VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

TÍTULO DEL PROYECTO:

PLAN DE SEGURIDAD BASADO EN LA NORMA ISO 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LA TRONCAL PROVINCIA DEL CAÑAR

AUTOR

ING. MARJORIE TOPACIO DUMAGUALA LEÓN

TUTOR

ING. EDGAR MORALES, MSC

MILAGRO, Marzo 2023

ECUADOR

ACEPTACIÓN DEL(A) TUTOR(A)

Por la presente hago constar que he analizado el proyecto de investigación con el tema **PLAN DE SEGURIDAD BASADO EN LA NORMA ISO 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LA TRONCAL, PROVINCIA DEL CAÑAR**, presentado por la **ING. MARJORIE TOPACIO DUMAGUALA LEÓN**, para optar por el título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN** y que acepto tutoriar a la maestrante, durante la etapa del desarrollo del trabajo hasta su presentación, evaluación y sustentación.

Milagro, a los 12 días del mes de septiembre del 2022

EDGAR ROLANDO
MORALES CALUNA

ING. EDGAR MORALES, MSC

C.I: 1803753704

DECLARACIÓN DE AUTORÍA DE LA INVESTIGACIÓN

El autor de esta investigación declara ante el Comité Académico del Programa de Maestría en Tecnologías de la Información de la Universidad Estatal de Milagro, que el trabajo presentado es de mi propia autoría, no contiene material escrito por otra persona, salvo el que está referenciado debidamente en el texto; parte del presente documento o en su totalidad no ha sido aceptado para el otorgamiento de cualquier otro título de una institución nacional o extranjera.

Milagro, 27 de marzo del 2023.

Firmado electrónicamente por:
MARJORIE TOPACIO DUMAGUALA LEON

ING. DUMAGUALA LEÓN MARJORIE TOPACIO

C.I: 0941315426

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

CERTIFICACIÓN DE LA DEFENSA

El TRIBUNAL CALIFICADOR previo a la obtención del título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**, presentado por **ING. MARJORIE TOPACIO DUMAGUALA LEON**, otorga al presente proyecto de investigación denominado “PLAN DE SEGURIDAD BASADO EN LA NORMA ISO 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LA TRONCAL, PROVINCIA DEL CAÑAR”, las siguientes calificaciones:

TRABAJO DE TITULACION	56.00
DEFENSA ORAL	35.33
PROMEDIO	**91.33**
EQUIVALENTE	**Muy Bueno**

Firmado electrónicamente por:
MANUEL ANDRES AVILES NOLES

M.P AVILES NOLES MANUEL ANDRES
PRESIDENTE/A DEL TRIBUNAL

Firmado electrónicamente por:
RICHARD IVAN RAMIREZ ANORMALIZA

Ph.D RAMIREZ ANORMALIZA RICHARD IVAN
VOCAL

Firmado electrónicamente por:
FELIPE EMILIANO AREVALO CORDOVILLA

Msc. AREVALO CORDOVILLA FELIPE EMILIANO
SECRETARIO/A DEL TRIBUNAL

CESIÓN DE DERECHOS DE AUTOR

Doctor
ING. FABRICIO GUEVARA VIEJÓ, PhD
Rector de la Universidad Estatal de Milagro

Presente
Mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor al Trabajo realizado como requisito previo para la obtención de mi Título de Cuarto Nivel, cuyo tema fue **PLAN DE SEGURIDAD BASADO EN LA NORMA ISO 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LA TRONCAL, PROVINCIA DEL CAÑAR**, elaborado por **ING. MARJORIE TOPACIO DUMAGUALA LEON** y que corresponde al Vicerrectorado de Investigación y Posgrado.

Milagro, 27 de marzo del 2023.


Firmado electrónicamente por:
MARJORIE TOPACIO DUMAGUALA LEON

ING. MARJORIE DUMAGUALA

C.I: 0941315426

DEDICATORIA

Dedico con mucho cariño este trabajo profesional a mi abuelito quien, durante su vida, me brindó su apoyo y sus mejores deseos siempre; lamento mucho no contar con su presencia física y que pudiese contemplar una meta más cumplida. Su cariño y amor estará presente siempre en mi corazón.

AGRADECIMIENTO

Agradezco a Dios Padre todo Poderoso por todas las bendiciones que me concede día a día, a mis padres que siempre han confiado en mi capacidad profesional, a mis hijas por ser un pilar fundamental en mi vida y a las personas que han sido parte de esta maravillosa etapa. Agradezco a mi tutor por su paciencia, sus conocimientos y guía para la elaboración del presente documento. Un agradecimiento especial a la Universidad Estatal de Milagro, una institución de prestigio, quien nos ha brindado una educación de calidad con la finalidad de crear buenos profesionales.

INDICE

ÍNDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

El Gobierno Autónomo Descentralizado Municipal del cantón La Troncal, tiene la necesidad de salvaguardar su activo más importante, es decir la información institucional; ante posibles amenazas internas y externas. En base a esta necesidad se desarrolla la presente investigación, cuyo objetivo es realizar un Plan de Seguridad basado en la Norma ISO 27001, enfocado en las áreas de: Jefatura de Rentas, Jefatura de Recaudación, Avalúos y Catastros y Control Urbano, con el fin de asegurar la confiablidad, integridad y disponibilidad de la información.

Para conseguir el objetivo planteado, se ha llevado a cabo un levantamiento de Información a través de encuestas, utilizando un cuestionario desarrollado en Google Forms, las mismas que fueron aplicadas al personal que opera los Sistemas Informáticos pertenecientes al GAD Municipal La Troncal. Además del uso de la metodología MAGERIT, analizando los tipos de activos, criterios de valoración, amenazas y vulnerabilidades. Para la valoración de la encuesta se empleó la escala de Likert (1- muy bajo, 2-bajo, 3 medio, 4 alto y 5 muy alto); (1 muy insatisfecho, 2 insatisfecho, 3 neutro, 4 satisfecho y 5 muy satisfecho) y se realizó un análisis a lo establecido en el Anexo A de la Norma ISO 27001, en base a la realidad del Gobierno Autónomo Descentralizado Municipal de La Troncal. Con los resultados de la investigación se construyó un Plan de Seguridad basado en la Norma ISO 27001, cuyo objetivo primordial es precautelar el activo más valioso (información institucional) del Gobierno Autónomo Descentralizado Municipal de La Troncal para mantener niveles tolerables de riesgo de la información y de los dispositivos tecnológicos que admite su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación, conveniente presentación y su correcto cumplimiento en el desarrollo de sus actividades.

Palabras Clave: Seguridad, ISO 27001, información, riesgo.

ABSTRACT

The Autonomous Decentralized Municipal Government of the La Troncal canton has the need to safeguard its most important asset, that is, institutional information, against possible internal and external threats. Based on this need, the present investigation is developed, whose objective is to carry out a Security Plan based on the ISO 27001 Standard, focused on the areas of: Revenue Headquarters, Collection Headquarters, Appraisals and Cadastres and Urban Control, in order to to ensure the reliability, integrity and availability of information.

To achieve the stated objective, an information survey has been carried out through surveys, using a questionnaire developed in Google Forms, the same ones that were applied to the personnel that operates the Computer Systems belonging to the La Troncal Municipal GAD. In addition to the use of the MAGERIT methodology, analyzing the types of assets, valuation criteria, threats and vulnerabilities. For the evaluation of the survey, the Likert scale was used (1-very low, 2-low, 3 medium, 4 high and 5 very high); (1 very dissatisfied, 2 dissatisfied, 3 neutral, 4 satisfied and 5 very satisfied) and an analysis was carried out according to what is established in Annex A of ISO 27001, based on the reality of the Autonomous Decentralized Municipal Government of La Troncal. With the results of the investigation, a Security Plan was built based on the ISO 27001 Standard, whose primary objective is to protect the most valuable asset (institutional information) of the Autonomous Decentralized Municipal Government of La Troncal to maintain tolerable levels of information risk and of the technological devices that support its collection, processing, access, exchange, storage, transformation, convenient presentation and its correct fulfillment in the development of its activities.

Keywords: Security, ISO 27001, information, risk.

INTRODUCCIÓN

La Norma ISO 27001 es un estándar internacional que establece una serie de controles para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI), comprende una serie de procesos como la ejecución, preservación y mejora continua de la Seguridad de la Información. Apto para cualquier tipo de institución, pública o privada.

Las instituciones actualmente se encuentran propensas a padecer un ataque informático, afectando la integridad de la información. Las Tecnologías de la Información y Comunicación (TIC), brindan beneficios en la ejecución de procesos, optimización de tiempo y recursos.

En el Sector Público se aprecian cambios significativos en el entorno laboral que influyen en el comportamiento de los servidores públicos en la gestión de sus labores cotidianas. La gestión apropiada de la información permitirá a toda institución ejecutar sus labores con tranquilidad y seguridad

El Gobierno Autónomo Descentralizado Municipal La Troncal es una institución pública que goza de una gran cantidad de información, correspondiente al registro de: predios, pagos, datos de contribuyentes, etc.; en consideración al flujo de información cotidiana de la institución y la manipulación de los funcionarios municipales que tienen acceso a los sistemas informáticos institucionales, se considera conveniente el desarrollo de un Plan de Seguridad de la Información.

CAPÍTULO I

1.1. PLANTEAMIENTO DEL PROBLEMA

En el cantón La Troncal perteneciente a la provincia del Cañar, se encuentra la institución pública denominada Gobierno Autónomo Descentralizado (GAD) Municipal La Troncal; cuyo establecimiento recibe gran cantidad de personas que realizan varios trámites correspondientes al registro de predios, datos de contribuyentes, pagos diversos (patentes, alcabalas, plusvalía, rodaje, títulos de crédito, etc.).

El GAD Municipal La Troncal al poseer este tipo de información (activo importante), debe considerar delimitar el acceso a personal autorizado y capacitado para el uso de los sistemas existentes en la Entidad Municipal.

En la actualidad el tema de Seguridad, ha sido frecuentemente citado en los últimos años y se ha convertido en un asunto de gran relevancia para todas las instituciones, a nivel mundial, nacional y local. Dentro de las administraciones municipales este tema no se considerado de envergadura y no ha existido interés en la aplicación de normas internas para la Seguridad de la Información; por consiguiente, existe vulnerabilidad de la información en la institución.

La Norma ISO 27001, es un estándar internacional cuyo tema central es la seguridad, privacidad e integridad de la información. La Seguridad Informática es un tema actual, de gran relevancia y con un amplio contenido de investigación. (Mantilla, 2018)

En base a estudios realizados en función de la Seguridad de la Información al aplicar Políticas de Seguridad basadas en la ISO 27001, como la investigación realizada en el año 2021 en Perú, donde se obtuvieron mejoras considerables en la gestión de Seguridad de la Información. (Bustamante García et al., 2021)

La Norma ISO 27001, define diversos controles para su adquisición, desarrollo, personalización, mantenimiento y operación de aplicaciones, por lo tanto, resulta complejo que sea cumplido por algunas Entidades Municipales, debido al bajo

presupuesto estatal asignado para estos fines. Una selección de los dominios y controles de la Norma ISO permitirá desarrollar un Plan de Seguridad personalizado para la Entidad Municipal, además de mantener un control ante posibles amenazas y riesgos de la información.(VASUDEVAN et al., 2020)

La presente investigación analiza la Norma ISO 27001 y su aplicación en las áreas de: Jefatura de Recaudación, Jefatura de Rentas, Avalúos y Catastros y Control Urbano, posteriormente se procede a determinar los puntos vulnerables de la institución, identificar las necesidades de los usuarios que manipulan los sistemas institucionales, analizando los resultados obtenidos a través de la encuesta, el uso de la Metodología MAGERIT para el análisis de riesgos, establecer procedimientos de seguridad y desarrollar un Plan de Seguridad de la Información de acuerdo a las necesidades de la Institución, utilizando métodos apropiados conforme lo indica la Norma ISO 27001.

Obteniendo una herramienta útil para brindar una respuesta efectiva ante futuros ataques informáticos, con la finalidad de brindar una respuesta confiable para determinar soluciones en las áreas de gran flujo de información como lo son: Jefatura de Recaudación, Jefatura de Rentas, Avalúos y Catastros y Control Urbano.

1.2. Formulación del problema

- ¿Cuáles son los factores que causan vulnerabilidad en los sistemas de información en la Jefatura de Rentas, Jefatura de Recaudación, Avalúos y Catastros y Control Urbano del Gobierno Autónomo Descentralizado Municipal del Cantón La Troncal?

- ¿Qué provoca la desincronización entre la estructura, funciones y responsabilidades del personal que garanticen la confidencialidad, integridad y disponibilidad de los datos e información institucional?

- ¿Qué genera la aplicación de métodos y prácticas empíricas en el control, tratamiento y uso de recurso físico y lógico de almacenamiento de información institucional del GAD La Troncal?

1.3. OBJETIVOS

1.3.1. Objetivo General

Aplicar la norma ISO 27001 con la finalidad de realizar un Plan de Seguridad enfocado en los Sistemas informáticos utilizados por las Jefaturas de Rentas, Recaudación, Avalúos y Catastros y Control Urbano del GAD Municipal La Troncal.

1.3.2. Objetivos Específicos

- Identificar las vulnerabilidades en los procedimientos, que incluya técnicas e instrumentos para el control, uso y acceso a un recurso físico o lógico específico de la información institucional del GAD Municipal La Troncal.
- Analizar los controles correspondientes a la norma ISO 27001 para establecer un Plan de Seguridad para GAD Municipal La Troncal.
- Proponer un Plan de Seguridad de la Información; referente control, tratamiento y uso de recursos físicos y lógicos de información por parte del personal del GAD La Troncal.

1.4. ALCANCE

Este proyecto tiene como alcance realizar el análisis de la situación actual de la Entidad Municipal y el desarrollo de un Plan de Seguridad basado en la Norma ISO 27001, donde se proponga estrategias para la seguridad de los sistemas de información, establecer reglas de control para el personal institucional, garantizando la integridad de la información (modificación, manipulación, borrado y almacenamiento de archivos), manteniendo un control estricto, preservando la confidencialidad de la información e identificando diversos puntos vulnerables (Autentificación de Usuarios y Gestión de Privilegios), brindando nuevas alternativas referente al tema de Seguridad; enfocado en las áreas de las Jefatura de Rentas, Recaudación y Avalúos y Catastros del Gobierno Autónomo Descentralizado Municipal La Troncal, provincia del Cañar

Mediante la investigación bibliográfica, además de la verificación de controles del Anexo A correspondiente a la Norma ISO 27001 y de un análisis de campo realizado a través de la encuesta, los resultados obtenidos han permitiendo evaluar el riesgo e identificar las áreas vulnerables vinculadas con el uso de los Sistemas Informáticos.

Este Plan de Seguridad Informática enfocado en el GAD Municipal La Troncal, contendrá indicaciones para aplicar mejoras en la institución basados en la Norma ISO 27001, priorizando la información correspondiente a la Entidad Municipal con la finalidad que se encuentre preparada ante cualquier riesgo, precautelando la integridad de tan importante activo y a su vez se dará cumplimiento a lo que establece el Esquema Gubernamental de Seguridad de la Información (EGSI)(Muyón et al., 2018)

1.5. ESTADO DEL ARTE

En una investigación realizada por Aburto Zamora Keith Yasira (2019), en Valencia (España) cuyo objetivo fue desarrollar una herramienta informática que ayude en la fase inicial de la implantación de un Sistema Integrado de Gestión

(SIG), de las Normas ISO/IEC 27001 e ISO/IEC 20000-1, para definir el nivel de sentido en los procesos de gestión de servicios de TI y los controles de Seguridad de la Información. En el estudio se señaló que la gestión de la Seguridad de la Información logra establecer un marco con procedimientos y políticas que ayudan a mantener la convicción frente a los incidentes causados por ataques o amenazas a la información. Se obtuvo como resultado el análisis de los procesos de gestión de servicios de TI de la Norma ISO/IEC 27001 lo que permitió controlar las normas mediante un mapa de relaciones. Este estudio se plasmó mediante metodología del diseño de investigación(Aburto Zamora, Keith Yasira,2019

Edwin Samuel Arias Quispe (2020) en la ciudad de Lima, elaboró un estudio sobre la “Implementación de la Norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao”, usando el método inductivo para valorar las características que se reflejan de los participantes y además de un análisis documental. El trabajo se desarrolla en implementar la Norma ISO 27001 ayudando a que el departamento de TI pueda conocer de una forma adecuada los riesgos, la vulnerabilidad existente y así lograr reducirlos; brindando un sistema de gestión de seguridad en donde permita administrar y controlar posibles ataques, resguardando la información de la institución. Los resultados del estudio presentan mejora en los procesos actuales y mantienen la integridad, confiabilidad y disponibilidad de la información, brindando una mejor experiencia a los clientes y miembros de la dirección(Quispe, 2020)

María González Sandoval (2016) en la ciudad de Distrito Nacional (República Dominicana) realizó un estudio sobre el “Modelo de Gestión de la Norma ISO/IEC 27001:2013 en la Seguridad de Información de una empresa de Telecomunicaciones” mediante el método de investigación bibliográfica. El trabajo tiene como propósito orientar el logro adecuado de la gestión de seguridad de información dentro de la empresa. Se elabora un modelo de gestión de seguridad basado en el ciclo de mejora continua Deming, el mismo que consiste en planificar, hacer, verificar, actuar, así mismo dependerá de las necesidades que presente el Sistema de Gestión de Seguridad de la Información (SGSI). Como resultado se obtuvo que la empresa debe implementar el modelo

de gestión debido a las falencias que presenta en el área de Seguridad de la Información, con el objetivo de disminuir el riesgo y adoptar controles de una manera eficaz, el sistema de gestión ayudará a prevenir riesgos y amenazas a la hora de acceder a su información confidencial y esto será de vital importancia para el crecimiento de su empresa.(González, 2016)

Jaime Andrés García Remache (2020) en la ciudad de Quito, efectuó el estudio denominado “Diseño de un sistema integrado de gestión basado en las Normas ISO 9001:2015 e ISO 27001:2013, para emitir documentos de identificación militar ubicado en la matriz de la Dirección de Movilización del Comando Conjunto de las Fuerzas Armadas”, cuyo objetivo fue crear un sistema basado en las normas ISO 9001:2015 e ISO 27001:2013, utilizando el método analítico a través de encuestas, entrevistas, revisión documental física y digital. El desarrollo del trabajo se basó en tres etapas acorde al ciclo Kurt Lewin y empleando las normas ISO, a través de ello se optimizaron procesos mediante la metodología EFI (Indicador Homologado de Eficiencia). El resultado final fue un manual del sistema integrado donde se establece los procesos del sistema y sus herramientas(García, 2020)

Carlos Freddy Saltos Peña e Ilse Lorena Ycaza Díaz (2017) en Guayaquil, efectuaron el estudio de “Desarrollo de un esquema de Seguridad de Información siguiendo el estándar ISO 27001-2013 aplicado al área de seguridad de la información para una cooperativa de ahorro y crédito” cuyo trabajo tiene como finalidad desarrollar un esquema de Seguridad de la Información mediante la metodología PDCA, obteniendo como resultado serias deficiencias en el control interno de la institución, basados en los procesos de gestión de usuario, monitoreo de la seguridad y después de la implementación de controles, a través de proyectos definidos evaluados por auditorias independientes para el cumplimiento de los requisitos normativos a la ISO, presenta que el 82% de controles sugeridos, no existen en la institución y solo un 18% existen y resultan pocos efectivos para el riesgo asociado. (Saltos Peña, 2017)

Manuel Rodrigo Aguilar Carrión (2017) en la ciudad de Ambato, realizó un estudio teniendo como tema un “Plan de Seguridad Informática basado en

estándar ISO-IEC 27001 para proteger la información y activos del Gobierno Autónomo Descentralizado (GAD) Cantonal de Pastaza". Por medio de la metodología cualitativa/cuantitativa, además de una investigación bibliográfica e investigación de campo. El proyecto realizó un análisis FODA al GAD cantonal de Pastaza, con el objetivo de visualizar la situación en la que se encontraba, mediante el uso de la herramienta Microsoft Security Assessment Tool (MSAT) evaluó los puntos débiles del entorno de la Seguridad de la Información y así se logró fortalecer esa vulnerabilidad en cuanto a la seguridad de un modo rápido y efectivo. Se recomienda que, al ser implementado el Sistema de Seguridad de Información en el GAD Cantonal de Pastaza, se prevengan futuros riesgos en la seguridad de los datos, controlando la normativa de Seguridad de la Información en base a los lineamientos y objetivos. (Aguilar, 2017)

Natalia Judith Crespo Chávez (2018) en Ambato, desarrolló una investigación denominada "La aplicación de las Normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior" para determinar la repercusión de la aplicación ISO 27001 y 27002, se utilizó el enfoque cuali-cuantitativo, la investigación bibliográfica y de campo. El trabajo desarrollado presenta evidencia de que la auditoria permite corroborar que los esfuerzos respecto a la Seguridad de la Información no son suficientes y se debe considerar una gestión de seguridad de planeación, monitoreo, evaluación y mejoras garantizando la continuidad y protección de los activos. (Crespo, 2018)

Antonio Guamán y Jorge Vinicio Cárdenas Muñoz (2022) realizaron un estudio cuyo tema es "Cumplimiento de las políticas de Seguridad de Información en las cooperativas de ahorro y crédito del cantón Cañar"; las investigaciones e indagaciones realizadas a las cooperativas del cantón Cañar, permiten identificar el desempeño de las políticas de seguridad de la información; obteniendo el siguiente resultado: el 100% en el dominio de políticas de seguridad; 57% referente al dominio de aspectos organizativos (seguridad de la información); 58% en el dominio de la seguridad enlazado a los recursos humanos;25% en la gestión de los activos; 65% referente al control de acceso; 100% en el dominio de cifrado; 57% en el dominio de seguridad física y ambiental; 67% en la seguridad de telecomunicaciones; 50% dominio de seguridad operativa; 27% en

función de la adquisición, mantenimiento y desarrollo; 10% dominio de relaciones con los proveedores; 7% correspondiente al dominio de gestión de incidentes de seguridad de la información, este es el nivel más importante de los dominios y a su vez es el más crítico en las cooperativas de ahorro y crédito. Obteniendo como resultado un 0% en el cumplimiento de la gestión de seguridad de la información (Guamán y Cárdenas, 2022)

1.5.1. Marco Conceptual

El avance tecnológico ha provocado la adquisición de nuevas tecnologías en diversas instituciones públicas y privadas, cuya información con anterioridad solo existía mediante un expediente en físico; en cambio en la actualidad la misma información se encuentra digitalizada y accesible mediante Sistemas Informáticos facilitando la búsqueda de trámites y el acceso a la misma para el desarrollo de procesos; por ello la Seguridad de la Información se ha convertido en un activo de vital importancia para las instituciones, siendo fundamental para intereses estratégicos institucionales. La seguridad de la norma ISO 27001 está relacionada con el objetivo de brindar seguridad en la información en los aspectos dimensionales de confidencialidad, integridad y disponibilidad(Ruíz et al., 2020)

Actualmente las amenazas tecnológicas son parte del día a día y más cuando se trata de la vida organizacional, con esto nos referimos a incomparables formas de virus desde los más sofisticados como el ataque del día cero a un ataque ransomware, siendo así que se requiere la implementación de controles que logren gestionar todo a través de un enfoque adecuado para brindar la seguridad de la información. (Valencia-Duque y Orozco-Alzate, 2017)

Toda información debe ser totalmente protegida pero así mismo, debe estar al alcance de cualquier necesidad, permitiendo el acceso a ella de una manera oportuna. Dentro del enfoque de la seguridad de la información se considera la confidencialidad, integridad y disponibilidad. Varias organizaciones han implementado políticas y acciones fundamentales, previniendo robo o

manipulación de la información; pero con la firme evolución de la tecnología el riesgo a su vez va en aumento y además las amenazas a la información de las empresas(Rodríguez et al., 2020).

La información se ha ido transformando en un activo intangible que necesita certificar disponibilidad, confidencialidad e integridad. Un Sistema de Gestión de la Seguridad de la Información permite administrar y dar seguridad a los activos como la propiedad intelectual, la información financiera, el detalle de los empleados y de los clientes(Tundidor-Montes de Oca et al., 2019)

La Seguridad Informática es esencial para la protección de información, en donde se permite delimitar el acceso a programas y archivos mediante claves o encriptaciones, asignando limitaciones precisas a los usuarios de cada sistema informático, esto significa que no se dará privilegios extras a una persona cuyo rol dentro de la empresa no requiera de dichos permisos. De esta manera protegemos los archivos y programas necesarios para el correcto funcionamiento sin exponer la información.(Figueroa Pérez y Malagón Sáenz, 2017)

Todo tipo de empresa está expuesta a riesgos, desde su exterior hasta el interior. Para que una empresa pueda crecer y tener un negocio o procesos solventes debe protegerse de las posibles amenazas. Cada empresa debe brindar una seguridad apropiada y una excelente protección de datos para su sostenibilidad. La ISO 27001 es una norma que consiste en la actividad de seguridad para los objetivos de la empresa dentro de un enfoque y marco en la información, la seguridad debe ser coherente con la cultura de la organización.(Merchán-Lima et al., 2021)

La gestión de Seguridad de la Información en una organización o empresa es un proceso que está perfectamente definido por lo que enlaza un gran esfuerzo entre usuarios, jefes de áreas y los demás servidores que se dan cita a conocer, para ellos poder responder ante cualquier evento que sea sospechoso y estar preparados para gestionar o identificar las vulnerabilidades(Ruíz et al., 2020b)

Para mejorar la Seguridad de la Información se debe tomar en consideración

todas las actividades que implican, entre ellas la política de seguridad, estructura empresarial, compromiso de la dirección para invertir en un Sistema de Gestión de Seguridad de Información “SGSI”. La información frente al desarrollo tecnológico, las empresas se enfrentan a nuevos y distintos riesgos para la seguridad de su información. Alcanzar un nivel adecuado a la protección de información requiere una aplicación muy efectiva del SGSI(Lilja SIKMAN et al., 2019)

La Norma ISO 27001 en términos generales se usa para describir los requisitos que se lleva a cabo para lograr implementar un Sistema de Gestión de Seguridad de la Información SGSI, teniendo como eje principal la evaluación de riesgos, facilitando a las organizaciones obtener una mejor visión logrando definir un mejor alcance, en el ámbito de la aplicación, políticas, procedimientos y normas a efectuarse; adoptando las metodologías que mejoren la Gestión del riesgo (Melo Reyes, 2019)

La creciente demanda en los panoramas de la Seguridad de la Información hace que los riesgos sean aún más desafiantes. La norma ISO 27001 ha dado mejoras a lo largo de los años, su adopción en cualquier tipo de empresa resulta ser beneficioso al establecer, implementar, monitorear, revisar, operar y administrar un Sistema de Gestión de Seguridad de la Información (Guerra, 2018)

1.5.2. Terminologías usadas en la investigación

Norma ISO 27001: se la reconoce de manera implícita como la seguridad de la información y en donde un SGSI debe formar parte esencial de cualquier sistema de control interno. La ISO 27001 tiene como respaldo a varias familias de normas bien relacionadas, en donde cada una de estas normas ofrecen precisión a la seguridad de la información(Calder, 2017)

SGSI: Definido como Sistema de Gestión de Seguridad de la Información, se encarga de abarcar características estructurales en una organización como son

el tamaño, los objetivos, el tipo, los servicios, los procesos, el personal y los requerimientos de seguridad. Basándose en las normas internacionales como es la ISO/IEC 27001(Ruíz et al., 2020c)

Seguridad de la Información: o también conocida como seguridad de tecnologías de la información, consiste en asegurar los recursos del sistema de información referente a los programas o material informático, sea de una empresa u organización para ser usados de una forma correcta (Figueroa-Suárez et al., 2018)

Integridad de la información: es la integración de los datos, se puede conceptualizar como la dificultad de que cualquier persona tenga acceso o modifique la información sin ser descubierto. Es la protección de la información mediante antivirus, códigos, ciclos de vida, etc. (Díaz Sánchez, 2021)

Confidencialidad de la información: la confidencialidad se basa en que solo usuarios que estén autorizados van a conocer la información, evitando el acceso malintencionado o a personas no autorizadas (Patiño et al., 2017)

Disponibilidad: facilitar el acceso a usuarios o personas autorizadas. Es decir, la información debe estar disponible en cualquier momento. Se rige bajo políticas como el nivel de servicio y la disponibilidad del sistema a través de redundancia y alta disponibilidad (Morales et al., 2020)

Vulnerabilidad: es la manera general en la que en un sistema pueda suceder, donde un atacante se aprovecha de ello para acceder a la información, dando un riesgo a la organización o al mismo sistema (Bolaño Rodríguez et al., 2019)

Municipio: se denomina así a las instalaciones físicas, espacio administrativo en el que da funcionamiento el gobierno. Se entiende como la institución, sea independiente o autónoma.

CAPÍTULO 2

2.1. Metodología

El uso de una metodología en esta investigación es primordial debido a que permite alcanzar un fin, en este caso en base a la naturaleza del problema, se ha considerado el método de investigación descriptiva a través de observaciones cualitativas. Esta metodología cualitativa permite observar, interactuar y obtener información sobre las opiniones, creencias y valores de una sociedad. Este método de recopilación de datos permite comprender mejor los procesos en estudio.

Adicionalmente, mediante la investigación bibliográfica acerca del uso de la Norma ISO 27001 para la implementación de un Sistema de Seguridad de la Información, he visto relación con el uso de la Metodología MAGERIT, la cual se enfoca en el análisis de riesgos en una organización; en base a los resultados favorables he considerado el uso de la presente metodología aplicado al GAD Municipal La Troncal.

2.1.1. Metodología MAGERIT

Es una metodología basada en el análisis y gestión de riesgos, producido por el “Consejo Superior de Administración Electrónica” de España que brinda un método sistemático para examinar los riesgos derivados del uso de Tecnologías de la Información y de esta forma ejecutar las medidas de control adecuadas que permitan disminuir los riesgos. Dispone de técnicas y ejemplos que conceden realizar el análisis de riesgos.(Ferruzola Gómez et al., 2019)

Esta metodología dentro de un marco de trabajo para que la organización tome decisiones en base al proceso de Gestión de Riesgos derivados del uso de tecnologías de la Información.

Objetivos Directos:

- Sensibilizar a los responsables de las organizaciones acerca de la

existencia de riesgos y de la necesidad de gestionarlos.

- Brindar un método sistemático para examinar los riesgos procedentes del uso de tecnologías de la información y comunicaciones (TIC).

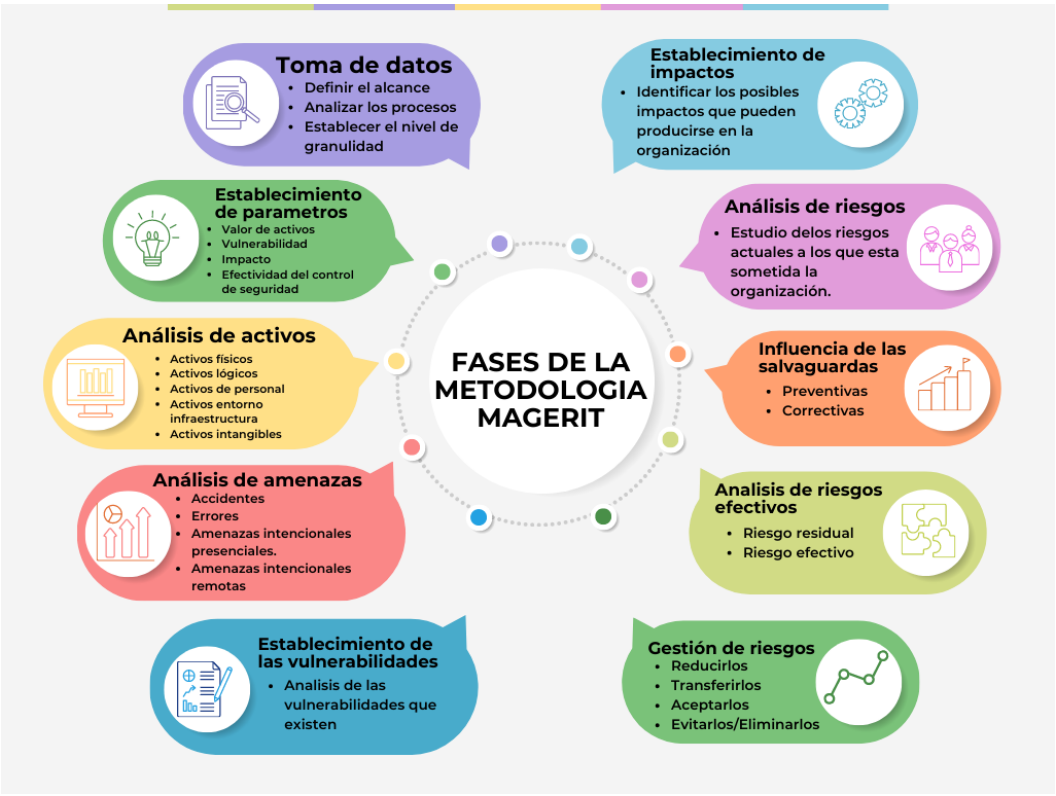
- Contribuir a detectar y proyectar el método oportuno para sostener los riesgos bajo control.

Objetivos Indirectos:

Prevenir a la Organización para futuros procesos de evaluación, auditoría, certificación o acreditación, según la necesidad de la misma. Esta metodología facilita una guía completa, acerca de cómo realizar un análisis de riesgos.

Ilustración 1

Fases de la Metodología MAGERIT



Fuente: Elaboración propia,2022

La metodología MAGERIT permite garantizar la Seguridad de los datos o

Información y resulta conveniente para iniciar con la administración de la Seguridad de la Información, mediante un análisis del impacto ante cualquier acción que cause un daño o perjuicio a la institución. Alcanzando medidas preventivas y correctivas adecuadas para la Seguridad de Información.

2.1.2. INVENTARIO DE ACTIVOS

Un activo es un bien de valor para la institución, por las acciones que realiza para alcanzar sus objetivos, por este motivo en cuestión de seguridad procura garantizar la confidencialidad, integridad y disponibilidad de los activos para asegurar una correcta operación en la institución y garantizar la prolongación de sus operaciones. Los activos (bienes, recursos y servicios) son aquellos elementos o característica de un Sistema de Información susceptible de ser perjudicado intencional o accidentalmente cuyo resultado para la organización incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. Para iniciar con la gestión de riesgos es indispensable tener un inventario de activos.

Tabla 1

Inventario de activos

CATEGORIA	ACTIVO
Datos	Datos Departamentales
	Copias de seguridad
	Base de datos
	Código fuente
	Logs registros de actividad
	Archivos de configuración
Servicios	Servicio Web
	Correo institucional
Software	SQL Server
	Antivirus
	Windows 10
Hardware	Portátil
	Computador todo en uno
	Computador de escritorio

	Impresoras
	Switches
	Servidores
Redes de Comunicaciones	Red LAN
	Red Wi Fi
	Internet
	Equipo de ventilación
Equipo Auxiliar	Consumibles varios
	Corriente eléctrica
	Cableado de la red

Fuente: Elaboración propia,2022

En la Tabla 1 se evidencia el inventario de activos pertenecientes a la institución, de acuerdo a su categoría.

Tabla 2

Detalle Equipos-Jefaturas

	JEFATURA DE RENTAS	JEFATURA DE RECAUDACION	AVALUOS Y CATASTROS	CONTROL URBANO
Portátil	0	1	1	2
Computador todo en uno	1	2	1	3
Computador de escritorio	5	1	8	2
Impresoras	2	1	2	1
Switches	1		1	
Servidores	1	1	1	1
TOTAL	10	6	14	9

Fuente: Elaboración propia,2022

En la Tabla 2 se puede verificar los equipos que dispone el GAD Municipal La Troncal, dentro de las áreas correspondientes a la presente investigación, se presenta a detalle de los equipos con su respectiva cantidad total de equipos correspondiente a cada Jefatura.

2.1.3. Criterios de Valoración

Para la valoración de los activos es importante considerar lo siguiente:

- Emplear un rango en común para todos los parámetros, permitiendo comparar riesgos.
- El manejo de una medida logarítmica, enfocado en diferencias concerniente al valor, no en desigualdad categórica.
- Utilizar una perspectiva uniforme que posibilite cotejar análisis realizados individualmente.

Frecuentemente la valoración es cualitativa, respondiendo a criterios subjetivos. La escala elegida detalla en diez estimaciones, partiendo del valor 0 como taxativo de un valor Muy Bajo (efecto de riesgo). En el caso de un análisis de riesgos limitado, se puede preferir una tabla sintetizada de niveles mínimos. Cualquier escala, detallada o limitada se relacionan como se demuestra a continuación:

Tabla 3
Criterios de Valoración

Valor		Criterio
10	Extremo	Daño Extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Muy Bajo	Irrelevante a efectos prácticos

Fuente: Elaboración propia,2022

Se empleó la metodología MAGERIT, para la valoración de riesgos en los Equipos Tecnológicos descritos en la Tabla 2, pertenecientes a la Jefatura de Recaudación, Jefatura de Rentas, Avalúos y Catastros y Control Urbano; en función de los Criterios de Valoración descritos en la Tabla 3, cuyos resultados

se pueden apreciar en la siguiente Tabla.

Tabla 4

Estado de Equipo Tecnológico

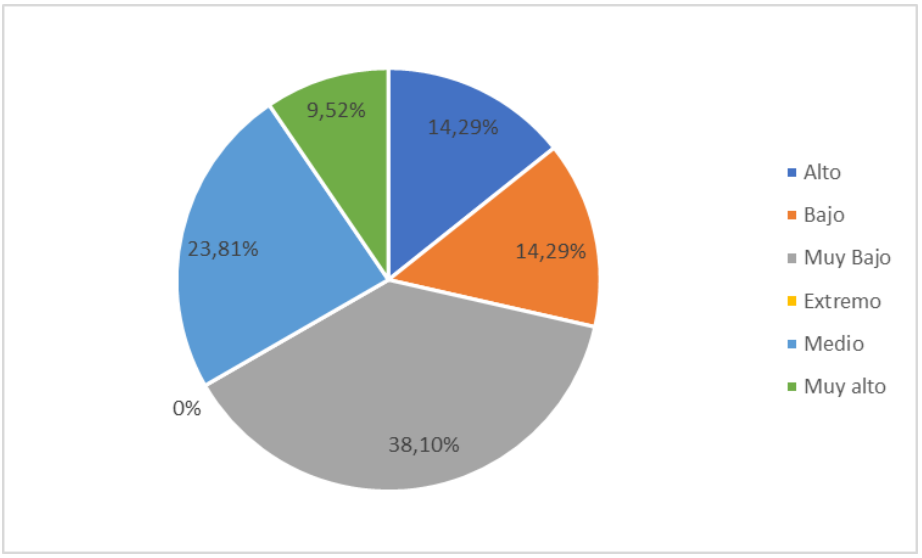
EQUIPOS	JEFATURA DE RENTAS	JEFATURA DE RECAUDACION	AVALUOS Y CATASTROS	CONTROL URBANO
Portátil	-	Muy alto	Muy Bajo	Muy Bajo
Computador todo en uno	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo
Computador de escritorio	Alto	Alto	Alto	Muy Alto
Impresoras	Medio	Muy Bajo	Medio	Bajo
Switches	Muy Bajo	-	Bajo	-
Servidores	Bajo	Medio	Medio	Medio

Fuente: Elaboración propia,2022

Los resultados obtenidos en la Tabla 4, ha logrado identificar el estado del Equipo Tecnológico, el estado de riesgo dificulta la realización de las actividades cotidianas a los funcionarios; ralentizando sus actividades, su rendimiento y afectando a la Seguridad de la Información en los Sistemas Informáticos pertenecientes al GAD Municipal La Troncal.

Ilustración 2

Niveles de Riesgo Equipo Tecnológico



Fuente: Elaboración propia,2022

En la Ilustración 2, refleja el porcentaje correspondiente al nivel de riesgo existente en la Jefatura de Recaudación, Jefatura de Rentas, Avalúos y Catastros y Control Urbano; de acuerdo a los niveles correspondientes a la Tabla 3 Criterios de Valoración y en base a los resultados de la Tabla 4 Estado del Equipo Tecnológico correspondiente a la evaluación de cada Jefatura del objeto de investigación

Además se llevó a cabo una investigación bibliográfica para la recolección de conceptos y definiciones, teorías o enfoques; mediante este tipo de investigación que está basada documentos bibliográficos, libros electrónicos, artículos científicos, tesis en donde se ha aplicado las normas ISO 27001:2013 a la seguridad de la información y demás documentos que permitan conocer más acerca del tema, que ha sido esencial para profundizar acerca de la investigación y llevar el desarrollo de esta propuesta.

La información recolectada en el campo de estudio debe ser confiable y demostrar garantía para obtener esa información. En la actualidad se encuentra variada información científica; la revisión bibliográfica es la descripción que se detalla de un tema, pero no influye en las decisiones estratégicas que se pueda tomar para la realización de un proyecto (José Hernández, 2019)

2.1.4. AMENAZAS Y VULNERABILIDADES

En las organizaciones, los activos de información están sujetos a diversas amenazas. Una amenaza puede ocasionar un percance no deseado, perjudicando a la organización y a sus activos. Para identificar las amenazas cuya influencia afecte los activos, conviene clasificarlas, conforme lo siguiente:

Ilustración 3

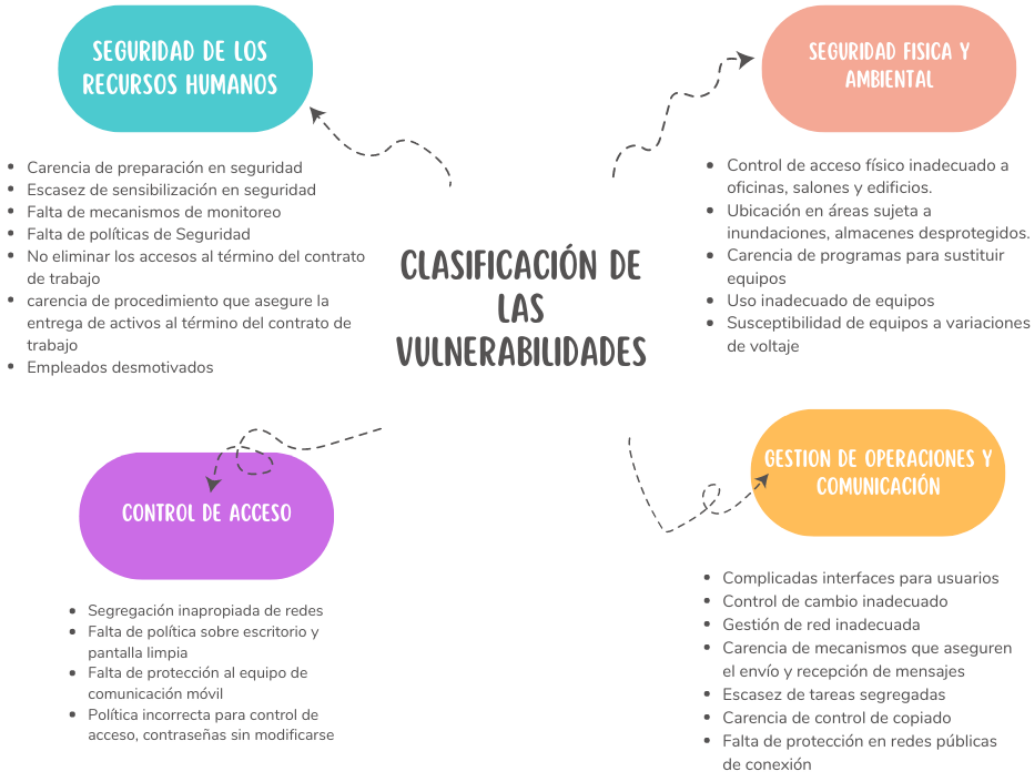
Clasificación de las amenazas

Fuente: Elaboración propia,2022

Las vulnerabilidades son debilidades de seguridad vinculadas con los activos de información de una organización. Se define como las debilidades del sistema de seguridad, no causan daño. Sencillamente su estado puede hacer que una amenaza afecte un activo.

Ilustración 4

Clasificación de las vulnerabilidades



Fuente: Elaboración propia,2022

2.2. Norma ISO 27001

Un SGSI eficaz requiere de la evaluación de riesgos, la norma ISO 27001 nos proporciona pautas eficientes y eficaces recomendados a nivel internacional, para la evaluación de defensas adecuadas.

De acuerdo con los lineamientos propuestos por la norma, es fundamental establecer las Políticas de Seguridad dentro de una empresa u organización para garantizar la confidencialidad, integridad y disponibilidad de la información.

2.2.1. Estructura de la Norma

La ISO 27001 es una guía realizada por la Organización Internacional de Normalización (ISO), utilizada en las organizaciones con la intención de contribuir con la gestión de la Seguridad de la Información.

Ilustración 5

Estructura de la Norma ISO 27001

Fuente: Elaboración propia,2022

La norma ISO 27001, se encuentra relacionado con la ISO 27002 en la misma se encuentra detallado el Anexo A; en el cual se definen los controles estratégicos que son una directriz para la implementación de los mismos, como lo indica (Chopra y Chaudhary, 2020) estos requisitos permiten establecer, implementar, mantener y mejorar continuamente la Seguridad de la Información.

2.2.2. Población

La población que se considera en la investigación está conformada por el personal que tiene acceso a los módulos de cada sistema informático en función de su cargo correspondientes a las áreas de jefatura de rentas, jefatura de recaudación, avalúos y catastros y Control Urbano para el estudio del proyecto.

Tabla 5

Sistemas Informáticos GAD LA Troncal - Módulos

Sistemas	Módulos
SGM-VENTANILLA UNICA	Certificado de no adeudar
	Certificado avalúos y catastros
	Certificados varios
	Diario de caja
	Recaudación
	Cobros por ventanilla
	Alcabalas
	Puestos y kioscos
	Rodaje vehicular
	Plusvalía
SGM- COBROS DIRECTOS	Título de crédito
	Título de crédito - varios
	Certificación exenta de pago
	Tasas transito
	Áridos y pétreos – tasa por autorizaciones y concesiones
	Turismo – licencia única anual de funcionamiento (LUAF)

SGM-CATASTRO RUSTICO	Cobro de planillas
	Reporte diario
	Cartera vencida y por vencer
	Tasas de interés BCE
	Tasas de descuento y/o interés según ordenanza
	Reliquidar cartas de pago años 2005-2013
	Reliquidar cartas de pago años 2014-2015
	Reliquidar cartas de pago años 2016-2019
	Reliquidar cartas de pago años 2020-2021
	Copias planillas pagadas
	Imprimir y/o reliquidar manualmente cartas de pago
	Cartera vencida por monto individual y años
SGM-CATASTRO URBANO	Cobro de planillas
	Reporte diario
	Cartera vencida y por vencer
	Tasas de interés BCE
	Tasas de descuento y/o interés según ordenanza
	Reliquidar cartas de pago años 2006-2013
	Reliquidar cartas de pago años 2014-2015
	Reliquidar cartas de pago años 2016-2019
	Reliquidar cartas de pago años 2020-2022
	Copias planillas pagadas
	Imprimir y/o reliquidar manualmente cartas de pago
CATASTROS-AUXILIAR	Imprimir cartas de pago para avisos
	Reportes – urbano
	Reportes – rustico
	Coactivas – copia títulos pagados urbano
	Coactivas – copia títulos pagados urbano
Total	44

Fuente: Elaboración propia,2022

La población fue evaluada en su totalidad enfocándose en las áreas: de jefatura de rentas, la jefatura de recaudación, avalúos y Catastros y Control Urbano, siendo así como se aprecia en la Tabla 5 cuenta con 44 módulos, donde se lleva a cabo el método censal para confirmar que la muestra tiene la misma cantidad que la población.

Tabla 6

Personal opera Sistemas Informáticos

Personal que usa el Sistema	Cantidad
Jefe de Sistemas	1
Analista de Sistemas	2
Personal que utiliza los Sistemas Informáticos	28
TOTAL	31

Fuente: Elaboración propia,2022

El detalle del Personal institucional que se aprecia en la Tabla 6, identifica a la población seleccionada para aplicar la encuesta; es preciso indicar que de acuerdo al cargo que desempeñan en institución tienen acceso a diversos sistemas con diferentes controles.

2.3. Técnica de recolección y análisis de datos

La encuesta se define como una técnica sistemática que sirve para obtener datos verídicos de un grupo definido de personas. Este tipo de técnica de investigación tiene la finalidad de dar valor agregado para la entidad municipal.(Quevedo Arnaiz et al., 2021)

La denominada, “Escala Likert” es una escala de calificación que permite entender al encuestado, quien manifiesta su acuerdo o desacuerdo sobre una determinada interrogante, lo que se realiza a través de una escala ordenada y de fácil interpretación. Esta herramienta permite medir actitudes y conocer el grado de consentimiento del encuestado ante una afirmación planteada.(Suárez & Maggi, 2020)

Tabla 7

Puntuación y Escala utilizada en el instrumento de recolección de datos

Puntuación Numérica	Rango o Nivel
1	Nada satisfecho
2	Insatisfecho
3	Neutro
4	Satisfecho
5	Totalmente satisfecho

Fuente: Elaboración propia,2022

Previo a la realización de la encuesta se solicitó autorización a la Máxima autoridad del Gobierno Autónomo Descentralizado Municipal La Troncal (ver Anexo 1); el requerimiento tuvo una respuesta favorable para la ejecución de la presente investigación aprobado por el Ing. Rómulo Ulises Alcívar Campoverde, Alcalde del Cantón La Troncal (ver Anexo 2).

La encuesta se realizó in situ, utilizado una de las herramientas que nos brinda Google; se trata de Google Forms, diseñando una encuesta para el personal que labora en las áreas de: Jefatura de Recaudación, la Jefatura de Rentas, Avalúos y Catastros y Control Urbano; adicional para obtener una perspectiva técnica se realizó una encuesta al personal de la Jefatura de Sistemas. Las encuestas fueron desarrolladas en base a lo establecido por la Norma ISO 27001, consiguiendo la opinión del personal que utiliza los Sistemas Informáticos e identificando los puntos vulnerables dentro de GAD Municipal La Troncal.

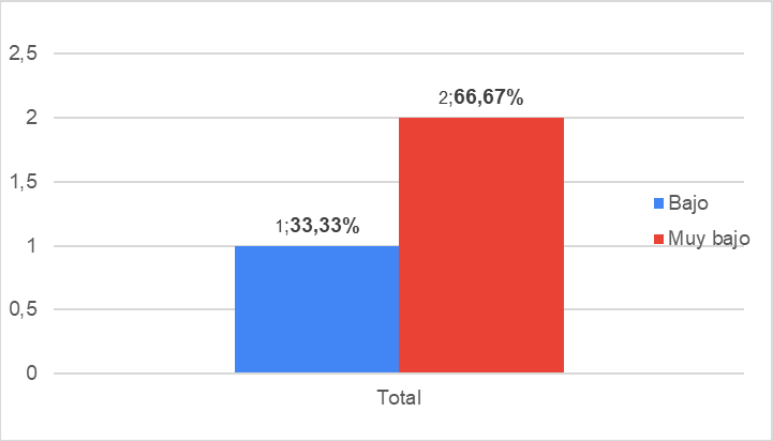
2.3.1. Análisis descriptivo de los resultados

La técnica de investigación que se aplicó en este proyecto ha sido la encuesta, utilizando la herramienta digital que nos brinda Google Drive – Formularios de Google. Este cuestionario esta realizado en base a lo que indica la Norma ISO 27001, con finalidad establecer la funcionalidad de los Sistemas Informáticos del GAD Municipal La Troncal.

Preguntas realizadas al personal de la Unidad de Sistemas del GAD Municipal La Troncal.

Ilustración 6

Nivel de Importancia acerca de la Seguridad de la Información

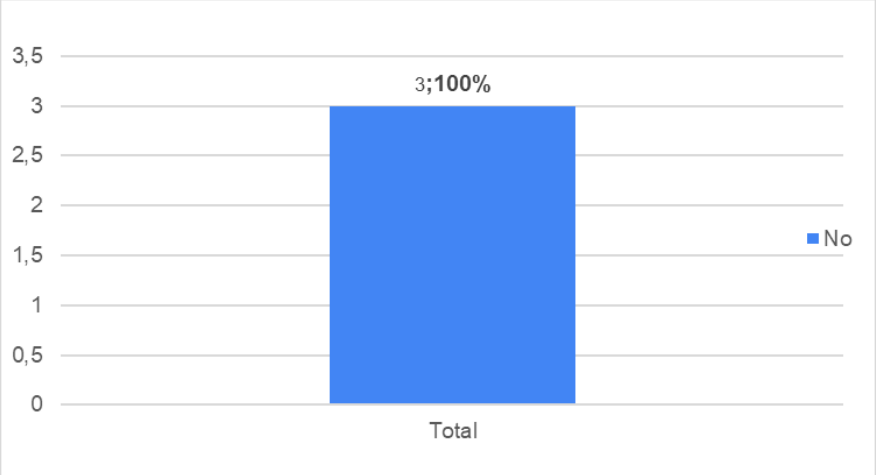


Fuente: Elaboración propia,2022

Referente al Nivel de importancia que asume la Entidad Municipal acerca de la Seguridad de la Información, como se aprecia en la Ilustración 6; en los resultados se evidencia que el 33,33% de los funcionarios consideran que existe en un nivel Bajo y el 66,67% indican que se encuentra en nivel Muy Bajo.

Ilustración 7

La entidad cuenta con software anti-spyware

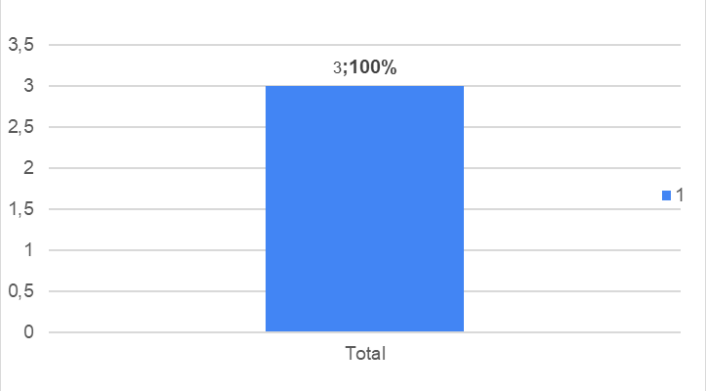


Fuente: Elaboración propia,2022

Los resultados obtenidos como indica la Ilustración 7, indican que los funcionarios de la unidad de Sistemas él (100%) afirman que el Gobierno Autónomo Descentralizado Municipal de La Troncal NO cuenta con software anti-spyware.

Ilustración 8

Nivel de satisfacción referente al software anti-spyware

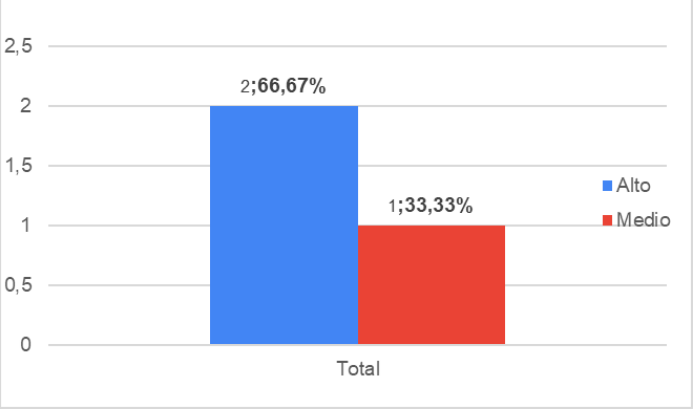


Fuente: Elaboración propia,2022

La Ilustración 8, nos indica que los funcionarios de la Unidad de Sistemas (100%) afirman un nivel Muy Insatisfactorio referente al nivel de satisfacción del software anti-spyware que posee la Entidad Municipal.

Ilustración 9

Nivel de control referente a la creación y autorización de permisos a los usuarios

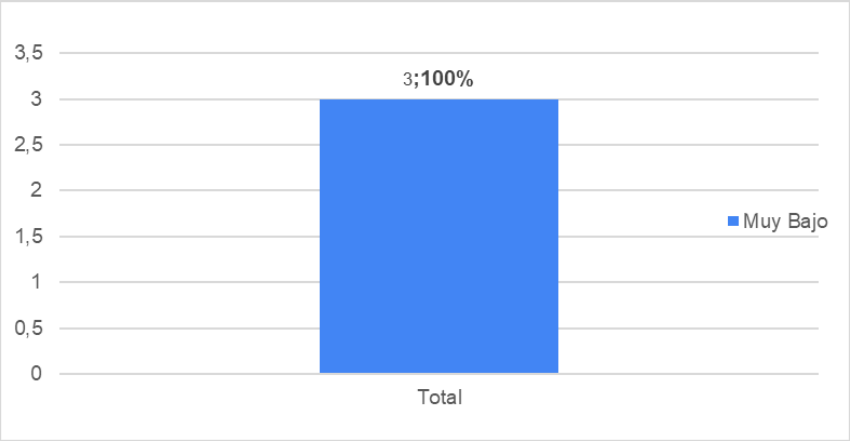


Fuente: Elaboración propia,2022

Referente al nivel de control en la creación y autorización de permisos a usuarios, como se puede apreciar en la Ilustración 9, la mayor cantidad de funcionarios de la unidad de Sistemas (66,67%) consideran que se encuentra en un nivel Alto y el (33,33%) indican que se encuentra en nivel Medio.

Ilustración 10

Nivel de comunicación entre las áreas

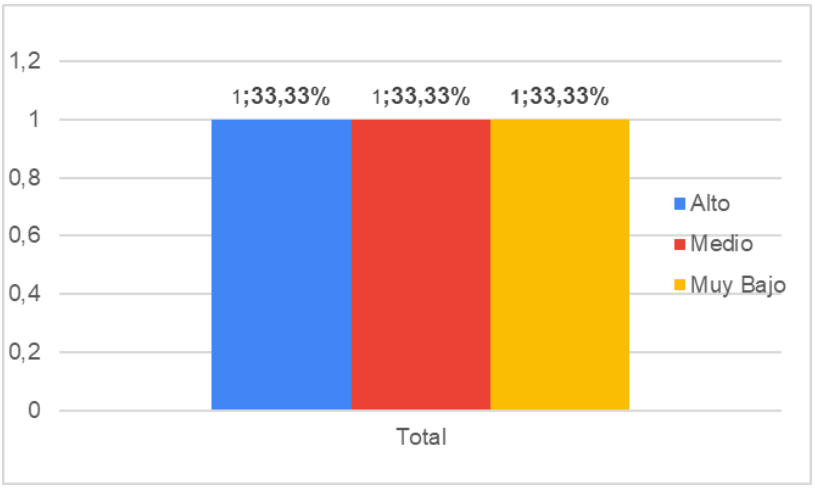


Fuente: Elaboración propia,2022

Como se aprecia en la Ilustración 10, los resultados obtenidos indican que el (100%) de los funcionarios de la Unidad de Sistemas afirman que existen un nivel Muy Bajo de comunicación entre las áreas referente a la terminación contractual del personal y la in habilitación de usuarios que tenían acceso los sistemas.

Ilustración 11

Nivel de seguridad en sus procesos y procedimientos

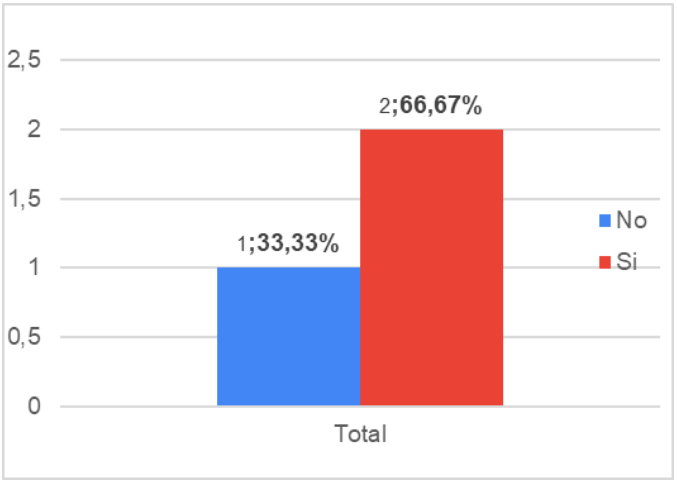


Fuente: Elaboración propia,2022

En relación al nivel de seguridad en sus procesos y procedimientos establecidos por el GAD Municipal La Troncal; la Ilustración 11, indica los siguientes resultados (33,33%) consideran que se encuentra en un nivel Alto, (33,33%) indican que se encuentra en nivel Medio y (33,33%) indican que se encuentra en nivel Muy Bajo.

Ilustración 12

Informe sobre la situación de la seguridad

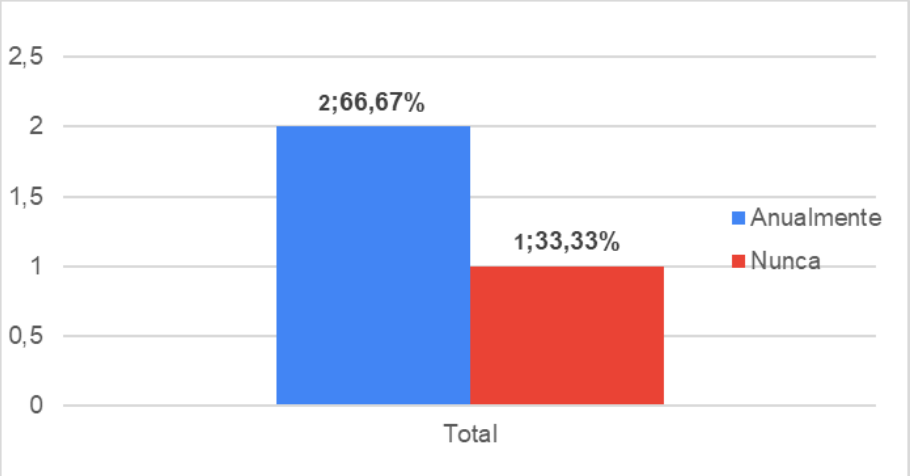


Fuente: Elaboración propia,2022

Como se puede observar en la Ilustración 12, acerca de la emisión de un informe sobre la situación de seguridad a las principales autoridades de la Entidad Municipal; los resultados indican que el (33,33%) de los funcionarios de la unidad de Sistemas afirman que No y (66,67%) afirma que Si.

Ilustración 13

Informe sobre la situación de seguridad a las principales autoridades



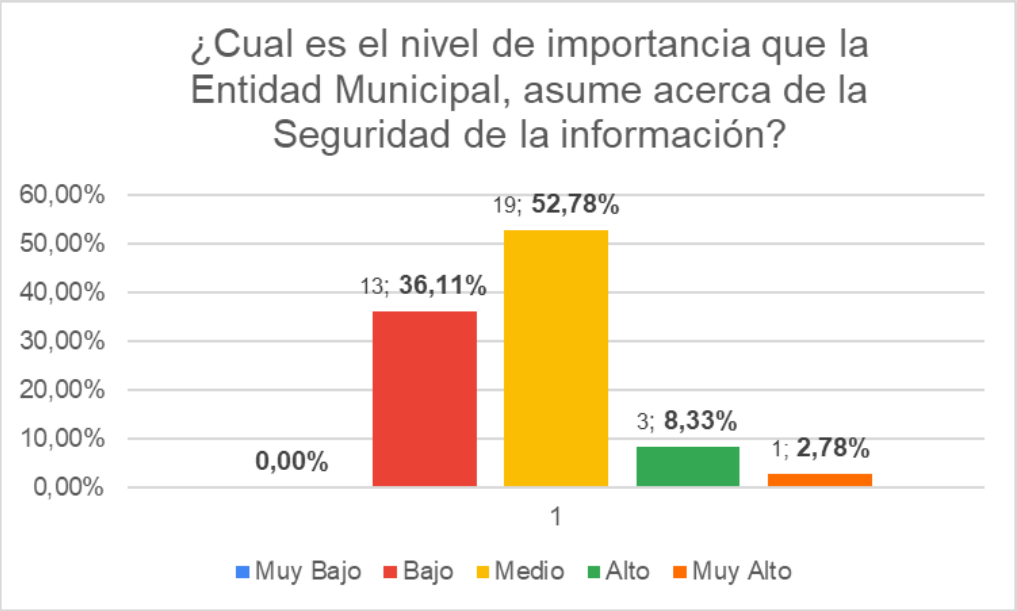
Fuente: Elaboración propia,2022

La frecuencia en la que se proporciona un informe acerca de la situación de seguridad a las principales autoridades de la Entidad Municipal; como se evidencia en la Ilustración 13, los resultados indican (66,67%) indican que se envía un reporte anualmente y (33,33%) indican que nunca. Además los comentarios realizados por parte de los participantes de Encuesta pertenecientes a la Jefatura de Sistemas Informáticos del GAD Municipal La Troncal, revela que en la Entidad Municipal No existe fundamental atención en el área de Sistemas, por lo tanto, los funcionarios actúan conforme los recursos existentes los cuales son limitados, la falta de capacitación, además de la falta de comunicación entre las áreas para la creación de usuarios y la designación de controles conforme a su rol dentro de la institución; evidenciándose vulnerabilidad de la Información.

Preguntas realizadas al personal que opera los Sistemas Informáticos pertenecientes al GAD Municipal La Troncal.

Ilustración 14

Nivel de importancia acerca de la Seguridad de la Información

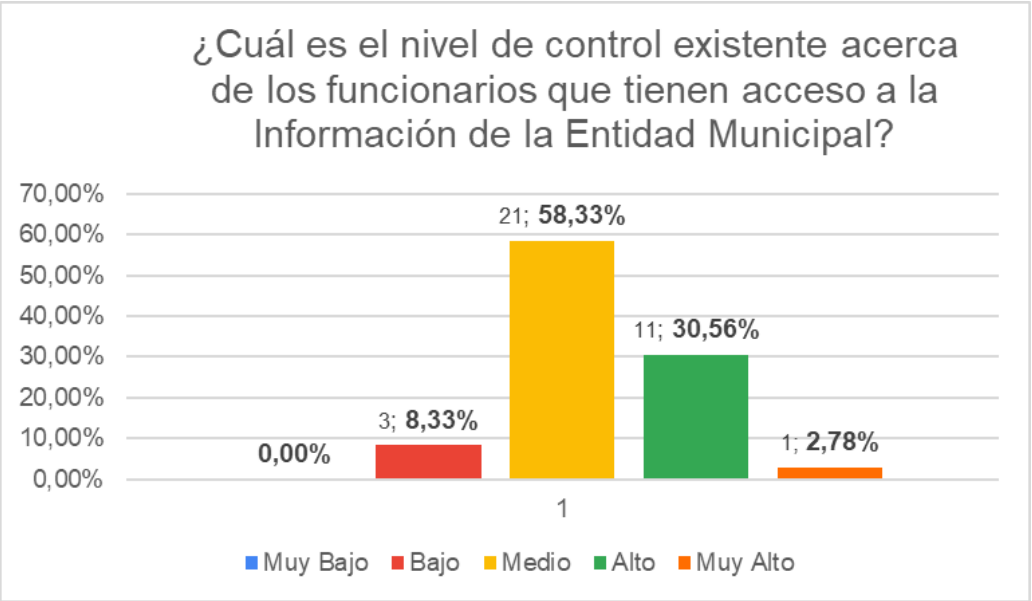


Fuente: Elaboración propia,2022

Como se puede observar en la Ilustración 14, los resultados de los funcionarios indican que el (52,78%) establecen un nivel Medio, (36,11%), indica que se encuentra en nivel Bajo, (8,33%) en nivel Alto y el (2,78%) en nivel Muy Alto.

Ilustración 15

Nivel de Control acerca del acceso a la Información

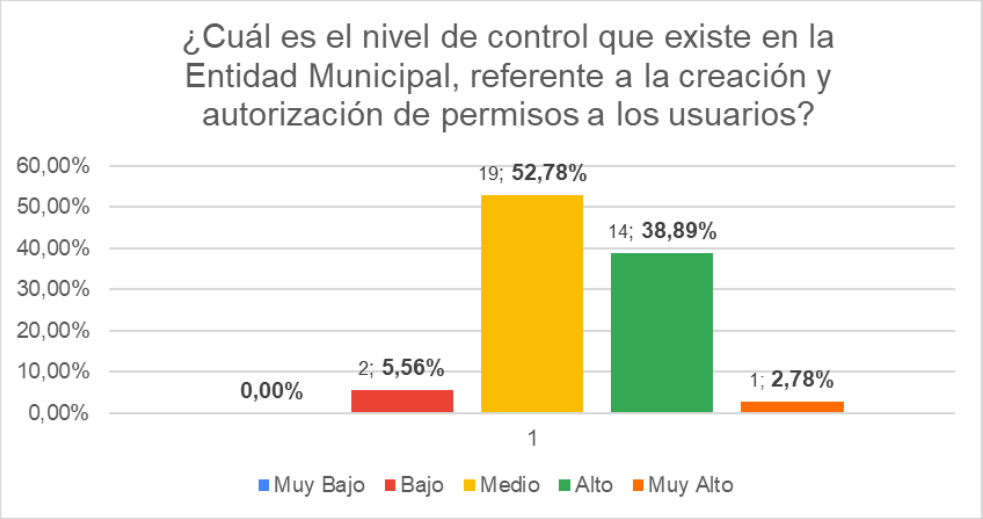


Fuente: Elaboración propia,2022

Referente al nivel de control existente acerca de los funcionarios que tienen acceso a la Información; como se identifica en la Ilustración 15, el (58,33%) establecen que existe un nivel Medio de control, (30,56%) indican que se encuentra en nivel Alto, (8,33%) en nivel Bajo y el (2,78%) en nivel Muy Alto.

Ilustración 16

Nivel de control referente a la creación y autorización de permisos a los usuarios

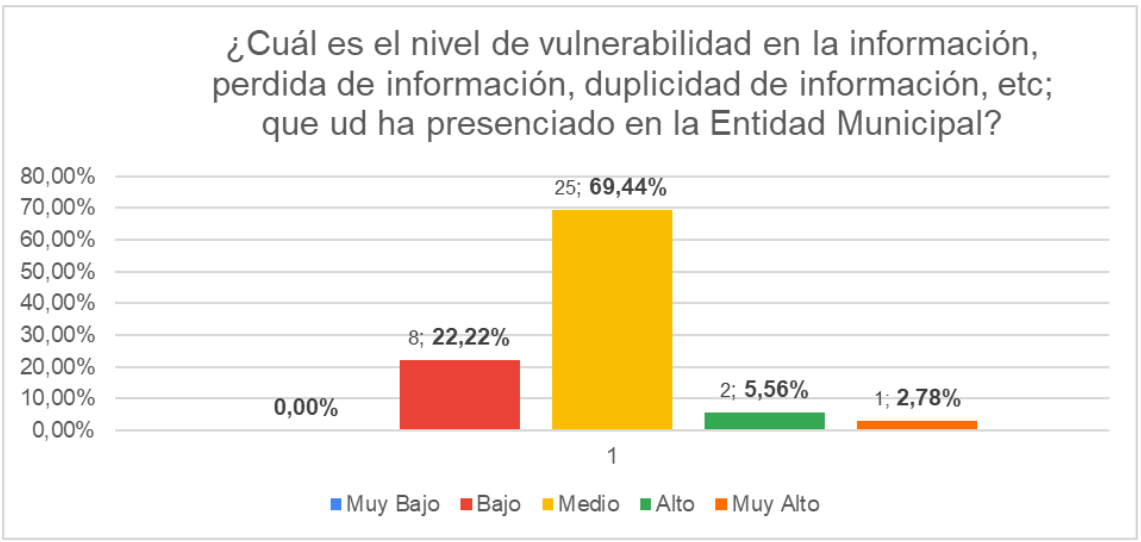


Fuente: Elaboración propia,2022

Referente al nivel de control existente en la Entidad Municipal acerca de la creación y autorización de permisos a los usuarios; los resultados que se aprecian en la Ilustración 16, el (52,78%) indican que existe un nivel Medio de control, (38,89%) se encuentra en nivel Alto, (5,56%) nivel Bajo y el (2,78%) nivel Muy Alto.

Ilustración 17

Nivel de vulnerabilidad en la información



Fuente: Elaboración propia,2022

Los resultados que se aprecian en la Ilustración 17, expresa que el (69,44%) se encuentra en un nivel Medio de control, (22,22%) se encuentra en nivel Bajo, (5,56%) nivel Alto y (2,78%) nivel Muy Alto.

Ilustración 18

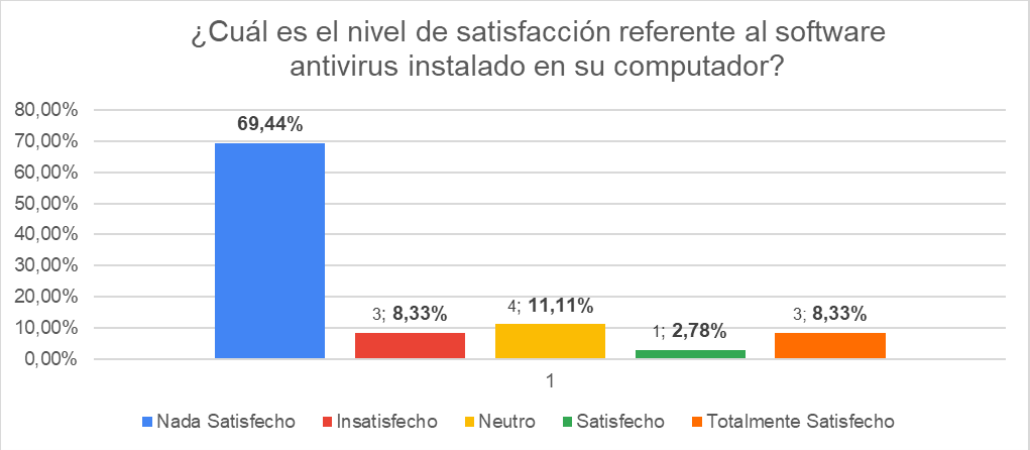
Software antivirus en su PC

Fuente: Elaboración propia,2022

La interrogante realizada acerca del software antivirus instalado en su computador la Ilustración 18, indica que el (66,67%) No tiene software antivirus, el (19,44%) indican que SI y (13,89%) contesta No sé; por lo tanto, sé entiende que los funcionarios desconocen del tema.

Ilustración 19

Nivel de satisfacción referente al Software antivirus instalado

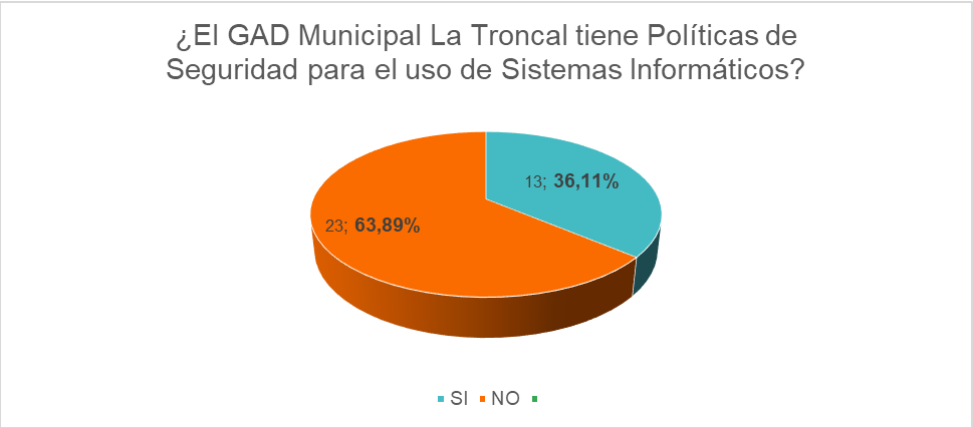


Fuente: Elaboración propia,2022

Como se aprecia en la Ilustración 19, referente al nivel de satisfacción del software antivirus instalado en su computador; el (69,44%) establecen un nivel Nada Satisfecho, (8,33%) indican un nivel Insatisfecho, (11,11%) nivel Neutro, (2,78%) nivel Satisfecho y (8,33%) nivel Totalmente Satisfecho.

Ilustración 20

Políticas de Seguridad

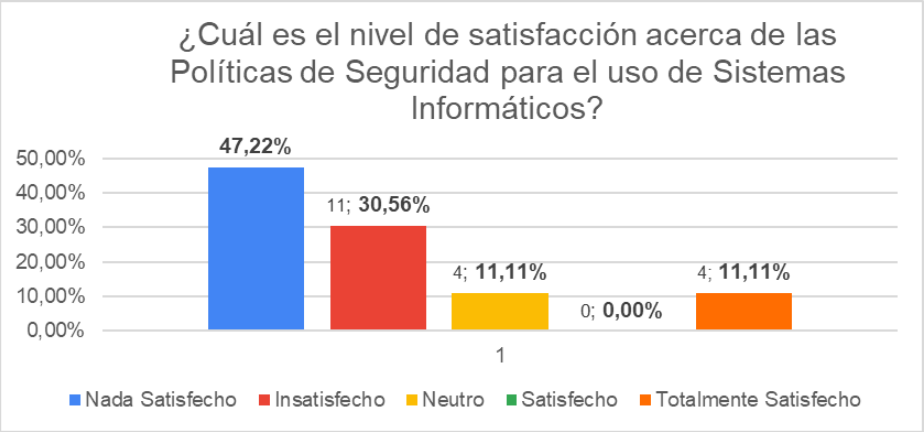


Fuente: Elaboración propia,2022

Como se puede apreciar en la Ilustración 20, referente a las Políticas de Seguridad para el uso de Sistemas Informáticos; los resultados indican que la mayor cantidad de funcionarios (63,89%) indican que No y (36,11%) afirman que Si.

Ilustración 21

Nivel de satisfacción Políticas de Seguridad

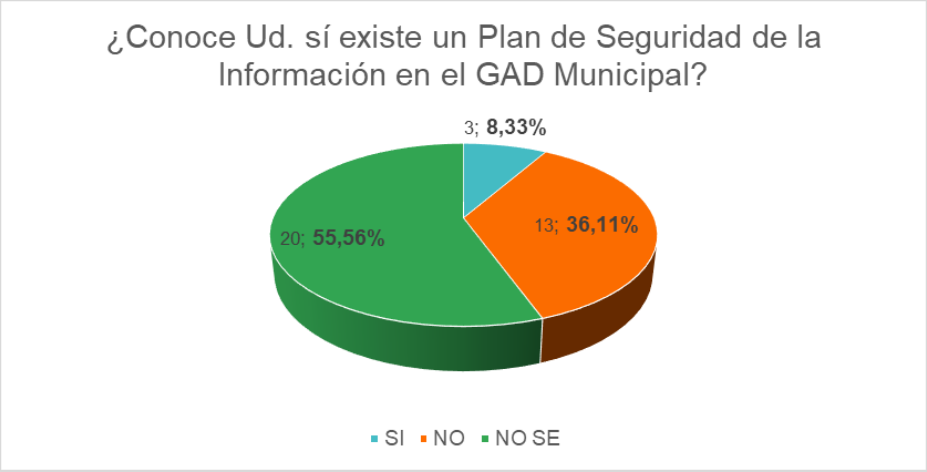


Fuente: Elaboración propia,2022

Como se visualiza en la Ilustración 21, referente al nivel de satisfacción de las Políticas de Seguridad para el uso de Sistemas Informáticos; los resultados indican que el (47,22%) Nada Satisfecho, el (30,56%) Insatisfecho, el (11,11%) Neutro y el (11,11%) afirma Totalmente Satisfecho.

Ilustración 22

Plan de Seguridad de la Información



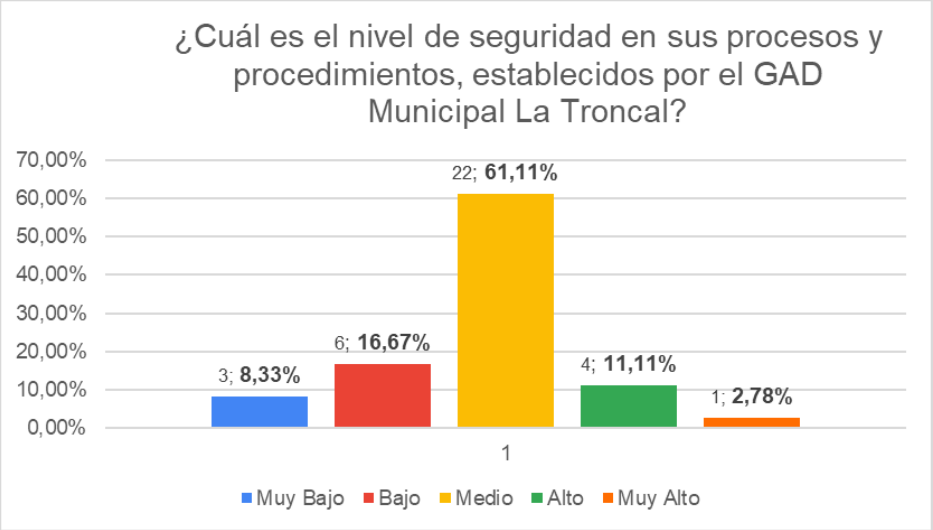
Fuente: Elaboración propia,2022

Los resultados que apreciamos en la Ilustración 22, cuya interrogante

establece si existe un Plan de Seguridad de la Información en el GAD Municipal; los resultados obtenidos indican que el (55,56%) No saben, es decir desconocen del tema, (36,11%) indican que No y (8,33%) afirman que Si.

Ilustración 23

Nivel de seguridad en sus procesos y procedimientos



Fuente: Elaboración propia,2022

Referente al nivel de seguridad en sus procesos y procedimientos, establecidos por el GAD Municipal La Troncal; los resultados que se aprecian en la Ilustración 23 indican que la mayor cantidad de funcionarios (61,11%) establecen que existe un nivel Medio, (16,67%) nivel Bajo, (11,11%) en nivel Alto, (8,33%) en nivel Muy Bajo y (2,78%) en nivel Muy Alto.

Ilustración 24

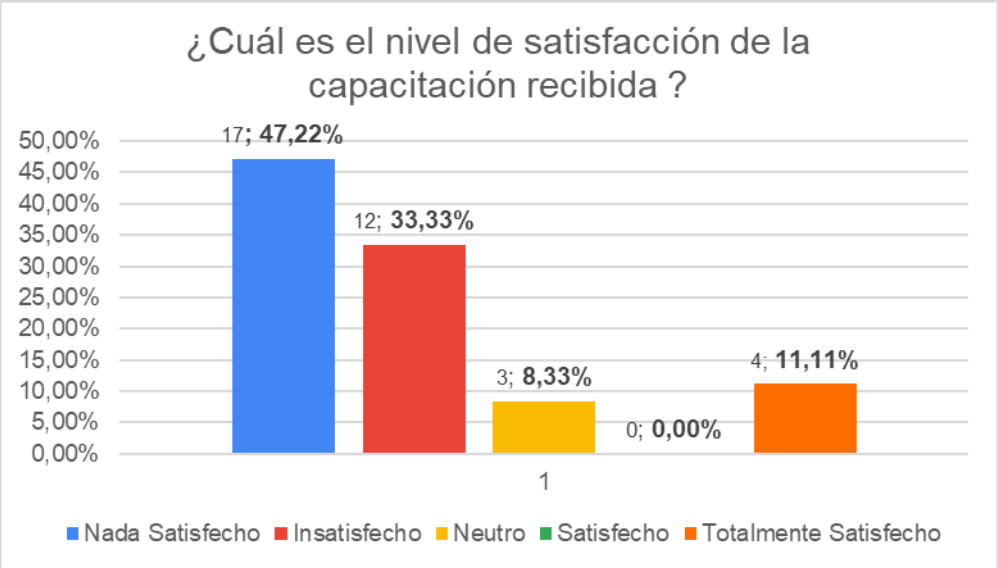
Capacitación acerca del uso de los Sistemas Informáticos

Fuente: Elaboración propia,2022

Los resultados que apreciamos en la Ilustración 24, acerca de la capacitación acerca del uso de los Sistemas Informáticos del GAD Municipal La Troncal; la mayor cantidad de funcionarios (66,67%) indican que No y el (33,33%) afirman que Si.

Ilustración 25

Nivel de satisfacción Capacitación



Fuente: Elaboración propia,2022

Referente al nivel de satisfacción de la capacitación recibida como indica la Ilustración 25; la mayor cantidad de funcionarios (47,22%) establecen un nivel Nada Satisfecho, el (33,33%) nivel Insatisfecho, el (11,11%) Totalmente Satisfecho y el (8,33%) nivel Neutro.

Ilustración 26

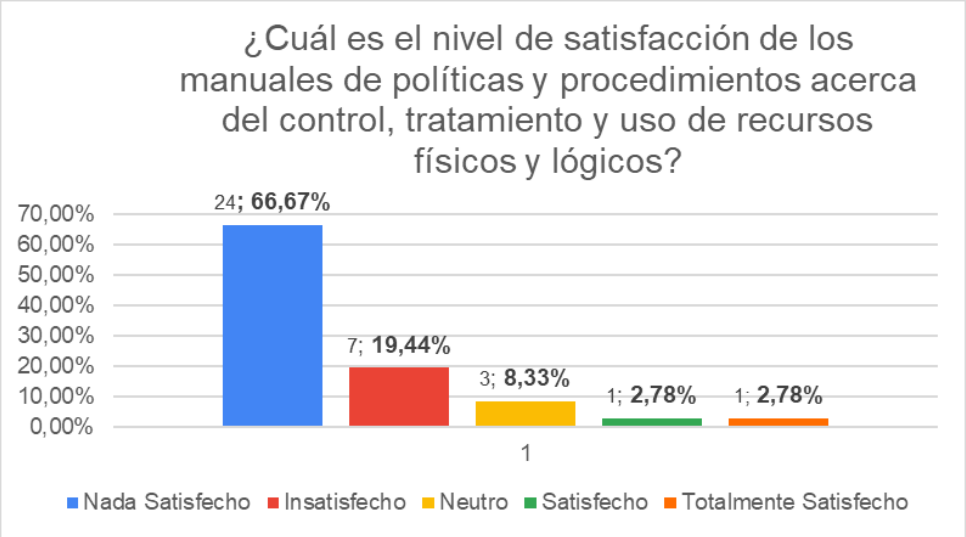
Manual Políticas y procedimientos

Fuente: Elaboración propia,2022

Los resultados que apreciamos en la Ilustración 26; referente a un manual de Políticas y procedimientos indican que la mayor cantidad de funcionarios el (97,22%) afirman que No y el (2,78%) indican que Si.

Ilustración 27

Nivel de Satisfacción Manuales de Políticas y Procedimientos



Fuente: Elaboración propia,2022

Referente al nivel de satisfacción de los manuales de políticas y procedimientos; como apreciamos en la Ilustración 27 los resultados indican que la mayor cantidad de funcionarios (66,67%) establecen un nivel Nada satisfecho, el (19,44%) nivel Insatisfecho, el (8,33%) nivel Neutro, el (2,78%) nivel Satisfecho y el (2,78%) nivel Totalmente Satisfecho.

Una vez que concluyó la etapa de encuestas y en base a los resultados obtenidos en los diversas preguntas realizadas a la Población establecida conforme el detalle de la Tabla 6, se identifica que existen diversas falencias en el Gobierno Autónomo Descentralizado Municipal La Troncal referente a Seguridad de la Información; el mayor porcentaje de la población encuestada no cuentan con Software Antivirus, además la mayoría de funcionarios no ha tenido una capacitación referente al uso de los Sistemas Informáticos pertenecientes al GAD Municipal La Troncal, no cuenta con un manual de procedimientos y no se posee un Plan de Seguridad de la Información

Se realizó un análisis enfocado en el Anexo A de la Norma ISO 27001, adicional, se ha visto la necesidad de profundizar la investigación aplicando Un

análisis de brechas (también conocido como análisis GAP o análisis de necesidades)

Los criterios establecidos en el Anexo A, se encuentran relacionados con Política de Seguridad, gestión de activos, control de acceso, seguridad física y ambiental, seguridad relacionada con el personal (Ramos et al., 2017)

2.4. Controles del Anexo A ISO 27001

Un análisis del Anexo A establecido por la Norma ISO 27001, pretende identificar una visión completa de las vulnerabilidades de la información del GAD Municipal La Troncal. El objetivo de esta etapa es identificar las inseguridades no admisibles en base a los controles del Anexo A.

Se procede a realizar una verificación conforme a lo que establece el Anexo A de la Norma ISO 27001, referente al estado de cada Jefatura en presente proyecto de investigación donde se empleó la escala de Likert (1-muy bajo, 2-bajo, 3-medio, 4-alto y 5 muy alto).

Tabla 8

Políticas de Seguridad de la Información

A5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Política de control de acceso	MEDIO	MEDIO	MEDIO	MEDIO
Política de clasificación y manejo de la información	BAJO	BAJO	BAJO	MEDIO
Política de seguridad física y ambiental	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO
Política de copia de seguridad	MEDIO	MEDIO	MEDIO	MEDIO
Política de transferencia de información	MEDIO	MEDIO	BAJO	BAJO

Política de protección contra software malicioso	BAJO	BAJO	MUY BAJO	MUY BAJO
Política de gestión de vulnerabilidades	BAJO	BAJO	MUY BAJO	BAJO

Fuente: Elaboración Propia, 2022

Los controles A5 Políticas de Seguridad de la Información, proporciona una orientación y soporte para la seguridad de la información, de acuerdo con los requisitos de la institución, la regularización y normativa legal vigente.

Este control solicita que se definan políticas de la seguridad de la información, las cuales deben ser aprobadas por la Máxima Autoridad de la Entidad, adicionalmente deben estar publicadas y socializadas a los funcionarios. Deben publicarse y comunicarse a los empleados y partes externas pertinentes, definir las responsabilidades de cada empleado o puesto de trabajo en relación a la Seguridad de la Información; es decir para cumplir con este control bastaría con sumar a las funciones de cada puesto aquellas que tengan que ver con la Seguridad de la Información

Tabla 9

Organización de la Seguridad de la Información

A6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Funciones y responsabilidades de la Seguridad de la información	MEDIO	MEDIO	BAJO	MEDIO
Separación de funciones	MEDIO	BAJO	BAJO	MEDIO
Contacto con autoridades	BAJO	BAJO	MEDIO	MEDIO
Contacto con grupos de interés especial	MEDIO	MEDIO	MEDIO	BAJO
Seguridad de la información en la gestión de proyectos	BAJO	BAJO	BAJO	BAJO
Política de dispositivos móviles	MUY BAJO	MEDIO	MUY BAJO	MEDIO
Teletrabajo	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO

Fuente: Elaboración Propia, 2022

Se debe definir las responsabilidades de cada empleado o puesto de trabajo en relación a la Seguridad de la Información (control de las funciones de cada puesto). Además, se debe comunicar a cada funcionario implicado sus roles y responsabilidades. Evitar usos o accesos ilícito a la información o los sistemas que la gestionan (activos de información) mediante la separación de las funciones asignando distintos perfiles de acuerdo a su rol en la institución.

Este control procura exponer que la Seguridad de la Información debe involucrarse en todos los procesos de una institución en sus diversos ámbitos.

Tabla 10

Seguridad Relativa a los recursos

A7 SEGURIDAD RELATIVA A LOS RECURSOS	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Selección	BAJO	BAJO	BAJO	BAJO
Términos y condiciones de empleo	BAJO	BAJO	BAJO	BAJO
Responsabilidades de la dirección	MEDIO	MEDIO	BAJO	MEDIO
Concientización, educación y formación en seguridad de la información	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO
Proceso disciplinario	BAJO	BAJO	BAJO	BAJO
Responsabilidades en la desvinculación	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO

Fuente: Elaboración Propia, 2022

Como se puede apreciar en la Tabla No. 10, establece controles previos al empleo, durante el empleo y en el caso de Finalización o cambio de relación laboral.

La Norma propone una serie de disposiciones para la evaluación previa a la selección del personal, adicional se establece obligaciones y responsabilidades ligadas a la Seguridad de la Información, además de acuerdos de confidencialidad o de no divulgación previo a la asignación de permisos para acceder a la información.

Durante la etapa contractual la norma nos brinda algunas indicaciones referentes a la formación y sensibilización del personal referente al tema de Seguridad de la Información. En el caso de finalización o cambio de relación laboral, este control trata de establecer y comunicar al empleado las responsabilidades sobre la Seguridad de la Información y el compromiso de respetar los acuerdos de confidencialidad.

Tabla 11

Gestión de Activos

A8 GESTION DE ACTIVOS	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Inventario de activos	MEDIO	MEDIO	MEDIO	MEDIO
Propiedad de los activos	MEDIO	MEDIO	MEDIO	MEDIO
Uso aceptable de los activos	BAJO	BAJO	BAJO	BAJO
Devolución de activos	MEDIO	MEDIO	MEDIO	MEDIO
Clasificación de la información	BAJO	MUY BAJO	MUY BAJO	BAJO
Etiquetado de la información	BAJO	BAJO	BAJO	BAJO
Manejo de los activos	BAJO	BAJO	MUY BAJO	MEDIO
Gestión de Soportes extraíbles	BAJO	BAJO	BAJO	BAJO
Eliminación de Soportes	BAJO	MEDIO	BAJO	MEDIO
Traslado de soportes físicos	MEDIO	MEDIO	BAJO	BAJO

Fuente: Elaboración Propia, 2022

Los controles que se observan la Tabla 11 se enfatizan en la responsabilidad hacia los activos, la clasificación de la información y el Manejo de los Soportes.

Se propone identificar los activos de información (Clasificar los activos por su importancia, por el tipo de activo o información e Identificar al propietario del activo) y las responsabilidades sobre los mismos

Tabla 12

Control de Acceso

A9 CONTROL DE ACCESO	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Política de control de acceso	MEDIO	BAJO	MEDIO	MEDIO
Acceso a las redes y a los servicios de red	MEDIO	MEDIO	MEDIO	MEDIO
Registro de usuarios y cancelación del registro	MEDIO	MEDIO	MEDIO	MEDIO
Gestión de acceso a los usuarios	MEDIO	MEDIO	MEDIO	MEDIO
Gestión de derechos de acceso privilegiados	MEDIO	MEDIO	MEDIO	MEDIO
Gestión de la información de autenticación secreta de los usuarios	MEDIO	MEDIO	MEDIO	MEDIO
Revisión de derechos de acceso de usuario	BAJO	BAJO	BAJO	BAJO
Remoción o ajuste de los derechos de acceso	BAJO	MEDIO	BAJO	MEDIO
Uso de la información de autenticación secreta	BAJO	BAJO	BAJO	BAJO
Restricción de acceso a la información	MEDIO	MEDIO	MEDIO	MEDIO
Procedimientos de conexión (log-on) seguros	MEDIO	MEDIO	MEDIO	MEDIO
Sistema de gestión de contraseñas	MEDIO	MEDIO	MEDIO	MEDIO
Uso de programas de utilidad privilegiados	BAJO	BAJO	BAJO	BAJO
Control de acceso al código de programas fuente	MEDIO	MEDIO	MEDIO	MEDIO

Fuente, Elaboración Propia, 2022

Como se aprecia en la Tabla 12, presenta el detalle de los Controles de Acceso, cuyos 4 objetivos establecen limitaciones en el acceso a la información y a las instalaciones donde se procesa la misma, garantizando el acceso a usuarios autorizados y prevenir el acceso a intrusos; fomentar la responsabilidad a los funcionarios con la finalidad de salvaguardar la información

Tabla 13

Criptografía

A10 CRIPTOGRAFIA	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Política sobre el empleo de controles criptográficos	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO
Gestión de claves	MEDIO	MEDIO	MEDIO	MEDIO

Fuente, Elaboración Propia, 2022

Como se observa en la Tabla 13, indica las medidas de control para el uso eficaz de la criptografía, cuyo objetivo es proteger la confidencialidad e integridad de la información; los controles criptográficos están enfocados en la seguridad de la información en el caso de que un advenedizo pueda tener acceso físico a la información.

Tabla 14

Seguridad física y del entorno

A11 SEGURIDAD FISICA Y DEL ENTORNO	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Perímetro de seguridad física	BAJO	BAJO	BAJO	BAJO
Controles de acceso físico	MEDIO	MEDIO	BAJO	BAJO
Seguridad de oficinas, despachos e instalaciones	MEDIO	MEDIO	BAJO	BAJO
Protección contra amenazas externas y del ambiente	BAJO	BAJO	BAJO	BAJO
El trabajo en las áreas seguras	BAJO	BAJO	MEDIO	MEDIO

Áreas de entrega y de carga	BAJO	MEDIO	MEDIO	MEDIO
Ubicación y protección del equipamiento	BAJO	MEDIO	MEDIO	MEDIO
Elementos de soporte	BAJO	BAJO	BAJO	BAJO
Seguridad en el cableado	MEDIO	BAJO	BAJO	BAJO
Mantenimiento del equipamiento	MEDIO	MEDIO	MEDIO	MEDIO
Retiro de bienes	MEDIO	MEDIO	MEDIO	MEDIO
Seguridad del equipamiento y de los activos fuera de las instalaciones	BAJO	BAJO	BAJO	BAJO
Seguridad en la reutilización o eliminación de equipos	BAJO	BAJO	MEDIO	MEDIO
Equipamiento desatendido por el usuario	MEDIO	MEDIO	MEDIO	MEDIO
Política de escritorio y pantalla limpios	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO

Fuente, Elaboración Propia: 2022

La Tabla 14 expresa las medidas control físicas óptimas para proteger los activos de información, y así evitar incidentes que afecten a la integridad física de la información, tales como accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de datos e información de la institución. Prevenir extravío, deterioro, robos o cualquier inconveniente que afecte a los activos, así como la suspensión de las actividades de la organización

Tabla 15

Seguridad de las operaciones

A12 SEGURIDAD DE LAS OPERACIONES	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Procedimientos documentados de operación	ALTO	ALTO	MEDIO	ALTO
Gestión de cambios	ALTO	ALTO	MEDIO	MEDIO
Gestión de la capacidad	MEDIO	MEDIO	MEDIO	MEDIO
Separación de los ambientes para desarrollo, prueba y operación	BAJO	MEDIO	BAJO	BAJO
Controles ante software malicioso	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO

Respaldo de la información	MEDIO	MEDIO	MEDIO	MEDIO
Registro de eventos	ALTO	ALTO	ALTO	ALTO
Protección de la información de registros (logs)	ALTO	ALTO	ALTO	ALTO
Registros del administrador y operador	ALTO	ALTO	ALTO	ALTO
Sincronización de relojes	ALTO	ALTO	ALTO	ALTO
Instalación de software en los sistemas operativos	MEDIO	MEDIO	MEDIO	MEDIO
Gestión de vulnerabilidades técnicas	ALTO	ALTO	ALTO	ALTO
Restricciones en la instalación de software	MEDIO	MEDIO	MEDIO	MEDIO
Controles de auditoría de sistemas de información	MEDIO	MEDIO	MEDIO	MEDIO

Fuente: Elaboración Propia, 2022

La Tabla 15 contiene una serie de controles enfocados en el análisis de riesgos para la seguridad de la información, cuyo enfoque se encuentra en asegurar la operación correcta y segura de las instalaciones de procesamiento de información; además de registrar eventos y generar evidencia de los mismos, garantizar la integridad de los sistemas Operativos, gestión de la vulnerabilidad técnica y considerar una auditoria de Sistemas de información.

Tabla 16

Seguridad en las comunicaciones

A13 SEGURIDAD EN LAS COMUNICACIONES	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Controles de Red	MEDIO	MEDIO	MEDIO	MEDIO
Seguridad de los servicios de red	MEDIO	MEDIO	MEDIO	MEDIO
Separación en redes	MEDIO	MEDIO	BAJO	MEDIO
Políticas y procedimientos de intercambio de información	BAJO	BAJO	BAJO	BAJO

Acuerdos de intercambio de información	BAJO	BAJO	BAJO	BAJO
Mensajería electrónica	MEDIO	MEDIO	MEDIO	MEDIO
Acuerdos de confidencialidad y de no divulgación	BAJO	BAJO	BAJO	BAJO

Fuente: Elaboración Propia, 2022

Como se detalla en la Tabla 16, indica los controles enfocados en la Seguridad en las comunicaciones. En la actualidad información viaja por la red de comunicaciones de cualquier institución, por ello es recomendable establecer los controles óptimos para proteger tanto las comunicaciones externas de la institución, así como las que viajan a través de las redes propias.

Tabla 17

Adquisición, desarrollo y mantenimiento en los sistemas de Información

A14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Análisis y especificación de los requisitos de seguridad	MEDIO	MEDIO	MEDIO	MEDIO
Aseguramiento de los servicios de aplicación en las redes públicas	MEDIO	MEDIO	MEDIO	MEDIO
Transacciones en línea	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO
Política de desarrollo seguro	ALTO	ALTO	ALTO	ALTO
Procedimiento de control de cambio del sistema	ALTO	ALTO	ALTO	ALTO
Revisión técnica de aplicaciones luego de haber realizado cambios en las plataformas operativas	ALTO	ALTO	ALTO	ALTO

Restricciones a los cambios en los paquetes de software	MEDIO	MEDIO	MEDIO	MEDIO
Principios de la ingeniería de Sistemas Seguros	MEDIO	MEDIO	MEDIO	MEDIO
Ambiente de desarrollo seguro	MEDIO	MEDIO	MEDIO	MEDIO
Desarrollo subcontratado	BAJO	BAJO	BAJO	BAJO
Pruebas de seguridad del sistema	MEDIO	MEDIO	MEDIO	MEDIO
Pruebas de aceptación del sistema	MEDIO	MEDIO	MEDIO	MEDIO
Protección de datos de prueba	MEDIO	MEDIO	MEDIO	MEDIO

Fuente: Elaboración Propia, 2022

La Tabla 17 detalla los controles sobre el ciclo de vida completo de los Sistemas de Información, propios como subcontratados. Se enfoca en la Seguridad en los procesos de desarrollo y soporte, además de garantizar la protección de los datos utilizados para las pruebas.

Tabla 18

Relación con proveedores

A15 RELACION CON PROVEEDORES	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Política de seguridad de la información para las relaciones con los proveedores	BAJO	BAJO	BAJO	BAJO
Tener en cuenta la seguridad en los acuerdos con proveedores	MEDIO	MEDIO	MEDIO	MEDIO
Cadena de suministro de tecnologías de la información y las comunicaciones	MEDIO	MEDIO	MEDIO	MEDIO
Seguimiento y revisión de los servicios de proveedores	BAJO	BAJO	BAJO	BAJO
Gestión de cambios en los servicios de los proveedores	BAJO	BAJO	BAJO	BAJO

Fuente, Elaboración Propia, 2022

Como se observa en la Tabla 18 sugiere que es necesario establecer condiciones para el para el uso de activos de la institución, además de supervisar el cumplimiento de dichas condiciones, para la protección de los Sistemas de Información o a los recursos que manejan activos de información, procurando mantener un nivel apropiado de Seguridad de la Información y que la entrega del servicio se realice acorde con los acuerdos establecidos.

Tabla 19

Gestión de incidentes de la seguridad de la información

A16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Responsabilidades y procedimientos	MEDIO	MEDIO	BAJO	BAJO
Reporte de eventos de seguridad de la información	ALTO	ALTO	ALTO	ALTO
Reporte de debilidades de seguridad de la información	MEDIO	MEDIO	MEDIO	MEDIO
Evaluación y decisión sobre los eventos de seguridad de información	MEDIO	BAJO	BAJO	BAJO
Respuesta a incidentes de seguridad de la información	MEDIO	MEDIO	MEDIO	MEDIO
Aprendiendo de los incidentes de seguridad de la información	MEDIO	MEDIO	MEDIO	MEDIO
Recolección de evidencia	BAJO	BAJO	BAJO	BAJO

Fuente: Elaboración Propia, 2022

Los controles detallados en la Tabla 19, se enfoca en la gestión de incidentes de la seguridad de la Información, garantizando un enfoque consistente y eficaz.

La Gestión de incidentes de seguridad se basa en diferentes pasos que

incluyen:

- Incidente Notificado
- Incidente Clasificado
- Incidente en tratamiento
- Incidente Solucionado
- Base de Conocimientos

Es importante implantar y documentar los procedimientos, además de informar al usuario sobre cualquier cambio en el estado del incidente.

Tabla 20

Aspectos de seguridad de la información en la gestión de continuidad del negocio

A17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Planificación de la continuidad de la seguridad de la información.	MEDIO	MEDIO	MEDIO	MEDIO
Implementación de la continuidad de la seguridad de la información.	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO
Verificar, revisar y evaluar la continuidad de la seguridad de la información.	BAJO	BAJO	BAJO	BAJO
Disponibilidad de las instalaciones de procesamiento de información.	BAJO	BAJO	BAJO	BAJO

Fuente: Elaboración Propia, 2022

Como se aprecia en la Tabla 20, los controles se enfocan en implantar medidas de protección y de recuperación ante posibles desastres naturales para minimizar los perjuicios en la institución y facilitar el restablecimiento de sus operaciones. Mantener un plan de continuidad o recuperación ante incidentes para precautelar la Seguridad de la Información, garantizando la disponibilidad de las instalaciones para el procesamiento de información.

Los planes de continuidad contemplan el análisis de las necesidades y riesgos de una organización, es decir va más allá de lo que establece un plan de contingencia.

Tabla 21
Cumplimiento

A18 CUMPLIMIENTO	JEFATURA DE RECAUDACION	JEFATURA DE RENTAS	AVALUOS Y CATASTROS	CONTROL URBANO
Identificación de la legislación aplicable y de los requisitos contractuales	BAJO	BAJO	BAJO	BAJO
Derechos de propiedad intelectual (/PR)	MEDIO	MEDIO	MEDIO	MEDIO
Protección de los registros	ALTO	ALTO	MEDIO	MEDIO
Protección de los datos y privacidad de la información personal	ALTO	ALTO	ALTO	ALTO
Regulación de los controles criptográficos	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO
Revisión independiente de la Seguridad de la Información	BAJO	BAJO	BAJO	BAJO
Cumplimiento de la política y las normas de seguridad	BAJO	BAJO	BAJO	BAJO

Revisión del cumplimiento técnico	MEDIO	MEDIO	MEDIO	MEDIO

Fuente, Elaboración Propia, 2022

La Tabla 21 indica los controles que permitan garantizar el cumplimiento con las políticas, normas y legislación aplicable enfocándose sobre todo a la Seguridad de la Información.

CAPÍTULO 3

3.1. Propuesta de solución

3.2. Plan de Seguridad basado en la Norma ISO 270001 para el GAD Municipal La Troncal

3.2.1. Antecedentes

El Gobierno Autónomo Descentralizado Municipal La Troncal, en base creciente avance tecnológico en los últimos años y en vista de los ataques informáticos que han afectado a diversas instituciones públicas y privadas a nivel nacional. Busca de salvaguardar su activo primordial (la información institucional).

Con la aprobación brindada por la Máxima Autoridad del GAD Municipal La Troncal, se procedió a realizar un levantamiento de información a través de la Metodología MAGERIT, la encuesta y el análisis del Anexo A que indica la Norma ISO 27001; todo enfocado en las áreas de: Jefatura de Recaudación, Jefatura de Rentas, Avalúos y Catastros y Control Urbano; con la finalidad de determinar los parámetros esenciales para realizar un Plan de Seguridad Informática.

3.2.2. Objetivo

Realizar un Plan de Seguridad basado en la Norma ISO 27001, que facilite la organización, dirección y control de las actividades ejecutadas en la institución, garantizando su correcto desenvolvimiento, la integridad física de los activos informáticos y preservando la información del GAD Municipal de La Troncal. Sensibilizar e involucrar al personal del perteneciente a la Entidad Municipal para que cumpla con el proceso de seguridad, agilizando la aplicación de los controles conforme a los parámetros establecidos en el documento.

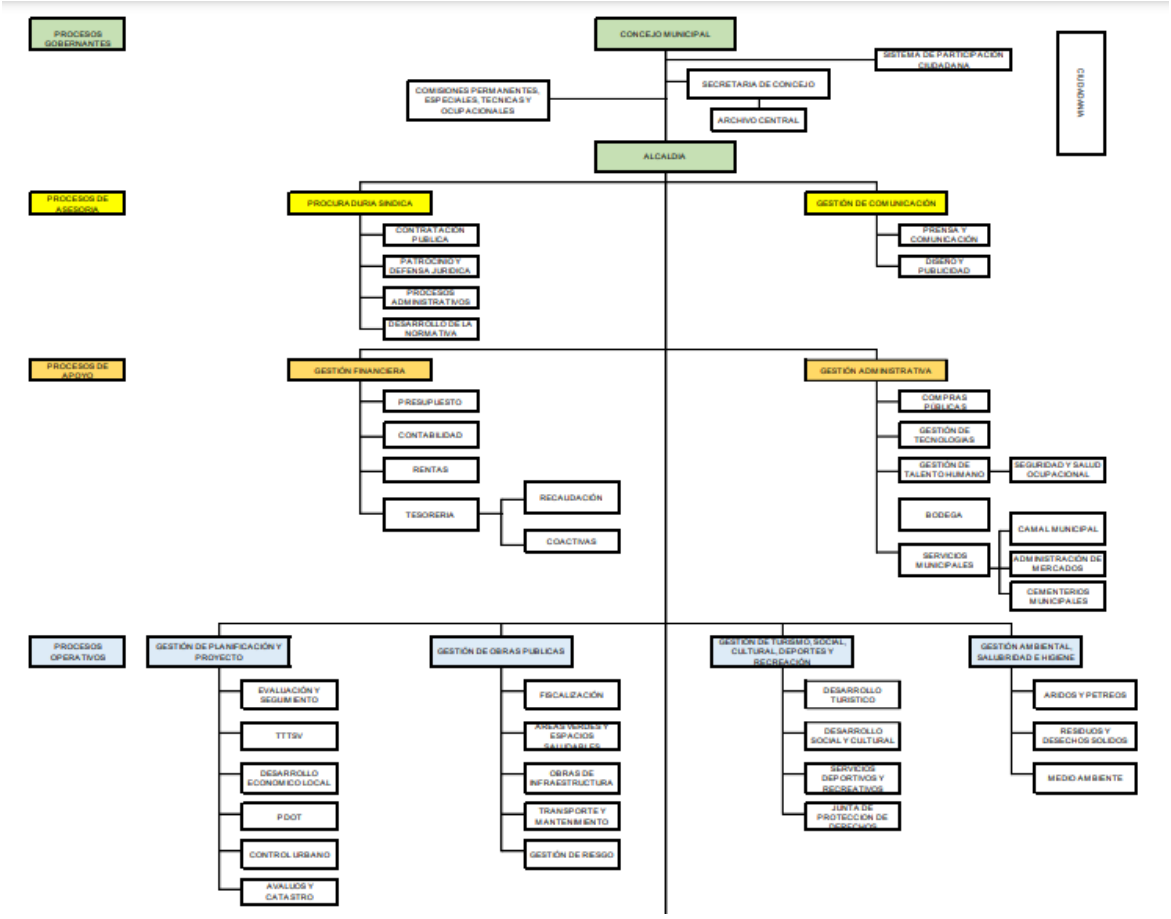
3.2.3. Alcance

El presente Plan de Seguridad Informática permitirá controlar los Riesgos de Seguridad y Privacidad de la Información, además de proporcionar los instrumentos necesarios para identificar, analizar, evaluar y solventar de manera adecuada los riesgos asociados a la operatividad y funcionalidad de la información del Gobierno Autónomo Descentralizado Municipal La Troncal.

3.2.4. Estructura Organizacional

Ilustración 28

Estructura Organizacional GAD Municipal La Troncal



Fuente: GAD Municipal La Troncal,2022

Como se aprecia en la Ilustración 28, se detalla la Estructura Organizacional del Gobierno Autónomo Descentralizado del Cantón La Troncal, se evidencia que la institución consta de diversas áreas; pero para el presente estudio nos enfocaremos en la Jefatura de Recaudación, Jefatura de Rentas, Avalúos y Catastros y Control Urbano.

3.2.5. Ámbito de Aplicación

Este Plan de Seguridad es adaptado al Gobierno Autónomo Descentralizado Municipal del Cantón La Troncal, Provincia del Cañar.

3.2.5. Requisitos de calidad aplicable

Este Plan de Seguridad para el GAD Municipal de La Troncal, da cumplimiento

a lo que establece la Norma ISO 27001.

3.2.6. Definiciones

La terminología utilizada en el presente documento ésta acorde a lo que indica la Norma ISO 27001.

Impacto: se refiere el daño que sufrir el valor del activo en el caso de materializarse una amenaza.

Riesgo: En la seguridad de la Información se refiere a la amenaza que detona una vulnerabilidad que puede causar daño a uno o varios activos.

Evasión del Riesgo: Consiste en prevenir cualquier actividad que pueda involucrar un riesgo

Comunicar el riesgo: Se refiere al intercambio de información de manera inmediata, sobre cualquier riesgo que se presente en la institución, teniendo como prioridad la comunicación.

Estimación del Riesgo: se define como análisis de la vulnerabilidad como resultado de un riesgo potencialmente identificado.

Identificación del riesgo: Es el proceso de gestión de riesgos en la que se percata de lo ocurrido en la institución y las consecuencias sobre los objeticos de la institución.

Reducción del riesgo: este proceso busca rectificar las condiciones de riesgo existentes y evitar uno nuevo.

Retención del riesgo: esta estrategia consiste en la aceptación de un riesgo, aceptando las pérdidas que pudiese ocasionar.

Tratamiento del Riesgo: se refiere a las decisiones tomadas en relación a cada activo de información. Estas decisiones se realizan en base al siguiente análisis: evitar el riesgo, aceptar el riesgo, reducir el riesgo, transferir el riesgo

Autenticidad: Se refiere a que una entidad es quien certifica el origen de su información.

Confiabilidad de la Información: Asegura que la procedencia de la información obtenida sea adecuada para una resolución segura, ejecución de trabajos y responsabilidades.

Confidencialidad: Se refiere a restringir el acceso a la información a individuos, entidades o procesos no autorizados.

Disponibilidad: la información debe ser accesible, permitiendo acceder a ella cuando la organización lo requiera conveniente.

Declaración de Aplicabilidad: Enumera los controles aplicados por el SGSI de la institución luego del resultado de los procesos de evaluación, tratamiento de riesgos y su justificación de controles del anexo A de la Norma ISO 27001.

Sistema de Gestión de la Seguridad de la Información: Un SGSI consiste en un conjunto de políticas, procedimientos y directrices conjuntamente con los recursos y actividades que son administrados por una organización, para la protección de sus activos e información esenciales.

Vulnerabilidad: Se define como una debilidad o fallo en un sistema de información, lo que provoca un riesgo la seguridad de la información, ocasionando que la institución se encuentre indefensa ante un atacante y comprometa la integridad, disponibilidad o confidencialidad.

3.2.7. Políticas de Seguridad.

Las políticas se determinan en base a los procesos, la gestión de los activos, el personal, seguridad operativa, física y ambiental, telecomunicaciones, proveedores, sobre todo basado en la gestión de la información y para ello se recomienda hacerlo mediante un análisis con la ISO 27001.

La Seguridad Informática ha tomado gran importancia, ante los riesgos que se enfrentan la Entidad, como consecuencia ha llevado al desarrollo de este documento de directrices que orientan el uso adecuado de las tecnológicas y brindar recomendaciones para obtener un mayor beneficio.

Las políticas de seguridad informática provienen del análisis de los riesgos a los que se encuentra vulnerable el GAD Municipal La Troncal, se manifiestan como una guía organizacional para sensibilizar a los funcionarios sobre la importancia y sensibilidad de la información con la finalidad de progresar y mantenerse competitivo.

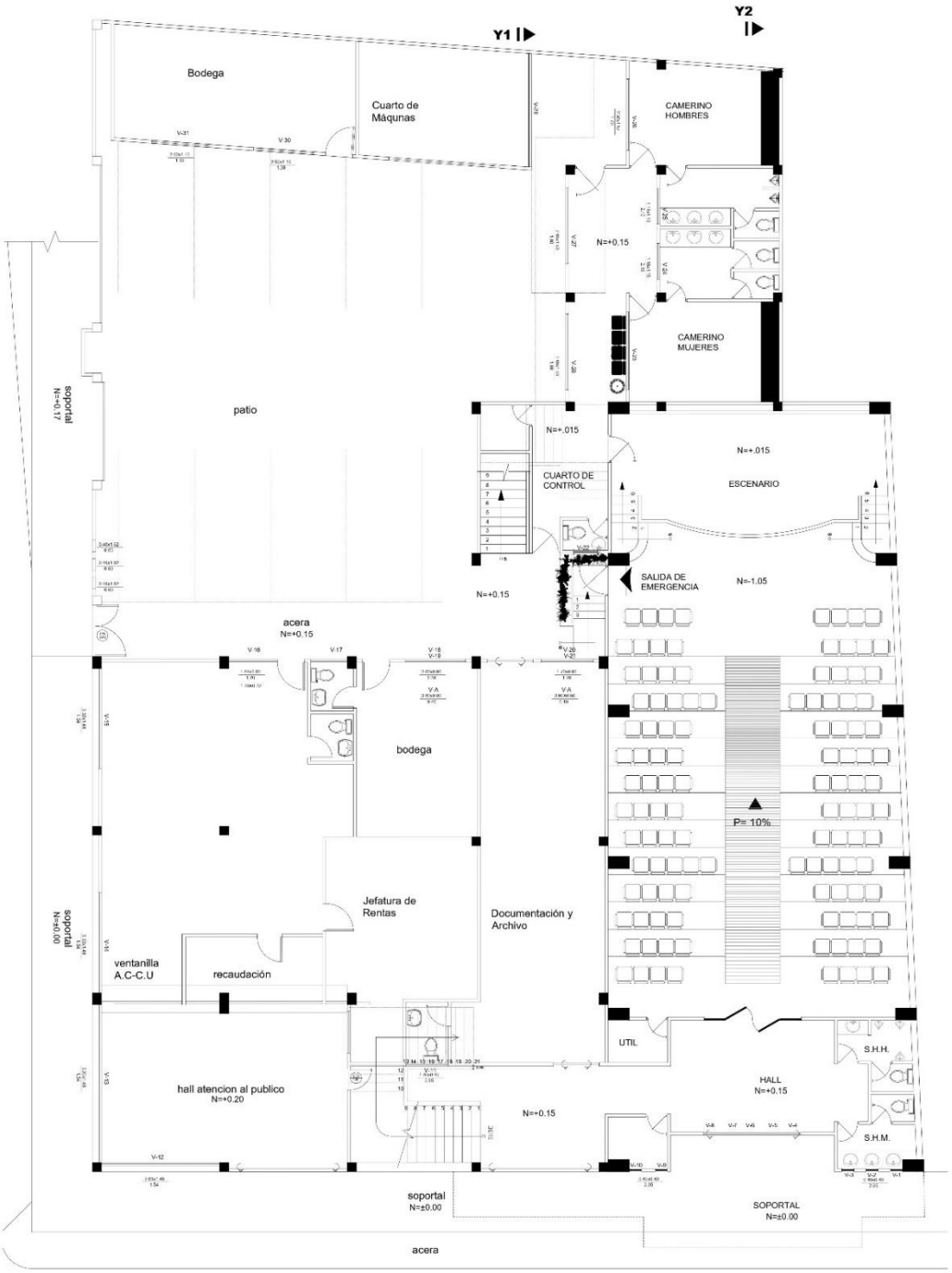
3.2.8. Alcance de las Políticas

El desarrollo de las políticas de seguridad, se realizó conforme al análisis de riesgos y vulnerabilidades correspondientes a las Jefaturas de Recaudación, Rentas, Avalúos y Catastros y Control Urbano, pertenecientes al GAD Municipal La Troncal.

Planos Estado Actual Oficinas GAD Municipal La Troncal

Ilustración 29

Plano Planta Baja Oficinas GAD La Troncal



PLANTA BAJA

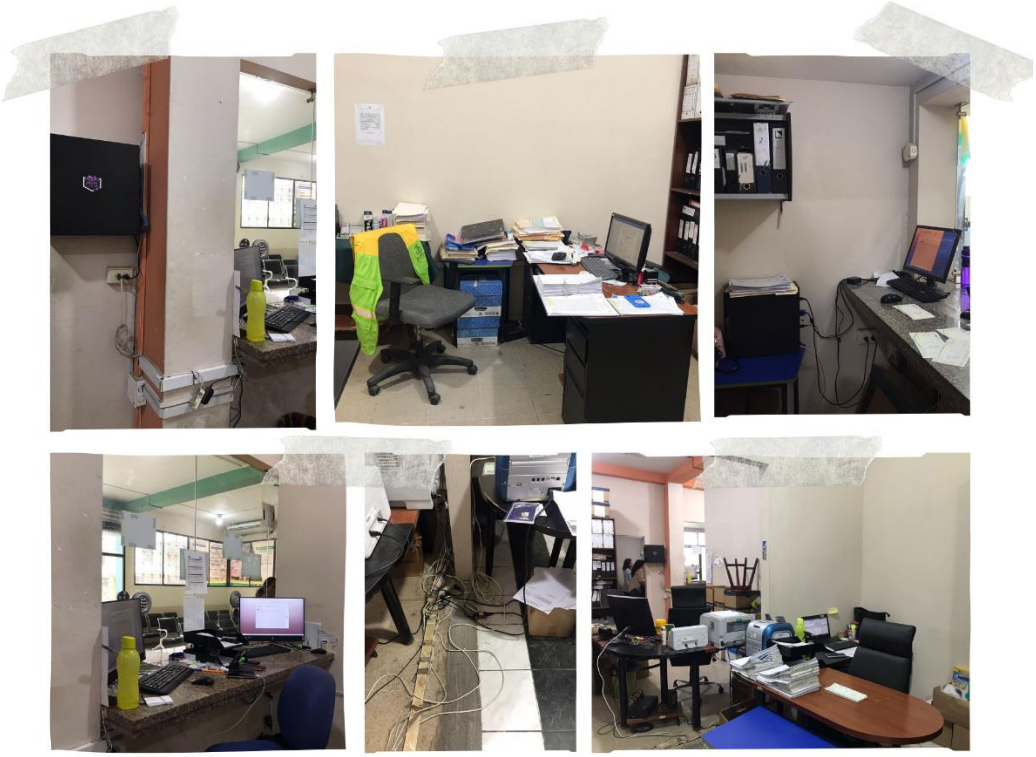
Fuente: GAD Municipal La Troncal,2022

En la Ilustración 29 se observa un plano correspondiente a la distribución

actual de las oficinas correspondientes a la Jefatura de Recaudación, Jefatura de Rentas, Avalúos y Catastros y Control Urbano. Adicional detallo ilustraciones correspondientes al estado físico de las mismas.

Ilustración 30

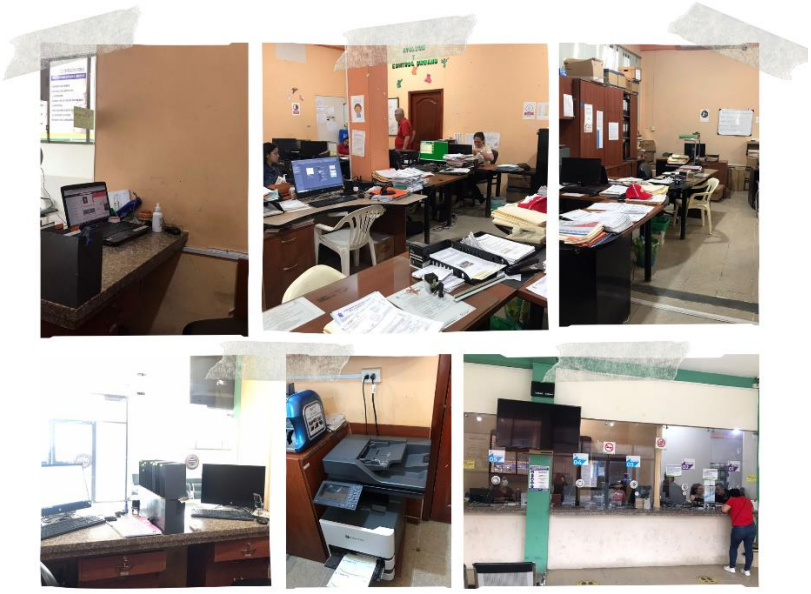
Jefatura de Recaudación y Jefatura de Rentas



Fuente: Elaboración propia,2022

Ilustración 31

Avalúos y Catastros y Control Urbano



Fuente: Elaboración propia,2022

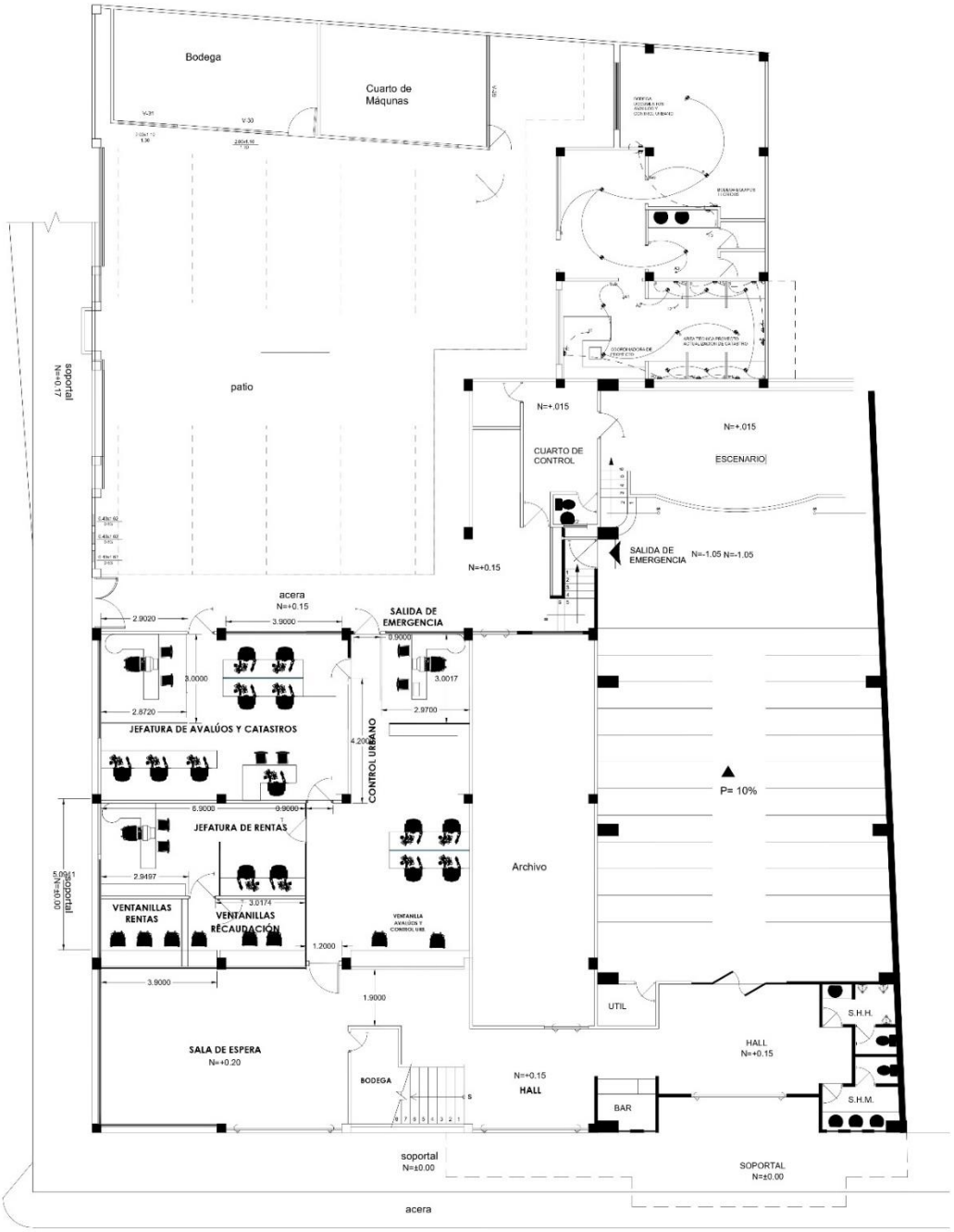
En base al análisis realizado al Anexo A correspondiente a la Norma ISO 27001 en relación al control A11 Seguridad Física y del Entorno cuyos resultados se aprecian en la Tabla 14. Además de la distribución y el estado de las oficinas, conforme se aprecian en la Ilustración 29 Plano Planta Baja Oficinas GAD La Troncal, Ilustración 30 Jefatura de Recaudación y Jefatura de Rentas y la Ilustración 31 Jefatura de Avalúos y Catastros y Control Urbano.

Se realiza una propuesta de distribución de las oficinas de la Planta baja del GAD Municipal La Troncal, enfocado en el cumplimiento del control A11 Seguridad Física y del Entorno. A continuación, se adjunta el Plano con la posible distribución.

Planos Propuesta Distribución Oficinas GAD Municipal La Troncal

Ilustración 32

Propuesta Plano Planta Baja GAD Municipal La Troncal



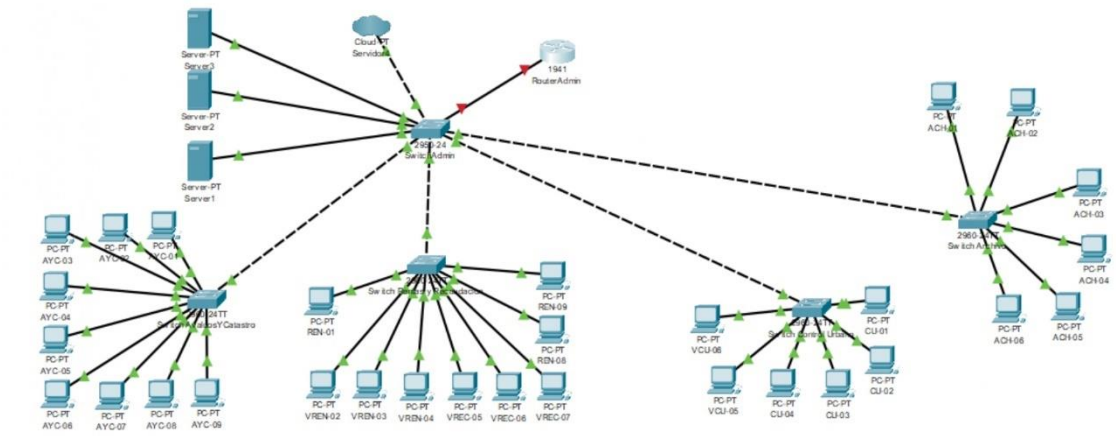
PLANTA BAJA

Fuente: GAD Municipal La Troncal,2022

Adicionalmente en función a lo establecido en el control A13 Seguridad en las Comunicaciones, presento una propuesta a la organización de la red conforme la distribución propuesta en la Ilustración 32 para la Planta Baja del GAD Municipal La Troncal.

Ilustración 33

Diagrama de Red



Fuente: Elaboración Propia,2022

Tabla 22

Valores Infraestructura - Cableado de Red

DETALLE	VALOR
Infraestructura e Instalaciones Eléctricas	15.000,00
Cableado de Red	3.500,00
Valor Total	18.500,00

Fuente: Elaboración Propia, 2022

En función del resultado obtenido al analizar la Metodología MAGERIT, primero identificamos los activos conforme al contenido de la Tabla 2 Detalle Equipos-Jefaturas, lo que indica la Tabla 3 Criterios de Valoración y en base a los resultados obtenidos acerca de la identificación de los riesgos de los activos

conforme al detalle de la Tabla 4 Estado de Equipo Tecnológico y la Ilustración 2 Niveles de Riesgo Equipo Tecnológico. Además del análisis realizado al control A8 Gestión de Activos detallado en la Tabla 11. Propongo la adquisición de Equipo tecnológico para las áreas que se encuentran en el nivel Muy Alto y Alto de riesgo, de acuerdo al siguiente detalle:

Tabla 23

Listado Actualización Equipos

	JEFATURA DE RENTAS	JEFATURA DE RECAUDACION	AVALUOS Y CATASTROS	CONTROL URBANO
Portátil	0	1	0	0
Computador todo en uno	0	0	0	0
Computador de escritorio	5	1	8	2
Impresoras	0	0	0	0
Switches	0	0	0	0
Servidores	0	0	0	0
TOTAL	5	2	8	2

Fuente: Elaboración Propia, 2022

Tabla 24

Especificación Técnica

DESCRIPCIÓN	ESPECIFICACIÓN TECNICA
Portátil Gama Media	Procesador: Core I5 o Ryzen 5 (11 Generación) Memoria: 8GB DDR4 Disco: SSD 480 GB Red: Ethernet RJ45 y WiFi

	Puertos: HDMI/SD Card/Jack 3.5mm/ USB 3.1 Type A/ USB 2.0 Type A Interfaz: Teclado en español extendido, Mouse, Parlantes Integrados, WebCam Pantalla: 15.6” HD 1366X768 pixels S.O.: Licencia Windows 10/11 Profesional en español. Maletín: Incluido
Computador de Escritorio Gama Media	Procesador: Core I5, Ryzen 5 (11 Generación) Memoria: 8GB RAM DDR4 Disco: SSD 480 GB Red: Ethernet RJ45 y WiFi Puertos: HDMI/SD Card/Jack 3.5mm/ 2 USB 3.1 Type A Interfaz: Teclado en español extendido, Mouse, Parlantes Integrados, WebCam Pantalla: 23” S.O. : Licencia Windows 10/11 Profesional UPS: 500VA 120V, 4 tomas UPS + 2 Regulador
Computador de Escritorio Gama Alta	Procesador: Core I7 o Ryzen 7 (10/11 Generación) Memoria: 16 GB RAM DDR4 Disco: SSD 480 GB + HDD 1TB Red: Ethernet RJ45 y WiFi Puertos: HDMI/SD Card/Jack 3.5mm/ 2 USB 3.1 Type A/ USB 2.0 Type A Interfaz: Teclado en español extendido, Mouse, Parlantes Integrados, WebCam Pantalla: 23” S.O.: Licencia Windows 10/11 Profesional en español UPS: 500VA 120V, 4 tomas UPS + 2 Regulador Tarjeta de gráficos especializada 4/6GB

Fuente: Elaboración Propia, 2022

Tabla 25

Valores Adquisición Equipo Tecnológico

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Portátil Gama Media	1	895,00	895,00
Computador de Escritorio Gama Media	6	1120,00	6720,00
Computador de Escritorio Gama Alta	10	1670,00	16.700,00
TOTAL	17	3685,00	24.315,00

Fuente: Elaboración Propia, 2022

Equipo Informático

Instalación

- Los activos tecnológicos (laptop, computador de escritorio o servidor) que trabajen enlazados a la red interna debe adaptarse a las reglas y métodos de instalación, establecidos por la Unidad de Sistemas.

- La Unidad de Sistemas en coordinación con la Unidad de Bodega deberá tener un registro de todos los equipos de computación y de comunicación.

- Cualquier equipo que cumpla una función determinada y tenga un propósito exclusivo, exige que su ubicación de cumplimiento a los requisitos de estabilidad física, disponibilidad eléctrica y acceso para el personal de la Unidad de Sistemas

- La protección física de los equipos es responsabilidad de la persona responsable del mismo, quien debe notificar al departamento de Sistemas cualquier anomalía o cambio de ubicación.

Mantenimiento

- La Unidad de sistemas, es la encargada de brindar este servicio;

realización del mantenimiento preventivo y correctivo de los equipos, instalación, verificación de la seguridad física y el acondicionamiento requerido. Se deben emitir normas y procedimientos para esta actividad.

- La Unidad de sistemas no está autorizada a brindar mantenimiento preventivo y correctivo a equipos que no pertenezcan a la institución.

- El personal técnico de la Unidad de Sistemas, debe acudir inmediatamente a la solicitud de cualquier departamento ante cualquier inconveniente físico o lógico.

Reubicación de equipos.

- La reubicación del equipo tecnológico deberá realizarse en base a las normas y procedimientos de la Unidad de sistemas.

- Previo al cambio de un equipo de computación se deberá realizar bajo la autorización de la Unidad de sistemas, con los medios necesarios para la instalación del equipo e informar conjuntamente a la Unidad de Bodega.

Control de Acceso:

- El acceso a un funcionario se realizará de acuerdo a las normas y procedimientos de la Unidad de sistemas.

- Referente a la política de seguridad, en las áreas críticas de la institución se deberá llevar un registro estable, señalando el ingreso y salida de personal, sin ninguna excepción.

- La Unidad de Sistemas, deberá informar acerca de los recursos necesarios para proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.

- Determinar las responsabilidades sobre control y distribución de la información a todas las unidades involucradas; implementar penalidades por uso inadecuado de la información.

- Asegurar que las credenciales y contraseñas de los usuarios cumplan con los niveles adecuados de Seguridad de Información y garantizar aplicaciones exijan cambios de contraseñas en periodos no mayor a tres meses.

- Impedir el acceso a los sistemas a los usuarios que se encuentren inactivos en periodos mayores a tres meses.

Control de Acceso- Equipo Tecnológico

- Los equipos son designados al Jefe del área o su encargado, y tiene la responsabilidad del uso adecuado de los mismos y protegerlos ante cualquier amenaza.

- Las Unidades en donde el equipo tecnológico tenga un propósito general y cuya misión es crítica se debe sujetar a los requerimientos de la Dirección a la que pertenece.

- Cada Dirección debe establecer normas estrictas a las áreas críticas de las Unidades de la Entidad Municipal.

Control acceso-remoto

- La Unidad de sistemas debe proporcionar el servicio de acceso remoto y debe establecer reglas de acceso a los activos tecnológicos.

- El usuario de los servicios de la red, deberá sujetarse al reglamento de uso y en concordancia con los lineamientos generales del uso de Internet.

Acceso a los Sistemas de la Institución.

- Brindar acceso a los Sistemas Informáticos de la institución solo a

personal autorizado y de acuerdo al perfil asignado.

- La manipulación de información institucional que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.

- La instalación y uso de los sistemas de información, se debe establecer a través de un reglamento de uso, organización, normas y procedimientos establecidos por la Unidad de Sistemas.

- Restringir el acceso a los sistemas a personal no autorizado.

- Previo a la elaboración de un contrato se debe realizar acuerdos de confidencialidad de la información y compartirlos con todas las unidades involucradas con los activos de información.

- Realizar capacitaciones periódicas y concientización acerca de la Seguridad de Información y dar a conocer a todos los funcionarios de la institución el impacto que ocasionan los incidentes de Seguridad en los objetivos de la entidad y operatividad de la misma.

- Implementar controles de acceso a los sistemas en base a perfil y rol; limitar el acceso a la información de acuerdo a las tareas asignadas.

- El control de acceso a cada Sistema de Informático, será establecido por cada Jefe o encargado.

- La Unidad de sistemas establecerá un procedimiento formal para la creación e inhabilitación de usuarios con objeto de mantener un control en la asignación de derechos de acceso.

- El acceso y la asignación de privilegios deberá ser restringido y supervisado.

- Los Jefes Departamentales deberán revisar con regularidad los derechos de acceso de los usuarios.

- Cuando se finaliza un contrato o existe un cambio de denominación; este

suceso debe ser comunicado a la Unidad de Sistemas para suprimir los derechos de acceso.

- La gestión de contraseñas debería ser interactivos y asegurar contraseñas de calidad combinando caracteres en mayúsculas, minúsculas numéricos y caracteres especiales permitidos.

El uso de contraseñas complejas es fundamental, las contraseñas complejas deben considerar de 8 a 14 caracteres e incluir caracteres alfanuméricos y especiales. Además, debe establecer una longitud mínima, un historial, un límite a la permanencia y un tiempo determinado de vencimiento. Para establecer la caducidad de las contraseñas se debe considerar: la duración (máxima 90 días), los usuarios nuevos deben cambiar su contraseña al iniciar sesión, poseer un historial de contraseñas (mínimo de 8 días).

Establecer controles de bloqueo de usuario considerar lo siguiente: bloqueo después de 3 y 5 intentos fallidas; designación a un funcionario que deshabilite el bloqueo y reactive nuevamente los usuarios.

- Restringir el uso de software que pueda perjudicar aplicaciones y sistemas del GAD Municipal La Troncal.

- Limitar la admisión al código fuente del software institucional, este debe ser un privilegio de personal autorizado.

Web

- El contenido de la página web institucional debe ser aprobado por la Dirección, respetando la ley de propiedad intelectual y normativa legal vigente.

- Referente a la seguridad, protección y diseño de las páginas web, deberá considerarse lo establecido por la Unidad de Sistemas.

- La Unidad de Sistemas de realizar una revisión periódica del ingreso a los Sistemas Informáticos y conservar el historial de acceso.

Software

- La adquisición de un nuevo software debe realizarse previo informe emitido por la Unidad de Sistemas donde se establezcan los requerimientos esenciales del mismo de acuerdo a la necesidad de la unidad requirente conjuntamente con su solicitud previa.

- La Unidad de Sistemas debe establecer normas y procedimientos para la instalación y supervisión de Software que vaya a instalarse en cualquier equipo.

- La Unidad de Sistemas debe brindar asesoría y revisión para la instalación de software informático.

- Con la finalidad de salvaguardar la integridad, disponibilidad y confidencialidad de los Sistemas Informáticos, se debe priorizar la adquisición de un software de seguridad como son los antivirus, determinar privilegios de acceso, parches de seguridad, etc.

Actualización del Software

- La actualización de software para los equipos de cómputo se realizará conforme al cronograma anual establecido por la Unidad de Sistemas.

- La Unidad de Sistemas deberá solicitar la adquisición y autorizar la actualización del software.

- Las actualizaciones correspondientes a software de uso común se ejecutarán de acuerdo a lo planificado por la Unidad de Sistemas.

Auditoría de software instalado

- La Entidad designará a un profesional a fin, quien dirigirá al grupo especializado en auditoría de sistemas.

- El personal especializado de auditoría será el responsable de dictar normas, procedimientos y calendarizar los procesos de control

establecidos

Software propiedad de la institución

- Los Sistemas desarrollados o adquiridos por la Entidad Municipal son propiedad del GAD Municipal La Troncal y mantendrán los derechos que la ley de propiedad intelectual les confiera.

- La Dirección en coordinación con la Unidad de Sistemas, deberá mantener un registro de los paquetes de programación pertenecientes la institución.

- En cumplimiento a la necesidad de todos los usuarios que manejan información masiva, se debe mantener el respaldo correspondiente de la misma ya es un activo de la institución que debe resguardarse.

- En base a la ética profesional se debe priorizar la información, base de datos, datos generados por el personal y los recursos informáticos de la institución.

- La Unidad de Sistemas debe realizar el respaldo y resguardo de los datos de los Sistemas Informáticos.

- La Unidad de Sistemas dispondrá los diferentes tipos de licencia de software y su vigencia conforme lo establecido en las políticas informáticas.

Uso de Software en la Institución

- Todo software deberá ser evaluado por la Unidad de Sistemas, previo a ser instalado para trabajar sobre la red.

- El software adquirido por la institución, debe ser de uso exclusivo para temas relacionados con las actividades relacionadas con la institución.

Supervisión y Evaluación

- Las auditorías que comprendan aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al cronograma establecido por la Dirección.

- Los sistemas informáticos considerados delicados, deberán estar bajo observación permanente.

Generales

1. Cada uno de los departamentos del Gobierno Autónomo Descentralizado Municipal La Troncal, deben emitir planes de contingencia en base a las actividades críticas que realicen.

2. El personal del Unidad de Sistemas, deberá dar cumplimiento a los códigos de ética profesional, normas y procedimientos establecidos por la institución. La Dirección Administrativa deberá asignar para el nuevo periodo fiscal los recursos necesarios para la ejecución de esta planificación, es necesario la reorganización de la Unidad de Sistemas según las tareas asignadas.

Conclusión Plan de Seguridad

El Presente Plan de Seguridad Informática puede ser utilizado como base para que la institución continue con la misión de precautelar la integridad de la información, con la finalidad de que a futuro logre acceder a una certificación ISO 27001.

Poner en consideración del Consejo Municipal para su observación el presente Plan de Seguridad Informática y su posterior aprobación.

Establecer un Presupuesto para el próximo año Fiscal para la mejora de infraestructura de la Entidad Municipal y la actualización del Equipo Tecnológico.

. **3.3. Discusión**

Análisis basado en la comparación, evolución, tendencia y perspectivas a partir de los resultados.

Los resultados obtenidos en la presente investigación realizada al GAD Municipal La Troncal, en base a sus características y realidad institucional; han proporcionado resultados seguros que permiten identificar los puntos vulnerables de la institución.

El uso de la metodología MAGERIT permitió determinar los niveles riesgos basado en los bienes pertenecientes a cada jefatura objeto de análisis de la presente investigación a la Entidad Municipal, facilitando su evaluación. (Ferruzola Gómez et al., 2019)

El desarrollo de la Encuesta efectuada al personal institucional de las diferentes áreas encargadas del uso de los diversos Sistemas Informáticos pertenecientes a la entidad municipal permite identificar diversos parámetros de Seguridad que no han sido considerados relevante para el correcto desempeño de los funcionarios; además de priorizar la Seguridad de la Información.

El análisis realizado al Anexo A que facilita la Norma ISO 27001, permitió que la entidad sea evaluada conforme establece cada control y el cumplimiento de la misma, obteniendo resultados preocupantes para la institución.

Dentro de los controles para la protección de información, es importante la documentación de la información, respaldo y su almacenamiento (ubicación). Los activos(bienes) se deben encontrar en buen estado físico y en óptimas condiciones para su correcta operatividad. Es imprescindible crear un buen ambiente laboral, una correcta estructura funcional, con una distribución afable como se puede apreciar en la *Ilustración* 32 del Plan de Seguridad.

El Plan de Seguridad desarrollado como resultado de la investigación, permitirá dar un paso inicial en el tema de Seguridad de la Información dentro del GAD Municipal La Troncal, la inversión económica inicial posibilitará mantener una óptima comunicación, mejorando las conexiones de red como se aprecia en la *Ilustración* 33. Además, la aplicación de los controles que nos facilita el Anexo A de la norma ISO 27001, permite mejorar la cultura de la institución y crear conciencia en los funcionarios sobre la importancia de la Seguridad de la Información.

Una institución segura dispondrá de un Sistema de Gestión de Seguridad de la Información cuyo enfoque se centra en los riesgos de la institución para crear, implementar, ejecutar, comprobar, preservar y perfeccionar la Seguridad de la Información, concediendo la comprobación de los Sistemas de Información pertenecientes al GAD Municipal La Troncal. La sensibilización del personal acerca del tema de seguridad es indispensable para la implementación de un SGSI en la entidad municipal y a su vez permitir que reflexionen, sobre la información que manipulan a diario.

Por consiguiente, se debe utilizar una guía para la implementación basada en la ISO 27001, obteniendo como resultados: mejorar la detección anomalías en la Seguridad de la Información, reflejado en distintos mecanismos de seguridad para salvaguardarla, prevenir su mal uso y divulgación no adecuada ocasionando perjuicios a la institución.

Al establecer, mantener los controles y las políticas de seguridad se tiene la constricción de preservar la confidencialidad, integridad y la disponibilidad de la información (activo intangible e importante) perteneciente al GAD Municipal La Troncal.

CONCLUSIONES

Conclusión 1.

En consideración a los resultados alcanzados mediante la adaptación de la Metodología MAGERIT, como se aprecia en la TABLA 4 e ILUSTRACION 2 (Niveles de Riesgo Equipo Tecnológico), se estableció las vulnerabilidades mediante un análisis y gestión de riesgos; obteniendo un 38,10% en estado muy bajo; por las razones antes mencionadas planteé la adquisición de equipo tecnológico de última generación, además de mejorar la estructura de red y distribución de oficinas, favoreciendo un ambiente laboral óptimo.

Conclusión 2.

Teniendo presente los resultados obtenidos mediante la verificación de los controles que estable el Anexo A de la norma ISO 270001, cuyo detalle se aprecia en el numeral 2.4 del presente documento. Se concluyó que el recurso humano constituye un punto esencial dentro del proceso de Seguridad de la Información y precisa consideración para reforzar su competencia operativa. Adicional en cada jefatura objeto de la presente investigación se evidencia omisiones a lo que establece el estándar internacional de Seguridad de la Información poniendo en riesgo la integridad de la Entidad Municipal.

Conclusión 3.

A partir de las principales vulnerabilidades identificadas, se recomendó un Plan de Seguridad que avala minimizar los riesgos mediante la adoptación de controles y procedimientos eficaces y razonables; con el propósito de ofrecer protección de información, control y privacidad de los Sistemas Informáticos y de los activos tangibles e intangibles (información) del Gobierno Autónomo Descentralizado Municipal La Troncal.

RECOMENDACIONES

Implementar el Plan de Seguridad de la Información propuesto en el presente documento con la finalidad de precautelar la integridad de la infraestructura tecnológica y física de los equipos informáticos e información de la Entidad Municipal, considerando la disponibilidad económica, técnica y humana.

Realizar un monitoreo continuo para que las vulnerabilidades existentes en el Gobierno Autónomo Descentralizado Municipal La Troncal sean solucionadas y que la Entidad Municipal mantenga un proceso sistematizado que comprenda regulaciones, monitoreo, mejora y continuidad de la Seguridad de la Información.

Se recomienda ejecutar auditorías informáticas en base a metodologías internacionales para mantener actualizadas las políticas de Seguridad de la Información, concediendo resguardar los activos informáticos ante posibles amenazas internas y externas, mediante la planificación, capacitación y empoderamiento de los funcionarios acerca del uso de los Sistemas de Informáticos.

BIBLIOGRAFÍA GENERAL

Aguilar, M. (2017). *PLAN DE SEGURIDAD INFORMÁTICA BASADO EN ESTÁNDAR ISO-IEC 27001 PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DEL GAD CANTONAL DE PASTAZA*.

Bolaño Rodríguez, Y., Vivas Ávila, E., & Hernández Calderín, E. E. (2019). Procedimiento para el fortalecimiento del sistema de control interno. *Folletos Gerenciales*, *23*(3).

Bustamante García, S., Valles Coral, M. Á., Cuellar Rodríguez, I. E., & Lévano Rodríguez, D. (2021). Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. *Enfoque UTE*, *12*(2). https://doi.org/10.29019/enfoqueute.743

Calder, A. (2017). ISO27001/ISO27002: Una guía de bolsillo. In *ISO27001/ISO27002: Una guía de bolsillo*.

Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System. In *Implementing an Information Security Management System*. https://doi.org/10.1007/978-1-4842-5413-4

Crespo, N. (2018). *La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior*.

Díaz Sánchez, N. (2021). Conservación en el ámbito documental: estabilidad de soportes e integridad de la información. *Revista Del Archivo General de La Nación*, *36*(1). https://doi.org/10.37840/ragn.v36i1.127

Ferruzola Gómez, E., Duchimaza S., J., Ramos Holguín, J., & Alejandro Lindao, M. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. *Revista Científica y Tecnológica UPSE*, *6*(1). https://doi.org/10.26423/rctu.v6i1.429

Figueroa Pérez, O., & Malagón Sáenz, N. E. (2017). Propuesta de Políticas de Seguridad de la Información para la institución Educativa de Educación Básica y Media del departamento de Boyacá, basadas en la norma ISO 27001:2013. In *instname:Universidad Nacional Abierta y a Distancia*.

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo Del Conocimiento*, *2*(12). https://doi.org/10.23857/pc.v2i12.420

Fin De Máster, T., Zamora, A., & Yasira, K. (n.d.). *Implantación de un sistema de gestión integrado con las normas ISO/IEC 27001:2013 e ISO/IEC 20000-1:2018*.

García, J. (2020). *Diseño de un Sistema Integrado de Gestión basado en las normas ISO 9001:2015 e ISO 27001:2013, para la emisión de documentos de identificación militar en la matriz de la Dirección de Movilización del Comando Conjunto de las Fuerzas Armadas*.

González, M. (2016). *Modelo de Gestión de la Norma ISO/IEC 27001:2013 en la Seguridad de Información de una empresa de Telecomunicaciones*.

Guamán, A., & Cárdenas, J. (2022). *Cumplimiento de las políticas de seguridad de información en las cooperativas de ahorro y crédito del cantón Cañar*. *6*(43), 2022. https://doi.org/10.29018/issn.2588-1000vol6iss43

Guerra, R. (2018). Gestión de seguridad de la información con la norma ISO 27001:2013. *Espacios*, *39*.

José Hernández. (2019). TEMA 1-SEGURIDAD INFORMÁTICA 1.1 Definición de Seguridad Informática. *José Hernández*.

Lilja SIKMAN, Tihomir LATINOVIC, & Darko PASPALJ. (2019). *ISO 27001 – INFORMATIONSYSTEMS SECURITY, DEVELOPMENT, TRENDS, TECHNICAL AND ECONOMIC CHALLENGES*.

Melo Reyes, O. J. (2019). *ASPECTOS A TENER EN CUENTA PARA EL ANÁLISIS*

DE RIESGOS CON BASE EN LAS NORMAS ISO/IEC 27001, ISO/IEC 27005 E ISO/ IEC 31000.

Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: a systematic review. *Annales Des Telecommunications/Annals of Telecommunications*, *76*(3–4). https://doi.org/10.1007/s12243-020-00783-2

Morales, F., Toapanta, S., & Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *E*(27).

Muyón, C., Guarda, T., Vargas, G., & Ninahualpa Quiña, G. (2018). Esquema Gubernamental de Seguridad de la Información EGSI y su aplicación en las entidades públicas del Ecuador. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao.*

Patiño, S., Mosquera, C., Suárez, F., & Nevarez, R. (2017). Evaluación de seguridad informática basada en ICREA e ISO27001. *Universidad, Ciencia y Tecnología*, *21*(85).

Quevedo Arnaiz, N. V., Acurio Jaramillo, M. N., & Paguay Pogo, M. S. (2021). Derechos de los inmigrantes en la ley ecuatoriana. Instrumento para medir datos sobre la inmigración. *Dilemas Contemporáneos: Educación, Política y Valores*. https://doi.org/10.46377/dilemas.v8i.2688

Quispe, E. S. A. (2020). Implementación de la norma ISO 27001 en el departamento de tecnologia de informacion de la empresa Esvicsac, Callao. *Repositorio Institucional - UCV*.

Ramos, Y., Urrutia, O., Bravo, A., & Ordoñez, D. (2017). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca. *Memorias de Congresos UTP*.

Rodriguez, B. L. S., Puente De La Vega, C. C. F., Mejía, C. C., & Alarcón, D. M. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana Application of ISO 27001 and its influence on the information security of a Peruvian private company. *Propósitos y Representaciones*, *8*, 786. https://doi.org/10.20511/pyr2020.v8n3.786

Ruíz, J., Estrada, C., & Sánchez, M. (2020a). Propuesta de un modelo de sistema de gestión de la seguridad de la información en una pyme basado en la norma ISO / IEC 27001. *Revista de Investigación Latinoamericana En Competitividad Organizacional*.

Ruíz, J., Estrada, C., & Sánchez, M. (2020b). Propuesta de un modelo de sistema de gestión de la seguridad de la información en una pyme basado en la norma ISO / IEC 27001. *Revista de Investigación Latinoamericana En Competitividad Organizacional*.

Ruíz, J., Estrada, C., & Sánchez, M. (2020c). Propuesta de un modelo de sistema de gestión de la seguridad de la información en una pyme basado en la norma ISO / IEC 27001. *Revista de Investigación Latinoamericana En Competitividad Organizacional*.

Saltos Peña, Yc. D. (2017). “DESARROLLO DE UN ESQUEMA DE SEGURIDAD DE INFORMACIÓN SIGUIENDO EL ESTÁNDAR ISO 27001-2013 APLICADO AL ÁREA DE SEGURIDAD DE LA INFORMACIÓN PARA UNA COOPERATIVA DE AHORRO Y CRÉDITO. *Journal of Chemical Information and Modeling*.

Suárez, B., & Maggi, B. (2020). Escala de Likert en el nivel de conocimiento de Diabetes Tipo 2 en la provincia de Santa Elena. *Revista Ciencias Pedagógicas e Innovación*, *VIII*(1).

Tundidor-Montes de Oca, L., Medina-León, Al., Nogeuira-Rivera, D., & Serrate-Alfonso, A. (2019). Evaluación del sistema de seguridad de la información para

empresas de proyectos. *Ciencias Holguín*, *25*(3).
Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *22*, 73–88. https://doi.org/10.17013/risti.22.73-88
VASUDEVAN, V., MANGLA, A., UMMER, F., SHETTY, S., PAKALA, S., & ANBALAHAN, S. (2020). THE ISO27001 IMPLEMENTATION PROJECT. In *Application security in the ISO27001:2013 Environment*. https://doi.org/10.2307/j.ctt19qgf1f.7

ANEXOS

Anexo 1

La Troncal, lunes 26 de septiembre del 2022

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL LA TRONCAL
FECHA 26 SEP 2022 HORA 14:54
ALCALDIA

Ingeniero
Rómulo Ulises Alcívar Campoverde
ALCALDE DEL CANTON LA TRONCAL
En su despacho. -

De mis consideraciones

Reciba un saludo cordial de parte de mi persona (Ing. Marjorie Topacio Dumaguala León), alumna de Maestría en Tecnología de la Información de la Universidad Estatal de Milagro del actual Proceso Titulación TIC - COHORTE I, periodo académico 2020 – 2022, solicito muy respetuosamente a su distinguida autoridad, disponga a quien corresponda, se me conceda los permisos necesarios para realizar un levantamiento de información referente a los Sistemas informáticos que se manejan en el Gobierno Autónomo Descentralizado Municipal de La Troncal; con la finalidad de presentar un "**PLAN DE SEGURIDAD BASADO EN LA NORMA ISO 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LA TRONCAL, PROVINCIA DEL CAÑAR"**, los mismos que m servirán para la obtención del título de Magister en Tecnologías de la Información, a la vez que dicho trabajo se considere para resguardar la información institucional.

Por la favorable acogida que le brinde a la presente, le anticipo mis agradecimientos.

Atentamente:

Ing. Marjorie Dumaguala L.
MAESTRANTE EN TECNOLOGÍAS DE LA INFORMACIÓN

Anexo 2

GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL LA TRONCAL
SECRETARÍA GENERAL

La Troncal, 26 de septiembre de 2022
2022- 1245-SGM-

Ingeniera
Marjorie Dumaguala
MAESTRANTE EN TECNOLOGÍAS DE LA INFORMACIÓN
Ciudad. -

De mi consideración:

En atención al oficio s/n de fecha septiembre 26 de 2022, mediante el cual solicita se le conceda el permiso respectivo para realizar un levantamiento de información referente a los sistemas informáticos que se manejan en este GAD municipal, información que servirá para la obtención del titulo de magister en tecnologías de la información, esta Alcaldía autoriza a usted realice lo requerido.

Particular que comunico para los fines consiguientes.

Atentamente,

Ing. Rómulo Alcívar Campoverde
ALCALDE DEL CANTÓN

Gobierno Autónomo Descentralizado LA TRONCAL ALCALDIA Municipal La Troncal