REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

CARRERA: MAESTRÍA EN EL CAMPO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

INFORME FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR, MODALIDAD PROYECTO DE INVESTIGACIÓN

TEMA:

PROTECCIÓN DE DATOS EN LA DIRECCION DE INFRACCIONES DE LA AGENCIA METROPOLITANA DE TRÁNSITO APLICANDO UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) CONSIDERANDO EL MARCO NORMATIVO VIGENTE Y CON UNA METODOLOGIA EGSI.

Trabajo de titulación previo a la obtención del título de Magister en Computación con mención en Seguridad Informática

Línea de investigación: Seguridad de la Información

AUTOR: ING.MAURICIO FABIAN MONTUFAR RIVERA

TUTOR: PHD. JORGE GEOVANNY RAURA RUIZ

ASESOR: PHD. JOSÉ ANTONIO QUIÑA MERA

Ibarra, febrero 2025

CERTIFICACION DIRECTOR DEL TRABAJO DE INTEGRACION CURRICULAR

Ibarra ,26 de febrero de 2025

Ing. Jorge Raura Ruiz, Phd.

DIRECTOR DEL TRABAJO DE INTEGRACION CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integraccion Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

.....

Ing, JORGE RAURA RUIZ. Phd

Cc; 0501773063

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	171150602-0		
APELLIDOS Y NOMBRES	MONTUFAR RIVERA MAURICIO FABIAN		
DIRECCIÓN	QUITO, URB CONDADO CALLE B Y G1		
EMAIL	mfmontufarr@utn.edu.ec		
TELÉFONO FIJO		**TELÉFONO MÓVIL:**	0995929865

DATOS DE LA OBRA	
TÍTULO:	PROTECCIÓN DE DATOS EN LA DIRECCION DE INFRACCIONES DE LA AGENCIA METROPOLITANA DE TRÁNSITO APLICANDO UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) CONSIDERANDO EL MARCO NORMATIVO VIGENTE Y CON UNA METODOLOGIA EGSI.
AUTOR (ES):	MONTUFAR RIVERA MAURICIO FABIAN
FECHA: DD/MM/AAAA	26-02-2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA DE POSGRADO	☐ PREGRADO [X] POSGRADO
TITULO POR EL QUE OPTA	Magister en computación con mención en Seguridad Informática
TUTOR	Phd. Jorge Geovanny Raura Ruiz

2. **CONSTANCIAS**

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 26 días del febrero de 2025

EL AUTOR:

Firmado electrónicamente por:
MAURICIO FABIAN
MONTUFAR RIVERA

Nombre: MONTUFAR RIVERA MAURICIO FABIAN

DEDICATORIA

Quiero dedicar esta tesis a mi esposa, mis hijas y mi madre, quienes han sido los pilares fundamentales que me han inspirado a buscar nuevos conocimientos para enfrentar con éxito los retos profesionales y educativos. Ellas son el motor que me impulsa a ser un baluarte en la vida.

También dedico este trabajo a mi hermana, cuyo valioso consejo siempre ha infundido en mí el sentido de responsabilidad y el compromiso con la superación personal. Y a mi padre, quien, desde el cielo, estoy seguro de que se siente orgulloso de cada objetivo alcanzado, siendo siempre un ejemplo de vida y perseverancia.

AGRADECIMIENTO

Agradezco a Dios por iluminar mi camino y guiarme siempre por el sendero del bien. Expreso mi gratitud a toda mi familia, cuyo apoyo incondicional ha sido fundamental para alcanzar mis objetivos, y a mis amigos, quienes han sido un pilar importante en este proceso.

También quiero agradecer a mis profesores de la UTN, especialmente a mi Director, por su orientación y dedicación, que han sido esenciales para la realización de esta tesis y mi crecimiento profesional.

ÍNDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE GRAFICOS

INDICE DE TABLAS

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

PROTECCIÓN DE DATOS EN LA DIRECCION DE INFRACCIONES DE LA AGENCIA METROPOLITANA DE TRÁNSITO APLICANDO UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) CONSIDERANDO EL MARCO NORMATIVO VIGENTE Y CON UNA METODOLOGIA EGSI.

Autor: Mauricio Fabián Montúfar Rivera
Tutor: PHD. GEOVANY RAURA RUIZ
Año: 2025

RESUMEN

La información es considerada como uno de los principales activos en el entorno de las organizaciones, por lo tanto, la protección y defensa de este activo intangible, constituye una tarea esencial para el cumplimiento de los objetivos del negocio. En la Agencia Metropolitana de Tránsito (AMT), perteneciente al Municipio del Distrito Metropolitano de Quito diversas aplicaciones y servicios presentan vulnerabilidades y brechas de seguridad que requieren atención.

Este trabajo propone la implementación de políticas de seguridad basadas en la metodología EGSI, enmarcadas dentro de un contexto normativo. Para ello, se utilizó una metodología Ad-hoc, fundamentada en un esquema gubernamental diseñado para su aplicación en instituciones públicas, y se validó la propuesta mediante el método Delphi.

Como resultado, el modelo de gestión de seguridad de la información fue implementado en la Dirección del Registro de Infracciones de la AMT, y contiene el diseño y definición de políticas específicas para fortalecer la seguridad de los sistemas de gestión de información.

Los procedimientos establecidos fueron evaluados por expertos, quienes otorgaron una calificación promedio de excelente en lo referente al cumplimiento de los estándares definidos en el modelo.

En base a estos resultados se puede prever que la gestión de la seguridad de la información (SGSI) basada en la metodología EGSI, permitirá a la Dirección del Registro de Infracciones, establecer mecanismos efectivos para la protección de datos considerando un marco normativo dictado por las entidades competentes. Esto permitirá proteger los activos y gestionar los riesgos de manera eficaz, abordando vulnerabilidades y estableciendo políticas de seguridad adaptadas a las necesidades identificadas.

Palabras clave: Política de seguridad de la información, activos de la información, vulnerabilidades, riesgo.

ABSTRACT

Information is considered one of the main assets within organizational environments; therefore, the protection and defense of this intangible asset constitutes an essential task for achieving business objectives. At the Metropolitan Transit Agency (AMT), part of the Municipality of the Metropolitan District of Quito, various applications and services present vulnerabilities and security gaps that require attention.

This work proposes the implementation of security policies based on the EGSI methodology, framed within a regulatory context. To achieve this, an ad-hoc methodology was used, grounded in a governmental framework designed for application in public institutions, and the proposal was validated using the Delphi method.

As a result, the information security management model was implemented in the Violations Registry Directorate of the AMT, including the design and definition of specific policies to strengthen the security of information management systems.

The established procedures were evaluated by experts, who gave an average rating of "excellent" regarding compliance with the standards defined in the model.

Based on these results, it can be foreseen that information security management (ISMS) based on the EGSI methodology will enable the Violations Registry Directorate to establish effective mechanisms for data protection, considering a regulatory framework dictated by competent authorities. This will allow for the protection of assets and effective risk management, addressing vulnerabilities and establishing security policies tailored to the identified needs.

Keywords: Information security policy, information assets, vulnerabilities, risk

CAPITULO I

1. EL PROBLEMA

1.1 PROBLEMA DE INVESTIGACIÓN

La información es considerada como uno de los principales activos en el entorno de las organizaciones, por lo tanto, la protección y defensa de este activo intangible, constituye una tarea esencial para el cumplimiento de los objetivos del negocio, siendo además una exigencia legal (protección de la propiedad intelectual, datos personales, y servicios para la sociedad de la información), que traslada confianza a los clientes y usuarios de la propia organización. Sin embargo, cuanto mayor es el valor de la información, mayor son los riesgos que se asocian a su deterioro, pérdida, manipulación indebida o malintencionada.

La seguridad de la información es fundamental para proteger los datos de una organización frente a amenazas y vulnerabilidades. La literatura identifica diversos problemas relacionados con la seguridad de la información, los cuales pueden clasificarse en tres categorías principales: hardware, software y personal. A continuación, se presentan algunos de los problemas más comunes en cada categoría, según (Admin, 2024)

PROBLEMAS DE SEGURIDAD A NIVEL DE HARDWARE

1. **Fallas Físicas**: Los dispositivos de almacenamiento y los servidores pueden fallar debido a defectos de fabricación, desgaste, sobrecalentamiento o daños físicos, lo que puede resultar en la pérdida de datos.
2. **Robo de Equipos**: El robo de dispositivos físicos como laptops, smartphones, y discos duros externos puede llevar a la pérdida de datos sensibles si no están adecuadamente protegidos.
3. **Interferencias Electromagnéticas**: Las interferencias o fluctuaciones eléctricas pueden dañar los componentes electrónicos, provocando fallos o pérdidas de información
4. **Acceso No Autorizado:** La falta de control físico adecuado puede permitir que personas no autorizadas accedan a equipos críticos, lo que puede resultar en manipulación o robo de información.

PROBLEMAS DE SEGURIDAD A NIVEL DE SOFTWARE

1. **Malware**: Virus, troyanos, ransomware, y spyware pueden comprometer la integridad y confidencialidad de los datos, además de interrumpir las operaciones normales.
2. **Vulnerabilidades y Exploits**: Fallos en el diseño o la implementación del software pueden ser explotados por atacantes para obtener acceso no autorizado o causar daños.
3. **Falta de Actualizaciones**: No mantener el software actualizado puede dejar sistemas vulnerables a ataques conocidos para los cuales ya existen parches.
4. **Configuraciones Inseguras**: La mala configuración del software (como bases de datos, servidores web, y aplicaciones) puede abrir puertas a ataques que de otro modo serían evitables.
5. **SQL Injection y XSS**: Vulnerabilidades en aplicaciones web que permiten a los atacantes ejecutar comandos arbitrarios o scripts en el contexto de un usuario.

PROBLEMAS DE SEGURIDAD RELACIONADOS CON EL PERSONAL

1. **Ingeniería Social**: Los atacantes pueden manipular a los empleados para obtener información sensible a través de técnicas como phishing, pretexting, o baiting.
2. **Insatisfacción o Mala Conducta del Personal**: Los empleados descontentos pueden actuar maliciosamente, ya sea borrando datos, robando información o introduciendo malware en los sistemas de la organización.
3. **Errores Humanos**: Errores como el envío de información sensible a destinatarios incorrectos, la configuración incorrecta de sistemas o el manejo inapropiado de datos pueden llevar a brechas de seguridad.
4. **Acceso Inapropiado**: Conceder acceso a datos o sistemas a empleados que no lo necesitan para su trabajo puede aumentar el riesgo de brechas de seguridad.

Los problemas de seguridad de la información descritos, afectan a personas y organizaciones, sean públicas o privadas, que enfrenta una serie de desafíos críticos, que pueden comprometer la confidencialidad, integridad y disponibilidad de datos sensibles. Aunque el factor humano sigue siendo el eslabón más débil en la cadena de seguridad. Errores como contraseñas débiles, phishing, ingeniería social y falta de concienciación son explotados por atacantes. Un estudio de Verizon Data Breach Investigations Report (2023) reveló que el 82% de las brechas de seguridad involucran un elemento humano. Por otro lado, el cumplimiento normativo y regulatorio, es crucial para las empresas e instituciones públicas, ya que su incumplimiento

puede resultar en sanciones económicas y daños a la reputación. Un estudio de IBM Cost of a Data Breach Report (2022) reveló que el costo promedio de una brecha de datos por incumplimiento normativo es de 4.35 millones de dólares.

En el ámbito público nacional, existen varias entidades como la Agencia Metropolitana de Tránsito del Ecuador, donde se presentan riesgos de seguridad de la información entre los cuales se puede mencionar afectaciones al sistema y a la base de datos, así como ataques cibernéticos y amenazas personales al equipo de servidores encargados del manejo de procesos críticos organizacionales (Gob.ec, 2024).

La Agencia Metropolitana de Tránsito está constituida por varias Coordinaciones y Direcciones, una de ellas es la Coordinación General de Fiscalización que es parte la Dirección de Registro de Infracciones. Esta Dirección controla distintos sistemas informáticos que permiten el control y manejo de las Infracciones que se sancionan a nivel del Distrito Metropolitano de Quito.

Para una mejor comprensión de la problemática existente en la organización tomada como caso de estudio, se ha identificado que la Dirección de Registro de Infracciones cuenta con los siguientes sistemas de información, considerados como críticos para el normal desarrollo de sus operaciones:

- **Sistema Axis Cloud**: Aplicativo que realiza el manejo de las infracciones, sentencias, impugnaciones, ingreso de citaciones y el control de recaudo de las mismas.
- **Sistema SOCRIT**: Sistema que maneja la captación, validación, sanción, notificación y subida a la ANT de las infracciones por medios tecnológicos.
- **Sistema Consulta CGM:** Sistema que se interrelaciona con webservice de ANT, Dinardap orientado a validar, verificar y completar la información al sistema SOCRIT.
- **Consulta Boletas:** Es el sistema que administra todas las boletas escaneadas tanto manuales, APP y tecnológicas.

También existen varios servidores de aplicaciones, gestores de base de datos y de almacenamiento, los mismos que no se encuentran integrados, afectando a la trazabilidad de la

información. Adicionalmente existe un único equipo donde se aloja la información de todos los medios de sanción del Distrito Metropolitano de Quito.

Además, como infraestructura adicional existen cámaras de foto multas y radares que interaccionan mediante enlaces dedicados al sistema SOCRIT para el ingreso de presuntas contravenciones.

La infraestructura disponible en la Dirección de Infracciones de la Agencia Metropolitana de Tránsito-AMT, es susceptible a delitos informáticos debido a que se encuentra instalada en puntos de control en las diferentes localidades de sanción, pudiendo ser vulnerados, hackeados o pinchados por personal ajeno a la institución. Por otra parte, desde estos puntos de control se puede acceder a toda la información que se dispone, como es las sanciones, captaciones o notificaciones.

De acuerdo a lo indicado por el Director de Infracciones de la AMT, se ha detectado diferentes incidentes de seguridad como la presencia de virus, intrusos que han ingresado a los servidores, vulneración de las seguridades de equipos tecnológicos, hackeo en accesos a páginas de consulta de infracciones, además de que ha existido fuga de información de contravenciones captadas y se han realizado registros injustificados de infracciones, dejando en evidencia las brechas de seguridad existentes, y las consecuentes pérdidas económicas que se han ocasionado.

Por otra parte, al haber información de las infracciones captadas por medios electrónicos, existe la posibilidad de chantajes, malas prácticas y fugas de la información; siendo posible que los funcionarios pueden archivar, discriminar o rechazar la información captada y no pueden realizarse las sanciones correspondientes según la normativa legal vigente.

En este sentido, existen denuncias sobre la fuga de la información referentes a infracciones de tránsito, como se puede verificar en diferentes medios de comunicación. Así, por ejemplo, en un artículo realizado por Pazán, se advierte: *"(...) La Empresa EMOV EP ya presentó una denuncia por el supuesto delito de difusión de información de circulación restringida el 28 de noviembre pasado(...)"*

Otro caso detectado por la empresa involucra a trabajadores que habrían borrado multas. *"Un funcionario con acceso a las claves del sistema de la empresa eliminaba multas inventándose providencias judiciales. Hacía cruce de información de procesos judiciales válidos para eliminar multas de otros ciudadanos. (...)" (Pazán, C. ,2023).*

Abordar estos problemas requiere un enfoque integral que combine tecnología, procesos y concienciación del personal. La inversión en ciberseguridad debe ser una prioridad para proteger los activos de información y garantizar la continuidad de las operaciones. En este contexto, la implementación de un Sistema de Gestión de Seguridad de la Información estandarizado, se vuelve crucial para la organización, para permitirle identificar y gestionar sus riesgos de seguridad de manera efectiva, considerando la confidencialidad, integridad y disponibilidad de los sistemas de información, y aplicando principalmente la mejora *continua (De Datos, P.,2019)*

1.2 Interrogantes de la investigación

De acuerdo al problema identificado en la sección anterior, se plantean las siguientes preguntas de investigación, mismas que guiarán el desarrollo del presente trabajo:

¿Cuáles son los activos de información que se encuentran en los sistemas de información de la Dirección de Infracciones de la Agencia Metropolitana de Tránsito?

¿Qué procedimientos y actividades son adecuados para la mitigación de riesgos de la Dirección de Infracciones de la Agencia Metropolitana de Tránsito?

¿Qué políticas de seguridad de la información se deben adoptar en la Dirección de Infracciones de la Agencia Metropolitana de Tránsito?

¿Cuál es el resultado preliminar de la aplicación de un SGSI contra las vulnerabilidades de la Dirección de Infracciones de la Agencia Metropolitana de Tránsito?

1.3 Objetivos de la investigación

1.3.1. Objetivo general

Implementar un sistema de gestión de seguridad de la Información (SGSI) basado en una metodología EGSI que permita a la Dirección de Infracciones de la Agencia Metropolitana de

Tránsito establecer mecanismos de protección de datos dentro de un marco normativo definido por los entes competentes.

1.3.2 Objetivos específicos

1. Identificar los activos de la información de la Dirección de Infracciones de la Agencia Metropolitana de Tránsito.

2. Brindar un conjunto de procedimientos para identificación de riesgo y definición de actividades de mitigación utilizando una metodología EGSI.

3. Definir políticas de Seguridad de la Información que deben llevarse a cabo en la Dirección de Infracciones de la Agencia Metropolitana de Tránsito.

4. Evaluar el sistema de gestión de seguridad de la información (SGSI) contra las vulnerabilidades detectadas.

1.4 Hipótesis de Trabajo.

El presente estudio será en esencia de tipo cualitativo, y no pretende demostrar una hipótesis utilizando técnicas de análisis cuantitativos, sin embargo, es pertinente formular una hipótesis de trabajo en función del objetivo general planteado. Esto es:

La gestión de seguridad de la Información (SGSI) con una metodología EGSI permitirá a la Dirección de Infracciones de la Agencia Metropolitana de Tránsito establecer mecanismos de protección de datos de forma efectiva dentro de un marco normativo definido por los entes competentes.

.

1.5 Hipótesis Alterativa

Para la hipótesis de trabajo antes definida, la hipótesis alternativa (llamada hipótesis nula en investigación cuantitativa) que se plantea es la siguiente:

Implementar un sistema de gestión de seguridad de la Información (SGSI) basado en una metodología EGSI permitirá a la Dirección de Infracciones de la Agencia Metropolitana de

Tránsito establecer mecanismos de protección de datos poco efectivos dentro de un marco normativo definido por los entes competentes.

1.6 Categorización de variables

Las variables que se derivan de la hipótesis planteada son:

Variable independiente: Sistema de gestión de seguridad de la Información (SGSI) basado en una metodología EGSI.
Variable dependiente: Mecanismos de protección de datos dentro de un marco normativo definido por los entes competentes.

1.7 Justificación

La seguridad de la información es una figura esencial de las tecnologías de la información de las instituciones de cualquier tipo o tamaño. Por lo tanto, se basa en un aspecto importante que guarda relación con la protección de datos contra ingresos no autorizados y para protegerlos de una eventual corrupción durante todo su ciclo de vida.

La Seguridad de información se constituye de varios conceptos tales como encriptación de datos, forence y prácticas de gestión optima de claves que de una u otra forma ayudan a la protección de datos en todas las plataformas y aplicaciones de una organización.

Actualmente, organizaciones en todo el mundo invierten fuertemente en la tecnología de información relacionada con la ciberdefensa con el fin de proteger sus activos críticos como son su marca, capital intelectual e información de sus clientes.

En todos los temas relacionados con la seguridad de la información resaltan elementos básicos que todas las organizaciones deben considerar en el momento de aplicar sus medidas: el talento humano, los procesos críticos y la tecnología que se va a aplicar

Las consecuencias de la no aplicación de seguridad de la información y los costos de huecos de seguridad son noticia de primera plana y abarcan todo, desde la pérdida de puestos de trabajo hasta la pérdida de ingresos e imagen institucional. Para lo cual se debe realizar modelos,

diseños y sistemas robustos que protejan el core del negocio y sus clientes, ya que es el activo fundamental de las Empresas. (Seguridad de Datos, s. f.)

El Gobierno Ecuatoriano mediante el Ministerio de Telecomunicaciones ha realizado el ACUERDO Nro. MINTEL-MINTEL-2024-0003 el cual implementará el Esquema Gubernamental de Seguridad de la Información EGSI en un plazo de doce (12) meses contados a partir de la publicación del Acuerdo Ministerial. En este sentido, este trabajo se enmarca en la necesidad que tienen diversas instituciones estatales, de implementar este esquema de seguridad de la información. (Gob.ec,2024)

Dentro de los aspectos relevantes de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) determinado en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, se pueden considerar los siguientes:

1. **Incremento en las Amenazas Cibernéticas:** La creciente sofisticación y frecuencia de ciberataques exige actualizar y fortalecer las medidas de seguridad.
2. **Protección de Datos:** Asegurar la integridad, confidencialidad y disponibilidad de la información gubernamental es crucial para mantener la confianza pública y proteger información sensible.
3. **Cumplimiento Normativo:** La implementación del EGSI asegura que las instituciones públicas cumplan con las normativas y estándares internacionales de seguridad de la información.
4. **Eficiencia Operativa:** Mejorar la seguridad de la información puede prevenir interrupciones en los servicios públicos, lo que contribuye a una administración más eficiente y confiable.
5. **Innovación y Modernización:** Actualizar el esquema de seguridad fomenta una cultura de mejora continua y adopción de nuevas tecnologías para una mejor gestión de la información.

La Dirección de Infracciones de la Agencia Metropolitana de Tránsito, busca reducir el número de incidentes dentro de la infraestructura que se maneja, previniendo y reaccionando de manera adecuada, optima y eficiente ante la presencia de amenazas. Es por ello que se pretende minimizar el impacto que puedan tener, considerando para ello los siguientes aspectos:

Política de seguridad de la información

Se establecerán políticas de seguridad de la información, para la Dirección de Registro de Infracciones de la AMT puesto que manejan sistemas fundamentales para el control del tránsito con medios tecnológicos.

Recursos necesarios

El talento humano dentro de la institución tiene un papel preponderante dentro de la alta gerencia de la institución, para lo cual se controlará las fugas de información y el personal será comprometido al 100% con procedimientos claros de actividades a realizarse.

Estructura organizacional

Se pretende que el manejo los sistemas informáticos se los realice de una manera estructurada, controlada y precautelando todos los activos de la información que tiene la Dirección de Registro de Infracciones de la AMT con roles y responsabilidades de la cadena de negocio.

Protección de datos a los activos.

A través de la ley de protección de datos vigente se busca un manejo adecuado de la información confidencial que indica la norma. Se definirán responsables del manejo de datos para cumplir la ley y en sí proteger los activos de la institución. La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en instituciones públicas es fundamental para proteger los activos de información críticos y garantizar la continuidad de los servicios esenciales. Como se puede advertir, un SGSI proporciona un marco estructurado para identificar, evaluar y mitigar los riesgos asociados a estos datos, reduciendo la probabilidad de filtraciones y accesos no autorizados. Además, permite identificar y corregir vulnerabilidades de manera proactiva, minimizando el impacto de posibles incidentes, lo cual fortalece la confianza en los servicios gubernamentales y promueve la transparencia, garantizando la continuidad de las operaciones críticas en caso de incidentes de seguridad, como ciberataques o desastres naturales [1].

---

[1] ISO/IEC 27001:2022: Estándar internacional para la gestión de la seguridad de la información. ISACA: Asociación de Auditoría y Control de Sistemas de Información. **OCDE:**

La presente propuesta de implementación del EGSI en la Dirección de Infracciones de la Agencia Metropolitana de Tránsito, fortalecerá la ciberseguridad gubernamental, adaptándose a los desafíos actuales y futuros en el ámbito digital mediante un proceso de mejora continua (Gob.ec,2024).

Organización para la Cooperación y el Desarrollo Económicos. **NIST**: Instituto Nacional de Estándares y Tecnología

CAPITULO II
2. MARCO REFERENCIAL.

2.1 Antecedentes

Para determinar los trabajos relacionados con la presente propuesta de investigación, se ha realizado una revisión de literatura preliminar, siguiendo un protocolo de búsqueda estandarizado para este tipo de estudios.

En primera instancia, se determinó una cadena de búsqueda que permita contestar a la siguiente interrogante de investigación: **¿Cómo se han implementado los sistemas de seguridad de la información basados en la norma ISO IEC 27001?,**

Para encontrar los artículos que respondan a esta interrogante, se definió la siguiente cadena de búsqueda: **("All Metadata":information security management system) AND ("All Metadata":ISO/IEC 27001)**

La cadena de búsqueda fue corrida en la base de datos de IEEE Xplore (IEEEX), misma que mostró un total de 48 publicaciones entre (conferencias, libros y revistas). Se utilizó como criterio de inclusión los trabajos relacionados con el manejo de sistemas de seguridad de la información publicados durante los últimos 5 años, que estén en idioma inglés y que hagan referencia al estándar ISO/IEC 27001, como se muestra en la siguiente gráfica:

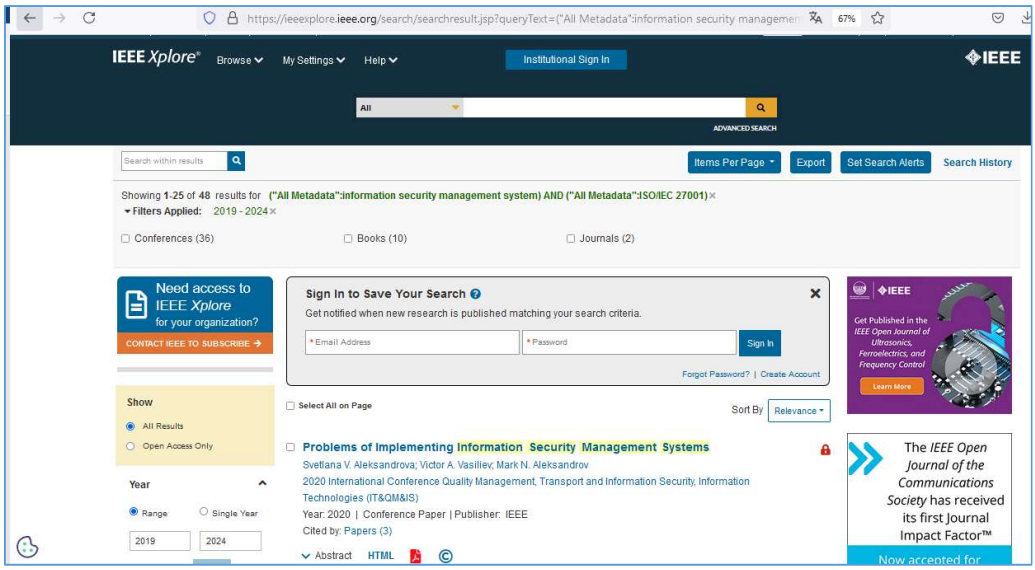


Tabla 1 Verificación IEEE Explore (Autoría Propia)

Posteriormente se analizó el resumen de los 48 artículos, para determinar aquellos que relevantes para el estudio. Se seleccionaron diez artículos, cuyo análisis se detalla a continuación:

Para mejorar la seguridad de información según (Svetlana V. Aleksandrova; Victor A. Vasiliev; Mark N. Aleksandrov,2020) a nivel de Rusia y de manera general en el mundo urge tomar decisiones a las amenazas que se están dando, por lo cual se tiene requisitos más estrictos para las empresas que almacenan y procesan datos personales. Se puntualiza que se tiene una atención prioritaria a la seguridad de la información que se debe gestionar con éxito para las empresas y permitirán minimizar los riesgos asociados con la seguridad de la información y es una ventaja competitiva en el mercado global.

En el estudio de (Masike Malatji,2023) se compara y se contrasta la ISO/IEC 27001:2022 and ISO/IEC 27001:2013 debido a los controles de seguridad implementados. Se concluyó que ISO/IEC 27001:2022 es una ligera mejora con respecto a ISO/IEC 27001:2013, abordando la protección de los servicios de computación en la nube, que han sido adoptados cada vez más por muchas empresas.

Según (Dea Saka Kurnia Putra; Saffana Tistiyani; Septia Ulfa Sunaringtyas,2021) la aplicación de la norma ISO/IEC 27001 puede ayudar a un país u organización a construir y mantener un sistema de gestión de seguridad de la información (SGSI). El objetivo principal de este estudio es proporcionar información al gobierno, expertos en seguridad de la información y académicos, sobre qué países están implementando la familia ISO/IEC 27001 en la implementación de sus requisitos de política de seguridad de la información también en comparación con el rango GCI.

De acuerdo a (Narong Chaiwut; Worasak Rueangsirarak,2022) realiza un análisis de brechas ISO/IEC 27001:2013 en línea para proporcionar una guía preliminar para que las organizaciones esbocen su política de seguridad cibernética. El resultado revela que los sectores industriales obtuvieron puntuaciones más altas que los sectores gubernamentales en el nivel de seguridad general. Además, los autores indican que es práctico implementar el sistema propuesto como parte del Sistema de Gestión de Seguridad de la Información (SGSI).

En el estudio de (Mark N. Aleksandrov; Victor A. Vasiliev; Svetlana V. Aleksandrova ,2021) se menciona el problema de mantener la confidencialidad, integridad y disponibilidad de la información, las empresas utilizan cada vez más la metodología establecida en base a la norma internacional ISO / IEC 27001. El artículo considera los problemas y enfoques para el desarrollo, la implementación práctica y la metodología de la gestión de riesgos basada en la norma internacional ISO 31000 en el sistema de gestión de seguridad de la información.

En el trabajo de investigación de (Ilya I. Livshitz; Pawel A. Lontsikh; Elena Y. Golovina; Egor P. Kunakov; Valentina V. Kozhukhova,2020) se analiza las opiniones de expertos rusos y extranjeros sobre una amplia gama de cuestiones relacionadas con la seguridad de TI como componentes de TI independientes y servicios integrales en la nube. El método propuesto permite obtener los resultados de trazabilidad de la evaluación de riesgos de seguridad de TI y de los componentes de TI de la nube en las restricciones dadas. Los autores mencionan que los resultados se pueden aplicar a los procesos de una evaluación independiente, incluida la infraestructura crítica.

De acuerdo a (Carla Carvalho; Eduardo Marques,2019) se indica que la metodología adoptada se basó en la gestión de riesgos y tuvo como objetivo el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información de acuerdo con los requisitos de la norma NP ISO/IEC 27001:2013. Los resultados preliminares mostraron avances relevantes. Se identificaron las áreas más urgentes y qué controles de seguridad necesitaban mejorar. El estudio propició un cambio de postura de la organización, que pasó de tener meras percepciones sobre sus niveles de seguridad de la información a tener un conocimiento objetivo de sus necesidades.

De acuerdo con (Jason Edwards; Griffin Weaver,2024) indica ISO/IEC 27001 sienta las bases para un sistema de gestión de seguridad de la información, lo que requiere que la organización diseñe e implemente un conjunto coherente e integral de controles de seguridad de la información, y se analiza la implementación de ISO/IEC 27001. Además, se controla una serie de acciones metódicamente priorizadas que, cuando se combinan, forman un sólido conjunto de mejores prácticas de defensa en profundidad para la ciberseguridad.

En el estudio de (Fatiha Djebbar,2023) se propone como objetivo ayudar a las organizaciones a seleccionar los controles de seguridad más adecuados para sus necesidades específicas y simplificar y aclarar el proceso de cumplimiento. Los hallazgos muestran una

superposición significativa entre los tres estándares seleccionados. Esta información puede ayudar a las organizaciones a obtener una comprensión integral de los requisitos y controles de seguridad comunes, lo que les permitirá optimizar sus esfuerzos de cumplimiento al eliminar el trabajo duplicado, especialmente cuando se cumplen los requisitos de múltiples estándares.

En el artículo de (Huaqun Guo; Meng Wei; Ping Huang; Eyasu Getahun Chekole,2021) se menciona la importancia de la adopción de la norma ISO/IEC 27001 por organizaciones y empresas de todo el mundo. Se aborda sistemáticamente los 21 requisitos compuestos por 7 obligatorios y 14 categorías en la norma ISO/IEC 27001 al diseñar y desarrollar políticas de sistemas de gestión de seguridad de la información (SGSI). Las 3 políticas de SGSI están diseñadas para abordar los requisitos individuales de la norma ISO/IEC 27001 de manera efectiva.

Conclusión de la revisión de literatura:

En base al análisis de los estudios citados, se determina que existen diversas implementaciones y análisis de la norma ISO/IEC 27001 y su aplicación para sistemas de gestión de seguridad de la información (SGSI). Esto se puede resumir en la siguiente tabla:

ARTICULO NO.	AUTOR	AÑO DE PUBLICACIÓN	TIPO DE ORGANIZACIÓN ESTUDIADA (GUBERNAMENTAL, EMPRESARIAL, SERVICIOS, ETC)	FACTORES DE ÉXITO	FACTORES DE ÉXITO
1	Svetlana V. Aleksandrova; Victor A. Vasiliev; Mark N. Aleksandrov	2020	Servicios	Se recomiendan requisitos más estrictos para las empresas que almacenan y procesan datos personales Atención prioritaria a la seguridad de la información	Amenazas que sufren Rusia y todo el mundo a nivel de seguridad de los recursos de Sistemas de Información
	Masike Malatji	2023	Normativa Internacional	Se utilizaron estadísticas descriptivas para determinar la distribución de frecuencia de cada control de seguridad	La comparación y contrastar ISO/IEC 27001:2022 e ISO/IEC 27001:2013

2				Se descubrió que la función de protección del NIST CF La ISO/IEC 27001:2022 introdujo once nuevos controles de seguridad	
3	Dea Saka Kurnia Putra; Saffana Tistiyani; Septia Ulfa Sunaringtyas	2021	Gubernamental /Empresarial	La aplicación de la norma ISO/IEC 27001 puede ayudar a un país u organización a construir y mantener un sistema de gestión de seguridad de la información (SGSI) Este estudio tiene como objetivo proporcionar información al gobierno, expertos en seguridad de la información, académicos e implementadores sobre qué países están implementando la familia ISO/IEC 27001	La familia de normas ISO/IEC 27001 está afectando el rango GCI que se encuentra en las medidas legales
4	Narong Chaiwut; Worasak Rueangsirarak	2022	Gubernamental	Proporciona una guía preliminar para que las organizaciones esbocen su política de seguridad cibernética. El resultado revela que los sectores industriales obtuvieron puntuaciones más altas que los sectores gubernamentales en el nivel de seguridad general	La norma ISO/IEC 27001:2013 requiere de un alto presupuesto para analizarla y adaptarla a la organización. No existe ningún estándar de seguridad que dependa de Ley de Protección de Datos Personales
5	Mark N. Aleksandrov; Victor A. Vasiliev; Svetlana V. Aleksandrova	2021	Empresarial	Para resolver el problema de mantener la confidencialidad, integridad y disponibilidad de la información, las empresas utilizan cada vez más la metodología establecida en base a la norma internacional ISO / IEC 27001	El artículo considera los problemas y enfoques para el desarrollo, la implementación práctica y la metodología de la gestión de riesgos basada en la norma internacional ISO 31000 en el moderno sistema de gestión de seguridad de la información.

				La gestión de riesgos de seguridad de la información es un proceso de monitoreo continuo y análisis sistemático de la entorno interno y externo del entorno de TI	
6	Ilya I. Livshitz; Pawel A. Lontsikh; Elena Y. Golovina; Egor P. Kunakov; Valentina V. Kozhukhova	2020	Empresarial	El artículo propone un enfoque práctico basado en la metodología "Híbrida" utilizando procedimientos formales de evaluación basados en dos criterios: la evaluación del grado de cumplimiento de los sistemas de gestión (basado en la serie ISO/IEC 27001) y la evaluación de los requisitos de seguridad funcional (basados en Serie IEC 61508 y serie ISO/IEC 15408) Minimizan el riesgo (riesgo residual) de activos importantes	Solo se pueden aplicar a los procesos de una evaluación independiente, incluida la infraestructura crítica, con la precisión de cálculo requerida
7	Carla Carvalho; Eduardo Marques	2019	Gubernamental	La metodología adoptada se basó en la gestión de riesgos y tuvo como objetivo el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información de acuerdo con los requisitos de la norma NP ISO/IEC 27001:2013 Esta metodología propició un cambio de postura de la organización, que pasó de tener meras percepciones sobre sus niveles de seguridad de la información a tener un conocimiento	Solo se realizaron una iteración para revisar las cuatro secciones del ciclo continuo PDCA

				objetivo de sus necesidades	
8	Jason Edwards; Griffin Weaver	2024	Empresarial	Analiza la implementación de ISO/IEC 27001 La Certificación del Modelo de Madurez de Ciberseguridad es un estándar integral y unificado diseñado meticulosamente para implementar la ciberseguridad en toda la base industrial de defensa en los Estados Unidos	ISO 27701 proporciona un marco integral para que las organizaciones gestionen y protejan eficazmente la información personal
9	Fatiha Djebbar; Kim Nordström	2023	Empresarial	En este trabajo, realizan un estudio comparativo para identificar posibles superposiciones y discrepancias entre tres estándares de seguridad: ETSI EN 303 645 v2.1.1 para dispositivos de consumo conectados a Internet, ISA/IEC 62443-3-3:2019 para automatización y control industrial. sistemas, e ISO/IEC 27001:2022 para sistemas de gestión de seguridad de la información Esta estudio puede ayudar a las organizaciones a obtener una comprensión integral de los requisitos y controles de seguridad comunes, lo que les permitirá optimizar sus esfuerzos de cumplimiento al eliminar el trabajo duplicado, especialmente cuando se cumplen los requisitos de múltiples estándares.	Existe el riesgo de duplicar los requisitos y controles de seguridad existentes entre los estándares, lo que genera costos y cargas de trabajo adicionales innecesarios
	Huaqun Guo; Meng Wei; Ping Huang; Eyasu	2021	Servicios	Abordar sistemáticamente los 21 requisitos compuestos por 7	No se encuentra dificultad en la aplicación de ISO/IEC 27001

10	Getahun Chekole			obligatorios y 14 categorías en la norma ISO/IEC 27001 al diseñar y desarrollar políticas de sistemas de gestión de seguridad de la información (SGSI) Se adopta el modelo PDCA y se evalúa la declaración de aplicabilidad.	

Tabla 2 Sistemas SGSI (Autoría Propia)

Se advierte que muchas organizaciones han adoptado modelos ya establecidos para la implementación del estándar ISO/IEC 27001. La aplicación varía desde pequeñas, medianas y grandes empresas, así como para organismos gubernamentales y de servicios.

Se han identificado que los principales beneficios en la aplicación del estándar ISO/IEC 27001 es la seguridad de la información que se da en todos los procesos sustanciales de las empresas, minimizando las vulnerabilidades que se pueden dar y proponiendo planes de mitigación que pueden ser aplicados para entrar en crisis. Las principales desventajas que se puede resaltar es el aspecto económico ya que los profesionales deben estar bien capacitados y conocer en qué áreas estratégicas de las empresas deben aplicarse políticas de seguridad para su implementación, lo cual supone gastos que muchas veces las organizaciones no contemplan en sus presupuestos. Hay que considerar que, en algunos resultados de la aplicación del estándar, reportados en la literatura, deben tomarse con cautela debido a aspectos metodológicos. Por ejemplo, (Carvalho, 2019) advierte que únicamente se realizó una iteración para revisar las cuatro secciones del ciclo continuo PDCA.

De acuerdo al análisis de la literatura realizado, la presente propuesta podría contribuir en el campo de conocimiento de la mejora de la seguridad de la información en general y de manera particular en los procesos de gestión de infracciones de tránsito a nivel de la AMT de la Dirección De Infracciones De La Agencia Metropolitana De Tránsito, aplicando un (SGSI) y considerando el marco normativo vigente. La implementación de este modelo también puede servir como guía a otros GAD que realicen actividades de control de tránsito. Por otra parte, se prevé que los resultados de este estudio, permitan complementar trabajos anteriormente realizados, específicamente en lo que respecta al cumplimiento del Esquema Gubernamental

de Seguridad de la Información EGSI, propuesto para instituciones ecuatorianas como se establece en el ACUERDO Nro. MINTEL-MINTEL-2024-0003.

2.2 Marco Teórico.

2.2.1. Introducción al Sistema de Gestión de la Seguridad de la Información - SGSI

La historia del SGSI se remonta a las primeras preocupaciones sobre la seguridad de la información en las organizaciones. Con el crecimiento de la dependencia de las empresas en la tecnología de la información y la comunicación, surgió la necesidad de gestionar y proteger la información de manera más efectiva. A medida que aumentaban las amenazas cibernéticas y la regulación relacionada con la privacidad y la seguridad de los datos, la importancia del SGSI se volvió aún más evidente.

El SGSI es una historia de adaptación y evolución continua en respuesta a las cambiantes amenazas y desafíos en el ámbito de la seguridad de la información. Su importancia seguirá creciendo a medida que la digitalización continúe transformando la forma en que trabajamos, nos comunicamos y almacenamos información en el mundo moderno (de La Información,2020)

El SGSI se implementó ante la necesidad creciente de protección de la información. A lo largo del tiempo, se han establecido estándares y marcos de referencia reconocidos internacionalmente para guiar la implementación y el mantenimiento de un SGSI efectivo. Uno de los más conocidos corresponde a la norma ISO/IEC 27001, que determina los requisitos para implementar, mantener, establecer y mejorar un SGSI dentro de una organización.

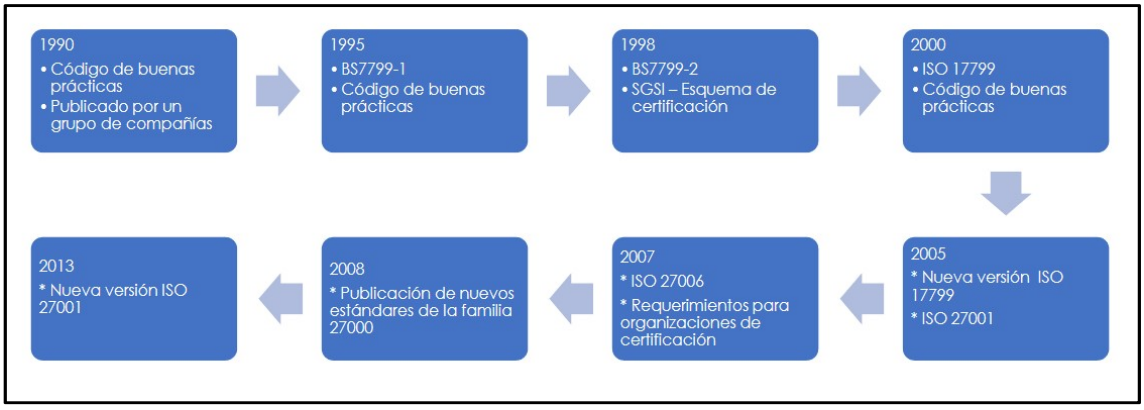


Figura 1 Historia del SGSI (Gobierno Electrónico de Ecuador,2020)

A continuación, determinaremos varios aspectos claves de un SGSI de acuerdo a (Disponibilidad – Seguridad informática,2020)

Políticas y procedimientos: Un SGSI establece políticas y procedimientos claros para proteger la información sensible. Esto incluye políticas de acceso, clasificación de la información, gestión de contraseñas, respaldo de datos, etc.

Identificación de activos de información: Un SGSI identifica y clasifica los activos de información críticos para la organización, como datos del cliente, propiedad intelectual, registros financieros, etc.

Evaluación de riesgos: Un SGSI realiza evaluaciones periódicas de riesgos para analizar e identificar algunos tipos de vulnerabilidades y amenazas que afectarían la seguridad de la información. Esto ayuda a priorizar las acciones y recursos de mitigación.

Controles de seguridad: Un SGSI implementa controles de seguridad adecuados para proteger los activos de información contra amenazas identificadas. Esto puede incluir controles técnicos, como firewalls y sistemas de detección de intrusiones, así como controles administrativos, como políticas y procedimientos.

Concienciación y formación: Un SGSI incluye programas de concienciación y formación para educar a los empleados sobre prácticas seguras de manejo de la información y concienciarlos sobre las amenazas cibernéticas.

Gestión de incidentes: Un SGSI establece procesos para detectar, responder y gestionar incidentes de seguridad de la información de manera efectiva y oportuna.

Revisión y mejora continua: Un SGSI se somete a revisiones periódicas para garantizar su eficacia y se mejora continuamente en función de las lecciones aprendidas y diversos cambios en el medio de la seguridad de la información.

El estándar internacional ISO/IEC 27001 proporciona un marco reconocido internacionalmente para establecer, implementar, mantener y mejorar un SGSI dentro de una organización. Muchas organizaciones utilizan este estándar como base para desarrollar su SGSI y obtener certificaciones de conformidad con la norma.

El Sistema de Gestión de Seguridad de la Información tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información (Disponibilidad – Seguridad informática,2020).

Figura 2 Pirámide del SGSI (Disponibilidad – Seguridad informática,2020).

- Confidencialidad: Todo tipo de información únicamente debe ser divulgada y debe ser accesible por aquellos que este netamente autorizados.
- Integridad: La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.

Disponibilidad: La información debe estar siempre accesible para aquellos que estén autorizados (Disponibilidad – Seguridad informática,2020)

A continuación, se presenta un análisis de sistemas de gestión de seguridad de la información de acuerdo a diferentes marcos metodológicos.

Tabla 3 Metodologías SGSI Autoría Propia

Metodología	**Entes de Aplicación**	**Objetivos Seguridad**	**Ventajas**	**Desventajas**

MAGERIT	Empresas Privadas y Públicas son utilizadas	Cumple con Objetivos de seguridad.	Es público su metodología y puede ser utilizado por cualquier ente. Dispone de tres libros para su aplicación Dispone de herramientas para gestionar los riesgos	En su implementación es costosa porque se debe traducir todas sus valoraciones No posee inventario completo de controles.
NIST SP 800:30	Utilización en empresa gubernamentales en EEUU.	No Cumple con Objetivos de trazabilidad y autenticidad	Tiene un enfoque técnico y Práctico. Uso de métricas cualitativas Tiene el manejo del ámbito de la seguridad de la información Implementación es de costo bajo.	En la implantación no se contempla los procesos los activos ni las dependencias.
OCTAVE	Empresas Privadas y Públicas son utilizadas	No Cumple con Objetivos de trazabilidad y autenticidad	Se desarrolla con personas de la institución con un equipo multidisciplinario. Involucra procesos, activos, amenazas, riesgos y vulnerabilidades Es gratuito	Es dificultoso su entendimiento por la complejidad de su documentación. Se debe tener conocimientos avanzados técnicos para su utilización. Se requiere conocimientos claros y avanzados de gestión de riesgos.
MEHARI	Empresas Privadas y Públicas son utilizadas	No cumple controles de seguridad.	Maneja información cualitativa y cuantitativa para gestión de riesgos Se adapta a la ISO 27001/002/005 Detecta vulnerabilidades para disminución de riesgos.	No se incluyen controles de seguridad en la gestión de riesgos. Proceso de manejo de riesgos es complejo en su implementación
CRAMM	Empresas Privadas y Públicas son utilizadas	No Cumple con Objetivos de trazabilidad y autenticidad	Realiza el estudio de riesgos cualitativos y cuantitativos. Categoriza los activos de TI	No maneja procesos y recursos en su análisis de riesgos.

			Identifica amenazas y vulnerabilidades y ejecuta los controles que se necesita	
CORAS	Se utiliza en cualquier empresa pública o privada	No Cumple con Objetivos de trazabilidad y autenticidad	Maneja varias herramientas para gestión de riesgos. Maneja modelos gráficos en UML Maneja sistemas de TI Críticos.	No hace análisis de riesgos cualitativos. No utiliza procesos y dependencias.
EBIOS	Se utiliza en cualquier empresa pública o privada	No Cumple con Objetivos de trazabilidad y autenticidad	Ayuda a empresas a tener mayor reconocimiento en niveles de seguridad Se adapta a la ISO 27001/002 y 31000 Herramientas de código libre y reutilizable	Es utilizado como herramientas de soporte
ISO/IEC 27005	Se aplica en cualquier tipo de empresa privada o gubernamental	No Cumple con Objetivos de trazabilidad y autenticidad	Ayuda a creas SGSI más eficaz Aborda los riesgos de maneja eficaz y oportuna.	No recomienda una metodología concreta
ISO/IEC 27001	Se aplica en cualquier tipo de empresa privada o gubernamental	Cumple con los controles de seguridad	Integra con sistemas de gestión de seguridad de la información. Los documentos necesarios se determinan en base al tamaño y la complejidad.	Es abstracto y de alto nivel. Cambiar los conceptos, debido a los requisitos que son difíciles de interpretar. No existe descripción detallada en identificar los riesgos
ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION (EGSI)	Se aplica en empresas gubernamentales	Cumple con los controles de seguridad	Se basa en la ISO 27005 Maneja formatos de activos, amenazas, vulnerabilidades controles existentes y análisis de riesgos Tratamiento de riesgos de seguridad de la información	No se ha identificado desventajas

De acuerdo al análisis presentado en la tabla anterior, se han identificado diez metodologías para aplicación de los sistemas de gestión de seguridad de la información, aplicados en empresas tanto públicas como privadas. Como se observa, existen ventajas y desventajas de acuerdo a los objetivos de seguridad establecidos.

En este estudio, se considera el Esquema Gubernamental de Seguridad de la Información, en razón de que se adapta a los objetivos institucionales y principalmente porque es un modelo que debe aplicarse de forma obligatoria en las empresas públicas del país.

2.2.2. Identificación De Activos.

De acuerdo al estándar, ISO 27001 y la Gestión de Activos, la norma establece que las organizaciones deben identificar y clasificar sus activos en función de su importancia, sensibilidad de la información que contienen e impacto potencial de una violación o pérdida de seguridad, (Toro R, 2015).

Por otra parte, Según COBIT 5, la identificación de activos es un proceso crítico dentro de la gestión de activos de TI (BAI09) que consiste en reconocer y documentar todos los componentes de TI que tienen valor para la organización. Esto incluye tanto activos físicos (hardware, redes, etc.) como lógicos (software, datos, servicios). (Fernandes V,2022)

De acuerdo con NIST SP 800-53, la identificación de activos es un proceso fundamental que consiste en descubrir, documentar y comprender todos los componentes de un sistema de información que tienen valor para una organización. Estos activos pueden abarcar desde hardware y software hasta datos personales. (Tecnetone, n.d.)

La guía de gestión de riesgos dada por el Mintel, establece que todo aquello que tiene valor dentro de una organización es considerado como un activo, en ese sentido se requiere de protección. Es así que, para identificar los activos, es recomendable que todos los sistemas de información contengan muchos más elementos que los más conocidos como son el software y hardware. (Gobierno Electrónico de Ecuador,2020)

Como se puede notar, tanto el estándar ISO 27001, Cobit 5, Nist SP 800 53, y el marco regulatorio del MINTEL, establecen como parte fundamental dentro de un SGSI la identificación de activos. En todos los casos se reconoce la importancia de documentar y

reconocer o descubrir todos los componentes de un sistema de información que requieren protección en la organización.

2.2.3. Identificación de Amenazas

Según la norma ISO 27001 indica que las amenazas con eventos que en algún momento pueden comprometer la seguridad de la información y su protección a los sistemas que son aplicados (Toro R, 2015)

La identificación de amenazas según la guía de gestión de riesgos dada por el Mintel, establece potenciales amenazas que causan daños a ciertos activos tales como procesos, información y sistemas. Varias de estas amenazas afectan ciertamente a más de un activo. En tales casos, pueden causar diferentes impactos dependiendo de los activos que se vean afectados (Gobierno Electrónico de Ecuador,2020)

Además, de acuerdo a COBIT 5 se busca satisfacer las necesidades institucionales y con la identificación de los mismos se realizan la minimización de los riesgos que se necesitan atacar a los riesgos. (Fernandes V,2022)

De acuerdo con NIST SP 800-53, la identificación de amenazas es un proceso fundamental que consiste en controles de seguridad ya que abordan una amplia gama de amenazas cibernéticas, para lo cual se aplican controles para eliminar el riesgo de seguridad (Tecnetone, n.d.)

Como se puede verificar, tanto el estándar ISO 27001, Cobit 5, Nist SP 800 53, y el marco regulatorio del MINTEL, establecen como parte fundamental dentro de un SGSI la identificación de amenazas, que en primer lugar se deben identificar y luego se debe contrarrestar para eliminar los riesgos que se pueden encontrar minimizando las amenazas de los sistemas informáticos.

2.2.4. Identificación de Vulnerabilidades

Según la norma ISO 27001 indica que las vulnerabilidades es la potencial posibilidad de que se materialice una amenaza sobre algún activo de la información con eventos que en algún

momento pueden comprometer la seguridad de la información y la protección a los sistemas que son aplicados (Toro R, 2015).

La identificación de vulnerabilidades según la guía de gestión de riesgos dada por el Mintel, establece que la presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios. Conviene anotar que un control implementado de manera incorrecta o que funciona mal, o un control que se utiliza de modo incorrecto podrían constituir una vulnerabilidad (Gobierno Electrónico de Ecuador,2020)

Además, de acuerdo a COBIT 5(BAI02, BAI03), la identificación de vulnerabilidades en dicha metodología evalúa los recursos actuales y análisis de riesgo que pueden atraer todos los activos que van a ser gestionados (Fernandes V,2022)

De acuerdo con NIST SP 800-53, la identificación de vulnerabilidades es un proceso fundamental en la implementación de esta norma siguiendo los requisitos, lo que aumentará la confianza de los clientes y socios comerciales (Tecnetone, n.d.).

Como se puede notar, tanto el estándar ISO 27001, Cobit 5, Nist SP 800 53, y el marco regulatorio del MINTEL, establecen como fundamental dentro de un SGSI la identificación de vulnerabilidades para aplicar controles y que, a su vez, las amenazas no puedan comprometer la implementación de la seguridad de la información y se puedan aplicar para gestionar un SGSI.

2.2.5. Evaluación del riesgo

Según la norma ISO 27001 indica que las evaluaciones de riesgo dentro de los sistemas de información se pueden identificar de forma rápida y sencilla. Además, la ISO-27001 presta solución a todas estas cuestiones que se plantean a la hora de implementar un Sistema de Gestión de Seguridad de la Información en una empresa. Toda protección es importante, por mínima que sea, ya que el mínimo descontrol puede ocasionar una pérdida de los datos. (Toro R, 2015)

La identificación de evaluación de riesgos, según la guía de gestión de riesgos dada por el Mintel, consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto, además del proceso de comparación del riesgo estimado contra un criterio de riesgo calculado dado para determinar la importancia del mismo. El grado del riesgo es expresado numéricamente basado en las medidas del valor de los activos de información, el impacto de la amenaza y el alcance de la vulnerabilidad (Gobierno Electrónico de Ecuador,2020)

También, de acuerdo a COBIT 5(BAI06), la evaluación de riesgos identifica los procesos de impacto, la verificación optimizada de los cambios aplicados para la gestión de los riesgos y mitigan los riesgos encontrados (Fernandes V,2022)

De acuerdo con NIST SP 800-53, las organizaciones pueden evitar problemas costosos y potencialmente grabes en el futuro, mitigando los riesgos de manera efectiva, lo que además permite aumentar la confianza de los clientes (Tecnetone, n.d.)

Como se puede notar, tanto el estándar ISO 27001, Cobit 5, Nist SP 800 53, y el marco regulatorio del MINTEL, establecen dentro de un SGSI la evaluación de riesgos como evaluaciones periódicas y con algoritmos matemáticos o fórmulas que evalúa los riesgos y el impacto que van a tener para que no haya pérdida de datos.

2.2.6. Políticas de seguridad informática.

Según la norma ISO 27001, menciona que las políticas de seguridad informática recogen las directrices que deben seguir la seguridad de la información de acuerdo con las necesidades de la organización y la legislación vigente, dichas políticas indicarán los límites de la gestión de riesgos (Toro R, 2015)

Por otra parte, las políticas de seguridad informática según la guía de gestión de riesgos dada por el Mintel, son un conjunto de reglas, directrices y procedimientos establecidos por una organización para proteger la información y los sistemas de tecnología de la información, contra amenazas y riesgos de seguridad. Estas políticas definen las medidas de seguridad digital que se deben implementar, los roles y responsabilidades de los usuarios, los procedimientos para la gestión de incidentes y la respuesta a eventos de amenaza contra la seguridad y son

esenciales para promover una cultura de seguridad organizacional y establecer un marco de trabajo que garantice la confiabilidad, integridad y disponibilidad de la información. Además, ayudan a cumplir con los requisitos legales y normativas relacionadas con la seguridad de la información, siendo importante que las políticas de seguridad informática sean comunicadas claramente a todos los colaboradores y que se establezcan mecanismos para hacer cumplir y monitorear el acatamiento de estas (DocuSign, C, 2023)

También, de acuerdo a COBIT 5(BAI11) las políticas de seguridad informática están basadas en una revisión del proyecto para disminución de riesgos y costos, además mejora la comunicación con el cliente final para asegurar la calidad del proyecto (Fernandes V,2022)

De acuerdo con NIST SP 800-53, identifica las políticas de seguridad que se pueden adaptar a las necesidades específicas de una organización. Esto indica que las empresas e instituciones pueden personalizar sus análisis de seguridad sin perder la efectividad y que se puedan gestionar políticas ajustables a sus necesidades. (Tecnetone, n.d.)

Como se puede notar, tanto en el estándar ISO 27001, Cobit 5, Nist SP 800 53, y el marco regulatorio del MINTEL, las políticas de seguridad informáticas establecen un marco normativo para su implementación, disminución de riesgos y pérdida de información. Además, son aplicados a los activos de las instituciones.

2.2.7. EGSI

El Esquema Gubernamental de Seguridad de la Información – EGSI, creada con acuerdo Nro. MINTEL-MINTEL-2024-0003 de 08 de febrero de 2024 y publicado en del tercer Suplemento Nº 509 - Registro Oficial del 1 de marzo de 2024, busca preservar la, integridad, confidencialidad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados

El EGSI, es un documento que se presenta anexo al Acuerdo Ministerial, como un mecanismo para implementar el Sistema De Gestión De Seguridad De La Información en el Sector Público (Gobierno Electrónico de Ecuador,2020).

2.2.8. Mejora Continua

La mejora continua implica realizar una revisión general de lo que se ha implementado en las instituciones, es decir: revisión de la política de seguridad, verificación de su efectividad, cumplimiento de los objetivos de seguridad, cambios en el contexto organizacional, resultado de las evaluaciones, no conformidades, acciones correctivas, entre otros.

La mejora continua en el Esquema Gubernamental de Seguridad de la Información (EGSI) es un proceso esencial para garantizar que los datos y la información estén protegidos de manera efectiva, para lo cual es recomendable observar entre otras las siguientes consideraciones:

- Compromiso de la máxima autoridad con la mejora continua.
- Políticas y procedimientos actualizados.
- Formación y concienciación a los funcionarios de la institución.
- Monitorización y detección de amenazas.
- Proceso sólido de gestión de incidentes.
- Auditorías internas y externas.

La mejora continua en el EGSI es un proceso cíclico y constante. A medida que evolucionan las amenazas, los riesgos cambian en la institución, por lo cual es fundamental adaptarse y mejorar constantemente para proteger los activos de información de manera efectiva.

Por otra parte, de acuerdo a la Ley Orgánica de protección de datos personales, notificada en el Registro Oficial Suplemento 459 de 26 mayo de 2021, se busca garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre la publicación de información y datos, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela (ley orgánica de protección de datos personales. gob.ec,2021).

2.3. Marco Legal.

La aplicación del ESGI en las instituciones del estado ecuatoriano, está regulado por diferentes marcos jurídicos. Dentro de esta normativa, la Constitución de la Republica en su Artículo 226, establece que:" Las *instituciones del Estado, sus organismos, dependencias, las*

servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución".

Por otra parte, la implementación del ESGI se realizará en la Dirección de Registro de Infracciones de la Agencia Metropolitana de Tránsito, adscrita del Municipio del Distrito Metropolitano de Quito. En este contexto, la RESOLUCIÓN No. AMT-DG-002-2022, 13 de enero de 2022, expide las atribuciones y competencias delegadas a las dependencias que conforman la agencia metropolitana de control del transporte terrestre, tránsito y seguridad vial. (Gob.ec,2024)

De acuerdo a la Resolución del MINTEL, No. MINTEL-2024-0003 de 08 de febrero de 2024 en su Artículo 2 establece: "El EGSI es de implementación obligatoria en las entidades, organismos e instituciones del sector público, de conformidad con lo establecido en el artículo 225 de la Constitución de la República del Ecuador y los artículos 7 literal o), y 20 de la Ley Orgánica para la Transformación Digital y Audiovisual; y, además, es de implementación obligatoria para terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas, quienes podrán incorporar medidas adicionales de seguridad de la información".

CAPITULO III

3. MARCO METODOLÓGICO

La seguridad informática está regulada por normas que permiten implementar mecanismos de seguridad para cuidar los activos relacionados con los sistemas informáticos. Una de ellas es el estándar ISO 27001, donde se describen los lineamientos de seguridad de las organizaciones para garantizar la confidencialidad, autenticidad e integridad de la información.

La norma UNE – ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo corporativo/empresarial, que se establece para crear, implementar, operar, supervisar, mantener y mejorar la seguridad de la información, permitiendo el control sobre los sistemas de información que se maneja en la organización. Algunos beneficios de un SGSI son:

- Conocimiento profundo de la organización, cómo funciona y a su vez proporciona un plan de mejoramiento continuo para solucionar las posibles inconsistencias de seguridad informática presentada.
- Analizar los riesgos, identificando amenazas, vulnerabilidades y su impacto dentro de las actividades de la organización.
- Generar y aplicar planes de mejoramiento continuo en la gestión de la seguridad informática.
- Garantizar la continuidad y disponibilidad del negocio.
- Reducir los costos vinculados a los incidentes presentados.
- Incrementar los niveles de confianza de los clientes y usuarios de los sistemas informáticos.
- Cumplir con la normativa legal vigente en cuanto a la protección de datos sensibles, comercio electrónico, propiedad intelectual, notificaciones electrónicas, impugnaciones, notificaciones de infracciones.

3.1 Descripción del área de estudio

Un SGSI basado en una metodología EGSI, son estructuras organizativas y técnicas diseñadas para proteger los activos de información. Esto incluye la gestión de riesgos, la implementación de controles de seguridad, la concienciación del personal y la respuesta a incidentes. La seguridad de la información es crucial en la era digital actual, donde las organizaciones enfrentan amenazas cibernéticas cada vez más sofisticadas y deben cumplir con regulaciones de privacidad y protección de datos cada vez más estrictas.

La metodología EGSI se aplicará en la Dirección de Infracciones de la Agencia Metropolitana de Tránsito que es parte del Municipio del Distrito Metropolitano de Quito, misma que cuenta con 42 funcionarios y un Director. Dentro de los procesos fundamentales que realiza la Institución, es el manejo de todas las infracciones de tránsito que son levantadas en la ciudad y adicionalmente procesos electrónicos como foto multas, foto radares y foto peajes que son operados por medios tecnológicos.

La Dirección de Registro de Infracciones se encuentra en el orgánico funcional de la institución y forma parte de los procesos generadores de valor en virtud de que en esta Dirección se maneja gran parte de las sanciones y citaciones interpuestas en la ciudad de Quito.

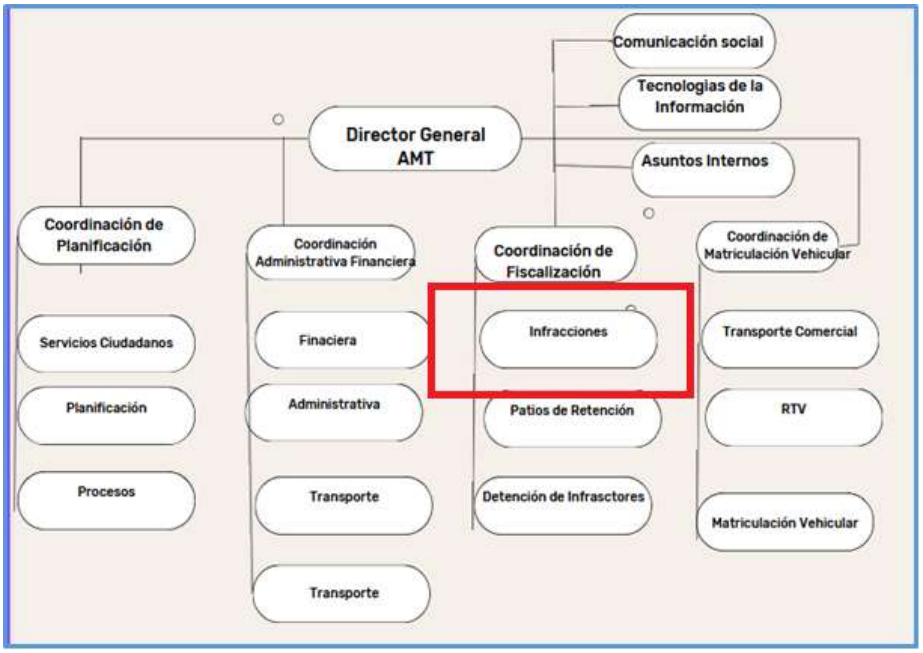


Tabla 4 Orgánico Funcional AMT, Archivo de Dirección de Infracciones

3.2 Enfoque y tipo de investigación

Tipo de investigación según su enfoque:

La investigación propuesta será realizada con un enfoque cualitativo la misma que utiliza la recolección de información sin medición numérica. En esencia se centra en el estudio de realidades subjetivas que pueden variar de un contexto, grupo o sujeto a otro mediante Santander Open Academy (2024)

De manera específica, la identificación de activos se realizó utilizando un enfoque cualitativo mediante la aplicación de una encuesta, adicionalmente la definición de riesgos, actividades de mitigación y definición de políticas se lo realizó mediante un análisis documental, y finalmente para la evaluación del SGSI propuesto, se aplicó como técnica el juicio de expertos.

Investigación Aplicada

La investigación aplicada, como indica QuestionPro. (2023) *" se centra en responder a preguntas concretas para resolver un problema específico. Trata de identificar una solución a un problema cultural u organizativo y suele ser un plan de investigación posterior "*, lo que en este caso particular se utiliza en la realización de políticas de seguridad para proteger la integridad de los datos que son sensibles y maneja la Institución.

Además, Este proyecto se lo considera como una investigación aplicada en razón de que, con la identificación de las vulnerabilidades en los activos de la institución, se buscó soluciones de mejora para que los riesgos puedan minimizarse y recomendar técnicamente soluciones para mejorar la ciberseguridad de la Agencia Metropolitana de Tránsito en la Dirección de Infracciones.

Grupo de Estudio

Como indica Rae, B (2023), en la identificación de un grupo de estudio se puede cuantificar los temas o sistemas que van a ser evaluados y en el contexto de un tema en particular. El grupo de estudio abarcó todos los activos más importantes que son manejados en la Dirección de Infracciones y que presentan riesgos por su vulnerabilidad, sensibilidad y su criticidad en la toma de decisiones que se dan en el nivel directivo de la institución.

Los resultados de las políticas de seguridad no solo benefician al GAD QUITO, sino también pueden aplicarse a cualquier GAD que maneja aspectos relacionados con los procesos de infracciones en los ámbitos de estudio que se manejan en este proyecto.

3.3 Procedimiento de investigación

Para alcanzar cada uno de los objetivos planteados en este trabajo, se propuso un procedimiento de investigación divido en fases, mismas que se describen a continuación:

Fase 1. Identificación de los activos de la información de la Dirección de Infracciones de la Agencia Metropolitana de Tránsito.

La norma ISO 27001 es una norma internacional cuyo enfoque se centra en el aseguramiento, integridad y confidencialidad de los datos, información y sistemas. Entre los elementos que ayudaron a una adecuada gestión de un sistema de seguridad informática se encuentran la gestión o evaluación de los riesgos y otro elemento fundamental es el inventario de activos de información.

La organización en ese sentido debió colocar todo su esfuerzo en la protección de los datos frente a las amenazas y riesgos posibles, de forma que aseguren el funcionamiento adecuado, disponibilidad e integridad. Con esto, además se ofrece la suficiente confianza a todos los colaboradores.

Para la adecuada identificación de activos se utilizó la ***Guía Figura para la gestión de riesgos de seguridad de la información*** *(RIESGOS DE SEGURIDAD DE LA INFORMACIÓN GUÍA PARA LA GESTIÓN DE, 2020)* de acuerdo con la siguiente clasificación:

- Actividades y procesos del negocio.
- Información.

Los activos de soporte (de los cuales dependen los elementos primarios del alcance) de todos los tipos:

- Hardware.
- Software.
- Redes.
- Personal.
- Ubicación.
- Estructura de la organización.

***Tabla 5**: Los activos primarios. (RIESGOS DE SEGURIDAD DE LA INFORMACIÓN GUÍA PARA LA GESTIÓN DE, 2020)*

Fase 2. Identificación de riesgo y definición de actividades de mitigación utilizando una metodología EGSI

Se estableció principios y procedimientos para identificar riesgos, definir actividades de mitigación y mejora continua en un Sistema de Gestión de Seguridad de la Información. Para el cumplimiento de esta fase, se siguió un enfoque estructurado y sistemático aplicando encuestas al personal de la Dirección de Infracciones de la AMT. En base a las encuestas, se pudo identificar los riesgos, vulnerabilidades y procedimientos para su mitigación considerando los parámetros establecidos por la metodología EGSI Gubernamental.

Fase 3. Definición de políticas de Seguridad de la Información.

Se hizo un seguimiento y trazabilidad de los datos de las infracciones registradas en la Agencia Metropolitana de Tránsito (AMT), ya que es fundamental la confidencialidad, integridad y confiabilidad de la información. Se plantearon políticas de seguridad de la información para que todo el procedimiento tenga concordancia con su aplicación y los procedimientos y actividades que se manejan en la Dirección de Infracciones de la AMT.

Fase 4. Evaluación del sistema de gestión de seguridad de la información (SGSI) contra las vulnerabilidades detectadas.

Se evaluó el sistema de gestión de la seguridad SGSI que se implementó mediante la aplicación de la técnica Delphi de la cual se obtuvo el criterio de tres expertos para su evaluación. Se realizó una entrevista introductoria con cada experto y posteriormente se les envió una tabla de evaluación en la cual se incluyó el objetivo de evaluación y los parámetros de evaluación que fueron ponderados en una escala Likert (alto, medio, deficiente, regular). Esto permitió establecer un criterio respecto al sistema de gestión de seguridad de la información planteado.

3.4 Consideraciones bioéticas

En esta investigación se realizaron entrevistas al personal de la Dirección de Infracciones de la AMT. Como parte del protocolo se puso en conocimiento de los jefes inmediatos el estudio que se va a realizar. Posteriormente se informó a los participantes sobre la privacidad y confiabilidad que se va a tener sobre el uso que se va a dar a la información suministrada, acatando los lineamientos que se tiene sobre la ley de protección de datos personales para que la misma no sea divulgada y peor usada de manera anti técnica. Durante todo el proceso de investigación se consideraron aspectos éticos y normativos.

CAPITULO IV
4. RESULTADOS

4.1 Identificación de activos de información de la Dirección de Infracciones de la Agencia Metropolitana de Tránsito

En esta fase se identifican los activos de acuerdo a los formatos y estándares de Gobierno Abierto del Ecuador que serán aplicados en la Dirección de Infracciones de la Agencia Metropolitana de Tránsito para obtener los resultados de la fase indicada (Vera ,2024).

4.1.1 Introducción a la aplicación del SGSI

En el actual entorno digital, la seguridad de la información hoy en día es uno de los pilares fundamentales para garantizar la integridad, confidencialidad y disponibilidad de los datos. Bajo este contexto, la Agencia Metropolitana de Tránsito reconoce la importancia estratégica de proteger la información sensible relacionada con sus operaciones, usuarios y socios.

La Agencia Metropolitana de Tránsito está comprometida con la protección de la seguridad de la información de su negocio frente a diversos eventos o circunstancias no deseadas, por lo tanto, ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) dando cumplimiento con la norma ISO/IEC 27001:2022, el cual es catalogado como el estándar internacional para la seguridad de la información.

En la presente fase se introduce el Sistema de Gestión de Seguridad de la Información (SGSI) de la Agencia Metropolitana de Tránsito, una iniciativa diseñada para salvaguardar la información crítica, promover buenas prácticas y mitigar posibles amenazas cibernéticas. Este sistema no solo cumple con los estándares y normativas internacionales en materia de seguridad de la información, sino que también se adapta a las necesidades específicas de la agencia y su entorno operativo, teniendo como propósito describir la forma en que opera el negocio, los factores internos y externos que influyen en él y resaltar en términos generales las posibles consecuencias de una brecha de seguridad. Esto permitirá poner en marcha la combinación más adecuada de medidas de control para reducir el nivel de riesgo y garantizar que se disponga de planes y se prueben para gestionar el impacto de cualquier interrupción que se produzca.

En concreto, se establece:

- El contexto de la organización
- Cuestiones externas e internas pertinentes para el propósito de Agencia Metropolitana de Tránsito Partes interesadas pertinentes para el SGSI
- Requisitos de seguridad de la información de estas partes interesadas
- El alcance del SGSI, incluidos sus límites y aplicabilidad

4.1.2 Contexto organizacional

La Agencia Metropolitana de Tránsito (AMT) se constituye como un organismo clave en la administración y regulación del tránsito en la ciudad, desempeñando un rol fundamental en la Movilidad urbana y la seguridad vial. Su principal objetivo es asegurar un sistema de transporte eficiente, seguro y sostenible para los habitantes y visitantes de la región metropolitana.

La AMT desempeña una función crucial en la creación de un entorno vial ordenado y seguro, priorizando la Movilidad sostenible y promoviendo una mejora continua en beneficio de la comunidad. Su compromiso con la seguridad vial y la eficiencia en el tránsito la convierte en un actor esencial en la planificación y ejecución de políticas orientadas a la Movilidad urbana.

El contexto organizativo de la Agencia Metropolitana de Tránsito se detalla en las siguientes secciones. Dado que los entornos de negocio y los mercados en los que opera son dinámicos, este contexto está sujeto a cambios. Este documento será revisado anualmente para incorporar cualquier modificación relevante. Asimismo, el Sistema de Gestión de la Seguridad de la Información (SGSI) se actualizará para reflejar las implicaciones de dichos cambios.

4.1.3 Actividades

Agencia Metropolitana de Tránsito lleva a cabo una amplia gama de actividades comerciales dentro de sus sectores objetivo y desarrolla constantemente nuevos productos y servicios para llevar al mercado.

- ¿Qué hace la organización?
    - Es una empresa de servicios a la comunidad que realiza el control de Tránsito y transporte dentro del Distrito Metropolitano de Quito

- Qué tipo de servicios en la nube se proporcionan, por ejemplo, SaaS, PaaS, IaaS (solo CSP)
    - Sistema de almacenamiento de correos electrónicos en la Nube
    - Sistema de resguardo de la información institucional
- ¿Cuándo se formó?
    - 2013
- ¿Cuál es su estructura, por ejemplo, grupo de empresas?
    - Director general de Tránsito
    - Coordinación general de fiscalización
    - Coordinación general de operaciones
    - Coordinación general de seguridad vial
    - Coordinación general administrativa financiera

- ¿Cuál es su principal sector industrial?
    - Servicio a la comunidad
- ¿Quiénes son sus principales clientes?
    - Usuario
    - Agencia Nacional de Tránsito
    - Empresa municipales
    - Secretaria de Movilidad
    - Unidades judiciales
    - Fiscalía
    - ¿En qué regiones geográficas opera?
    - Distrito Metropolitano de Quito
- ¿Cuál es su facturación anual?
    - Ingresos por multas, matriculación, RTV, 20.000.000

4.1.4 Funciones

Agencia Metropolitana de Tránsito consta de las siguientes funciones organizativas:

- Coordinación de Planificación
- Coordinación Administrativa Financiera
- Comunicación Social
- Tecnología de la Información y Asuntos Internos
- Coordinación de Fiscalización
- Coordinación de Matriculación Vehicular.

La Coordinación de Planificación, Coordinación Administrativa Financiera, Comunicación Social, Tecnología de la Información y Asuntos Internos se encuentran físicamente en el edificio matriz de la institución donde se verifica y se administra su infraestructura.

Coordinación de Fiscalización se encuentran físicamente en el edificio sucursal edificio ex hotel colonial de la institución donde se verifica y se administra su infraestructura mediante enlace dedicado

Coordinación de Matriculación Vehicular. se encuentran físicamente en el edificio sucursal edificio Bicentenario de la institución donde se verifica y se administra su infraestructura mediante enlace dedicado

4.1.4 Servicios

La Agencia Metropolitana de Tránsito ofrece los siguientes servicios principales a sus clientes:

Servicio de Matriculación Vehicular

- Se realiza la Matriculación de todos los vehículos que circulan dentro del Distrito Metropolitano de Quito
- Se realiza la revisión técnica vehicular, para verificar puntos visuales y temas de revisión de índices de calidad para no afectar el aire de DMQ
- Se da permiso de revisión de permisos operaciones para que puedan circular transporte comercial en Quito.

Servicios de Fiscalización.

- Se maneja las infracciones de tránsito cometidas tanto manual (levantas por ACT) y electrónicas (radares, foto multas)

- Se realiza la verificación del ingreso, verificación y posterior conciliación de valores
- Se gestiona el manejo de los vehículos ingresados a los patios de retención
- Se gestiona a los infractores de Tránsito que cometieron infracciones y fueron ingresados al centro de detención de tránsito.

Servicios de Coordinación Financiera

- Se gestiona la parte financiera de toda la institución y pagos que se debe dar a todos los proveedores.
- Se realiza la administración de todos los bienes de la institución.
- Se gestiona toda la flota y control vehicular que se tiene, tanto vehículo liviano, pesados y motocicletas
- Se gestiona la base de datos y archivos de la institución, tanto activo como pasiva.

Servicios de Planificación

- Se gestiona el POA de la institución
- Se maneja todos los procesos y optimización de los mismos
- Se da atención a todos los usuarios y sus requerimientos y se recibe documentación para entrega a todas las áreas de la institución.

Servicios de Tecnología de la información

- Realiza el análisis, implementación, pruebas y producción de nuevos u optimizaciones de sistemas
- Realizar el soporte a los aplicativos con sus mesas de ayuda
- Verificar el óptimo funcionamiento de la red institucional, servidores y data center.

4.1.5 **Productos**

Agencia Metropolitana de Tránsito ofrece los siguientes productos principales a sus clientes:

- Revisión Técnica Vehicular (RTV)
- Matriculación Vehicular
- Infracciones de Tránsito

- Coactivas
- Seguridad vial

¿Todos los productos se ofrecen a todos los clientes?

- A todos los ciudadanos que circulen dentro del DMQ o que hagan cometido alguna infracción en DMQ

¿Qué productos generan más ingresos y ganancias?

Los que generan más ingresos a la municipalidad son:

- RTV
- Matriculación Vehicular
- Infracciones de Tránsito
- Coactiva
- Seguridad Vial

No generan ganancias: porque son rubros o multas por incumplimientos

¿Algún producto depende de otros (requisitos previos)?

- Si para Matricular primero se debe realizar el RTV.

¿Qué productos son los más destacados?

- Los 5 productos indicados

¿Alguno de los productos está sujeto a regulación externa?

- Tasas ANT y al COIP

¿Alguno de los productos tiene un aspecto de salud y seguridad?

- Infracciones a la seguridad vial, y cumplimiento de normas

4.1.6 **Principales asociaciones**

Agencia Metropolitana de Tránsito tiene una política de formar asociaciones con otras organizaciones que complementan sus propias ofertas y brindan mayores beneficios a sus clientes.

En la actualidad existen las siguientes asociaciones importantes:

La Agencia Metropolitana de Tránsito no tienen asociaciones debido a que la competencia la delego la Agencia Nacional de Tránsito en el 2013 por cumplir todos los requerimientos de acuerdo a los requisitos y por ser un Municipio de tipo “A”.

4.1.7 Cadenas de suministro

Con el fin de proporcionar nuestros productos y servicios a nuestros clientes, existen una serie de importantes rutas de la cadena de suministro. Los principales son:

Los productos y servicios afectados:

- RTV
- Matriculación Vehicular
- Infracciones de Tránsito
- Coactivas
- Seguridad vial

Los eslabones de la cadena de suministro, tanto en términos de organizaciones involucradas como de geografía:

- Están involucradas las áreas generadoras de valor de la institución y son la cadena de suministros para que el usuario final tenga altos índices de solución a sus necesidades.

Qué tan establecida está la cadena de suministro:

- Se tiene protocolos, lineamientos, ordenanzas para cumplimientos de las cadenas de suministro.
- Valor de los ingresos y beneficios que dependen de la cadena de suministro
- Todos los valores de los procesos y servicios dependes de tarifario tanto de ANT y COIP para su cumplimiento.

Cualquier otra información relevante:

- Es importante señalar que con todos estos servicios el ciudadano puede validar sus requisitos y puede circular a nivel nacional sin ningún impedimento.

4.1.8 Objetivos y Políticas

El objetivo del Sistema de Gestión de Seguridad de la Información (SGSI) es asegurar que la Agencia Metropolitana de Tránsito mantenga su capacidad para cumplir con los objetivos de negocio establecidos y adherirse a sus políticas ante incidentes de seguridad, tanto potenciales como reales. En esta sección se detallan los principales objetivos y políticas empresariales vigentes para el ejercicio en curso, con el propósito de establecer una relación clara y directa entre estos y los objetivos del SGSI.

4.1.9 Objetivos de negocio

Para el ejercicio 2024 Agencia Metropolitana de Tránsito ha establecido los siguientes objetivos empresariales principales:

1. Ejecutar y planificar el control del transporte terrestre, tránsito y seguridad vial en el DMQ, sobre lo que se determina en base de la planificación municipal y demanda ciudadana, en el marco de la normativa nacional y metropolitana vigente alineado al Plan Metropolitano de Desarrollo y Ordenamiento Territorial (PMDOT);

2. Gestionar la planificación y fiscalización del control del transporte terrestre, tránsito y seguridad vial en eventos programados, en función del cumplimiento de indicadores operacionales del transporte comercial y de los operativos de control, con base a la normativa metropolitana vigente;

3. Implementar acciones encaminadas a la prevención, seguridad y educación vial, así como emitir criterios técnicos de ingeniería vial que contribuyan a una Movilidad segura de los ciudadanos del DMQ;

4. Verificar la prestación de los servicios de revisión técnica y matriculación vehicular en el DMQ, así como la gestión de permisos de operación de transporte comercial en taxi, carga liviana, transporte escolar e institucional en el DMQ;

5. Actuar con integridad por medio de la transparencia, rendición de cuentas, inclusión y diversidad;

6. Cumplir y hacer cumplir con la normativa legal vigente, dentro de sus competencias

4.1.10 Políticas de Negocios

La organización ha establecido políticas en una variedad de áreas y estas deben tenerse en cuenta durante el proceso de planificación de la seguridad de la información para garantizar que se cumplan. Las principales políticas relevantes son:

- Por un Quito conectado, brindar opciones de Movilidad y conectividad confiables, de calidad, eficiencia y seguras.
- Consolidar y fomentar la cultura de seguridad vial, sobre todo con respecto al respeto al peatón y al ciclista, para disminuir el número de accidentes de tránsito y sobre todo de víctimas fatales.
- Implementar los procesos necesarios para consolidar y fomentar una cultura de seguridad vial, sobre todo con respecto a las personas que transitan a pie y en bicicleta, esto con el fin de disminuir el número de accidentes de tránsito y sobre todo de víctimas que lamentar.

4.1.11 Problemas internos y externos

Hay una serie de cuestiones internas y externas que son relevantes para el propósito de Agencia Metropolitana de Tránsito y que afectan a la capacidad del SGSI para lograr los resultados previstos.

a. Problemas internos

Con respecto a la Agencia Metropolitana de Tránsito negocio en sí, hay una serie de cuestiones internas relevantes.

Entre ellas se encuentran:

- Se tiene descentralizado todo el personal administrativo en diferentes localizaciones.
- No se dispone de presupuesto propio se depende de planta central.
- Mucha rotación de autoridades y no se tiene de directrices claras para el manejo de la institución.

- Personal de la institución no está capacitado en temas de contratación pública por dicho motivo se han caído procesos importantes.
- No se tiene personal a gusto por sueldos bajos en comparación a sus actividades y horarios que se tiene.
- Todo el personal son islas y no se tiene una cultura de integración institucional.
- No se cuenta con incentivos para tareas de cumplimiento y esto es una gran desventaja porque el personal fuga la información

Estas cuestiones internas generales se examinarán con más detalle como parte del proceso de evaluación de riesgos.

b. Problemas externos

Con respecto al entorno externo en el que Agencia Metropolitana de Tránsito opera, hay una serie de cuestiones externas relevantes.

Entre ellas se encuentran:

Político

b. Cambios en autoridades recurrentes.
b. Autoridades desconocen del modelo de negocio de la institución
b. Mala imagen institucional.

Económico

a. No se dispone de flujo efectivo contable, ya que se depende de planta central
b. Se tiene proveedores incumplidos, y causa retraso en proceso de contratación.

Social

a. Cambios demográficos
b. Cambios en el crecimiento de la población
c. Actitudes sociales
d. Tecnología
e. Ritmo de innovación

f. Tecnologías e infraestructura de apoyo
g. Automatización e inteligencia artificial

Legal

a. Posibles cambios COIP
b. Cambios Ordenanzas y resoluciones
c. protección de datos
d. Medio ambiente
e. cambio climático
f. incendios, inundaciones, terremotos, etc.
g. contaminación

Estas cuestiones externas generales se examinarán con más detalle como parte del proceso de evaluación de riesgos.

4.1.12 Activos de la Dirección de Infracciones

Después de los análisis del EGSI de la Dirección de Registro de Infracciones de la AMT se ha podido identificar los siguientes activos, en las cuales están catalogadas por las diferentes esquematizaciones que indican la normativa actual vigente:

Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo	Intención del Uso	Tipo de soporte	Ubicación
A1	Infracciones	Fotomultas	Hardware	Camaras de Fotmultas	Equipos que se utilizan para infraccionar multas tecnol+ogicas	Seguridad Vial, control del tránsito	Físico	Puntos de control Distrito Metropolitano de Quito
A2	Infracciones	Fotomultas	Hardware	Hand Held	Equipos que se utilizan para infraccionar multas por APP	Seguridad Vial, control del tránsito	Físico	Agentes Civiles de Tránsito
A3	Infracciones	Fotomultas	Software	Sistema Socrit Infracciones	Es el sistema que recepta todas las infracciones , valida , sanciona y notifica	Notificación de Infracciones de tránsito	Físico y Digital	Validadores , personal Tecnico de infracciones
A4	Infracciones	Fotomultas	Software	Sistema Axis Cloud	Sistema de ingreso de recaudaciones de infracciones de tránsito	Recaudar montos generados de infracciones	Físico y Digital	Personal de Recaudación y de servicios Ciudadanos.
A5	Infracciones	Fotomultas	Software	Webservice ANT	Interconección con sistema de ANT para consultar vechiculos y Propietarios	Interconexion para consulta de informacion por la placa	Digital	Data Center Matriz
A6	Infracciones	Fotomultas	Software	Sistema Dinardap	Interconección con sistemas de SRI	Interconexion para consulta de informacion por ciudadano	Digital	Data Center Matriz
A7	Infracciones	Fotomultas	Hardware	Servidor de Aplicaciones	Es el equipo donde esta el sistema de Infracciones de la Institución	Para manejo de Fotomultas	Digital	Data Center Matriz
A8	Infracciones	Fotomultas	Hardware	Servidor de base de datos	Es el equipo donde esta la base de datos de Infracciones de la Institución	Para manejo de Fotomultas	Digital	Data Center Matriz
A9	Infracciones	Fotomultas	Hardware	Seguridad Perimetral	Es la seguridad perimetral que se tiene instalada en la institución.	Para manejo de Fotomultas	Físico y Digital	Data Center Matriz
A10	Infracciones	Fotomultas	Hardware	Enlaces comunicaciones puntos de control	Son los medios de comunicación para el sistema de fotomultas	Para manejo de Fotomultas	Físico y Digital	Data Center Matriz
A11	Infracciones	Fotomultas	Hardware	Enlaces comunicaciones data center	Son los medios de comunicación para que abarca todos los enlances entrantes y salientes del data center para el funcionamiento	Para manejo de Fotomultas	Físico y Digital	Data Center Matriz
A12	Infracciones	Fotomultas	Hardware	Chip de comunicación de radares	Son los enlaces mediante chipo para comunicación de radares	Para manejo de Fotomultas	Físico y Digital	Radares DMQ
A13	Infracciones	Fotomultas	Software	Sistema SERT zona tarifaria	Es el sistema que recepta todas las evasiones de irrespeto a la zona tarifaria	Para manejo de Fotomultas	Digital	Data Center Matriz
A14	Infracciones	Fotomultas	Organización	Personal que maneja sistema Fotomultas , SERT , Agentes Civiles de Tránisto	Talento Humano necesario para funcionamiento Infracciones	Pesonal necesario para el proceso	Físico	Oficina Matriz , vias asignadas a Agentes Civiles de Tránisto
A15	Infracciones	Fotomultas	Software	Portal Institucional	Portal donde se presenta todos los servicios a los ciudadanos .	Page Web Insticional	Digital	Data Center Matriz

Tabla 6 Activos de Hardware (*Autoría Propia)*

4.2 Procedimientos para identificación de riesgos y definición de actividades de mitigación utilizando una metodología EGSI Gubernamental

Uno de los aspectos clave para el desarrollo del proyecto es la investigación destinada a establecer procedimientos para la identificación de riesgos en la Dirección de Infracciones de la AMT, en cumplimiento con las normas y políticas de seguridad de la información.

Para identificar los riesgos y definir actividades de mitigación, se aplicará la metodología EGSI Gubernamental, utilizando un procedimiento estructurado que garantice la consistencia y efectividad en la gestión de riesgos. Este enfoque permitirá identificar vulnerabilidades, priorizarlas y actuar de manera proactiva para reducir su impacto.

Se han definido principios y procedimientos específicos para este propósito, los cuales incluyen la realización de encuestas dirigidas a los responsables de la Dirección de Infracciones. Estas encuestas ayudarán a identificar riesgos y vulnerabilidades existentes. Con base en los resultados, se implementarán medidas de mitigación alineadas con la metodología EGSI Gubernamental, ya integrada en la dirección.

Posteriormente, se llevará a cabo un análisis detallado de las respuestas obtenidas, estableciendo un punto de partida sólido para desarrollar una gestión efectiva de riesgos en el departamento.

Estos procedimientos aseguran una gestión de riesgos sistemática y proactiva, en línea con las mejores prácticas y las normativas gubernamentales vigentes. La metodología EGSI (Esquema Gubernamental de Seguridad de la Información) proporciona un marco robusto para proteger la seguridad y la integridad de la información en el ámbito gubernamental.

Entrevistado / Pregunta	Encargado de Fotomultas y Radares	Técnico de Mantenimiento de Fotomultas Y Radares	Auditor de Fotomultas y Radares	Validador de Fotomultas y Radares	Validador de Fotomultas y Radares
1.- ¿Actualmente existen políticas que gestionen la seguridad de la información?	Si existen para ingreso a los sistemas , control de usuarios , acceso al internet es por perfiles	Si existen para ingreso a sistemas	Si existen para ingreso a sistemas	Si existen para ingreso a sistemas	Desconozco si existen
2.-¿Los usuarios se encuentran capacitados para el uso de los recursos tecnológicos?	Si, se encuentran	Si, se encuentran	Parcialmente	No, estan capacitados	No, estan capacitados
3.-¿Existen controles sobre el acceso de personal interno y externo al equipamiento y Sistemas de Fotomultas?	Si, solo ingresa personal de TIC	Si, solo ingresa personal de TIC	Existen controles , pero no sobre todo los procesos	No existe ningún control	No existe ningún control
4.- ¿Existe un plan de mantenimiento para los equipos tecnológico de fotomultas.?	Si, existe contrato de mantenimiento	Si, existe contrato de mantenimiento	Si, pero no se sabe los alcances	Es necesario una socialización de que se hace en los mantenimientos	Es necesario una socialización de que se hace en los mantenimientos
5 .- ¿Existe un plan de contingencia para cualquier eventualidad que pueda suceder o amenazar a los sistemas de información	Si existen plan de contigencia por TIC	Si existen plan de contigencia por TIC	Si existe, pero se necesita mas planes para toda la Dirección	Existe Plan pero deben ser mejor socializados	Si existe, pero se necesita mas planes para toda la Dirección
6.- ¿Se establece controles de acceso físico a los lugares donde se	Si mediante claves y procedimientos	Si mediante claves y procedimientos	Si mediante claves y procedimientos	No, se desconoce los controles	No, se desconoce los controles
7 .- ¿La AMT establece seguridad en la instalación de sus enlaces de datos para los dispositivos que captan información de dispositivos tecnológicos?	Si, de acuerdo a politicas se seguridad perimetral	Si, de acuerdo a politicas se seguridad perimetral	Si, pero deben ser mas robustas	No, se desconoce los controles	No, se desconoce los controles
8.- ¿La AMT establece y aplica protocolos y tecnologías para la autenticación segura?	Si, de acuerdo a politicas internas y municipales	Si, de acuerdo a politicas internas y municipales	Si, de acuerdo a politicas internas y municipales	Si, pero no esta bien socializado	Si, pero no esta bien socializado
9.- ¿La AMT establece y aplica un procedimiento debidamente documentado y conocido por todos para los controles de seguridad cibernética que los terceros/proveedores deben seguir para relacionarse con la entidad?	No, se dispone de procedimietos de ciberseguridad	No, se dispone de procedimietos de ciberseguridad	No, se ha socializado procedimientos	No, se ha socializado procedimientos	No, se ha socializado procedimientos
10 .- ¿Han firmado algún acuerdo de confidencialidad o de protección de datos en el último año?	Si, se firma para los sistemas que maneja la Dirección de Infracciones	Si, se firma para los sistemas que maneja la Dirección de Infracciones	Si, se firma para los sistemas que maneja la Dirección de Infracciones	Si, se firma para los sistemas que maneja la Dirección de Infracciones, pero no de protección de datos	Si, se firma para los sistemas que maneja la Dirección de Infracciones, pero no de protección de datos
11- ¿Conoce Ud. Acerca de algún Sistema de Gestión de Seguridad de la Información(SGSI)?	Si, conozco sistemas SGSI	Si, deben implementarse en Infracciones para evitar vulnerabilidades	Si, deben implementarse en Infracciones para evitar vulnerabilidades	Dezconosco el tema indicado	Dezconosco el tema indicado

Tabla 7 Encuestas (*Autoría Propia)*

4.2.1. Tabulación de Resultados.

1.- Actualmente *existen políticas que gestionen la seguridad de la información?*

RESPUESTA	CANTIDAD	PORCENTAJE
Si existen para ingreso a los sistemas , control de usuarios , acceso al internet es por perfiles	1	20%
Si existen para ingreso a sistemas	3	60%
Desconozco si existen	1	20%
Total	**5**	**100%**

Tabla 8 Pregunta 1 (*Autoría Propia)*

Grafico 1 Pregunta 1 (*Autoría Propia)*

Interpretación. – Del total de los entrevistados, el 60% afirma que si existen políticas para ingresar a sistemas e ingreso al internet otro 20% afirma que existen políticas para los ingreso a los sistemas dentro de la Dirección de Infracciones de la AMT y 20% desconoce si existen

Análisis. – Existen políticas para la seguridad de información dirigidas a los sistemas de información y al acceso de internet sin embargo, se puede concluir que los sistemas de información tienen un nivel confiable de protección de acuerdo a lo evaluado.

2.-¿Los usuarios se encuentran capacitados para el uso de los recursos tecnológicos?

RESPUESTA	CANTIDAD	PORCENTAJE
Si, se encuentran	2	40%
Parcialmente	1	20%
No, estan capacitados	2	40%
Total	**5**	**100%**

Tabla 9 Pregunta 2 (*Autoría Propia)*

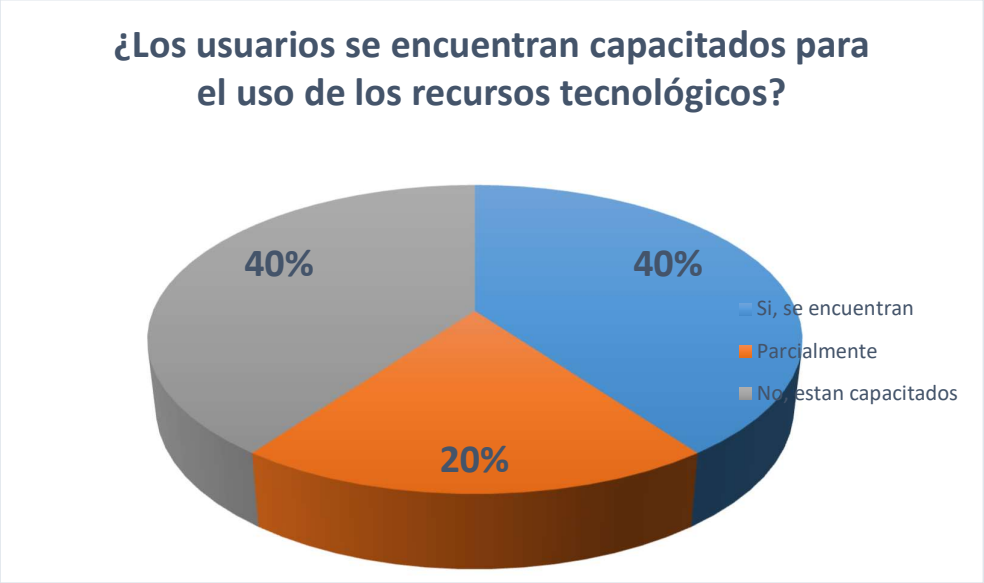


Grafico 2 Pregunta 2 (*Autoría Propia)*

Interpretación. – Del total de los entrevistados, el 40% afirma que si encuentran capacitados , el 40% indica que se encuentra parcialmente capacitados y el 20% no se encuentra capacitados en los sistemas dentro de la Dirección de Infracciones de la AMT.

Análisis. – Existen políticas para la seguridad de información dirigidas a los sistemas de información por lo cual es imperante se masifique las capacitaciones dentro de la Dirección de Infracciones de la AMT , para que el personal se eficaz y eficiente en todos sus procesos.

3.-¿Existen controles sobre el acceso de personal interno y externo al equipamiento y Sistemas de Fotomultas?

RESPUESTA	CANTIDAD	PORCENTAJE
Si, solo ingresa personal de TIC	2	40%
Existen controles , pero no sobre todo los procesos	1	20%
No existe ningún control	2	40%
Total	**5**	**100%**

Tabla 10 Pregunta 3 (*Autoría Propia)*

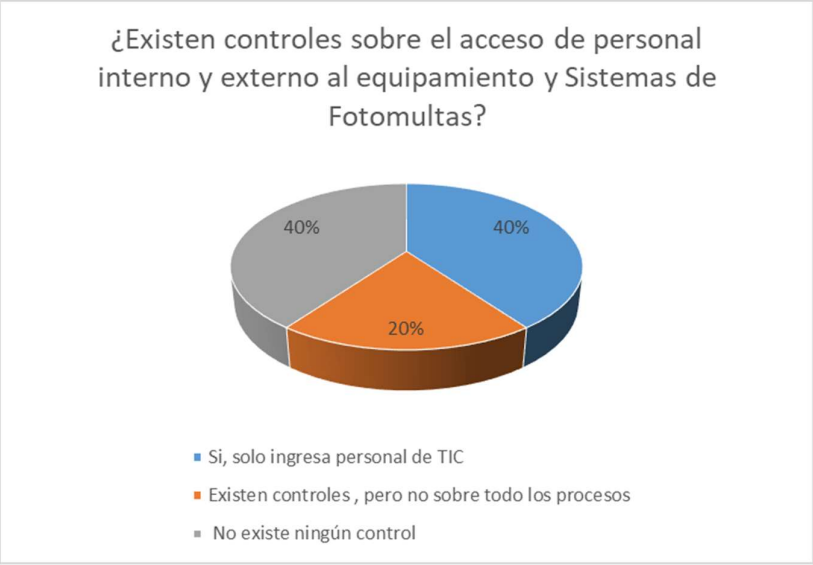


Grafico 3 Pregunta 3 (*Autoría Propia)*

Interpretación. – Del total de los entrevistados, el 40% indica que ingresa solo personal de TIC, 40% indica que existen controles , y el 20% indica que no existe dentro de la Dirección de Infracciones de la AMT.

Análisis. – Existen controles acceso de personal interno y externo al equipamiento pero se debe generar procedimientos y protocolos de acceso para que no exista vulnerabilidad de la información que se maneja.

4.- ¿Existe un plan de mantenimiento para los equipos tecnológico de foto multas?

RESPUESTA	CANTIDAD	PORCENTAJE
Si, existe contrato de mantenimiento	2	40%
Si, pero no se sabe los alcances	1	20%
Existe Plan pero deben ser mejor socializados	2	40%
Total	**5**	**100%**

Tabla 11 Pregunta 4 (*Autoría Propia)*

Grafico 4 Pregunta 4 (*Autoría Propia)*

Interpretación. – Del total de los entrevistados, el 40% indica que existe un contrato de mantenimiento , 40% indica que existe un plan pero no es socializado y el 20% indica q si existe pero no sabe los alcance dentro de la Dirección de Infracciones de la AMT.

Análisis. – Existe planes de mantenimientos pero los funcionarios no sabe sus alcance de los mismos , que serían importante socializar los documentos dentro de la Dirección de Infracciones de la AMT.

5 .- ¿Existe un plan de contingencia para cualquier eventualidad que pueda suceder o amenazar a los sistemas de información

RESPUESTA	CANTIDAD	PORCENTAJE
Si existen plan de contigencia por TIC	2	40%
Existe Plan pero deben ser mejor socializados	1	20%
Si existe, pero se necesita mas planes para toda la Dirección	2	40%
Total	**5**	**100%**

Tabla 12 Pregunta 5 (*Autoría Propia)*

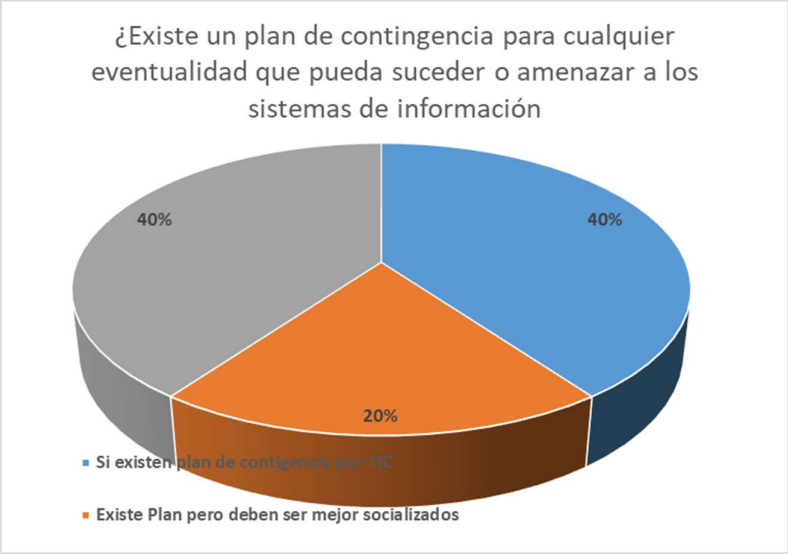


Grafico 5 Pregunta 5 (*Autoría Propia)*

Interpretación. – Del total de los entrevistados, el 40% indica que existe plan de contingencia , 40% sabe que existe pero no son socializados y el 20% existen pero necesita más planes de contingencia dentro de la Dirección de Infracciones de la AMT.

Análisis. – Existe planes de contingencia pero los funcionarios no sabe sus alcance de los mismos , que serían importante socializar los documentos dentro de la Dirección de Infracciones de la AMT.

6.- ¿Se establece controles de acceso físico a los lugares donde se almacena la información?

RESPUESTA	CANTIDAD	PORCENTAJE
Si mediante claves y procedimientos	3	60%
No, se desconoce los controles	2	40%
Total	**5**	**100%**

Tabla 13 Pregunta 6 (*Autoría Propia)*

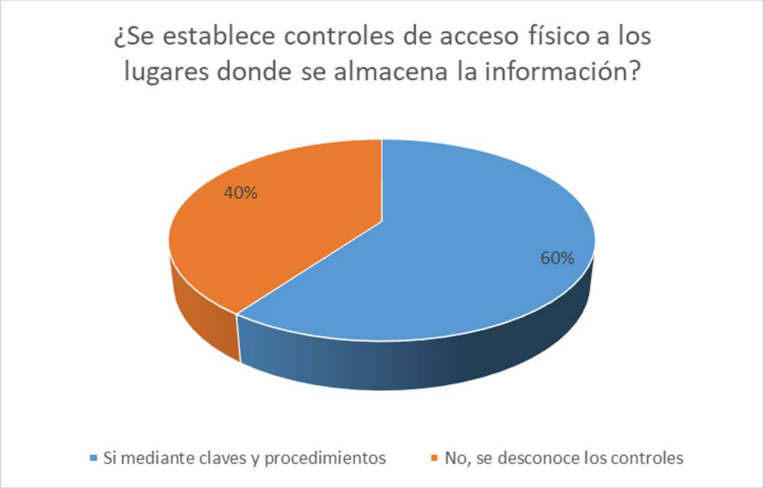


Grafico 6 Pregunta 6 (*Autoría Propia)*

Interpretación. – Del total de los entrevistados, el 60% indica que existe claves y procedimientos de almacenaje de la información , 40% desconoce los controles que se aplica para el almacenamiento dentro de la Dirección de Infracciones de la AMT

Análisis. – Existen controles de almacenaje de la información pero se debería informar a todo el personal de TIC sobre sus procedimientos que se deben cumplir socializar con personal técnico de la Dirección de Infracciones de la AMT.

7 .- ¿La AMT establece seguridad en la instalación de sus enlaces de datos para los dispositivos que captan información de dispositivos tecnológicos?

RESPUESTA	CANTIDAD	PORCENTAJE
Si, de acuerdo a politicas se seguridad perimetral	2	40%
Si, pero deben ser mas robustas	1	20%
No, se desconoce los controles	2	40%
Total	**5**	**100%**

Tabla 14 Pregunta 7 (*Autoría Propia)*

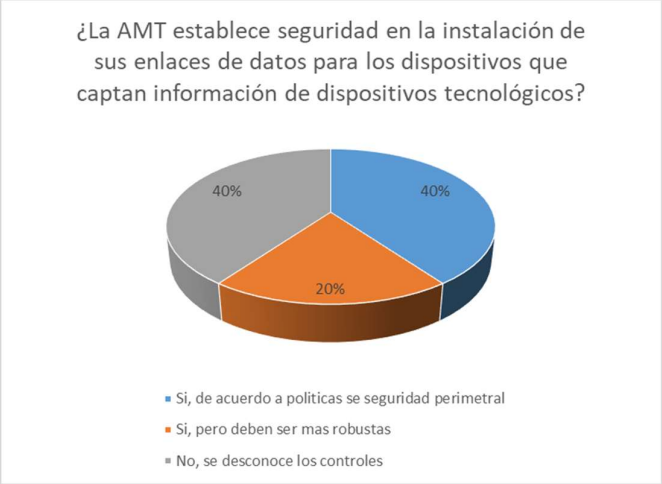


Grafico 7 Pregunta 7 (*Autoría Propia)*

Interpretación. – Del total de los entrevistados, el 40% indica que existe políticas de seguridad perimetral para sus enlaces de datos , 40% desconoce los controles que se aplica para la seguridad de enlaces de comunicación y el 20% indica que las seguridades deben ser más robustas dentro de la Dirección de Infracciones de la AMT

Análisis. – Existen seguridad en la instalación de sus enlaces de datos para los dispositivos que captan información, pero se debe realizar consultorías del nivel de protección que se maneja a nivel de la institución , para min minimizar vulnerabilidad y tener altos % de confidencialidad en los enlaces de la Institución.

8.- ¿La AMT establece y aplica protocolos y tecnologías para la autenticación segura?

RESPUESTA	CANTIDAD	PORCENTAJE
Si, de acuerdo a politicas internas y municipales	3	60%
Si, pero no esta bien socializado	2	40%
Total	**5**	**100%**

Tabla 15 Pregunta 8 (*Autoría Propia)*

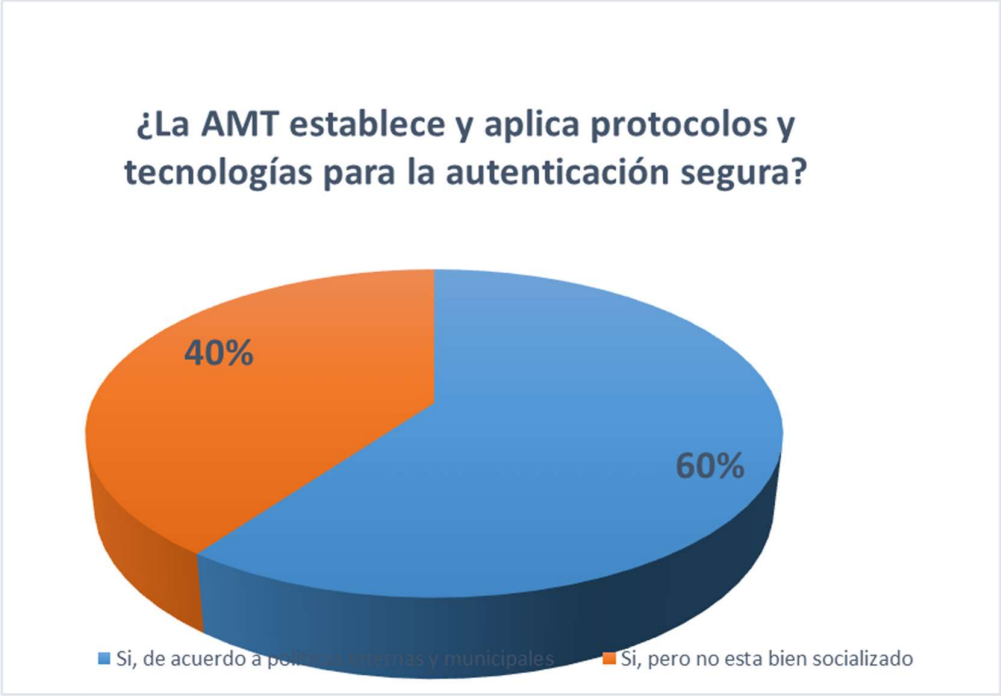


Grafico 8 Pregunta 8 (*Autoría Propia)*

Interpretación. – Del total de los entrevistados, el 60 % está de acuerdo que existe políticas de autentificación segura y el 40% afirma que si existe pero no se ha socializado dentro de la Dirección de Infracciones de la AMT.

Análisis. – Existen políticas de autentificación segura pero con una consultoría de seguridad de información se va a brindar y atacar a sistemas que no cumple los requerimientos mínimos para su utilización y no son seguros en su autentificación.

9.- ¿La AMT establece y aplica un procedimiento debidamente documentado y conocido por todos para los controles de seguridad cibernética que los terceros/proveedores deben seguir para relacionarse con la entidad?

RESPUESTA	CANTIDAD	PORCENTAJE
No, se dispone de procedimietos de ciberseguridad	2	40%
No, se ha socializado procedimientos	3	60%
Total	**5**	**100%**

Tabla 16 Pregunta 9 (*Autoría Propia)*

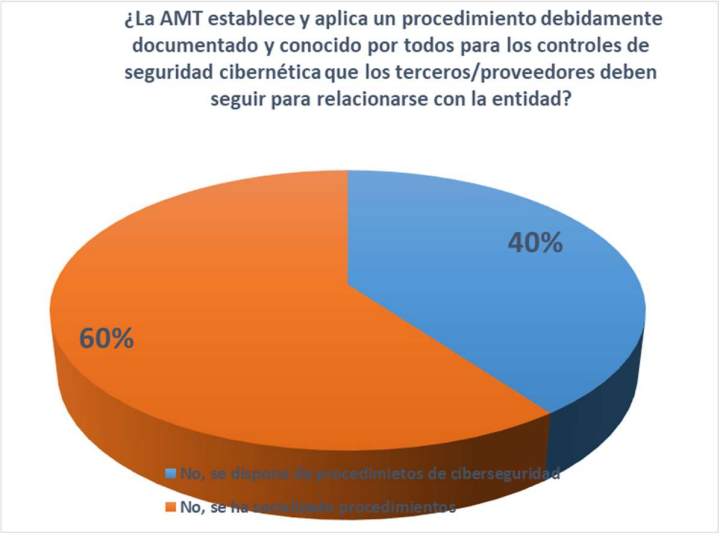


Grafico 9 Pregunta 9 (*Autoría Propia)*

Interpretación. – Del total de los entrevistados, el 60% afirma que no se ha socializado procedimientos de ciberseguridad y el 40% afirma que no se dispone procedimientos dentro de la AMT.

Análisis. – se debe gestionar una consultoría de ciberseguridad para que la institución tenga procedimientos, políticas de protección a los sistemas de seguridad.

10 .- ¿Han firmado algún acuerdo de confidencialidad o de protección de datos en el último año?

RESPUESTA	CANTIDAD	PORCENTAJE
Si, se firma para los sistemas que maneja la Dirección de Infracciones	3	60%
Si, se firma para los sistemas que maneja la Dirección de Infracciones, pero no de protección	2	40%
Total	**5**	**100%**

Tabla 17 Pregunta 10 (*Autoría Propia)*

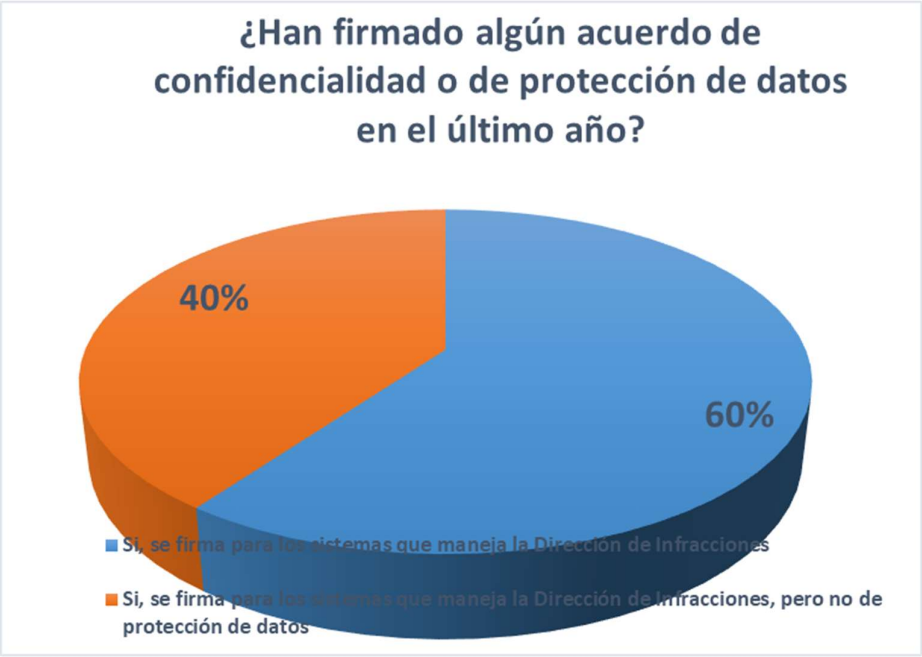


Grafico 10 Pregunta 10 (*Autoría Propia)*

Interpretación. – Del total de los entrevistados, el 60% afirma que si se firma acuerdos de confidencialidad y el 40 % si se tienes acuerdo de confidencialidad pero no de protección de datos para los sistemas dentro de la Dirección de Infracciones de la AMT.

Análisis. – Se debe realizar una verificación por parte del Departamento Legal de la AMT del modelo de acuerdo de confidencialidad para que aplique también la protección de datos que es requisito principal de acuerdo a la nueva ley enmarcada para su uso y aplicación obligatoria.

11- ¿Conoce Ud. Acerca de algún Sistema de Gestión de Seguridad de la Información(SGSI)?

RESPUESTA	CANTIDAD	PORCENTAJE
Si, conozco sistemas SGSI	1	20%
Si, deben implementarse en Infracciones para evitar vulnerabilidades	2	40%
Dezconosco el tema indicado	2	40%
Total	**5**	**100%**

Tabla 18 Pregunta 11 (*Autoría Propia)*

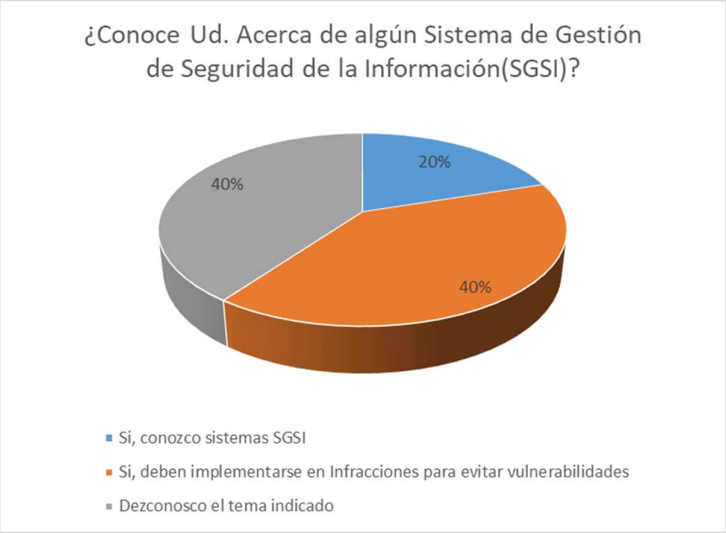


Grafico 11 Pregunta 11 (*Autoría Propia)*

Interpretación. – Del total de los entrevistados, el 20 % indica que si conoce de sistemas SGSI , 40% indica que debe implementarse en Infracciones para evitar vulnerabilidades y el 20% indica que desconoce del tema.

Análisis. – Existen un % alto dentro de la institución que conoce el uso y manejo de SGSI para lo cual se debe implementar en la dentro de la Dirección de Infracciones de la AMT para su difusión en toda la Institución

A partir de las entrevistas realizadas al personal de la Dirección de Registro de Infracciones, se han identificado los riesgos detallados en los formatos establecidos por el ACUERDO Nro. MINTEL-MINTEL-2024-0003, el cual regula la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) para las instituciones públicas.

Estos datos han servido como base para evaluar la efectividad de las prácticas actuales de seguridad de la información y para proporcionar recomendaciones orientadas a su mejora. Mediante un análisis riguroso y la elaboración de un plan de acción detallado, la Agencia Metropolitana de Tránsito, y en particular la Dirección de Infracciones, puede fortalecer su postura de seguridad, optimizar la gestión de riesgos y garantizar una protección más efectiva de la información sensible.

Para lo cual se detallan a continuación los siguientes análisis que se han efectuado de acuerdo a la metodología EGSI:

- Listado y valoración de activos de la información
- Análisis de riesgos
    - Evaluación de riesgos
    - Tratamiento de Riesgos
    - Implementación de control
- Plan de tratamiento de riesgos.

Listado y valoración de los activos de información

Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo	Intención del Uso	Tipo de soporte	Ubicación	Valoración de Impacto (pérdida) C: Confidencialidad I: Integridad D: Disponibilidad			
									C	I	D	VA
A1	Infracciones	Fotomultas	Hardware	Camaras de Fotmultas	Equipos que se utilizan para infraccionar multas tecnol+ogicas	Seguridad Vial, control del tránsito	Físico	Puntos de control Distrito Metropolitano de Quito	3	2	1	2,00
A2	Infracciones	Fotomultas	Hardware	Hand Held	Equipos que se utilizan para infraccionar multas por APP	Seguridad Vial, control del tránsito	Físico	Agentes Civiles de Tránsito	2	1	2	1,67
A3	Infracciones	Fotomultas	Software	Sistema Socrit Infracciones	Es el sistema que recepta todas las infracciones , valida , sanciona y notifica	Notificación de Infracciones de tránsito	Físico y Digital	Validadores , personal Tecnico de infracciones	3	2	3	2,67
A4	Infracciones	Fotomultas	Software	Sistema Axis Cloud	Sistema de ingreso de recaudaciones de infracciones de tránsito	Recaudar montos generados de infracciones	Físico y Digital	Personal de Recaudación y de servicios Ciudadanos.	3	3	3	3,00
A5	Infracciones	Fotomultas	Software	Webservice ANT	Interconección con sistema de ANT para consultar vechiculos y Propietarios	Interconexion para consulta de informacion por la placa	Digital	Data Center Matriz	3	2	3	2,67
A6	Infracciones	Fotomultas	Software	Sistema Dinardap	Interconección con sistemas de SRI	Interconexion para consulta de informacion por ciudadano	Digital	Data Center Matriz	1	2	1	1,33
A7	Infracciones	Fotomultas	Hardware	Servidor de Aplicaciones	Es el equipo donde esta el sistema de Infracciones de la Institución	Para manejo de Fotomultas	Digital	Data Center Matriz	3	2	3	2,67
A8	Infracciones	Fotomultas	Hardware	Servidor de base de datos	Es el equipo donde esta la base de datos de Infracciones de la Institución	Para manejo de Fotomultas	Digital	Data Center Matriz	3	2	3	2,67
A9	Infracciones	Fotomultas	Hardware	Seguridad Perimetral	Es la seguridad perimetral que se tiene instalada en la institución.	Para manejo de Fotomultas	Físico y Digital	Data Center Matriz	1	2	3	2,00
A10	Infracciones	Fotomultas	Hardware	Enlaces comunicaciones puntos de control	Son los medios de comunicación para el sistema de fotomultas	Para manejo de Fotomultas	Físico y Digital	Data Center Matriz	2	2	2	2,00
A11	Infracciones	Fotomultas	Hardware	Enlaces comunicaciones data center	Son los medios de comunicación para que abarca todos los enlances entrantes y salientes del data center para el funcionamiento	Para manejo de Fotomultas	Físico y Digital	Data Center Matriz	2	2	2	2,00
A12	Infracciones	Fotomultas	Hardware	Chip de comunicación de radares	Son los enlaces mediante chipo para comunicación de radares	Para manejo de Fotomultas	Físico y Digital	Radares DMQ	1	2	1	1,33
A13	Infracciones	Fotomultas	Software	Sistema SERT zona tarifaria	Es el sistema que recepta todas las evasiones de irrespeto a la zona tarifaria	Para manejo de Fotomultas	Digital	Data Center Matriz	3	3	1	2,33
A14	Infracciones	Fotomultas	Organización	Personal que maneja sistema Fotomultas , SERT , Agentes Civiles de Tránisto	Talento Humano necesario para funcionamiento Infracciones	Pesonal necesario para el proceso	Físico	Oficina Matriz , vias asignadas a Agentes Civiles de Tránisto	2	2	2	2,00
A15	Infracciones	Fotomultas	Software	Portal Institucional	Portal donde se presenta todos los servicios a los ciudadanos .	Page Web Insticional	Digital	Data Center Matriz	3	3	3	3,00

Tabla 19 Listado y Valoración de activos (*Autoría Propia)*

Análisis de Riesgos

Análisis de Riesgos						Evaluación de Riesgos					
						Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Proceso Macro	Subprocesos	Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad			
Infracciones	Fotomultas	A1	Camaras de Fotmultas	Manifestaciones , vandalismos	Desastres naturales	2,00	3	2	Protocolos de seguridad	12,00	ALTO
Infracciones	Fotomultas	A2	Hand Held	Dispositivos Dañados	Falta de mantenimientos	1,67	1	3		5,00	MEDIO
Infracciones	Fotomultas	A3	Sistema Socrit Infracciones	Hackeo	Fuga de información	2,67	3	3	Politicas de seguridad, sistema de perfiles y auditoria	24,00	ALTO
Infracciones	Fotomultas	A4	Sistema Axis Cloud	Hackeo	Fuga de información	3,00	3	3	Politicas de seguridad, sistema de perfiles y auditoria	27,00	ALTO
Infracciones	Fotomultas	A5	Webservice ANT	No disponibilidad de Webservice	Información incorrecta de recuperación de propietarios y vechiculos	2,67	3	3	Webservice seguros	24,00	ALTO
Infracciones	Fotomultas	A6	Sistema Dinardap	No disponibilidad de Webservice	Información incorrecta de recuperación de propietarios , vechiculos y otras	1,33	2	2	Webservice seguros	5,33	MEDIO
Infracciones	Fotomultas	A7	Servidor de Aplicaciones	Hackeo	Falta de mantenimiento , no contar con personal capacitado	2,67	3	3	Control de accesos por acive directory	24,00	ALTO
Infracciones	Fotomultas	A8	Servidor de base de datos	Hackeo	Falta de mantenimiento , no contar con personal capacitado	2,67	3	3	Control de accessos a DBA y usuarios autorizados	24,00	ALTO
Infracciones	Fotomultas	A9	Seguridad Perimetral	Acceso no Permitidos	Equipos sin vida útil, renovación tecnólogica	2,00	3	3	Firewall	18,00	ALTO
Infracciones	Fotomultas	A10	Enlaces comunicaciones puntos de control	Acceso no Permitidos	Accesos de contratación largas, caidas de procesos	2,00	3	3		18,00	ALTO
Infracciones	Fotomultas	A11	Enlaces comunicaciones data center	Acceso no Permitidos	Accesos de contratación largas, caidas de procesos	2,00	3	3		18,00	ALTO
Infracciones	Fotomultas	A12	Chip de comunicación de radares	Perdida de chips , no llevar control donde estan fisicamente instalados los chips	Accesos de contratación largas, caidas de procesos	1,33	2	2	Se acoje politicas de proveedor existente	5,33	MEDIO
Infracciones	Fotomultas	A13	Sistema SERT zona tarifaria	Hackeo	Fuga de información	2,33	2	2	Politicas de seguridad, sistema de perfiles y auditoria	9,33	ALTO
Infracciones	Fotomultas	A14	Personal que maneja sistema Fotomultas , SERT , Agentes Civiles de Tránisto	Personal no comprometido por sueldos bajos	Fuga de información	2,00	3	3	Convenios de confidencialidad	18,00	ALTO
Infracciones	Fotomultas	A15	Portal Institucional	Hackeo	Fuga de información	3,00	3	3	Politicas de seguridad, firewall	27,00	ALTO

Tabla 20 Análisis de riesgo (*Autoría Propia)*

Análisis de Riesgos						Tratamiento de Riesgos						
Proceso Macro	Subprocesos	Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	Riesgo residual
Infracciones	Fotomultas	A1	Camaras de Fotmultas	Manifestaciones , vandalismos	Desastres naturales	CONTROL CORRECTIVO	Compra de nuevos camaras de Fotomultas y con politicas de seguridad de acuerdo al fabricante	1	1	2,00	BAJO	ACEPTABLE
Infracciones	Fotomultas	A2	Hand Held	Dispositivos Dañados	Falta de mantenimientos	CONTROL PREVENTIVO	Renovación de equipos con tecnologia y seguridades de punta	3	2	12,00	ALTO	INACEPTABLE
Infracciones	Fotomultas	A3	Sistema Socrit Infracciones	Hackeo	Fuga de información	CONTROL PREVENTIVO	Contratación de consultoria de ciberseguridad para evaluacion y aplicación de correcciones de vulnerabilidades	3	3	18,00	ALTO	INACEPTABLE
Infracciones	Fotomultas	A4	Sistema Axis Cloud	Hackeo	Fuga de información	CONTROL PREVENTIVO	Contratación de consultoria de ciberseguridad para evaluacion y aplicación de correcciones de vulnerabilidades	3	3	18,00	ALTO	INACEPTABLE
Infracciones	Fotomultas	A5	Webservice ANT	No disponibilidad de Webservice	Información incorrecta de recuperación de propietarios y vechiculos	CONTROL PREVENTIVO	Contratación de consultoria de ciberseguridad para evaluacion y aplicación de correcciones de vulnerabilidades	3	3	18,00	ALTO	INACEPTABLE
Infracciones	Fotomultas	A6	Sistema Dinardap	No disponibilidad de Webservice	Información incorrecta de recuperación de propietarios , vechiculos y otras	CONTROL PREVENTIVO	Contratación de consultoria de ciberseguridad para evaluacion y aplicación de correcciones de vulnerabilidades	2	2	8,00	MEDIO	INACEPTABLE
Infracciones	Fotomultas	A7	Servidor de Aplicaciones	Hackeo	Falta de mantenimiento , no contar con personal capacitado	CONTROL PREVENTIVO	Contratación de consultoria de ciberseguridad para evaluacion y aplicación de correcciones de vulnerabilidades	2	3	12,00	ALTO	INACEPTABLE
Infracciones	Fotomultas	A8	Servidor de base de datos	Hackeo	Falta de mantenimiento , no contar con personal capacitado	CONTROL PREVENTIVO	Contratación de consultoria de ciberseguridad para evaluacion y aplicación de correcciones de vulnerabilidades	3	2	12,00	ALTO	INACEPTABLE
Infracciones	Fotomultas	A9	Seguridad Perimetral	Acceso no Permitidos	Equipos sin vida útil, renovación tecnólogica	CONTROL PREVENTIVO	Contratación de consultoria de ciberseguridad para evaluacion y aplicación de correcciones de vulnerabilidades	2	3	12,00	ALTO	INACEPTABLE
Infracciones	Fotomultas	A10	Enlaces comunicaciones puntos de control	Acceso no Permitidos	Accesos de contratación largas, caidas de procesos	CONTROL PREVENTIVO	Contratación de consultoria de ciberseguridad para evaluacion y aplicación de correcciones de vulnerabilidades	2	3	12,00	ALTO	INACEPTABLE
Infracciones	Fotomultas	A11	Enlaces comunicaciones data center	Acceso no Permitidos	Accesos de contratación largas, caidas de procesos	CONTROL PREVENTIVO	Contratación de consultoria de ciberseguridad para evaluacion y aplicación de correcciones de vulnerabilidades	3	3	18,00	ALTO	INACEPTABLE
Infracciones	Fotomultas	A12	Chip de comunicación de radares	Perdida de chips , no llevar control donde estan fisicamente instalados los chips	Accesos de contratación largas, caidas de procesos	CONTROL PREVENTIVO	Contratacion de nueva empresa para que entregue chip con politicas de seguridad	2	2	8,00	MEDIO	INACEPTABLE
Infracciones	Fotomultas	A13	Sistema SERT zona tarifaria	Hackeo	Fuga de información	CONTROL PREVENTIVO	Contratación de consultoria de ciberseguridad para evaluacion y aplicación de correcciones de vulnerabilidades	3	3	18,00	ALTO	INACEPTABLE
Infracciones	Fotomultas	A14	Personal que maneja sistema Fotomultas , SERT , Agentes Civiles de Tránisto	Personal no comprometido por sueldos bajos	Fuga de información	CONTROL PREVENTIVO	Homologación salarial de acuerdo a actividades y perfiles	2	3	12,00	ALTO	INACEPTABLE
Infracciones	Fotomultas	A15	Portal Institucional	Hackeo	Fuga de información	CONTROL PREVENTIVO	Contratación de consultoria de ciberseguridad para evaluacion y aplicación de correcciones de vulnerabilidades	3	3	18,00	ALTO	INACEPTABLE

Tabla 21 Análisis de riesgo (*Autoría Propia)*

Análisis de Riesgos						Implementación de Control			
Proceso Macro	Subprocesos	Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	Actividades	Fecha Inicio implementación	Fecha de verificación	Responsable
Infracciones	Fotomultas	A1	Camaras de Fotmultas	Manifestaciones , vandalismos	Desastres naturales	VPN de salida a la red de cámaras Actualizacion de Fireware con mejoras en seguridad	1/1/2025	31/12/2025	Infracciones
Infracciones	Fotomultas	A2	Hand Held	Dispositivos Dañados	Falta de mantenimientos	Renovación de equipos con tecnologia y seguridades de punta	1/1/2025	31/12/2025	TIC
Infracciones	Fotomultas	A3	Sistema Socrit Infracciones	Hackeo	Fuga de información	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	1/1/2025	31/12/2025	TIC
Infracciones	Fotomultas	A4	Sistema Axis Cloud	Hackeo	Fuga de información	Asegurar la Infraestructura perimetral Verificar pruebas ciberseguridad	1/1/2025	31/12/2025	Infracciones
Infracciones	Fotomultas	A5	Webservice ANT	No disponibilidad de Webservice	Información incorrecta de recuperación de propietarios y vechiculos	Webservice Seguros	1/1/2025	31/12/2025	TIC
Infracciones	Fotomultas	A6	Sistema Dinardap	No disponibilidad de Webservice	Información incorrecta de recuperación de propietarios , vechiculos y otras	Webservice Seguros	1/1/2025	31/12/2025	
Infracciones	Fotomultas	A7	Servidor de Aplicaciones	Hackeo	Falta de mantenimiento , no contar con personal capacitado	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	1/1/2025	31/12/2025	TIC
Infracciones	Fotomultas	A8	Servidor de base de datos	Hackeo	Falta de mantenimiento , no contar con personal capacitado	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	1/1/2025	31/12/2025	TIC
Infracciones	Fotomultas	A9	Seguridad Perimetral	Acceso no Permitidos	Equipos sin vida útil, renovación tecnólogica	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	1/1/2025	31/12/2025	TIC
Infracciones	Fotomultas	A10	Enlaces comunicaciones puntos de control	Acceso no Permitidos	Accesos de contratación largas, caidas de procesos	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	1/1/2025	31/12/2025	TIC
Infracciones	Fotomultas	A11	Enlaces comunicaciones data center	Acceso no Permitidos	Accesos de contratación largas, caidas de procesos	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	1/1/2025	31/12/2025	TIC
Infracciones	Fotomultas	A12	Chip de comunicación de radares	Perdida de chips , no llevar control donde estan fisicamente instalados los chips	Accesos de contratación largas, caidas de procesos	Bitacora de chip entregados a cámaras por periodo de funcionamiento. Testeo de funcionamiento de chip con ancho de banda. Protocolos y politicas de utilizacion para manejo de configuraciones	1/1/2025	31/12/2025	Infracciones
Infracciones	Fotomultas	A13	Sistema SERT zona tarifaria	Hackeo	Fuga de información	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	1/1/2025	31/12/2025	TIC
Infracciones	Fotomultas	A14	Personal que maneja sistema Fotomultas , SERT , Agentes Civiles de Tránisto	Personal no comprometido por sueldos bajos	Fuga de información	Se debe hacer una hopmologación salarial , verificando actividades y perfiles del puesto	1/1/2025	31/12/202	Infracciones
Infracciones	Fotomultas	A15	Portal Institucional	Hackeo	Fuga de información	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	1/1/2025	31/12/2025	TIC

Tabla 22 Análisis de riesgo (*Autoría Propia)*

PLAN DE TRATAMIENTO DE RIESGOS

ID riesgo	Tipo de Activo	Nivel del Riesgo	Opción de tratamiento	Controles a implementar EGSI V2	Descripción de actividades (acciones)	Responsable de implementación	Área funcional	Plazo de implementación		
								C/M/L	Fecha de inicio	Fecha de fin
R1	Camaras de Fotmultas	ALTO	REDUCIR	VPN de salida a la red de cámaras Actualizacion de Fireware con mejoras en seguridad	Contrato de adquisición de Cámaras y Contrato de Mantenimiento de Cámaras	Administrador del Contrato	Infracciones	M	1/1/2025	31/12/2025
R2	Hand Held	MEDIO	EVITAR	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	Elaboracion de TDR, INFORME ECONOCIMICO , INFORME DE NECESIDAD PUBLICACION SERCOP ADJUDICACION PARTE CONTRACTUAL EJECUCION DEL CONTRATO VERIFICACION DE ENTREGABLES PRUEBAS IMPLEMENTACION DE MEJORAS INFORME FINAL DEL CONTRATO	Administrador del Contrato Delegado de Direccion de Infracciones Delegados de areas funcionales	TIC	M	1/1/2025	31/12/2025
R3	Sistema Socrit Infracciones	ALTO	REDUCIR	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	Elaboracion de TDR, INFORME ECONOCIMICO , INFORME DE NECESIDAD PUBLICACION SERCOP ADJUDICACION PARTE CONTRACTUAL EJECUCION DEL CONTRATO VERIFICACION DE ENTREGABLES PRUEBAS IMPLEMENTACION DE MEJORAS INFORME FINAL DEL CONTRATO	Administrador del Contrato Delegado de Direccion de Infracciones Delegados de areas funcionales	TIC	M	1/1/2025	31/12/2025
R4	Sistema Axis Cloud	ALTO	REDUCIR	Asegurar la Infraestructura perimetral Verificar pruebas ciberseguridad	Contrato de mantenimiento Verificar pruebas en conjuntos para eliminar brechas de seguridad	Administrador del Contrato Delegado de Direccion de Infracciones Delegados de areas funcionales	Infracciones	M	1/1/2025	31/12/2025
R5	Webservice ANT	ALTO	EVITAR	Webservice Seguros	Convenio de interoperabilidad Pruebas de webservices seguros	Administrador del Convenio	TIC	M	1/1/2025	31/12/2025
R6	Sistema Dinardap	MEDIO	EVITAR	Webservice Seguros	Convenio de interoperabilidad Pruebas de webservices seguros	Administrador del Convenio		M	1/1/2025	31/12/2025
R7	Servidor de Aplicaciones	ALTO	REDUCIR	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	Elaboracion de TDR, INFORME ECONOCIMICO , INFORME DE NECESIDAD PUBLICACION SERCOP ADJUDICACION PARTE CONTRACTUAL EJECUCION DEL CONTRATO VERIFICACION DE ENTREGABLES PRUEBAS IMPLEMENTACION DE MEJORAS INFORME FINAL DEL CONTRATO	Administrador del Contrato Delegado de Direccion de Infracciones Delegados de areas funcionales	TIC	M	1/1/2025	31/12/2025

Tabla 23 Plan de Tratamiento de riesgo (*Autoría Propia)*

ID riesgo	Tipo de Activo	Nivel del Riesgo	Opción de tratamiento	Controles a implementar EGSI V2	Descripción de actividades (acciones)	Responsable de implementación	Área funcional	Plazo de implementación		
								C/M/L	Fecha de inicio	Fecha de fin
R8	Servidor de base de datos	ALTO	REDUCIR	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	Elaboracion de TDR, INFORME ECONOCIMICO , INFORME DE NECESIDAD PUBLICACION SERCOP ADJUDICACION PARTE CONTRACTUAL EJECUCION DEL CONTRATO VERIFICACION DE ENTREGABLES PRUEBAS IMPLEMENTACION DE MEJORAS INFORME FINAL DEL CONTRATO	Administrador del Contrato Delegado de Direccion de Infracciones Delegados de areas funcionales	TIC	M	1/1/2025	31/12/2025
R9	Seguridad Perimetral	ALTO	REDUCIR	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	Elaboracion de TDR, INFORME ECONOCIMICO , INFORME DE NECESIDAD PUBLICACION SERCOP ADJUDICACION PARTE CONTRACTUAL EJECUCION DEL CONTRATO VERIFICACION DE ENTREGABLES PRUEBAS IMPLEMENTACION DE MEJORAS INFORME FINAL DEL CONTRATO	Administrador del Contrato Delegado de Direccion de Infracciones Delegados de areas funcionales	TIC	M	1/1/2025	31/12/2025
R10	Enlaces comunicaciones puntos de control	ALTO	REDUCIR	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	Elaboracion de TDR, INFORME ECONOCIMICO , INFORME DE NECESIDAD PUBLICACION SERCOP ADJUDICACION PARTE CONTRACTUAL EJECUCION DEL CONTRATO VERIFICACION DE ENTREGABLES PRUEBAS IMPLEMENTACION DE MEJORAS INFORME FINAL DEL CONTRATO	Administrador del Contrato Delegado de Direccion de Infracciones Delegados de areas funcionales	TIC	M	1/1/2025	31/12/2025
R11	Enlaces comunicaciones data center	ALTO	REDUCIR	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	Elaboracion de TDR, INFORME ECONOCIMICO , INFORME DE NECESIDAD PUBLICACION SERCOP ADJUDICACION PARTE CONTRACTUAL EJECUCION DEL CONTRATO VERIFICACION DE ENTREGABLES PRUEBAS IMPLEMENTACION DE MEJORAS INFORME FINAL DEL CONTRATO	Administrador del Contrato Delegado de Direccion de Infracciones Delegados de areas funcionales	TIC	M	1/1/2025	31/12/2025
R12	Chip de comunicación de radares	MEDIO	EVITAR	Bitacora de chip entregados a cámaras por periodo de fiuncionamiento. Testeo de funcionamiento de chip con ancho de banda. Protocolos y politicas de utilizacion para manejo de configuraciones	Lineamiento de uso de chips en camaras de sistemas tecnológicos Desarrollo de sistema de bitacora de chips	TIC E Infracciones	Infracciones	M	1/1/2025	31/12/2025
R13	Sistema SERT zona tarifaria	MEDIO	REDUCIR	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	Elaboracion de TDR, INFORME ECONOCIMICO , INFORME DE NECESIDAD PUBLICACION SERCOP ADJUDICACION PARTE CONTRACTUAL EJECUCION DEL CONTRATO VERIFICACION DE ENTREGABLES PRUEBAS IMPLEMENTACION DE MEJORAS INFORME FINAL DEL CONTRATO	Administrador del Contrato Delegado de Direccion de Infracciones Delegados de areas funcionales	TIC	M	1/1/2025	31/12/2025
R14	Personal que maneja sistema Fotomultas , SERT , Agentes Civiles de Tránisto	ALTO	EVITAR	Se debe hacer una hopmologación salarial , verificando actividades y perfiles del puesto	Validación de FOTOMULTAL , SERT Auditoria de Infracciones Técnicos de Campo Administradores de Contrato	Direccion de Infracciones	Infracciones	L	1/1/2025	31/12/202
R15	Portal Institucional	ALTO	REDUCIR	Se esta contratando una consultoria de Ciberseguridad para medir todos los sistemas y seguridades de la AMT	Elaboracion de TDR, INFORME ECONOCIMICO , INFORME DE NECESIDAD PUBLICACION SERCOP ADJUDICACION PARTE CONTRACTUAL EJECUCION DEL CONTRATO VERIFICACION DE ENTREGABLES PRUEBAS IMPLEMENTACION DE MEJORAS INFORME FINAL DEL CONTRATO	Administrador del Contrato Delegado de Direccion de Infracciones Delegados de areas funcionales	TIC	M	1/1/2025	31/12/2025

Tabla 24 Plan de Tratamiento de riesgo (*Autoría Propia)*

4.3 Diseñar políticas de Seguridad de la Información que deben llevarse a cabo en la Dirección de Infracciones de la Agencia Metropolitana de Tránsito

4.3.1 Antecedentes

La Agencia Metropolitana de Tránsito reconoce la importancia fundamental de salvaguardar la confidencialidad, integridad y disponibilidad de la información relacionada con el tránsito y la Movilidad. Esta política establece las directrices y define las responsabilidades necesarias para garantizar la seguridad de la información, con un enfoque específico en la gestión de las infracciones de tránsito.

4.3.2 Políticas de la Dirección de Infracciones de la Agencia Metropolitana de Tránsito.

Para salvaguardar la información que se genera en los medios tecnológicos de la Dirección de Infracciones de la Agencia Metropolitana de Tránsito, se han diseñado las siguientes políticas de seguridad de información.

- Política de Seguridad de la Información

Esta política regula la gestión de la seguridad de la información dentro de la entidad, garantizando niveles adecuados de integridad, confidencialidad y disponibilidad en la Dirección de Infracciones de la Agencia Metropolitana de Tránsito. Para ello, todos los servidores y funcionarios de esta Dirección están obligados a aplicar y cumplir las disposiciones establecidas en la misma.

- Política de Gestión de usuarios y contraseñas:

Establece los parámetros para la gestión segura de cuentas de usuario y contraseñas del personal de la Dirección de Infracciones de la Agencia Metropolitana de Tránsito.

- Política de acceso a para captación de contravenciones de Tránsito por medios tecnológicos.

Realiza el proceso de gestión de captación y envío por enlaces de comunicación o red celular las contravenciones captadas por medios tecnológicos.

- Política de firma de convenios de confidencialidad de sistemas tecnológicos.

Establece la normativa para la firma de convenios de confidencialidad del personal de la Dirección de Infracciones de la Agencia Metropolitana de Tránsito de uso de sistemas, bases de datos e información sensible de manejo de la Dirección.

- Políticas de manejo de ftp para repositorio de fotografías de infracciones

Realiza el manejo del proceso de almacenamiento temporal de imágenes captadas por sistemas tecnológicos con sus seguridades y políticas de manejo para los sistemas de infracciones de tránsito.

4.3.3 Definición de Políticas.

- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

4.3.3.1 Introducción

La información constituye un activo fundamental para la Dirección de Infracciones de la Agencia Metropolitana de Tránsito, ya que es esencial para cumplir con los objetivos estratégicos y facilita la toma de decisiones por parte de las autoridades responsables de la gestión de los sistemas tecnológicos de tránsito. Por ello, resulta crucial establecer un marco que garantice la protección adecuada de la información en todas las etapas de su ciclo de vida: desde su captura, procesamiento y validación, hasta su notificación.

4.3.3.2 Antecedentes

La Dirección de Infracciones de la Agencia Metropolitana de Tránsito proporciona servicios tecnológicos a la ciudadanía, mediante los cuales se gestiona información confidencial relacionada con las infracciones registradas por sistemas tecnológicos debido al incumplimiento de la normativa legal vigente. Esta información debe ser manejada con estricta confidencialidad para prevenir su divulgación no autorizada.

El Esquema Gubernamental de Seguridad de la Información (EGSI) establece la obligatoriedad de implementar normas y procedimientos que garanticen la seguridad de la información, integrando de manera permanente su gestión en los procesos y la cultura institucional.

4.3.3.3 Justificación

El establecimiento de políticas es esencial para alcanzar los objetivos de la Dirección. Las políticas de seguridad de la información fortalecen la protección de los datos manejados en los servicios tecnológicos internos.

El Acuerdo Ministerial No. Mintel-Mintel-2024-0003, en su artículo 1, dispone la expedición del Esquema Gubernamental de Seguridad de la Información (EGSI), el cual se incluye como anexo al acuerdo y constituye el mecanismo para implementar el Sistema de Gestión de Seguridad de la Información (SGSI) en el sector público.

En cumplimiento de este esquema, las instituciones deberán realizar una evaluación de riesgos sobre sus activos de información críticos y diseñar un plan para el tratamiento de dichos riesgos. Este proceso se llevará a cabo utilizando como referencia la *Guía para la Gestión de Riesgos de Seguridad de la Información*.

.

4.3.3.4 Objetivo

Implementar una política de seguridad de la información en la Dirección de Infracciones de la Agencia Metropolitana de Tránsito con el objetivo de regular la gestión de la seguridad, garantizando niveles óptimos de confidencialidad, integridad y disponibilidad de la información relevante. Esta política busca además asegurar la continuidad de los procesos y servicios esenciales de la Dirección.

4.3.3.5 Alcance

Las políticas de seguridad de la información son aplicables a los servidores, contratistas, ciudadanos infractores que laboran en la Dirección, así como a todos los usuarios que gestionan los servicios tecnológicos proporcionados por la misma.

4.3.3.6 Políticas de seguridad de la información

La información generada o almacenada en medios de la Dirección es de propiedad de la Agencia Metropolitana de Tránsito y deberán ser exclusivamente utilizadas para las tareas propias de la función a desarrollarse.

- Para el manejo de la información de la Dirección debe tener relación laboral con la AMT, o contar con la autorización escrita de un funcionario Directivo.
- Los/las servidores/as, funcionarios/as cualquier persona de tenga relación con la AMT y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información deben seguir lineamientos y en los

documentos relacionados con el fin de mantener la confidencialidad, integridad y asegurar la disponibilidad de la información

4.3.3.7 Roles y Responsabilidades

La máxima autoridad a través del Comité de Seguridad de la Información (CSI - equipo directivo) es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la institución.

Cada funcionario directivo, es responsable de garantizar que los funcionarios que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la institución.

El Oficial de Seguridad de la Información (OSI) asesora al equipo directivo, proporciona apoyo especializado al personal de la institución y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.

Cada uno de los funcionarios de la institución tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

4.3.3.8 Alcance y usuarios

Esta Política se aplica a todo lo que contempla el Esquema Gubernamental de Seguridad de la Información (EGSI), según se define en el documento del Alcance del EGSI.

Los usuarios de este documento son todos los funcionarios de Dirección de Infracciones de la Agencia Metropolitana de Tránsito como también terceros externos a la institución como son contratistas o ciudadanos infractores.

4.3.3.9 Comunicación de la Política

Se comunicará la Política de Seguridad de la Información a todos los servidores de la institución, mediante página web institucional y procedimientos internos de notificación de máxima autoridad de la Institución y a través de: correo electrónico.

4.3.3.10 Excepciones y sanciones

Incumplimiento de esta política será puesto en conocimiento de Asuntos Internos para que sea aplicado el régimen sancionatorio de acuerdo a reglamento interno de la Institución

4.3.4 Definición de Políticas.

- POLÍTICA DE FIRMA DE CONVENIOS DE CONFIDENCIALIDAD DE SISTEMAS TECNOLÓGICOS.

4.3.4.1 Introducción

La información es un activo esencial para la Dirección de Infracciones de la Agencia Metropolitana de Tránsito, ya que facilita la toma de decisiones por parte de las autoridades encargadas de gestionar los servicios de los sistemas tecnológicos de tránsito, contribuyendo al cumplimiento de los objetivos estratégicos. Por lo tanto, es crucial establecer un marco que garantice la protección adecuada de la información en todas sus fases: captura, procesamiento, validación y notificación. Para ello, se deberán firmar convenios de confidencialidad que resguarden la seguridad de los sistemas tecnológicos utilizados.

4.3.4.2 Antecedentes

La Dirección de Infracciones de la Agencia Metropolitana de Tránsito ofrece servicios tecnológicos a los ciudadanos, a través de los cuales se gestiona información confidencial relacionada con las infracciones cometidas por incumplimiento de la normativa legal vigente. Esta información debe ser manejada con estricta confidencialidad para evitar su divulgación no autorizada.

El Esquema Gubernamental de Seguridad de la Información (EGSI) establece la necesidad de aplicar normas y procedimientos para garantizar la seguridad de la información, así como integrar su gestión continua en la cultura y los procesos institucionales.

Por ello, es fundamental proteger los datos mediante convenios de confidencialidad que deben ser firmados por funcionarios y contratistas, asegurando que la información se maneje con el máximo nivel de sigilo.

4.3.4.3 Justificación

El establecimiento de políticas es esencial para alcanzar los objetivos de la Dirección. Las políticas de seguridad de la información fortalecerán la protección de los datos manejados en los servicios tecnológicos internos.

El Acuerdo Ministerial No. Mintel-Mintel-2024-0003, en su artículo 1, dispone la expedición del Esquema Gubernamental de Seguridad de la Información (EGSI), que se incluye como anexo al acuerdo. Este esquema es el mecanismo para implementar el Sistema de Gestión de Seguridad de la Información en el sector público. En este contexto, se realizará una evaluación de riesgos sobre los activos de información críticos y se diseñará un plan para el tratamiento de los riesgos en la institución, utilizando como referencia la *Guía para la Gestión de Riesgos de Seguridad de la Información*.

4.3.4.4 Objetivo

Establecer la política de seguridad de la información en la Dirección de Infracciones de la Agencia Metropolitana de Tránsito con el objetivo de regular la gestión de la seguridad de la información, garantizando niveles óptimos de integridad, confidencialidad y disponibilidad para toda la información relevante de la Dirección, y asegurando la continuidad de los procesos y servicios.

4.3.4.5 Alcance

Las políticas de seguridad de la información aplican a los/las servidores/as, contratistas y ciudadanos infractores que labora en la Dirección y a los usuarios que utilizan servicios tecnológicos provistos por la misma.

4.3.4.6 Políticas de seguridad de la información

La información generada o almacenada en medios de la Dirección es de propiedad de la Agencia Metropolitana de Tránsito y deben ser utilizadas exclusivamente para las tareas propias de la función desarrollada

•Para el manejo de la información de la Dirección debe tener relación laboral con la AMT, o contar con la autorización escrita de un funcionario Directivo.

• Los/las servidores/as, funcionarios/as cualquier persona de tenga relación con la AMT y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información deben seguir lineamientos y en los documentos

relacionados con el fin de mantener la confidencialidad, integridad y asegurar la disponibilidad de la información

4.3.4.7 Roles y Responsabilidades

La máxima autoridad a través del Comité de Seguridad de la Información (CSI - equipo directivo) es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la institución.

Cada funcionario directivo, es responsable de garantizar que los funcionarios que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la institución.

El Oficial de Seguridad de la Información (OSI) asesora al equipo directivo, proporciona apoyo especializado al personal de la institución y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.

Cada uno de los funcionarios de la institución tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

4.3.4.8 Alcance y usuarios

Esta Política se aplica a todo lo que contempla el Esquema Gubernamental de Seguridad de la Información (EGSI), según se define en el documento del Alcance del EGSI.

Los usuarios de este documento son todos los funcionarios de Dirección de Infracciones de la Agencia Metropolitana de Tránsito como también terceros externos a la institución como son contratistas o ciudadanos infractores.

4.3.4.9 Comunicación de la Política

Se comunicará la Política de Seguridad de la Información a todos los servidores de la institución, mediante página web institucional y procedimientos internos de notificación de máxima autoridad de la Institución y a través de: correo electrónico.

4.3.4.10 Excepciones y sanciones

Incumplimiento de esta política será puesto en conocimiento de Asuntos Internos para que sea aplicado el régimen sancionatorio de acuerdo a reglamento interno de la Institución

4.3.5 Documentos de referencia

- Acuerdo Nro. Mintel-Mintel-2024-0003
- Acuerdo Ministerial 025-2019
- Esquema Gubernamental de Seguridad de la Información (EGSI v2.0)
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001
- Alcance del Esquema Gubernamental de Seguridad de la Información
- Plan estratégico institucional
- Lineamientos de políticas estratégicas
- Normativa referente al tránsito y seguridad vial (COIP)
- Ordenanzas Metropolitanas referente al Tránsito y Seguridad Vial
- Ley de Tránsito
- Constitución de la República

4.4 Evaluación del sistema de gestión de seguridad de la información (SGSI) contra las vulnerabilidades detectadas.

Para evaluar el Sistema de Gestión de Seguridad de la Información (SGSI) frente a las vulnerabilidades detectadas, se utilizará la metodología Delphi, que se basa en juicios de expertos. Esta metodología implica la revisión y valoración del sistema por parte de dos especialistas en seguridad de la información, con experiencia en el control de tránsito y la seguridad vial.

El proceso se llevará a cabo en varias etapas que incluirán la evaluación de políticas, procedimientos, controles y prácticas implementadas para proteger la información. A continuación, se detallan los pasos clave y las consideraciones para realizar el juicio de expertos, en el cual se asignarán puntuaciones para evaluar el cumplimiento, describiendo los criterios y los pesos correspondientes a cada puntuación.

CALIFICACIÓN EXPERTO	CRITERIOS DE EVALUACION			
DEFICIENTE	**5**	**10**	**15**	**20**
BAJO	**25**	**30**	**35**	**40**
REGULAR	**45**	**50**	**55**	**60**
BUENO	**65**	**70**	**75**	**80**
MUY BUENO	**85**	**90**	**95**	**100**

Tabla 25 Criterios de Evaluación para Juicio de expertos (*Autoría Propia)*

Los expertos podrán evaluar los contenidos de la investigación según los parámetros establecidos. Posteriormente, cada profesional asignará una calificación, la cual será cuantificada para determinar la calificación final del proyecto verificado, tal como se muestra en la tabla a continuación:

CALIFICACION FINAL TESIS	CUMPLIMIENTO
EXCELENTE	90-100 %
MUY BUENA	75-89 %
BUENA	50-74 %
REGULAR	0-49 %

Tabla 26 Calificación para Juicio de expertos (*Autoría Propia)*

4.4.1. Informe sobre la aplicación del Juicio de Expertos en el caso de estudio.

En este apartado se hace referencia al grupo de expertos que colaboraron en la revisión del proyecto, presentando sus principales credenciales. Estos expertos han sido responsables de la identificación y evaluación del proyecto, así como de la asignación de las calificaciones correspondientes.

No.	Nombre y Apellido	Profesión	Especializacion /Conocimiento SI	Cargo	Ubicación
1	Carlos Alberto Tituaña Anaguano	Ingeniero en Sistemas e Informática	Consultor en temas de Seguridad Informática	Responsable de Redes	Quito -Ecuador
2	LOZANO GUADALUPE FERNANDO	Ing Sistemas	Magister en Sistemas de Información	Gerente Técnico /Consultor TI	Quito -Ecuador
3	GUALOTO COYAGO LUIS ENRIQUE	Ing Sistemas	Consultor en temas Transito y Transporte	Supervisor Infracciones AMT	Quito -Ecuador

Tabla 27 Expertos (*Autoría Propia)*

En la tabla presentada, se registran los expertos que expresaron su opinión y perspectiva sobre la coherencia y correspondencia del proyecto diseñado en relación con el Acuerdo Nro. Mintel-Mintel-2024-0003, que hace referencia a la metodología EGSI para su aplicación en empresas públicas. En este contexto, los expertos evaluaron el grado de alineación del proyecto con los requisitos establecidos por dicho acuerdo. Para llevar a cabo esta evaluación, fue necesario contactar a los expertos de manera presencial en la fecha indicada, proporcionarles un resumen del modelo del proyecto y su funcionamiento, y luego proceder a evaluar los puntos descritos en el informe del experto

4.4.2 Tabulación de resultados

Los resultados obtenidos fueron registrados y tabulados para su posterior análisis, y su registro se presenta en la siguiente tabla:

No. Experto	Fecha de Evaluación	Valoración Experto	Observaciones
1	27-dic-24	96,92	Se felicita por el Análisis Realizado para aportar a la academia en temas de aplicación SGSI
2	27-dic-24	96,54	Se debe socializar con otros GAD para que conozcan metodologias actuales de seguridad de la información
3	27-dic-24	88,85	Se debe aplicar estas tecnologías para que la Direcciíon de Infracciones precautele sus activos sencibles de manejo que se tiene
	Modelo Calificado:	**94,10**	**EXCELENTE**

Tabla 28 Resultados Juicio de expertos (*Autoría Propia)*

Se indica el detalle del análisis realizado por los expertos en base a los objetivos y contenido del caso de estudio, y a continuación se tabula la evaluación:

VALOR DE CONTENIDO EXPERTO 1

		DEFICIENTE				BAJO				REGULAR				BUENO				MUY BUENO					
OBJETIVO	CONTENIDO	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100		
Claridad	Lenguaje apropiado																		X				
Objetividad	Es Preciso																			X			
Actualización	Vigencia																			X			
Organización	Tiene Lógica																			X			
Suficiencia	Es Integral																			X			
Intencionalidad	Es Adecuado																				X		
Consistencia	Tiene base teórica																				X		
Coherencia	Hay Pertinencia																				X		
Metodologia	Tiene sentido																			X			
Pernitencia	Es Aplicable																			X			
Objetivo 1	Cumple Requerimientos																				X		
Objetivo 2	Cumple Requerimientos																				X		
Objetivo 3	Cumple Requerimientos																				X		CALIFICACION
		RESULTADOS																	90	570	600		96,92

Tabla 29 Evaluación experto 1 (*Autoría Propia)*

VALOR DE CONTENIDO EXPERTO 2

OBJETIVO	CONTENIDO	DEFICIENTE				BAJO				REGULAR				BUENO				MUY BUENO					
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100		
Claridad	Lenguaje apropiado																			X			
Objetividad	Es Preciso																			X			
Actualización	Vigencia																			X			
Organización	Tiene Lógica																			X			
Suficiencia	Es Integral																		X				
Intencionalidad	Es Adecuado																			X			
Consistencia	Tiene base teórica																				X		
Coherencia	Hay Pertinencia																				X		
Metodologia	Tiene sentido																				X		
Pernitencia	Es Aplicable																			X			
Objetivo 1	Cumple Requerimientos																				X		
Objetivo 2	Cumple Requerimientos																			X			
Objetivo 3	Cumple Requerimientos																				X		CALIFICACION
		RESULTADOS																	90	665	500		96,54

Tabla 30 Evaluación experto 2 (*Autoría Propia)*

VALOR DE CONTENIDO EXPERTO 3

		DEFICIENTE				BAJO				REGULAR				BUENO				MUY BUENO					
OBJETIVO	CONTENIDO	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100		
Claridad	Lenguaje apropiado																				X		
Objetividad	Es Preciso																	X					
Actualización	Vigencia																			X			
Organización	Tiene Lógica																		X				
Suficiencia	Es Integral																			X			
Intencionalidad	Es Adecuado																				X		
Consistencia	Tiene base teórica																			X			
Coherencia	Hay Pertinencia																				X		
Metodologia	Tiene sentido																				X		
Pernitencia	Es Aplicable																		X				
Objetivo 1	Cumple Requerimientos																			X			
Objetivo 2	Cumple Requerimientos																			X			
Objetivo 3	Cumple Requerimientos																				X		CALIFICACION
		RESULTADOS																85	180	475	500	1155	88,85

Tabla 31 Evaluación experto 3 (*Autoría Propia)*

4.4.3. Análisis de resultados de acuerdo al Juicio de Expertos y conclusión respecto a la hipótesis de trabajo

De acuerdo a los resultados obtenidos en la aplicación del juicio de expertos, se puede señalar que el modelo presenta una excelente concordancia, con objetivos claros y resultados consistentes. Se considera procedente su implementación y puesta en marcha en la Agencia Metropolitana de Tránsito, específicamente en la Dirección de Infracciones, para la gestión de la seguridad de la información (SGSI) utilizando la metodología EGSI.

De acuerdo a la hipótesis de trabajo planteada, se confirma que la gestión de seguridad de la Información (SGSI) con una metodología EGSI permitirá a la Dirección de Infracciones de la Agencia Metropolitana de Tránsito establecer mecanismos de protección de datos de forma efectiva dentro de un marco normativo definido por los entes competentes.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

La investigación realizada permitió identificar todos los activos de información de la Dirección de Infracciones de la Agencia Metropolitana de Tránsito, los cuales son esenciales para la aplicación de la metodología EGSI, establecida en el acuerdo Nro. Mintel-Mintel-2024-0003 para instituciones públicas.

Se diseñó un conjunto de procedimientos para identificar los riesgos, así como actividades de mitigación, en conformidad con la metodología EGSI.

Se elaboraron políticas de seguridad de la información específicas para su implementación en la Dirección de Infracciones de la Agencia Metropolitana de Tránsito, con el objetivo de mejorar la integridad, confidencialidad y disponibilidad de la información.

Al aplicar la Técnica Delphi, se pudo evaluar el sistema de gestión de seguridad de la información (SGSI) contra las vulnerabilidades detectadas. De los resultados obtenidos se advierte que la gestión de seguridad de la información (SGSI) mediante la metodología EGSI permitirá a la Dirección de Infracciones de la Agencia Metropolitana de Tránsito establecer mecanismos efectivos de protección de datos, dentro de un marco normativo definido por los entes competentes.

5.2. Recomendaciones

Es necesario socializar el proyecto en la Dirección General de la Agencia Metropolitana de Tránsito, para que la máxima autoridad de la institución disponga la implementación y puesta en marcha de lo establecido en la metodología EGSI.

El Departamento de TIC de la Agencia Metropolitana de Tránsito debe aplicar las políticas de seguridad y los tratamientos de riesgos, con el fin de mejorar la seguridad de la información en la institución.

La Dirección de Infracciones de la Agencia Metropolitana de Tránsito debe considerar la aplicación del proyecto diseñado para reducir los riesgos identificados en cuanto a la seguridad de la información.

Se debe promover la socialización con otros GAD, para que puedan incorporar mejoras en sus procesos de gestión de infracciones de tránsito, posicionando a la Agencia Metropolitana de Tránsito como un modelo y referente en la implementación de Sistemas de Gestión de Seguridad de la Información.

REFERENCIAS

De Datos, P. (2019, 20 enero). ISO 27001 - Sistema de gestión de seguridad de la información (SGSI) - Proteccion de datos. Proteccion de Datos. https://www.protecciondatos.org/iso-27001-sistema-de-gestion-de-seguridad-de-la-informacion-sgsi/

Pazán, C. (2023, 7 diciembre). Cuenca: Infracciones de tránsito en el ojo público tras denuncias de corrupción. www.expreso.ec. https://www.expreso.ec/actualidad/cuenca-infracciones-Tránsito-ojo-publico-denuncias-corrupcion-181780.html

Pirani. (s. f.). Guía para hacer una Política de Seguridad de la Información. https://www.piranirisk.com/es/academia/especiales/guia-politica-de-seguridad-de-la-informacion

RIESGOS DE SEGURIDAD DE LA INFORMACIÓN GUÍA PARA LA GESTIÓN DE. (2020).QUITO. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Problems of Implementing Information Security Management Systems. (2020b, septiembre 7). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9322896

Implementation of the Risk-based Approach Methodology in Information Security Management Systems. (2021b, septiembre 6). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9642767

Information Security Risk Management. (2020, 7 septiembre). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9322901

Research on the Application of Computer Big Data Technology in Information Security Management. (2023, 24 febrero). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10090574

Research on Design Model of Enterprise Safety Risk Monitoring System Based on Information Technology. (2023, 1 abril). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10158200

De, L. 0. R. O. S. 459. (s/f). LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES. Gob.ec. Recuperado el 9 de marzo de 2024, de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Disponibilidad – Seguridad informática. (s. f.). Seguridad Informática. https://infosegur.wordpress.com/tag/disponibilidad/ de La Información, R. D. E. S. (s/f). GUÍA PARA LA. Gob.ec. Recuperado el 12 de marzo de 2024, de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Gobierno Electrónico de Ecuador. (2020). Guía para la gestión de riesgos de seguridad de la información. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

de DocuSign, C. (2023, agosto 17). La importancia de las políticas de seguridad informática en el entorno empresarial. DocuSign. https://www.docusign.com/es-mx/blog/politicas-de-seguridad-informatica

(S/f). Com.ec. Recuperado el 14 de marzo de 2024, de https://strapi.lexis.com.ec/uploads/3_SRO_509_20240301_bb51b6331d.pdf

Vera, S. (2024, 16 marzo). Guías y formatos (EGSI). Gobierno Electrónico de Ecuador. https://www.gobiernoelectronico.gob.ec/guias-y-formatos-egsi/

(S/f). Gob.ec. Recuperado el 15 de julio de 2024, de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2024/03/Registro-Oficial-Acuerdo-Ministerial-No.-0003-2024-EGSI-version-3.0.pdf

Admin. (2024, 7 junio). Seguridad de hardware, redes informáticas y software. Ci2.es. https://www.ci2.es/seguridad-informatica-en-redes-software-y-hardware/

Seguridad de datos: En qué consiste y qué es importante en tu empresa. (s. f.). https://www.powerdata.es/seguridad-de-datos

(S/f). Gob.ec. Recuperado el 23 de junio de 2024, de https://www.ant.gob.ec/la-ant-informa-sobre-ataque-cibernetico-a-sus-sistemas/

De, D. L. 0. R. O. 449. (s/f). CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. Gob.ec. Recuperado el 15 de julio de 2024, de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

(S/f-b). Gob.ec. Recuperado el 15 de julio de 2024, de https://www.amt.gob.ec/index.php/informacion/normativa-legal-vigente/

Livshitz, I. I., Lontsikh, P. A., Golovina, E. Y., Kunakov, E. P., & Kozhukhova, V. V. (2020). Security assessment process of IT-components for cloud infrastructure. *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 110–113.

Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6.

Putra, D. S. K., Tistiyani, S., & Sunaringtyas, S. U. (2021). The use of ISO/IEC 27001 family of standards in regulatory requirements in some countries. *2021 2nd International Conference on ICT for Rural Development (IC-ICTRuDev)*, 1–6.

Chaiwut, N., & Rueangsirarak, W. (2022). An online gap analysis on cyber security principles for Thailand organizations based on ISO/IEC 27001:2013 standard. *2022 6th International Conference on Information Technology (InCIT)*, 479–484.

Aleksandrov, M. N., Vasiliev, V. A., & Aleksandrova, S. V. (2021). Implementation of the risk-based approach methodology in information security management systems. *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 137–139.

Livshitz, I. I., Lontsikh, P. A., Golovina, E. Y., Kunakov, E. P., & Kozhukhova, V. V. (2020). Security assessment process of IT-components for cloud infrastructure. *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 110–113.

Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6.

Edwards, J., & Weaver, G. (2024). Cybersecurity frameworks. En *The Cybersecurity Guide to Governance, Risk, and Compliance* (pp. 209–229). Wiley. https://doi.org/10.1002/9781394250226.ch12

Djebbar, F., & Nordström, K. (2023). A comparative analysis of industrial cybersecurity standards. *IEEE access: practical innovations, open solutions*, *11*, 85315–85332. https://doi.org/10.1109/access.2023.3303205

Guo, H., Wei, M., Huang, P., & Chekole, E. G. (2021). Enhance enterprise security through implementing ISO/IEC 27001 standard. *2021 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 1–6.

Tecnetone. (n.d.). NIST SP 800-53: Controles de seguridad NIST. Tecnetone. https://blog.tecnetone.com/nist-sp-800-53-controles-de-seguridad-nist

PMG SSI. (2015, abril). *ISO 27001: Amenazas y vulnerabilidades*. https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

4Matt Technology. (n.d.). *COBIT 2019: Construir, adquirir e implementar (BAI)*. https://4matt.com.br/es-mx/cobit-2019-construir-adquirir-e-implementar-bai/

Fernandes, V. (2022, June 29). COBIT 2019: Construir, adquirir e implementar (BAI). 4Matt Tecnologia. https://4matt.com.br/es-mx/cobit-2019-construir-adquirir-e-implementar-bai/

Toro, R. (2015, abril 6). ISO 27001: Amenazas y vulnerabilidades. PMG SSI - ISO 27001. https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

Santander Open Academy. (n.d.). Cualitativa y cuantitativa. Santander Open Academy. Retrieved September 21, 2024, from https://www.santanderopenacademy.com/es/blog/cualitativa-y-cuantitativa.html

Bernardino, D. (2024). Investigación explicativa: Entendiendo los fenómenos en profundidad. QuestionPro. Retrieved September 21, 2024, from https://www.questionpro.com/blog/es/investigacion-explicativa/

Parra, A. (n.d.). Características de la investigación documental. QuestionPro. Retrieved September 21, 2024, from https://www.questionpro.com/blog/es/investigacion-documental/

QuestionPro. (2023, August 16). ¿Qué es la investigación de campo? Características y ejemp

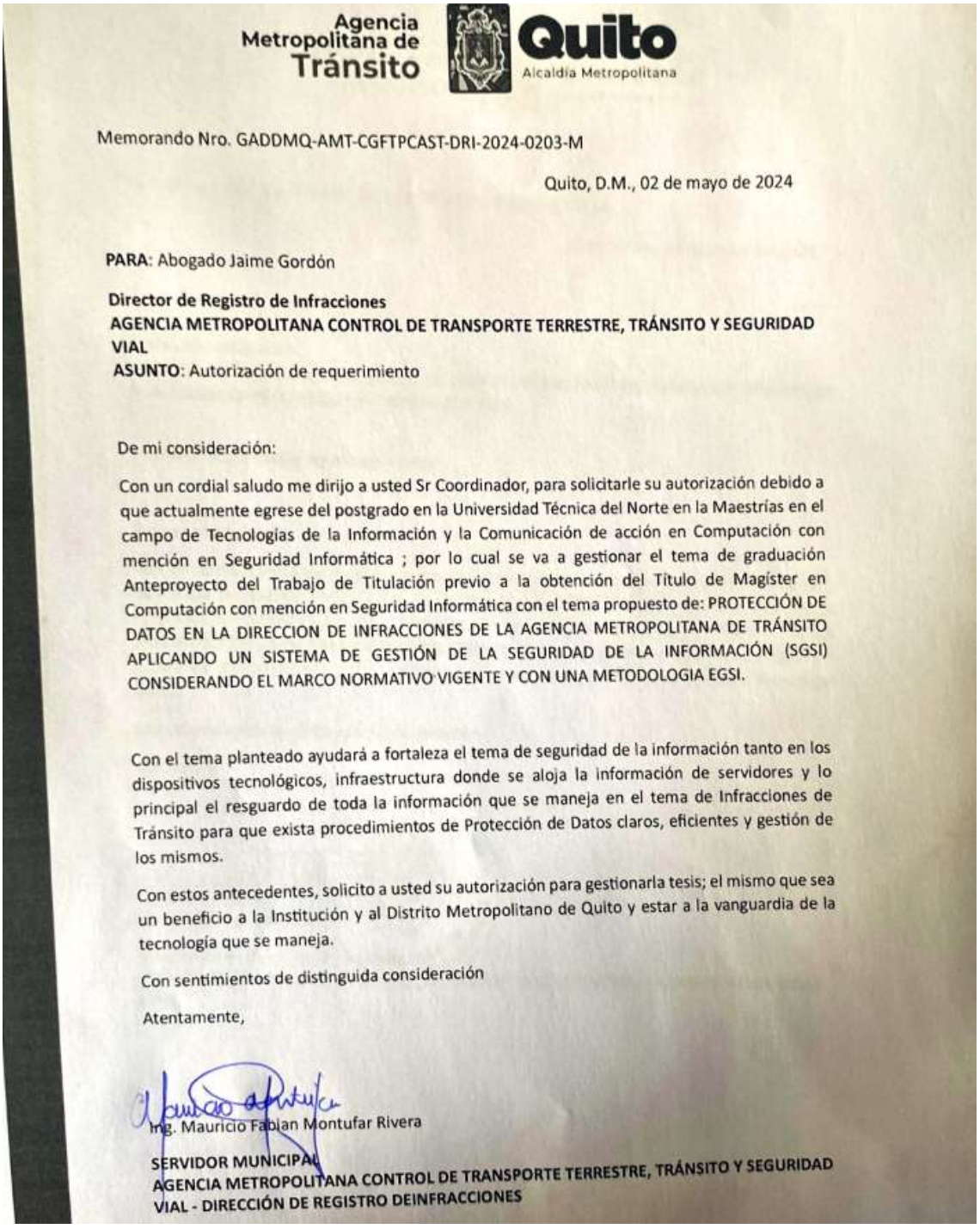
los. QuestionPro. https://www.questionpro.com/es/investigacion-de-campo.html

QuestionPro. (2023, September 13). Investigación aplicada: Qué es, características y ejemplos. https://www.questionpro.com/blog/es/investigacion-aplicada/

Rae, B. (2023, December 4). ¿Qué es un grupo de estudio?. Doodle. https://doodle.com/es/study-group/

ANEXOS

ANEXO I. Solicitud para realizar tesis de grado.



Agencia Metropolitana de Tránsito

Quito Alcaldía Metropolitana

Memorando Nro. GADDMQ-AMT-CGFTPCAST-DRI-2024-0203-M

Quito, D.M., 02 de mayo de 2024

PARA: Abogado Jaime Gordón

Director de Registro de Infracciones
AGENCIA METROPOLITANA CONTROL DE TRANSPORTE TERRESTRE, TRÁNSITO Y SEGURIDAD VIAL
ASUNTO: Autorización de requerimiento

De mi consideración:

Con un cordial saludo me dirijo a usted Sr Coordinador, para solicitarle su autorización debido a que actualmente egrese del postgrado en la Universidad Técnica del Norte en la Maestrías en el campo de Tecnologías de la Información y la Comunicación de acción en Computación con mención en Seguridad Informática ; por lo cual se va a gestionar el tema de graduación Anteproyecto del Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con mención en Seguridad Informática con el tema propuesto de: PROTECCIÓN DE DATOS EN LA DIRECCION DE INFRACCIONES DE LA AGENCIA METROPOLITANA DE TRÁNSITO APLICANDO UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) CONSIDERANDO EL MARCO NORMATIVO VIGENTE Y CON UNA METODOLOGIA EGSI.

Con el tema planteado ayudará a fortaleza el tema de seguridad de la información tanto en los dispositivos tecnológicos, infraestructura donde se aloja la información de servidores y lo principal el resguardo de toda la información que se maneja en el tema de Infracciones de Tránsito para que exista procedimientos de Protección de Datos claros, eficientes y gestión de los mismos.

Con estos antecedentes, solicito a usted su autorización para gestionarla tesis; el mismo que sea un beneficio a la Institución y al Distrito Metropolitano de Quito y estar a la vanguardia de la tecnología que se maneja.

Con sentimientos de distinguida consideración

Atentamente,

Ing. Mauricio Fabian Montufar Rivera

SERVIDOR MUNICIPAL
AGENCIA METROPOLITANA CONTROL DE TRANSPORTE TERRESTRE, TRÁNSITO Y SEGURIDAD VIAL - DIRECCIÓN DE REGISTRO DEINFRACCIONES

Agencia Metropolitana de Tránsito

Quito Alcaldía Metropolitana

Memorando Nro. GADDMQ-AMT-CGFTPCAST-DRI-2024-0303-M

Quito, D.M., 09 de mayo de 2024

PARA: Ing. Mauricio Fabian Montufar Rivera

SERVIDOR MUNICIPAL
AGENCIA METROPOLITANA CONTROL DE TRANSPORTE TERRESTRE, TRÁNSITO Y SEGURIDAD VIAL - DIRECCIÓN DE REGISTRO DEINFRACCIONES

ASUNTO: Autorización de requerimiento

De mi consideración:

Con un cordial saludo me dirijo a usted para su respectiva autorización en la gestión de su tesis con tema propuesto: PROTECCIÓN DE DATOS EN LA DIRECCION DE INFRACCIONES DE LA AGENCIA METROPOLITANA DE TRÁNSITO APLICANDO UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) CONSIDERANDO EL MARCO NORMATIVO VIGENTE Y CON UNA METODOLOGIA EGSI ; el mismo que cursa su posgrado en la Universidad Técnica del Norte.

Con sentimientos de distinguida consideración

Atentamente,

AGENCIA METROPOLITANA DE TRÁNSITO AMT TRÁNSITO DIRECCIÓN DE REGISTRO DE INFRACCIONES

Abogado Jaime Gordón

Director de Registro de Infracciones
AGENCIA METROPOLITANA CONTROL DE TRANSPORTE TERRESTRE, TRÁNSITO Y SEGURIDAD VIAL

ANEXO II. CONSTANCIA DE JUICIO DE EXPERTOS.

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Carlos Alberto Tituaña Anaguano

ESPECIALIDAD: Ingeniero en Sistemas e Informática

CEDULA DE IDENTIDAD: 1500594096

Por medio del presente, informo que realice la evaluación de la tesis con tema de "PROTECCIÓN DE DATOS EN LA DIRECCION DE INFRACCIONES DE LA AGENCIA METROPOLITANA DE TRÁNSITO APLICANDO UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) CONSIDERANDO EL MARCO NORMATIVO VIGENTE Y CON UNA METODOLOGIA EGSI"; elaborado por el Ing. Mauricio Fabián Montúfar Rivera que cursó estudios de Maestría en el campo de Tecnologías de la Información y la Comunicación para obtención del Título de Magíster en Computación con mención en Seguridad Informática en la Universidad Técnica del Norte.

Se indica, que el modelo presenta una EXCELENTE concordancia, objetivos claros y resultados consistentes; considerándose procedente su implementación y puesta en marcha en la Agencia Metropolitana de Tránsito en la Dirección de Infracciones en estudio de la gestión de seguridad de la Información (SGSI) con una metodología EGSI la cual permitirá a la Dirección de Infracciones de la Agencia Metropolitana de Tránsito establecer mecanismos de protección de datos de forma efectiva dentro de un marco normativo definido por los entes competentes.

Quito, 27 días de diciembre de 2024

CARLOS ALBERTO TITUAÑA ANAGUANO

CI: 1500594096

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: LOZANO GUADALUPE FERNANDO

ESPECIALIDAD: Magister en Sistemas de Información

CEDULA DE IDENTIDAD: 1710554914

Por medio del presente, informo que realice la evaluación de la tesis con tema de " PROTECCIÓN DE DATOS EN LA DIRECCION DE INFRACCIONES DE LA AGENCIA METROPOLITANA DE TRÁNSITO APLICANDO UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) CONSIDERANDO EL MARCO NORMATIVO VIGENTE Y CON UNA METODOLOGIA EGSI"; elaborado por el Ing. Mauricio Fabián Montúfar Rivera que cursó estudios de Maestría en el campo de Tecnologías de la Información y la Comunicación para obtención del Título de Magíster en Computación con mención en Seguridad Informática en la Universidad Técnica del Norte.

Se indica, que el modelo presenta una EXCELENTE concordancia, objetivos claros y resultados consistentes; considerándose procedente su implementación y puesta en marcha en la Agencia Metropolitana de Tránsito en la Dirección de Infracciones en estudio de la gestión de seguridad de la Información (SGSI) con una metodología EGSI la cual permitirá a la Dirección de Infracciones de la Agencia Metropolitana de Tránsito establecer mecanismos de protección de datos de forma efectiva dentro de un marco normativo definido por los entes competentes.

Quito, 27 días de diciembre de 2024

LOZANO GUADALUPE FERNANDO

CI: 1710554914

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: GUALOTO COYAGO LUIS ENRIQUE

ESPECIALIDAD: Ingeniero de Sistemas e Informática

CEDULA DE IDENTIDAD: 1716275209

Por medio del presente, informo que realice la evaluación de la tesis con tema de " PROTECCIÓN DE DATOS EN LA DIRECCION DE INFRACCIONES DE LA AGENCIA METROPOLITANA DE TRÁNSITO APLICANDO UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) CONSIDERANDO EL MARCO NORMATIVO VIGENTE Y CON UNA METODOLOGIA EGSI"; elaborado por el Ing. Mauricio Fabián Montúfar Rivera que cursó estudios de Maestría en el campo de Tecnologías de la Información y la Comunicación para obtención del Título de Magíster en Computación con mención en Seguridad Informática en la Universidad Técnica del Norte.

Se indica, que el modelo presenta una EXCELENTE concordancia, objetivos claros y resultados consistentes; considerándose procedente su implementación y puesta en marcha en la Agencia Metropolitana de Tránsito en la Dirección de Infracciones en estudio de la gestión de seguridad de la Información (SGSI) con una metodología EGSI la cual permitirá a la Dirección de Infracciones de la Agencia Metropolitana de Tránsito establecer mecanismos de protección de datos de forma efectiva dentro de un marco normativo definido por los entes competentes.

Quito, 27 días de diciembre de 2024

GUALOTO COYAGO LUIS ENRIQUE

CI: 1716275209