UNIVERSIDAD DEL AZUAY

DEPARTAMENTO DE POSGRADOS

MAESTRIA EN AUDITORÍA INTEGRAL Y GESTIÓN DE RIESGOS FINANCIEROS VERSION III

"Gestión de riesgo de tecnologías de la información aplicado al Sector Financiero de Empresas Municipales de Movilidad, utilizando la Metodología ECU@Risk."

Trabajo de graduación previa la obtención del título de:

Magister en Auditoría Integral y Gestión de Riesgos Financieros

Autor:

CPA. Janneth Fernanda Velecela Aguilar

Director:

MBA, MSc. Esteban Crespo Martínez

Cuenca –Ecuador

Diciembre 2020

DEDICATORIA

Este logro va dedicado a mis papás Janneth y Fernando , a mis hermanos Mishel y Nando, a mis abuelitas Julia y Lupe, a mi enamorado Juan Pablo y a mis amados hijos de 4 patas Goofy, Dulce y Prometeo; por sin duda ser el motor que me impulsa a ser mejor cada día y a luchar por mis sueños.

Janneth Fernanda Velecela Aguilar

AGRADECIMIENTO

A Dios por ser la luz de mi camino, por permitirme obrar y actuar conforme a su voluntad, y bendecirme sin medida.

Al Magister, Esteban Crespo por su incondicional y preciso apoyo para llevar a cabo este proyecto, por permitirme trabajar de su mano y compartirme su vasto conocimiento.

Janneth Fernanda Velecela Aguilar

Resumen

La información se ha convertido en uno de los recursos más valiosos para el desarrollo de las actividades empresariales. El garantizar la disponibilidad, integridad y confidencialidad de la información ha dejado de ser un aspecto opcional, sin embargo, no se le otorga la importancia necesaria. Este trabajo estudia el riesgo de tecnologías de la información sobre los procesos en los que intervienen los productos informáticos desarrollados dentro del área financiera del sector de empresas públicas municipales de movilidad de la ciudad de Cuenca, mediante la aplicación de la metodología de gestión ECU@Risk, la cual ha sido desarrollada considerando el entorno empresarial ecuatoriano. Su aplicación permitió identificar y valorar los activos de información y sus amenazas, establecer valores de riesgo absoluto y proponer medidas de tratamiento, aportando significativamente al cumplimiento de los objetivos empresariales a partir de un tratamiento adecuado de este valioso recurso dentro del área financiera de la empresa.

Palabras Clave: Riesgos, activos de información, gestión de riesgo, Ecu@Risk

Abstract

Information has become one of the most valuable resources for the development of business activities. Guaranteeing the availability, integrity and confidentiality of the information is no longer an optional aspect, however, it has been given due importance. This work studied the risk of information technologies on processes in which computer products developed within the financial area of the sector of municipal public mobility companies of Cuenca intervene. This analysis was carried out through the application of the management methodology ECU@Risk, which has been developed considering the Ecuadorian business environment. Its application made it possible to identify and assess information assets and their threats, establish absolute risk values and propose treatment measures, significantly contributing to the fulfillment of business objectives based on an adequate treatment of this valuable resource within the financial area of the company.

Keywords: Risks, information assets, risk management, ECU @ Risk

Translated by

Janeth Velecela

Gestión de riesgo de tecnologías de la información aplicado al Sector Financiero de Empresas Municipales de Movilidad, utilizando la Metodología ECU@Risk

Fernanda Velecela-Aguilar[a], Esteban Crespo-Martínez[a, b]
[a]*Departamento de Posgrados,Universidad del Azuay*
[b]*LIDI, Universidad del Azuay*
Cuenca, Ecuador
fernandavelecela@es.uazuay.edu.ec; ecrespo@uzuay.edu.ec

***Resumen*—La información se ha convertido en uno de los recursos más valiosos para el desarrollo de las actividades empresariales. El garantizar la disponibilidad, integridad y confidencialidad de la información ha dejado de ser un aspecto opcional, sin embargo, no se le otorga la importancia necesaria. Este trabajo estudia el riesgo de tecnologías de la información sobre los procesos en los que intervienen los productos informáticos desarrollados dentro del área financiera del sector de empresas públicas municipales de movilidad de la ciudad de Cuenca, mediante la aplicación de la metodología de gestión ECU@Risk, la cual ha sido desarrollada considerando el entorno empresarial ecuatoriano. Su aplicación permitió identificar y valorar los activos de información y sus amenazas, establecer valores de riesgo absoluto y proponer medidas de tratamiento, aportando significativamente al cumplimiento de los objetivos empresariales a partir de un tratamiento adecuado de este valioso recurso dentro del área financiera de la empresa.**

Palabras Clave: Riesgos, activos de información, gestión de riesgo, Ecu@Risk

Abstract*—Information has become one of the most valuable resources for the development of business activities. Guaranteeing the availability, integrity and confidentiality of the information is no longer an optional aspect, however, it has been given due importance. This work studied the risk of information technologies on processes in which computer products developed within the financial area of the sector of municipal public mobility companies of Cuenca intervene. This analysis was carried out through the application of the management methodology ECU@Risk, which has been developed considering the Ecuadorian business environment. Its application made it possible to identify and assess information assets and their threats, establish absolute risk values and propose treatment measures, significantly contributing to the fulfillment of business objectives based on an adequate treatment of this valuable resource within the financial area of the company.

Keywords: Risks, information assets, risk management, ECU @ Risk

INTRODUCCIÓN

Hoy en día la información está considerada como uno de los bienes más preciados y de mayor importancia para las empresas, en virtud de aquello es indispensable considerar que dicha información está expuesta a diversas amenazas que podrían afectar su seguridad, integridad, disponibilidad y confidencialidad, lo que podría generar en consecuencia problemas con respecto al logro de los objetivos de una empresa.

La Empresa Pública de Movilidad, Tránsito y Transporte de Cuenca EMOV EP fue constituida el 9 de abril de 2010 mediante Ordenanza Municipal para la prestación de servicios públicos dentro de la circunscripción cantonal.

El presente artículo tiene por objetivo valorar los activos de información y sus amenazas para la posterior gestión del riesgo y propuesta de medidas de tratamiento al mismo, aplicable a los procesos en los que intervienen productos informáticos desarrollados dentro del área financiera de la EMOV EP, con el fin de determinar los activos de información con los que cuenta el área, pues si bien la empresa realiza levantamientos de activos en general, no se ha puesto énfasis en realizar una clasificación de activos tecnológicos, se pretende también identificar las amenazas en relación a éstos activos, obtener valores de riesgo absoluto y en virtud de éste considerar aquellas amenazas y activos que requieren la puesta en práctica de contramedidas.

La estructura de este trabajo se ha establecido en 8 apartados, descritos a continuación: i) Fundamentación teórica, donde se establecen aspectos importantes para el desarrollo de la gestión de riesgo de TI; ii) la situación actual de la empresa sobre el riesgo relativo a tecnologías de la información, en donde se ha determinado la factibilidad de la aplicar la metodología, iii) la aplicación de ECU@Risk, en este punto se lleva a cabo el proceso de gestión de riesgos en base al proceso establecido por la metodología, iv) los resultados obtenidos, derivados de la aplicación de ECU@Risk; v) la discusión, en la cual se evidencian trabajos de autores que tratan sobre la gestión de riesgos de TI mediante la aplicación de diferentes metodologías, así como también trabajos realizados utilizando la metodología ECU@Risk; en el apartado vi) se hace referencia a trabajos futuros que se podrían considerar en base a los resultados obtenidos en el presente; vii) las conclusiones y recomendaciones generales de este proceso de análisis; y finalmente viii) las referecias bibliográficas utilizadas en este documento.

I. FUNDAMENTACIÓN TEÓRICA

El riesgo es un factor que se ha presentado de manera inherente en cada acción del hombre, el mundo globalizado en el que vivimos ha provocado que la sociedad actual se vea inmersa en un ambiente altamente tecnológico en el cual la

información es el centro de actividades de la mayoría de las organizaciones.

Previo a hacer una reseña de los marcos de referencia y metodologías de gestión de riesgo de mayor utilización es importante definir lo siguiente:

La información es un activo que, al igual que otros activos del negocio, es esencial para la organización, la cual es registrada en un inventario de activos de información [1] y por lo tanto, debe ser protegida de forma adecuada [2] para afrontar los elementos de incertidumbre sobre el cumplimiento de los objetivos [3] conocido como riesgo, los cuales deben ser gestionados mediante medidas para análisis, evaluación, tratamiento, aceptación y comunicación [4].

A. Marcos de referencia relativos a la gestión de riesgos de tecnologías de la información

Dentro de los marcos de referencia de mayor divulgación a nivel mundial relativos a la gestión de riesgos de tecnologías de la información, se encuentran las normas ISO 27001, 27002, 27005 e ISO 31000, puntualizadas a continuación:

La norma ISO 27001 se fundamenta en el ciclo de mejora continua que consiste en Planificar-Hacer-Verificar-Actuar, creada para brindar un modelo que busca establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), pero, ¿A que nos referimos con seguridad de la información? Se trata de salvaguardar la información de los diversos tipos de amenazas para garantizar la continuidad de un negocio, minimizando riesgos y maximizando las oportunidades, ante lo cual la norma ISO 27002 proporciona un marco de gestión de seguridad de la información aplicable a todo tipo de organización, con el fin de satisfacer todos los objetivos y necesidades de una empresa [5], estableciendo recomendaciones de las mejores prácticas para la gestión de la seguridad de la información a todos los interesados y responsables de la implementación y mantenimiento de sistemas de gestión de la seguridad de la información [6].

Para el autor Esteban Crespo [1], ésta seguridad se fundamenta en tres principios básicos: confidencialidad, disponibilidad e integridad; se entiende por confidencialidad a los mecanismos que garantizan el acceso a la información a personas y organismos autorizados, por integridad al hecho de que esta se encuentre libre de modificaciones o alteraciones deliberadas, y por disponibilidad a la característica de que la información debe estar disponible cuando se la requiera.

Por otra parte, la norma ISO 27005, ha sido diseñada para ayudar a la aplicación eficiente de la seguridad de la información con un enfoque en la gestión de riesgos [7], contribuyendo de esta manera a la identificación, valoración, tratamiento, aceptación, comunicación, monitoreo y revisión de los riesgos [5],considera principalmente los requisitos y conceptos generales establecidos en la ISO 27001 [8].

Lo que se busca es conseguir seguridad de la información mediante el manejo o la gestión de riesgos efectiva dentro de la empresa, para lo que la Norma [3] recoge una serie de buenas prácticas internacionales que permiten una eficiente gestión de riesgos a todos los niveles de una organización, pues proporciona una guía de principios que ayudan a las empresas al análisis y evaluación de los riesgos, así también recomienda que las organizaciones implanten, desarrollen y mejoren continuamente un marco de trabajo que incluya en cada una de sus actividades integrar el proceso de gestión de riesgos.

La inadecuada administración, o la carencia de un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización, puede conllevar a un efecto llamado Riesgo Operativo [1], lo que podría desencadenar en pérdidas económicas y un deterioro en la imagen de la organización [9], por lo que, asegurarse de que se han instaurado los controles adecuados para mitigar el riesgo que suponen las amenazas graves para la seguridad de los datos y evitar que se aprovechen los puntos débiles del sistema, ha dejado de ser opcional [10].

Esto motiva que hoy en día sea cada vez mayor el número de organizaciones conscientes del impacto que pueden tener en el cumplimiento de sus objetivos los riesgos referentes a las Tecnologías de Información (TI) [11].

B. Metodologías de gestión de riesgos

Existen diversas metodologías enfocadas en el análisis y gestión de riesgos, entre las más utilizadas tenemos:

La guía Security Risk Management Guide creada por Microsoft [12], es un documento que se centra en la gestión de riesgos de seguridad, tomando como base tanto las experiencias propias de esta empresa como las de sus clientes, es una guía que ha sido probada y revisada por clientes, socios y personal técnico de Microsoft durante su desarrollo, así también toma como referencia estándares industrialmente aceptados para brindar un hibrido modelo de gestión de riesgos, en el cual los procedimientos cualitativos identifican oportunamente los riesgos más relevantes mientras que los cuantitativos se basan en roles y responsabilidades [13], ofreciendo a una organización como lo mencionan los autores López y Vásquez [7] una forma clara y de fácil entendimiento para organizar y asignar prioridades a cada activo de información, con el fin de identificar y gestionar de manera adecuada los riesgos y amenazas de las cuales son víctimas.

Con un enfoque similar en cuanto a gestión de riesgo se refiere, en el Centro de Coordinación CERT en Carnegie Mellon University [14] se creó la metodología Octave, esta se centra en el riesgo tecnológico y mantiene un enfoque estratégico, lo cual resulta de fácil aplicación para cualquier tipo de organización

Octave se centra en el trabajo diario de las empresas, identificando en primera instancia los activos de información, para el posterior estudio y análisis de cómo estos activos influyen en cada actividad contribuyendo al cumplimiento de metas y objetivos [7].

Así también es importante mencionar a la Metodología de Análisis y Gestión de Riesgos de Sistemas de la Información (Magerit), la cual fue promovida por el Consejo Superior de Administración Electrónica (CSAE), con el fin de sistematizar el análisis de los riesgos que pueden presentar los activos en una organización [15] como respuesta a la consideración del Gobierno español de investigar los riesgos que soportan los sistemas de información, propone la implementación del proceso de gestión de riesgos dentro de un marco de trabajo oportuno para que los órganos de gobiernos tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información [16].

En este punto cabe citar a la metodología CCTA Risk Analysis and Management Method (Cramm) [17], la cual permite identificar, medir y reducir al mínimo los ataques a los que están expuestas las organizaciones a diario, se define como una metodología que pone en práctica conceptos de manera formal, estructurada y disciplinada procurando los principios de la seguridad de la información y sus activos [15].

Se la conoce como una metodología mixta, pues abarca escenarios técnicos y no técnicos, cualitativos y cuantitativos [15], y proporciona un método riguroso por etapas que permite a las organizaciones tener una visión clara y priorizada de las amenazas a las que están expuestas y que pueden afectar al cumplimiento de las metas y objetivos del negocio [17].

Finalmente es preciso traer a contexto a la metodología ECU@Risk, propuesta por el autor Esteban Crespo [1], la cual parte de la necesidad de la organizaciones MPYMES ecuatorianas, al no estar preparadas en cuanto a gestión de riesgo se refiere, está basada en principios de administración de riesgos provistos en marcos de referencia internacionales como son las normas ISO 27001, 27002, 27005 e ISO 31000, así como también en el estudio de metodologías de amplia divulgación usadas para la gestión de riesgos de seguridad de la información como son Security Risk Management Guide, Octave, Magerit y Cramm.

ECU@Risk contempla 4 dominios, que incluyen, i) introducción al manejo del riesgo, donde se explica la importancia de la gestión de riesgos de información, ii) el marco de gestión de riesgo, punto en el cual se detallan los procedimientos para analizar el contexto, los responsables y las actividades a realizar por parte de los gestores de riesgos de información, iii) el proceso de gestión de riesgo, en este punto se realiza la identificación y valoración tanto de activos de información así como de amenazas sobre éstos, el cálculo de valores de riesgos y la determinación de medidas de tratamiento, iv) los recursos necesarios para realizar el proceso de gestión, como matrices para el cálculo de riesgos, u otras herramientas usadas para la recolección de información [18], la metodología está resumida en un manual, el cual brinda los procesos mínimos requeridos para gestionar de forma adecuada la información de una organización.

Así pues, ECU@Risk [19] sugiere roles y responsabilidades del personal que debe dar soporte y participar en los procesos de gestión, en los que debe considerarse la participación de la alta dirección, los propietarios de la información, los propietarios de los sistemas de información, un comité de riesgos de TI, el coordinador de seguridad designado, los profesionales de TI y un comité de certificación de productos y servicios de TI.

La metodología plantea el ciclo de un sistema para la gestión de riesgos, el cual consta de 4 etapas: i) Planificar, ii) Ejecutar, iii) Verificar y iv) Actuar, conformando 7 procesos de gestión, 1 proceso de monitoreo y control y 1 proceso de comunicación, mismo que será de suma importancia para las organizaciones en su afán de asegurar la información [20].

II. Situación actual de la empresa sobre el riesgo relativo a tecnologías de la información

Para establecer la situación actual de la empresa respecto al riesgo de tecnologías de la información, se consideran diversas normas jurídicas que emanan directrices a aplicar por parte de entidades del sector público dentro del cual se enmarca la EMOV EP.

En el numeral 2 del Artículo 18 de La Constitución de la República del Ecuador [21], se establece que es derecho de todas las personas el acceso a la información generada en instituciones públicas, o privadas que manejen fondos públicos, así como el derecho de acceso universal a las tecnologías de la información y comunicación.

Así mismo, el Artículo 66 en sus numerales 19 y 28, garantizan los derechos a la identidad, ya sea personal o colectiva, y a la protección de datos de índole personal, que incluye el acceso y la decisión sobre información y datos de este carácter. El mismo Artículo, en su numeral 25 y 26, garantizan el derecho a acceder a bienes y servicios públicos y privados de calidad, efectivos y eficientes y a un buen trato, así como a recibir información adecuada y veraz y el derecho a la propiedad en todas sus formas.

La Ley Orgánica del Sistema Nacional de Registro de Datos Públicos [22] en su artículo 4, establece "Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros…". La Ley Orgánica del Sistema Nacional de Registro de Datos Públicos [22] en su Artículo 6, se refiere a Información Confidencial y establece: "Se considerará información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de información personal o su divulgación, dará lugar a las acciones legales pertinentes…".

Así también la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional [23] en su Artículo 17 establece que: "…No se podrá acceder a información pública que tenga el carácter de confidencial o reservada, declarada en los términos establecidos por la ley. Tampoco se podrá acceder a la información estratégica y sensible a los intereses de las empresas públicas."

Por su parte las Normas de Control Interno de la Contraloría General del Estado [24] en su número 410-01 establecen: "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…", número 410-04 " …Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información…"

Considerando las directrices antes citadas la empresa de movilidad EMOV EP en su Reglamento Interno de Administración de Talento Humano [25] establece

parámetros con respecto al uso, manejo y tratamiento de la información.

Como parte de los deberes de las servidoras o servidores de la empresa está: i) el custodiar y cuidar la documentación e información que tengan bajo su responsabilidad, e impedir o evitar su uso indebido, sustracción, ocultamiento o inutilización; deben también: ii) guardar absoluta reserva y confidencialidad sobre asuntos y documentos que les corresponda conocer en razón de sus actividades y responsabilidades, absteniéndose de divulgar cualquier información que solo deberán conocer los interesados mediante la realización del trámite pertinente; en virtud de lo cual los funcionarios o personas que presten servicios en la empresa, junto con su contrato o nombramiento suscriben un convenio de confidencialidad en el que se comprometen a guardar reserva sobre información considerada como estrategia o sensible a los intereses de la Empresa; iii) Así mismo previo a la implementación, manejo o uso de cualquier sistema informático que involucre datos, documentos o firmas de uso personal de la empresa, los funcionarios recibirán la capacitación correspondiente.

Metodología

En base a la normativa anteriormente citada y previo a poner en práctica la metodología ECU@Risk, se realizó una encuesta con el fin de tener un punto de partida respecto a la conveniencia o no de la aplicabilidad de esta.

Las interrogantes se aplicaron a funcionarios pertenecientes al área de TIC's al ser esta dependencia la encargada de proveer soluciones, servicios tecnológicos e información para el desempeño y desenvolvimiento de las diferentes áreas que conforman la EMOV EP.

III. APLICACIÓN DE ECU@RISK EN EL ÁREA FINANCIERA DE LA EMPRESA DE MOVILIDAD

- *Paso 1: Determinación del contexto*

Como primer paso la metodología plantea la determinación del contexto tanto externo como interno en el cual se desenvuelve la empresa, el tipo y tamaño de esta. Aquí se define el alcance de la investigación y los objetivos, es decir qué proyecto, programa, actividad o dependencia es la que requiere análisis.

Haciendo referencia a la clasificación de las sociedades establecida por el Servicio de Rentas Internas, la empresa de movilidad se enmarca dentro del sector jurídico de derecho público; considerado el número de empleados pertenece al segmento de grandes empresas ya que cuenta con más de 700 funcionarios entre personal operativo y administrativo distribuido entre sus diferentes dependencias; su ámbito de acción es local, es decir su jurisdicción se manifiesta a nivel del cantón Cuenca.

Para la determinación del contexto externo fue necesario realizar el análisis PESTEL, que consiste en ir identificando situaciones que representen posibles oportunidades o en su defecto amenazas para la empresa, considerando 6 factores de los cuales se deriva su nombre, mismos que son: Político, Económico, Social, Tecnológico, Ecológico y Legal. Los resultados de la aplicación ver en anexos tabla 1.

Para la determinación del contexto interno, fueron considerados los valores organizaciones que dictan el actuar de la empresa los cuales se muestran en anexos tabla 2.

Análisis FODA

Lo siguiente a realizar es recabar los aspectos positivos y negativos de le empresa, tanto internos cuantos externos clasificados en Fortalezas y Debilidades, Oportunidades y Amenazas, estos aspectos se resumen en la tabla 3.

Para darle un carácter objetivo a las fortalezas, oportunidades, debilidades y amenazas éstas se han valorado considerando una escala que va del 1 al 5, siendo 1 poco importante y 5 muy importante.

Para continuar con el análisis de la matriz FODA se ha utilizado la herramienta de Posición Estratégica y Evaluación de Acciones PEEA, la cual se estructura en 4 cuadrantes que permiten ubicar a la empresa en diferentes posiciones estratégicas como: Agresiva, Conservadora, Defensiva o Competitiva [26]. Con los resultados obtenidos de la valoración de las fortalezas, oportunidades, debilidades y amenazas mediante el cálculo del valor de la balanza exógena y endógena, se determinó la posición en la que se encuentra ubicada la empresa [20].

En cuanto al alcance de la investigación, se ha decidido aplicar la metodología ECU@Risk sobre los procesos tecnológicos desarrollados por la empresa dentro de su área financiera, a razón de la importancia que tienen las actividades y funciones que en ésta se desarrollan, pues es el área financiera de la EMOV EP la dependencia que tiene a su cargo la administración, regulación y control del correcto uso de los recursos financieros de la institución [27]**.**

Para el análisis de contexto se utilizó la herramienta de análisis 7 S de McKinsey, esto mediante la elaboración de dos matrices, la primera necesaria para la identificación de roles y actividades incompatibles y la segunda para la identificación de habilidades. Así se ha realizado una matriz de identificación para cada cargo que comprenden los procesos del área financiera.

El paso 1 finalmente concluye con la determinación del estilo organizacional en este caso y considerando el objeto de estudio se aplicó un cuestionario de preguntas de la matriz de identificación del estilo organizacional al Gerente General y al Subgerente Financiero, por ser quienes están al frente de la empresa y del área financiera respectivamente.

- *Paso 2: Identificación de los activos de información*

La metodología ECU@Risk [19] plantea que los activos de información de una empresa pueden clasificarse en los siguientes grupos:

(ED) Edificaciones
(HW) Hardware
(SW) Software
(IE) Información electrónica
(IP) Información en papel
(Extraíble) Medios de almacenamiento extraíble
(IC) Infraestructura de comunicaciones
(RRHH) Recursos humanos

Figura 1 Clasificación de los Activos de información

El procedimiento por seguir para la identificación de los activos de información es el siguiente:

1. Identificar los activos de información

El proceso de identificación de activos de información (IA) se ha realizado considerando la "Clasificación de los Activos de información" que se muestra en la figura 1. En ella se presenta la clasificación de los activos de información pertenecientes al área financiera de la empresa agrupados en función de las diferentes categorías.

2. Valorar los activos de información

Posterior a la identificación, se valoran los activos de información. Para ello, como bien plantea la metodología ECU@Risk [19], se consideró las 3 dimensiones de valoración que son: Disponibilidad, Integridad y Confidencialidad. En este punto fue necesario plantearse las siguientes interrogantes con respecto a cada dimensión:

- Disponibilidad (D) ¿Qué pasaría si la información de esos activos no estaría disponible cuando se la necesite?
- Integridad (I) ¿Qué pasaría si los datos fueran modificados sin conocimiento ni control?
- Confidencialidad (C) ¿Qué pasaría si esa información es conocida por personas o sistemas no autorizados?

Bajo este preámbulo, se siguió con la valoración de los activos en función de cada dimensión y considerando una escala que va del 1 al 5 en donde 1 significa un daño menor y 5 un daño extremadamente grave, como se puede observar anexos figura 2.

- *Paso 3: Identificación de los riesgos*

El proceso de identificación de riesgos parte del cuestionamiento de las siguientes preguntas:

¿Qué puede pasar en caso de presentarse un evento de riesgo?

¿Qué factores pueden provocar su ocurrencia?

¿En dónde puede suceder?

¿Debido a qué puede suceder?

¿En caso de que ocurra, cuáles serían las consecuencias?

ECU@Risk propone la clasificación de riesgos de información empresariales que se muestra en anexos figura 3.

En función de esta clasificación se realizó la identificación de las amenazas sobre los activos de información, determinando los problemas, asignando e identificando con códigos las amenazas y determinando su probabilidad de ocurrencia para lo cual la metodología propone la escala de valores que se muestra en anexos figura 4.

- *Paso 4: Análisis de riesgos*

Una vez determinados los eventos de riesgo, lo siguiente a realizar es el análisis de riesgos. Este proceso requiere: i) identificar los controles que ya han sido implementados en la empresa para conocer si son efectivos, ii) la necesidad de llevar a cabo otras acciones para tratarlos, o en su defecto si lo mejor es no seguir actuando; iii) evaluar la probabilidad y las consecuencias que supondría el que los eventos de riesgos se lleguen a presentar; y iv) valorar el nivel de riesgo absoluto del área de estudio.

Una vez analizados los riesgos e identificado los controles actuales que mantiene la empresa, el siguiente paso consiste en valorar o calcular el nivel de riesgo, para lo cual la metodología propone valorar tanto la probabilidad de ocurrencia así como las potenciales consecuencias de llegar a materializarse el riesgo, esto se ha llevado a cabo en base a la matriz de riesgos, como se muestra en la figura 5, la cual considera una escala a 5 niveles tanto para la probabilidad que va desde *"Raro"* hasta *"Casi certero",* así como para la consecuencia o impacto que va desde *"Leve"* a *"Extremo".*

Consecuentemente se procede con el;

- *Paso 5: Evaluación de los riesgos*

Aquí se priorizan los riesgos identificados para formular posteriormente las contramedidas que harán frente a las amenazas identificadas en el contexto de los procesos de negocio.

- *Paso 6: Tratamiento de los riesgos y determinación de contramedidas*

El tratamiento de riesgos se enfoca en definir, en función de los niveles de riesgos, las acciones para gestionarlos, ya sea para evitar, reducir, transferir o aceptar el riesgo existente. Esto se realiza identificando en qué nivel de riesgo se encuentran los activos analizados y determinando las medidas de control.

IV. RESULTADOS

Con la aplicación de la encuesta, en primera instancia, se determinó que el 100% de los funcionarios de la empresa no están capacitados sobre la importancia que actualmente juegan las tecnologías de la información para el cumplimiento de sus funciones y el logro de objetivos empresariales. Referirse a los anexos, figura 6.

Para conocer la manera en que la empresa identifica sus activos de información, se planteó la siguiente pregunta: Con respecto a los activos de información, entendiéndose por estos: Hardware, Software, Información electrónica, Información en papel, Medios de almacenamiento extraíble, Infraestructura de comunicaciones, Recursos humanos, Edificaciones. ¿La empresa ha identificado correctamente sus activos de información? A lo que el 89% respondió que NO y el 11% restante que SI, ver anexos figura 7. Al preguntar sobre el inventario de activos de información que mantiene la empresa, clasificado en función de las diferentes categorías y en base a criterios de integridad, confidencialidad y disponibilidad, el 78% respondió que NO y el 22% que SI, ver anexos figura 8.

En cuanto a la existencia de procesos establecidos en base al cual se identifiquen las amenazas que podrían afectar los activos de información, el 89% de los encuestados respondió que NO y el 11% restante que SI, ver anexos figura 9. Así mismo era necesario saber si la empresa aplica alguna metodología para la gestión del riesgo de tecnologías de la información, interrogante a la cual el 100% de los encuestados coincidió que la empresa no se apoya en la aplicación de ninguna herramienta metodológica para gestionar el riesgo de TI, ver anexos figura 10.

A manera de saber si se tienen establecidas actividades a realizar luego de la materialización de un evento de riesgo, se preguntó: ¿Se tienen definidas las acciones a ejecutar posterior a la materialización de un riesgo? Respondiendo el 89% que NO existen definidas acciones a ejecutar, ver anexos figura

11. Cuando se preguntó a los funcionarios si la empresa considera como prioridad el tema de gestión de riesgos de tecnologías de la información, el 89% respondió que NO y el 11% restante que SI, la respuesta negativa se fundamenta principalmente en la falta de conocimiento sobre la importancia que tienen la gestión de riesgos de tecnologías de la información, ver anexos figura 12 y 13.

Para conocer si la empresa tiene identificadas sus áreas sensibles ante la materialización de un riesgo informático, se planteó dos preguntas, la primera muestra con un 78% que no se tienen definidas áreas sensibles, sin embargo, al preguntar cual consideran sería el área de mayor impacto ante la presencia de riesgos de tecnologías de la información, un 67% coincidió que sería el área Financiera, ver anexos figura 14 y 15. Al preguntar si se realizan auditorías informáticas en la empresa, el 78% respondió que NO y el 22% restante que SI, ver anexos figura 16.

Finalmente se buscó conocer sobre la existencia de un comité de Riesgos de Tecnologías de la información en la organización, a lo que el 100% de encuestados respondió que NO. Hacer referencia a los anexos, figura 17.

En cuanto al análisis de contexto, los resultados obtenidos aplicando la herramienta PEEA muestran que la empresa se encuentra dentro del escenario óptimo, al ubicarse en el cuadrante de fortalezas y oportunidades, esto significa que la empresa debe aprovechar los aspectos que representan fortalezas para de este modo poder generar oportunidades de negocio. (ver anexos tablas 4 - 8, y figura 18).

A continuación, se presenta la estructura organizacional del área de estudio.

Figura 19 Estructura organizacional área financiera

Fuente: [27]

El área financiera está compuesta por 6 procesos de apoyo que son: Subgerencia Financiera, Contabilidad, Tesorería, Cartera, Presupuestos y Coactivas; para finales del año 2019 se definieron procedimientos internos que se desarrollan en cada uno de ellos y se visualizan a continuación:

Tabla 9 Procesos del área financiera

ÁREA FINANCIERA		
Nro.	Proceso	Subproceso
1	Cartera	Ingreso de boletas de citación por infracciones de tránsito
2	Tesorería	Recaudación de Valores en los puntos Winchaje, Terminal Terrestre, Misicata
3	Coactivas	Recuperación de Cartera a través del cobro persuasivo y coactivo
4	Presupuestos	Emisión de Registro de Compromiso previo al pago
5	Contabilidad	Pago a proveedores
6	Subgerencia Financiera	Otorgamiento de Facilidades de Pago

Con la aplicación de la herramienta de McKinsey, se unificaron las matrices y se elaboró la Matriz de Identificación de roles y actividades, para esto se consideró la información que se encuentra establecida en el Manual de Funciones y Perfiles de Cargo implementado en la empresa desde el año 2016, el manual define las funciones para cada cargo en base a una recopilación de las tareas, actividades, destrezas y habilidades que debe poseer cada funcionario en virtud del proceso al que pertenezca y del cargo que desempeñe.

El proceso SUBGERENCIA FINANCIERA cuenta con 3 funcionarios, el Subgerente, 1 Asistente Financiero, 1 Auxiliar Financiero, ver anexos tablas 10, 11 y 12. El proceso CONTABILIDAD cuenta con 4 funcionarios, Contadora, 2 Analistas Contabilidad y 1 Asistente contabilidad, ver anexos tablas 13 - 15.

El proceso TESORERÍA cuenta con 42 funcionarios, Tesorero, 1 Especialista Tesorería, 1 Analista Tesorería, 1 Asistente Administrativo Tesorería, 1 Auxiliar Tesorería, 3 Auxiliar Ventas y 34 Auxiliares Recaudación, ver anexos tablas 16 – 22.

El proceso CARTERA cuenta con 7 funcionarios, esto es: 1 Analista, 1 Asistente Administrativo de Cartera y 5 Auxiliares de Cartera, ver anexos tablas 23-25.

El proceso PRESUPUESTO cuenta con 2 funcionarios, esto es el Experto en Presupuestos y el Auxiliar de Presupuestos, ver anexos tablas 26 y 27. El proceso COACTIVAS cuenta con 1 funcionario que es el Juez de coactivas, ver tabla 28.

Con respecto a la Matriz de identificación del estilo organizacional dirigida al Gerente General fue respondida considerando 5 niveles, donde 1 es “Muy Baja” y 5 es “Muy Alto”, por su parte la Matriz de identificación del estilo aplicada al área financiera y dirigida al Subgerente Financiero fue respondida considerando los siguientes niveles: 1 = “NUNCA”, 2 = “CASI NUNCA”, 3 = “A VECES”, 4 = “CON FRECUENCIA”, 5 = “SIEMPRE”.

Los resultados de las matrices de identificación del estilo organizacional muestran que la empresa no funciona de manera óptima, ya que por ejemplo la frecuencia con la que usuarios se quejan por un servicio deficiente o por mala atención por parte de los funcionarios, es alta. Así también con frecuencia se presentan casos de funcionarios con exceso de carga laboral y se presentan situaciones que afectan al clima laboral, ver anexos tablas 29 y 30.

Los puntos analizados anteriormente permiten tener una referencia sobre el entorno en el que se desenvuelve la empresa y de manera muy particular el área financiera.

Una vez cumplida esta etapa, se inició con el paso Nro. 2 de la metodología, que en primera instancia hace referencia a la identificación de los activos de información.

Los resultados de este proceso se visualizan en 8 matrices, ver como referencia en anexos tablas 31-38 en cada una de las cuales se realizó a través de un inventario, la identificación de los activos de información del área en función de la clasificación de activos antes definida.

Para finalizar el paso 2, se propone realizar la valoración de los activos de información para lo cual en las tablas 39 a la 44 se resumen los activos identificados con la valoración

respectiva en términos de integridad, disponibilidad y confidencialidad, ver anexos.

A continuación, se llevó a cabo el paso 3 de la metodología, referente a la identificación de riesgos, ver en anexos tabla 45 en la que se reflejan los problemas presentes dentro de los diferentes procesos del área financiera, los cuales desencadenan en amenazas relacionadas a cada uno de ellos y la frecuencia con la que se han producido el último año.

Como paso 4 se realizó el análisis de riesgos, en anexos tabla 46 se puede observar tanto el análisis, así como la determinación de controles existentes realizado dentro del área de estudio.

Posterior al análisis de riesgos y determinación de controles, corresponde realizar el paso 5, el cual consistió en el cálculo de valores de riesgos de cada proceso que conforma el área financiera de la empresa, en anexos tabla 47 se visualizan niveles de riesgo acumulado y absoluto determinados en función de las amenazas identificadas previamente y considerando las consecuencias que podrían generar sobre la disponibilidad, integridad y confidencialidad de los activos de información.

Finalmente, en base a los resultados obtenidos del cálculo de riesgo absoluto, se procede con el paso 6 que implica el tratamiento de riesgos y determinación de contramedidas. En la siguiente tabla se presentan el nivel de riesgo, su priorización y las acciones propuestas para mitigarlos.

Tabla 48 Matriz nivel de riesgo y acciones requeridas

Nivel Riesgo	Acción requerida	Riesgo identificado	Contramedidas
Riesgo extremo (E)	Requiere respuesta y atención inmediata.	Funcionamiento incorrecto del módulo de recaudación	Levantar un listado que abarque los requerimientos por parte de los usuarios del módulo para mejorar el servicio
			Integrar las diferentes opciones de cobro que mantiene el sistema de recaudación en un solo módulo que muestre un único total de valores adeudados y permita un desarrollo óptimo de las operaciones diarias
Nivel Riesgo	Acción requerida	Riesgo identificado	Contramedidas
Riesgo alto (A)	Debe otorgársele la atención apropiada.	Propagación de virus	Implementar una política de control de malware.
			Establecer acciones de respuesta ante un ataque.
		Pérdida accidental de información	Implementar una política de clasificación y tratamiento de información crítica y sensible, que incluya medidas a considerar como el realizar copias de seguridad o cifrado de información
		Falta de comunicación de procesos de ingreso y cobro de infracciones	Implementar una política de selección, inducción y capacitación al personal, previo al desempeño de sus funciones.
		Errores en la operación del servidor de matriz	Mantener un registro diario de los eventos, necesidades y actualizaciones de los equipos para evitar que se sobrecarguen y dejen de operar correctamente.
		Registro incompleto de actividades	Realizar la detección de errores, situaciones fuera de lo normal o intrusiones mediante el establecimiento de mecanismos de monitorización continua sobre los registros de actividades
		Inadecuado registro de actividades	
Riesgo medio (M)	Evaluar el riesgo y determinar si los controles implementados son suficientes y si están siendo efectivos.	Inadecuado uso de computadoras	Implementar una política que garantice el uso y tratamiento adecuado de hardware. Disponer de un stock de equipos a usar ante el fallo de otro
		Uso excesivo de equipos	
		Errores de instalación de los equipos	
		Denegación de servicio web	Establecer una política de web confiable. Realizar mantenimiento y soporte permanente a la página web.
		Negligencia en la entrega de especies valoradas	Definir un procedimiento para realizar la distribución de especies valoradas a los diferentes puntos de recaudación
		Desconocimiento de funciones y roles de cargo	Difundir al personal el manual de funciones según cada cargo.
			Formar, capacitar y promover entre el personal una cultura que priorice la seguridad de la información.
		Ataques mediante difusión de correos maliciosos	Implementar una política de control de malware. Establecer acciones de respuesta ante un ataque.
		Información sensible de usuarios expuesta	Implementar herramientas que garanticen la confidencialidad, disponibilidad e integridad de la información a través de la monitorización, detección y prevención de fugas de información sensible.
		Falta de mantenimiento de red de infraestructuras	Implementar una política de mantenimiento preventivo
		Exceso de carga laboral	Cumplir con la política de contratación de personal ante una necesidad institucional
Nivel Riesgo	Acción requerida	Riesgo identificado	Contramedidas
Riesgo Bajo (B)	Administrar mediante procedimientos rutinarios; informar a los gestores locales; supervisar y revisar localmente como sea necesario.	Acceso de personal no autorizado	Implementar un sistema de control de acceso que permita el ingreso a estos espacios solamente por personal autorizado
			Llevar un registro de accesos con fecha, hora y personal que ingrese.
			Actualizar el sistema de alarma,
		Corto circuito	Implementar un sistema de control eléctrico

Fuente: [19] Elaborado por el autor

V. DISCUSIÓN

Como se puede apreciar, los resultados de la encuesta muestran aspectos fundamentales como el hecho de que para la empresa el tema relacionado con la gestión de riesgos de TI no es una situación de prioridad, brevemente se puede notar la falta de conocimiento sobre el rol fundamental que desempeñan las tecnologías de la información en el cumplimiento de los objetivos empresariales, situación que podría fundamentarse en la carencia de procesos de capacitación a los funcionarios en cuanto a temas de TI se refiere, la empresa no dispone de un inventario de activos de información oficial, estos no se clasifican en virtud de criterios básicos de disponibilidad, confidencialidad e integridad, así también la empresa no tiene definidos procesos y acciones a

ejecutar ante la materialización de un riesgo de TI, otra situación importante es que la empresa no dispone de un comité de riesgos de TI y si bien no se tienen identificadas áreas o procesos críticos, se considera al área financiera como una de las de mayor riesgo ante posibles amenazas. En base a estos aspectos se considera oportuno la aplicación de la metodología ECU@Risk para gestionar el riesgo de tecnologías de la información en el área financiera de la EMOV EP.

Los resultados derivados de la aplicación de la metodología ECU@RISK permitieron cumplir con el objetivo planteado en este trabajo, al finalizar el proceso de gestión de riesgo de tecnologías de la información para los departamentos que forman el área financiera de la empresa de movilidad, se logró:

1. Determinar el contexto tanto interno cuanto externo en el cual se desenvuelve la empresa, estableciendo de esta manera aquellos factores que pueden representar una oportunidad de mejora o por el contrario una situación de riesgo.

2. Identificar los activos de información, obteniendo un inventario de 59 activos fundamentales para el cumplimiento de las actividades propias del área financiera, los cuales fueron clasificados en función de las diferentes categorías como son: Edificaciones, Hardware, Software, Información electrónica, Información en papel, Medios de almacenamiento extraíble, Infraestructura de comunicaciones y Recursos humanos; en este paso se realizó también la valoración de los activos considerando criterios de integridad, disponibilidad y confidencialidad y una escala de valores que permitió definir el daño que se provocaría en los activos si una de estas 3 dimensiones se viera vulnerada;

3. Identificar y valorar las amenazas sobre los activos considerando la probabilidad de ocurrencia y el impacto que podrían generar de llegar a materializarse, determinando así 19 potenciales amenazas,

4. Analizar los riesgos y determinar los controles actuales que se mantienen sobre los procesos tecnológicos creados por la empresa dentro del área financiera, pudiéndose observar un deficiente actuar respecto a los riesgos de TI,

5. Evaluar y calcular valores de riesgo sobre los activos de información, paso en el que se realizó la matriz de registro y cálculo de riesgos, en la cual se fusionaron los activos de información identificados, con sus respectivas amenazas, valoración, frecuencia e impacto, dando como resultado un valor de riesgo absoluto para cada activo

6. Determinar los niveles de riesgo dentro de los cuales se enmarcan la amenazas sobre los activos, siendo así que: 2 amenazas concretamente relacionadas con la categoría de edificaciones y medios de almacenamiento extraíble se encuentran dentro de un nivel de riesgo bajo; 10 amenazas relacionadas con software, hardware, información en papel y recursos humanos, en un nivel de riesgo medio, 6 amenazas sobre las mismas categorías anteriormente mencionadas en un nivel de riesgo alto y 1 de las amenazas está dentro de un nivel de riesgo extremo, se trata de la categoría de software que tiene que ver con el sistema único de recaudación creado e implementado por la empresa, finalmente para cada una de las amenazas se establecieron medidas de tratamiento a considerar para mitigar los riesgos sobre los activos de información.

En este punto es pertinente traer a contexto artículos y trabajos realizados en relación con el tema de estudio. Tola y Freire [28] realizan un trabajo conjunto al analizar las probabilidades e impactos de los riesgos sobre activos de información y buscan calcular niveles de riesgo para una empresa de consultoría y auditoría, utilizando la metodología MAGERIT [29]. Tola y Freire [28] esperan que con la adopción de esta metodología puedan identificar la probabilidad y el impacto de que se materialicen los riesgos para establecer controles que ayuden a prevenirlos. Sin embargo, su trabajo concluye únicamente con la determinación de políticas y estrategias para el manejo de riesgos, pero exclusivamente en el plano teórico, pues en ninguna etapa del artículo se llevó a cabo un análisis y gestión de riesgo como tal; cabe recalcar que la metodología planteada por los autores fue creada considerando parámetros y métricas internacionales.

Por su parte, los autores Valencia Duque y Orozco Alzate [30] en su artículo que trata sobre la implementación de un sistema de gestión de seguridad de la información en base a la familia de normas ISO/IEC 27000, concluyen que si bien actualmente la familia de las normas ISO 27000 cuenta con gran cantidad de normativa referente al tratamiento y gestión de riesgos, el llevar a cabo su propuesta puso en manifiesto una complejidad adicional al proceso metodológico por esta misma razón, por lo cual en el desarrollo de su trabajo tuvieron que considerar las normas que a su criterio son las más relevantes.

En contraste con los trabajos anteriores, cabe mencionar que la metodología ECU@Risk ha sido desarrollada en base a la recopilación de las mejores prácticas y métodos existentes, ha logrado diseñar un modelo de gestión de riesgos de tecnologías de la información particularmente a ser aplicado dentro del marco legal ecuatoriano [31], lo cual hace aún más viable y efectiva su puesta en práctica por empresas nacionales.

Así también, es oportuno mencionar el trabajo de los autores Gómez et al. [11] en el que se evidencia que utilizan como metodología para el análisis de riesgos de TI a OCTAVE, ellos concluyen que ésta herramienta se ha implementado con el fin de que una organización pueda cumplir con sus objetivos, para lo cual es necesario que los miembros de ésta conozcan que activos relacionados con la información son importantes y cómo deben ser protegidos, siendo fundamental que en la evaluación se cuente con la participación de personas de los diferentes niveles y jerarquías de la organización.

La autora Nelly Ávila [20] en su trabajo de titulación implementa la Metodología ECU@Risk, para gestionar los riesgos de tecnologías de la información dentro del sector hospitalario, Ávila concluye que la metodología provee de manera detallada los principios y procesos necesarios para identificar y valorar los activos y las amenazas, calcular los riesgos, identificar las contramedidas y establecer políticas de seguridad.

Los autores, Crespo y Bermeo [32] determinan la ventaja que ECU@Risk tiene frente a Microsoft Risk Management, pues contempla un contexto mayor sobre seguridad de la información, pues no se enfoca únicamente en los activos de hardware y software, sino considera una amplia gama de elementos que contienen información. Así mismo Crespo y Bermeo mencionan que con respecto a CRAMM, la

metodología ECU@Risk se enfoca en el análisis y aseguramiento de información en el segmento de empresas del sector PYME; mientras que sobre las metodologías OCTAVE y Magerit, ECU@Risk visualiza fortalezas en cuanto a la identificación de contexto empresarial; a más de concentrar su atención en un contexto de realidad ecuatoriana.

Finalmente, Carvajal Portilla, Cardona Londoño y Valencia Duque [33] autores a quienes se le atribuye el artículo titulado "Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana" terminan su trabajo mencionando que para lograr una exitosa gestión de riesgos de tecnologías de la información se debe considerar siempre contar con la concientización de los colaboradores, el compromiso de la alta dirección y mantener una cultura organizacional orientada al objetivo, afirmación que coincide con el pensar del autor Esteban Crespo [31] quien manifiesta que para que sea efectiva la aplicación de la metodología ECU@Risk será importante la participación de la gerencia en los procesos de gestión de riesgo, pues el compromiso que ésta mantenga será fundamental para lograr mitigar los riesgos, junto con el actuar de un buen equipo de trabajo logrando de esta manera alcanzar las metas y objetivos empresariales.

VI. TRABAJOS FUTUROS

Considerando la importancia de la gestión de riesgos de TI y los resultados derivados de la aplicación de ECU@Risk, en un próximo trabajo se buscará emplear la metodología a nivel de todas las áreas que conforman la empresa, así como también en base a los resultados obtenidos dentro del área financiera poder determinar el riesgo residual obtenido una vez ejecutadas las medidas de tratamiento propuestas.

VII. CONCLUSIONES Y RECOMENDACIONES

Desde hace siglos se considera que *"la información es poder" Francis Bacon,* no obstante, quien tiene el poder no es quien sabe dónde encontrar determinado material, fuente o dato, sino quien sabe qué hacer con aquello que encontró.

Actualmente el planeta atraviesa una situación de riesgo generado por la pandemia del COVID-19, que ha significado un salto importante en el uso de las telecomunicaciones para resolver temas de teletrabajo, aprovisionamiento de bienes, conectividad social y acceso a la información. [34].

Si bien el sector público de empresas municipales dispone de normativa relativa a temas de acceso a la información, protección de datos de índole personal, manejo de fondos públicos en pro de implementar procesos que garanticen transparencia, seguridad, calidad, control en el uso de firmas electrónicas, mensajería de datos, legalidad de software entre otros, cabe recalcar que en la práctica son muy pocas las empresas municipales que atribuyen la importancia que se merecen las tecnologías de la información desde siempre y aún más en los tiempos actuales.

Con respecto al sector financiero de empresas municipales de movilidad, objeto de este análisis se puede concluir que:

1. Con la aplicación de la metodología ECU@Risk se consiguió determinar los riesgos a los que hace frente el área financiera de la empresa día a día en el cumplimiento de cada uno de sus procesos. A este resultado se llegó con desarrollo de cada paso propuesto por la metodología, identificando y valorando los activos de información, amenazas presentes, estableciendo niveles de riesgo absoluto de cada activo y determinando medidas de tratamiento para mitigar los riesgos.
2. La aplicación de ECU@Risk sin duda, ha sido de gran oportunidad y efectividad, pues a través de éste análisis se han podido determinar aspectos críticos a considerar por parte del personal directivo de la empresa, para mejorar el desenvolvimiento del área financiera así como a nivel de toda la estructura empresarial, pues el anticiparse y ganarle ventaja al riesgo siempre traerá beneficios que permitan proteger y garantizar la seguridad de uno de los activos más importantes con los que cuenta la empresa como es la información, y en consecuencia contribuir al logro de los objetivos.
3. Las tecnologías de la información sin duda constituyen parte fundamental en las operaciones que tiene a cargo el área financiera, y si bien la empresa de movilidad cuenta con un área de tecnologías de la información y comunicación, al fin del día no es suficiente para la cantidad de acciones, procedimientos y medidas a poner en práctica para resguardar la seguridad, integridad y confidencialidad de la información, base para cumplir las actividades diarias de la empresa.
4. Resulta necesario considerar la idea de implementar un comité de riesgos de tecnologías de la información (CRTI), necesario para evaluar y monitorear la seguridad de la información. Este comité será el que sugiera acciones y encamine la toma de decisiones en base a un adecuado programa de gestión de riesgo.
5. Así también se debe considerar dotar de personal calificado para reforzar el área de tecnologías pues es ésta quien sirve de soporte y sustento de servicios tecnológicos de la empresa.
6. La capacitación al personal en temas relativos al manejo, tratamiento y uso de tecnologías de la información debe ser una acción prioritaria, más no opcional, sobre todo considerando la falta de conocimiento que es latente entre los funcionarios.
7. Finalmente es imprescindible contar con el apoyo y accionar conjunto de todo el personal de la empresa, tanto el nivel directivo como administrativo y operativo, pues únicamente con la colaboración de todos se podrán alcanzar los objetivos empresariales.

VIII. REFERENCIAS BIBLIOGRÁFICAS

[1] Crespo, «Metodología de Seguridad de la Información para la Gestión del Riesgo Informático aplicable a MPYMES,» 2016.

[2] ISO/IEC, *17799:2005 Código de práctica para la Gestión de la Seguridad de la Información.*, 2005.

[3] ISO 31000, Norma ISO 31000: el valor de la gestión de riesgos en las organizaciones.

[4] E. S. d. R. RED CEDIA, «Gestión de la Seguridad de la Información,» s,f. [En línea]. Available: https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI8.pdf.

[5] G. Cordero Torres, *Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información,* Cuenca , 2015.

[6] C. De la Torre y M. De la Torre , «Planteamientos Básicos para la implementación de las Normas ISO 27001 E,» *Revista virtual de seguridad informática,* p. 19, s,f.

[7] D. Lopez y S. Vásquez, *Comparación entre Metodologías de Gestión de Riesgo Informático,* Cuenca, 2016.

[8] E. ISO Tools, «Cómo implantar eficazmente la norma ISO 27005,» 2015.

[9] P. S. S. Council, «PCI Security,» 2018. [En línea]. Available: https://www.pcisecuritystandards.org/pci_security/.

[10] A. ISO 27001, *Sistema de Gestión de Seguridad de la Información,* 2015.

[11] Gomez R, Pérez D, Donoso Y, Herrera A, «Metodología y gobierno de la gestión de riesgos de tecnologías de la información,» *Revista de Ingeniería,* pp. 109-118, 2010.

[12] C. Microsoft, *The Security Risk Management Guide,* 2006.

[13] M. Cobb, «ComputerWeekly.com,» 10 05 2011. [En línea]. Available: https://www.computerweekly.com/tip/How-to-use-the-free-Microsoft-Security-Risk-Management-Guide.

[14] G. Vanegas Devia y C. Pardo, *Revista S&tT,* pp. 35-48, 2014.

[15] A. Abril, J. Pulido y J. Bohada, «Análisis de Riesgos en Seguridad de la Información,» *Revista Ciencia, Innovación y Tecnología (RCIYT),* 2013.

[16] Ministerio de Hacienda y Administraciones Públicas, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.Magerit 3.0, Madrid-Española, 2012.

[17] M. Fernandez, *Estudio de una estrategia para la implantación de los Sistemas de Gestión de la Seguridad de la Información,* 2003.

[18] Crespo, Esteban; Bermeo, Jorge, «Evaluando el nivel de riesgo de información en PYMES con ECU@Risk,» 2018.

[19] E. Crespo, «Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMES,» *Enfoque UTE, V.7-Sup. 1,* pp. 107-121, 24 02 2017.

[20] Ávila Nelly, Cuenca, 2018.

[21] «Constitución de la República del Ecuador,» Montecristi, 2008.

[22] «Ley Orgánica del Sistema Nacional de Registro de Datos Publicos,» 2010.

[23] «Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional,» 2009.

[24] «Normas de control Interno de la Contraloría General del Estado,» 2009.

[25] EMOV EP, «Reglamento Interno de Administración de Talento Humano,» 2013.

[26] ISO, *La matriz PE y EA para formular la estrategia,* 2017.

[27] EMOV EP, de *Manual de funciones y perfiles de cargo,* 2016.

[28] Tola D, Freire L, «Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de consultoría y auditoría, aplicando la Norma ISO/IEC 27001,» 2015.

[29] Ministerio de Hacienda y Administraciones Públicas, Gobierno de España, «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.».

[30] F. X. Valencia Duque y M. Orozco Alzate, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000.,» *Revista Ibérica de Sistemas y Tecnologias de Información,* pp. 73-88, Junio 2017.

[31] Crespo E, «Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs,» *Enfoque UTE,* pp. 107-121, 2017.

[32] *Evaluando el nivel de riesgo de información en PYMES con ECU@Risk,* 2018.

[33] D. Carvajal Portilla, A. Cardona Londoño y F. Valencia Duque , «Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana,» *Entre Ciencia e Ingeniería, Vol. 13,* pp. 68-76, 2019.

[34] B. D. D. D. A. L. CAF, «COVID-19:¿Cúal es el estado de la digitalización de América Latina para la resilencia social, económica y productiva?,» 07 04 2020.

[35] «Código Orgánico de Organización Territorial Autonomía Descentralización,» Quito, 2010.

[36] «Ordenanza de Constitución, Organización y Funcionamiento de la EMOV EP,» Cuenca, 2010.

[37] «Norma de Concentraciones de Emisión al Aire Desde fuentes Fijas de Combustión».

[38] EMOV EP, *Plan Estratégico EMOV EP,* 2015.

[39] C. Alberts, A. Dorofee y C. Woody, 2003.

[40] Crespo, Esteban; Bermeo, Jorge, «Evaluando el nivel de riesgo de información en PYMES con ECU@Risk,» 2018.

[41] E. Crespo, «Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMES,» *Enfoque UTE, V.7-Sup. 1,* pp. 107-121, 24 02 2017.

[42] «Ley Orgánica de Transparencia y Acceso a la Información Pública,» 2004.

ANEXOS

Tabla 1 Análisis PESTEL

CUADRO DE ANÁLISIS PESTEL EMPRESA DE MOVILIDAD				
Factor	**Fuentes de análisis**	**Descripción**	**C**	**P**
POLÍTICO	Constitución de la República del Ecuador 2008	Art. 315. El Estado constituirá empresas públicas para la gestión de sectores estratégicos, la prestación de servicios públicos, el aprovechamiento sustentable de recursos naturales o de bienes públicos y el desarrollo de otras actividades económicas	O	
	Código Orgánico Organización Territorial Autonomía Descentralización COOTAD	Art. 55…Los gobiernos autónomos descentralizados municipales tendrán las siguientes competencias exclusivas sin perjuicio de otras que determine la ley…b) Ejercer el control sobre el uso y ocupación del suelo en el cantón, …f) Planificar, regular y controlar el tránsito y el transporte terrestre dentro de su circunscripción cantonal.	O	
ECONÓMICO	Ordenanza de Constitución, Organización y Funcionamiento de la EMOV EP	Art. 41.- Son recursos de la Empresa los siguientes: a) Ingresos corrientes, que provinieren de las fuentes de financiamiento que se derivaren de su poder de imposición, de la prestación de servicios de movilización, tránsito y transporte…	A	P
	Constitución de la República del Ecuador 2008	Art. 315…Las empresas públicas estarán bajo la regulación y el control específico de los organismos pertinentes, de acuerdo con la ley; funcionarán como sociedades de derecho público, con personalidad jurídica, autonomía financiera, económica…	A	
SOCIAL	Ordenanza de Constitución, Organización y Funcionamiento de la EMOV EP	La EMOV EP orientará su acción con criterios de eficiencia, racionalidad y rentabilidad social, preservando el ambiente, promoviendo el desarrollo sustentable, integral y descentralizado de las actividades económicas de acuerdo con la Constitución, siendo su objeto organizar, administrar, regular y controlar las actividades de gestión, ejecución y operación de los servicios relacionados con la movilidad, tránsito y transporte terrestre en el cantón Cuenca, propendiendo al mejoramiento y ampliación de los servicios públicos y de sus sistemas, buscando aportar soluciones convenientes, desde el punto de vista social, técnico, ambiental, económico y financiero	O	P
TECNOLÓGIO	Normas de Control Interno de la Contraloría General del Estado	Norma. 410-01 “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…”	O	
ECOLÓGICO	Constitución de la República del Ecuador 2008	Art. 14.- Se reconoce el derecho de la población a vivir en un ambiente sano y ecológicamente equilibrado, que garantice la sostenibilidad y el buen vivir.	O	
	Norma de Concentraciones de emisión al Aire desde Fuentes Fijas de Combustión	Creada con el objeto de preservar la salud pública, la calidad del aire ambiente, las condiciones de los ecosistemas y del ambiente en general.	O	
LEGAL	Constitución de la República del Ecuador 2008	Art. 264.- Los gobiernos municipales tendrán las siguientes competencias exclusivas… 6.- Planificar, regular y controlar el tránsito y el transporte público dentro de su territorio cantonal.	O	
	Código Orgánico Organización	Art. 55…Los gobiernos autónomos descentralizados municipales tendrán las siguientes competencias exclusivas sin perjuicio de otras que determine la	O	

	Territorial Autonomía Descentralización COOTAD	ley…b) Ejercer el control sobre el uso y ocupación del suelo en el cantón, …f) Planificar, regular y controlar el tránsito y el transporte terrestre dentro de su circunscripción cantonal.		
OBSERVACIONES				
SIMBOLOGÍA: C= CONDICIÓN; P= PRIORIDAD; O= OPORTUNIDAD; A= AMENAZA				

Fuente: *[21] [24] [35] [36] [37] [19]*.

Tabla 2 Valores Organizacionales Compartidos

VALORES COMPARTIDOS ORGANIZACIONALES	
Misión	Trabajar por un sistema de movilidad responsable en el cantón Cuenca de manera sustentable y eficaz, mediante la gestión, administración, regulación y control del tránsito, transporte terrestre y movilidad no motorizada, precautelando el bienestar, la vida y la salud de la ciudadanía, mediante la concientización
Visión	Contando con Talento Humano Motivado y Comprometido, con el apoyo de procesos y tecnología de punta, en el término de ocho años, generar una cultura permanente de convivencia entre la movilidad motorizada y no motorizada, contribuyendo al bienestar de la ciudadanía y al ordenamiento del cantón
Valores	• Transparencia • Capacidad y excelencia para la prestación de un servicio integral e integrado. • Vocación de trabajo en equipo. • Respeto y amabilidad en la relación con el cliente usuario. • Capital humano motivado. • Conciencia del empoderamiento de la responsabilidad ambiental. • Responsabilidad social
Objetivos institucionales	• Elaborar, implementar y controlar el cumplimiento de acciones en el ámbito del sistema de movilidad para el mejoramiento de la calidad de vida, seguridad ciudadana, salud pública, y la mitigación de los efectos ambientales constantes en el eje de movilidad del plan de ordenamiento territorial del cantón. • Implementar un plan de posicionamiento institucional y de imagen corporativa. • Establecer un modelo de negocios que permita la sostenibilidad financiera de la Empresa. • Ejecutar proyecto y campañas permanentes de educación ciudadana. • Proponer reformas a la normativa vigente relativa a la Movilidad en lo local. • Promover la tecnificación e investigación científica en temas de Movilidad: convenios de cooperación interinstitucional, alianzas estratégicas, contratos de servicios. • Proponer un Plan de Movilidad elaborado de manera participativa con los actores del sistema para el cantón Cuenca. • Mejorar los estándares de calidad que garanticen la seguridad ciudadana en atención a las políticas públicas de Movilidad. • Propender a la prestación de servicio de transporte público de calidad, que brinde seguridad, agilidad, oportunidad, disponibilidad, comodidad, accesibilidad, a los usuarios del cantón Cuenca, mejorando la calidad de vida, precautelando la salud ambientalmente sustentable, fortaleciendo la generación productiva y económica del cantón

Fuente: *[19] [38]*

Tabla 3 Matriz FODA

MATRIZ FODA EMOV EP		
Aspectos positivos	Aspectos negativos	
Fortalezas 1. Marca bien posicionada, genera réditos políticos 2. Campañas públicas bien aceptadas 3. Reducción de índices de accidentes 4. Aceptación social al trabajo realizado 5. Empoderamiento de las competencias 6. Servicios destinados al bienestar social 7. Equidad en el cumplimiento de las normas. 8. Pioneros en asumir las competencias en movilidad, tránsito y transporte 9. Recurso humano joven en su mayoría 10. Liderazgo del nivel de gobierno y en nivel ejecutivo	***Debilidades*** 1. Es considerada una empresa sancionadora 2. Cartera vencida elevada por falta de cultura de pago 3. Carencia de procesos formales 4. Falta de aplicación de normas de calidad 5. Gestión susceptible de cambios en la regulación 6. Recurso humano desmotivado por la falta de capacitación y compromiso 7. Sistemas informáticos desintegrados 8. Falta de cultura organizacional en el servicio al cliente 9. Falta de aplicativos informáticos 10. Organigrama vertical obsoleto	*De origen interno*
Oportunidades 1. Incremento del ingreso por uso de tecnologías 2. Interacción con la comunidad que genera credibilidad y posibilidad de continuar en el proceso y potenciarlo 3. Ciudadanos conscientes de que la movilidad mejora la calidad de vida 4. Posibilidad de incremento de ingresos con mayor cobertura de servicios 5. Determinación de procesos al tener autonomía en la gestión 6. Apoyo del alcalde a la gestión de la empresa 7. Oferta tecnológica para la línea de negocio 8. Apoyo interinstitucional de acuerdo a las necesidades 9. Experiencia del alcalde en la gestión pública 10. Oportunidades de reorganizar las estructuras	***Amenazas*** 1. El éxito de las campañas genera interés de otras instituciones de usufructuar el posicionamiento de la marca 2. Las redes sociales generan un espacio inmediato de ataque a la gestión 3. Falta de fondos y financiamiento para municipalizar el transporte 4. La sociedad Cuencana requiere de un transporte administrativo y subvencionado por la Municipalidad y, no existe financiamiento 5. Repudio ciudadano por control 6. Confusión entre entidades nacionales y locales basadas en su mala reputación 7. Retiro de la competencia por falta de cumplimiento 8. Falta de modelos a seguir en procesos 9. Falta de estándares de calidad 10. Continuos cambios en la normativa	*De origen externo*

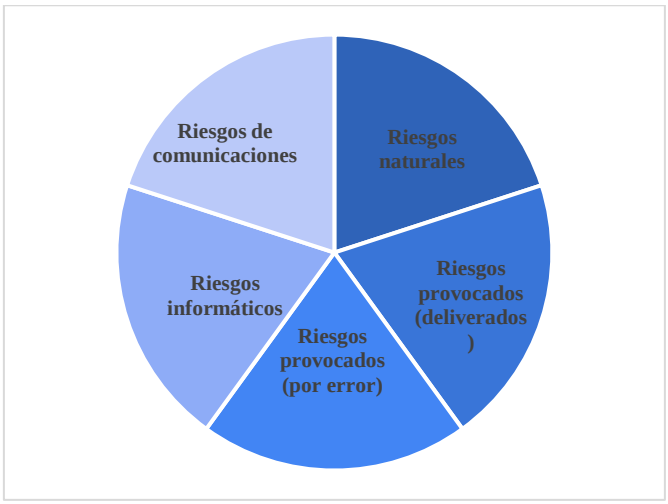
Fuente: *[38] [19]*

Figura 2 Criterios de valoración

Valor	Criterio	
5	Extremo	Daño extremadamente grave
4	Alto	Daño muy grave
3	Moderado	Daño grave
2	Menor	Daño importante
1	Leve	Daño menor
0	Despreciable	Irrelevante

Fuente: *[19]*

Figura 3 Clasificación de los riesgos de información



Fuente: *[19]*

Figura 4 Representación de probabilidades

	Número de eventos similares producidos en el último año	Probabilidad (%) de que ocurra de nuevo	Calificación
E - Casi certero	11 en adelante	85 - 100	5
A - Probable	7 - 10	70 - 84	4
M - Posible	4 - 6	30 - 69	3
B - No muy común	2 - 3	4 - 29	2
L - Raro	1	1 - 3	1

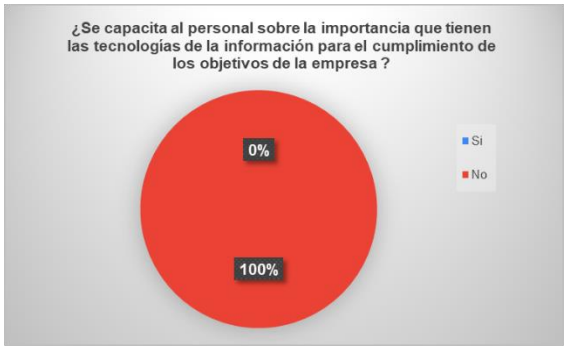
Fuente: *[19]*

Figura 5 Matriz de Riesgos

		Consecuencia				
		1. Leve	2.Menor	3. Moderado	4. Alto	5. Extremo
Probabilidad	E - Casi certero	M	M	A	E	E
	A - Probable	B	M	A	A	E
	M - Posible	B	M	M	A	A
	B - No muy común	B	B	M	M	A
	L - Raro	L	L	B	B	M

Fuente: *[19]*

Figura 6 Capacitación al personal sobre la importancia de las TI

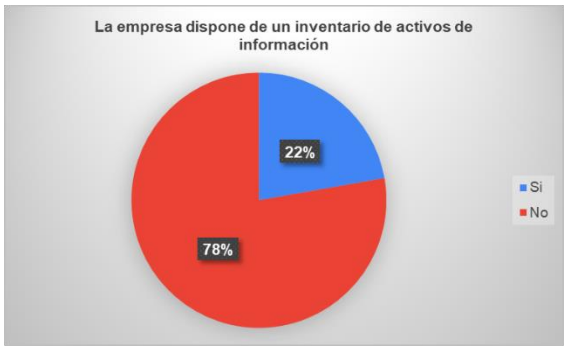


Fuente: encuesta aplicada por el autor

Figura 7 Identificación de los Activos de Información

Fuente: encuesta aplicada por el autor

Figura 8 Inventario de Activos de la Información.



Fuente: encuesta aplicada por el autor

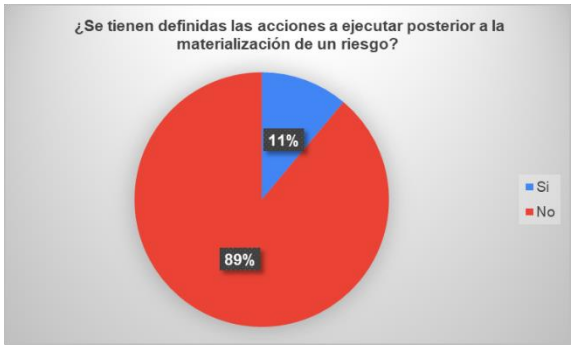
Figura 9 Procesos para la identificación de amenazas sobre los activos

Fuente: encuesta aplicada por el autor

Figura 10 Aplicación de una metodología para la gestión de riesgos.

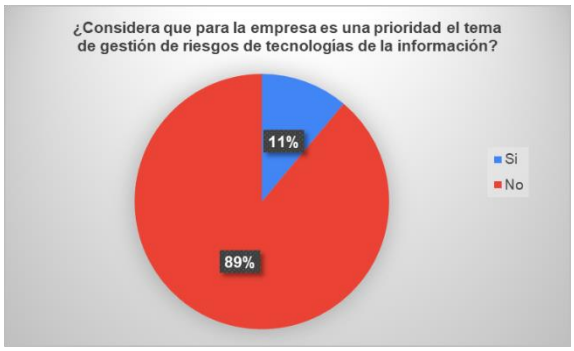
Fuente: encuesta aplicada por el autor

Figura 11 Acciones definidas ante la materialización de riesgos



Fuente: encuesta aplicada por el autor

Figura 12 Es prioridad o no para la empresa la gestión de riesgos de TI.



Fuente: encuesta aplicada por el autor

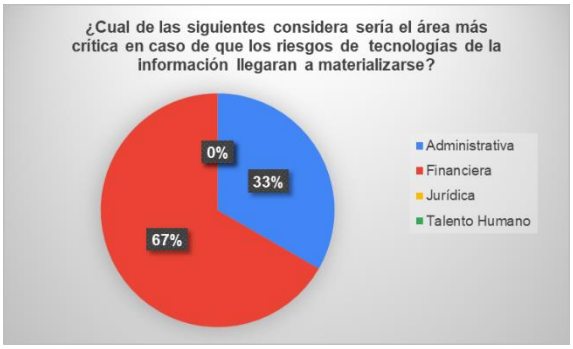
Figura 13 Razones.

Fuente: encuesta aplicada por el autor

Figura 14 Se tienen determinadas las áreas sensibles

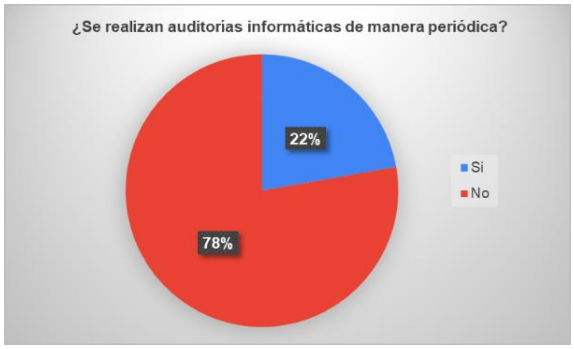
Fuente: encuesta aplicada por el autor

Figura 15 Área más crítica ante los riesgos



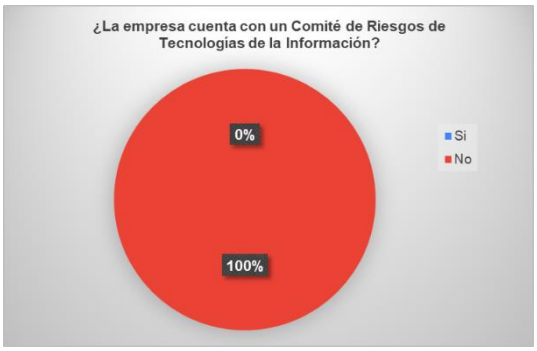
Fuente: encuesta aplicada por el autor

Figura 16 Se realizan auditorías informáticas.



Fuente: encuesta aplicada por el autor

Figura 17 Existe un Comité de Riesgos de TI.



Fuente: encuesta aplicada por el autor

Tabla 4 Valoración de las Fortalezas

Fortalezas	Peso relativo	Valoración	Peso Ponderado
Marca bien posicionada, genera réditos políticos	5%	2	0,10
Campañas públicas bien aceptadas	10%	4	0,40
Reducción de índices de accidentes	15%	5	0,75
Aceptación social al trabajo realizado	10%	4	0,40
Empoderamiento de las competencias	10%	4	0,40
Servicios destinados al bienestar social	20%	5	1,00
Equidad en el cumplimiento de las normas.	5%	4	0,20
Pioneros en asumir las competencias en movilidad, tránsito y transporte	10%	5	0,50
Recurso humano joven en su mayoría	10%	4	0,40
Liderazgo del nivel de gobierno y en nivel ejecutivo	5%	4	0,20
Total	**100%**		**4,35**

Fuente: [19] Elaborado por el autor

Tabla 5 Valoración de Debilidades

Debilidades	**Peso relativo**	**Valoración**	**Peso Ponderado**
Es considerada una empresa sancionadora	15%	5	0,75
Cartera vencida elevada por falta de cultura de pago	10%	5	0,50
Carencia de procesos formales	10%	4	0,40
Falta de aplicación de normas de calidad	10%	3	0,30
Gestión susceptible de cambios en la regulación	5%	3	0,15
Recurso humano desmotivado por la falta de capacitación y compromiso	10%	5	0,50
Sistemas informáticos desintegrados	15%	5	0,75
Falta de cultura organizacional en el servicio al cliente	10%	4	0,40
Falta de aplicativos informáticos	10%	4	0,40
Organigrama vertical obsoleto	5%	3	0,15
Total	**100%**		**4,30**

Fuente: [19] Elaborado por el autor

Tabla 6 Valoración de Oportunidades

Oportunidades	**Peso relativo**	**Valoración**	**Peso Ponderado**
Incremento del ingreso por uso de tecnologías	15%	5	0,75
Interacción con la comunidad que genera credibilidad y posibilidad de continuar en el proceso y potenciarlo	10%	3	0,30
Ciudadanos conscientes de que la movilidad mejora la calidad de vida	15%	5	0,75
Posibilidad de incremento de ingresos con mayor cobertura de servicios	15%	4	0,60
Poder determinar procesos al tener autonomía en la gestión	10%	3	0,30
Apoyo del alcalde a la gestión de la empresa	5%	3	0,15
Oferta tecnológica para la línea de negocio	10%	4	0,40
Apoyo interinstitucional de acuerdo a las necesidades	10%	3	0,30
Experiencia del alcalde en la gestión pública	5%	3	0,15
Oportunidades de reorganizar las estructuras	5%	4	0,20
Total	**100%**		**3,90**

Fuente: [19] Elaborado por el autor

Tabla 7 Valoración de Amenazas

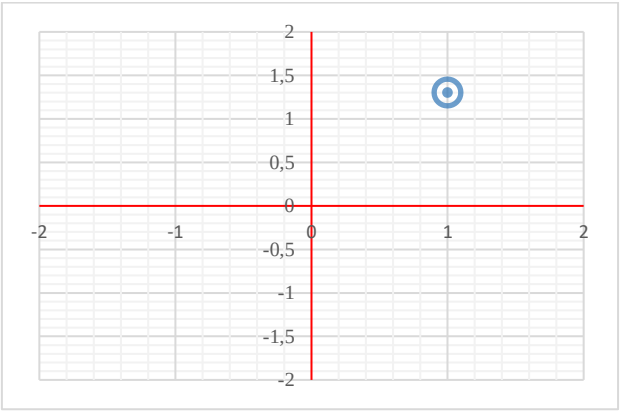
Amenazas	Peso relativo	Valoración	Peso Ponderado
El éxito de las campañas genera interés de otras instituciones de usufructuar el posicionamiento de la marca	10%	3	0,30
Las redes sociales generan un espacio inmediato de ataque a la gestión	15%	5	0,75
No hay fondos ni financiamiento para municipalizar el transporte	10%	3	0,30
La sociedad Cuencana requiere de un transporte administrativo y subvencionado por la Municipalidad y, no existe financiamiento	10%	3	0,30
Repudio ciudadano por control	10%	4	0,40
Confusión entre entidades nacionales y locales basadas en su mala reputación	15%	4	0,60
Retiro de la competencia por falta de cumplimiento	15%	4	0,60
Falta de modelos a seguir en procesos	5%	4	0,20
Falta de estándares de calidad	5%	3	0,15
Continuos cambios en la normativa	5%	3	0,15
Total	**100%**		**3,75**

Fuente: [19] Elaborado por el autor

Tabla 8 Valoración Balanza exógena y endógena

Valor Balanza exógena = ∑ Peso Ponderado Oportunidades - ∑ Peso Ponderado Amenazas	Valor Balanza endógena =∑ Peso Ponderado Fortalezas - ∑ Peso Ponderado Debilidades
Valoración Oportunidades = 4,60	Valoración Fortalezas = 4.55
Valoración Amenazas = 3.60	Valoración Debilidades = 3.45
Resultado = 1	Resultado = 1,10
PEEA = (X, Y)	
PEEA = (1;1,30)	

Figura 18 Matriz PEEA EMOV EP



Fuente: Elaborada por el autor

Tabla 10 Actividades proceso Subgerencia Financiera

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario	(RRHH)(SGF) (001)		
Jefe inmediato:	Gerencia General		
Cargo:	Subgerente Financiero		
Proceso:	Subgerencia Financiera		
Perfil	Funciones	R. Incomp.	Obs.
*Título profesional: Economista *Rol del Cargo: Gestión y control *Reporta a: Gerente General *Supervisa a: Tesorero, Contadora, Experto en Presupuestos, Experto Coactivas, Analista Cartera	*Planificar y controlar las actividades financieras que incluyen la Contabilidad, Análisis Financiero, Tesorería, Tributación, Financiamiento de proyectos y Presupuestos de la EMOV –EP *Desarrollar e Implementar procesos y procedimientos que estén direccionados a mejorar la recaudación diaria por concepto de parqueaderos Públicos, Multas, Sistema de parqueo Tarifado, Matriculación, certificaciones *Disponer y autorizar las diversas fases relativas a los procesos contables, presupuestarios, tributarios y de información a las entidades de control interno y externo en el área financiera, como Contraloría General del Estado, Ministerio de Finanzas, SRI. *Cumplir y hacer cumplir los procesos y procedimientos de gestión de la información para facilitar la auditoría de los organismos de control del sector público. *Elaborar y Controlar el Presupuesto Anual según la normativa del COTAD *Elaborar informes de gestión y cumplimiento en base a los procesos y proyectos financieros *Autorizar el otorgamiento de facilidades de pago a usuarios que lo requieran		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 11 Actividades proceso Subgerencia Financiera

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario	(RRHH)(SGF) (047)		
Jefe inmediato:	Subgerente Financiero		
Cargo:	Auxiliar 1 Financiero		
Proceso:	Subgerencia Financiera		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: Bachiller *Rol del Cargo: Servidor de Apoyo *Reporta a: Subgerente Financiero *Supervisa a: Ninguno	*Elaborar y despachar de forma oportuna por solicitud de la subgerencia financiera: oficios, memorandos, comunicados, circulares, para una adecuada ejecución del proceso solicitado por las diferentes áreas *Sistematizar y archivar la documentación que ingresa al área financiera *Recibir y organizar la documentación que sea asignada al departamento *Receptar facturar y demás comprobantes de venta para trámites de pago *Distribuir la documentación a las diferentes áreas previa disposición del Subgerente Financiero.		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 12 Actividades proceso Subgerencia Financiera

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (055)		
Jefe inmediato:	Subgerente Financiero		
Cargo:	Asistente Financiero		
Proceso:	Subgerencia Financiera		
Perfil	Funciones	R. Incom	Obs.
*Título profesional: Ingeniera *Rol del Cargo: Administrativo *Reporta a: Subgerente Financiero *Supervisa a: Auxiliar 1 Financiero	*Elaborar conciliaciones bancarias *Elaborar el flujo de caja de la programación financiera *Verificar los saldos de las cuentas de la empresa *Custodiar y mantener Actualizado el archivo de transferencias SPI *Generar contratos de espacios, custodiar pólizas y garantías recibidas		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 13 Actividades proceso Contabilidad

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (002)		
Jefe inmediato:	Subgerente Financiero		
Cargo:	Contadora		
Proceso:	CONTABILIDAD		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: Ingeniera Comercial *Rol del Cargo: Control y Coordinación de Procesos *Reporta a: Subgerencia Financiera *Supervisa a: Analistas de Contabilidad	*Aplicar los principios y normas técnicas de Contabilidad en base a las políticas y procedimientos establecidos en la norma de control Interno. *Realizar el control previo a la aceptación de una obligación, o al reconocimiento de un derecho, verificando que se cumpla con las Normas de Control Interno. *Organizar y actualizar el sistema contable y sugerir la adopción de medidas que se estimen necesarias en base a los principios y normas técnicas para una adecuada toma de decisiones *Registrar las operaciones oportunamente de los hechos económicos y presentación de Informes financiero *Conciliar los saldos de las cuentas contables para verificar la conformidad de la situación reflejada en los registros *Supervisar los procesos contables realizados por los auxiliares y las transferencias de depósito efectuadas desde los bancos acreditados para verificar su ejecución. *Entregar, registrar y controlar los anticipos de fondos destinados a cubrir gastos específicos *Ejecutar arqueos sorpresivos de los valores recaudados en efectivo al personal a su cargo *Desarrollar análisis y conformación de saldos con el fin de comprobar que los anticipos y cuentas por cobrar estén debidamente registrados *Efectuar la conciliación entre los registros del mayor auxiliar o general de los anticipos de fondos y las cuentas por cobrar		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 14 Actividades proceso Contabilidad

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (003) (RRHH)(SGF) (004)		
Jefe inmediato:	Contadora		
Cargo:	Analista de Contabilidad 1		
Proceso:	CONTABILIDAD		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: 1. Ingeniera en Contabilidad 2. Bachiller *Rol del Cargo: Coordinación a falta del jefe inmediato *Reporta a: Contadora *Supervisa a: Ninguno	*Recopilar información de facturas de proveedores y contratistas de la EMOV EP *Elaborar los comprobantes de obligaciones y pagos previo a las transferencias *Aplicar los Principios y Normas Técnicas de Contabilidad al momento de revisar la documentación *Efectuar retenciones, descuentos, contabilizar nómina *Preparar la información para la elaboración del Anexo Transaccional del SRI *Elaborar comprobantes de egresos a favor de acreedores *Confirmar a los proveedores las transferencias realizadas *Mantener actualizado el archivo de ingreso, egreso de la documentación respaldo *Realizar la reposición y liquidación de fondos de Cajas Chicas de las unidades administrativas *Contabilizar el pago de servicios básicos *Realizar demás funciones inherentes al cargo que le sean asignadas		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 15 Actividades proceso Contabilidad

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (005)		
Jefe inmediato:	Contadora		
Cargo:	Asistente de Contabilidad		
Proceso:	CONTABILIDAD		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: Bachiller *Rol del Cargo: Apoyo *Reporta a: Contadora *Supervisa a: ninguno	*Realizar la entrega y recepción de trámites provenientes de las diferentes dependencias *Elaborar comprobantes de pago y obligación por servicios básicos *Elaborar registro de comprobantes de Diarios *Contabilizar Notas de Crédito, Débito, y facturas por comisión de los bancos *Elaborar comprobantes de pago a Danton *Mantener el archivo del departamento actualizado		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 16 Actividades proceso Tesorería

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (006)		
Jefe inmediato:	Subgerente Financiero		
Cargo:	Tesorero		
Proceso:	TESORERIA		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: Magister *Rol del Cargo: Control y Coordinación de Procesos *Reporta a: Subgerencia Financiera *Supervisa a: Especialista de Tesorería	*Control previo al pago de transferencias, carga del archivo en su calidad del registrador al sistema SPI del BCE *Efectuar las gestiones y trámite de revisión, supervisión previa y ejecución de devolución de valores y bajas de cuentas por cobrar *Coordinar, controlar y supervisar las actividades y gestiones de cobranza y análisis con el departamento de cartera *Coordinar, controlar y supervisar las labores que realizan los auxiliares de recaudación *Control, custodia y entrega de Especies Valoradas *Reportes e informes que se envían a Contabilidad y a la Subgerencia Financiera *Cuadre y conciliación de cuentas con Contabilidad *Velar por la correcta ejecución de los Convenios de Recaudación que mantiene la EMOV EP a fin de que se cumplan de manera puntual conforme a las cláusulas y Normas de Control Interno *Otras actividades que disponga la Subgerente Financiera.		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 17 Actividades proceso Tesorería

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (007)		
Jefe inmediato:	Tesorero		
Cargo:	Especialista 1 Tesorería		
Proceso:	TESORERIA		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: Economista *Rol del Cargo: Ejecución de Procesos y apoyo Técnico *Reporta a: Tesorero *Supervisa a: Analista de Tesorería	*Revisar y verificar los ingresos recaudados en los diferentes puntos *Revisar constantemente el uso y destino de formularios, comprobantes y especies valoradas y notificar de manera inmediata cualquier anomalía *Conciliar y monitorear los ingresos recaudados en las diferentes formas de pago *Hacer inspecciones físicas a los puntos de recaudación y gestionar las medidas de seguridad pertinentes *Verificar y controlar el cumplimiento de las Leyes, Códigos y demás normativa tributaria *Mantener el stock de inventarios de especies valoradas, formularios y comprobantes de pago *Conciliar los saldos que muestra el sistema informático con los saldos de mayores contables *Analizar en conjunto con personal de cartera la morosidad de las cuentas por cobrar *Reportar a los auxiliares de recaudación diariamente sobre faltantes en cada turno *Presentar mensualmente reportes de faltantes de caja y especies valoradas *Realizar arqueos sorpresivos de caja *Verificar el cumplimiento de las Normas de Control Interno		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 18 Actividades proceso Tesorería

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (008)		
Jefe inmediato:	Tesorero		
Cargo:	Analista de Tesorería		
Proceso:	TESORERIA		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: CPA *Rol del Cargo: Técnico *Reporta a: Tesorero *Supervisa a: Recaudadores	*Verificar que los reportes de recaudación emitidos en los diferentes puntos coincidan con las guías enviadas al banco y el sistema interno para comprobar si los valores cuadran *Controlar la secuencia numérica de los comprobantes de pago y facturas emitidas en los puntos de recaudación *Contabilizar los registros de las citaciones de tránsito *Notificar e informar a cada recaudador sobre errores detectados en sus respectivos turnos *Contabilizar la recaudación en base a los depósitos realizados en las cuentas de la EMOV EP *Revisar la emisión de los comprobantes de ingresos de caja por diferentes conceptos y cuadrar con el número de facturas emitidas *Realizar reversos de infracciones en caso de que el recaudador justificadamente los solicite *Revisar y controlar los cobros realizados por la ANT		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 19 Actividades proceso Tesorería

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (009)		
Jefe inmediato:	Tesorero		
Cargo:	Asistente Administrativo de Tesorería		
Proceso:	TESORERIA		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: No requiere *Rol del Cargo: Apoyo *Reporta a: Tesorero *Supervisa a: Ninguno	*Apoyar en la entrega y recepción de trámites del departamento *Apoyar en la custodia de recursos económicos y financieros, especies valoradas y demás documentos *Verificar facturas y comprobantes antes de efectuar el pago para controlar que el pago sea el correcto *Registrar la recaudación de dinero por la venta de especies valoradas, certificados, multas e infracciones de Revisión Técnica Vehicular RTV *Realizar conciliaciones bancarias para verificar que los movimientos efectuados en las cuentas de la empresa sean los correctos *Mantener actualizada la documentación respecto de proformas, RTV, Mayancela, Capulispamba *Apoyar en la realización de arqueos de caja		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 20 Actividades proceso Tesorería

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (010)		
Jefe inmediato:	Tesorero		
Cargo:	Auxiliar 1 Tesorería		
Proceso:	TESORERIA		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: CPA *Rol del Cargo: Apoyo *Reporta a: Analista Financiero *Supervisa a: Ninguno	*Apoyar en los procesos de revisión y comprobación de los valores recaudados por la EMOV EP *Apoyar en las actividades de conciliaciones bancarias *Apoyar en el arqueo de especies valoradas en los puntos de recaudación *Verificar que los valores especificados en las actas de juzgamiento estén correctos *Apoyar en la elaboración de asientos contables de la recaudación *Elaborar reportes y conciliar información de cuadre por valores recaudados de la ANT		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 21 Actividades proceso Tesorería

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (011) (RRHH)(SGF) (057) (RRHH)(SGF) (058)		
Jefe inmediato:	Tesorero		
Cargo:	Auxiliar 2 Ventas		
Proceso:	TESORERIA		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: No requiere *Rol del Cargo: Servicio y Apoyo *Reporta a: Tesorero *Supervisa a: Ninguno	*Efectuar la distribución de tarjetas de parqueo SERT en cada uno de los puntos autorizados *Emitir el listado de compradores a recaudación para la emisión del correspondiente comprobante de pago *Coordinar con Tesorería los procesos de distribución y cobro de tarjetas adquiridas por nuestros clientes *Emitir informes diarios de las ventas y depósitos realizados por la venta de tarjetas parqueo SERT		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 22 Actividades proceso Tesorería

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	Desde (RRHH)(SGF) (012) Hasta (RRHH)(SGF) (045) Total 34		
Jefe inmediato:	Tesorero		
Cargo:	Auxiliar 1 Recaudación		
Proceso:	TESORERIA		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: No requiere *Rol del Cargo: Apoyo *Reporta a: Analista Tesorería *Supervisa a: Ninguno	*Efectuar la cobranza por uso de parqueadero, compra de tarjetas, multas, permisos, certificados y otro rubro que se determine por recaudo a los usuarios del servicio *Emitir la respectiva factura o comprobante de pago por la venta o utilización de algún servicio que presta la EMOV EP *Coordinar con Tesorería los procesos de recaudación personalizada a los clientes por ventas de tarjetas de parqueo *Conciliar caja antes de la finalización de la jornada laboral y entregar los reportes de valores recaudados a Tesorería para el respectivo registro *Elaborar informes y actas respectivas a Tesorería por los valores entregados o depositados en las entidades bancarias, para constancia del proceso efectuado *Informar oportunamente a la subgerencia financiera cuando las especies valoradas y comprobantes de pago estén en los stocks mínimos *Custodiar las especies valoradas a su cargo *Remitir los reportes de recaudación a la Analista de Tesorería debidamente firmados		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 23 Actividades proceso Cartera

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (046)		
Jefe inmediato:	Subgerente Financiero		
Cargo:	Analista de Cartera		
Proceso:	CARTERA		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: Economista *Rol del Cargo: Técnico *Reporta a: Subgerente Financiero *Supervisa a: Asistente Cartera	*Análisis y confirmación de saldos para determinar la morosidad, las gestiones de cobro realizadas, los derechos y la antigüedad del saldo de las cuentas *Informes de gestión de cobros de multas realizadas a los usuarios deudores. *Informes de cobros realizados mediante el sistema de persuasión. *Informes y Notificaciones de deudas de arriendos de locales del TTT y Terminales de Transferencia. *Análisis mensual de verificación de eficiencia en la recaudación de las cuentas vencidas. *Reporte de irregularidades en el saldo, para investigación y análisis para toma de las acciones correctivas y los ajustes pertinentes. *Informes de comprobación de la legalidad de los documentos de respaldo, que garanticen la integridad y existencia física.		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 24 Actividades proceso Cartera

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (048)		
Jefe inmediato:	Subgerente Financiero		
Cargo:	Asistente Administrativo Cartera		
Proceso:	CARTERA		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: En proceso *Rol del Cargo: Servicio y Apoyo *Reporta a: Subgerente Financiero *Supervisa a: Auxiliar de Cartera	*Coordinar y supervisar las funciones designadas al personal de cartera *Asesorar a usuarios sobre trámites y procesos correspondientes al cobro de cartera *Elaborar y emitir informes sobres resultados de la gestión de cobro de infracciones *Elaborar y emitir informes sobre valores recaudados por arriendos, multas *Elaborar y coordinar la entrega de notificaciones sobre arriendos a locales *Mantener el archivo de valores cobraros actualizado, realizar procesos de control y comprobación		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 25 Actividades proceso Cartera

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	Desde (RRHH)(SGF) (049) Hasta (RRHH)(SGF) (053) Total 5		
Jefe inmediato:	Subgerente Financiero		
Cargo:	Auxiliar 1 Cartera		
Proceso:	CARTERA		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: Bachiller *Rol del Cargo: Servicio y Apoyo *Reporta a: Asistente Administrativo Cartera *Supervisa a: Ninguno	*Realizar gestiones de cobranza a los infractores mediante la base de datos de la EMOV EP *Persuadir a los usuarios infractores mediante la ejecución de llamadas en base a técnicas de intervención que permitan recuperar valores por multas impuestas *Atender y asesoras a usuarios en procesos y trámites inherentes al área *Elaborar informes para dar a conocer novedades suscitadas y los avances en los procesos de gestión		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 26 Actividades proceso Presupuestos

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (056)		
Jefe inmediato:	Subgerente Financiero		
Cargo:	Experto en Presupuestos		
Proceso:	PRESUPUESTOS		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: Magister *Rol del Cargo: Ejecución y coordinación de procesos *Reporta a: Subgerente Financiero *Supervisa a: Auxiliar 1 Presupuestos	*Cumplir con las fases del ciclo presupuestario *Emitir certificaciones presupuestarias *Realizar el proceso de Control Previo al compromiso, elaboración, impresión y legalización del registro *Realizar reformas presupuestarias y traspasos *Realizar informes de cédulas y auxiliares presupuestarios *Realizar informes de estado de ejecución presupuestaria *Elaborar índices presupuestarios *Informar y controlar la evaluación en la ejecución del presupuesto por resultados *Informar sobre la ejecución detallada por proyectos		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 27 Actividades proceso Presupuestos

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (054)		
Jefe inmediato:	Experto en Presupuestos		
Cargo:	Auxiliar 1 Presupuestos		
Proceso:	PRESUPUESTOS		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: CPA *Rol del Cargo: Servicio y Apoyo *Reporta a: Experta en Presupuestos *Supervisa a: Ninguno	*Llevar el registro de trámites que entran y salen del departamento *Apoyar en la revisión de Certificaciones Presupuestarias *Apoyar en la ejecución de Registros de Compromiso y Reformas Presupuestarias *Mantener actualizado y custodiar el archivo con toda la documentación generada en el departamento		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 28 Actividades proceso Coactivas

Matriz de identificación de roles y actividades incompatibles			
Fecha:	25/08/2020		
Área:	FINANCIERA		
Funcionario:	(RRHH)(SGF) (059)		
Jefe inmediato:	Subgerente Financiero		
Cargo:	Juez de Coactivas		
Proceso:	COACTIVAS		
Perfil	Funciones	R.Incom.	Obs.
*Título profesional: Abogada *Rol del Cargo: Ejecución y Coordinación de Procesos *Reporta a: Subgerente Financiero *Supervisa a: Ninguno	*Ejercer la jurisdicción coactiva dentro del Cantón Cuenca a nombre de la EMOV EP *Sustanciar el proceso coactivo correspondiente de acuerdo a las competencias establecidas *Realizar procesos de evaluación a los aspectos procesales y administrativos en las acciones de juzgamiento coactivo *Mantener un inventario actualizado de los procesos coactivos que se lleven a cabo *Informar periódicamente a la Subgerencia Financiera y Gerencia General sobre los resultados obtenidos *Sugerir la toma de decisiones conducentes a mejorar y optimizar el ejercicio de la jurisdicción coactiva		
Elaborado por:	CPA. Fernanda Velecela		

Fuente: [27] [19] Elaborado por el autor

Tabla 29 Matriz identificación estilo organizacional aplicada a la Gerencia General

Matriz de identificación del estilo organizacional					
Cuestionamientos	1	2	3	4	5
¿La gerencia general tiene reclamos por parte de sus empleados?			x		
¿Los usuarios han reclamado por mala atención del personal?				x	
¿Los usuarios han reclamado por servicios deficientes?				x	
¿Los usuarios han reclamado por negligencia?			x		
¿Se han producido robos internos?			x		
¿La empresa ha sido víctima de actos fraudulentos?		x			
¿La empresa ha sido víctima de sabotajes de información?		x			
Los valores compartidos organizacionales son transmitidos (durante el año)				x	

Fuente: [19] Elaborado por el autor

Tabla 30 Matriz identificación estilo organizacional aplicada al Subgerente Financiero

Matriz de identificación del estilo organizacional aplicada al Área Financiera					
Cuestionamientos	1	2	3	4	5
¿La rotación del personal en el área es?			x		
¿Tiene dentro del área funcionarios con exceso de trabajo?				x	
¿Existen situaciones de controversia entre los funcionarios?				x	
¿El índice de reclamos por parte del usuario es?				x	
¿El número de empleados que trabaja horas adicionales es?	x				

Fuente: [19] Elaborado por el autor

Tabla 31 Inventario de Activos de Información - Edificaciones

Código Activo	Secuencial	Descripción	Ubicación
(ED)(CPD)	(001)	DATA CENTER	Matriz Misicata
(ED)(BDC)	(002)	BODEGA AREA FINANCIERA	Matriz Misicata

Fuente: [19] Elaborado por el autor

Tabla 32 Inventario Activos Información - Hardware

Cod.Activo	Secuencial	Tipo	Serie	Fecha adquisición	Proveedor
(HW)(LAPTOP)	(001)	BLD	1S0A33932R9Y980D	19/09/2012	CORESOLUTIONS SA.
(HW)(MULTI)	(001)	BLD	9BR535435	13/12/2017	OFFICE SOLUCIONES CIA LTDA
(HW)(MULTI)	(002)	BLD	LA2284976	15/12/2015	OFFICE SOLUCIONES CIA LTDA
(HW)(MULTI)	(003)	BLD	LA2284915	15/12/2015	OFFICE SOLUCIONES CIA LTDA
(HW)(MULTI)	(004)	BLD	LA2284920	15/12/2015	OFFICE SOLUCIONES CIA LTDA
(HW)(MULTI)	(005)	BLD	BA9410185	21/11/2012	OFFICE SOLUCIONES CIA LTDA
(HW)(PC)	(001)	BLD	V3KD579	16/11/2012	CORESOLUTIONS SA.
(HW)(PC)	(002)	BLD	V3KD733	16/11/2012	CORESOLUTIONS SA.
(HW)(PC)	(003)	BLD	V3KH183	16/11/2012	CORESOLUTIONS SA.
(HW)(PC)	(004)	BLD	MJTGGAPV	16/11/2012	CORESOLUTIONS SA.
(HW)(PC)	(005)	BLD	MJ74T1B	16/11/2012	OFICINA COMERCIAL RAYMOND WELLS CIA. LTDA
(HW)(PC)	(006)	BLD	V3KH213	16/11/2012	CORESOLUTIONS SA.
(HW)(PC)	(007)	BLD	MJ74T1L	24/07/2007	ALVARADO LOPEZ ANDREA VERONICA
(HW)(PC)	(008)	BLD	MJTGATC	16/11/2012	CORESOLUTIONS SA.
(HW)(PC)	(009)	BLD	1S3597AW6MJVWACV	16/11/2012	CORESOLUTIONS SA.
(HW)(PC)	(010)	BLD	V3KD746	16/11/2012	CORESOLUTIONS SA.
(HW)(PC)	(011)	BLD	MJVVANH	16/11/2012	CORESOLUTIONS SA.
(HW)(PC)	(012)	BLD	1S32642P7MJ909ND	14/05/2007	AVILA MERCHAN DIEGO GERARDO
(HW)(PC)	(013)	BLD	NO REGISTRA	14/05/2012	MERCHAN MONTESDEOCA RAUL ALFREDO
(HW)(PC)	(014)	BLD	MJRELHW	28/09/2012	CORESOLUTIONS SA.
(HW)(PC)	(015)	BLD	MJRELKD	28/09/2012	CORESOLUTIONS SA.
(HW)(PRINT)	(001)	BLD	9BR535950	13/12/2017	OFFICE SOLUCIONES CIA LTDA
(HW)(PRINT)	(002)	BLD	9BR536180	13/12/2017	OFFICE SOLUCIONES CIA LTDA
(HW)(PRINT)	(003)	BLD	NO REGISTRA	13/10/2010	REPYCOM CIA LTDA
(HW)(SCAN)	(001)	BLD	GW322743	23/12/2015	WANDA TECNOLOGIA CIA. LTDA.
(HW)(SCAN)	(002)	BLD	GW322783	23/12/2015	WANDA TECNOLOGIA CIA. LTDA.
(HW)(SVR)	(003)	BLD	06LRE81	19/07/2012	CORESOLUTIONS SA.

Fuente: [19] Elaborado por el autor

Tabla 33 Inventario Activos Información - Software

Cod.Activo	Secuencial	Descripción	Serie	Fecha creación	Proveedor
(SW)(PROPIO)	(001)	SISTEMA UNICO DE RECAUDACIÓN (SUR)		15/05/2015	PROPIO
(SW)(STD)(SRVMAIL)	(001)	cobranzas@emov.gob.ec			
(SW)(WEB)	(001)	www.emov.gob.ec			

Fuente: [19] Elaborado por el autor

Tabla 34 Inventario Activos Información - Información Electrónica

Cod.Activo	Secuencial	Tipo de Archivo	Descripción	Fecha creación	Fecha última modificación	Ubicación
(IE)(DATA)	(001)	Hoja de cálculo de Microsoft Excel (.xlsx)	REPORTE DE VALORES COBRADOS Y PENDIENTES	01/12/2017	01/09/2020	(HW)(PC) (001)
(IE)(DATA)	(002)	Hoja de cálculo de Microsoft Excel (.xlsx)	BASE DE DATOS DE USUARIOS	01/01/2020	01/09/2020	(HW)(PC) (009)

Fuente: [19] Elaborado por el autor

Tabla 35 Inventario Activos Información - Información en Papel

Cod.Activo	Secuencial	Descripción	Funcionario a cargo	Ubicación
(IP)(DOCUMENTOS)	(001)	BOLETAS DE CITACIONES DE TRÁNSITO	(RRHH)(UI) (046)	BODEGA AREA FINANCIERA
(IP)(DOCUMENTOS)	(002)	ESPECIES VALORADAS	(RRHH)(UI) (006)	OFICINA RECAUDACIÓN MATRIZ
(IP)(DOCUMENTOS)	(003)	REPORTE DE CIERRE DE TURNOS	(RRHH)(UI) (012) al (RRHH)(UI) (016)	BODEGA AREA FINANCIERA
(IP)(DOCUMENTOS)	(004)	CERTIFICACIONES PRESUPUESTARIAS - REGISTROS DE COMPROMISO	(RRHH)(UI) (054)	BODEGA AREA FINANCIERA
(IP)(DOCUMENTOS)	(005)	COMPROBANTES DE RETENCIÓN, OBLIGACIÓN Y PAGO	(RRHH)(UI) (002)	BODEGA AREA FINANCIERA

Fuente: [19] Elaborado por el autor

Tabla 36 Inventario Activos información-Medios de almacenamiento extraíble

Cod.Activo	Secuencial	Tipo	Capacidad	Marca	Serie	Fecha adquisición	Proveedor
(EXTRAIBLE)(DISCO)	(001)	BLD	1TB	TOSHIBA	45BATPEYT19B	28/12/2015	GUEVARA CORDOVA JORGE OSWALDO

Fuente: [19] Elaborado por el autor

Tabla 37 Activos información Infraestructura de comunicaciones

Cod.Activo	Secuencial	Tipo	Nombre	Marca	Fecha adquisición	Proveedor
(IC)(ROUTER)	(001)	BLD	ROUTER	CISCO	20/09/2013	COMUNICACIONES DEL AUSTRO AUTELCOM S.A.

Fuente: [19] Elaborado por el autor

Tabla 38 Inventario Activos Información - Recursos Humanos

Cod.Activo	Secuencial	Cargo	Género	Fecha ingreso	Fecha salida
(RRHH)(UI)	(001)	SUBGERENTE FINANCIERO	M	15/02/2020	N/A
(RRHH)(UI)	(002)	CONTADORA	F	01/01/2010	N/A
(RRHH)(UI)	(003)	ANALISTA DE CONTABILIDAD 1	F	18/12/2015	N/A
(RRHH)(UI)	(004)	ANALISTA DE CONTABILIDAD 1	F	10/04/2012	N/A
(RRHH)(UI)	(005)	ASISTENTE DE CONTABILIDAD	F	03/09/2010	N/A
(RRHH)(UI)	(006)	TESORERO	F	01/09/2020	N/A
(RRHH)(UI)	(012)	AUXILIAR 1 RECAUDACIÒN	F	15/04/2017	N/A
(RRHH)(UI)	(013)	AUXILIAR 1 RECAUDACIÒN	F	15/04/2017	N/A
(RRHH)(UI)	(014)	AUXILIAR 1 RECAUDACIÒN	F	15/04/2017	N/A
(RRHH)(UI)	(015)	AUXILIAR 1 RECAUDACIÒN	F	18/05/2018	N/A
(RRHH)(UI)	(016)	AUXILIAR 1 RECAUDACIÒN	F	07/08/2015	N/A
(RRHH)(UI)	(046)	ANALISTA DE CARTERA	F	01/01/2014	N/A
(RRHH)(UI)	(049)	AUXILIAR 1 CARTERA	F	01/03/2019	N/A
(RRHH)(UI)	(050)	AUXILIAR 1 CARTERA	F	01/01/2010	N/A
(RRHH)(UI)	(051)	AUXILIAR 1 CARTERA	F	01/03/2019	N/A
(RRHH)(UI)	(054)	AUXILIAR 1 PRESUPUESTOS	F	02/03/2014	N/A
(RRHH)(UI)	(056)	EXPERTO EN PRESUPUESTOS	F	03/06/2010	N/A
(RRHH)(UI)	(059)	ABOGADO DE COACTIVAS	F	01/01/2017	N/A

Fuente: [19] Elaborado por el autor

Tabla 39 Valoración de activos de información del proceso Cartera

SUBPROCESO	ACTIVIDADES	ACTIVO	DESCRIPCIÓN	D	I	C	TOTAL	VALOR
INGRESO DE BOLETAS DE CITACIÓN POR INFRACCIONES DE TRÁNSITO	1. Analista de Cartera: Receptar las boletas de citación de tránsito, de forma física y digital, del Área de Estadísticas de Control de Tránsito 2. Distribuir las citaciones a los auxiliares de cartera 3. Auxiliar de Cartera. - Validar el contenido de la citación - Si es efectiva: pasa a la actividad 4 -Si es inconsistente: pasa a la actividad 5 4. Registrar la citación de tránsito efectiva - Pasa a la actividad 6 5. Registrar la citación de tránsito como inconsistente - Pasa a la actividad 6 6. Analista de Cartera. - Generar el reporte diario 7. Realizar el análisis, control y seguimiento. En caso de detectarse un ingreso erróneo de la citación por parte del Auxiliar Cartera: - Pasa a la actividad 8 - De lo contrario pasa a la actividad 9 8. Solicitar autorización a tesorería de la corrección o cambio a realizar Modificar la información de la citación - Pasa a la actividad 9 9. Remitir el listado de citaciones inconsistentes al Área de Estadísticas de Control de Tránsito. 10. Emitir informe para la Subgerencia Financiera con copia a Tesorería 11. Archivar documentación	(ED)(CPD) (001)	DATA CENTER MISICATA	4	0	0	4	ALTO
		(ED)(BDC) (002)	BODEGA ARERA FINANCIERA	4	0	0	4	ALTO
		(HW)(PC) (001)-(002)-(003)	COMPUTADOR DE ESCRITORIO LENOVO	3	2	0	3	MODERADO
		(HW)(PRINT) (001)-(002)	IMPRESORA LÁSER MARCA XEROX MODELO PHASER 3330	2	1	0	2	MENOR
		(HW)(MULTI) (001)	IMPRESORA MULTIFUNCION MARCA XEROX PHASER 3330	2	1	0	2	MENOR
		(HW)(SCAN) (001)	SCANNER CANON DRC225	3	1	0	3	MODERADO
		(SW)(PROPIO) (001)	SISTEMA UNICO DE RECAUDACIÓN (SUR)	5	5	4	5	EXTREMO
		(IP)(DOCUMENTOS) (001)	BOLETAS DE CITACIONES DE TRÁNSITO	4	4	2	4	ALTO
		(RRHH)(UI) (046)-(049)-(050)- (051)	PERSONAL CARTERA	3	0	0	3	MODERADO

Fuente: [19] Elaborado por el autor

Tabla 40 Valoración de activos de información del proceso Tesorería

SUBPROCESO	ACTIVIDADES	ACTIVO	DESCRIPCIÓN	D	I	C	TOTAL	VALOR
RECAUDACIÓN DE VALORES EN LOS PUNTOS: WINCHAJE, TERMINAL TERRESTRE, MISICATA	1. Verificar que el punto de establecimiento asignado sea el correcto 2. Abrir el turno en el sistema informático 3. Verificar en los sistemas disponibles los valores que el usuario vaya a pagar -SI el usuario está conforme, pasa a la actividad 4 -NO está conforme el usuario, fin del proceso 4. Emitir el componte de pago por los valores cobrados 5. Seleccionar la forma de pago que notifique el usuario 6. En caso de emitir un comprobante de forma incorrecta, emitir una Nota de Crédito 7. En caso de que se requiera una Nota de Crédito fuera del turno -Solicitar a la analista de tesorería para que proceda con la emisión de la NC 8. Si el usuario requiere el reverso de una Especie Valorada -Solicitar a la analista de tesorería el reverso siempre y cuando la especie no haya sido utilizada 9. Realizar el cierre del turno una vez finalice la jornada laboral 10. Conciliar el reporte del turno con los valores recaudados 11. Llenar la papeleta de depósito y guía de blindado y enviar con el valor íntegro recaudado 12. Preparar la funda a enviar mediante el servicio de blindado. 13. Enviar los reportes de recaudación a tesorería	(ED)(CPD) (001)	DATA CENTER MISICATA	4	0	0	4	ALTO
		(HW)(SVR) (001)	SERVIDOR IBM HC22	4	3	1	4	ALTO
		(HW)(PC) (004)-(005)-(006)-(007)-(008)	COMPUTADOR DE ESCRITORIO LENOVO	3	2	0	3	MODERADO
		(HW)(MULTI) (002)-(003)-(004)	IMPRESORA MULTIFUNCION MARCA XEROX MODELO PHASER 3320	2	1	0	2	MENOR
		(SW)(PROPIO) (001)	SISTEMA UNICO DE RECAUDACIÓN (SUR)	5	5	4	5	EXTREMO
		(SW)(WEB) (001)	www.emov.gob.ec	4	3	1	4	ALTO
		(IP)(DOCUMENTOS) (002)	CERTIFICADOS NO ADEUDAR	3	3	1	3	MODERADO
		(IP)(DOCUMENTOS) (003)	REPORTE DE CIERRE DE TURNOS	3	2	1	3	MODERADO
		(RRHH)(UI) (006)-(012)-(013)-(014)-(015)-(016)	PERSONAL TESORERÍA	4	0	0	4	ALTO

Fuente: [19] Elaborado por el autor

Tabla 41 Valoración de activos de información del proceso Coactivas

SUBPROCESO	ACTIVIDADES	ACTIVO	DESCRIPCIÓN	D	I	C	TOTAL	VALOR
RECUPERACIÓN DE CARTERA A TRAVÉS DEL COBRO COACTIVO	1. Analista de Cartera: emitir el informe de deudores que se niegan a pagar previa gestión de cobro persuasivo, presenta a la Subgerencia Financiera 2. Subgerente Financiero: Revisar el listado de deudores, valores e infracciones 3. Dar paso al Abogado de coactivas y Tesorero para que se inicie el proceso de cobro coactivo. 4. Tesorero: Emitir los títulos de crédito, 5. Notificar de manera escrita a cada deudor que forme parte del proceso - SI el deudor realiza el pago dentro del plazo establecido, el trámite coactivo finaliza , pasa a la actividad 7 -NO realiza el pago, se hace constar en un archivo para informar nuevamente a la subgerencia financiera 6. Informar mensualmente a la subgerencia financiera los resultados del proceso coactivo	(HW)(PC) (009)	COMPUTADOR DE ESCRITORIO LENOVO	3	2	0	3	MODERADO
		(HW)(SCAN) (002)	SCANNER CANON DRC225	3	1	0	3	MODERADO
		(SW)(PROPIO) (001)	SISTEMA UNICO DE RECAUDACIÓN (SUR)	5	5	4	5	EXTREMO
		(SW)(STD)(SRVMAIL) (001)	@emov.gob.ec	4	3	3	4	ALTO
		(IE)(DATA) (001)	REPORTE DE VALORES COBRADOS Y PENDIENTES	3	3	4	4	ALTO
		(IE)(DATA) (002)	BASE DE DATOS DE USUARIOS	4	3	4	4	ALTO
		(RRHH)(UI) (046)	PERSONAL CARTERA	3	0	0	3	MODERADO
		(RRHH)(UI) (059)	PERSONAL COACTIVAS	3	0	0	3	MODERADO

Fuente: [19] Elaborado por el autor

Tabla 42 Valoración de activos de información del proceso Subgerencia Financiera

SUBPROCESO	ACTIVIDADES	ACTIVO	DESCRIPCIÓN	D	I	C	TOTAL	VALOR
OTORGA-MIENTO DE FACILIDA-DES DE PAGO	1. Analista de cartera: solicitar y receptar la información al usuario que desee acceder a la concesión de Facilidad de Pago 2. Revisar multas y verifica capacidad de pago -SI tiene capacidad de pago, pasa a la actividad 3 3. Remitir al peticionario el Formulario de Solicitud y los datos para el depósito inicial 4. Verificar la documentación -SI está completo, pasa a la actividad 5 -NO está completo, Remitir trámite al usuario para que complete lo que haga falta 5. Entregar a la subgerencia financiera la información para revisión correspondiente -SI se considera factible pasa a la actividad 6 -NO se considera factible se notifica al usuario el fin del proceso 6. Subgerente Financiero: Generar la Resolución, tabla de amortización y pagaré 7. Autorizar y suscribir la resolución de otorgamiento de facilidades de pago 8. Autorizar la habilitación al usuario para que pueda realizar cualquier trámite 9. Remitir y notificar a Secretaría General, Tesorería, Contabilidad y TIC´s	(HW)(LAPTOP) (001)	COMPUTADORA PORTATIL LENOVO	3	2	0	3	MODERADO
		(HW)(PRINT) (003)	IMPRESORA LÁSER HP MODELO P2055	2	1	0	2	MENOR
		(SW)(PROPIO) (001)	SISTEMA UNICO DE RECAUDACIÓN (SUR)	5	5	4	5	EXTREMO
		(RRHH)(UI) (001)	PERSONAL SUBGERENCIA FINANCIERA	3	0	0	3	MODERADO

Fuente: [19] Elaborado por el autor

Tabla 43 Valoración de activos de información del proceso Presupuestos

SUBPROCESO	ACTIVIDADES	ACTIVO	DESCRIPCIÓN	D	I	C	TOTAL	VALOR
EMISIÓN DE REGISTRO DE COMPROMISO PREVIO AL PAGO	1. Auxiliar de Presupuestos: Recibir y registrar el ingreso del trámite al departamento. 2. Verificar que el trámite incluya la documentación necesaria y le entregar el trámite al Experto en Presupuestos 3. Experto en Presupuestos: verificar que el valor a ser pagado cuente con una certificación presupuestaria previamente emitida. - SI hay certificación presupuestaria, pasa a la actividad 4 -NO hay certificación previa, el trámite es devuelto al área requirente 4. Comprobar que la certificación presupuestaria tenga saldo disponible -SI tiene saldo, pasa a la actividad 5 -NO tiene saldo, el trámite es devuelto al área requirente 5. Realizar control previo y se emitir el Registro de Compromiso 6. Auxiliar de Presupuestos: Entregar el trámite al subgerente financiero para que lo legalice 7. Entregar el trámite a Contabilidad para el pago	(HW)(PC) (010)-(011)	COMPUTADOR DE ESCRITORIO LENOVO	3	2	0	3	MODERADO
		(IP)(DOCUMENTOS) (004)	CERTIFICACIONES PRESUPUESTARIAS - REGISTROS DE COMPROMISO	3	2	1	3	MODERADO
		(RRHH)(UI) (054)-(056)	PERSONAL PRESUPUESTOS	3	0	0	3	MODERADO

Fuente: [19] Elaborado por el autor

Tabla 44 Valoración de activos de información del proceso Contabilidad

SUBPROCESO	ACTIVIDADES	ACTIVO	DESCRIPCIÓN	D	I	C	TOTAL	VALOR
PAGO A PROVEEDORES	1. Asistente de Contabilidad: Recibir y registrar los trámites previos a entregarle a la Contadora 2. Contadora: Revisar que los trámites que tiene en documento físico, le hayan sido enviados por Quipux 3. Distribuir los trámites a las Analistas de Contabilidad 4. Analistas de Contabilidad: realizar el proceso de control previo al pago -SI la documentación está completa, pasa a la actividad 5 -NO está completa la documentación, el trámite es devuelto al área requirente 5. Emitir comprobantes de retención, comprobantes de obligación y comprobantes de pago 6. Contadora: Validar y aprobar las actividades del paso 5 7. Reasignar los trámites a Tesorería para proceder con la carga de la transferencia	(HW)(PC) (012)-(013)-(014)-(015)	COMPUTADOR DE ESCRITORIO LENOVO	3	2	0	3	MODERADO
		(HW)(MULTI) (005)	IMPRESORA MULTIFUNCION XEROX MODELO PHASER3635	2	1	0	2	MENOR
		(IP)(DOCUMENTOS) (005)	COMPROBANTES DE RETENCIÓN, OBLIGACIÓN Y PAGO	4	4	2	4	ALTO
		(EXTRAIBLE)(DISCO) (001)	DISCO DURO EXTERNO	2	0	0	2	MENOR
		(IC)(ROUTER)	ROUTER CISCO	3	3	2	3	MODERADO
		(RRHH)(UI) (002)-(003)-(004)-(005)	PERSONAL CONTABILIDAD	3	0	0	3	MODERADO

Fuente: [19] Elaborado por el autor

Tabla 45 Matriz de identificación de Amenazas

Problema	Código amenaza	Nombre	Frec	Descripción	Dimensión	Activos afectados
Espacio físico vulnerable a ataques	[PROVOCADO.1]	Desastres provocados	1	Acceso de personal no autorizado	Disponibilidad (D)	(ED) Edificaciones
Bodega ubicada en el mismo espacio para las demás bodegas	[PROVOCADO.1]	Desastres provocados	1	Acceso de personal no autorizado	Disponibilidad (D)	(ED) Edificaciones
Sobre carga del disco duro del servidor	[NO_INTENCIONADO.2]	Errores del administrador	3	Errores en la operación del servidor de matriz	Disponibilidad (D) Integridad (I) Confidencialidad (C)	(HW) Hardware
Equipos expuestos a sustancias liquidas	[PROVOCADO.2]	Desastres provocados	3	Inadecuado uso de computadoras	Disponibilidad (D)	(HW) Hardware
Errores en la impresión de documentos	[NO_INTENCIONADO.1]	Errores de los usuarios	4	Uso excesivo de equipos	Disponibilidad (D)	(HW) Hardware
Fallas en el escaneo de documentos	[NO_INTENCIONADO.2]	Errores del administrador	2	Errores de instalación de los equipos	Disponibilidad (D) Integridad (I) Confidencialidad (C)	(HW) Hardware (IE) Información electrónica (IP) Información en papel
Caída del sistema (SUR)	[NO_INTENCIONADO.2]	Errores del administrador	5	Funcionamiento incorrecto del módulo de recaudación	Disponibilidad (D) Integridad (I) Confidencialidad (C)	(SW) Software (IE) Información electrónica (IP) Información en papel
	[EL.1]	Difusión de software dañino	3	Propagación inocente de virus	Disponibilidad (D) Integridad (I) Confidencialidad (C)	(SW) Software (IE) Información electrónica
Reportes de valores cobrados incorrectos	[NO_INTENCIONADO.3]	Errores de monitorización	3	Registro incompleto de actividades	Integridad (I)	(IE) Información electrónica (IP) Información en papel
Base de datos de usuarios incompleta	[NO_INTENCIONADO.3]	Errores de monitorización	3	Inadecuado registro de actividades	Integridad (I)	(IE) Información electrónica (IP) Información en papel
Filtro de información de usuarios	[EL.2]	Copia no controlada de información	2	Información sensible de usuarios expuesta	Confidencialidad (C)	(SW) Software (IE) Información electrónica
Inadecuado tratamiento de la documentación respaldo	[NO_INTENCIONADO.7]	Destrucción de información	4	Pérdida accidental de información	Disponibilidad (D)	(IE) Información electrónica (IP) Información en papel

Uso indebido de especies valoradas	[NO_INTENCIOADO.1]	Errores de los usuarios	3	Negligencia en la entrega de especies valoradas	Disponibilidad (D) Integridad (I) Confidencialidad (C)	(IE) Información electrónica (IP) Información en papel
Extravío de reportes de cierre de turno	[NO_INTENCIONADO.5]	Deficiencias en la organización	2	Desconocimiento de funciones y roles de cargo	Disponibilidad (D)	(P) Personal
Errores en operaciones de recaudación e ingreso de infracciones	[NO_INTENCIONADO.5]	Deficiencias en la organización	4	Falta de comunicación de procesos de cobro e ingreso de infracciones	Disponibilidad (D)	(P) Personal
Retraso en procesos de pago a proveedores, concesión de facilidades pago, emisión de certificaciones presupuestarias	[NO_INTENCIONADO.5]	Deficiencias en la organización	3	Exceso de carga laboral	Disponibilidad (D)	(P) Personal
Caída del correo institucional	[EL.1]	Difusión de software dañino	2	Ataques mediante difusión de correos maliciosos	Disponibilidad (D) Integridad (I) Confidencialidad (C)	(SW) Software (IE) Información electrónica
Ataques a la página web	[EL.1]	Difusión de software dañino	2	Denegación de servicio	Disponibilidad (D) Integridad (I) Confidencialidad (C)	(SW) Software (IE) Información electrónica
Disco duro deja de funcionar a causa de un corto circuito	[PROVOCADO.3]	Desastres provocados	2	Corto circuito	Disponibilidad (D)	(EXTRAIBLE) Medios de almacenamiento extraíble
Fallas en el funcionamiento del router	[NO_INTENCIONADO.2]	Errores del administrador	2	Falta de mantenimiento de red de infraestructuras	Disponibilidad (D) Integridad (I) Confidencialidad (C)	(IC) Infraestructura de comunicaciones

Fuente: [19] Elaborado por el autor

Tabla 46 Matriz de análisis de riesgos y controles

Problema	Análisis	Control Actual
Espacio físico de DataCenter vulnerable a ataques	El data center está ubicado en la planta baja en las dependencias de la oficina matriz, junto a oficinas de libre acceso por usuarios internos y externos	Puerta de acceso blindada, se dispone de un sistema de alarma
Bodega ubicada en el mismo espacio para las demás bodegas	El espacio en el que se ubica la bodega del financiero es compartido con las bodegas de los demás departamentos, los archivos están susceptibles a ser tomados deliberadamente.	Se dispone de un sistema de alarma
Sobre carga del disco duro del servidor	La cantidad de datos que soporta el servidor es extremadamente grande y en ocasiones excede la capacidad máxima.	Se cuenta con un sistema de notificación que alerta cuando el disco duro se ha saturado.
Equipos expuestos a sustancias liquidas	Los usuarios exponen los equipos a sustancias líquidas que tienen en su escritorio, como café, agua etc.	No existe
Errores en la impresión de documentos	Los equipos de impresión son utilizados jornadas completas por varios usuarios internos, ante la cantidad de usuarios externos que requieren la solución de trámites. Llega un punto en el que las impresoras dejan de funcionar y se detienen.	Mantenimiento bimensual de equipos
Fallas en el escaneo de documentos	Las fallas son generalmente producidas por uso inadecuado de los escáneres, una hoja mal colocada, doblada, hojas grapadas.	Política de seguridad de la información, numeral 5.1 Disposiciones generales
Caída del sistema (SUR)	Generalmente se produce cuando se intenta sacar reportes que contiene gran cantidad de datos.	No existe
	Algunos equipos tienen acceso libre plataformas como: YouTube, Facebook entre otras	Sistema de antivirus implementado en la mayor parte de equipos
Reportes de valores cobrados incorrectos	Valores reportados no exactos ni confiables	Monitorización frecuente de actividades.
Base de datos de usuarios incompleta	Varios usuarios internos tienen acceso a modificar o actualizar la base de datos, al momento de pretender unificarla la información, ésta no coincide	Monitorización frecuente de actividades.
Filtro de información de usuarios	Los datos de usuarios están expuestos a ser copiados libremente.	No existe
Inadecuado tratamiento de la documentación respaldo	Descuido en el tratamiento de boletas físicas de citaciones de tránsito, registros de compromiso, comprobantes de pago	No existe
Uso indebido de especies valoradas	Asignación de especies valoradas por solicitud de los puntos de recaudación sin llevar un control de stock	No existe
Extravío de reportes de cierre de turno	Personal no hace llegar el respaldo de valores recaudados	No existe
Errores en operaciones de recaudación e ingreso de infracciones	Existen casos de cobros indebidos de valores, ingresos incorrectos de infracciones, entre otros	Ninguno, es de conocimiento del área financiera cuando el usuario externo hace el reclamo

Retraso en procesos de pago a proveedores	Los trámites de pago llegan generalmente los últimos días del mes, por lo que la acumulación de estos genera demoras en el proceso	No existe
Caída del correo institucional	Correos electrónicos masivos que invitan a actualizar datos de los usuarios.	Soporte al servidor de correo electrónico
Ataques a la página web	Vulnerabilidades de la página web fácilmente detectables	Se monitorea la página web institucional generalmente cada 15 días
Disco duro deja de funcionar a causa de un corto circuito	Soporte de almacenamiento de datos de disco duro insuficiente	No existe
Fallas en el funcionamiento del router	No se realizan mantenimientos frecuentes a los rúters	Mantenimiento mensual de la red de infraestructura

Fuente: [19] Elaborado por el autor

Tabla 47 Matriz de registro y cálculo de riesgos de los procesos del área financiera

PROCESO			VALOR				IMPACTO				RIESGO ACUMLADO			RIESGO ABSOLUTO
	ACTIVO	DESCRIPCIÓN	D	I	C	TOTAL	F	D	I	C	D	I	C	
CARTERA	(ED)(CPD) (001)	DATA CENTER MISICATA	4	0	0	4								
	[PROVOCADO.1]	Acceso de personal no autorizado	D				1	4			4	0	0	4
	(ED)(BDC) (002)	BODEGA AREA FINANCIERA	4	0	0	4								
	[PROVOCADO.1]	Acceso de personal no autorizado	D				1	3			3	0	0	4
	(HW)(PC) (001)-(002)-(003)	COMPUTADOR DE ESCRITORIO LENOVO	3	2	0	3								
	[PROVOCADO.2]	Inadecuado uso de computadoras	D	I			3	3	2		9	6	0	9
	(HW)(PRINT) (001)-(002)	IMPRESORA LÁSER MARCA XEROX MODELO PHASER	2	1	0	2								
	[NO_INTENCIONADO.1]	Uso excesivo de equipos	D	I			4	2	1		8	4	0	8
	(HW)(MULTI) (001)	IMPRESORA MULTIFUNCION MARCA XEROX PHASER	2	1	0	2								
	[NO_INTENCIONADO.1]	Uso excesivo de equipos	D	I			4	2	1		8	4	0	8
	(HW)(SCAN) (001)	SCANNER CANON DRC225	3	1	0	3								
	[NO_INTENCIONADO.2]	Errores de instalación de los equipos	D	I			2	3	1		6	2	0	6
	(SW)(PROPIO) (001)	SISTEMA UNICO DE RECAUDACIÓN (SUR)	5	5	4	5								
	[NO_INTENCIONADO.2]	Funcionamiento incorrecto del módulo de recaudación	D	I	C		5	4	4	3	20	20	15	25
	[EL.1]	Propagación inocente de virus	D	I	C		3	4	4	3	12	12	9	15
	(IP)(DOCUMENTOS) (001)	BOLETAS DE CITACIONES DE TRÁNSITO	4	4	2	4								
	[NO_INTENCIONADO.7]	Pérdida accidental de información	D				4	4			16	0	0	16
	(RRHH)(UI) (046)-(049)-(050)-(051)	PERSONAL CARTERA	3	0	0	3								
	[NO_INTENCIONADO.5]	Falta de comunicación de procesos de ingreso de infracciones	D				4	4			16	0	0	12
TESORERÍA	(ED)(CPD) (001)	DATA CENTER MISICATA	4	0	0	4								
	[PROVOCADO.1]	Acceso de personal no autorizado	D				1	4			4	0	0	4
	(HW)(SVR) (001)	SERVIDOR IBM HC22	4	3	1	4								
	[NO_INTENCIONADO.2]	Errores en la operación del servidor de matriz	D	I	C		3	4	4	2	12	12	6	12
	(HW)(PC) (004)-(005)-(006)-(007)-(008)	COMPUTADOR DE ESCRITORIO LENOVO	3	2	0	3								
	[PROVOCADO.2]	Inadecuado uso de computadoras	D	I			3	3	2		9	6	0	9
	(HW)(MULTI) (002)-(003)-(004)	IMPRESORA MULTIFUNCION MARCA XEROX MODELO PHASER	2	1	0	2								
	[NO_INTENCIONADO.1]	Uso excesivo de equipos	D	I			4	2	1		8	4	0	8
	(SW)(PROPIO) (001)	SISTEMA UNICO DE RECAUDACIÓN (SUR)	5	5	4	5								
	[NO_INTENCIONADO.2]	Funcionamiento incorrecto del módulo de recaudación	D	I	C		5	4	4	3	20	20	15	25
	[EL.1]	Propagación inocente de virus	D	I	C		3	4	4	3	12	12	9	15
	(SW)(WEB) (001)	www.emov.gob.ec	4	3	1	4								
	[EL.1]	Denegación de servicio	D	I	C		2	4	2	2	8	4	4	8
	(IP)(DOCUMENTOS) (002)	CERTIFICADOS NO ADEUDAR	3	3	1	3								
	[NO_INTENCIONADO.1]	Negligencia en la entrega de especies valoradas	D	I	C		3	3	1	1	9	3	3	9
	(IP)(DOCUMENTOS) (003)	REPORTE DE CIERRE DE TURNOS	3	2	1	3								
	[NO_INTENCIONADO.5]	Desconocimiento de funciones y roles de cargo	D				2	3			6	0	0	6
	(RRHH)(UI) (006)-(012)-(013)-(014)-(015)-(016)	PERSONAL TESORERÍA	4	0	0	4								
	[NO_INTENCIONADO.5]	Falta de comunicación de procesos de cobro	D				4	4			16	0	0	16

PROCESO			VALOR				IMPACTO				RIESGO ACUMLADO			RIESGO ABSOLUTO
	ACTIVO	DESCRIPCIÓN	D	I	C	TOTAL	F	D	I	C	D	I	C	
COACTIVAS	(HW)(PC) (009)	COMPUTADOR DE ESCRITORIO LENOVO	3	2	0	**3**								
	[PROVOCADO.2]	Inadecuado uso de computadoras	D	I			3	3	2		9	6	0	9
	(HW)(SCAN) (002)	SCANNER CANON DRC225	3	1	0	**3**								
	[NO_INTENCIONADO.2]	Errores de instalación de los equipos	D	I			2	3	1		6	2	0	6
	(SW)(PROPIO) (001)	SISTEMA UNICO DE RECAUDACIÓN (SUR)	5	5	4	**5**								
	[NO_INTENCIONADO.2]	Funcionamiento incorrecto del módulo de recaudación	D	I	C		5	4	4	3	20	20	15	25
	[EL.1]	Propagación inocente de virus	D	I	C		3	4	4	3	12	12	9	15
	(SW)(STD)(SRVMAIL) (001)	@emov.gob.ec	4	3	3	**4**								
	[EL.1]	Ataques mediante difusión de correos maliciosos	D	I	C		2	4	4	3	8	8	6	8
	(IE)(DATA) (001)	REPORTE DE VALORES COBRADOS Y PENDIENTES	3	3	4	**4**								
	[NO_INTENCIONADO.3]	Registro incompleto de actividades		I			3		4		0	12	0	12
	(IE)(DATA) (002)	BASE DE DATOS DE USUARIOS	4	3	4	**4**								
	[EL.2]	Información sensible de usuarios expuesta			C		2			4	0	0	8	8
	[NO_INTENCIONADO.3]	Inadecuado registro de actividades		I			3		4		0	12	0	12
	(RRHH)(UI) (046)	PERSONAL CARTERA	3	0	0	**3**								
	[NO_INTENCIONADO.5]	Exceso de carga laboral	D				3		3		0	9	0	9
	(RRHH)(UI) (059)	PERSONAL COACTIVAS	3	0	0	**3**								
	[NO_INTENCIONADO.5]	Exceso de carga laboral	D				3		3		0	9	0	9
SUBGERENCIA FINANCIERA	(HW)(LAPTOP) (001)	COMPUTADORA PORTATIL LENOVO	3	2	0	**3**								
	[PROVOCADO.2]	Inadecuado uso de computadoras	D	I			3	3	2		9	6	0	9
	(HW)(PRINT) (003)	IMPRESORA LÁSER HP MODELO P2055	2	1	0	**2**								
	[NO_INTENCIONADO.1]	Uso excesivo de equipos	D	I			4	2	1		8	4	0	8
	(SW)(PROPIO) (001)	SISTEMA UNICO DE RECAUDACIÓN (SUR)	5	5	4	**5**								
	[NO_INTENCIONADO.2]	Funcionamiento incorrecto del módulo de recaudación	D	I	C		5	4	4	3	20	20	15	25
	[EL.1]	Propagación inocente de virus	D	I	C		3	4	4	3	12	12	9	15
	(RRHH)(UI) (001)	PERSONAL SUBGERENCIA FINANCIERA	3	0	0	**3**								
	[NO_INTENCIONADO.5]	Exceso de carga laboral	D				3	3			9	0	0	9
PRESUPUESTO	(HW)(PC) (010)-(011)	COMPUTADOR DE ESCRITORIO LENOVO	3	2	0	**3**								
	[PROVOCADO.2]	Inadecuado uso de computadoras	D	I			3	3	2		9	6	0	9
	(IP)(DOCUMENTOS) (004)	CERTIFICACIONES PRESUPUESTARIAS - REGISTROS DE COMPROMISO	3	2	1	**3**								
	[NO_INTENCIONADO.7]	Pérdida accidental de información	D				4	3			12	0	0	12
	(RRHH)(UI) (054)-(056)	PERSONAL PRESUPUESTOS	3	0	0	**3**								
	[NO_INTENCIONADO.5]	Exceso de carga laboral	D				3	3			9	0	0	9
CONTABILIDAD	(HW)(PC) (012)-(013)-(014)-(015)	COMPUTADOR DE ESCRITORIO LENOVO	3	2	0	**3**								
	[PROVOCADO.2]	Inadecuado uso de computadoras	D	I			3	3	2		9	6	0	9
	(HW)(MULTI) (005)	IMPRESORA MULTIFUNCION XEROX MODELO PHASER	2	1	0	**2**								
	[NO_INTENCIONADO.1]	Uso excesivo de equipos	D	I			4	2	1		8	4	0	8
	(IP)(DOCUMENTOS) (005)	COMPROBANTES DE RETENCIÓN, OBLIGACIÓN Y PAGO	4	4	2	**4**								
	[NO_INTENCIONADO.7]	Pérdida accidental de información	D				4	3			12	0	0	16
	(EXTRAIBLE)(DISCO) (001)	DISCO DURO EXTERNO	2	0	0	**2**								
	[PROVOCADO.3]	Corto circuito	D				2	2			4	0	0	4
	(IC)(ROUTER)	ROUTER CISCO	3	3	2	**3**								
	[NO_INTENCIONADO.2]	Falta de mantenimiento de red de infraestructuras	D	I	C		2	3	2	1	6	4	2	6
	(RRHH)(UI) (002)-(003)-(004)-(005)	PERSONAL CONTABILIDAD	3	0	0	**3**								
	[NO_INTENCIONADO.5]	Exceso de carga laboral	D				3	3			9	0	0	9

Fuente: [19] Elaborado por el autor