UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERA EN SISTEMAS INFORMÁTICOS

TEMA:

PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGO TECNOLÓGICOS PARA LA EMPRESA PÚBLICA METROPOLITANA DE TRANSPORTE DE PASAJEROS DE QUITO

AUTORA:
MAYRA ZULEMA FUENTES YANCHA

TUTOR:
MG. IVÁN FERNANDO ANDOCILLA OLEAS

QUITO, ECUADOR

2019

DECLARACIÓN DE AUTORÍA

El documento de tesis con título: **"PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGO TECNOLÓGICOS PARA LA EMPRESA PÚBLICA METROPOLITANA DE TRANSPORTE DE PASAJEROS DE QUITO"**, ha sido desarrollado por la señorita Mayra Zulema Fuentes Yancha con C.C. No. 0803503911 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

_____

Mayra Zulema Fuentes Yancha

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación **"PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGO TECNOLÓGICOS PARA LA EMPRESA PÚBLICA METROPOLITANA DE TRANSPORTE DE PASAJEROS DE QUITO"**, presentado por Mayra Zulema Fuentes Yancha estudiante de la Carrera Ingeniería en Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D. M. 16 de agosto de 2019

TUTOR

Ing. Iván Fernando Andocilla Oleas

AGRADECIMIENTOS

En primer lugar, a Dios por haberme guiado por un buen camino a mi querida Madre y mi Padre con mucho cariño le dedico todo mi esfuerzo y a mis hermanos por siempre haberme dado su fuerza y apoyo incondicional que me han ayudado y llevado hasta donde estoy ahora. Por ultimo a mi tutor por haberme dedicado tiempo y paciencia en la elaboración de mi tesis.

DEDICATORIA

Dedico esta tesis a DIOS, a mis hermanos y a mis queridos Padres quienes inspiraron mi espíritu para la conclusión de esta tesis, a mis profesores en especial a mi tutor quien fue tan paciente y comprensivo sin su apoyo no hubiera concluido. A todos ellos se los agradezco desde el fondo de mi alma. Para todos ellos hago esta dedicatoria.

TABLA DE CONTENIDOS

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

Este documento presenta una propuesta de un plan de gestión de riesgo tecnológicos (PGRTI), para la Empresa Pública Metropolitana de Transportes de Pasajeros de Quito EPMTPQ, tiene por objetivo la aplicación del modelo Magerit versión 3- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, el que contribuirá a que la EPMTPQ, posea un conocimiento claro sobre los riesgos que puedan presentarse en los procesos o actividades que realiza el personal administrativo.

Para la selección de la metodología que se aplicó al proceso de la gestión de riesgos tecnológicos, se decidió realizar una tabla de comparación entre algunas metodologías de análisis de riesgos como son OCTAVE, CRAMM, IRAN y MAGERIT; esta comparación arrojo como resultado que la metodología más adecuada para la identificación y valoración de riesgos y salvaguardas de activos tecnológicos de la EPMTPQ es MAGERIT.

La metodología de MAGERIT define como se aplican la identificación y valoración de activos, la identificación y valoración de amenazas, la determinación del riesgo y la identificación y valoración de las salvaguardas. El análisis de los activos tecnológicos en cada uno de estos pasos permite identificar factores y criterios que se deben tener en cuenta para identificar y valorar los riesgos y salvaguardas que se presentan en el análisis de gestión de riesgos tecnológicos

PALABRAS CLAVES

ACTIVOS, AMENAZAS, RIESGO, SALVAGUARDAS, VALORACIÓN.

ABSTRACT

This document presents a proposal for a technology risk management plan (PGRTI), for the Public Metropolitan Passenger Transport Company of Quito EPMTPQ, aims at the application of the Magerit model version 3- Methodology of Analysis and Risk Management of Information Systems, which will contribute to the EPMTPQ, have a clear knowledge about the risks that may arise in the processes or activities carried out by administrative staff.

To identify the methodology that was applied to the technological risk management process, it was decided to make a comparison table between some risk analysis methodologies such as OCTAVE, CRAMM, IRAN and MAGERIT; This comparison showed that the methodology for the identification and assessment of risks and safeguards of technological assets of the EPMTPQ is MAGERIT.

The MAGERIT methodology defines how the four steps are applied such as the identification and valuation of assets, the identification and valuation of threats, the determination of risk and the identification and valuation of safeguards. The analysis of technological assets in each of these steps allows identifying factors and criteria that must be taken into account to identify and assess the risks and safeguards presented in the analysis of technological risk management

KEY WORDS

ACTIVE, THREATS, RISK, SAFEGUARDS, ASSESSMENT.

INTRODUCCIÓN

Antecedentes de la situación objeto de estudio

En el presente trabajo se han descrito los conceptos relacionados con la gestión de los riesgos de la seguridad de los activos informáticos, estándares, metodologías y herramientas que proporcionan las guías necesarias para reducir el nivel de vulnerabilidad que tienen los activos ante una amenaza. Es de vital importancia que una organización, dedicada a brindar servicio de transporte público deba mantener respaldada mucha información confidencial de forma segura, y además cuente con un plan de gestión de riesgos para garantizar la continuidad del servicio.

A partir del año 1995 se inicia la operación del servicio de transporte municipal urbano TROLEBUS, con la primera etapa en el tramo comprendido entre la estación Sur "El Recreo" y la calle Esmeraldas, con la operación 17 trolebuses. (Diaz & Trujillo, 2017)

A partir del año 1996 se amplía el servicio desde la Estación Sur "El Recreo" hasta la Avenida Colón, incrementándose la flota operativa en 15 unidades adicionales de trolebuses; a partir del mes de abril de 1996 se extiende la operación a la estación norte "La Y", contándose para dicha operación con 54 unidades de trolebús. Con la capacidad descrita de unidades, se transportó aproximadamente cien mil pasajeros. (Diaz & Trujillo, 2017)

El incremento en la demanda del servicio público municipal en los años subsiguientes y la mejora del servicio de transporte, obligó a la empresa a incrementar su capacidad operacional y operar con 113 unidades en el año 2000, con la incorporación de

nuevas rutas para servicio a la ciudadanía de Distrito Metropolitano, partiendo desde la estación norte "La Y", hasta la nueva extensión en el sur "Moran Valverde".

La demanda del servicio por efectos del crecimiento poblacional, la creación de nuevos barrios, tanto en el sector urbano del Distrito como en la periferia, obligó al Municipio Metropolitano y a la empresa en particular a ofrecer varios servicios adicionales en el sistema integrado de transporte público-(SITP), de invalorable contenido para la movilidad de la comunidad metropolitana, incorporándose tres corredores a la operación: Corredor Ecovía, Sur Oriental y Sur Occidental. (Diaz & Trujillo, 2017)

Al momento la Empresa cuenta con una flota de 279 vehículos, compuesta de 13 trolebuses, 162 unidades articuladas y 4 buses tipo; sin embargo, del total de flota descrita, se encuentran 15 unidades con más de 360 días do operativas, lo que da una flota efectiva en operación de 264 vehículos al mes de julio 2015, a la que debe descontarse un promedio de 36 unidades que ingresan a mantenimiento y que, por lo tanto, refleja una flora promedio entregada a operación de 228 unidades al des de julio de 2015. (Diaz & Trujillo, 2017, pág. 5)

El crecimiento sostenido de la EPMTPQ, se refleja en las siguientes cifras: 134.4 millones de pasajeros pago transportados entre enero-julio 2015; 19 mil % de crecimiento en el promedio mensual de pasajeros; administración de 5 corredores: Trolebús, Ecovía, Sur Oriental, Carcelén y Sur Oriental. Por otro lado, las cifras de recaudación entre enero-julio 2015, revelan un ingreso de 29.8 millones de dólares, que representa el 37 % del presupuesto del ejercicio económico 2015. (Diaz & Trujillo, 2017, pág. 5)

Planteamiento del problema

El análisis de gestión de riesgos tecnológicos, para la Empresa Pública Metropolitana de Transportes de Pasajeros de Quito EPMTPQ, como su nombre lo indica es todo un conjunto de procesos que se involucran en el ciclo de vida de la información para garantizar la confidencialidad, integridad y disponibilidad de la misma. La información y los sistemas que hacen uso de ella (sistemas de información, equipos tecnológicos), son activos demasiado importantes para la empresa, el análisis de gestión de riesgos ayuda a prevenir la materialización de las amenazas (una hipótesis de todo aquello que pudiera ocurrir y que tuviera un impacto para la organización) a la que los activos puedan estar expuestos, por lo tanto es de propósito general determinar los componentes de un sistema que requieren protección, evaluar las vulnerabilidades que los debilitan y así como determinar las amenazas que lo ponen en peligro.

La Empresa Pública Metropolitana de Transportes de Pasajeros de Quito EPMTPQ, se encuentran en crecimiento, que, a pesar de tener un flujo constante de empleados, no se anticipan a las situaciones adversas en donde se vean involucrados los activos de la empresa, debido a la gran demanda del personal que se vinculan y se desvinculan de la empresa, los problemas que se presentan actualmente en la empresa y las posibles pérdidas que estas puedan generar, debido a varios factores, entre los que se encuentran:

- La falta de interés y/o de tiempo de las personas encargadas de revisar periódicamente las cuentas y permisos de acceso establecidos, con el fin de establecer los accesos de cada personal, de acuerdo a las necesidades de la EPMTPQ.
- Pérdida de información de datos almacenados en dispositivos propios de los empleados.
- Falta de conocimiento del personal en el cambio en roles, funciones o cargos de un funcionario, que requiera acceso a diferente información o infraestructura tecnológica de la EPMTPQ, por lo que no es notificado a través de gerencias o coordinaciones mediante memorando a la Gerencia de Tecnologías de la Información, para que procedan con el cambio respectivo.
- Falta de control de seguridad de los activos tecnológicos en especial con los relojes biométricos.

Justificación

Teniendo en cuenta el problema de la EPMTPQ, los riesgos tecnológicos se evalúan mediante un análisis de gestión de riesgos, en donde se realice una valoración de cada uno de los activos, se puede lograr validar el nivel de riesgo con el que puede contar cada activo, además de verificar los posibles riesgos con los que puede contar y así evaluar el nivel de incidencia y amenazas.

Hoy en día existen varias metodologías como OCTAVE, CRAMM, IRAM y MAGERIT que permiten realizar un análisis de riesgos del grado de confiabilidad y seguridad dentro de un sistema de información, entre ellas se encuentra la metodología Magerit, metodología de análisis y gestión de riesgos de tecnologías de la información, mediante la cual se sigue una serie de pasos y se mostrará el estado actual de seguridad que se encuentran los activos tecnológicos tanto software como hardware de la EPMTPQ.

La aplicación de la metodología Magerit permite disponer de un plan de mitigación en el cual se detallará los riesgos que están expuestos los activos tecnológicos de la empresa ya que podrían ser víctimas de agentes externos o internos generando daños en los equipos o pérdidas de información.

Objetivos

General

- Desarrollar un plan de gestión de riesgos tecnológicos de los activos relevantes, para la Empresa Pública Metropolitana de Transporte de Pasajeros de Quito, siguiendo la metodología Magerit para el análisis y gestión de riesgos, con la finalidad de mitigar riesgos informáticos que afecte a la información y a las actividades de la empresa.

Objetivos específicos

- Determinar los activos relevantes de la EPMTPQ y la valoración de aquellos.

- Identificar las amenazas a los que están expuestos los activos y la valoración de la probabilidad o impacto de los mismos.
- Determinar el valor del riesgo asociado a las amenazas identificadas de acuerdo a la escala de colores nivel bajo, medio y alto.
- Determinar que salvaguardas hay dispuestas y la valoración de cuán eficaces son frente al riesgo.

Descripción de los capítulos

Capítulo I: Describe el estado del arte de los diferentes riesgos tecnológicos que se puedan presentar en otros países con la finalidad de conocer los tipos de riesgos y que puedan ser aplicados en el análisis de gestión de riesgos de la EPMTPQ.

Capítulo II. Se habla sobre la metodología que se utilizará para el proyecto de investigación con sus respectivas herramientas y los recursos utilizados en cada una de las actividades para llevar a cabo el análisis de riesgos y así obtener resultados verídicos del riesgo que la empresa posee, posteriormente se realiza los resultados de las encuestas mediante tabulaciones.

Capítulo III. Se centra en el desarrollo del plan de gestión de riesgos tecnológicos, formaliza las actividades y la justificación del uso de cada herramienta incluyendo costos y ventajas del producto desde su concepción inicial hasta su puesta en producción, así como a la protección de los equipos tecnológicos.

Capítulo IV. Se centra la seguridad de los sistemas de información considerando varios puntos de vista para mitigar los riesgos, estableciendo las actividades principales que serán requeridas para el análisis de riesgos informáticos, se realizará la identificación de clases de activos y se evaluará a través de matrices.

CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA

1.1. Estado del arte

Perfil de peligros naturales de Europa

Europa se caracteriza por varios elementos geofísicos y climáticos que la hacen susceptible de una amplia gama de catástrofes naturales extremas. Entre 1998 y 2002, los desastres naturales y los accidentes tecnológicos afectaron a más de siete millones de personas en Europa y causaron al menos 60 billones de euros en pérdidas aseguradas, muy por debajo de las pérdidas totales, ya que muchos afectados no estaban asegurados. (Muerza, 2011)

Dentro del territorio europeo, la distribución de peligros naturales es muy distinta. Europa Occidental, Central y Oriental, con sus grandes sistemas fluviales, pero también con las pequeñas corrientes del Mediterráneo, son vulnerables a las inundaciones. El Sur de Europa y el Mediterráneo se caracterizan por los peligros de sequía e incendios forestales, aunque este último también se aplica a Europa Oriental. Del mismo modo, Europa Occidental y las Islas Británicas son propensas a las tormentas y las áreas montañosas de los Alpes, los Pirineos y los Cárpatos, a desprendimientos de tierra y avalanchas. Finalmente, algunas áreas específicas del Mediterráneo central y oriental están amenazadas por seísmos y erupciones volcánicas (Agencia Europea del Medio Ambiente, 2016)

Riesgos naturales y tecnológicos

En la Unión Europea, el número de accidentes industriales graves que se registran anualmente se ha mantenido más o menos constante desde 1984. Teniendo en cuenta que tanto la notificación de accidentes como la actividad industrial se han incrementado desde entonces, es probable que haya disminuido la cantidad de accidentes por unidad de actividad.

En la actualidad, no hay bases de datos relativos a los accidentes en Europa central y oriental ni en los NEI. (Agencia Europea de Medio Ambiente , 2016)

Con arreglo a la Escala internacional de sucesos nucleares (INES) del Organismo internacional de la energía atómica, en Europa no ha habido "accidentes" (niveles 4 a 7 de la INES) desde 1986 (el de Chernobil fue del nivel 7 de la INES). La mayoría de los sucesos registrados se consideran "anomalías" (nivel 1 de la INES), y sólo algunos alcanzan la categoría de "incidentes" (niveles 2 y 3 de la INES).

En los últimos diez años, se ha registrado en todo el mundo una notable reducción del número anual de vertidos de petróleo que puedan considerarse de importancia. Sin embargo, en los últimos años se produjeron en Europa occidental tres de los vertidos de mayor gravedad de todos los acaecidos, a los que puede atribuirse la mayor proporción de todo el petróleo derramado hasta la fecha. (Agencia Europea de Medio Ambiente , 2016)

Riesgos y oportunidades de las nuevas tecnologías informáticas

La historia del procesamiento de datos en línea se inicia en el país en 1975. Marcel Laniado de Wind, con su gran vocación de atención al cliente y la acertada asesoría de la que se rodeó, había logrado la instalación en el Banco del Pacífico del primer procesador en línea IBM, Modelo 3/10 (10K de memoria). Gran avance tecnológico. El Ecuador se había puesto a la altura de Brasil y Argentina, y ganado la institución un hito que significó una gran ventaja competitiva en sus plataformas de atención, gestión operativa y ahorro en recursos humanos. La amplia visión que caracterizó a Marcel, lo llevó a crear una gerencia de tecnología responsable de la investigación de los avances aplicables a los servicios bancarios, cuyos principales resultados fueron la creación en el país de una de las primeras redes de cajeros automáticos de Sudamérica y las primeras redes telefónica y digital de servicio al cliente. Constituido en 1972, a fines de los ochenta el banco se había convertido en la más grande institución financiera del país. Producto de su genial visión, quizás su mayor contribución social en el tema que nos atañe fue traer el servicio de internet, cuando

su única función era el acceso digital a las bibliotecas de las principales universidades del mundo para uso de entidades educativas. (Cuestas, 2014)

Desde los años ochenta del siglo pasado a la fecha, el avance en el desarrollo de telecomunicaciones, hardware, software y herramientas digitales y el uso en las empresas de variadas y modernas aplicaciones de informática fue abrumador, como abrumador es el gran desafío que representan las nuevas tecnologías por la posibilidad de crear incontables nuevos modelos de negocios que pueden resultar en nuevas estrellas que opaquen a las actuales. Por ello, directivos y gerentes deben considerar el impacto combinado que ocasiona sobre sus entidades el servicio de internet en la nube, o procesamiento en línea sin inversión en hardware y ahorro en personal de tecnología de la información, facilidad que ayuda a iniciar nuevos negocios con menor inversión fija; la cada vez mayor versatilidad para manejar aplicaciones soportadas en el poder de los equipos móviles; integración de redes sociales con redes empresariales convertidas en fundamental herramienta para llegar a los clientes; el video en redes que cobra cada vez más importancia en sus acciones de marketing publicitario, y la MegaData o Big Data, todavía aprovechada únicamente por los grandes consorcios, que captura terabytes de datos valiosos sobre los clientes, prospectos, productos, vendedores y competidores, información de fuentes internas y externas que se combinan formando una herramienta inteligente que entregará ventajas competitivas para aquellas empresas que lo sepan usar. (Cuestas, 2014)

Las recientes aplicaciones de billeteras electrónicas ya están en el mercado. En tiendas de departamentos de Estados Unidos se pagan los artículos en las cajas usando Google Wallet, Apple Wallet, o tarjetas de crédito. Al respecto, un ejemplo del aprovechamiento de ventajas competitivas tecnológicas y de ganadores y perdedores fue la iniciativa de las tiendas de la firma MCX de crear su propia billetera electrónica bajo el nombre MCX-CurrentC, para servir digitalmente a sus clientes y ahorrar el pago de comisiones a las compañías emisoras de tarjetas de crédito. (Cuestas, 2014)

En el proyecto de tesis se plantea una propuesta de un plan de gestión de riesgo tecnológicos para la Empresa Pública Metropolitana de Transporte de Pasajeros de Quito, tiene como principal objetivo realizar el análisis de gestión de riesgos de los activos tecnológicos más relevantes de la EPMTPQ, para lo cual se utilizó la metodología Magerit (Metodología para el Análisis y Gestión de Riesgos de los Sistemas de Información), que ofrece un método estructurado y sistemático para la realización de un AGR (Análisis y

Gestión de Riesgos), otra gran ventaja de aplicar Magerit es la posibilidad que permite usar una herramienta informática diseñada específicamente para Magerit.

1.2. Lógica del negocio

La Empresa Pública Metropolitana de Transporte de Pasajeros de Quito, su actividad principal es operar y administrar el servicio de transporte público de pasajeros en el Distrito Metropolitano de Quito y brindar asesoría técnica especializada a instituciones públicas o privadas, nacionales o extranjeras en el ámbito del transporte.

Los servicios de la EPMTPQ se centran en los siguientes ejes estratégicos.

Figura 1.1. Servicios de la EPMTPQ, ejes estratégicos
Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito.

Sobre la base de los ejes mencionados, la Empresa Pública Metropolitana de Transportes de Pasajeros encargada de cumplir con los siguientes propósitos:

- Aplicar criterios de eficiencia, eficacia y efectividad, consistente con su relación costo/beneficio.
- Proveer un servicio seguro y de calidad.

En la figura 1.2, podrá visualizar la estructura Orgánica Funcional de la EPMTPQ, la cual posee divisiones por gerencias y coordinaciones de acuerdo a la siguiente estructura funcional.

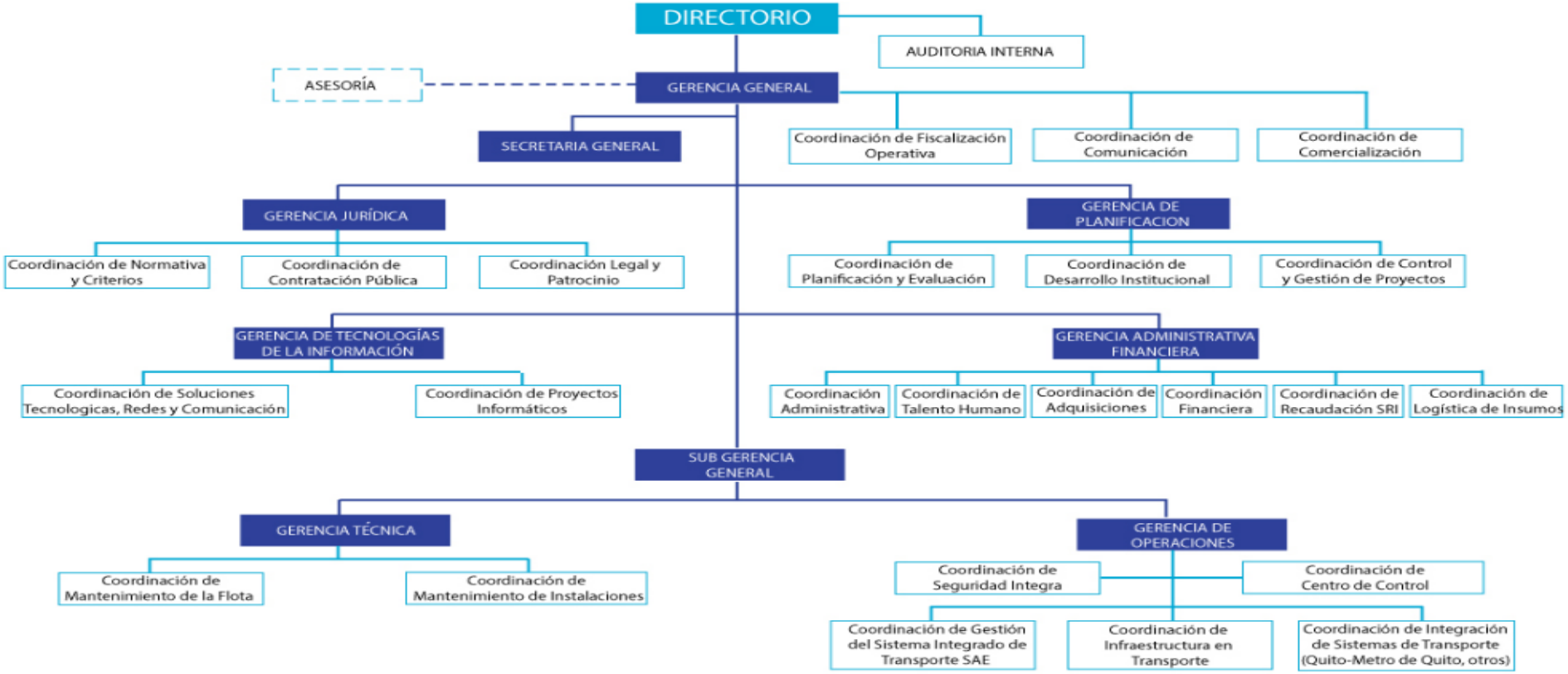


Figura 1.2. Estructura Orgánica Funcional de la EPMTTPQ
Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito.

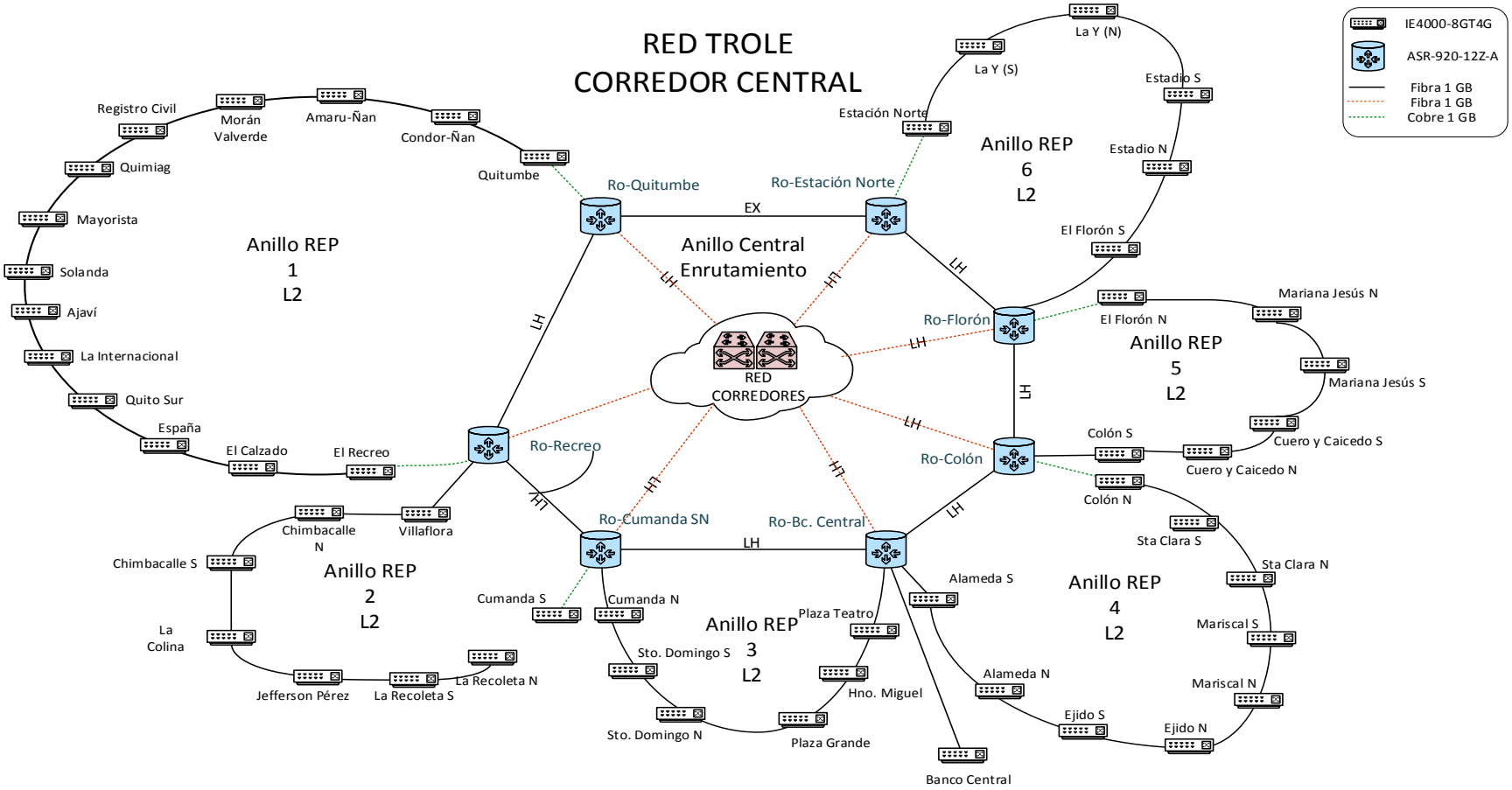


Figura 1.3. Diagrama de RED
Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito

❖ **Direccionamiento IP**

– **Dirección de Loopback de los Routers del anillo principal (ASR)**

Cada uno de los equipos ASR tiene configurada una dirección IP de loopback como requisito del protocolo de enrutamiento dinámico OSPF, esta puede emplearse para la gestión de los equipos.

Tabla 1.1. Dirección de loopback ASR

EQUIPO	LOOPBACK 10	OBSERVACIONES
Ro-Bco. Central	172.19.0.1	
Ro-Colón	172.19.0.2	
Ro-Florón	172.19.0.3	
Ro-Estación Norte	172.19.0.4	NO INSTALADO
Ro-Quitumbe	172.19.0.5	
Ro-Recreo	172.19.0.6	
Ro-Cumandá SN	172.19.0.7	

Fuente: Empresa Pública Metropolitana de Transportes de Pasajeros de Quito

❖ **Direccionamiento IP de los equipos de Acceso**

– **Anillo 1**

A continuación, se detalla la dirección IP de gestión para cada uno de los equipos de Acceso:

Tabla 1.2. Direccionamiento IP equipos de acceso anillo 1

Nº	PARADA	IP VLAN 10 /24
1	Terminal Quitumbe	172.19.21.101
2	Cóndor ñan	172.19.21.102
3	Amaruñan	172.19.21.103
4	Moran Valverde	172.19.21.104
5	Registro Civil	172.19.21.105
6	Quimiag	172.19.21.106
7	Mercado Mayorista	172.19.21.107
8	Marquesa de Solanda	172.19.21.108
9	Ajavi	172.19.21.109
10	La Internacional	172.19.21.110
11	Quito Sur	172.19.21.111

Fuente: Empresa Pública Metropolitana de Transportes de Pasajeros de Quito

– **Anillo 2**

A continuación, se detalla la dirección IP de gestión para cada uno de los equipos de Acceso:

Tabla 1.3. Direccionamiento IP equipos de acceso anillo 2

Nº	PARADA	IP VLAN 10 /24
1	Villaflora	172.19.22.101
2	Chimbacalle n/s	172.19.22.102
3	Chimbacalle s/n	172.19.22.103
4	Colina	172.19.22.104
5	Jefferson Pérez	172.19.22.105
6	Recoleta s/n	172.19.22.106
7	Recoleta n/s	172.19.22.107
8	Cumanda s/n	172.19.22.108

Fuente: Empresa Pública Metropolitana de Transportes de Pasajeros de Quito

– **Anillo 3**

A continuación, se detalla la dirección IP de gestión para cada uno de los equipos de Acceso:

Tabla 1.4. Direccionamiento IP equipos de acceso anillo 3

Nº	PARADA	IP VLAN 10 /24
1	Cumanda n/s	172.19.23.101
2	Santo Domingo s/n	172.19.23.102
3	Santo Domingo n/s	172.19.23.103
4	Plaza Grande	172.19.23.104
5	Hermano Miguel	172.19.23.105
6	Plaza del teatro n/s	172.19.23.107
*****	Banco Central	172.19.23.108

Fuente: Empresa Pública Metropolitana de Transportes de Pasajeros de Quito

– **Anillo 4**

A continuación, se detalla la dirección IP de gestión para cada uno de los equipos de Acceso:

Tabla 1.5. Direccionamiento IP equipos de acceso anillo 4

Nº	PARADA	IP VLAN 10 /24
1	Alameda s/n	172.19.24.101
2	Alameda n/s	172.19.24.102
3	Ejido s/n	172.19.24.103
4	Ejido n/s	172.19.24.104
5	Mariscal n/s	172.19.24.105
5	Mariscal s/n	172.19.24.106
7	Santa Clara n/s	172.19.24.107
8	Santa Clara s/n	172.19.24.108
9	Colon n/s	172.19.24.109

Fuente: Empresa Pública Metropolitana de Transportes de Pasajeros de Quito

– **Anillo 5**

A continuación, se detalla la dirección IP de gestión para cada uno de los equipos de Acceso:

Tabla 1.6. Direccionamiento IP equipos de acceso anillo 5

Nº	PARADA	IP VLAN 10 /24
1	Colon s/n	172.19.25.101
2	Cuero y Caicedo n/s	172.19.25.105
3	Cuero y Caicedo s/n	172.19.25.102
4	Mariana de Jesús s/n	172.19.25.103
5	Mariana de Jesús n/s	172.19.25.104
6	Florón n/s	172.19.25.106

Fuente: Empresa Pública Metropolitana de Transportes de Pasajeros de Quito

- **Anillo 6**

A continuación, se detalla la dirección IP de gestión para cada uno de los equipos de Acceso:

Tabla 1.7. Direccionamiento IP equipos de acceso anillo 6

Nº	PARADA	IP VLAN 10 /24
1	Florón s/n	172.19.26.101
2	Estadio n/s	172.19.26.103
3	Estadio s/n	172.19.26.104
4	La Y n/s	172.19.26.105
5	La Y s/n	172.19.26.106

Fuente: Empresa Pública Metropolitana de Transportes de Pasajeros de Quito

1.3. Herramientas técnicas

1.3.1. Metodología MAGERIT

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de Administraciones públicas, Magerit, es un método formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Objetivos

- Determinar los activos relevantes para la Organización, su valor en el sentido de qué perjuicio (coste) supondría su degradación.
- Identificar y valorar las amenazas según la probabilidad o impacto a los que están expuestos aquellos activos.
- Determinar el valor del riesgo asociado a las amenazas identificadas de acuerdo a la escala de colores nivel bajo, medio y alto.

- Determinar que salvaguardas hay dispuestas y la valoración de cuán eficaces son frente al riesgo.

La estimación del riesgo definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza, de acuerdo a los riesgos más altos se ha elaborado fichas de salvaguardas de los activos en riesgo. (Soto Suárez, 2018)

MAGERIT consiste en 3 libros

- ✓ Libro I: Método
- ✓ Libro II: Catálogo de Elementos
- ✓ Libro III: Guía de Técnicas

Elementos del Magerit

(Magerit, Seguridad Informática - Magerit, 2015) En la realización de un Análisis y Gestión de Riesgos según Magerit, el Analista de Riesgos es el profesional especialista que maneja seis elementos básicos:

- ❖ **Activos:** Recursos del sistema de información o relacionados con este, necesarios para que funcione correctamente y alcance los objetivos propuestos por su dirección. El activo esencial es la información o dato.

- ❖ **Amenazas:** Determinar las amenazas que pueden afectar a cada activo, hay que estimar cuán vulnerable es el activo en dos sentidos: Degradación: Como es de perjudicial y Frecuencia: Cada cuanto se materializa la amenaza.

- ❖ **Vulnerabilidades:** Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.

- ❖ **Impactos:** Es el daño sobre el activo causado por la amenaza, conociendo el valor de los activos sería muy sencillo calcular el valor del impacto.

- ❖ **Riesgo:** Es la medida de la posibilidad que existe en que se materialice una amenaza. Conociendo el riesgo se podrá calcular la frecuencia.

- **Salvaguardas (Funciones, Servicios y Mecanismos):** Una salvaguarda es un mecanismo de protección frente a las amenazas, reducen la frecuencia de las amenazas y limitan el daño causado por estas.

Análisis de Riesgos para identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados al Sistema de Información (activos); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener en la organización, obteniendo cierto conocimiento del riesgo que se corre.

Gestión de Riesgos basada en los resultados obtenidos en el análisis anterior, que permite seleccionar e implantar las medidas o "salvaguardas" de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. (Bolaños, 2014)

Figura 1.4. Modelo Magerit.

Fuente: Magerit. V3

Pasos a seguir

1.3.2. Paso 1: Identificación y valoración de los activos

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia. Se compone de 3 sub-tareas: (Magerit-V3, Libro I - Método, 2012)

Esta actividad se basa en recolectar la información necesaria para identificar los activos, mediante entrevistas al personal, solicitando diagramas de proceso y de flujos de datos. De esta manera, se puede medir el alcance del proyecto y obtener las relaciones entre los activos.

- ✓ **Dependencias entre Activos**

El objetivo de esta tarea es identificar y valorar las dependencias entre activos, es decir, conocer la medida en que un activo de orden superior se puede ver perjudicado por una amenaza sobre un activo de orden inferior; resultando diagramas de dependencia.

- ✓ **Valoración de los Activos**

El objetivo es identificar en qué dimensión es valioso el activo, para lo cual a la organización significará una pérdida en caso de que fuese afectado. El resultado de esta actividad es el informe denominado “modelo de valor”.

Figura 1.5. Escala de valoración de activos

Fuente: Libro II. Catálogo de elementos. Metodología Magerit

Tabla 1.8. Criterios de valoración de activos

Valor			Criterio
10	Muy Alto	MA	Daño muy grave a la organización
7-9	Alto	A	Daño grave a la organización
4-6	Medio	M	Daño importante a la organización
1-3	Bajo	B	Daño menor a la organización
0	Despreciable	D	Irrelevante a efectos prácticos

Fuente: Libro II. Catálogo de elementos. Metodología Magerit.

Para continuar con la descripción de los elementos que componen la tabla se seguirá de acuerdo al rango de criterios:

Se puede considerar Daño muy grave [10] a:

- Daños excepcionalmente serios que pueden afectar la eficacia de los activos informáticos o la seguridad de la información.
- Daños que pueden causar un incumplimiento grave de una ley, contrato o normas ya sean externas o internas.
- Daños que puedan causar un incidente serio de seguridad y dificulte la investigación de los mismos.
- Daños que pueden causar serias pérdidas económicas.
- Daños que pueden causar la pérdida de confidencialidad de Datos o información.

Se puede considerar daño Grave [7-9] a:

- Daños que pueden causar una interrupción de las actividades de la E.P.M.P.Q, con un impacto para las demás áreas de la organización.
- Daños que pueden causar una publicidad negativa de la operatividad a nivel general con las demás áreas de la organización.
- Daños que pueden causar la pérdida de confidencialidad de datos o información clasificada como reservada o confidencialidad para los procesos de la E.P.M.T.P.Q.

Se puede considerar daño importante [4-6] a:

- Daños que pueden afectar labores de un grupo de individuos de la seguridad de la información.
- Daños que pueden causar la pérdida de confidencialidad de datos o información.
- Daños que pueden causar la interrupción de actividades propias de cada área.

Se puede considerar daño menor [1-3] a:

- Daños que probablemente causen interrupción de las actividades propias de cada área.
- Daños que probablemente afecten la eficacia de los activos informáticos o la seguridad de la información.
- Daños que probablemente afecten a un individuo del área administrativa usuario no encuentre correos enviados.
- Daños que probablemente causen un incumplimiento de una ley, contrato o normas ya sean externas o internas.
- Daños que pueden causar mal manejo de información.

Se puede considerar daño despreciable [0] a:

- Daños que no afecten las actividades propias de cada área.
- Daños que no afecten la eficacia de los activos informáticos.
- Daños que no causan incumplimiento de una ley, contrato o normas ya sean externas o internas.

La suma de la valoración de las tres variables sobre el activo determina el valor total del activo en el proceso de los riesgos informáticos. El valor máximo de un activo es de 30 y un mínimo es 0.

Tabla 1.9. Estimación de valor de activos

VALOR	CLASIFICACIÓN
0 – 10	Bajo
10 – 20	Medio
20 – 30	Alto

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito

Llevar a cabo un inventario de equipo de cómputo, software y mobiliario, para determinar cuál es la información crítica que se tiene que resguardar, adicionalmente levantar un inventario de los equipos tecnológicos que son requeridos más importantes a fin de evaluar los riesgos a que están expuestos.

Dependencias. - Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos,

las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.

- **Activos esenciales**
  - información que se maneja
  - servicios prestados
- **Servicios internos.**
  - que estructuran ordenadamente el sistema de información
- **El equipamiento informático**
  - aplicaciones (software)
  - equipos informáticos (hardware)
  - comunicaciones
  - soportes de información: discos, cintas, etc.
- **El entorno:** activos que se precisan para garantizar las siguientes capas
  - equipamiento y suministros: energía, climatización, etc.
  - Mobiliario
- **Los servicios subcontratados a terceros**
- **Las instalaciones físicas**
- **El personal**
  - usuarios
  - operadores y administradores
  - desarrolladores

La seguridad de la información es evaluada por tres pilares fundamentales: Disponibilidad, Integridad y Confidencialidad.

- **Confidencialidad:** asegura que solo los usuarios con acceso autorizado puedan acceder a la información.
- **Integridad:** proteger la exactitud, totalidad de los datos y métodos de procesamiento de la información que los usuarios autorizados gestionan.
- **Disponibilidad:** los recursos deben estar disponibles cuando sean requeridos en cualquier instante de tiempo

A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que se acerquen a la percepción de los usuarios de los sistemas de información:

- **Autenticidad:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Trazabilidad:** Aseguramiento de que en todo momento se podrá determinar Quién hizo qué y en qué momento.

  Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. Análisis de riesgos: proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

  Tratamiento de los riesgos: proceso destinado a modificar el riesgo.

1.3.3. Paso 2: Identificación y valoración de las amenazas

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia o probabilidad y daño causado o degradación. Se compone de 2 sub-tareas:

- ✓ **Identificación de las amenazas**

Se debe identificar las amenazas más relevantes sobre cada activo, se lo consigue analizando los informes y registros de incidentes y vulnerabilidades. Además, realizando árboles de ataque, los cuales permiten estudiar y analizar cómo se puede atacar un objetivo permitiendo identificar qué salvaguardas se necesitan desplegar para impedirlo.

- ✓ **Valoración de las amenazas**

El objetivo es estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo, estimando la degradación que causaría la amenaza en cada dimensión del activo si llegara

a materializarse. El resultado de esta actividad es el informe denominado “mapa de riesgos”. (Magerit-V3, Libro I - Método, 2012)

- **[N] Desastres Naturales:** sucesos que pueden ocurrir de forma sin intervención de los seres humanos como causa directa o indirecta, en esta categoría se encuentran incendios, inundaciones o demás desastres naturales.
- **[1] De origen industrial:** Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial; estas amenazas pueden darse de forma accidental o intencional. En esta categoría se encuentran incendios, daños por agua, desastres industriales, contaminación mecánica, contaminación electromagnética, avería de origen físico o lógico corte del suministro eléctrico, condiciones inadecuada de temperatura y/o humedad, fallo de servicios o comunicaciones, interrupción de otros servicios y suministros esenciales, degradación de los soportes de almacenamiento de la información y emanaciones electromagnéticas.
- **[E] Errores y fallos no intencionados:** Fallos no intencionados causados por las personas. En esta categoría se encuentran errores de usuarios, errores del administrador, errores de monitorización, errores de configuración, deficiencias de la organización, difusión del software dañino, errores de re-encaminamiento, errores de secuencia, escapes de información, alteración de la información, introducción de información incorrecta, degradación de la información, destrucción de la información, divulgación de la información, vulnerabilidades de los programas, errores de mantenimiento / actualización de programas, errores de mantenimiento, actualización de equipos, caída del sistema por agotamiento de recurso e indisponibilidad del personal.

- **[A]Ataques deliberados o intencionados:** Fallos deliberados causados por las personas. En esta categoría se encuentran: manipulación de la configuración, suplantación de la identidad del usuario, abuso de privilegios de acceso, uso no previsto, difusión de software dañino, re-encaminamiento de mensajes, alteración de secuencia, acceso no autorizado análisis de tráfico, repudio, interceptación de información, modificación de la información, introducción de falsa información, corrupción de la información, destrucción de la información, divulgación de la información, manipulación de programas, denegación de servicios, robo, ataque destructivo, ocupación enemiga, indisponibilidad del personal, extorción e ingeniería social. (Amutio Gómez, 2012)

Una amenaza no afecta a un activo totalmente, sino que lo puede afectar en alguna de sus dimensiones de seguridad y en alguna magnitud determinada.

Cuando se ha determinado si una amenaza afecta a un activo se debe estimar cuan vulnerable es el activo en dos sentidos:

Degradación o impacto: Que tan perjudicado resultaría el activo.

Frecuencia: Cada cuanto se materializa la amenaza.

❖ **Valoración de las amenazas**

La probabilidad de ocurrencia se modela de forma cualitativa y cuantitativa.

Tabla 1.10. Degradación del valor

MA	Muy Alta	Casi Seguro	Fácil
A	Alta	Muy Alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco Probable	Muy Difícil
MB	Muy Baja	Muy Raro	Extremadamente Difícil

Fuente: Libro II. Catálogo de elementos. Metodología Magerit.

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra. Son valores típicos:

Tabla 1.11. Probabilidad de ocurrencia

MA	**100**	**muy frecuente**	**a diario**
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: Libro II. Catálogo de elementos. Metodología Magerit.

1.3.4. Paso 3. Determinación y valoración del riesgo

El riesgo, es la medida del daño probable sobre un sistema. Al conocer el impacto de las amenazas sobre los activos, se puede determinar el riesgo teniendo en cuenta la frecuencia de la ocurrencia. El riesgo crece con el impacto y con la frecuencia.

Riesgo Residual. - Al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegada. (Magerit-V3, Libro I - Método, 2012)

La siguiente fórmula permite determinar el valor del riesgo que tiene un activo de información.

Tabla 1.12. Fórmula para determinar el Valor del Riesgo.

Valor Total de Activo	**x**	**Valor Frecuencia de Amenaza**	**x**	**Valor Degradación o Impacto**	**=**	**Valor Riesgo**

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito

Conociendo el valor total y el nivel que representa; en la siguiente tabla se define a que riesgos se les debe hacer un proceso de tratamiento de riesgos.

Tabla 1.13. Escala de Valoración de Riesgo

VALOR RIESGO	NIVEL		TRATAMIENTO
0 - 149	Bajo	Aceptable	Aceptar el riesgo, se debe realizar un análisis del costo beneficio con el que se pueda decidir entre asumir el riesgo o compartirlo.
150 - 299	Medio	Importante	Reducir, compartir o transferir el riesgo. La organización debe diseñar planes de contingencia, para protegerse en caso de que se materialicen riesgos de este nivel.
300 - 750	Alto	Inaceptable	Evitar, Reducir, Compartir o transferir el riesgo. Es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible, de lo contario se deben implementar controles de prevención para evitar la probabilidad del riesgo, de Protección para disminuir el impacto o combatir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponible.

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito

1.3.5. Paso 4. Identificación y valoración de las salvaguardas

Son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Revisar la seguridad, controles físicos y ambientales existentes, evaluando si son adecuados respecto a las posibles amenazas. Se debe estar preparado para cualquier percance, verificando que dentro de la organización se cuente con los elementos necesarios para salvaguardar sus activos.

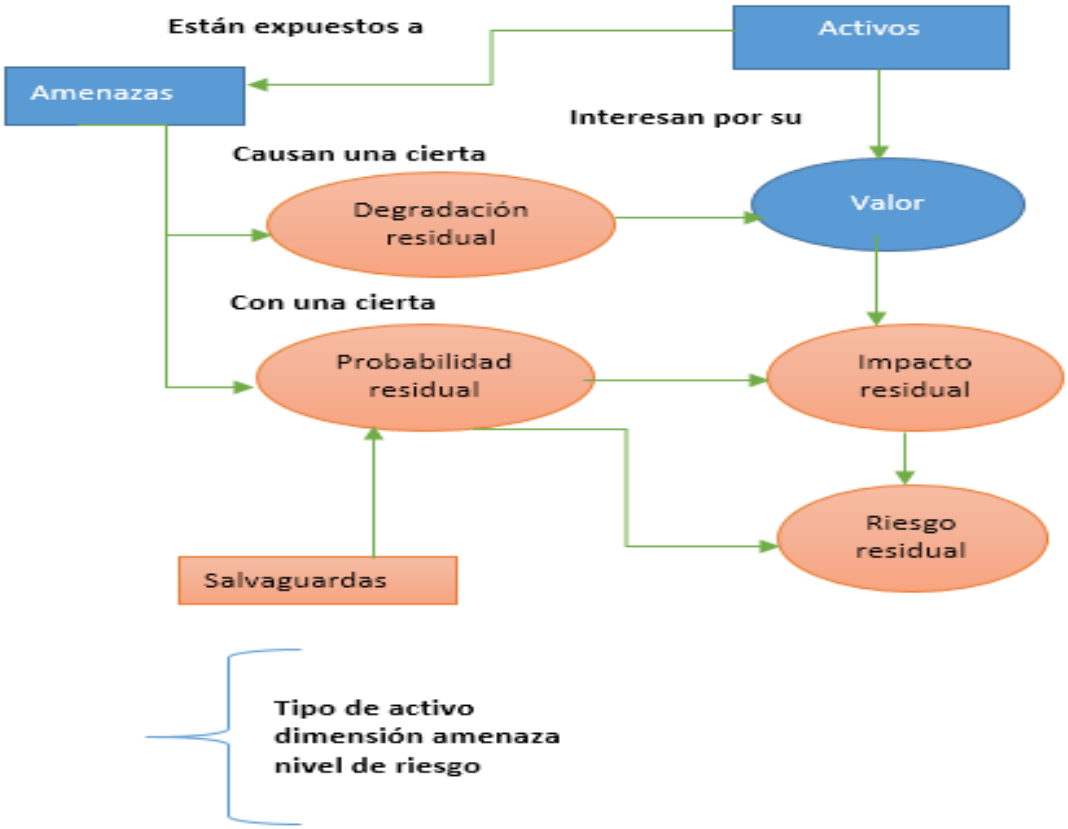


Figura 1.6. Elementos de análisis del riesgo residual

Fuente: Magerit V.3

Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar. Se compone de 2 sub-tareas:

- ✓ **Identificación de las salvaguardas pertinentes**

Esto se logra analizando los informes de productos y servicios, indicadores de impacto y riesgo residual y los modelos de activos y amenazas del sistema.

- **Protección de los datos / información**

Protección de la Información

Copias de seguridad de los datos (backup)

Aseguramiento de la integridad

Cifrado de la información

Uso de firmas electrónicas

Uso de servicios de fechado electrónico (time stamping)

- **Protección de las aplicaciones (software)**

Protección de las Aplicaciones Informáticas

Copias de seguridad (backup)

Puesta en producción

Se aplican perfiles de seguridad

Explotación / Producción

Cambios (actualizaciones y mantenimiento)

Terminación

- **Protección de los equipos (hardware)**

Protección de los Equipos Informáticos

Puesta en producción

Se aplican perfiles de seguridad

Aseguramiento de la disponibilidad

Operación

Cambios (actualizaciones y mantenimiento)

Terminación

Informática móvil

Reproducción de documentos

Protección de la centralita telefónica (PABX)

- ✓ **Valoración de las salvaguardas**

Luego de tener el listado de salvaguardas, conviene determinar la eficacia sobre los activos considerando:

- La idoneidad de la salvaguarda para el fin perseguido
- Calidad de implantación
- Formación de los responsables de su configuración y operación
- Existencia de controles de medida de su efectividad.

El resultado de esta actividad se concreta en varios informes: declaración de aplicabilidad, evaluación de salvaguardas, y de insuficiencias o vulnerabilidades del sistema de protección. (Magerit-V3, Libro I - Método, 2012)

Las salvaguardas técnicas varían con el avance tecnológico ya que aparecen tecnologías nuevas y desaparecen antiguas; porque cambian los de tipo de activos a considerar; porque evolucionan las posibilidades de los atacantes o porque evoluciona el catálogo de salvaguardas disponibles.

La metodología Magerit da una valoración a las salvaguardas de la siguiente manera:

La valoración de la efectividad se ha realizado sobre una escala de 4 valores.
Se puede visualizar en la siguiente tabla 1.14 valoración de salvaguardas

Tabla 1.14. Valoración de Salvaguardas

EFECTIVIDAD	DESCRIPCIÓN
100% - 75%	Efectividad muy alta: Salvaguarda diseñada específicamente para la amenaza
74% - 50%	Efectividad alta: Reduce la frecuencia o la degradación de la amenaza sobre el activo significativamente.
49% - 25%	Efectividad Media: La salvaguarda tiene un impacto indirecto o general sobre la amenaza.
24% - 0%	Efectividad Baja: Tiene un impacto muy bajo sobre la amenaza o en el peor de los casos (0) no tienen ningún impacto sobre dicha amenaza.

Fuente: Libro II: Catalogo de elementos. Metodología Magerit

Vulnerabilidades

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial. Traducido a los términos empleados en los párrafos anteriores, son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre un activo. A veces se emplea el término "insuficiencia" para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza. (Magerit, 2012, pág. 35)

1.4. Alternativas de solución

Para la elaboración del análisis y gestión de riesgos de los activos tecnológicos, existen varias guías informales, aproximaciones metodológicas, estándares y herramientas de soporte que buscan gestionar y mitigar los riesgos. Las principales metodologías de análisis y gestión de riesgos de uso habitual en el mercado de la seguridad de las tecnologías de la información son: OCTAVE, CRAMM, IRAM, MAGERIT.

Metodologías de análisis de gestión de riesgos

1.4.1. Octave

Es la metodología de Evaluación de Amenazas Operacionalmente Críticas, Activos y Vulnerabilidades para agilizar y optimizar el proceso de evaluación de riesgos de seguridad de la información alineados a los objetivos y metas de la organización.

Existen tres metodologías publicadas: OCTAVE aplicable en organizaciones con más de 300 empleados, OCTAVE-S aplicable en organizaciones de hasta 100 empleados y OCTAVE Allegro que permite una amplia evaluación del entorno del riesgo operativo sin la necesidad de un amplio conocimiento de evaluación de riesgos y requiere menos tiempo de implementación.

1.4.2. Cramm

Es la metodología de análisis de riesgos desarrollado por la Agencia Central de Comunicación y Telecomunicación del gobierno británico. El significado del acrónimo proviene de ***CC****TA* ***R****isk* ***A****nalysis and* ***M****anagement Method*. Su versión inicial data de 1987 y la versión vigente es la 5.2. Al igual que Magerit, tiene un alto calado en administración pública británica, pero también en empresas e instituciones de gran tamaño. Dispone de un amplio reconocimiento.
La metodología de CRAMM incluye las siguientes 3 etapas:

- La primera de las etapas recoge la definición global de los objetivos de seguridad entre los que se encuentra la definición del alcance, la identificación y evaluación de los activos físicos y software implicados, la determinación del valor de los datos en cuanto a impacto en el negocio y la identificación.
- En la segunda etapa de la metodología se hace el análisis de riesgos, identificando las amenazas que afecta al sistema, así como las vulnerabilidades que explotan dichas amenazas y por último el cálculo de los riesgos de materialización de las mismas.
- En la tercera etapa se identifican y seleccionan las medidas de seguridad aplicadas en la entidad obteniendo los riesgos residuales, CRAMM proporciona una librería unas 3000 medidas de seguridad. (Huerta, 2012)

1.4.3. Iram

La norma IRAM-ISO 31000: 2018 recomienda que las organizaciones desarrollen, implementen y mejoren en forma continua una estructura, cuya finalidad sea integrar el proceso de Gestión de Riesgos, que colabora con las organizaciones y empresas a la hora de realizar una gestión integral de sus riesgos. Así, este documento les permite llevar a cabo una evaluación y tratamiento de los mismos de manera eficiente, aumentando la probabilidad de alcanzar sus objetivos, y mejorando, al mismo tiempo, la identificación de oportunidades y amenazas, así como la toma de decisiones a todo nivel.

La gestión de riesgos crea y protege el valor asegurando la viabilidad y el éxito de las organizaciones a largo plazo.

La norma IRAM 3801 ofrece lineamientos guía sobre la Estructura organizativa, Planificación e implementación, Evaluación de Riesgos, Medición del Desempeño y Auditoría, todos ellos necesarios para un efectivo sistema de gestión de SySO. Las pequeñas y medianas empresas (PyMEs) deben tener en cuenta que, si bien los principios generales tratados en esta norma se aplican a toda organización, deberán ser selectivas con los aspectos que se aplican directamente a ellas. Las organizaciones pequeñas necesitan primero asegurar que cumplen con los requisitos legales y luego en el tiempo apuntar al mejoramiento continuo. (Moyano, 2000)

1.4.4. Magerit

Es una de las metodologías más utilizadas que permite el análisis de gestión de riesgos de los Sistemas de Información; fue creada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información siguiendo la terminología de la norma ISO 31000. En el año 2012 se actualizó a la versión 3.

Los objetivos que busca alcanzar son:

- Hacer que los responsables de los sistemas de información sean conscientes de la existencia de riesgos y de la necesidad de tratarla a tiempo.
- Ofrecer un método sistemático para el análisis de riesgos.
- Ayudar en la descripción y planificación de las medidas adecuadas para mantener los riesgos bajo control.

- De forma indirecta, preparar la organización de los procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Para determinar por qué Magerit es una buena elección para el desarrollo del AGR se presenta un cuadro comparativo.

Tabla 1.15. Comparativa de Metodologías de Análisis y Gestión de Riesgos

	Tipo de análisis				
Metodología	**Cuantitativo**	**Cualitativo**	**Mixto**	**Análisis de Riesgos**	**Gestión de Riesgos**
MAGERIT	SI	SI	SI	SI	SI
OCTAVE	NO	NO	NO	SI	SI
CRAMM	SI	SI	NO	SI	SI
IRAM	SI	SI	NO	SI	SI

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito

Se ha analizado las metodologías para el análisis de gestión de riesgos y se ha catalogado a la metodología Magerit como la más apropiada sobre todo completa para el estudio de riesgos informáticos de la E.P.M.T.P.Q

CAPÍTULO 2. MARCO METODOLÓGICO

2.1. Tipo de investigación

En el presente proyecto se realizará una investigación a nivel exploratorio, con la finalidad de establecer los fundamentos del problema, diagnosticar las causas, condiciones, relaciones, fenómenos, componentes, entre otras.

Se establecen como métodos de análisis, la recopilación de información confiable y definición de variables.

- **Descriptiva**

La metodología de investigación será de tipo descriptiva, la misma que permitirá conocer la descripción correcta de las actividades que se desarrollan en la Gerencia de Tecnologías de la Información y los procedimientos que de cada uno de las competencias organizacionales.

- **Explicativa**

El análisis de la gestión de riesgos tecnológicos será de tipo explicativa a fin de determinar las relaciones causa-efecto; sobe el funcionamiento de la Empresa Pública Metropolitana de Transporte de Pasajeros de Quito y una investigación de tipo documental, mediante el análisis y revisión del material bibliográfico que fundamente teórica y técnicamente el diseño de la Gestión de Riesgos.

2.2. Recopilación de información

- **Método Inductivo – Deductivo**

La investigación se realizará mediante el método inductivo deductivo, siendo que va de lo general a lo particular en el hallazgo de respuestas o soluciones de un problema, desde su inicio, mediante el análisis busca formas posibles para una solución.

Inductivo

Con lo que respecta a la inducción se plantea de la lógica de los hechos particulares a los generales, obtenidos mediante el estudio de encuestas o de casos a partir del diseño de hipótesis para la generación de resultados, este resultado se logra a través de los hechos empíricos con el objetivo es alcanzar nuevos conocimientos más estructurados, enfocados en la realidad inmediata atados a una realidad directa o indirecta.

- **Deductivo**

  En el contexto de la investigación por deducción trata de ir de lo general a lo particular, como algunos autores lo llaman el método del descenso, considerando axiomas como respaldo a la necesidad de una prueba lógica o a un punto de vista lógico, sin embargo, el método deductivo aporta con valiosas colaboraciones a la ciencia mediante casos generales a particulares, encontrando principios desconocimos, no analizados mediante la utilización de otros conocidos. (Tena & Rivas, 1995, pág. 84)

2.2.1. Técnicas de recopilación de información

La recopilación de la información se realizó a través de encuestas, donde se encuesto a un grupo de personas de la EPMTPQ, puede visualizar el modelo de encuesta que se realizó para la recolección de información en el **ANEXO A**

Tabulación de la encuesta

De acuerdo a la información recopilada se realizó la tabulación de las encuestas a fin de obtener los resultados de las mismas lo cual se logró establecer los problemas que presenta actualmente la empresa, las cuales podrá visualizar en el **ANEXO B**.

CAPÍTULO 3. PROPUESTA

3.1. Diagnóstico de la situación actual

La Empresa Pública Metropolitana de Transportes de Pasajeros de Quito, cuenta con varios sistemas de información, entre los cuales se encuentra el Sistema de Nómina SIAP y el Sistema de control de asistencia SIRHA Time que tiene como objetivo realizar el pago a los empleados y el control de asistencia biométrica, utilizando servidores para el flujo e intercambio de la información a través de una red que conecta a las diferentes áreas. Así mismo permiten el acceso a través de la intranet para ingresar y solicitar permisos personales, médicos, laborales y calamidades domésticas.

El problema que se presenta es la falta de interés y/o de tiempo de las personas encargadas de revisar periódicamente las cuentas y permisos de acceso establecidos, con el fin de establecer los accesos de cada persona, de acuerdo a las necesidades de la EPMTPQ, la pérdida de información de datos almacenados en dispositivos propios de los empleados, la falta de conocimiento del personal en el cambio de roles, funciones o cargos de un funcionario, que requiera acceso a diferente información o infraestructura tecnológica de la EPMTPQ y la falta de control de seguridad de los activos tecnológicos en especial con los relojes biométricos.

A) Entorno físico

El control de acceso al edificio se resguarda por 1 puerta, tiene un detector de huellas; una persona en recepción se encarga de llevar un control de personal que ingresa y sale del edificio un guardia de seguridad, Además, hay cámaras de seguridad instaladas.

En el centro de datos se componen por cinco armarios: cuatro armarios son abiertos donde se encuentran los equipos de comunicaciones y servidores de tipo rack y un armario con puerta.

B) Infraestructura

La organización cuenta con una conexión permanente de Internet a través de enlace fibra óptica con el proveedor, protegido por un enlace de respaldo; y una red estrella de fibra óptica que conecta a las diferentes áreas.

3.2. Factibilidad técnica

Para el desarrollo de la gestión de riesgos se utilizará la metodología Magerit v3, y un computador equipado con las siguientes herramientas: El sistema operativo Windows, con su respectiva hoja de cálculo Excel para el análisis de los cálculos.

3.3. Factibilidad operacional

El caso estudio estará desarrollado en base a la metodología Magerit. Debido al diseño no demanda un equipo con grandes recursos de cómputo.

En cuanto a la factibilidad operativa a nivel de recurso humano, las personas a cargo del proyecto se encuentran capacitadas y se tiene acceso a bibliografía relevante para el desarrollo tanto del caso estudio.

3.4. Factibilidad económica-financiera

La factibilidad económica discriminada por recursos de hardware, software y recurso humano. Se determina que el proyecto es económicamente factible.

Tabla 3.1. Recursos utilizados para el análisis de riesgos

	Recursos	Proveedor	Costo
Hardware	1. Laptop Características: Memoria RAM 8 GB Procesador 2.2 GHz Disco Duro: 1 TB Sistema Operativo: Windows 7, 8,10	Personal	$1.500
Personal	Técnico	1 Técnico salario mensual 901 x 3 meses	$2.703
Otros	Transporte, Alimentación		$300
Imprevistos			$500
		TOTAL	**$4.703**

Fuente: Propia

3.5. Plan de gestión de riesgos

Para la realización del plan de gestión de riesgos se ha utilizado el diagrama de Gantt, que es una herramienta que se emplea para planificar y programar tareas a lo largo de un período determinado de tiempo, permite realizar el seguimiento y control del progreso de cada una de las etapas de un proyecto.

El Plan se lo divide en 4 etapas: prerrequisitos, inicio, desarrollo y operaciones.

- En la etapa de prerrequisitos, se realiza el levantamiento de requerimientos de bienes y se planteará objetivos de acuerdo a las necesidades a finalidad de que sean cumplidos, se lleva a cabo mediante reuniones con el personal de la Gerencia de Tecnologías, conformados por el Ing. Dennis Cueva, Ing. Julia Escobar, Ing. Sandro Enríquez y el Ing. Michael Ruiz, conjuntamente con dos delegados de la Coordinación de Logística e Insumos, Unidad de Bienes, el Ing. Alejandro Muñoz y el Tlgo. Javier Escobar.
- En la etapa de inicio, se determina la documentación, materiales, equipos con la que se realiza la aplicación de la metodología Magerit y la caracterización de activos según su grupo, esto se lo realiza conjuntamente con el personal de la Gerencia de Tecnologías y de la Coordinación de Logística e Insumos en un tiempo aproximado de un mes.
- En la etapa de desarrollo, se sigue la metodología Magerit de los libros I, II, se elabora una matriz en Excel en donde se registran todos los activos más relevantes de la empresa, la valoración de los mismos, se identifican las amenazas a los que se encuentren expuestos de acuerdo al listado de amenazas **ANEXO C**, se identificará el riesgo y la valoración de los mismos de acuerdo a la fórmula que establece la metodología Magerit, se visualizan los riegos según la escala de colores baja, media y alta, e inmediatamente se escogen las salvaguardas de acuerdo a los riegos arrojados mediante la matriz de riegos, esto se realiza con el personal antes mencionado.
- En la última etapa, se elabora conjuntamente con el Ing. Dennis Cueva y el Ing. Sandro Enríquez quienes son las personas indicadas para la elaboración del plan de seguridad de acuerdo a la matriz de riesgo (activos con mayores riesgos) y se realizan las respectivas fichas de componentes con su justificación y las acciones que se deberían aplicar a fin de mitigar los riesgos, y por último se realiza la capacitación del plan de gestión de riesgo.

Nombre	Recursos	Fecha de inicio	Fecha de fin	Duración	Estado
PRE-REQUISITOS		01/04/19	01/04/19	0	
Reunión levantamineto de requerimientos con el presonal del área	Personas	02/04/19	08/04/19	5	Completada
Definir los objetivos	Personas y PC	15/04/19	24/04/19	8	Completada
INICIO		24/04/19	24/04/19	0	
Determinar los documentación (analizar riesgos)	Personal técnico, laptops, documentación	26/04/19	07/05/19	8	Completada
Requisitos de Hardware	Personas, servidores, impresoras, telefonos etc.	08/05/19	16/05/19	7	Completada
Caracterización de activos Software y Hardware	Cuaderno de apuntes, esfero y laptos	17/05/19	07/06/19	16	Completada
DESARROLLO		10/06/19	10/06/19	0	
Identificación de los activos	Laptop, Excel, Personas, Libro I Magerit	11/06/19	18/06/19	6	Completada
Valoración de los activos	Libro II Magerit, Listado de activos, personas	19/06/19	26/06/19	6	Completada
Identificación de las amenazas	Laptop, Excel, Libro II Magerit, Personas	27/06/19	04/07/19	6	Completada
Valoración de las amenazas	Libro II Magerit, Listado de amenazas, personas	05/07/19	12/07/19	6	Completada
Identificación del riesgo	Laptop, mariz de riesgo, Libro II Magerit, Personas	15/07/19	22/07/19	6	Completada
Valoración del riesgo	Libro II Magerit, Tablas de riego, personas	23/07/19	30/07/19	6	Completada
Identificación de las salvaguardas	Laptop, Excel, Libro III Magerit, Personas	01/08/19	14/08/19	10	Completada
Valoración de salvaguardas	Listado de salvaguardas, personas	15/08/19	21/08/19	5	
OPERACIONES		22/08/19	22/08/19	0	
Plan de Seguridad (activos con mayor riesgo)	Laptop, Libro III Magerit, perosna	26/08/19	11/09/19	13	Completada
Fichas de Componentes	Laptop, persona, matriz de riesgo, personal técnico	12/09/19	18/09/19	5	Completada
Capacitación del Plan de Gestión de riesgo tecnológicos	Peronas, laptop, cuadernos, proyector, diapositivas	19/09/19	23/09/19	3	Completada

Figura 3.1. Plan de gestión de riesgos, diagrama de Gantt

Fuente: Diagrama de Gantt

3.6. MAGERIT

MAGERIT v.3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de Administraciones públicas, Magerit, es un método formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Objetivos de Magerit

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- Determinar a qué amenazas están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenas, obteniendo unos resultados. (Bolaños, 2014)

CAPÍTULO 4. IMPLEMENTACIÓN

4.1. Aplicación del modelo, estándar o metodología

En este capítulo se detalla la aplicación de la metodología Magerit mediante:

- Método de Análisis de riesgos (**MAR**)

Adaptando la estructura de procesos, actividades y tareas que plantea Magerit, ya antes mencionadas en el capítulo anterior, a la estructura diseñada en la presente tesis.

Teniendo en cuenta que se realiza un análisis cualitativo para la identificación de activos tecnológicos y la evaluación de los riesgos y así mitigar los mismos para la evaluación de riesgos mediante matrices, es decir no se recibe ningún pago por su uso, lo cual hace que el estudio no se centre en aumentar ganancias y disminuir perdidas sino en plantear mejoras en la seguridad informática de los bienes activos tecnológicos de la EPMTPQ.

El desarrollo del proyecto de análisis y gestión de riesgo de los activos tecnológicos se realiza mediante la metodología Magerit y con el uso matrices elaboradas en Excel. Por lo cual se muestra el desarrollo de la metodología y por ende los resultados en diagramas apropiados

4.2. Diseño

4.2.1. Tarea 1: Identificación y valoración de los Activos de la E.P.M.T.P.Q

La tarea tiene como objetivo, identificar los activos más relevantes de la EPMTPQ, así mismo de realizar una valoración según la importancia que tenga cada activo para el caso de estudio de acuerdo a la metodología Magerit, en la siguiente tabla de identificarán y se clasificarán los activos informáticos por tipo y con su respectiva descripción.

La identificación de activos es importante ya que permite valorar los activos con exactitud a fin de identificar y valorar las amenazas.

- **Identificación de los Activos de la E.P.M.T.P.Q**

Tabla 4.1 Listado de activos importantes pertenecientes a la EPMTPQ

LISTADO DE ACTIVOS	
[D]DATOS / INFORMACIÓN	COPIA DE RESPALDO
	DATOS DE ACCESO A SERVIDORES
	DATOS DE ACCESO A USUARIOS
	CÓDIGOS FUENTES SW
[IS] SERVICIOS INTERNOS	SERVICIO DE INTERNET
	SERVICIO DE TELEFONÍA
	SERVICIO DE MANTENIMIENTO
[SW] SOFTWARE(APLICACIONES INFORMÁTICAS)	OFIMÁTICA
	ANTIVIRUS
	SISTEMA BIOMÉTRICO SIRHA
	SISTEMA DE GESTIÓN DE BASE DE DATOS
	SERVIDOR DE CORREO(APLICACIÓN DE RED)
	SISTEMA DE NÓMINA SIAP
	SOFTWARE NETWORKING
[HW] HARDWARE (EQUIPOS INFORMÁTICOS)	COMPUTADORAS DE ESCRITORIO
	COMPUTADORAS PERSONALES
	IMPRESORAS
	SWITCH
	FIREWALL
	ROUTER
	ACCESS POINT
	RELOJES BIOMÉTRICOS
	SERVIDORES FÍSICOS
[COM] REDES DE COMUNICACIONES	TELEFONÍA IP
	RED LAN
	RED WIFI
	INTERNET
[AUX] EQUIPOS AUXILIARES	CABLEADO
	PLANTA ELÉCTRICA
	UPS
	FUENTES DE ALIMENTACIÓN
	FIBRA ÓPTICA
[SS] SERVICIOS SUBCONTRATADOS	SISTEMA SIRHA(SISTEMA BIOMÉTRICO)
	SISTEMA SIAP(NÓMINA ROL DE PAGOS)
[L] INSTALACIONES	OFICINAS
	VEHÍCULOS
	ESTACIONES TROLEBÚS Y ECOVIA
[P] PERSONAL	COORDINADOR DE SISTEMAS INFORMÁTICOS
	COORDINADOR DE REDES Y TELECOMUNICACIONES
	ESPECIALISTAS DE TECNOLOGÍAS 2
	ESPECIALISTA DE BIENES 2
	TÉCNICOS ADMINISTRATIVO DE BIENES
	ESPECIALISTA DE TELECOMUNICACIONES 4
	COORDINADORA DE TALENTO HUMANO
	COORDINADORA DE SEGURIDAD

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito.

La tarea tiene como objetivo, identificar los activos dentro del dominio, determinando sus características y atributos del activo a tratar que son el código, nombre y una descripción.

Para el desarrollo de la tarea se toma en cuenta lo siguiente:

- Como código se considera letras que en su mayor parte son las primeras letras de las palabras que forman el nombre de cada activo.
- Para los nombres se considera la actividad principal o el software que tenían instalados que formaban parte del objeto de estudio.
- En la descripción se considera el mismo caso que en el de los nombres.

De acuerdo a las reuniones mantenidas con el personal de TIC'S sea logrado concluir los activos más importantes de la E.P.M.T.P.Q, destacado un valor de cada activo.

Personal que conformo las reuniones.

Ing. Richard Salas, Gerente de Tecnologías de la Información

Ing. Erick Cerón, Coordinador de Soluciones Tecnológicas, Redes y Comunicaciones

Ing. Byron Viera, Coordinador de Proyectos Informáticos.

Ing. Dennis Cueva, Especialista de Tecnologías 2.

Ing. Sandro Enríquez, Especialista de Tecnologías 2.

Ing. Julia Escobar, Especialista de Tecnologías 1.

Ing. Michael Ruiz, Especialista de Tecnologías 2.

Conjuntamente con el personal del departamento de tecnologías se ha determinado los activos esenciales a través de análisis de procesos de acuerdo a la lógica del negocio.

[D] DATOS/INFORMACIÓN

Toma los activos correspondientes a los datos de la organización, los cuales son el núcleo de la organización, esté activo en sí es un activo abstracto que será constantemente manipulado y almacenado en los equipos de cómputo.

- [COPRESP_EPQ] COPIA DE RESPALDO
- [DACCSER_EPQ] DATOS DE ACCESO SERVIDORES
- [DACCUSR_EPQ] DATOS ACCESO USUARIOS
- [CODFUSW_EPQ] CODIGOS FUENTE SW

[IS] SERVICIOS INTERNOS

Esta función recoge los activos esenciales a nivel interno en la organización es decir los activos que involucran al personal y por lo tanto satisfacen sus necesidades elementales para poder realizar su labor.

- [SERVINT_EPQ] SERVICIO DE INTERNET
- [SERVTLF_EPQ] SERVICIO DE TELEFONÍA
- [SERMANT_EPQ] SERVICIO DE MANTENIMIENTO

[SW] SOFTWARE (APLICACIONES INFORMÁTICAS)

Esta función recoge los activos esenciales a nivel lógico en la organización es decir los activos que involucran al de software.

- [OFIMATI_EPQ] OFIMÁTICA
- [ANTIVIR_EPQ] ANTIVIRUS
- [SISBIOM_EPQ] SISTEMA BIOMÉTRICO SIRHA
- [SISGEBD_EPQ] SISTEMA DE GESTIÓN DE BASE DE DATOS
- [SERCORR_EPQ] SERVIDOR DE CORREO (APLICACIÓN DE RED)
- [SISSIAP_EPQ] SISTEMA DE NÓMINA SIAP
- [SWNETWO_EPQ] SOFTWARE NETWORKING

[HW] HARDWARE (EQUIPOS INFORMÁTICOS)

Esta función recoge los activos esenciales a nivel físico en la organización es decir los activos que involucran al de hardware.

- [COMPESC_EPQ] COMPUTADORAS DE ESCRITORIO
- [COMPERS_EPQ] COMPUTADORAS PERSONALES
- [IMPLASE_EPQ] IMPRESORAS
- [SWITCH_EPQ] SWITCH
- [FIREWAL_EQP] FIREWALL
- [ROUTER_EQP] ROUTER
- [ACPOINT_EPQ] ACCESS POINT
- [RELOBIOM_EPQ] RELOJES BIOMÉTRICOS
- [SERVFIS_EPQ] SERVIDORES FÍSICOS

[COM] REDES DE COMUNICACIONES

Esta función recoge los activos a nivel de comunicaciones, que son básicos para la comunicación a nivel organizacional.

- [TELTIP_EPQ] TELEFONÍA IP
- [REDLAN_EPQ] RED LAN
- [REDWIFI_EPQ] RED WIFI
- [INTERET_EPQ] INTERNET

[AUX] EQUIPOS AUXILIARES

Esta función recoge los activos suplementarios que, aunque no son de primera necesidad si cumplen una funcionalidad necesaria e importante.

- [CABLEAD_EPQ] CABLEADO
- [PLAELEC_EPQ] PLANTA ELÉCTRICA
- [UPS_EPQ] UPS
- [FUENALI_EPQ] FUENTES DE ALIMENTACIÓN
- [FIBROPT_EPQ] FIBRA ÓPTICA

[SS] SERVICIOS SUBCONTRATADOS

- [SISSIRHA_EPQ] SISTEMA SIRHA (SISTEMA BIOMÉTRICO)
- [SISSIAP_EPQ] SISTEMA DE NÓMINA SIAP (ROL DE PAGOS)

[L] INSTALACIONES

Esta función recoge los activos físicos a nivel de instalaciones físicas de la organización.

- [OFICINA_EPQ] OFICINAS
- [VEHICUL_EPQ] VEHÍCULOS
- [ESTROECV_EPQ] ESTACIONES TROLEBÚS Y ECOVIA

[P] PERSONAL

Esta función recoge los activos de personal y desarrollo humano en la organización

- [COORSIN_EPQ] COORDINADOR DE SISTEMAS INFORMÁTICOS
- [COORTEL_EPQ] COORDINADOR DE REDES Y TELECOMUNICACIONES
- [ESPTEC2_EPQ] ESPECIALISTAS DE TECNOLOGÍAS 2
- [ESPBIE2_EPQ] ESPECIALISTA DE BIENES 2

- [TECBIEN_EPQ] TÉCNICOS ADMINISTRATIVO DE BIENES
- [ESPTEL4_EPQ] ESPECIALISTA DE TELECOMUNICACIONES 4
- [COORTH2_EPQ] COORDINADORA DE TALENTO HUMANO
- [COORSEG_EPQ] COORDINADORA DE SEGURIDAD

❖ Valoración de los Activos

La valoración de los activos permite evaluar el nivel de protección que debe tener un activo, desde luego es necesario dar un valor dependiendo del nivel de importancia y el valor que tiene dentro de la organización. Se debe dar un nivel de protección que en Magerit es dado por las dimensiones de seguridad. Estas dimensiones son dadas de la siguiente manera:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad
- Trazabilidad

A través de esa metodología los activos deben ser valorados de acuerdo al siguiente criterio que fue establecido mediante las reuniones con el personal de TIC'S:

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

Tabla 4.2. Criterios de valoración

Valor			Criterio
10	Muy Alto	MA	Daño muy grave a la organización
7-9	Alto	A	Daño grave a la organización
4-6	Medio	M	Daño importante a la organización
1-3	Bajo	B	Daño menor a la organización
0	Despreciable	D	Irrelevante a efectos prácticos

Fuente: Libro II. Catálogo de elementos. Metodología Magerit.

De acuerdo a la tabla de valoración de activos se va realizar la evaluación de los activos identificados con anterioridad.

Se ha analizado con el personal de sistemas y se ha definido que se valorara a los activos en las siguientes dimensiones.

Dimensiones o Variables

- **[D]** Disponibilidad
- **[I]** Integridad de los datos
- **[C]** Confidencialidad de los datos

En esta tabla se muestra la valoración de los activos de la Empresa Pública Metropolitana de Transportes de pasajeros de Quito, la tabla desarrollada permite ver el valor que tiene los activos en cada una de las variables de seguridad; la tabla de valoración que surge es la siguiente teniendo en cuenta la importancia que tiene cada activo se ha valorado en escala del 1 al 10 y realizando la suma total de cada variable a fin de obtener el valor que tiene cada activo.

Tabla 4.3. Valoración de los activos

ITEM	DESCRIPCIÓN DEL ACTIVO	VALORACIÓN			VALORACIÓN DEL ACTIVO(C+I+D)
		[C]	[I]	[D]	
[D] DATOS/INFORMACIÓN					
1	COPIA DE RESPALDO	9	9	10	28
2	DATOS DE ACCESO A SERVIDORES	9	9	9	27
3	DATOS DE ACCESO A USUARIOS	9	9	9	27
4	CÓDIGOS FUENTES SW	9	9	9	27
[IS] SERVICIOS INTERNOS					
5	SERVICIO DE INTERNET	7	8	9	24
6	SERVICIO DE TELEFONÍA	8	7	7	22
7	SERVICIO DE MANTENIMIENTO	0	7	6	13
[SW] SOFTWARE(APLICACIONES INFORMÁTICAS)					
8	OFIMÁTICA	6	7	7	20
9	ANTIVIRUS	4	6	7	17
10	SISTEMA BIOMÉTRICO SIRHA	4	7	7	18
11	SISTEMA DE GESTIÓN DE BASE DE DATOS	7	6	6	19
12	SERVIDOR DE CORREO(APLICACIÓN DE RED)	7	6	6	19
13	SISTEMA DE NÓMINA SIAP	8	7	7	22
14	SOFTWARE NETWORKING	6	6	6	18
[HW] HARDWARE (EQUIPOS INFORMÁTICOS)					
15	COMPUTADORAS DE ESCRITORIO	6	9	9	24
16	COMPUTADORAS PERSONALES	6	9	9	24

17	IMPRESORAS	4	6	7	17
18	SWITCH	4	6	7	17
19	FIREWALL	7	8	9	24
20	ROUTER	5	7	7	19
21	ACCESS POINT	6	7	7	20
22	RELOJES BIOMÉTRICOS	5	9	9	23
23	SERVIDORES FÍSICOS	5	6	7	18
[COM] REDES DE COMUNICACIONES					
24	TELEFONÍA IP	8	6	6	20
25	RED LAN	5	5	5	15
26	RED WIFI	6	7	7	20
27	INTERNET	6	5	5	16
[AUX] EQUIPOS AUXILIARES					
28	CABLEADO	6	5	5	16
29	PLANTA ELÉCTRICA	0	9	10	19
30	UPS	5	5	6	16
31	FUENTES DE ALIMENTACIÓN	4	4	4	12
32	FIBRA ÓPTICA	6	7	7	20
[SS] SERVICIOS SUBCONTRATADOS					
33	SISTEMA SIRHA(SISTEMA BIOMÉTRICO)	4	7	7	18
34	SISTEMA SIAP(NÓMINA ROL DE PAGOS)	8	7	7	22
[L] INSTALACIONES					
35	OFICINAS	0	0	8	8
36	VEHÍCULOS	0	0	8	8
37	ESTACIONES TROLEBÚS Y ECOVIA	0	0	8	8
[P] PERSONAL					
38	COORDINADOR DE SISTEMAS INFORMÁTICOS	3	6	7	16
39	COORDINADOR DE REDES Y TELECOMUNICACIONES	3	6	7	16
40	ESPECIALISTAS DE TECNOLOGÍAS 2	2	6	7	15
41	ESPECIALISTA DE BIENES 2	2	4	5	11
42	TÉCNICOS ADMINISTRATIVO DE BIENES	2	4	5	11
43	ESPECIALISTA DE TELECOMUNICACIONES 4	2	5	5	12
44	COORDINADORA DE TALENTO HUMANO	5	6	4	15
45	COORDINADORA DE SEGURIDAD	4	4	5	13

Fuente: Empresa Pública Metropolitana de Transportes de Pasajeros de Quito.

4.2.2. Tarea 2: Identificación y Valoración de las Amenazas

Se busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado

(degradación). Se puede decir que el objetivo de esta tarea es caracterizar el entorno al que se enfrenta el sistema y qué acciones pueden suceder.

El objetivo de la tarea es identificar las amenazas relevantes sobre cada activo.

La metodología Magerit indica que las amenazas están clasificadas en cuatro grupos:

- **[N] Desastres Naturales**
- **[1] De origen industrial**
- **[E] Errores y fallos no intencionados**
- **[A]Ataque deliberados**

Para verificar la tabla del listado de amenazas según la metodología Magerit V3 libro II catálogo de elementos, dirigirse al **ANEXO C**

❖ **Identificación de las Amenazas**

El origen de cada una de las amenazas utilizadas en la siguiente tabla es a partir del listado de las amenazas extraídas de la metodología Magerit, las mismas que se identificaron de acuerdo al criterio del personal del área de tecnologías.

En la tabla adjunta se identifican las amenazas sobre cada activo de acuerdo la lista de amenazas del Libro Magerit II, esto se realizó de acuerdo a las amenazas que estaría expuestos los activos tanto software como hardware.

Tabla 4.4. Identificación de amenazas

	ACTIVOS	AMENAZA
[D] DATOS/INFORMACIÓN	COPIA DE RESPALDO	[E.1] Errores de los usuarios [E.2] Errores del administrador
	DATOS DE ACCESO A SERVIDORES	[E.7] Deficiencias en la organización [A.4] Manipulación de la configuración [A.5] Suplantación de la identidad del usuario [A.11] Acceso no autorizado
	DATOS DE ACCESO A USUARIOS	[A.5] Suplantación de la identidad del usuario [A.11] Acceso no autorizado
	CÓDIGOS FUENTES SW	[E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario
[IS] SERVICIOS INTERNOS	SERVICIO DE INTERNET	[I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios y suministros esenciales [A.7] Uso no previsto
	SERVICIO DE TELEFONÍA	[E.1] Errores de los usuarios [E.2] Errores del administrador [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios y suministros esenciales
	SERVICIO DE MANTENIMIENTO	[E.7] Deficiencias en la organización [E.21] Errores de mantenimiento / actualización de programas (software) [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.28] Indisponibilidad del personal
[SW] SOFTWARE(APLICACIONES INFORMÁTICAS)	OFIMÁTICA	[E.21] Errores de mantenimiento / actualización de programas (software) [E.1] Errores de los usuarios
	ANTIVIRUS	[E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software)
	SISTEMA BIOMÉTRICO SIRHA	[I.5] Avería de origen físico o lógico [E.15] Alteración accidental de la información [E.21] Errores de mantenimiento / actualización de programas (software)

		[A.5] Suplantación de la identidad del usuario [A.24] Denegación de servicio
	SISTEMA DE GESTIÓN DE BASE DE DATOS	[I.5] Avería de origen físico o lógico [E.15] Alteración accidental de la información [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario
	SERVIDOR DE CORREO(APLICACIÓN DE RED)	[I.5] Avería de origen físico o lógico [E.15] Alteración accidental de la información [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario
	SISTEMA DE NÓMINA SIAP	[I.5] Avería de origen físico o lógico [E.15] Alteración accidental de la información [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario [A.24] Denegación de servicio
	SOFTWARE NETWORKING	[I.5] Avería de origen físico o lógico [E.15] Alteración accidental de la información [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario
[HW] HARDWARE (EQUIPOS INFORMÁTICOS)	COMPUTADORAS DE ESCRITORIO	[N.1]Fuego [N.2]Daños por agua [N. *]Desastres naturales [1.3]Contaminación ambiental [I.5]Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento hardware/ actualización de programas hardware [A.11]Acceso no autorizado [A.23]Manipulación del hardware
	COMPUTADORAS PERSONALES	[N.1]Fuego [N.2]Daños por agua [N. *]Desastres naturales [1.3]Contaminación ambiental [I.5]Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento hardware/ actualización de programas hardware

	[A.11]Acceso no autorizado [A.23]Manipulación del hardware
IMPRESORAS	[I.5]Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperatura o humedad [E.23]Errores de mantenimiento hardware/ actualización de programas hardware [A.11]Acceso no autorizado
SWITCH	[N.1]Fuego [N.2]Daños por agua [I.6]Corte del suministro eléctrico [E.21]Errores de mantenimiento software/ actualización de programas software [A.6]Abuso de privilegios de acceso [A.11]Acceso no autorizado [A.25]Robo de equipos [A.26]Ataque destructivos
FIREWALL	[I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad
ROUTER	[N.1]Fuego [N.2]Daños por agua [I.6]Corte del suministro eléctrico [E.21]Errores de mantenimiento software/ actualización de programas software [A.6]Abuso de privilegios de acceso [A.11]Acceso no autorizado [A.25]Robo de equipos [A.26]Ataque destructivos
ACCESS POINT	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.5] Avería de origen físico o lógico [E.4] Errores de configuración
RELOJES BIOMÉTRICOS	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [A.11]Acceso no autorizado [A.25] Robo
SERVIDORES FISICOS	[N.1]Fuego [N.2]Daños por agua [N. *]Desastres naturales [1.3]Contaminación ambiental [I.5]Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento hardware/ actualización de programas hardware [A.11]Acceso no autorizado

		[A.23]Manipulación del hardware
[COM] REDES DE COMUNICACIONES	TELEFONÍA IP	[1.8]Fallo de servicios de comunicaciones [E.9]Errores de re-encaminamiento [E.15] Alteración de la información [E.19]Fugas de información [A.7]Uso no previsto [A.9]Encaminamiento de mensajes [A.10]Alteración de secuencia [A.12]Análisis de trafico [A.14]1nterceptación de información (escucha)
	RED LAN	[I.8]Fallo de servicios de comunicaciones [E.9]Errores de re-encaminamiento [E.10]Errores de secuencia [A.5]Suplantación de la identidad [A.9]Encaminamiento de mensajes [A.10] Alteración de secuencia [A.11]Acceso no autorizado
	RED WIFI	[I.8]Fallo de servicios de comunicaciones [E.9]Errores de re-encaminamiento
	INTERNET	[I.8]Fallo de servicios de comunicaciones [E.15] Alteración de la información
[AUX] EQUIPOS AUXILIARES	CABLEADO	[I.11] Emanaciones electromagnéticas [I.1] Fuego [I.2] Daños por agua [I.7] Condiciones inadecuadas de temperatura o humedad [I.11] Emanaciones electromagnéticas [I.*] Desastres industriales [A.25] Robo
	PLANTA ELÉCTRICA	[I.1] Fuego [I.2] Daños por agua [I.9] Interrupción de otros servicios y suministros esenciales [I.*] Desastres industriales [A.25] Robo
	UPS	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [A.25] Robo
	FUENTES DE ALIMENTACIÓN	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales

		[A.25] Robo
	FIBRA ÓPTICA	[I.1] Fuego [I.2] Daños por agua [I.7] Condiciones inadecuadas de temperatura o humedad [I.*] Desastres industriales [A.25] Robo
[SS] SERVICIOS SUBCONTRATADOS	SISTEMA SIRHA(SISTEMA BIOMÉTRICO)	[I.5] Avería de origen físico o lógico [E.15] Alteración accidental de la información [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario [A.24] Denegación de servicio
	SISTEMA SIAP(NÓMINA ROL DE PAGOS)	[I.5] Avería de origen físico o lógico [E.15] Alteración accidental de la información [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario [A.24] Denegación de servicio
[L] INSTALACIONES }	OFICINAS	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [A.26]Ataque destructivos [A.27] Ocupación enemiga
	VEHÍCULOS	[I.1] Fuego [I.2] Daños por agua [A.26]Ataque destructivos [I.*] Desastres industriales
	ESTACIONES TROLEBÚS Y ECOVIA	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [A.26]Ataque destructivos [A.27] Ocupación enemiga
[P] PERSONAL	COORDINADOR DE SISTEMAS INFORMÁTICOS	[E.7]Deficiencias en la organización [E.14]Fugas de información (>E.19) [A.6] Abuso de privilegios de acceso [A.18] Destrucción de información [A.29]Extorsión [A.30] ingeniería social (picaresca)
	COORDINADOR DE REDES Y TELECOMUNICACIONES	[E.7]Deficiencias en la organización [E.14]Fugas de información (>E.19) [A.6] Abuso de privilegios de acceso

	[A.18] Destrucción de información [A.29]Extorsión [A.30] ingeniería social (picaresca)
ESPECIALISTAS DE TECNOLOGÍAS 2	[E.7]Deficiencias en la organización [E.14]Fugas de información (>E.19) [A.6] Abuso de privilegios de acceso [A.18] Destrucción de información [A.29]Extorsión [A.30] ingeniería social (picaresca)
ESPECIALISTA DE BIENES 2	[E.7]Deficiencias en la organización [E.14]Fugas de información (>E.19) [A.6] Abuso de privilegios de acceso [A.18] Destrucción de información [A.29]Extorsión [A.30] ingeniería social (picaresca)
TÉCNICOS ADMINISTRATIVO DE BIENES	[E.7]Deficiencias en la organización [E.14]Fugas de información (>E.19) [A.6] Abuso de privilegios de acceso [A.18] Destrucción de información [A.29]Extorsión [A.30] ingeniería social (picaresca)
ESPECIALISTA DE TELECOMUNICACIONES 4	[E.7]Deficiencias en la organización [E.14]Fugas de información (>E.19) [A.6] Abuso de privilegios de acceso [A.18] Destrucción de información [A.29]Extorsión [A.30] ingeniería social (picaresca)
COORDINADORA DE TALENTO HUMANO	[E.7]Deficiencias en la organización [E.14]Fugas de información (>E.19) [A.6] Abuso de privilegios de acceso [A.18] Destrucción de información [A.29]Extorsión [A.30] ingeniería social (picaresca)
COORDINADORA DE SEGURIDAD	[E.7]Deficiencias en la organización [E.14]Fugas de información (>E.19) [A.6] Abuso de privilegios de acceso [A.18] Destrucción de información [A.29]Extorsión [A.30] ingeniería social (picaresca)

Fuente: Empresa Pública Metropolitana de Transportes de pasajeros de Quito

❖ **Valoración de las Amenazas**

Los objetivos planteados en esta tarea son:

- Evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo.
- Estimar la degradación que causaría en cada dimensión del activo si llegara a materializarse

Para valorar las amenazas de cada activo se han tomado en cuenta la degradación de valor y la probabilidad de ocurrencia.

Tabla 4.5. Degradación o impacto del valor

FRECUENCIA	DESCRIPCIÓN
5	Muy Alta
4	Alta
3	Medio
2	Baja
1	Sin degradación o impacto

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito.

Por otro lado, medir la probabilidad se puede medir de la siguiente manera:

Tabla 4.6. Probabilidad de ocurrencia o frecuencia

FRECUENNCIA	DESCRIPCIÓN	
5	Muy frecuente	a diario
4	Frecuente	Mensualmente
3	Normal	Una vez al año
2	Poco frecuente	Cada varios años
1	Nunca Ocurre	Siglos

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito.

En el **ANEXO D** se observa las diferentes amenazas a las que están expuestos los activos.

4.2.3. Tarea 3: Identificación y Valoración del Riesgo

Las amenazas identificadas corresponden al listado que suministran la Metodología Magerit en su Libro II. Catálogo de elementos

Los riesgos asociados a las amenazas son los riesgos más comunes que se generarán por cada una de las mismas; se hace la aclaración ya que por una misma amenaza se pueden generar múltiples riesgos, pero solamente se tratan los más importantes y comunes.

- **Valoración del Riesgo**

En el siguiente cuadro se identifican y valoran los riesgos más importantes a los que están expuestos los activos de la E.P.M.T.P.Q.

La tabla de la valoración de riesgos dirigirse al **ANEXO E**

4.2.4. Tarea 4: Identificación y valoración de salvaguardas

Permite identificar y valorar las salvaguardas a fin de mitigar las amenazas a las que están expuestos los activos de la E.P.M.T.P.Q.

- **Identificación de las salvaguardas**

Esto se logra analizando los riesgos que tal altos son y cuánto podría afectar a la empresa a fin de escoger una determinada salvaguarda de acuerdo a cada activo.

- **Protección de los datos / información**

Protección de la Información

Copias de seguridad de los datos (backup)

- **Protección de las aplicaciones (software)**

Se aplican perfiles de seguridad

- **Protección de los equipos (hardware)**

Protección de los Equipos Informáticos.

- **Tarea Valoración de las salvaguardas**

En el siguiente cuadro se identifican y valoran los riesgos más importantes a los que están expuestos los activos de la E.P.M.T.P.Q, según las amenazas a las que está expuesto.

Para visualizar la tabla de la valoración de las salvaguardas dirigirse al **ANEXO F**

4.3. Plan de Seguridad

Una vez identificado las amenazas con mayor riesgo se procede a listar las mismas, con el fin de elaborar el plan de seguridad.

Activos con mayor riesgo

[D] Datos/Información

Copia de respaldo

Datos de acceso a servidores

Códigos Fuentes SW

[SW] Software (Aplicaciones Informáticas)

Sistema de Nómina SIAP

[HW] Hardware (Equipos Informáticos)

Relojes biométricos

ACTIVOS	VALOR DEL ACTIVO	AMENAZA	FRECUENCIA O PROBBABILIDAD	DEGRADACIÓN O IMPACTO	RIESGO ASOCIADO A LA AMENAZA	VALOR DEL RIESGO
[D] DATOS/INFORMACIÓN						
COPIA DE RESPALDO	28	[E.2] Errores del administrador	3	4	Pérdida de integridad en la copia de respaldo	336
DATOS DE ACCESO A SERVIDORES	27	[A.4] Manipulación de la configuración	3	5	Pérdida de integridad en los datos de acceso a servidores	405
CÓDIGOS FUENTES SW	27	[E.20] Vulnerabilidades de los programas (software)	3	5	Fallos en su código o en su configuración	405
		[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	No disponibilidad de codigos fuentes	324
		[A.5] Suplantación de la identidad del usuario	3	5	Manipulación de códigos fuentes.	405
[SW] SOFTWARE(APLICACIONES INFORMÁTICAS)						
SISTEMA DE NÓMINA SIAP	22	[E.15] Alteración accidental de la información	3	5	Pérdida de integridad del sistema de nómina, debido a la alteración accidental de la información.	330
[HW] HARDWARE (EQUIPOS INFORMÁTICOS)						
RELOJES BIOMÉTRICOS	23	[I.*] Desastres industriales	3	5	No disponibilidad de relojes biométricos, otros desastres debidos a la actividad humana: corte de cables.	345

Figura 4.1. Activos con riesgos muy altos
Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito

El principal objetivo de esta tarea es la identificación de salvaguardas eficaces y pertinentes que permitan mitigar el riesgo potencial que pueda afectar activos de información relevantes de la empresa y las acciones que deberán ser aplicadas para salvaguardar los activos con mayor riesgo.

4.3.1. Fichas de Componentes

[D] DATOS/INFORMACIÓN

COPIA DE RESPALDO

Tabla 4.7. Salvaguarda Copia de respaldo

<table>
<tr><td colspan="2">SALVAGUARDA: Protección de los datos/información
[D] Copias de Seguridad de los datos (backup)</td></tr>
<tr><td colspan="2">JUSTIFICACIÓN: Siendo que para la empresa los datos correspondientes a los funcionarios directos, que vienen siendo los empleados, son de vital importancia, al igual que toda la información generada en sus equipos de trabajo, se escogió esta salvaguarda ya que en algunas ocasiones la información correspondiente se almacena en dispositivos de almacenamiento propios de los empleados, y cuando éstos se dan de baja de su puesto de trabajo, ésta información en muchas ocasiones se pierde.</td></tr>
<tr><td>ACTIVOS EN LOS QUE SE APLICA:
• Datos o Información [D]
COPIA DE RESPALDO</td><td>DIMENSIONES:
• Confidencialidad
• Integridad
• Disponibilidad</td></tr>
<tr><td colspan="2">AMENAZAS MITIGADAS:
• E.2 Errores del administrador.</td></tr>
<tr><td colspan="2">ACCIONES A APLICAR
- El resguardo de la información se hará en dos ubicaciones: local y fuera de sitio. La primera se realizará en los equipos de cómputo de la organización, el segundo resguardo se hará en el servidor, la frecuencia del respaldo será cada semana.
- Para el caso de la información crítica de la empresa, los empleados que tengan acceso a ella, tendrán que resguardar esta información mínimo con frecuencia diaria, tanto en la ubicación local o de su equipo.</td></tr>
</table>

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito

– **DATOS DE ACCESO A SERVIDORES**

Tabla 4.8. Salvaguarda datos de acceso a servidores

<table>
<tr><td colspan="2">SALVAGUARDA: Protección de los datos/información
Aseguramiento de la integridad</td></tr>
<tr><td colspan="2">JUSTIFICACIÓN: Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, registro de actividad.</td></tr>
<tr><td>ACTIVOS EN LOS QUE SE APLICA:
• Datos o Información [D]
DATOS DE ACCESO A SERVIDORES</td><td>DIMENSIONES:
• Confidencialidad
• Integridad
• Disponibilidad</td></tr>
<tr><td colspan="2">AMENAZAS MITIGADAS:
• [A.4] Manipulación de la configuración.</td></tr>
<tr><td colspan="2">ACCIONES A APLICAR
- Se debe eliminar toda la información del personal pasivo de la empresa tales como: usuarios y contraseñas esto se debe hacer previo aviso de la Coordinación de Talento Humano.
- Revisar los privilegios de acceso de los usuarios, el ing. Dennis Cueva, Especialista de Tecnologías 2 es la persona indicada para realizar la gestión de privilegios debido a que cuenta con nombramiento permanente, esto se lo debe hacer semanalmente a fin de eliminar información del personal desvinculado de la empresa.</td></tr>
</table>

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito

– **CÓDIGOS FUENTES SW**

Tabla 4.9. Salvaguarda códigos fuentes SW

<table>
<tr><td colspan="2">SALVAGUARDA: Protección de los datos/información

Cifrado de la información</td></tr>
<tr><td colspan="2">JUSTIFICACIÓN: Siendo que el programador de software de la empresa no cuenta con una amplia experiencia en la protección de datos debido a la alta rotación del personal y a los movimientos de los funcionarios que se encuentran en otras áreas y cumpliendo con el perfil es decir proceden a encargar puestos y a realizar actividades de alta responsabilidad como la asignación de perfiles, esto implica que por falta de conocimiento de las tareas que realizan los analistas proceden asignar privilegios a los individuos que no suelen realizar actividades de su competencia.</td></tr>
<tr><td>ACTIVOS EN LOS QUE SE APLICA:
• Datos o Información [D]
CÓDIGOS FUENTES SW</td><td>DIMENSIONES:
• Confidencialidad
• Integridad
• Disponibilidad</td></tr>
<tr><td colspan="2">AMENAZAS MITIGADAS:

• [E.20] Vulnerabilidades de los programas (software).
• [E.21] Errores de mantenimiento / actualización de programas (software)
• [A.5] Suplantación de la identidad del usuario.</td></tr>
<tr><td colspan="2">ACCIONES A APLICAR

- Se debe quitar los accesos autorizados a los funcionarios que ya no desempeñen funciones en ciertas actividades a fin de evitar suplantación de la identidad del usuario, esto se debe hacer de acuerdo a previo aviso de la Coordinación de Talento Humano quienes son los encargados de realizar el movimiento del personal o la desvinculación de los mismos.
- Siempre hacer copias de seguridad periódicas. Esto permitirá recuperar los datos y no perderlos ante un ataque malicioso, se debe realizar las copias de seguridad diariamente.
- Se debe instruir al ing. Fausto Valencia, analista de tecnologías 2 del área de soluciones informáticas quien, si cumple con el perfil y mantiene un nombramiento permanente en la empresa, por lo que es más factible capacitar a un funcionario permanente que aun provisional que en cualquier momento puede ser desvinculado de la empresa.</td></tr>
</table>

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito

[SW] SOFTWARE (APLICACIONES INFORMÁTICAS*)*

– SISTEMA DE NÓMINA SIAP

Tabla 4.10. Salvaguarda Sistema de nómina SIAP

SALVAGUARDA: Protección de las aplicaciones (software) SW Se aplican perfiles de seguridad	
JUSTIFICACIÓN: Puesto que no se cuenta con personal para realizar diferentes funciones como: ingreso de datos al sistema de nómina, nombres, cargo, sueldo, cuenta bancaria entre otros, esto lo hacen alternamente dos personas encargadas del sistema de nómina, se realiza variación de sueldos, cambio de cargos, esto implica responsabilidad y al contar con dos personas suele ocurrir alteración accidental de la información; por lo que se ha previsto la necesidad de crear cuentas de usuarios de acuerdo al cargo.	
ACTIVOS EN LOS QUE SE APLICA: • [SW] Software (Aplicaciones Informáticas) SISTEMA DE NÓMINA SIAP	**DIMENSIONES:** • Confidencialidad • Integridad • Disponibilidad
AMENAZAS MITIGADAS: • [E.15] Alteración accidental de la información	
ACCIONES A APLICAR - Tomar posesión de los datos y asumir la responsabilidad de garantizar su integridad. Solo el personal de la unidad de nómina correspondiente puede ocuparse de ciertas tareas asignadas. - Controlar los derechos y privilegios de acceso. - Se debe cambiar usuarios y contraseñas cada 3 meses al igual que la revisión de las actividades del personal a fin de deshabilitar módulos que no estén utilizando.	

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito

[HW] HARDWARE (EQUIPOS INFORMÁTICOS

- RELOJES BIOMÉTRICOS

Tabla 4.11. Salvaguarda relojes biométricos

<table>
<tr><td colspan="2">SALVAGUARDA: Protección de los equipos (hardware)
Protección de los Equipos Informáticos</td></tr>
<tr><td colspan="2">JUSTIFICACIÓN: Esta salvaguarda tiene lugar debido a las quejas del personal operativo en la que manifiestan los retrasos del personal (conductores y recaudadores) no registran la asistencia debido a que los relojes biométricos se encuentran dañados o fuera de servicio.
Otros desastres debidos a la actividad humana: como cortes de cables de la conexión eléctrica, derrame de productos líquidos, manipulación del teclado.</td></tr>
<tr><td>ACTIVOS EN LOS QUE SE APLICA:
• [HW] Hardware (Equipos Informáticos)
RELOJES BIOMÉTRICOS</td><td>DIMENSIONES:
• Disponibilidad</td></tr>
<tr><td colspan="2">AMENAZAS MITIGADAS:
• [I.*] Desastres industriales.</td></tr>
<tr><td colspan="2">ACCIONES A ACTIVAR
- Para solventar este incidente se debe instalar cajas de protección metálica a fin de que el personal operativo no pueda manipular físicamente los equipos biométricos ni derramar productos líquidos sobre los mismos.
- Se debe solicitar al centro de control la vigilancia de los relojes las 24 horas ya que el personal operativo tales como: recaudadores, conductores, supervisores de seguridad, sub jefes de trabajos, técnicos de mantenimiento de la flota, despachadores de combustible, laboran las 24 horas en horarios rotativos por lo que es importante mantener funcionando correctamente los relojes.</td></tr>
</table>

Fuente: Empresa Pública Metropolitana de Transporte de Pasajeros de Quito

- PERSONAL TÉCNICO

Soporte Técnico 1 (Centro de Procesamiento de Datos, Infraestructura)

Celular: 099-9160229

PBX: (02)2665018 – (02)2665022

Extensión: 33022

(Ing. Dennis Cueva)

E-mail: dcueva@trolebus.gob.ec

Soporte Técnico 2 (Centro de Procesamiento de Datos, Seguridades)

Celular: 099-9160229

PBX: (02)2665018 – (02)2665022

Extensión: 33022

(Ing. Carlos Taipe)

E-mail: ctaipe@trolebus.gob.ec

Soporte Técnico 3 (Sistemas de Software, Desarrollo)

Celular: 099-9160229

PBX: (02)2665018 – (02)2665022

Extensión: 33054

(Ing. Sandro Enríquez)

E-mail: senrique@trolebus.gob.ec

Soporte Técnico 4 (Centro de Procesamiento de Datos, Seguridades)

Celular: 099-9161234

PBX: (02)2665018 – (02)2665022

Extensión: 33022

(Ing. Juan Morocho)

E-mail: jmorocho@trolebus.gob.ec

Soporte Técnico 5 (Centro de Procesamiento de Datos, Seguridades)

Celular: 099-91607890

PBX: (02)2665018 – (02)2665022

Extensión: 33022

(Ing. Julia Arrobo)

E-mail: jarrobo@trolebus.gob.ec

Soporte Técnico 6 (Centro de Procesamiento de Datos, Infraestructura)

Celular: 099-9164323

PBX: (02)2665018 – (02)2665022

Extensión: 33022

(Ing. Fausto Valencia)

E-mail: fvalencia@trolebus.gob.ec

COORDINADOR DE ÁREA:

Si el inconveniente persiste pasados los 60 minutos (1.0 horas), su caso puede ser escalado a las Coordinación competente.

Ing. Richard Salas (Coordinador de Soluciones Tecnológicas, Redes y Comunicaciones)

PBX: (02) 2665018 / 2665022 ext. 33026

Email: rsalas@trolebus.gob.ec

CONCLUSIONES

- Se identificó los activos tecnológicos más relevantes de la empresa tales como: Datos / información, Servicios internos, Software (Aplicaciones Informáticas), Hardware (Equipos Informáticos), Redes de comunicaciones, Equipos Auxiliares, Servicios Subcontratados, Instalaciones y Personal y se valoró a los mismo en una escala del 1 al 10.

- Se identificó las amenazas a los que están expuestos aquellos activos tecnológicos que fueron valorados como activos relevantes de la empresa y se obtuvo una valoración de las amenazas en una escala del 1 al 5 de acuerdo a la probabilidad e impacto de los riesgos.

- Se calculó el valor de los riesgos de acuerdo al valor del activo, de la probabilidad y del impacto y se identificó los riesgos asociados a las amenazas de acuerdo a la escala de colores nivel bajo, medio y alto.

- Se determinó que salvaguardas hay disponibles y la valoración de cuán eficaces son frente al riesgo. Del análisis de los resultados obtenidos se identificaron los activos con mayor riesgo y se procedió a asignar salvaguardas a fin de mitigar los riesgos.

RECOMENDACIONES

- Se sugiere realizar el inventario de bienes y dar prioridad de resguardo a los activos de mayor importancia de la empresa este procedimiento se debe realizar trimestralmente o de acuerdo a las necesidades de la empresa a fin de mantener en orden y con su respectivo custodio de bienes.

- Se recomienda que haya una revisión periódicamente de las amenazas y riesgos ya que la tecnología está cambiando constantemente y deben ser controlados para evitar futuros problemas, por lo que se debe instalar cámaras de seguridad a fin de monitorear los activos y mantenerlos operando correctamente, realizar copias de seguridad de información constantemente.

- Para reducir los riesgos que existen en los activos de la empresa se debe asignar funciones al personal con mayor experiencia en los procedimientos sobre todo al personal con nombramiento permanente ya que son los indicados y tendrían menor probabilidad de cambio de área o de desvinculación.

- Se recomienda capacitación y concientización acerca de la seguridad de la información a los empleados de la organización ya que muchas de las brechas de seguridad encontradas, se debe a la falta de conocimiento sobre seguridad de algunos de los empleados.

REFERENCIAS BIBLIOGRÁFICAS

Agencia Europea de Medio Ambiente . (19 de 04 de 2016). *Riesgos naturales y tecnológicos*. Obtenido de https://www.eea.europa.eu/es/publications/92-9167-087-1/page014.html

Agencia Europea del Medio Ambiente. (19 de 04 de 2016). *Conclusions par problème environnemental.* Obtenido de https://www.eea.europa.eu/es/publications/92-9167-087-1/page014.html

Amutio Gómez, M. A. (01 de Octubre de 2012). *Magerit – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

Bolaños, M. C. (25 de 03 de 2014). *AUDITORÍA DE SI*. Obtenido de https://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-de-anlisis-y-gestin-de-riesgos-de-los-sistemas-de-informacin

Cuestas, R. (8 de Noviembre de 2014). *Riesgos y oportunidades de las nuevas tecnologías de informática*. Obtenido de https://www.eluniverso.com/opinion/2014/11/08/nota/4195936/riesgos-oportunidades-nuevas-tecnologias-informatica

Diaz, P., & Trujillo, R. (15 de Marzo de 2017). *Plan Estrattegico.* Obtenido de http://www.trolebus.gob.ec/index.php/gestion/plan-estrategico

EPMTPQ. (15 de Marzo de 2017). *Trolebus.* Obtenido de http://www.trolebus.gob.ec/index.php/sobre-nosotros/historia-institucional

Huerta, A. (30 de Marzo de 2012). *Introducción al análisis de riesgos – Metodologías (I)*. Obtenido de https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

Magerit. (1 de Octubre de 2012). Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Magerit. (05 de Julio de 2015). *Seguridad Informática - Magerit*. Obtenido de http://seguridadmagerit.blogspot.com/2015/07/elementos-del-analisis-de-riesgos.html

Magerit-V3. (1 de Octubre de 2012). *Libro I - Método*. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Magerit-V3. (1 de Octubre de 2012). *Libro II - Catálogo de Elementos*. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

Moyano, C. (1 de Abril de 2000). *Sistemas de Gestión de Seguridad y Salud Ocupacional.* España: IRAM 3800:1998 . Obtenido de http://www.minagri.gob.ar/sitio/areas/d_recursos_humanos/concurso/normativa/_archivos//000007_Otras%20normativas%20especificas/000000_NORMA%20IRAM%203800.pdf

Muerza, A. (17 de Febrero de 2011). *Desastres naturales en Europa*. Obtenido de http://www.consumer.es/web/es/medio_ambiente/naturaleza/2011/02/17/198967.php

Soto Suárez, A. (26 de Mayo de 2018). *Magerit Metodologia*. Obtenido de https://es.slideshare.net/AndresSotoSuarez1/magerit-metodologia

Tena , A., & Rivas, R. (1995). *Manual de investigación documental* (2a ed.). Chile: illustrated.

ANEXO A- ENCUESTAS

Gestión de Riesgos Tecnológicos

Empresa Pública Metropolitana de Transportes de Pasajeros de Quito

Objetivo: Obtener información, lo más exacta y válida posible, sobre el problema.

Dependencia: Gerencia de Tecnologías de la Información

Orientado al personal administrativo que labora en la EPMTPQ

Fecha: ……

1. ¿Su computador recibe mantenimiento de manera periódica?

   Sí ☐ No ☐

2. ¿Si en caso de daño su computador que tiempo se demoran en arreglarlos?

   1 hora ☐ 2 hora ☐ 1 día ☐

   Otros_____

3. Usted guarda la información que está realizando cuando se va almorzar.

   SI () NO ()

4. Con que frecuencia cambia su contraseña.

   Nunca ( )
   Cada mes ( )
   Tres meses ( )
   Seis meses ( )
   Una vez al año ( )

5. ¿Con qué frecuencia anual realiza la actualización de su software de Antivirus?

   1 vez ( ) 2 veces ( ) 3 veces ( ) 4 veces ( )

6. ¿Qué unidades de almacenamiento utiliza frecuentemente?

   DISCO DURO EXTRAÍBLE ☐
   CD ☐
   USB ☐
   FOTOCOPIAS, IMPRESIÓN, ESCANEO. ☐

7. Califique de 1 a 5 el servicio de soporte técnico por el personal de mantenimiento y soporte de computadores.
   1. ☐
   2. ☐
   3. ☐
   4. ☐
   5 ☐

8. ¿Ha presentado caídas en la base de datos?

   SI ☐
   NO ☐

9. ¿Las tareas que le han sido encomendadas involucran la custodia de información que puede ser catalogada como sensible o de carácter confidencial?

   SI ☐
   NO ☐

ANEXO B -TABULACIONES DE ENCUESTAS

Mediante la tabulación de las encuestas se logró establecer los problemas que presenta actualmente la empresa.

1. **¿Su computador recibe mantenimiento de manera periódica**?

   Sí ☐ No ☐

No	ÍTEM	FRECUENCIA	%
1	Si	3	25,00
2	No	9	75,00
	TOTAL	12	100%

Más de la mitad de empleados encuestados mencionaron que sus equipos no reciben mantenimiento en determinado tiempo, sino que el equipo debe presentar problemas serios para proceder con el respectivo mantenimiento.

2. **¿Si en caso de daño su computador que tiempo se demoran en arreglarlos?**

   1 hora ☐ 2 hora ☐ 1 día ☐

   Otros_____

No	ÍTEM	FRECUENCIA	%
1	1 hora	0	0
2	2 horas	0	0
3	1 día	7	100
4	Otros	0	0
	TOTAL	7	100%

Los empleados de EPMTPQ, dijeron que cuando el computador no funciona deben llamar al personal de sistemas para que arregle el equipo y por lo general se demora 1 día realizando los ajustes correspondientes, retrasando las actividades laborales.

3. **Usted guarda la información que está realizando cuando se va almorzar.**

   SI () NO ()

No	ÍTEM	FRECUENCIA	%
1	Si	7	70
2	No	3	30
	TOTAL	10	100%

No todos los empleados guardan la información para ir a almorzar por lo que ocasiona pérdida de información.

4. **Con que frecuencia cambia su contraseña.**

   8 días ( )
   15 días ( )
   30 días ( )
   45 días ( )
   Nunca ( )

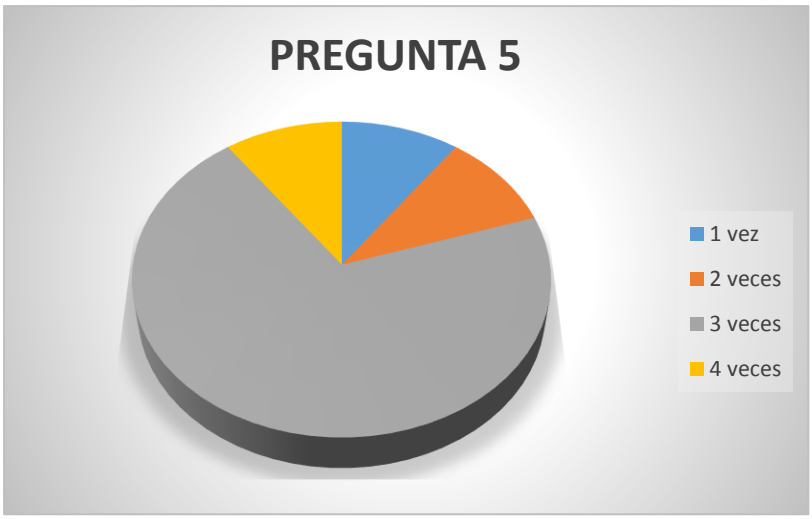
No	ÍTEM	FRECUENCIA	%
1	8 días	0	0
2	15 días	0	0
3	30 días	0	0
4	45 días	10	100
5	Nunca	0	0
	TOTAL	10	100%

Las contraseñas caducan cada 45 días, pero si el funcionario sospecha que la contraseña es conocida por otra persona, debe cambiarle inmediatamente.

5. **¿Con qué frecuencia anual realiza la actualización de su software de Antivirus?**

   1 vez ( ) 2 veces ( ) 3 veces ( ) 4 veces ( )

No	ÍTEM	FRECUENCIA	%
1	1 vez	10	10
2	2 veces	10	10
3	3 veces	70	70
4	4 veces	10	10
	TOTAL	100	100%

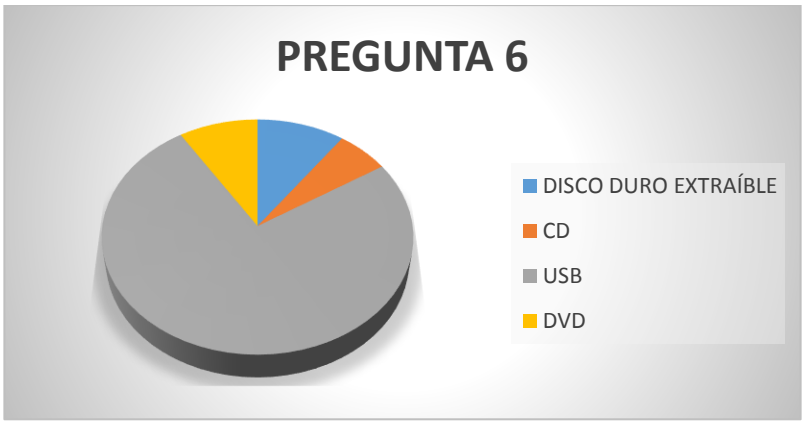


La mayoría de los encuestados contestaron 3 veces al año es decir de forma trimestral de ya que el área de tecnologías es responsable de instalar y activar herramientas de antivirus en los equipos informáticos de la EPMTPQ, la cual debe mantenerse actualizada periódicamente.

6. ¿Qué unidades de almacenamiento utiliza frecuentemente?

DISCO DURO EXTRAÍBLE ☐
CD ☐
USB ☐
DVD. ☐

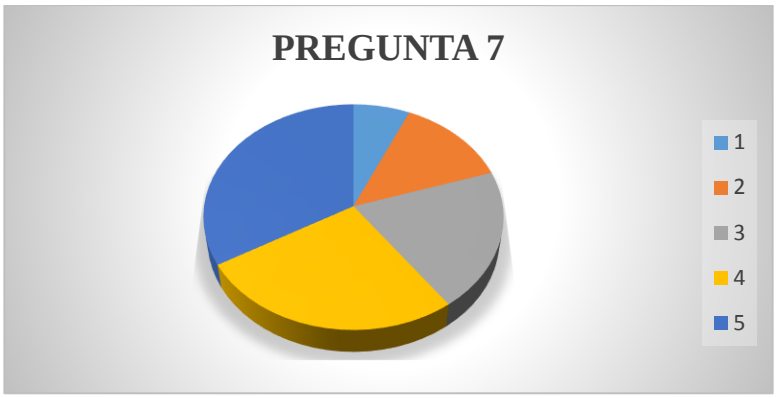
No	ÍTEM	FRECUENCIA	%
1	DISCO DURO EXTRAÍBLE	10	10
2	CD	6	6
3	USB	75	75
4	DVD	9	9
	TOTAL	100	100%



El almacenamiento físico es esencial en la empresa, lo que requiere un servicio de archivo bastante numeroso y se debe únicamente guardar en el dispositivo USB información ya guardada en un servicio de archivos y sea utilizado para la trasferencia de archivos de suma urgencia debido a una caída de red.

7. **Califique de 1 a 5 el servicio de soporte técnico por el personal de mantenimiento y soporte de computadores.**
   1. ☐
   2. ☐
   3. ☐
   4. ☐
   5 ☐

No	ÍTEM	FRECUENCIA	%
1	1	7	7
2	2	20	20
3	3	50	50
4	4	10	10
5	5	13	13
	TOTAL	100	100%



La mitad del personal califico como aceptable el servicio de soporte y mantenimiento del área de tecnología.

8. **¿Ha presentado caídas en la base de datos?**

SI ☐

NO ☐

No	ÍTEM	FRECUENCIA	%
1	SI	60	60
2	N0	40	40
	TOTAL	100	100%

Las caídas en la base de datos son frecuentes, no hay una confianza generalizada por la información que se encuentra allí almacenada, por lo que esto ocasiona pérdida de información.

9. **¿Las tareas que le han sido encomendadas involucran la custodia de información que puede ser catalogada como sensible o de carácter confidencial?**

SI ☐

NO ☐

No	ÍTEM	FRECUENCIA	%
1	SI	30	30,00
2	NO	70	70,00
	TOTAL	100	100%

Los empleados se encuentran divididos, y no entienden en muchos casos la importancia de la custodia de la información y de que si esta es mal utilizada podría tener riesgos importantes para la empresa, esto se debe a la alta rotación del personal y a la falta de responsabilidad.

De acuerdo a las encuestas se obtuvo las medidas de tendencia central lo cual permitió destacar los problemas que se presentan en la empresa.

DATOS					MEDIDAS DE TENDECIA CENTRAL			
					MEDIA	MEDIANA	MODA	VARIANZA
SI	3	7	30	60	25	30	0	686
NO	3	9	40	70	30,5	40	0	956,3

Conclusiones

- Todos los funcionarios deben reportar de forma inmediata a la Gerencia de Tecnologías de la Información, los riesgos reales o potenciales que están expuestos los equipos computacionales en la estación de trabajo, durante el desempeño de sus funciones.

- La información de la EPMTPQ, clasificada como sensible, confidencial o de uso restringido, debe guardarse y transmitirse en forma segura, utilizando dispositivos, medios y/o herramientas de seguridad fuertes y que hayan sido aprobadas por la Gerencia de Tecnologías de la Información.

- Todos los medios de almacenamiento de información de tipo extraíble (cintas magnéticas, CD, DVD o memorias tipo USB) asignados por la EPMTPQ en función de las tareas del Funcionario, son responsabilidad del mismo, junto con la información contenida, aun cuando no se utilicen.
- La Gerencia de Tecnologías de la Información es responsable de realizar auditorías internas trimestralmente, a todos los equipos informáticos de la EPMTPQ, para verificar las versiones de software, actualización de antivirus y la existencia de aplicativos no autorizados, los cuales se procederá a eliminarlos de forma inmediata.
- Los funcionarios de las Gerencias y/o Coordinaciones de la EPMTPQ, que detecten cualquier falla en los equipos, software o servicios, debe reportar inmediatamente a la Gerencia de Tecnologías de la Información, a través del sistema de soporte técnico publicado en la Intranet.
- Las cuentas de acceso a los sistemas y los recursos informáticos son propiedad de la EPMTPQ y se usarán exclusivamente para actividades relacionadas con el desarrollo del trabajo de cada Funcionario.

ANEXO C- LISTADO DE AMENAZAS

En la tabla se muestra el listado de las diferentes amenazas que se tomó del Libro Magerit II, las mismas que están expuestos los activos tecnológicos como desastres naturales, origen industrial, contaminación ambiental, contaminación electromagnética, corte de suministro eléctrico, vulnerabilidades de los programas, indisponibilidad del personal entre otras amenazas que se detallan a continuación:

LISTADO DE AMENZAS
[N]Desastres naturales
[N.1]Fuego
[N.2]Daños por agua
[N. *]Desastres naturales
[N.* .1]Tormentas
[N.* .2]Tormentas eléctricas
[N.*.3]Huracanes
[N.* .4]Terremotos
[N.* .5]Tornados
[N.* .6]Ciclones
[N.* .7]Deslizamientos del terreno
[N.* .8] Meteoritos
[N.* .9]Tsunamis
[N.* .10]Tormentas de invierno y frío extremo
[N.* .11]Calor extremo
[N.* .12]Volcanes
[I]De origen industrial
[I.1]Fuego
[I.2]Daños por agua
[I. *]Desastres industriales
[1.3]Contaminación ambiental
[I.3.1]Vibraciones
[1.3.2]Ruido
[I.3.3]Polvo
[I.3.4]Humo
[I.3.5]Vapor
[I.4]Contaminación electromagnética
[I.4.11]Ruido electromagnético accidental

[I.4.12] Ruido electromagnético deliberado
[I.4.15] Ruido electromagnéticos accidentales
[I.4.16] Ruido electromagnéticos deliberados
[I.4.21]Ruido termino accidental
[I.4.22]Ruido termino deliberado
[I.4.31]Jamming
[I.5]Avería de origen físico o lógico
[1.5.1]Software
[I.5.2]Hardware
[I.5.3]Equipos de comunicaciones
[I.5.4]Equipamiento auxiliar
[I.6]Corte del suministro eléctrico
[I.6.11]1nterrupción accidental
[I.6.12]interrupción deliberada por un agente externo
[I.6.13] interrupción deliberada por un agente interno
[I.7]Condiciones inadecuadas de temperatura o humedad
[1.8]Fallo de servicios de comunicaciones
[I.8.11]1nterrupción accidental
[I.8.12]interrupción deliberada por un agente externo
[I.8.13] interrupción deliberada por un agente interno
[I.9]interrupción de otros servicios o suministros esenciales
[I.9.1]Papel
[I.9.2]Refrigerante
[I.9.3]Diésel
[I.10]Degradación de los soportes de almacenamiento de la información
[I.11]Emanaciones electromagnéticas
[I.11.1]Radio
[I.12.2]Térmica
[E] Errores y fallos no intencionados
[E.1]Errores de los usuarios
[E.2]Errores del administrador del sistema/ seguridad
[E.3]Errores de monitorización
[E.4]Errores de configuración
[E.7]Deficiencias en la organización
[E.8]Difusión de software dañino
[E.8.0]Gusano
[E.8.1]Virus
[E.8.2]Caballos de Troya
[E.8.3]Spyware

[E.9]Errores de re-encaminamiento
[E.9.1]Queda en casa
[E.9.2]A terceros con acuerdo establecido
[E.9.3]AI mundo entero
[E.10]Errores de secuencia
[E.14]Fugas de información
[E.15] Alteración de la información
[E.18]Destrucción de la información
[E.19]Fugas de información
[E.19.1]A personal interno que no necesita conocerlo
[E.19.2]A contratistas que no necesitan conocerlo
[E.19.3]A personas externas que no necesitan conocerlo
[E.19.4]AI público en general
[E.19.5]A los medios de comunicación
[E.19.11]1dentificación de la localización
[E.20]Vulnerabilidades de los programas (software)
[E.20.dos]Denegación de servicio
[E.20.read]Acceso de lectura
[E.20.write]Acceso de escritura
[E.20.escalation]Escalada de privilegios
[E.21]Errores de mantenimiento software/ actualización de programas software
[E.23]Errores de mantenimiento hardware/ actualización de programas hardware
[E.24]Caída del sistema por agotamiento de recursos
[E.25]Perdida de equipos
[E.28]1ndisponibilidad del personal
[E.28.1] Enfermedad
[E.28.2]Huelga
[E.28.3]No hay personal
[E.28.4]Personal insuficiente
[A]Ataques deliberados
[A.3]Manipulación de los registros de actividad
[A.4]Manipulación de los ficheros de configuración
[A.5]Suplantación de la identidad
[A.5.1]Por personal interno
[A.5.2]Por subcontratistas
[A.5.3]Por personas externas
[A.6]Abuso de privilegios de acceso
[A.6.1]Por personal interno
[A.6.2]Por subcontratistas

[A.6.3]Por personas externas
[A.7]Uso no previsto
[A.7.1]Por personal interno
[A.7.2]Por subcontratistas
[A.7.3]Por personas externas
[A.8]Difusión de software dañino
[A.8.0]Gusano
[A.8.1]Virus
[A.8.2]Caballos de Troya
[A.8.3]Spyware
[A.9]Encaminamiento de mensajes
[A.10]Alteración de secuencia
[A.11]Acceso no autorizado
[A.11.1]Por personal interno
[A.11.2]Por subcontratistas
[A.11.3]Por personas externas
[A.12]Análisis de trafico
[A.12.1]Por personal interno
[A.12.2]Por subcontratistas
[A.12.3]Por personas externas
[A.13]Repudio (negociación de actuaciones)
[A.14]1nterceptación de información (escucha)
[A.14.1]Por personal interno
[A.14.2]Por subcontratistas
[A.14.3]Por personas externas
[A.15]Modificación de la información
[A.18]Destrucción de la información
[A.19]Revelación de información
[A.19.1]A personal interno
[A.19.2]A subcontratistas
[A.19.3]A personas externas
[A.19.4]A público general
[A.19.5]A los medios de comunicación
[A.19.11]Identificación de la localización
[A.22]Manipulación de programas
[A.22.1]Bombas lógicas
[A.22.2]Caballos de Troya
[A. 22. 3] KeyLogger (spyware)
[A.22.4]Puertas traseras

[A.22.5]Autenticación débil
[A.22.6]Se elude la autenticación
[A.23]Manipulación del hardware
[A.24]Denegación de servicios
[A.24.1]Saturación de los canales de comunicaciones
[A.24.2] Saturación de los recursos software
[A.24.3] Saturación de los recursos hardware
[A.25]Robo de equipos
[A.25.1]Por personal interno
[A.25.2]Por subcontratistas
[A.25.3]Por personas externas
[A.26]Ataque destructivos
[A.26.1]Vandalismo
[A.26.2]Bombas
[A.26.3]Terrorismo
[A.27]Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.28.1] Enfermedad
[A.28.2] Huelga
[A.28.3] Absentismo
[A.29]Extorsión
[A.29.1] Ataque desde el exterior
[A.29.2] Ataque desde el interior
[A.30] ingeniería social (picaresca)
[A.30.1] Ataque desde el exterior
[A.30.2] Ataque desde el interior
[A.31] Distracción
[A.40] Incumplimiento (leyes, reglamentos, normas,…)

ANEXO D- VALORACIÓN DE ACTIVOS

En la siguiente tabla se valoran las amenazas en una escala del 1 al 5, se mide la frecuencia o probabilidad que se da por las diferentes amenazas de acuerdo a cada tipo de activo y el impacto o degradación que se produce por las amenazas a los activos de la Empresa Publica Metropolitana de Transporte de Pasajeros de Quito.

	ACTIVOS	AMENAZA	FRECUENCIA O PROBBABILIDAD	DEGRADACIÓN O IMPACTO
[D] DATOS/INFORMACIÓN	COPIA DE RESPALDO	[E.1] Errores de los usuarios	2	**4**
		[E.2] Errores del administrador	3	4
	DATOS DE ACCESO A SERVIDORES	[E.7] Deficiencias en la organización	2	4
		[A.4] Manipulación de la configuración	3	5
		[A.5] Suplantación de la identidad del usuario	2	5
		[A.11] Acceso no autorizado	2	5
	DATOS DE ACCESO A USUARIOS	[A.5] Suplantación de la identidad del usuario	2	5
		[A.11] Acceso no autorizado	2	4
	CÓDIGOS FUENTES SW	[E.20] Vulnerabilidades de los programas (software)	3	5
		[E.21] Errores de mantenimiento / actualización de programas (software)	3	4

		[A.5] Suplantación de la identidad del usuario	3	5
[IS] SERVICIOS INTERNOS	SERVICIO DE INTERNET	[I.6] Corte del suministro eléctrico	2	5
		[I.8] Fallo de servicios de comunicaciones	2	4
		[I.9] Interrupción de otros servicios y suministros esenciales	2	4
		[A.7] Uso no previsto	2	3
	SERVICIO DE TELEFONÍA	[E.1] Errores de los usuarios	2	4
		[E.2] Errores del administrador	3	4
		[I.8] Fallo de servicios de comunicaciones	2	4
		[I.9] Interrupción de otros servicios y suministros esenciales	2	4
	SERVICIO DE MANTENIMIENTO	[E.7] Deficiencias en la organización	3	5
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	4
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	4
		[E.28] Indisponibilidad del personal	2	3
[SW] SOFTWARE(APLICACIONES INFORMÁTICAS)	OFIMÁTICA	[E.21] Errores de mantenimiento / actualización de programas (software)	2	3
		[E.1] Errores de los usuarios	2	4
	ANTIVIRUS	[E.8] Difusión de software dañino	2	4
		[E.20] Vulnerabilidades de los programas (software)	2	5
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	5

	SISTEMA BIOMÉTRICO SIRHA	[I.5] Avería de origen físico o lógico	3	3
		[E.15] Alteración accidental de la información	2	4
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	4
		[A.5] Suplantación de la identidad del usuario	2	5
		[A.24] Denegación de Servicio	2	4
	SISTEMA DE GESTIÓN DE BASE DE DATOS	[I.5] Avería de origen físico o lógico	3	3
		[E.15] Alteración accidental de la información	2	5
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	5
		[A.5] Suplantación de la identidad del usuario	2	5
	SERVIDOR DE CORREO(APLICACIÓN DE RED)	[I.5] Avería de origen físico o lógico	3	3
		[E.15] Alteración accidental de la información	2	5
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	5
		[A.5] Suplantación de la identidad del usuario	2	5
	SISTEMA DE NÓMINA SIAP	[I.5] Avería de origen físico o lógico	3	3
		[E.15] Alteración accidental de la información	3	5
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	5

		[A.5] Suplantación de la identidad del usuario	2	5
		[A.24] Denegación de Servicio	2	4
	SOFTWARE NETWORKING	[I.5] Avería de origen físico o lógico	3	3
		[E.15] Alteración accidental de la información	2	4
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	5
		[A.5] Suplantación de la identidad del usuario	2	5
[HW] HARDWARE (EQUIPOS INFORMÁTICOS)	**COMPUTADORAS DE ESCRITORIO**	[N.1]Fuego	1	5
		[N.2]Daños por agua	2	5
		[N. *]Desastres naturales	2	5
		[1.3]Contaminación ambiental	2	4
		[I.5]Avería de origen físico o lógico	3	3
		[I.7]Condiciones inadecuadas de temperatura o humedad	2	4
		[E.2]Errores del administrador del sistema/ seguridad	2	4
		[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5
		[A.11]Acceso no autorizado	2	4
		[A.23]Manipulación del hardware	2	5
	COMPUTADORAS PERSONALES	[N.1]Fuego	1	5
		[N.2]Daños por agua	2	5
		[N. *]Desastres naturales	2	5
		[1.3]Contaminación ambiental	2	4
		[I.5]Avería de origen físico o lógico	3	3
		[I.7]Condiciones inadecuadas de temperatura o humedad	2	4

		[E.2]Errores del administrador del sistema/ seguridad	2	4
		[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5
		[A.11]Acceso no autorizado	2	4
		[A.23]Manipulación del hardware	2	5
	IMPRESORAS	[I.5]Avería de origen físico o lógico	3	3
		[I.7]Condiciones inadecuadas de temperatura o humedad	2	5
		[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5
		[A.11]Acceso no autorizado	2	4
	SWITCH	[N.1]Fuego	1	5
		[N.2]Daños por agua	2	5
		[I.6]Corte del suministro eléctrico	2	5
		[E.21]Errores de mantenimiento software/ actualización de programas software	2	5
		[A.6]Abuso de privilegios de acceso	2	4
		[A.11]Acceso no autorizado	2	5
		[A.25]Robo de equipos	1	5
		[A.26]Ataque destructivos	2	5
	FIREWALL	[I.6]Corte del suministro eléctrico	2	5
		[I.7]Condiciones inadecuadas de temperatura o humedad	2	5
	ROUTER	[N.1]Fuego	1	5
		[N.2]Daños por agua	2	5
		[I.6]Corte del suministro eléctrico	2	5
		[E.21]Errores de mantenimiento software/ actualización de programas software	2	5
		[A.6]Abuso de privilegios de acceso	2	4
		[A.11]Acceso no autorizado	2	5
		[A.25]Robo de equipos	1	5

		[A.26]Ataque destructivos	2	5
	ACCESS POINT	[I.1] Fuego	1	5
		[I.2] Daños por agua	2	5
		[I.*] Desastres industriales	2	5
		[I.5] Avería de origen físico o lógico	3	3
		[E.4] Errores de configuración	2	4
	RELOJES BIOMÉTRICOS	[I.1] Fuego	1	5
		[I.2] Daños por agua	2	5
		[I.*] Desastres industriales	3	5
		[A.11]Acceso no autorizado	2	5
		[A.25] Robo	1	5
	SERVIDORES FISICOS	[N.1]Fuego	1	5
		[N.2]Daños por agua	2	5
		[N. *]Desastres naturales	2	5
		[1.3]Contaminación ambiental	2	4
		[I.5]Avería de origen físico o lógico	3	3
		[I.7]Condiciones inadecuadas de temperatura o humedad	2	5
		[E.2]Errores del administrador del sistema/ seguridad	2	5
		[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5
		[A.11]Acceso no autorizado	2	5
		[A.23]Manipulación del hardware	2	5
[COM] REDES DE COMUNICACIONES	**TELEFONÍA IP**	[1.8]Fallo de servicios de comunicaciones	2	5
		[E.9]Errores de re-encaminamiento	2	4
		[E.15] Alteración de la información	2	5
		[E.19]Fugas de información	2	4
		[A.7]Uso no previsto	2	4
		[A.9]Encaminamiento de mensajes	2	4

		[A.10]Alteración de secuencia	2	5
		[A.12]Análisis de trafico	2	5
		[A.14]1nterceptación de información (escucha)	2	5
	RED LAN	[I.8]Fallo de servicios de comunicaciones	2	4
		[E.9]Errores de re-encaminamiento	2	5
		[E.10]Errores de secuencia	2	5
		[A.5]Suplantación de la identidad	2	5
		[A.9]Encaminamiento de mensajes	2	4
		[A.10] Alteración de secuencia	2	4
		[A.11]Acceso no autorizado	2	5
	RED WIFI	[I.8]Fallo de servicios de comunicaciones	2	5
		[E.9]Errores de re-encaminamiento	2	5
	INTERNET	[I.8]Fallo de servicios de comunicaciones	2	5
		[E.15] Alteración de la información	2	4
[AUX] EQUIPOS AUXILIARES	**CABLEADO**	[I.1] Fuego	1	5
		[I.2] Daños por agua	2	5
		[I.7] Condiciones inadecuadas de temperatura o humedad	2	5
		[I.11] Emanaciones electromagnéticas	2	5
		[I.*] Desastres industriales	2	4
		[A.25] Robo	1	5
	PLANTA ELÉCTRICA	[I.1] Fuego	1	5
		[I.2] Daños por agua	1	5
		[I.9] Interrupción de otros servicios y suministros esenciales	2	5
		[I.*] Desastres industriales	2	5

		[A.25] Robo	2	5
	UPS	[I.1] Fuego	2	5
		[I.2] Daños por agua	2	5
		[I.*] Desastres industriales	2	5
		[A.25] Robo	1	5
	FUENTES DE ALIMENTACIÓN	[I.1] Fuego	2	5
		[I.2] Daños por agua	2	5
		[I.*] Desastres industriales	2	5
		[A.25] Robo	1	5
	FIBRA ÓPTICA	[I.1] Fuego	2	5
		[I.2] Daños por agua	2	5
		[I.7] Condiciones inadecuadas de temperatura o humedad	2	4
		[I.*] Desastres industriales	2	5
		[A.25] Robo	1	5
[SS] SERVICIOS SUBCONTRATADOS	**SISTEMA SIRHA(SISTEMA BIOMÉTRICO)**	[I.5] Avería de origen físico o lógico	3	4
		[E.15] Alteración accidental de la información	2	5
		[E.21] Errores de mantenimiento / actualización de programas (software)	3	4
		[A.5] Suplantación de la identidad del usuario	2	5
		[A.24] Denegación de Servicio	2	5
	SISTEMA SIAP(NÓMINA ROL DE PAGOS)	[I.5] Avería de origen físico o lógico	3	3
		[E.15] Alteración accidental de la información	2	5

		[E.21] Errores de mantenimiento / actualización de programas (software)	2	5
		[A.5] Suplantación de la identidad del usuario	2	5
		[A.24] Denegación de Servicio	2	5
[L] INSTALACIONES }	**OFICINAS**	[I.1] Fuego	1	5
		[I.2] Daños por agua	2	5
		[I.*] Desastres industriales	2	5
		[A.26]Ataque destructivos	2	5
		[A.27] Ocupación enemiga	2	5
	VEHÍCULOS	[I.1] Fuego	1	5
		[I.2] Daños por agua	2	5
		[A.26]Ataque destructivos	2	5
		[I.*] Desastres industriales	2	5
	ESTACIONES TROLEBÚS Y ECOVIA	[I.1] Fuego	1	5
		[I.2] Daños por agua	2	5
		[I.*] Desastres industriales	2	5
		[A.26]Ataque destructivos	2	5
		[A.27] Ocupación enemiga	2	5
[P] PERSONAL	**COORDINADOR DE SISTEMAS INFORMÁTICOS**	[E.7]Deficiencias en la organización	2	4
		[E.14]Fugas de información (>E.19)	2	4
		[A.6] Abuso de privilegios de acceso	2	4
		[A.18] Destrucción de información	2	5
		[A.29]Extorsión	1	5
		[A.30] ingeniería social (picaresca)	3	4
		[E.7]Deficiencias en la organización	2	4

	COORDINADOR DE REDES Y TELECOMUNICACIONES	[E.14]Fugas de información (>E.19)	2	4
		[A.6] Abuso de privilegios de acceso	2	4
		[A.18] Destrucción de información	2	5
		[A.29]Extorsión	1	5
		[A.30] Ingeniería social (picaresca)	3	4
	ESPECIALISTAS DE TECNOLOGÍAS 2	[E.7]Deficiencias en la organización	2	4
		[E.14]Fugas de información (>E.19)	2	4
		[A.6] Abuso de privilegios de acceso	2	4
		[A.18] Destrucción de información	2	5
		[A.29]Extorsión	1	5
		[A.30] ingeniería social (picaresca)	3	4
	ESPECIALISTA DE BIENES 2	[E.7]Deficiencias en la organización	2	4
		[E.14]Fugas de información (>E.19)	2	4
		[A.6] Abuso de privilegios de acceso	2	4
		[A.18] Destrucción de información	2	5
		[A.29]Extorsión	1	5
		[A.30] ingeniería social (picaresca)	3	4
	TÉCNICOS ADMINISTRATIVO DE BIENES	[E.7]Deficiencias en la organización	2	4
		[E.14]Fugas de información (>E.19)	2	4
		[A.6] Abuso de privilegios de acceso	2	4
		[A.18] Destrucción de información	2	5
		[A.29]Extorsión	1	5
		[A.30] ingeniería social (picaresca)	3	4
	ESPECIALISTA DE TELECOMUNICACIONES 4	[E.7]Deficiencias en la organización	2	4
		[E.14]Fugas de información (>E.19)	2	4
		[A.6] Abuso de privilegios de acceso	2	4
		[A.18] Destrucción de información	2	5
		[A.29]Extorsión	1	5

		[A.30] ingeniería social (picaresca)	3	4
	COORDINADORA DE TALENTO HUMANO	[E.7]Deficiencias en la organización	2	4
		[E.14]Fugas de información (>E.19)	2	4
		[A.6] Abuso de privilegios de acceso	2	4
		[A.18] Destrucción de información	2	5
		[A.29]Extorsión	1	5
		[A.30] Ingeniería social (picaresca)	3	4
	COORDINADORA DE SEGURIDAD	[E.7]Deficiencias en la organización	2	4
		[E.14]Fugas de información (>E.19)	2	4
		[A.6] Abuso de privilegios de acceso	2	4
		[A.18] Destrucción de información	2	5
		[A.29]Extorsión	1	5
		[A.30] Ingeniería social (picaresca)	3	4

ANEXO E- TABLA DE IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

En la siguiente tabla se identifican y valoran los riesgos más importantes a los que están expuestos los activos de la Empresa Pública Metropolitana de Transporte de Pasajeros de Quito según las amenazas a los que se exponen y los valores de mayor riesgo y así aplicar acciones pertinentes a fin de mitigar el riesgo se realizó un plan de seguridad de los riesgos con un valor de 300 hasta 750 según la escala de valoración de riesgos.

ACTIVOS	ACTIVOS	VALOR DEL ACTIVO	AMENAZA	FRECUENCIA O PROBBABILIDAD	DEGRADACIÓN O IMPACTO	RIESGO ASOCIADO A LA AMENAZA	VALOR DEL RIESGO
[D] DATOS/INFORMACIÓN	**COPIA DE RESPALDO**	**28**	[E.1] Errores de los usuarios	2	**4**	Pérdida de información	224
			[E.2] Errores del administrador	3	4	Pérdida de Integridad en la copia de respaldo	336
	DATOS DE ACCESO A SERVIDORES	**27**	[E.7] Deficiencias en la organización	2	4	Abandono del trabajo	216
			[A.4] Manipulación de la configuración	3	5	Pérdida de integridad en los datos de acceso a servidores	405
			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	270

			[A.11] Acceso no autorizado	2	5	Pérdida de Integridad y confidencialidad de datos de acceso a servidores	270
	DATOS DE ACCESO A USUARIOS	**27**	[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	270
			[A.11] Acceso no autorizado	2	4	Pérdida de Integridad y confidencialidad de datos de acceso a servidores	216
	CÓDIGOS FUENTES SW	**27**	[E.20] Vulnerabilidades de los programas (software)	3	5	Fallos en su código o en su configuración	405
			[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	No disponibilidad de códigos fuentes	324
			[A.5] Suplantación de la identidad del usuario	3	5	Manipulación de códigos fuentes	405
[IS] SERVICIOS INTERNOS	**SERVICIO DE INTERNET**	**24**	[I.6] Corte del suministro eléctrico	2	5	No disponibilidad de internet	240
			[I.8] Fallo de servicios de comunicaciones	2	4	No disponibilidad mediante el servicio de internet	192
			[I.9] Interrupción de otros servicios y suministros esenciales	2	4	No disponibilidad de algunos servicios	192

			[A.7] Uso no previsto	2	3	Mal uso del recurso asignado	144
	SERVICIO DE TELEFONÍA	**22**	[E.1] Errores de los usuarios	2	4	Pérdida del servicio de telefonía	176
			[E.2] Errores del administrador	3	4	Interrupciones programadas	264
			[I.8] Fallo de servicios de comunicaciones	2	4	No disponibilidad del servicio de telefonía	176
			[I.9] Interrupción de otros servicios y suministros esenciales	2	4	Pérdida de comunicaciones el personal interno	176
	SERVICIO DE MANTENIMIENTO	**13**	[E.7] Deficiencias en la organización	3	5	Abandono del trabajo	195
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	No disponibilidad del servicio de software	104
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	4	No disponibilidad del servicio de hardware	104
			[E.28] Indisponibilidad del personal	2	3	Falta de personal	78

[SW] SOFTWARE(APLICACIONES INFORMÁTICAS)	**OFIMÁTICA**	**20**	[E.21] Errores de mantenimiento / actualización de programas (software)	2	3	No disponibilidad de paquete de ofimática	120
			[E.1] Errores de los usuarios	2	4	Desinstalación de programas	160
	ANTIVIRUS	**17**	[E.8] Difusión de software dañino	2	4	Infección mediante aplicaciones	136
			[E.20] Vulnerabilidades de los programas (software)	2	5	Fallos en los antivirus	170
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad de antivirus	170
	SISTEMA BIOMÉTRICO SIRHA	**18**	[I.5] Avería de origen físico o lógico	3	3	No disponibilidad del sistema biométrico	162
			[E.15] Alteración accidental de la información	2	4	Pérdida de integridad en los datos del sistema biométrico	144
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	No disponibilidad del sistema biométrico	144
			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	180
			[A.24] Denegación de servicio	2	4	No disponibilidad del servicio	144
	SISTEMA DE GESTIÓN DE BASE DE DATOS	**19**	[I.5] Avería de origen físico o lógico	3	3	No disponibilidad del sistema de base de datos	190

			[E.15] Alteración accidental de la información	2	5	Pérdida de integridad en los datos del sistema de BD	190
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad del sistema de base de datos	190
			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	190
	SERVIDOR DE CORREO(APLICACIÓN DE RED)	**19**	[I.5] Avería de origen físico o lógico	3	3	No disponibilidad del correo electrónico	171
			[E.15] Alteración accidental de la información	2	5	Pérdida de integridad de los correos	190
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad del sistema de nómina	190
			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	190
	SISTEMA DE NÓMINA SIAP	**22**	[I.5] Avería de origen físico o lógico	3	3	No disponibilidad del sistema de nómina	198
			[E.15] Alteración accidental de la información	3	5	Pérdida de integridad del sistema de nómina, debido a la alteración accidental de la información	330

			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad del sistema de nómina	220
			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	220
			[A.24] Denegación de servicio	2	4	No disponibilidad del sistema de nómina	176
	SOFTWARE NETWORKING	**18**	[I.5] Avería de origen físico o lógico	3	3	No disponibilidad del sistema de almacenamiento de datos	162
			[E.15] Alteración accidental de la información	2	4	Perdida de integridad de información	144
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad del sistema de almacenamiento de datos	180
			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	180
[HW] HARDWARE (EQUIPOS INFORMÁTICOS)	**COMPUTADORAS DE ESCRITORIO**	**24**	[N.1]Fuego	1	5	No disponibilidad del computador	120
			[N.2]Daños por agua	2	5	No disponibilidad del computador	240
			[N. *]Desastres naturales	2	5	No disponibilidad del computador	240
			[1.3]Contaminación ambiental	2	4	No disponibilidad del computador	192

			[I.5]Avería de origen físico o lógico	3	3	No disponibilidad del computador	216
			[I.7]Condiciones inadecuadas de temperatura o humedad	2	4	No disponibilidad del computador	192
			[E.2]Errores del administrador del sistema/ seguridad	2	4	Errores en la operación	192
			[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5	Errores en la operación	240
			[A.11]Acceso no autorizado	2	4	Uso incorrecto del computador	192
			[A.23]Manipulación del hardware	2	5	Mal uso del recurso asignado	240
	COMPUTADORAS PERSONALES	**24**	[N.1]Fuego	1	5	No disponibilidad del computador	120
			[N.2]Daños por agua	2	5	No disponibilidad del computador	240
			[N. *]Desastres naturales	2	5	No disponibilidad del computador	240
			[1.3]Contaminación ambiental	2	4	No disponibilidad del computador	192
			[I.5]Avería de origen físico o lógico	3	3	No disponibilidad del computador	216
			[I.7]Condiciones inadecuadas de temperatura o humedad	2	4	No disponibilidad del computador	192
			[E.2]Errores del administrador del sistema/ seguridad	2	4	Errores en la operación	192
			[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5	Errores en la operación	240

			[A.11]Acceso no autorizado	2	4	Uso incorrecto del computador	192
			[A.23]Manipulación del hardware	2	5	Mal uso del recurso asignado	240
	IMPRESORAS	**17**	[I.5]Avería de origen físico o lógico	3	3	No disponibilidad de impresiones	153
			[I.7]Condiciones inadecuadas de temperatura o humedad	2	5	No disponibilidad de impresiones	170
			[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5	Errores en la operación	170
			[A.11]Acceso no autorizado	2	4	Uso incorrecto de impresoras	136
	SWITCH	**17**	[N.1]Fuego	1	5	No disponibilidad de switch	85
			[N.2]Daños por agua	2	5	No disponibilidad de switch	170
			[I.6]Corte del suministro eléctrico	2	5	No disponibilidad de switch	170
			[E.21]Errores de mantenimiento software/ actualización de programas software	2	5	Errores en la operación	170
			[A.6]Abuso de privilegios de acceso	2	4	Errores en la operación	136
			[A.11]Acceso no autorizado	2	5	Uso incorrecto de switch	170
			[A.25]Robo de equipos	1	5	No disponibilidad de switch	85

			[A.26]Ataque destructivos	2	5	No disponibilidad de switch	170
	FIREWALL	**24**	[I.6]Corte del suministro eléctrico	2	5	No disponibilidad del firewall	240
			[I.7]Condiciones inadecuadas de temperatura o humedad	2	5	No disponibilidad del firewall	240
	ROUTER	**19**	[N.1]Fuego	1	5	No disponibilidad de switch	95
			[N.2]Daños por agua	2	5	No disponibilidad de router	190
			[I.6]Corte del suministro eléctrico	2	5	No disponibilidad de Router	190
			[E.21]Errores de mantenimiento software/ actualización de programas software	2	5	Errores en la operación	190
			[A.6]Abuso de privilegios de acceso	2	4	Errores en la operación	152
			[A.11]Acceso no autorizado	2	5	Uso incorrecto de Router	190
			[A.25]Robo de equipos	1	5	No disponibilidad de Router	95
			[A.26]Ataque destructivos	2	5	No disponibilidad de Router	190
	ACCESS POINT	**20**	[I.1] Fuego	1	5	No disponibilidad de Access Point	100
			[I.2] Daños por agua	2	5	No disponibilidad de Access Point	200
			[I.*] Desastres industriales	2	5	No disponibilidad de Access Point	200

			[I.5] Avería de origen físico o lógico	3	3	No disponibilidad de Access Point	180
			[E.4] Errores de configuración	2	4	Errores en la operación	160
	RELOJES BIOMÉTRICOS	**23**	[I.1] Fuego	1	5	No disponibilidad de relojes biométricos	115
			[I.2] Daños por agua	2	5	No disponibilidad de relojes biométricos	230
			[I.*] Desastres industriales	3	5	No disponibilidad de relojes biométricos, otros desastres debidos a la actividad humana: corte de cables.	345
			[A.11]Acceso no autorizado	2	5	Uso incorrecto de relojes biométricos	230
			[A.25] Robo	1	5	No disponibilidad de relojes biométricos	115
	SERVIDORES FISICOS	**18**	[N.1]Fuego	1	5	No disponibilidad de servidores físicos	90
			[N.2]Daños por agua	2	5	No disponibilidad de servidores físicos	180
			[N. *]Desastres naturales	2	5	No disponibilidad de servidores físicos	180

			[1.3]Contaminación ambiental	2	4	No disponibilidad de servidores físicos	144
			[I.5]Avería de origen físico o lógico	3	3	No disponibilidad de servidores físicos	162
			[I.7]Condiciones inadecuadas de temperatura o humedad	2	5	No disponibilidad de servidores físicos	180
			[E.2]Errores del administrador del sistema/ seguridad	2	5	Errores en la operación	180
			[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5	Errores en la operación	180
			[A.11]Acceso no autorizado	2	5	Uso incorrecto de los servidores	180
			[A.23]Manipulación del hardware	2	5	No disponibilidad de servidores físicos	180
[COM] REDES DE COMUNICACIONES	**TELEFONÍA IP**	**20**	[1.8]Fallo de servicios de comunicaciones	2	5	No disponibilidad de telefonía ip	200
			[E.9]Errores de re-encaminamiento	2	4	No disponibilidad de telefonía ip	160
			[E.15] Alteración de la información	2	5	Mal uso del recurso asignado	200
			[E.19]Fugas de información	2	4	Mal uso del recurso asignado	160
			[A.7]Uso no previsto	2	4	Mal uso del recurso asignado	160

			[A.9]Encaminamiento de mensajes	2	4	No disponibilidad de telefonía ip	160
			[A.10]Alteración de secuencia	2	5	Mal uso del recurso asignado	200
			[A.12]Análisis de trafico	2	5	No disponibilidad de telefonía ip	200
			[A.14]1nterceptación de información (escucha)	2	5	Errores en la operación	200
	RED LAN	**15**	[I.8]Fallo de servicios de comunicaciones	2	4	No disponibilidad de las redes	120
			[E.9]Errores de re-encaminamiento	2	5	No disponibilidad de las redes	150
			[E.10]Errores de secuencia	2	5	No disponibilidad de las redes	150
			[A.5]Suplantación de la identidad	2	5	Errores en la operación	150
			[A.9]Encaminamiento de mensajes	2	4	Errores en la operación	120
			[A.10] Alteración de secuencia	2	4	Errores en la operación	120
			[A.11]Acceso no autorizado	2	5	Mal uso del recurso asignado	150
	RED WIFI	**20**	[I.8]Fallo de servicios de comunicaciones	2	5	No disponibilidad de las redes	200
			[E.9]Errores de re-encaminamiento	2	5	No disponibilidad de las redes	200
	INTERNET	**16**	[I.8]Fallo de servicios de comunicaciones	2	5	No disponibilidad de las redes	160

			[E.15] Alteración de la información	2	4	Errores en la operación	128
	CABLEADO	**16**	[I.1] Fuego	1	5	No disponibilidad del cableado	80
			[I.2] Daños por agua	2	5	No disponibilidad del cableado	160
			[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	No disponibilidad del cableado	160
			[I.11] Emanaciones electromagnéticas	2	5	No disponibilidad del cableado	160
			[I.*] Desastres industriales	2	4	No disponibilidad del cableado	128
			[A.25] Robo	1	5	No disponibilidad de la planta eléctrica	80
	PLANTA ELÉCTRICA	**19**	[I.1] Fuego	1	5	No disponibilidad de la planta eléctrica	95
			[I.2] Daños por agua	1	5	No disponibilidad de la planta eléctrica	95
			[I.9] Interrupción de otros servicios y suministros esenciales	2	5	No disponibilidad de la planta eléctrica	190
			[I.*] Desastres industriales	2	5	No disponibilidad de la planta eléctrica	190
			[A.25] Robo	2	5	No disponibilidad de UPS	190

	UPS	**16**	[I.1] Fuego	2	5	No disponibilidad de UPS	160
			[I.2] Daños por agua	2	5	No disponibilidad de UPS	160
			[I.*] Desastres industriales	2	5	No disponibilidad de UPS	160
			[A.25] Robo	1	5	No disponibilidad de Fuentes de alimentación	80
	FUENTES DE ALIMENTACIÓN	**12**	[I.1] Fuego	2	5	No disponibilidad de Fuentes de alimentación	120
			[I.2] Daños por agua	2	5	No disponibilidad de Fuentes de alimentación	120
			[I.*] Desastres industriales	2	5	No disponibilidad de Fuentes de alimentación	120
			[A.25] Robo	1	5	No disponibilidad de fibra	60
	FIBRA ÓPTICA	**20**	[I.1] Fuego	2	5	No disponibilidad de fibra	200
			[I.2] Daños por agua	2	5	No disponibilidad de fibra	200
			[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	No disponibilidad de fibra	160

			[I.*] Desastres industriales	2	5	No disponibilidad de fibra	200
			[A.25] Robo	1	5	No disponibilidad del sistema biométrico	100
[SS] SERVICIOS SUBCONTRATADOS	**SISTEMA SIRHA(SISTEMA BIOMÉTRICO)**	**18**	[I.5] Avería de origen físico o lógico	3	4	Pérdida de integridad en los datos del sistema biométrico	216
			[E.15] Alteración accidental de la información	2	5	No disponibilidad del sistema biométrico	180
			[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	Robo de información	216
			[A.5] Suplantación de la identidad del usuario	2	5	No disponibilidad del servicio	180
			[A.24] Denegación de servicio	2	5	No disponibilidad del sistema de nomina	180
	SISTEMA SIAP(NÓMINA ROL DE PAGOS)	**22**	[I.5] Avería de origen físico o lógico	3	3	Pérdida de integridad del sistema de nómina	198
			[E.15] Alteración accidental de la información	2	5	No disponibilidad del sistema de nómina	220
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad del sistema de nómina	220

			[A.5] Suplantación de la identidad del usuario	2	5	No disponibilidad del sistema de nómina	220
			[A.24] Denegación de servicio	2	5	No disponibilidad del sistema	220
[L] INSTALACIONES }	**OFICINAS**	**8**	[I.1] Fuego	1	5	No disponibilidad de oficinas	40
			[I.2] Daños por agua	2	5	No disponibilidad de oficinas	80
			[I.*] Desastres industriales	2	5	Daños de oficinas	80
			[A.26]Ataque destructivos	2	5	Daños de oficinas	80
			[A.27] Ocupación enemiga	2	5	No disponibilidad de vehículos	80
	VEHÍCULOS	**8**	[I.1] Fuego	1	5	No disponibilidad de vehículos	40
			[I.2] Daños por agua	2	5	Daños de vehículos	80
			[A.26]Ataque destructivos	2	5	Daños de vehículos	80
			[I.*] Desastres industriales	2	5	No disponibilidad de oficinas	80
	ESTACIONES TROLEBÚS Y ECOVIA	**8**	[I.1] Fuego	1	5	No disponibilidad de oficinas	40
			[I.2] Daños por agua	2	5	No disponibilidad de oficinas	80

			[I.*] Desastres industriales	2	5	Daños de oficinas	80
			[A.26]Ataque destructivos	2	5	Daños de oficinas	80
			[A.27] Ocupación enemiga	2	5	Abandono de trabajo	80
[P] PERSONAL	**COORDINADOR DE SISTEMAS INFORMÁTICOS**	**16**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	128
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	128
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	128
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	160
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	80
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	192
	COORDINADOR DE REDES Y TELECOMUNICACIONES	**16**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	128
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	128
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	128
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	160

			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	80
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	192
	ESPECIALISTAS DE TECNOLOGÍAS 2	**15**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	120
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	120
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	120
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	150
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	75
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	180
	ESPECIALISTA DE BIENES 2	**11**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	88
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	88
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	88

			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	110
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	55
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	132
	TÉCNICOS ADMINISTRATIVO DE BIENES	**11**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	88
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	88
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	88
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	110
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	55
			[A.30] ingeniería social (picaresca)	3	4	Abandono de trabajo	132
	ESPECIALISTA DE TELECOMUNICACIONES 4	**12**	[E.7]Deficiencias en la organización	2	4	Perdida de integridad de información	96
			[E.14]Fugas de información (>E.19)	2	4	Abandono de trabajo	96
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	96

			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	120
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	60
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	144
	COORDINADORA DE TALENTO HUMANO	**15**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	120
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	120
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	120
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	150
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	75
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	180
	COORDINADORA DE SEGURIDAD	**13**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	104
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	104
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	104

			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	130
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	65
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	156

ANEXO F- IDENTIFICACIÓN, VALORACIÓN DE SALVAGUARDAS Y RIESGO RESIDUAL.

En la siguiente tabla se identifican y valoran las salvaguardas que nos permiten mitigar las amenazas a las que están expuestos los activos de la Empresa Pública Metropolitana de Transporte de Pasajeros de Quito según las amenazas a las que está expuesto.

Las amenazas identificadas correspondientes al listado que sumista la metodología Magerit en su Libro II que se visualiza en el anexo C, las salvaguardas han sido valoradas de acuerdo al porcentaje del 1 al 100% el análisis de las salvaguardas se realizó conjuntamente con los especialistas del área de tecnologías y se determinó los resultados dejando valores aceptables del riesgo residual a continuación se muestra en la tabla.

ACTIVOS		VALOR DEL ACTIVO	AMENAZA	FRECUENCIA O PROBBABILIDAD	DEGRADACIÓN O IMPACTO	RIESGO ASOCIADO A LA AMENAZA	VALOR DEL RIESGO	SALVAGUARDAS	VALOR SALVAGUARDAS %	VALOR RIESGO RESIDUAL
[D] DATOS/INFORMACIÓN	COPIA DE RESPALDO	**28**	[E.1] Errores de los usuarios	2	**4**	Pérdida de información	224	Pruebas de Cambios en el sistema antes de salir a operación	60	89,6
			[E.2] Errores del administrador	3	4	Pérdida de Integridad en la copia de respaldo	336	Copias de Seguridad de los datos (backup)	80	67,2
	DATOS DE ACCESO A SERVIDORES	**27**	[E.7] Deficiencias en la organización	2	4	Abandono del trabajo	216	Revisión de políticas internas	60	86,4
			[A.4] Manipulación de la configuración	3	5	Pérdida de integridad en los datos de acceso a servidores	405	Aseguramiento de la integridad	80	81

			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	270	Continuidad del negocio	65	94,5
			[A.11] Acceso no autorizado	2	5	Pérdida de Integridad y confidencialidad de datos de acceso a servidores	270	Establecimiento de perfiles de usuarios	65	94,5
	DATOS DE ACCESO A USUARIOS	**27**	[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	270	Revisión de políticas internas	69	83,7
			[A.11] Acceso no autorizado	2	4	Pérdida de Integridad y confidencialidad de datos de acceso a servidores	216	Establecimiento de perfiles de usuarios	60	86,4
	CÓDIGOS FUENTES SW	**27**	[E.20] Vulnerabilidades de los programas (software)	3	5	Fallos en su código o en su configuración	405	Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.	85	60,75
			[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	No disponibilidad de códigos fuentes	324	Modificación del software para mejorar las propiedades de dicho software (calidad y mantenibilidad) sin alterar sus especificaciones funcionales, reestructuración de los programas para aumentar su legibilidad.	80	64,8

			[A.5] Suplantación de la identidad del usuario	3	5	Manipulación de códigos fuentes	405	Implementar seguridad e n los accesos de usuarios por medio de técnicas de autenticación y autorización.	80	81
[IS] SERVICIOS INTERNOS	**SERVICIO DE INTERNET**	**24**	[I.6] Corte del suministro eléctrico	2	5	No disponibilidad de internet	240	Implementación del sistema de contingencia	65	84
			[I.8] Fallo de servicios de comunicaciones	2	4	No disponibilidad mediante el servicio de internet	192	Implementación del sistema de contingencia	50	96
			[I.9] Interrupción de otros servicios y suministros esenciales	2	4	No disponibilidad de algunos servicios	192	Implementación del sistema de contingencia	65	67,2
			[A.7] Uso no previsto	2	3	Mal uso del recurso asignado	144	Implementación del sistema de contingencia	60	57,6
	SERVICIO DE TELEFONÍA	**22**	[E.1] Errores de los usuarios	2	4	Pérdida del servicio de telefonía	176	Pruebas de Cambios en el sistema antes de salir a operación	60	70,4
			[E.2] Errores del administrador	3	4	Interrupciones programadas	264	Copias de Seguridad (backup)	75	66
			[I.8] Fallo de servicios de comunicaciones	2	4	No disponibilidad del servicio de telefonía	176	Implementación del sistema de contingencia	65	61,6

			[I.9] Interrupción de otros servicios y suministros esenciales	2	4	Pérdida de comunicaciones el personal interno	176	Implementación del sistema de contingencia	65	61,6
	SERVICIO DE MANTENIMIENTO	13	[E.7] Deficiencias en la organización	3	5	Abandono del trabajo	195	Revisión de políticas internas	55	87,75
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	No disponibilidad del servicio de software	104	Cambios (actualizaciones y mantenimiento)	60	41,6
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	4	No disponibilidad del servicio de hardware	104	Cambios (actualizaciones y mantenimiento)	55	46,8
			[E.28] Indisponibilidad del personal	2	3	Falta de personal	78	Medición de capacity	40	46,8
[SW] SOFTWARE(APLICACIONES INFORMÁTICAS)	OFIMÁTICA	20	[E.21] Errores de mantenimiento / actualización de programas (software)	2	3	No disponibilidad de paquete de ofimática	120	Cambios (actualizaciones y mantenimiento)	50	60
			[E.1] Errores de los usuarios	2	4	Desinstalación de programas	160	Capacitación del personal	60	64
	ANTIVIRUS	17	[E.8] Difusión de software dañino	2	4	Infección mediante aplicaciones	136	Implementación de antivirus	40	81,6
			[E.20] Vulnerabilidades de los programas (software)	2	5	Fallos en los antivirus	170	Soporte por parte del proveedor	50	85

			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad de antivirus	170	Cambios (actualizaciones y mantenimiento)	50	85
	SISTEMA BIOMÉTRICO SIRHA	**18**	[I.5] Avería de origen físico o lógico	3	3	No disponibilidad del sistema biométrico	162	Soporte por parte del proveedor	55	72,9
			[E.15] Alteración accidental de la información	2	4	Pérdida de integridad en los datos del sistema biométrico	144	Soporte por parte del proveedor	40	86,4
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	No disponibilidad del sistema biométrico	144	Cambios (actualizaciones y mantenimiento)	56	63,36
			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	180	Soporte por parte del proveedor	65	63
			[A.24] Denegación de servicio	2	4	No disponibilidad del servicio	144	Implementación del sistema de contingencia	50	72
	SISTEMA DE GESTIÓN DE BASE DE DATOS	**19**	[I.5] Avería de origen físico o lógico	3	3	No disponibilidad del sistema de base de datos	190	Soporte por parte del proveedor	60	76
			[E.15] Alteración accidental de la información	2	5	Pérdida de integridad en los datos del sistema de BD	190	Protección de las Aplicaciones Informáticas	65	66,5
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad del sistema de base de datos	190	Cambios (actualizaciones y mantenimiento)	60	76
			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	190	Se aplican perfiles de seguridad	55	85,5

	SERVIDOR DE CORREO(APLICACIÓN DE RED)	**19**	[I.5] Avería de origen físico o lógico	3	3	No disponibilidad del correo electrónico	171	Soporte por parte del proveedor	50	85,5
			[E.15] Alteración accidental de la información	2	5	Pérdida de integridad de los correos	190	Protección de las Aplicaciones Informática	45	104,5
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad del sistema de nomina	190	Cambios (actualizaciones y mantenimiento)	40	114
			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	190	Se aplican perfiles de seguridad	60	76
	SISTEMA DE NÓMINA SIAP	**22**	[I.5] Avería de origen físico o lógico	3	3	No disponibilidad del sistema de nómina	198	Soporte por parte del proveedor	45	108,9
			[E.15] Alteración accidental de la información	3	5	Pérdida de integridad del sistema de nómina, debido a la alteración accidental de la información	330	Se aplican perfiles de seguridad	60	132
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad del sistema de nomina	220	Cambios (actualizaciones y mantenimiento)	45	121
			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	220	Se aplican perfiles de seguridad	46	118,8

			[A.24] Denegación de servicio	2	4	No disponibilidad del sistema de nomina	176	Implementación del sistema de contingencia	65	61,6
	SOFTWARE NETWORKING	18	[I.5] Avería de origen físico o lógico	3	3	No disponibilidad del sistema de almacenamiento de datos	162	Soporte por parte del proveedor	40	97,2
			[E.15] Alteración accidental de la información	2	4	Perdida de integridad de información	144	Protección de directorio	50	72
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad del sistema de almacenamiento de datos	180	Cambios (actualizaciones y mantenimiento)	55	81
			[A.5] Suplantación de la identidad del usuario	2	5	Robo de información	180	Se aplican perfiles de seguridad	50	90
[HW] HARDWARE (EQUIPOS INFORMÁTICOS)	COMPUTADORAS DE ESCRITORIO	24	[N.1]Fuego	1	5	No disponibilidad del computador	120	Establecimiento de políticas de buen uso de recursos	60	48
			[N.2]Daños por agua	2	5	No disponibilidad del computador	240	Establecimiento de políticas de buen uso de recursos	65	84
			[N. *]Desastres naturales	2	5	No disponibilidad del computador	240	Continuidad del negocio	50	120
			[1.3]Contaminación ambiental	2	4	No disponibilidad del computador	192	Aseguramiento de la disponibilidad	65	67,2
			[I.5]Avería de origen físico o lógico	3	3	No disponibilidad del computador	216	Soporte por parte del proveedor	70	64,8
			[I.7]Condiciones inadecuadas de temperatura o humedad	2	4	No disponibilidad del computador	192	Climatización	60	76,8
			[E.2]Errores del administrador del sistema/ seguridad	2	4	Errores en la operación	192	Protección de los Equipos Informáticos	55	86,4

			[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5	Errores en la operación	240	Cambios (actualizaciones y mantenimiento)	60	96
			[A.11]Acceso no autorizado	2	4	Uso incorrecto del computador	192	Establecimiento de perfiles de usuarios	55	86,4
			[A.23]Manipulación del hardware	2	5	Mal uso del recurso asignado	240	Aseguramiento de la disponibilidad	60	96
	COMPUTADORAS PERSONALES	**24**	[N.1]Fuego	1	5	No disponibilidad del computador	120	Establecimiento de políticas de buen uso de recursos	55	54
			[N.2]Daños por agua	2	5	No disponibilidad del computador	240	Establecimiento de políticas de buen uso de recursos	55	108
			[N. *]Desastres naturales	2	5	No disponibilidad del computador	240	Control de los accesos físicos	65	84
			[1.3]Contaminación ambiental	2	4	No disponibilidad del computador	192	Aseguramiento de la disponibilidad	69	59,52
			[I.5]Avería de origen físico o lógico	3	3	No disponibilidad del computador	216	Soporte por parte del proveedor	60	86,4
			[I.7]Condiciones inadecuadas de temperatura o humedad	2	4	No disponibilidad del computador	192	Climatización	55	86,4
			[E.2]Errores del administrador del sistema/ seguridad	2	4	Errores en la operación	192	Protección de los Equipos Informáticos	55	86,4
			[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5	Errores en la operación	240	Cambios (actualizaciones y mantenimiento)	55	108

			[A.11]Acceso no autorizado	2	4	Uso incorrecto del computador	192	Establecimiento de perfiles de usuarios	65	67,2
			[A.23]Manipulación del hardware	2	5	Mal uso del recurso asignado	240	Aseguramiento de la disponibilidad	50	120
	IMPRESORAS	**17**	[I.5]Avería de origen físico o lógico	3	3	No disponibilidad de impresiones	153	Soporte por parte del proveedor	55	68,85
			[I.7]Condiciones inadecuadas de temperatura o humedad	2	5	No disponibilidad de impresiones	170	Climatización	55	76,5
			[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5	Errores en la operación	170	Cambios (actualizaciones y mantenimiento)	60	68
			[A.11]Acceso no autorizado	2	4	Uso incorrecto de impresoras	136	Establecimiento de perfiles de usuarios	50	68
	SWITCH	**17**	[N.1]Fuego	1	5	No disponibilidad de switch	85	Establecimiento de políticas de buen uso de recursos	50	42,5
			[N.2]Daños por agua	2	5	No disponibilidad de switch	170	Establecimiento de políticas de buen uso de recursos	50	85
			[I.6]Corte del suministro eléctrico	2	5	No disponibilidad de switch	170	Implementación del sistema de contingencia	60	68
			[E.21]Errores de mantenimiento software/ actualización de programas software	2	5	Errores en la operación	170	Cambios (actualizaciones y mantenimiento)	50	85

			[A.6]Abuso de privilegios de acceso	2	4	Errores en la operación	136	Establecimiento de perfiles de usuarios	55	61,2
			[A.11]Acceso no autorizado	2	5	Uso incorrecto de switch	170	Establecimiento de perfiles de usuarios	55	76,5
			[A.25]Robo de equipos	1	5	No disponibilidad de switch	85	Sistemas de mecanismos de monitoreo y vigilancia	55	38,25
			[A.26]Ataque destructivos	2	5	No disponibilidad de switch	170	Aseguramiento de la disponibilidad	55	76,5
	FIREWALL	**24**	[I.6]Corte del suministro eléctrico	2	5	No disponibilidad del firewall	240	Implementación del sistema de contingencia	55	108
			[I.7]Condiciones inadecuadas de temperatura o humedad	2	5	No disponibilidad del firewall	240	Climatización	50	120
	ROUTER	**19**	[N.1]Fuego	1	5	No disponibilidad de switch	95	Establecimiento de políticas de buen uso de recursos	65	33,25
			[N.2]Daños por agua	2	5	No disponibilidad de Router	190	Establecimiento de políticas de buen uso de recursos	65	66,5
			[I.6]Corte del suministro eléctrico	2	5	No disponibilidad de Router	190	Implementación del sistema de contingencia	50	95

			[E.21]Errores de mantenimiento software/ actualización de programas software	2	5	Errores en la operación	190	Cambios (actualizaciones y mantenimiento)	65	66,5
			[A.6]Abuso de privilegios de acceso	2	4	Errores en la operación	152	Establecimiento de perfiles de usuarios	50	76
			[A.11]Acceso no autorizado	2	5	Uso incorrecto de Routers	190	Establecimiento de perfiles de usuarios	60	76
			[A.25]Robo de equipos	1	5	No disponibilidad de Router	95	Sistemas de mecanismos de monitoreo y vigilancia	55	42,75
			[A.26]Ataque destructivos	2	5	No disponibilidad de Router	190	Sistemas de mecanismos de monitoreo y vigilancia	60	76
	ACCESS POINT	**20**	[I.1] Fuego	1	5	No disponibilidad de Access Point	100	Establecimiento de políticas de buen uso de recursos	50	50
			[I.2] Daños por agua	2	5	No disponibilidad de Access Point	200	Establecimiento de políticas de buen uso de recursos	60	80
			[I.*] Desastres industriales	2	5	No disponibilidad de Access Point	200	Continuidad del negocio	80	40
			[I.5] Avería de origen físico o lógico	3	3	No disponibilidad de Access Point	180	Soporte por parte del proveedor	65	63
			[E.4] Errores de configuración	2	4	Errores en la operación	160	Soporte por parte del proveedor	60	64

	RELOJES BIOMÉTRICOS	**23**	[I.1] Fuego	1	5	No disponibilidad de relojes biométricos	115	Establecimiento de políticas de buen uso de recursos	60	46
			[I.2] Daños por agua	2	5	No disponibilidad de relojes biométricos	230	Establecimiento de políticas de buen uso de recursos	56	101,2
			[I.*] Desastres industriales	3	5	No disponibilidad de relojes biométricos, otros desastres debidos a la actividad humana: corte de cables.	345	Continuidad del Negocio y Recuperación de Desastres	55	155,25
			[A.11]Acceso no autorizado	2	5	Uso incorrecto de relojes biométricos	230	Establecimiento de perfiles de usuarios	50	115
			[A.25] Robo	1	5	No disponibilidad de relojes biométricos	115	Sistemas de mecanismos de monitoreo y vigilancia	65	40,25
	SERVIDORES FISICOS	**18**	[N.1]Fuego	1	5	No disponibilidad de servidores físicos	90	Establecimiento de políticas de buen uso de recursos	60	36
			[N.2]Daños por agua	2	5	No disponibilidad de servidores físicos	180	Establecimiento de políticas de buen uso de recursos	50	90
			[N. *]Desastres naturales	2	5	No disponibilidad de servidores físicos	180	Continuidad del negocio	65	63
			[1.3]Contaminación ambiental	2	4	No disponibilidad de servidores físicos	144	Aseguramiento de la disponibilidad	55	64,8
			[I.5]Avería de origen físico o lógico	3	3	No disponibilidad de servidores físicos	162	Soporte por parte del proveedor	60	64,8

			[I.7]Condiciones inadecuadas de temperatura o humedad	2	5	No disponibilidad de servidores físicos	180	Climatización	55	81
			[E.2]Errores del administrador del sistema/ seguridad	2	5	Errores en la operación	180	Aseguramiento de la disponibilidad	60	72
			[E.23]Errores de mantenimiento hardware/ actualización de programas hardware	2	5	Errores en la operación	180	Cambios (actualizaciones y mantenimiento)	45	99
			[A.11]Acceso no autorizado	2	5	Uso incorrecto de los servidores	180	Establecimiento de perfiles de usuarios	60	72
			[A.23]Manipulación del hardware	2	5	No disponibilidad de servidores físicos	180	Establecimiento de políticas de buen uso de recursos	45	99
[COM] REDES DE COMUNICACIONES	**TELEFONÍA IP**	**20**	[1.8]Fallo de servicios de comunicaciones	2	5	No disponibilidad de telefonía IP	200	Protección de las Comunicaciones	45	110
			[E.9]Errores de re-encaminamiento	2	4	No disponibilidad de telefonía IP	160	Protección de las Comunicaciones	45	88
			[E.15] Alteración de la información	2	5	Mal uso del recurso asignado	200	Se aplican perfiles de seguridad	69	62
			[E.19]Fugas de información	2	4	Mal uso del recurso asignado	160	Se aplican perfiles de seguridad	45	88
			[A.7]Uso no previsto	2	4	Mal uso del recurso asignado	160	Establecimiento de políticas de buen uso de recursos	45	88
			[A.9]Encaminamiento de mensajes	2	4	No disponibilidad de telefonía IP	160	Aseguramiento de la disponibilidad	45	88
			[A.10]Alteración de secuencia	2	5	Mal uso del recurso asignado	200	Se aplican perfiles de seguridad	45	110

			[A.12]Análisis de trafico	2	5	No disponibilidad de telefonía IP	200	Aseguramiento de la disponibilidad	65	70
			[A.14]1nterceptación de información (escucha)	2	5	Errores en la operación	200	Protección de las Comunicaciones	50	100
	RED LAN	**15**	[I.8]Fallo de servicios de comunicaciones	2	4	No disponibilidad de las redes	120	Protección de las Comunicaciones	50	60
			[E.9]Errores de re-encaminamiento	2	5	No disponibilidad de las redes	150	Protección de las Comunicaciones	55	67,5
			[E.10]Errores de secuencia	2	5	No disponibilidad de las redes	150	Establecimiento de políticas de buen uso de recursos	60	60
			[A.5]Suplantación de la identidad	2	5	Errores en la operación	150	Protección de la integridad de los datos intercambiados	55	67,5
			[A.9]Encaminamiento de mensajes	2	4	Errores en la operación	120	Se aplican perfiles de seguridad	55	54
			[A.10] Alteración de secuencia	2	4	Errores en la operación	120	Se aplican perfiles de seguridad	56	52,8
			[A.11]Acceso no autorizado	2	5	Mal uso del recurso asignado	150	Se aplican perfiles de seguridad	56	66
	RED WIFI	**20**	[I.8]Fallo de servicios de comunicaciones	2	5	No disponibilidad de las redes	200	Seguridad Wireless (Wifi)	61	78
			[E.9]Errores de re-encaminamiento	2	5	No disponibilidad de las redes	200	Seguridad Wireless (Wifi)	61	78
	INTERNET	**16**	[I.8]Fallo de servicios de comunicaciones	2	5	No disponibilidad de las redes	160	Protección de la comunicaciones	61	62,4
			[E.15] Alteración de la información	2	4	Errores en la operación	128	Se aplican perfiles de seguridad	56	56,32

	CABLEADO	**16**	[I.1] Fuego	1	5	No disponibilidad del cableado	80	Establecimiento de políticas de buen uso de recursos	50	40
			[I.2] Daños por agua	2	5	No disponibilidad del cableado	160	Establecimiento de políticas de buen uso de recursos	61	62,4
			[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	No disponibilidad del cableado	160	Climatización	61	62,4
			[I.11] Emanaciones electromagnéticas	2	5	No disponibilidad del cableado	160	Puntos de interconexión: conexiones entre zonas de confianza	61	62,4
			[I.*] Desastres industriales	2	4	No disponibilidad del cableado	128	Puntos de interconexión: conexiones entre zonas de confianza	56	56,32
			[A.25] Robo	1	5	No disponibilidad de la planta eléctrica	80	Aseguramiento del medio donde se encuentran el cableado	55	36
	PLANTA ELÉCTRICA	**19**	[I.1] Fuego	1	5	No disponibilidad de la planta eléctrica	95	Establecimiento de políticas de buen uso de recursos	55	42,75
			[I.2] Daños por agua	1	5	No disponibilidad de la planta eléctrica	95	Establecimiento de políticas de buen uso de recursos	45	52,25

			[I.9] Interrupción de otros servicios y suministros esenciales	2	5	No disponibilidad de la planta eléctrica	190	Establecimiento de políticas de buen uso de recursos	61	74,1
			[I.*] Desastres industriales	2	5	No disponibilidad de la planta eléctrica	190	Continuidad del negocio	61	74,1
			[A.25] Robo	2	5	No disponibilidad de UPS	190	Sistemas de mecanismos de monitoreo y vigilancia	61	74,1
	UPS	**16**	[I.1] Fuego	2	5	No disponibilidad de UPS	160	Puesta en producción	61	62,4
			[I.2] Daños por agua	2	5	No disponibilidad de UPS	160	Puesta en producción	61	62,4
			[I.*] Desastres industriales	2	5	No disponibilidad de UPS	160	Puesta en producción	61	62,4
			[A.25] Robo	1	5	No disponibilidad de Fuentes de alimentación	80	Aseguramiento del medio donde se encuentran los UPS	45	44
	FUENTES DE ALIMENTACIÓN	**12**	[I.1] Fuego	2	5	No disponibilidad de Fuentes de alimentación	120	Establecimiento de políticas de buen uso de recursos	45	66
			[I.2] Daños por agua	2	5	No disponibilidad de Fuentes de alimentación	120	Establecimiento de políticas de buen uso de recursos	45	66
			[I.*] Desastres industriales	2	5	No disponibilidad de Fuentes de alimentación	120	Puesta en producción	45	66
			[A.25] Robo	1	5	No disponibilidad de fibra	60	Aseguramiento del medio donde se encuentran las fuentes de alimentación	55	27

	FIBRA ÓPTICA	**20**	[I.1] Fuego	2	5	No disponibilidad de fibra	200	Establecimiento de políticas de buen uso de recursos	69	62
			[I.2] Daños por agua	2	5	No disponibilidad de fibra	200	Establecimiento de políticas de buen uso de recursos	45	110
			[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	No disponibilidad de fibra	160	Climatización	45	88
			[I.*] Desastres industriales	2	5	No disponibilidad de fibra	200	Continuidad del negocio	45	110
			[A.25] Robo	1	5	No disponibilidad del sistema biométrico	100	Aseguramiento del medio donde se encuentra la fibra óptica	45	55
[SS] SERVICIOS SUBCONTRATADOS	**SISTEMA SIRHA(SISTEMA BIOMÉTRICO)**	**18**	[I.5] Avería de origen físico o lógico	3	4	Pérdida de integridad en los datos del sistema biométrico	216	Soporte por parte del proveedor	65	75,6
			[E.15] Alteración accidental de la información	2	5	No disponibilidad del sistema biométrico	180	Aseguramiento de la disponibilidad	50	90
			[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	Robo de información	216	Cambios (actualizaciones y mantenimiento)	65	75,6
			[A.5] Suplantación de la identidad del usuario	2	5	No disponibilidad del servicio	180	Establecimiento de perfiles de usuarios	45	99
			[A.24] Denegación de servicio	2	5	No disponibilidad del sistema de nomina	180	Implementación del sistema de contingencia	60	72

	SISTEMA SIAP(NÓMINA ROL DE PAGOS)	**22**	[I.5] Avería de origen físico o lógico	3	3	Pérdida de integridad del sistema de nómina	198	Soporte por parte del proveedor	45	108,9
			[E.15] Alteración accidental de la información	2	5	No disponibilidad del sistema de nómina	220	Aseguramiento de la disponibilidad	65	77
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	5	No disponibilidad del sistema de nómina	220	Cambios (actualizaciones y mantenimiento)	65	77
			[A.5] Suplantación de la identidad del usuario	2	5	No disponibilidad del sistema de nómina	220	Establecimiento de perfiles de usuarios	55	99
			[A.24] Denegación de servicio	2	5	No disponibilidad del sistema	220	Implementación del sistema de contingencia	60	88
[L] INSTALACIONES }	**OFICINAS**	**8**	[I.1] Fuego	1	5	No disponibilidad de oficinas	40	Establecimiento de políticas de buen uso de recursos	40	24
			[I.2] Daños por agua	2	5	No disponibilidad de oficinas	80	Establecimiento de políticas de buen uso de recursos	45	44
			[I.*] Desastres industriales	2	5	Daños de oficinas	80	Continuidad del negocio	40	48
			[A.26]Ataque destructivos	2	5	Daños de oficinas	80	Sistemas de mecanismos de monitoreo y vigilancia	40	48
			[A.27] Ocupación enemiga	2	5	No disponibilidad de vehículos	80	Sistemas de mecanismos de monitoreo y vigilancia	40	48

	VEHÍCULOS	**8**	[I.1] Fuego	1	5	No disponibilidad de vehículos	40	Establecimiento de políticas de buen uso de recursos	40	24
			[I.2] Daños por agua	2	5	Daños de vehículos	80	Establecimiento de políticas de buen uso de recursos	40	48
			[A.26]Ataque destructivos	2	5	Daños de vehículos	80	Análisis de impacto	40	48
			[I.*] Desastres industriales	2	5	No disponibilidad de oficinas	80	Continuidad del negocio	40	48
	ESTACIONES TROLEBÚS Y ECOVIA	**8**	[I.1] Fuego	1	5	No disponibilidad de oficinas	40	Establecimiento de políticas de buen uso de recursos	35	26
			[I.2] Daños por agua	2	5	No disponibilidad de oficinas	80	Establecimiento de políticas de buen uso de recursos	40	48
			[I.*] Desastres industriales	2	5	Daños de oficinas	80	Continuidad del negocio	35	52
			[A.26]Ataque destructivos	2	5	Daños de oficinas	80	Sistemas de mecanismos de monitoreo y vigilancia	45	44
			[A.27] Ocupación enemiga	2	5	Abandono de trabajo	80	Sistemas de mecanismos de monitoreo y vigilancia	40	48

[P] PERSONAL	COORDINADOR DE SISTEMAS INFORMÁTICOS	16	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	128	Formación y concienciación	40	76,8
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	128	Gestión del Personal	45	70,4
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	128	Aseguramiento de la disponibilidad	45	70,4
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	160	Planificación de la seguridad	60	64
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	80	Estudio de seguridad	45	44
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	192	Capacitación del personal	65	67,2
	COORDINADOR DE REDES Y TELECOMUNICACIONES	16	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	128	Formación y concienciación	45	70,4
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	128	Gestión del Personal	45	70,4
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	128	Aseguramiento de la disponibilidad	40	76,8
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	160	Planificación de la seguridad	40	96
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	80	Estudio de seguridad	55	36
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	192	Capacitación del personal	60	76,8

	ESPECIALISTAS DE TECNOLOGÍAS 2	**15**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	120	Formación y concienciación	55	54
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	120	Gestión del Personal	50	60
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	120	Aseguramiento de la disponibilidad	55	54
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	150	Planificación de la seguridad	45	82,5
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	75	Estudio de seguridad	55	33,75
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	180	Capacitación del personal	55	81
	ESPECIALISTA DE BIENES 2	**11**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	88	Formación y concienciación	55	39,6
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	88	Gestión del Personal	55	39,6
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	88	Aseguramiento de la disponibilidad	55	39,6
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	110	Planificación de la seguridad	60	44
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	55	Estudio de seguridad	40	33
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	132	Capacitación del personal	60	52,8

	TÉCNICOS ADMINISTRATIVO DE BIENES	**11**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	88	Formación y concienciación	65	30,8
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	88	Gestión del Personal	69	27,28
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	88	Aseguramiento de la disponibilidad	75	22
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	110	Planificación de la seguridad	60	44
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	55	Estudio de seguridad	60	22
			[A.30] ingeniería social (picaresca)	3	4	Abandono de trabajo	132	Capacitación del personal	65	46,2
	ESPECIALISTA DE TELECOMUNICACIONES 4	**12**	[E.7]Deficiencias en la organización	2	4	Perdida de integridad de información	96	Formación y concienciación	65	33,6
			[E.14]Fugas de información (>E.19)	2	4	Abandono de trabajo	96	Gestión del Personal	50	48
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	96	Aseguramiento de la disponibilidad	65	33,6
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	120	Planificación de la seguridad	55	54
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	60	Estudio de seguridad	65	21
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	144	Capacitación del personal	60	57,6

	COORDINADORA DE TALENTO HUMANO	**15**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	120	Formación y concienciación	55	54
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	120	Gestión del Personal	55	54
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	120	Aseguramiento de la disponibilidad	50	60
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	150	Planificación de la seguridad	60	60
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	75	Estudio de seguridad	55	33,75
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	180	Capacitación del personal	65	63
	COORDINADORA DE SEGURIDAD	**13**	[E.7]Deficiencias en la organización	2	4	Abandono de trabajo	104	Formación y concienciación	40	62,4
			[E.14]Fugas de información (>E.19)	2	4	Robo de información	104	Gestión del Personal	40	62,4
			[A.6] Abuso de privilegios de acceso	2	4	Pérdida de información	104	Aseguramiento de la disponibilidad	50	52
			[A.18] Destrucción de información	2	5	Pérdida de confidencialidad de la operación	130	Planificación de la seguridad	60	52
			[A.29]Extorsión	1	5	Pérdida de confidencialidad de la operación	65	Estudio de seguridad	40	39
			[A.30] ingeniería social (picaresca)	3	4	Pérdida de confidencialidad de la operación	156	Capacitación del personal	60	62,4

ANEXO G- CUMPLIMIENTO DEL ANALISÍS DE GESTÍON DE RIESGOS

La tabla adjunta muestra el cumplimiento de la metodología que se escogió para realizar el análisis de gestión de riesgos tecnológicos así mismo el cumplimiento de los objetivos planteados para la propuesta de gestión de riesgos tecnológicos para la EPMTPQ.

OBJETIVOS	DESCRIPCIÓN	VALORACIÓN	DETALLE ACTIVOS MAYOR RIESGOS	CUMPLIMIENTO	RESPONSABLES
1.- Determinar los activos relevantes de la EPMTPQ y la valoración de aquellos.	Software y Hardware	En una escala del 1 al 10	Copia de respaldo	SI	Ing. Dennis Cueva. Ing. Sandro Enríquez. Ing. Julia Escobar. Ing. Juan Morocho. Ing. Carlos Taipe Ing. Fausto Valencia.
			Datos de acceso a servidores	SI	
		Confidencialidad, Integridad y Disponibilidad.	Códigos fuentes SW	SI	
		Valor del activo suma de C+I+D	Sistema de nómina SIAP	SI	
			Relojes biométricos	SI	
2.- Identificar las amenazas a los que están expuestos los activos y la valoración de la probabilidad o impacto de los mismos.	Se identificó de acuerdo al listado de amenazas Anexo C	En una escala del 1 al 5	[E.2] Errores del administrador	SI	
			[A.4] Manipulación de la configuración	SI	
			[E.20] Vulnerabilidades de los programas (software)	SI	
		Valoración de la Probabilidad o Impacto de los activos.	[E.21] Errores de mantenimiento / actualización de programas (software)	SI	

			[A.5] Suplantación de la identidad del usuario	SI	
			[E.15] Alteración accidental de la información	SI	
			[I.*] Desastres industriales	SI	
3.- Determinar el valor del riesgo asociado a las amenazas identificadas de acuerdo a la escala de colores de los niveles bajo, medio y alto.	Valoración del riesgo y el riesgo asociado a la amenaza	Valoración del riesgo escala de 0 a 750	Pérdida de integridad en la copia de respaldo	SI	
			Pérdida de integridad en los datos de acceso a servidores	SI	
			Fallos en su código o en su configuración.	SI	
		Valor del riesgo Activo*Probabilidad*Impacto.	No disponibilidad de códigos fuentes.	SI	
			Manipulación de códigos fuentes.	SI	
			Pérdida de integridad del sistema de nómina, debido a la alteración accidental de la información.	SI	
			No disponibilidad de relojes biométricos, otros desastres debidos a la actividad humana: corte de cables.	SI	
4.- Determinar que salvaguardas hay dispuestas y la valoración de cuán eficaces son frente al riesgo.	Identificación y valoración de salvaguardas	Valoración en una escala de 0 al 100%	Copias de Seguridad de los datos (backup)	SI	
			Aseguramiento de la integridad	SI	
			Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.	SI	

			Modificación del software para mejorar las propiedades de dicho software (calidad y mantenibilidad) sin alterar sus especificaciones funcionales, reestructuración de los programas para aumentar su legibilidad.	SI	
		Valor Riesgo. * (1-VALOR_SALVAGUARDA)	Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.	SI	
			Se aplican perfiles de seguridad	SI	

Conclusiones

- Todo cambio en roles, funciones o cargos de un funcionario, que requiera acceso a diferente información o infraestructura tecnológica de la EPMTPQ, debe ser notificado mediante memorando a la Gerencia de Tecnologías de la Información, para que procedan con el cambio respectivo.
- La Gerencia de Tecnologías de la Información a través de los Especialista o Analistas son responsables de revisar periódicamente las cuentas y permisos de acceso establecidos, con el fin de establecer los accesos de cada personal, de acuerdo a las necesidades de la EPMTPQ.
- La Gerencia de Tecnologías de la Información es responsable de auditar mensualmente los servidores de almacenamiento, para verificar la existencia de archivos no autorizados, configuraciones no válidas o permisos extras que pongan en riesgo la seguridad de la información.
- Todos los Funcionarios deben reportar de forma inmediata a la Gerencia de Tecnologías de la Información, los riesgos reales o potenciales que están expuestos los equipos computacionales en la estación de trabajo, durante el desempeño de sus funciones.