auditoria tomando en cuenta a los procesos que cumplían parcialmente.
- Fase de ejecución de auditoría informática, mediante la aplicación de *check lis*t y la matriz de verificación basados en la metodología COBIT® 5. El método de verificación utilizado se fundamentó en cinco hojas de trabajo correspondientes a Director de Gestión Administrativa, Talento Humano, Control Interno, Supervisor Informático y Analista de sistemas.

- Fase de dictamen o informe de resultados con base a la evaluación de auditoría informática a 33 procesos COBIT® 5 aplicables, de los cuáles 2 resultaron efectivos y 31 no efectivos, el nivel general obtenido en cumplimiento de capacidad de proceso para la EPMAPA-T fue 1 de 5, indicando que los procesos actualmente se ejecutan y cumplen con los propósitos, pero no se encuentran en condiciones favorables o en el nivel 3 que es recomendable para la organización.

Finalmente, se determinaron 26 riesgos con base a los hallazgos de auditoría correspondiente a 31 procesos no efectivos, los mismos que fueron priorizados en la matriz de riesgos con base a impacto y probabilidad. Finalmente se emitieron estrategias de mitigación y fueron designados responsables de cumplimiento para cada uno de ellos, adicional a ello se establecieron riesgos externos que son inciertos o se encuentran asociados de forma permanente al desarrollo de funciones y actividades en la EPMAPA-T.

5.2. RECOMENDACIONES

Finalizado el proceso de investigación, y contando con un conocimiento sobre la estructura y procesos de la empresa, se pone en consideración lo siguiente:

Es importante tomar en cuenta que la presente investigación es un trabajo inicial, que pone de relevancia la vinculación de los activos de la empresa con los procesos tecnológicos de la misma, siendo una acción necesaria para una adecuada toma de decisiones de la EPMAPA-T, por lo que este estudio puede ser tomado como base para el desarrollo de una segunda parte.

Es pertinente realizar la actualización de los riesgos o amenazas para cada una de las planificaciones dispuestas en la EPMAPA-T debido a que pueden aumentar o disminuir con el tiempo, considerando que la empresa se enfrenta a cambios de fondo debido a la nueva administración.

Es recomendable que la EPMAPA-T aplique las estrategias emitidas en el plan de mitigación de riesgos tecnológicos, para llevar el cumplimiento de procesos tecnológicos hacia nivel 3 o superiores, de esta manera se consideran aceptables e indican que los procesos se han establecido, gestionado y son capaces de generar resultados con una adecuada optimización de recursos, tomando en cuenta que a mayor nivel de capacidad de proceso menor es el riesgo tal como lo menciona la metodología COBIT® 5.

Es importante tener claro la responsabilidad de registrar las estrategias de mitigación a las cuáles se ha dado cumplimiento, por lo que es recomendable que el DSI documente las estrategias cumplidas, responsables y evidencias de cumplimiento, con la finalidad de evaluar los resultados obtenidos en un futuro.

Para el desarrollo de documentación requerida, se considera de gran importancia la aplicación de metodologías especializadas en ciertas áreas tales como, Organización Internacional de Normalización (ISO), Information Technology Infrastructure Library (ITIL®), Norma de Control Interno del Ecuador, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), etc.

VI. REFERENCIAS BIBLIOGRÁFICAS

Arcentales, D., y Caycedo, X. (22 de agosto de 2017). Auditoría informática: un enfoque efectivo. *Revista Científica Dominio de las Ciencias.* 3, pp.157-173.

Asociación de Auditoría y Control de Sistemas de Información. (2012). *COBIT® 5 para la seguridad de la información.* Estados Unidos

Asociación de Auditoría y Control de Sistemas de Información. (2012). *COBIT® 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Estados Unidos.

Asociación de Auditoría y Control de Sistemas de Información. (2012). *COBIT® 5 Procesos Catalizadores.* Estados Unidos.

Asociación de Auditoría y Control de Sistemas de Información. (2013). *Guía de Auto-Evaluación: Usando COBIT® 5*. Estados Unidos.

Asociación de Auditoría y Control de Sistemas de Información. (2015). *ISACA® Glossary of Termss.* Estados Unidos.

Benavides, C. (2017). *Como crear un plan de mitigación o un plan de contingencia de riesgos.* Recuperado de https://calidadparapymes.com/plan-de-mitigacion-de-riesgos/

Calderón, J., y Ocaña, D. (2014). *Auditoria informática basada en el análisis de riesgos a la empresa Tecniseguros S.A* (Trabajo de postgrado). Universidad de las Fuerzas Armadas, Sangolquí, Ecuador.

Carcelén, Y. (2015). *Auditoria informática mediante la aplicación de la metodología COBIT (Control Objectives for Information and Related Technology) en la compañía I COACH SERVICIOS Consulting & Training Cia. Ltda* (Tesis de pregrado). Universidad Técnica de Ambato, Ambato, Ecuador.

Castillo, C. (2016). Factores clave de éxito en la implementación de un Plan de Continuidad de Negocio, como parte del Riesgo Operacional y Tecnológico. *VIII Congreso Regional de riesgos financieros.* Superintendencia de Bancos, Guatemala.

Centro de Ciberseguridad Industrial y Check Point. (2019). *Incidentes de ciberseguridad industrial en servicios esenciales en España*. (Edición 2019). Recuperado de

https://cybersecuritynews.es/wp-content/uploads/2019/10/Check-Point_Informe-incidentes-de-ciberseguridad-en-infraestructuras-cri%CC%81ticas-en-Espan%CC%83a.pdf

Chicano, E. (2014). *Auditoría de seguridad Informática. IFCT010*. Málaga, España: IC Editorial.

Contraloría General del Estado Ecuatoriano. (2014). *Normas de Control Interno de la Contraloría General del Estado Ecuatoriano*. Quito, Ecuador.

De Hoyos, S. (enero 2020). De Hoyos, S. (2020). El método científico y la filosofía como herramientas para generar conocimiento. *Revista Filosofía UIS.* 19(1), pp.230-245. doi: 10.18273/revfil.v19n1-2020010

Encalada, C., y Cordero, D. (diciembre de 2016). Guía de auditoría para la evaluación del control interno de seguridad de la información con enfoque COBIT 5: caso Universidad Católica de Cuenca (UCACUE). *Revista Científica y Tecnología UPSE*. 3(3), pp.113-121. doi: https://doi.org/10.26423/rctu.v3i3.204.

Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán. (2019). *Sitio web EPMAPA-T.* Recuperado de http://www.EPMAPA-Tulcan.gob.ec/

Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán. (2018). *Transparencia EPMAPA-T 2018.* Recuperado de http:// www.EPMAPA-Tulcan.gob.ec /ley-de-transparencia

Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán. (2019). *Plan Operativo Anual EPMAPA-T.* Tulcán, Ecuador.

Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán. (2010). *Reglamento Orgánico Funcional EPMAPA-T.* Tulcán, Ecuador.

Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán. (2010). *Ordenanza de constitución de la EPMAPA-T.* Tulcán, Ecuador.

Hernández, R., Fernández, C., y Baptista, P. (2014). *Metodología de la Investigación.* México D.F, México: Mc Graw Hill Education.

Ministerio de Finanzas Ecuador. (2017). *Metodología para la gestión integral de riesgos*. Recuperado de https://www.finanzas.gob.ec/wp-

content/uploads/downloads/2017/04/Metodolog%C3%ADa-para-la-Gesti%C3%B3n-de-Riesgos-30-03-17.pdf

Molina, M. (2015). *Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral* (Trabajo de postgrado). Universidad Politécnica de Madrid. Madrid, España.

Redacción Justicia. (16 de agosto de 2016). En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario. *Diario el Telégrafo*. Recuperado de https://www.eltelegrafo.com.ec/noticias/judicial/13/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

Samillan, G., y Castillo, E. (2017). *Auditoría informática usando las normas COBIT en el Centro de Sistemas de Información del Hospital Regional Docente las Mercedes de Chiclayo – 2016* (Tesis de pregrado). Universidad Nacional Pedro Ruiz Gallo. Lambayeque, Perú

Superintendencia de Bancos de Guatemala. (2017). Riesgo Tecnológico, *Programa de Capacitación sobre Gestión de Riesgos con enfoque en seguros*. Guatemala.

Ulloa, J. (2017). *Auditoría informática aplicando la metodología COBIT en el Gobierno Autónomo Descentralizado Municipal de San Cristóbal de Patate* (tesis de pregrado). Universidad Técnica de Ambato, Ecuador.

Universidad Autónoma del Estado de Hidalgo. (UAEH, 2011). *Auditoria Informática.* Escuela Superior de Tlahuelilpan. Recuperado de https://www.uaeh.edu.mx/docencia/P_Presentaciones/tlahuelilpan/sistemas/auditoria_informatica/auditoria_informatica.pdf

VII. ANEXOS

Anexo 1: Aprobación para realizar el proyecto de titulación en la EPMAPA-T

EPMAPA-T
Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán
Somos Vida

Si Podemos Tulcán Avancemos ..! Si Podemos Tulcán Avancemos ..! Si Podemos Tulcán Avancemos ..! Si Podemos Tulcán Avancemos ..! Si Podemos Tulcán Avancemos ..!

A petición verbal de la parte interesada y en mi calidad de Director de Gestión Administrativa de la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán me permito:

CERTIFICAR:

Que la Srta. Pantoja Miño Yuly Estefanía con cédula de ciudadanía No. 0401916713, realizará el Tema de Investigación: Plan de Mitigación de Riesgos Tecnológicos en la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán.

Es todo cuanto puedo certificar en honor a la verdad por lo cual se faculta a la interesada hacer uso del presente documento como estime conveniente, a excepción de trámites judiciales.

Dado en la ciudad de Tulcán a los once días del mes de junio del dos mil dieciocho.

Atentamente.

Ing. Andrés Velasco.
DIRECTOR DE GESTIÓN ADMINISTRATIVA DE LA EPMAPA-T

EPMAPA-T
DIRECTOR DE GESTIÓN
ADMINISTRATIVA

andresvelasco@epmapatulcan.ec
CELULAR: 0984654522

Dirección: Juan Ramón Arellano y Bolívar, sector Terminal Terrestre
E-mail: epmapatulcan@hotmail.com TULCÁN - ECUADOR
Dirección Web: www.epmapatulcan.ec
Telefono: (06)2-960-077

Anexo 2: Estado inicial - Entrevista al Supervisor Informático

Entrevista correspondiente al área de Gestión de TI					
Entrevistado	MSc. Jackson Obando				
Cargo	Supervisor Informático EPMAPA-T				
N	**Preguntas**	**Si**	**No**	**N/A**	**Observaciones**
1	¿Existen objetivos de TI implementados en el Departamento de Supervisión Informática?	x			Reglamento Orgánico Funcional
2	¿Los objetivos de TI se alinean a los objetivos corporativos?	X			
3	¿Se han establecido estrategias para el cumplimiento de los Objetivos de TI?	x			Plan Estratégico de Tecnologías
4	¿Existe planes de Continuidad de Negocio en el marco de TI?		x		
5	¿Existe planes de Disponibilidad de Negocio en el marco de TI?		x		
6	¿Se ha trabajo en aspectos relacionados a la Seguridad de Información?	x			No existe documentación
7	¿Se ha trabajado en Gestión de los Riesgos de negocio de acuerdo con las TI?		x		
8	¿Existe conexión del Departamento de Supervisión Informática con las direcciones de gestión?	x			Todas las direcciones necesitan de TI
9	¿Existe una política de planificación de las actividades a desarrollar en el Departamento de Supervisión Informática?	x			POA (Dir. de Gestión Administrativa)
10	¿Se ha evaluado la gestión de TI en la empresa?	x			No existe documentación
11	¿Se incluye planes de mejora TI en el Departamento de Supervisión Informática?		x		
12	¿Se incluye planes de aseguramiento de TI en el Departamento de Supervisión Informática?		x		
13	¿La Empresa se rige a un Marco Referencia que regule los procesos y recursos de TI?		x		Auditoría General por Cambio de Autoridades, NCI-Empresa Pública
14	¿Se ha evaluado el uso de los recursos de TI de la manera más efectiva y eficiente?	x			No existe documentación

15	¿Existe evaluación de capacidad del servicio de acuerdo a los recursos de TI?			X	
16	¿La capacidad de servicio a la comunidad está acorde al procesamiento de información?	x			
17	¿El personal de TI es capacitado para la realización de tareas?	x			Personal con títulos de tercer y cuarto nivel-Capacitaciones no muy frecuentes.
18	¿Se realiza estudios de vialidad para la ejecución de proyectos de TI?	x			No existe documentación
19	¿Se ha realizado un estudio de posibles riesgos vinculados a TI?		x		
20	¿Existe mecanismos que contribuyan a la solución de problemas de TI generados en la Empresa?	x			Red telefónica
21	¿El Departamento de Supervisión Informática cuenta con un presupuesto fijo?	x			Realiza la EPMAPA-T, mediante la presentación de plan o documentación debida.
22	¿Existe un manual de procesos internos y externos en el Departamento de Supervisión Informática?		x		En proceso / Consultora Externa
23	¿Se han establecido objetivos para alcanzar la mejora de los procesos de TI?		x		Inexistencia del manual
24	¿Se han establecido políticas de seguimiento al cumplimiento de los procesos de TI?		x		Inexistencia del manual
25	¿Se identificado las deficiencias en el cumplimiento de los procesos de TI?		x		Inexistencia del manual
26	¿Se considera que el personal que labora en el Departamento de Supervisión Informática es suficiente para el cumplimiento de los procesos realizados?	x			Por el momento sí, debido al tamaño de la Empresa. EPMAPA-T se rige al Plan Anual de Contratación (PAC)
27	¿Se han establecido políticas de servicio al usuario internamente en la Empresa de acuerdo con las Ti?		x		
28	¿Se han establecido políticas de control interno informático?		x		
29	¿Existe catálogo de servicios internos y externos de TI?		x		

Anexo 3: Estado inicial - Entrevista al Director de Gestión Administrativa

Entrevista correspondiente al área de Gobierno de TI

Entrevistado	Ing. Andrés Velasco
Cargo	Director de Gestión Administrativa EPMAPA-T

N	Preguntas	Si	No	N/A	Observaciones
1	¿La Empresa cuenta con metas corporativas?	x			Ordenanza EPMAPA-T
2	¿La Empresa cuenta con objetivos corporativos?	x			Plan Operativo Anual (POA)
3	¿La Empresa cuenta con estrategias para el cumplimiento de objetivos y metas?	x			Plan Operativo Anual (POA)
4	¿Existe una estructura organizativa en la Empresa?	x			Reglamento Orgánico Funcional
5	¿Existe planes de Continuidad de Negocio?	x			
6	¿Existe planes de Disponibilidad de Negocio?	x			
7	¿Existe un manual de procesos internos y externos de negocio?		x		En proceso /Consultora Externa
8	¿Existe catálogo de servicios internos y externos Institucionales?	x			Reglamento de Servicios
9	¿Se han establecido principios y políticas dentro del negocio?	x			Reglamento Interno
10	¿Existe políticas de ética y comportamiento en la Empresa?	x			Reglamento Interno
11	¿Existe una correcta definición de funciones en la Dirección de Gestión Administrativa?	x			Documento de Valoración puestos- Reglamento orgánico
12	¿Existe política de planificación en la Dirección de Gestión Administrativa?	x			Plan Operativo Anual (POA)
13	¿Se ha trabajado en procesos de respaldo de información producida por la Empresa?	x			Sistemas
14	¿La Empresa se rige a un Marco Referencia que regule los procesos y recursos de TI?			X	Sistemas
15	¿Se ha trabajo en aspectos relacionados a la Seguridad de Información?			X	Sistemas
16	¿Se realiza gestión de Planes, Proyectos y Programas relacionados con TI?	x			Capacitaciones
17	¿Existe evaluación de capacidad del servicio a la comunidad de acuerdo a los recursos de TI?			X	
18	¿Se ha trabajo en Gestión de Riesgos de negocio?	x			No existe documentación
19	¿Se ha evaluado la gestión de TI en la Empresa?		x		Sistemas

Anexo 4: Estado inicial - Entrevista al Analista de Sistemas

Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán

Entrevista al Analista de Sistemas de la EPMAPA-T

Objetivo. Determinar el nivel de aplicación de los dominios de COBIT® 5 en la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán, por parte del Departamento de Supervisión Informática.

Siglas

EPMAPA-T	Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán
DSI	Departamento de Supervisión Informática
TI	Tecnologías de Información

EVALUAR, ORIENTAR Y SUPERVISAR - EDM

1. ¿El asistente de talento humano ha cumplido, con la difusión de políticas y normas de ética – comportamiento hacia el DSI?

SI [ ] NO [X]

2. ¿Se ha realizado la inducción al integrarse a la EPMAPA-T?

SI [X] NO [ ]

2.1 ¿Se realizó la entrega de Funciones y Responsabilidades al cargo al integrarse a la EPMAPA-T?

SI [X] NO [ ]

2.2 ¿Quién o Quienes le dieron a conocer sus funciones?

Talento Humano

2.3 ¿Cuáles son sus funciones?

- ***Diseño y mantenimiento del sitio web.***
- ***Mantenimiento de equipos informáticos***
- ***Brindar soporte técnico.***
- ***Mantener seguridades LAN y WAN.***
- ***Administración de servidores.***

2.4 En caso de inasistencia a la Empresa. ¿Quién asume sus funciones?

Supervisor Informático

3. ¿Conoce si la Dirección de Gestión Administrativa ha definido los procesos exclusivos para el área de TI?

SI [ ] NO [X]

4. ¿Conoce si la Dirección de Gestión Administrativa ha trabajado en procedimientos, vinculados a la Gestión de riesgos de TI?

SI [ ] NO [X]

ALINEAR, PLANIFICAR Y ORGANIZAR – APO

5. ¿Considera usted que el personal dedicado al DSI es suficiente, para el cumplimiento de funciones?

SI [X] NO [ ]

6. ¿Conoce usted si existe asignación presupuestaria para el DSI?

SI [X] NO [ ]

En caso de ser afirmativa

6.1 La asignación presupuestaria, cada qué periodo de tiempo se actualiza.

Trimestral [ ] Semestral [X] Anual [ ] Nunca [ ]

6.2 ¿Considera que la asignación presupuestaria para el DSI es suficiente?

SI [X] NO [ ]

6.3 ¿Cuáles son las áreas que se deben fortalecer con la asignación presupuestaria para el DSI?

Seguridad Informática

7. ¿Existe control sobre los recursos materiales y económicos que se usan en el DSI?

SI [X] NO [ ]

En caso de ser afirmativa

7.1 ¿Quién o Quienes realizan el control?

Bodeguero

7.2 ¿Como se realiza el control?

Mediante actas

8. ¿Existe presupuesto asignado para el proceso de adquisición de hardware, software y otros tecnológicos necesarios?

SI [X] NO [ ]

En caso de ser afirmativa

8.1 ¿El presupuesto cumple con los requerimientos para la adquisición de hardware, software y otros tecnológicos?

SI [X] NO [ ]

CONSTRUIR, ADQUIRIR E IMPLEMENTAR – BAI

9. ¿Usted ha participado en proyectos de mejora vinculado a soluciones tecnológicas en la EPMAPA-T?

SI [ ] NO [X]

En caso de ser afirmativa.

9.1 ¿Cuáles son los proyectos de mejora que contaron con su participación?

…….

9.2 La participación fue como:

Líder [ ] Colaborador [ ]

9.3 ¿Durante que tiempo se llevó a cabo el Proyecto de mejora más reciente?

……

9.4 ¿A qué área se desarrolló el proyecto de mejora?

Totalidad de la EPMAPA-T [ ]
Área de TI [ ]
Otra Dirección o Área [ ] ¿Cuál?.....

10. ¿Conoce usted sobre la clasificación general de los activos de TI en la EPMAPA-T?

SI [X] NO [ ]

En caso de ser afirmativa

10.1 ¿Cuál es la clasificación de activos de TI, en la EPMAPA-T?

Equipos de cómputo, servidores, routers, switches, cableado estructurado
Teléfonos celulares.

11. ¿Se ha desarrollado la inducción al usuario sobre los cuidados a los activos de TI de la EPMAPA-T, con fines de evitar su daño, deterioro o mal uso por parte del usuario?

SI [X] NO [ ]

12. ¿Se desarrolla una planificación para al mantenimiento preventivo y /o correctivo de los equipos de cómputo de la EPMAPA-T?

SI [X] NO [ ]

12.1 ¿Cuál es el período de tiempo en que se realiza el mantenimiento preventivo de equipos en la EPMAPA-T?

Semanal [ ] Trimestral [X] Semestral [ ] Anual [ ] Nunca [ ]

12.2 ¿Cuál es el período de tiempo en que se realiza el mantenimiento correctivo de equipos en la EPMAPA-T?

Semanal [ ] Trimestral [X] Semestral [ ] Anual [ ] Nunca [ ]

12.3 ¿Se ha informado con anterioridad al usuario interno acerca de los mantenimientos preventivo y/o correctivo en el equipo que ocupa?

SI [X] NO [ ]

12.4 ¿Se lleva una bitácora de acciones sobre los equipos informáticos, después del mantenimiento de los mismos?

SI [X] NO [ ]

ENTREGAR, DAR SERVICIO Y SOPORTE – DSS

13. ¿Cuál es el canal de comunicación entre los usuarios internos y el DSI?
Vía telefónica
14. ¿Se dispone de un procedimiento para la atención al usuario interno?

SI [ ] NO [X]

15. ¿Se dispone de un procedimiento definido para detectar problemas, causas y soluciones asociadas con TI, en él DSI?

SI [X] NO [ ]

16. ¿Se dispone de un Plan de Contingencia, en caso de interrupción o falla de algún servicio de TI, sistema o equipo informático?

SI [X] NO [ ]

17. ¿Existe un procedimiento para respaldar la información digital generada en la EPMAPA-T?

SI [X] NO [ ]

En caso de ser afirmativa

17.1 ¿Cuál es el periodo de tiempo, en que se realiza el procedimiento de obtención de respaldos?

El servidor respalda mediante un software instalado con una frecuencia diaria.

SUPERVISAR, EVALUAR Y VALORAR – MEA

18. ¿Se evalúa y monitorea la Gestión del DSI, en la EPMAPA-T?

SI [X] NO [ ]

19. ¿Se ha controlado que los Sistemas Informáticos cumplan con leyes y normas vigentes (*tomando en cuenta que es una Empresa Pública*)

SI [X] NO [ ]

20. ¿Se ha realizado control interno en el DSI?

SI [ ] NO [X]

En caso de ser afirmativa.

20.1 ¿Quién o Quienes han realizado el control interno?

……

20.2 ¿Cuándo fue la última vez que se realizó el control interno?

……

21. ¿Conoce usted si se ha llevado un proceso de auditoría informática a su área en ocasiones anteriores?

SI [X] NO [ ]

Si la respuesta es afirmativa

21.1 ¿Hace que tiempo fue realizada la última auditoría informática?

No se recuerda

21.2 ¿Cuáles fueron los principales hallazgos o no conformidades?

No se cuenta con ese tipo de información

21.3 ¿Cuáles fueron las principales recomendaciones?

No se cuenta con ese tipo de información

21.4 ¿Cuáles fueron las principales acciones correctivas, en consideración a las recomendaciones?

No se cuenta con ese tipo de información

21.5 ¿Cuáles fueron las principales acciones preventivas, en consideración a las recomendaciones?

No se cuenta con ese tipo de información

21.6 ¿Cuáles fueron las principales acciones de mejora, en consideración a las recomendaciones?

No se cuenta con ese tipo de información

Anexo 5: Aprobación para realizar la encuesta a los usuarios internos.

Tulcán, 05 de junio de 2019

Ing.

Mauricio Larrea

GERENTE (E) EPMAPA-T

Presente. –

EPMAPA-T
INGRESO DE DOCUMENTOS
SECRETARÍA GENERAL
Fecha: 05-06-2019
Hora: 9:26
Procedencia: CST
Recibido por: N.D.

De mi consideración:

Reciba un atento y cordial saludo, a la vez desearle toda clase de éxitos en las funciones que acertadamente desempeña.

El presente tiene como finalidad solicitar respetuosamente su autorización para realizar el levantamiento de información, aplicando la técnica de encuesta a la totalidad de servidores públicos de la EPMAPA-T, como parte del desarrollo del Proyecto de Titulación denominado "Plan de mitigación de riesgos tecnológicos basado en Auditoría Informática a la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán", el contenido de la encuesta busca evaluar principalmente la Gestión del Departamento de Supervisión Informática en las diferentes Direcciones.

Adjunto una copia de la certificación otorgada por la Dirección de Gestión Administrativa, en la cual consta la aprobación del Proyecto de Investigación en la EPMAPA-T.

Esperando una favorable acogida al presente, anticipo mis agradecimientos.

Atentamente

Yuly Estefanía Pantoja Miño

CI. 0401916713

Estudiante de la Carrera de Ingeniería en Informática

Universidad Politécnica Estatal del Carchi

DIRECTOR ADMINISTRATIVO
AUTORIZADO
FECHA: 11-09-2019

Anexo 6: Estado inicial – Modelo de encuesta a usuarios internos

Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán

Encuesta de servicios prestados por el Departamento de Supervisión Informática hacia Usuarios Internos.

Objetivo. Evaluar el nivel de satisfacción de los servidores públicos de la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán, con respecto a los servicios prestados por el Departamento de Supervisión Informática Institucional.

Siglas

EPMAPA-T	Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán
DSI	Departamento de Supervisión Informática

EQUIPO INFORMÁTICO

1. ¿Para desarrollar las funciones y actividades dentro de la EPMAPA-T, utiliza un equipo informático? Si su respuesta es SI continúe con la encuesta, de lo contrario, la misma finaliza.

   SI ☐ NO ☐

2. ¿El equipo Informático que se encuentra a su disposición es?

   Personal ☐ Institucional ☐ Desconoce ☐

3. ¿Conoce usted si al equipo que ocupa se le ha realizado mantenimiento preventivo y/o correctivo por el DSI.?

   SI ☐ NO ☐

   3.1. ¿Con que frecuencia se le ha realizado mantenimiento preventivo y/o correctivo al equipo que se encuentra a su disposición?

   Bimestral ☐ Trimestral ☐ Semestral ☐ Anual ☐ Nunca ☐

4. ¿Ha sido informado con anterioridad acerca de los mantenimientos preventivo y/o correctivo en el equipo que ocupa?

   SI ☐ NO ☐

   4.1 ¿Conoce usted si se lleva un registro de las acciones realizadas en el mantenimiento sobre el equipo informático que utiliza?

   SI ☐ NO ☐

SERVICIO DE INTERNET

5. ¿Para el cumplimiento de sus funciones, necesita de servicio de Internet?

SI ☐ NO ☐

En caso de ser afirmativa.

5.1 ¿Cómo califica usted el servicio de internet?

Excelente ☐ Muy bueno ☐ Bueno ☐ Regular ☐ Malo ☐

6. ¿Conoce usted si el servicio de internet tiene políticas de restricción institucionales?

SI ☐ NO ☐

En caso de ser afirmativa.

6.1 Marque las restricciones que usted ha identificado

Restricciones de acceso a red social Facebook	☐
Restricciones de acceso a red social Twiter	☐
Restricciones de acceso a plataforma Youtube	☐
Restricciones de internet en horas definidas	☐
Otras ……	☐

SISTEMA INFORMÁTICO

7 Para el desarrollo de sus funciones y actividades. ¿Usted hace uso de un sistema informático?

SI ☐ NO ☐

En caso de ser afirmativa

7.1 ¿Cuál o cuáles sistemas y/o aplicativos utiliza?

SISTEMAS		APLICATIVOS	
SIIM	☐	Microsoft Office	☐
MEGAN	☐	AutoCAD	☐
Aplicativo móvil de lectura	☐	Proexcel	☐
Otro ……	☐	QGIS	☐
		Otro……	☐

7.2 ¿Dentro del proceso de inducción, ha recibido capacitación para el uso de los sistemas informáticos que utiliza?

SI ☐ NO ☐

7.3 ¿Cuáles sistemas y/o aplicativos ha recibido inducción?

SISTEMAS		APLICATIVOS	
SIIM	☐	Microsoft Office	☐
MEGAN	☐	AutoCAD	☐
Aplicativo móvil de lectura	☐	Proexcel	☐
Otro	☐	QGIS	☐
……			
		Otro……	☐

7.4 ¿El o los sistemas han presentado fallas?

SI ☐ NO ☐

En caso de ser afirmativa.

7.4.1 ¿Qué tipo de fallas?

……
……
……
……

7.4.2 ¿Con que frecuencia se presentan las fallas?

Diario ☐ Semanal ☐ Mensual ☐ Anual ☐ Nunca ☐

SEGURIDAD Y CONTRASEÑAS

8 ¿Usted utiliza contraseñas para el acceso a los sistemas y/o servicios informáticos de la EPMAPA-T?

SI ☐ NO ☐

En caso de ser afirmativa.

8.1 ¿Para cuáles sistemas y /o servicios informáticos usa contraseñas?

……
……
……
……

8.2 ¿Con que frecuencia se realiza el cambio de contraseñas, en los sistemas y /o servicios informáticos?

Trimestral	☐
Semestral	☐
Anual	☐
Nunca	☐

8.3 El cambio de contraseña se realiza por:

Decisión personal	
Por solicitud del sistema o servicio	
Por políticas de seguridad	

9 ¿Usted utiliza contraseñas para el acceso al equipo informático qué usa?

SI ☐ NO ☐

En caso de ser afirmativa.

9.1 ¿Con que frecuencia se realiza el cambio de contraseñas, para acceso al equipo informático?

Trimestral	
Semestral	
Anual	
Nunca	

9.2 El cambio de contraseña se realiza por:

Decisión personal	
Por solicitud del equipo informático	
Por políticas de seguridad	

10 ¿Cuál es la manera en la usted protege las contraseñas, para los equipos o Sistemas que dispone la EPMAPA-T?

Memoriza		
Notas personales		
Otro		Cuál……

11 De las siguientes opciones, cuál o cuáles cumplen con la política de contraseñas establecida por la institución: (*varias opciones en caso que aplique*)

Mayúsculas	
Minúsculas	
Números	
Caracteres especiales	
Mínimo ocho caracteres	

CALIFICACIÓN DEL SERVICIO

12 ¿Con qué frecuencia solicita soporte al DSI de la EPMAPA-T?

1 a 5 días ☐ 6 a 15 días ☐ 16 a 30 días ☐ Mayor a un mes ☐ Nunca ☐

13 ¿El DSI, le ha informado a usted acerca de los tiempos de respuesta a una solución en caso de los siguientes problemas?

	SI	NO
Problemas críticos		
Problemas altos		
Problemas carácter medio		
Problemas carácter bajo		

En caso de que una de las opciones haya sido afirmativa.

13.1 ¿El DSI ha cumplido con los tiempos de solución estipulados?

SI ☐ NO ☐

13.2 En caso de que se supere los tiempos de solución. ¿Cuáles son las acciones que toma el DSI?

……
……
……
……

13.3 ¿Cuál ha sido el tiempo máximo de respuesta del DSI a la solicitud de atención técnica, en relación a la criticidad del problema?

Criticidad / Tiempo	Problemas críticos	Problemas altos	Problemas carácter medio	Problemas de carácter bajo
1 a 15 min				
16 a 30 min				
31 a 45 min				
46 a 60 min				
Mas de 60 min				

14 ¿Existe un método para medir la calidad del servicio prestado por el DSI?

SI ☐ NO ☐

15 ¿Cómo califica el servicio brindado por el DSI de la EPMAPA-T?

Excelente ☐ Muy bueno ☐ Bueno ☐ Regular ☐ Malo ☐

Anexo 7: Planificación de auditoria

Tulcán, 11 de diciembre de 2019

Ing.

Galo Tipaz

GERENTE GENERAL EPMAPA-T

Presente. –

De mi consideración:

Reciba un atento y cordial saludo, a la vez desearle toda clase de éxitos en las funciones que acertadamente desempeña.

El presente tiene como finalidad solicitar respetuosamente su autorización para aplicar las entrevistas finales, como parte del Proyecto de Titulación denominado "Plan de mitigación de riesgos tecnológicos basado en Auditoría Informática a la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán", el contenido de las entrevistas busca evaluar el estado de los procesos tecnológicos que se desarrollan en la Empresa y con ello determinar el Plan de mitigación de riesgos tecnológicos.

Adjunto la planificación y las hojas de trabajo a evaluar.

Esperando una favorable acogida al presente, anticipo mis agradecimientos.

Atentamente

Yuly Estefanía Pantoja Miño

CI. 0401916713

Estudiante de la Carrera de Ingeniería en Informática

Universidad Politécnica Estatal del Carchi

EPMAPA-T
INGRESO DE DOCUMENTOS
SECRETARÍA GENERAL
Fecha: 11-12-19
Hora: 10:53
Procedencia: -P106-
Recibido por TATY2

Planificación de Auditoría

Tema

Plan de mitigación de riesgos tecnológicos basado en Auditoría Informática a la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán.

Empresa a auditar

Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán.

Objetivo de auditoría

Desarrollar una evaluación informática a los procesos internos de la EPMAPAT, con la finalidad de identificar riesgos de TI que afecten el cumplimiento de los objetivos institucionales y/o del área de TI.

Equipo auditor

Auditor	Yuly Pantoja Estudiante de la Carrera de Ingeniería en Informática
Asesor	Ing. Carlitos Guano, MSc. Docente de la Carrera de Ingeniería en Informática

Áreas a auditar

Gobierno de TI	Dirección de Gestión Administrativa Departamento de Supervisión Informática
Control Interno	Dirección de Gestión Administrativa
Talento Humano	Talento Humano
Gestión de TI	Supervisor Informático
	Analistas de sistemas

Cronograma de auditoría (aplicación de hojas de trabajo)

Área	Procesos	Responsable	Fecha	Hora Inicio - Hora Fin
Gobierno de TI	• Auditoría Interna. • Evaluación de desempeño. • Cartera de servicios de TI. • Planificación POA.	Director de Gestión Administrativa	16-12-2019	10:30 - 12:30
Control Interno	• Inversión presupuestaria de TI. • Transparencia Institucional. • Verificación de cumplimiento.	Director de Gestión Administrativa	16-12-2019	14:30 - 16:00
Talento Humano	• Comunicación con el DSI. • Contratación de personal de TI. • Capacitación de personal de TI.	Asistente de Talento Humano.	17-12-2019	14:30 – 16:00
Dirección de TI	• Gestión Tecnológica. • Implementación de soluciones informáticas. • Gestión de incidentes de TI. • Administración de redes	Supervisor Informático	18-12-2019	10:30 – 12:30
Operativo de TI	• Ejecución de planes, proyectos y/o programas de TI. • Implementación de soluciones informáticas. • Soporte Técnico • Administración de redes.	Analista de Sistemas	18-12-2019	14:30 – 16:30

Anexo 8: Resultado hoja de trabajo - Dirección Administrativa

Hoja de Trabajo- Dirección de Gestión Administrativa

Objetivo de auditoría

Desarrollar una evaluación informática a los procesos internos de la EPMAPA-T, con la finalidad de identificar riesgos de TI que afecten el cumplimiento de los objetivos institucionales y/o del área de TI.

Procesos a evaluar.

- Auditoría Interna.
- Evaluación de desempeño.
- Catálogo de servicios de TI.
- Planificación POA.

Dominio	Cod. Objetivo	N°	Preguntas	Si	No	N/A	Observaciones
EDM	EDM01.01	1	¿Se ha evaluado la situación actual de las TI, en la EPMAPA-T?	X			I estado de equipos
	EDM01.01	2	¿Se han realizado procesos de auditoría interna empresarial?		X		
	EDM01.02	3	¿Existe un procedimiento que permita evaluar el desempeño del DSI?		X		
	EDM02.02	4	¿Se ha establecido un catálogo de servicios de TI?		X		
APO	APO01.01	5	¿Se ha incluido al personal de TI, en la conformación de comités institucionales?	X			C. participación ciudadana.
	APO01.05	6	¿Se han posicionado las funciones de TI, dentro de la estructura organizativa institucional?	X			
	APO06.02	7	¿Se ha realizado un diagnóstico de las necesidades, previa una asignación de presupuesto en el POA?	X			I previo asignación
	APO06.02	8	¿Se ha realizado una asignación presupuestaria adicional al POA, debido a solicitud del DSI?	X			Adquisición software
BAI	BAI05.01	9	¿Se ha considerado iniciativas de mejora para el DSI?	X			

Anexo 9: Resultado hoja de trabajo – Control Interno

Hoja de Trabajo- Control Interno

Objetivo de auditoría

Desarrollar una evaluación informática a los procesos internos de la EPMAPA-T, con la finalidad de identificar riesgos de TI que afecten el cumplimiento de los objetivos institucionales y/o del área de TI

Procesos a evaluar.

- Inversión presupuestaria de TI.
- Transparencia Institucional.
- Verificación de cumplimiento.

Dominio	Cod. Objetivo	N°	Preguntas	Si	No	N/A	Observaciones
EDM	EDM02.01	1	¿Se ha evaluado la inversión en TI, enfocada al cumplimiento de objetivos institucionales?		X		
	EDM04.01	2	¿Se ha hecho seguimiento de los recursos asignados al DSI?		X		
	EDM05.01	3	¿La sección de transparencia institucional incluye ítems, relacionados al cumplimiento de funciones del DSI?		X		
	EDM05.01	4	¿Se recepta informes de cumplimiento de funciones por el DSI?	X			Reportes mensuales
	EDM05.02	5	¿Se han definido formatos para los informes de cumplimiento de funciones y actividades para el DSI?	X			Formato general
APO	APO01.03	6	¿Se han verificado que los objetivos de TI, estén alineados a los objetivos institucionales?		X		
MEA	MEA01.01	7	¿Se ha definido procesos de supervisión hacia el servicio brindado por el DSI?		X		
	MEA01.04	8	¿El sistema de control interno considera los riesgos de TI, que pueden aparecer?		X		
	MEA03.01	9	¿En el proceso de supervisión, se incluyen ítems de normas gubernamentales?	X			Para la Dirección Administrativa
	MEA03.01	10	¿Se incluye la gestión TI, dentro de los informes generales?		X		
	MEA03.04	11	¿Existe acciones correctivas, después la evaluación realizada hacia él DSI?		X		

Anexo 10: Resultado hoja de trabajo – Talento Humano

Hoja de Trabajo- Talento Humano

Objetivo de auditoría

Desarrollar una evaluación informática a los procesos internos de la EPMAPA-T, con la finalidad de identificar riesgos de TI que afecten el cumplimiento de los objetivos institucionales y/o del área de TI.

Procesos a evaluar.

- Comunicación con el DSI.
- Contratación de personal de TI.
- Capacitación de personal de TI.

Dominio	Cod. Objetivo	N°	Preguntas	Si	No	N/A	Observaciones
APO	APO01.02	1	¿Se han comunicado las funciones y responsabilidades al personal de TI?	X			Contrato / M. funciones
	APO03.01	2	¿Se dispone una documentación legal, en la cual se fundamenta la distribución de la estructura orgánica funcional?	X			R. Orgánico Funcional
	APO03.02	3	¿Existe documentación interna que indique las funciones del personal del DSI?	X			M. funciones
	APO07.01	4	¿Se dispone de lineamientos para la contratación del personal de DSI?	X			M. funciones
	APO07.01	5	¿Se ha comunicado el proceso de contratación institucional?	X			PAC
	APO07.01	6	¿Se ha cumplido con el proceso legal, para la contratación del personal del DSI?	X			PAC
	APO07.01	7	¿Se han evaluado las necesidades del personal del DSI?		X		
	APO07.01	8	¿El personal del DSI, ha participado en jornadas de capacitación institucional?	X			Atención al cliente
	APO07.03	9	¿Se dispone de un proceso, que permita identificar las habilidades del personal contratado en el DSI?		X		
	APO07.03	10	¿Se ha realizado una evaluación periódica de la evolución de las habilidades y destrezas del personal disponible en el DSI?		X		
	APO07.03	11	¿Se realiza un control de las normas de ética y comportamiento en el DSI?	X			Reglamento interno

Anexo 11: Resultado hoja de trabajo – Supervisor Informático

Hoja de Trabajo- Supervisor Informático

Objetivo de auditoría

Desarrollar una evaluación informática a los procesos internos de la EPMAPA-T, con la finalidad de identificar riesgos de TI que afecten el cumplimiento de los objetivos institucionales y/o del área de TI.

Procesos a evaluar.

- Gestión Tecnológica.
- Implementación de soluciones informáticas.
- Gestión de incidentes de TI.
- Administración de redes

Dominio	Cod. Objetivo	N°	Preguntas	Si	No	N/A	Observaciones
EDM	EDM02.02	1	¿Se ha establecido un catálogo de servicios de TI?		X		
APO	APO01.02	2	¿Los miembros del DSI, cumplen con las funciones asignadas?	X			Manual de funciones
	APO01.02	3	¿Se realizan reportes de cumplimiento de funciones?		X		
	APO01.03	4	¿Se han establecido objetivos del área de TI?	X			
	APO02.01	5	¿Se ha establecido un Plan Estratégico de TI?		X		
	APO06.02	6	¿Se han documentado las necesidades a cubrir previa la asignación de recursos en el POA?	X			Informe previo
	APO06.03	7	¿Se ha elaborado un Plan Presupuestario en el DSI?	X			Adquisición h/s
	APO07.01	8	¿El personal del DSI, ha participado en planes de capacitación institucional?	X			Atención al cliente
	APO07.01	9	¿El personal del DSI, es suficiente para el cumplimiento de funciones y actividades?	X			
	APO07.02	10	¿Se designa funciones, de acuerdo de las habilidades y destrezas del personal?	X			
	APO08.01	11	¿Se ha identificado los incidentes de TI, que alteran el cumplimiento de objetivos institucionales?		X		
	APO08.02	12	¿Se ha establecido un proceso de gestión de incidentes?		X		
	APO08.02	13	¿Se han focalizado las situaciones emergentes de TI?		X		
	APO09.01	14	¿Se han establecido niveles de servicio de TI?		X		

	APO09.01	15	¿Se han implementado procesos de mejora enfocado al catálogo de servicios de TI?		X		Iniciativas de cambio
BAI	BAI01.01	16	¿Se ha establecido un procedimiento para la administración de planes, proyectos y/o programas referentes a las TI?		X		
	BAI01.02	17	¿Actualmente se lleva a cabo un plan, proyecto y/o programa referente a las TI?	X			Adquisición h/s
	BAI01.03	18	¿Se han designado tareas específicas al personal del DSI, en la ejecución de un plan, proyecto y/o programa?	X			
	BAI01.03	19	¿Se ha incluido a los usuarios internos que formaran parte de planes, proyectos y/o programas vinculados a TI?	X			
	BAI01.04	20	¿Se han evaluado las tareas encomendadas, durante la ejecución del plan, proyecto y/o programa de TI?	X			
	BAI03.01	21	¿Se han identificado soluciones informáticas, para problemas en el desarrollo de actividades de la EPMAPA-T?	X			
	BAI03.02	22	¿Se ha construido una solución informática en el DSI?	X			Sitio web ERP
	BAI03.03	23	¿Se ha determinado un presupuesto adicional al asignado por el POA, para la adquisición de soluciones informáticas?	X			
	BAI03.10	24	¿Se ha evaluado el rendimiento de las soluciones informáticas implementadas?		X		
	BAI04.01	25	¿Se han documentado los recursos invertidos para brindar un servicio de TI?	X			Partida presupuestaria
	BAI05.01	26	¿El DSI, se proyecta a iniciativas de mejora del servicio para la siguiente planificación?	X			
	BAI09.01	27	¿Se ha realizado inventario de activos de TI institucional?	X			Inventario
	BAI09.02	28	¿Se ha priorizado los activos, con mayor importancia?		X		
	BAI09.03	29	¿Se ha establecido el tiempo de vida útil de los activos?	X			
	BAI09.05	30	¿Se dispone de licencias para aplicativos utilizados en la EPMAPA-T?		X		ERP /antivirus
DSS	DSS01.05	31	¿Las instalaciones eléctricas de la EPMAPA-T son aprobadas por un técnico experto?		X		
	DSS04.02	32	¿Se dispone de un plan de continuidad, frente a incidentes de TI?		X		
	DSS05.02	33	¿La instalación de elementos de red, son realizados con base a una norma externa que brinde seguridad?	X			Categoría

	DSS05.04	27	¿Se ha documentado el diagrama topológico con la finalidad de gestionar el acceso lógico de los usuarios internos de la EPMAPA-T	X			
	DSS06.03		¿Se ha designado privilegios, roles y permisos de red dependiendo las funciones del usuario interno?		X		

Anexo 12: Resultado hoja de trabajo – Analista de Sistemas

Hoja de Trabajo- Analista de Sistemas

Objetivo de auditoría

Desarrollar una evaluación informática a los procesos internos de la EPMAPA-T, con la finalidad de identificar riesgos de TI que afecten el cumplimiento de los objetivos institucionales y/o del área de TI.

Procesos a evaluar.

- Ejecución de planes, proyectos y/o programas de TI.
- Implementación de soluciones informáticas.
- Soporte Técnico
- Administración de redes.

Dominio	Cod.	N°	Preguntas	Si	No	N/A	Observaciones
BAI	BAI01.02	1	¿Actualmente forma parte de la ejecución de un plan, proyecto y /o programa referente a las TI?	X			P. cambio de paquete informático
	BAI01.04	2	¿Ha sido evaluado durante la ejecución de un plan, proyecto y/o programa?		X		
	BAI03.01	3	¿Ha participado en la implementación de soluciones informáticas en la EPMAPA-T?	X			
DSS	DSS01.01	4	¿Para el cumplimiento de sus funciones cumple con procedimientos documentados?	X			
	DSS01.01	5	¿Registra las actividades realizadas, después de realizar un procedimiento informático?	X			Registro de soporte
	DSS03.01	6	¿En el proceso de soporte técnico se han identificado incidentes frecuentes?	X			
	DSS03.01	7	¿Se ha definido modelos de incidentes para problemas frecuentes?		X		
	DSS03.05	8	¿Se han categorizado los incidentes de TI, en la EPMAPA-T?		X		
	DSS03.05	9	¿Se ha realizado un catálogo de soluciones para problemas de TI?		X		
	DSS04.07	10	¿Se realizan procedimientos de respaldo de información?	X			Del servidor
	DSS04.08	11	¿Se ha mejorado el procedimiento de respaldos, después un incidente?	X			
	DSS05.01	12	¿Se provee de antivirus, a los activos de la EPMAPA-T?	X			Kaspersky antivirus
	DSS05.04	13	¿Se gestiona la configuración de red, para todos los activos de la EPMAPA-T?	X			Diagrama topológico
	DSS06.03	14	¿Se verifica que las configuraciones de privilegios, roles y responsabilidades de los equipos se mantengan conforme al registro?		x		Que las direcciones no cambien

Anexo 13: Entrega del plan de mitigación de riesgos tecnológicos.

Tulcán, 10 de enero de 2020

EPMAPA-T
INGRESO DE DOCUMENTOS
SECRETARÍA GENERAL
Fecha: 10/01/2020
Hora: 12h46
Procedencia: - 050 -
Recibido por Johana

Ing.

Galo Tipaz

GERENTE GENERAL EPMAPA-T

Presente. –

De mi consideración:

Reciba un atento y cordial saludo, a la vez desearle toda clase de éxitos en las funciones que acertadamente desempeña.

El presente tiene como finalidad realizar la entrega formal del **PLAN DE MITIGACIÓN DE RIESGOS TECNOLÓGICOS,** resultado propuesto para el Proyecto de Titulación denominado "Plan de mitigación de riesgos tecnológicos basado en auditoría informática a la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán".

Adjunto los siguientes documentos tanto en físico como en digital.

- Informe de resultados de Auditoría Informática.
- Plan de mitigación riesgos tecnológicos

Los documentos han sido previamente revisados por el Supervisor Informático Institucional.

Atentamente

Realizado por:

Yuly Estefanía Pantoja Miño
Estudiante de la Carrera de Ingeniería en Informática
Universidad Politécnica Estatal del Carchi

Revisado por:

Ing. Alejandro Obando
Supervisor Informático EPMAPAT

EPMAPA-T
SISTEMAS

Anexo 14: Certificación otorgada por el Gerente General EPMAPA-T

EPMAPA-T
Empresa Pública Municipal de Agua Potable y Alcantarillado

CERTIFICO

Que la Señorita Yuly Estefanía Pantoja Miño con cédula Nº 040191671-3 estudiante de la Carrera de Ingeniería en Informática de la Universidad Politécnica Estatal del Carchi, trabajó en esta dependencia en el desarrollo del proyecto **"Plan de Mitigación de Riesgos Tecnológicos basado en Auditoria Informática a la Empresa Pública Municipal de Agua Potable y Alcantarilladlo de la ciudad de Tulcán"** la Institución ha brindado las facilidades para llevar acabo la finalización del mismo.

La propuesta del Proyecto que constituye el Informe de resultados de Auditoría Informática y el Plan de Mitigación de riesgos tecnológicos ha sido revisado y validado por el Supervisor Informático de la EPMAPA-T.

Estos resultados contribuyen a la Gestión Institucional por lo que extendemos nuestro agradecimiento a la academia por los resultados obtenidos.

Es todo cuanto puedo certificar en honor a la verdad, facultando a la interesada hacer uso del presente que estima conveniente. Con la excepción de que está certificación no será válida para ser presentada si se encuentra procesando cualquier trámite jurídico.

Dado y firmado en la cuidad de Tulcán a los veinte días del mes de Enero del año dos mil veinte.

Atentamente,

Ing. Galo Tipaz.
GERENTE GENERAL EPMAPA-T

EPMAPA-T
Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán
Somos Vida
GERENCIA GENERAL

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE INGENIERIA EN INFORMATICA

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL INFORME DE INVESTIGACIÓN DE:

NOMBRE: PANTOJA MIÑO YULY ESTEFANIA
CÉDULA DE IDENTIDAD: 0401916713
NIVEL/PARALELO: EGRESADA
PERIODO ACADÉMICO: OCT 2019 - FEB 2020

TEMA DE INVESTIGACIÓN: "Plan de mitigación de riesgos tecnológicos basado en auditoría informática a la Empresa Pública Municipal de Agua Potable y Alcantarillado de Tulcán"

Tribunal designado por la dirección de esta Carrera, conformado por:
PRESIDENTE: MSC. YANDÚN VELASTEGUI MARCO ANTONIO
LECTOR: MSC. GUADALUPE ALVÁREZ SANDRA DOLORES
ASESOR: MSC. GUANO CÁRDENAS CARLITOS ALBERTO

De acuerdo al artículo 21: Una vez entregados los requisitos para la realización de la pre-defensa el Director de Carrera integrará el Tribunal de Pre-defensa del informe de investigación, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS: 4 **AULA:** 214
FECHA: jueves, 30 de enero de 2020
HORA: 10H30
Obteniendo las siguientes notas:
1) Sustentación de la predefensa: 6,30
2) Trabajo escrito 1,90
Nota final de PRE DEFENSA **8,20**
Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo acatar el siguiente artículo:

Art. 24.- De los estudiantes que aprueban el Plan de Investigación con observaciones. - El estudiante tendrá el plazo de 10 días laborables para proceder a corregir su informe de investigación de conformidad a las observaciones y recomendaciones realizadas por los miembros Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el jueves, 30 de enero de 2020

MSC. YANDUN VELASTEGUI MARCO ANTONIO
PRESIDENTE

MSC. GUANO CÁRDENAS CARLITOS ALBERTO
TUTOR

MSC. GUADALUPE ALVÁREZ SANDRA DOLORES
LECTOR

Adj.: Observaciones y recomendaciones