UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

REPÚBLICA DEL ECUADOR

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN

TÍTULO DEL PROYECTO:

MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA ESTABLECER CONTROLES BASADOS EN LA NORMA ISO/IEC 27001:2013 MEDIANTE EL CÓDIGO DE PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27002:2022 EN EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN NARANJAL

TUTOR

MIRELLA AZUCENA CORREA PERALTA, MSC

AUTOR

ALEX ARMANDO ÁVILA COELLO

MILAGRO, MARZO 2023

ECUADOR

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

DIRECCIÓN DE INVESTIGACIÓN Y POSGRADO

Milagro, Septiembre, 2022

CERTIFICACIÓN DE ACEPTACIÓN DEL TUTOR

En calidad de Tutor del Proyecto de Investigación, nombrado por el Comité Académico del Programa de Maestría en Tecnologías de la Información de la Universidad Estatal de Milagro.

CERTIFICO

Que he analizado el Proyecto de Investigación con el tema **MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA ESTABLECER CONTROLES BASADOS EN LA NORMA ISO/IEC 27001:2013 MEDIANTE EL CÓDIGO DE PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27002:2022 EN EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN NARANJAL,** elaborado por **ALEX ARMANDO ÁVILA COELLO**, el mismo que reúne las condiciones y requisitos previos para ser defendido ante el tribunal examinador, para optar por el título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**.

Firmado electrónicamente por:
MIRELLA AZUCENA CORREA PERALTA

MIRELLA AZUCENA CORREA PERALTA, MSC
C.I: 0919615906

UNEMI

UNIVERSIDAD ESTATAL DE MILAGRO

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, a los seis días del mes de marzo del 2023

ALEX ARMANDO AVILA COELLO

FIRMA DEL EGRESADO
NOMBRE: ÁVILA COELLO ALEX ARMANDO
CÉDULA: 0704120369

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO
DIRECCIÓN DE POSGRADO
CERTIFICACIÓN DE LA DEFENSA

El TRIBUNAL CALIFICADOR previo a la obtención del título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**, presentado por **ING. ÁVILA COELLO ALEX ARMANDO**, otorga al presente proyecto de investigación denominado "MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA ESTABLECER CONTROLES BASADOS EN LA NORMA ISO/IEC 27001:2013 MEDIANTE EL CÓDIGO DE PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27002:2022 EN EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN NARANJAL", las siguientes calificaciones:

TRABAJO DE TITULACION	59.33
DEFENSA ORAL	39.00
PROMEDIO	**98.33**
EQUIVALENTE	**Excelente**

JORGE LUIS VINUEZA MARTINEZ

Mgti. VINUEZA MARTINEZ JORGE LUIS
PRESIDENTE/A DEL TRIBUNAL

OSCAR XAVIER BERMEO ALMEIDA

Mgti. BERMEO ALMEIDA OSCAR XAVIER
VOCAL

RAFAEL SELEYMAN LAZO SULCA

Msc Bio V LAZO SULCA RAFAEL SELEYMAN
SECRETARIO/A DEL TRIBUNAL

DEDICATORIA

Mi tesis se la dedico A Dios por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mis amados padres Papá. Néstor Porfirio Ávila Cárdenas, Madre. Victoria Ernestina Coello Vera por haberme brindado su apoyo incondicional.

A mi amada esposa Mayra Sugey Olivo Alvarado por su comprensión y esfuerzo, durante este dificultoso camino para convertirme en un profesional.

A mis amados hijos: Alex Armando Ávila Olivo, Alisson Victoria Ávila Olivo, Xian Aarón Ávila Olivo por ser mi motivación para poder superarme para que la vida nos depare un futuro mejor.

A mis queridos maestros por impartir sus conocimientos y no cesaron al enseñarme.

AGRADECIMIENTO

A Dios omnipresente por protegerme durante todo mi camino y darme fuerzas para superar obstáculos y dificultades a lo largo de mi vida.

A mis amados padres que me han brindado su amor, confianza y me han enseñado a no desfallecer ni rendirme ante nada y están orgullosos de la persona en la cual me he convertido.

A mi esposa e hijos por la confianza, paciencia y apoyo brindado durante el transcurso mis estudios.

Al Coordinador de la maestría, PhD. Jorge Rodas Silva y docentes tutores de la Universidad Estatal de Milagro le agradezco por su tiempo, su apoyo y comprensión durante mis años de estudio. A mi tutora, Msc. Mirella Azucena Correa Peralta por su apoyo y tiempo incondicional en la realización de mi proyecto.

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

CESIÓN DE DERECHOS DE AUTOR

Doctor
ING. FABRICIO GUEVARA VIEJÓ, PhD

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 **MODELO DE SISEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA ESTA BLECER CONTROLES BASADOS EN LA NORMA ISO/IEC 27001:2013 MEDIANTE EL CÓDIGO DE PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27002:2022 EN EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN NARANJAL**, y que corresponde al Vicerrectorado de Investigación y Posgrado.

Milagro, 6 de marzo del 2023

ALEX ARMANDO AVILA COELLO

FIRMA DEL EGRESADO
NOMBRE: ÁVILA COELLO ALEX ARMANDO
CÉDULA: 0704120369

ÍNDICE

INDICE DE FIGURAS

ÍNDICE DE TABLAS

RESÚMEN

El presente trabajo de investigación trata acerca del modelo de sistema de gestión de seguridad de la información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del Gobierno Autónomo Descentralizado Municipal del cantón Naranjal, se pudo realizar observaciones en la entidad la cual posee una inadecuada administración en la red informática interna y servicio de internet, causando que la información municipal tenga pérdida o genere duplicidad o ambigüedad de la información. Incluso como parte de la problemática están la deficiente aplicación de políticas, asignación de responsabilidades y segregación de tareas de acuerdo a las actividades que realizan los funcionarios, dentro del proceso metodológico el trabajo se realizó con conocimientos de gestión de la seguridad de la información, al grupo del departamento de Tecnología aplicando una encuesta para receptar la opinión de 55 personas que laboran en la entidad Municipal. Para el desarrollo de la propuesta este proyecto se utilizará el ciclo PHVA (Planificar, Hacer, Verificar y Actuar), la cual partirá la asociación entre las acciones y la ISO/IEC 27002:2022 como se observa la figura. Se optó por dicha metodología debido a la mejora continua de los servicios y procesos en una organización.

Palabras claves: seguridad de la información, norma ISO/IEC 27001:2013, método PHVA

ABSTRACT

The present research work deals with the information security management system model, to establish controls based on the ISO / IEC 27001: 2013 standard in the municipal decentralized autonomous governments of Ecuador: case of the Government's information technology department Municipal Decentralized Autonomous of the Naranjal canton, it was possible to make observations the entity has an inadequate administration of the internet service, causing the municipal information to have loss or generate duplicity or ambiguity of the information. Even as part of the problem is the poor application of policies for assigning responsibilities and segregating tasks according to the activities carried out by officials, within the methodological process the work was carried out with knowledge of information security management, at Technology department group applying a survey to receive the opinion of 55 people from the Municipal GAD. For the development of the proposal, this project will use PHVA (Plan, Do, Verify and Act), which will start the association between the actions and ISO IEC 27002 as shown in the figure. This methodology was chosen due to the continuous improvement of services and processes in an organization.

Keywords: information security, ISO/IEC 27001:2013 standard, PHVA method

CAPÍTULO 1

1.1. Planteamiento del problema

En el 2021 el Ecuador lideró la lista de países más vulnerados por los ciberataque según Kaspersky; incluso, según en el reporte titulado Panorama de Amenazas en Latino América 2021, hay un aumento del 24 % en ciberataques en los primeros ocho meses, en comparación con el mismo periodo al 2020. Pues, la filtración de documentos e información en Instituciones Gubernamentales han provocado problemas, un ejemplo de esto fue el ataque informático a la Agencia Nacional de Tránsito a su sistema AXIS en el 2021 o el ciberataque que recibió el Municipio de Quito el pasado 16 de abril del presente año.

El desarrollo de la tecnología ha creado beneficios, pero también ha generado serios problemas de vulnerabilidades en las organizaciones ya sean por riesgos, inseguridades, fraudes informáticos, espionajes, sabotajes, intrusiones o ataques de denegación de servicio, entre otros; pues el uso inadecuado de recursos tecnológicos en Instituciones Gubernamentales provocan serios problemas ante la seguridad y resguardo de la información creando un aumento desmesurados en índices de delitos informáticos que afectan a la consecución de los objetivos de las instituciones.

En el caso del GAD Municipal de Naranjal en su estructura organizacional se encuentra la Gestión de Tecnología e Informática responsable de resguardar información crítica y sensible como son las transacciones municipales que son realizadas a través del Sistema Integral de Información Multifinalitario SIIM V7 Comercial y V6 OpenERP Financiero; es ahí, donde es necesario soportar con normativas de seguridad de la Información para minimizar riesgos físicos y lógicos de la data; además, la entidad posee una inadecuada administración de la red interna y servicio de internet, causando que la información municipal tenga pérdida o genere duplicidad o ambigüedad de la información. Incluso como parte de la problemática están la deficiente aplicación de políticas de asignación de responsabilidades y segregación de tareas de acuerdo a las actividades que realizan los funcionarios, generando:

- Inadecuado uso de las herramientas informáticas o medios de almacenamiento electrónico.
- No precaución en salvaguardar información.
- Escaso control de accesos.
- Equipos informáticos de telecomunicaciones sin credenciales robustas.

De ahí que un Modelo de Sistema de gestión de Seguridad de la Información para el municipio se vuelve necesario para analizar, evaluar y proponer, desde el criterio de la ISO 27001 como estándar al establecer requisitos para implementar, mantener y mejorar como sistema de gestión de seguridad de la información, más aún las Instituciones públicas que tienen información sensible, por:

- No disponer de controles para garantizar accesos externos que pueden comprometer la seguridad de la data integral municipal.
- No se ha implementado políticas para el uso de controles criptográficos para resguardar las claves de acceso de servidores, equipos de cómputo y dispositivos de telecomunicaciones.
- Deficiencia en el control de los activos fijos: No existe un uso adecuado de los equipos Informáticos en relación a las tareas que se realizan.
- Improvisada planificación de seguridad informática asociados a servicios en red e intercambio de información.
- Inexistencia de políticas de desarrollo de software que incluyen: control de cambios en los sistemas, revisión de versionamiento y técnica para la protección de los datos.

Formulación del problema

¿De qué manera la propuesta de un Modelo de Sistemas de gestión de Seguridad de la Información, basado en ISO/IEC 27001:2013 para el Gobierno Autónomo Descentralizado Municipal del cantón Naranjal, aportará a la seguridad de la data integral transaccional para reducir posibles problemas informáticos?

¿Cómo se puede evaluar riesgos, estrategias y controles para brindar seguridad, disponibilidad e integridad de la información en el Gobierno Autónomo Descentralizado Municipal del cantón Naranjal?

¿De qué modo se podría valorar el Modelo de Sistema de Gestión de Seguridad de la Información para garantizar su correcta aplicación de los controles basados en la ISO27001:2013 en el Gobierno Autónomo Descentralizado Municipal del cantón Naranjal?

1.2. Objetivos

1.2.1. Objetivo General

Proponer un Modelo de sistema de gestión de seguridad de la información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado Municipal del cantón Naranjal.

1.2.2. Objetivos Específicos

1. Identificar los componentes para el Modelo de Sistema de Gestión de Seguridad de la Información.
2. Establecer una metodología de gestión y mejora continua del Modelo de Sistema de Gestión de Seguridad de la Información, lo cual garantice un adecuado tratamiento de la información.
3. Evaluar el Modelo de Sistema de Gestión de Seguridad de la Información, mediante grupos de expertos de seguridad focal.

1.3. Alcance

El presente proyecto tiene como finalidad definir una propuesta como alternativa a la problemática actual que presentan las instituciones públicas del Ecuador, específicamente dirigido al GAD Municipal de Naranjal, tomando como base el sistema de gestión de Seguridad de la Información basado en ISO/IEC 27001:2013, utilizando como guía la ISO ISO/IEC 27002:2022.

La propuesta utilizada propondrá una solución para la conexión, administración y gestión de los datos existentes en la institución Municipal, creando un nuevo concepto de gestión, auxiliando en el despliegue de los recursos que se encuentran incluidos en la red informática interna, brindando nuevas alternativas con respecto a la seguridad y transferencia de la información con el mejor desarrollo de sus actividades diarias al servicio de la comunidad.

El alcance absoluto para el desarrollo de este proyecto será satisfacer a los clientes externos e internos, ya que se proporcionara un servicio transparente y de calidad, el sistema informático estará operativo y funcional transmitiendo la información de las transacciones de manera segura y controlada. Todo ello contribuirá a la eficacia de los servicios que la institución Municipal busca a través de sus políticas y controles de seguridad de la información normados y estandarizados.

1.4. Estado del arte

En la investigación realizada por Tigse Moposita (Tigse Moposita (2020)) titulado “Plan de gestión de seguridad informática fundamentado en la norma ISO 27001 para el departamento de tecnología de la información en la empresa Plasticaucho industrial S.A.”, tiene como objetivo principal proveer el plan de gestión de seguridad informática fundamentado en la Norma ISO 27001 para mejorar la seguridad de la información. Para realizar su investigación utilizó la metodología bibliográfica y así hacer uso de fuentes obtenidas de libros, artículos científicos y

tesis elaboradas en centros universitarios. Tigse llego a la conclusión que, al minimizar las tareas del departamento de tecnología, el resultado mejoró la calidad del servicio.

La segunda investigación de Lema y Donoso (Lema Vinlasaca (2018)) titulada "Implementación de un sistema de seguridad de información basado en la Norma ISO 27001:2013 para el control físico y digital de documentos aplicado a la empresa Lockers S.A.", su objetivo general es poner en práctica un sistema de gestión de seguridad fundamentados en la Norma ISO 27001:2013 para el control físico y digital de documentos. Llegando a concluir así que los controles implantados para los riesgos inaceptables, moderados y tolerable fueron disminuidos dentro del tiempo estipulado obteniendo buenos resultados a favor de la organización.

De León Camelo (De León Camelo (2019)), en su investigación "Diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para instituciones gubernamentales de La Guajira, se fundamentó en la construcción y diseño de una guía de buenas prácticas y procedimientos sistémicos, que consisten en reducir los riesgos y mantener la custodia de la información. De León determinó que en la fase de reconocimiento se obtuvo a partir del inventario lo cual ayudo a evidenciar que factores son los que ponen en peligro la integridad, confidencialidad y disponibilidad en una organización.

Según Nacipucha Cumbe (Nacipucha Cumbe (2019)), en su investigación titulada "Análisis y diseño para un modelo de gestión de seguridad de la información basados en normas ISO/IEC 27001:2013 para la empresa artehogar en la ciudad de Guayaquil", permite la protección de los activos físicos y no físicos de la información.Este proyecto utilizó métodos cualitativos y cuantitativos de análisis de los datos obtenidos para validar los resultados obtenidos en el proceso de investigación y análisis. Se concluye que la implementación de un sistema de seguridad de la información asegura, mantiene y asegura la disponibilidad, integridad, confidencialidad y acceso a los activos informáticos físicos y no físicos de la empresa.

Según Nieves (Nieves (2017)) en su trabajo de investigación titulada "Diseño de un sistema de gestión de la seguridad de la información apoyado en la norma ISO/IEC 27001:2013", el asunto de la investigación trata de una guía destinada a evaluar la integridad, confidencialidad y disponibilidad de los activos de información a las oficinas que dan acceso a centros de educación técnica. Deduciendo así que con la creación de un plan de entrenamiento y concientización sobre seguridad de la información, se lograra ambientes de buen manejo y uso de los activos de información.

En la investigación realizada por Benavides y Blandón (Benavides Sepúlveda (2018))titulada "Modelo sistema de gestión de seguridad de la información Para Instituciones Educativas en el Nivel Fundamental se detalla un proyecto para realizar un análisis de riesgo basado en la norma ISO 27001 para identificar activos clave en el área de secretaría académica de una institución educativa. Cuya conclusión es que el modelo de sistema de gestión de seguridad de la información pueda contribuir a la sociedad evitando que los niños y niñas transmitan información sensible y que los adolescentes sean manipulados por personas sin escrúpulos o que estos sean involucrados en redes de prostitución o pornografía infantil.

Lucano (Lucano Cordones (2019)) afirma, "Diagnóstico y Diseño de un sistema de gestión de seguridad de la información basado en La Norma ISO/IEC 27001:2013 en Banca Pública cubre la investigación de la seguridad de la información, el diagnóstico del estado actual de la banca pública y el diseño de sistemas de gestión basados en la norma ISO 27001:2013. Para el desarrollo de la investigación, Lu-

cano utilizó un método bibliográfico, con documentos de diversas áreas del Banco del Instituto de Seguridad Social del Ecuador (BIESS). Hemos llegado así a la conclusión de que se han definido un conjunto de actividades, documentos producidos y una estrategia de seguridad que forman parte del diagnóstico y diseño de un sistema de gestión de seguridad de la información aplicable a un banco público mediano. sector.

El propósito de esta revisión sistemática de la literatura ha permitido hacer referencia e identificar otras investigaciones y trabajos desarrollados en ISO/IEC 27001:2013. Aspectos que los GAD de los gobiernos locales pueden tomar en cuenta. Esto se debe a que comprende estándares ISO para Sistemas de Gestión de Seguridad de la Información (SGSI) para evaluar los riesgos y aplicar los controles necesarios para mitigarlos o eliminarlos.(Isotools (2022)).

De manera similar, ISO/IEC 27001:2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información que satisfaga las necesidades y los objetivos estratégicos de una organización. Son genéricos y aplicables a todas las organizaciones (ISO (2022)). Para la (ISO.ORG (2022)) establece que esta seguridad de la información se logra mediante la implementación de un conjunto de controles, políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Un SGSI, como el especificado en ISO/IEC 27001, debe tener una imagen completa de los riesgos de seguridad de la información. Esto se puede lograr respaldando la información mediante controles y procedimientos apropiados, ya que muchos sistemas de información no se diseñaron teniendo en cuenta la seguridad. Ahora bien, el SGSI requiere del involucramiento de todos los que trabajan en la organización, como es el caso del GAD Municipal de Naranjal. También puede seleccionar o diseñar controles para satisfacer las necesidades, decisiones o estrategias de su organización desde su enfoque de gestión de riesgos.

Las tres fuentes principales de requisitos de seguridad, son:

a) Necesidad de identificar una evaluación de riesgos considerando la estrategia y los objetivos como amenazas a los activos y evaluar las vulnerabilidades, probabilidades y valoración del impacto.

b) Requisitos estatutarios, legales reglamentarios y Contractuales.

c) Comienzos, finalidad y clausulas para el manejo, evolución, almacenamiento, comunicación y archivo de la información para amparar sus operaciones.

Como se mencionó anteriormente (Tariq (2020)) la computación en la nube y las redes inalámbricas de sensores están aumentando el número de ciberataques. El objetivo que propuso en su investigación fue utilizar un enfoque formalizado, a saber, el proceso jerárquico de enfoque analítico (AHP) y el proceso de priorización basados en la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional (ISO/IEC) 27001:2013. El objetivo era mejorar cómo se analiza la gestión de la seguridad de la información.

De manera similar (Hamit (2020)) comparte preocupaciones sobre: Para la filtración de datos móviles de 2017, comenzaremos a investigar la causa de la filtración. ISO/IEC 27001:2013 Anexo A para la Mitigación de Riesgos Aplicación de un marco de gestión de riesgos a las unidades de desarrollo de software para abordar el riesgo mediante controles. De manera similar, (Alghiani, 2019) supuestamente desarrolló un modelo integrado de gestión de riesgos para sistemas de gestión estandarizados.

(Phirke (2019)) presentó el estado de los procesos de ejecución en su estudio ISO/CEI 27001. Las organizaciones han tenido la oportunidad de demostrar su confiabilidad siguiendo las mejores prácticas aceptadas. Y concluyó que además de la necesidad de pensar en los aspectos técnicos y legales de una organización, también hay aspectos relacionados con las personas como: Capacitación, conocimiento y concientización para lograr la gestión de la seguridad de la información.

(Kur (2018)) señala que la seguridad de la información es un proceso que está influenciado por cuestiones organizacionales y utiliza el estándar ISO/IEC 27001:2013 para realizar una evaluación de alto nivel y observar la solidez de la seguridad de la información y los estados de ISO/IEC : El estándar 27001:2013 certifica los niveles de madurez de la gestión de la seguridad de la información y ayuda a abordar los problemas de vulnerabilidad de la seguridad de la información.

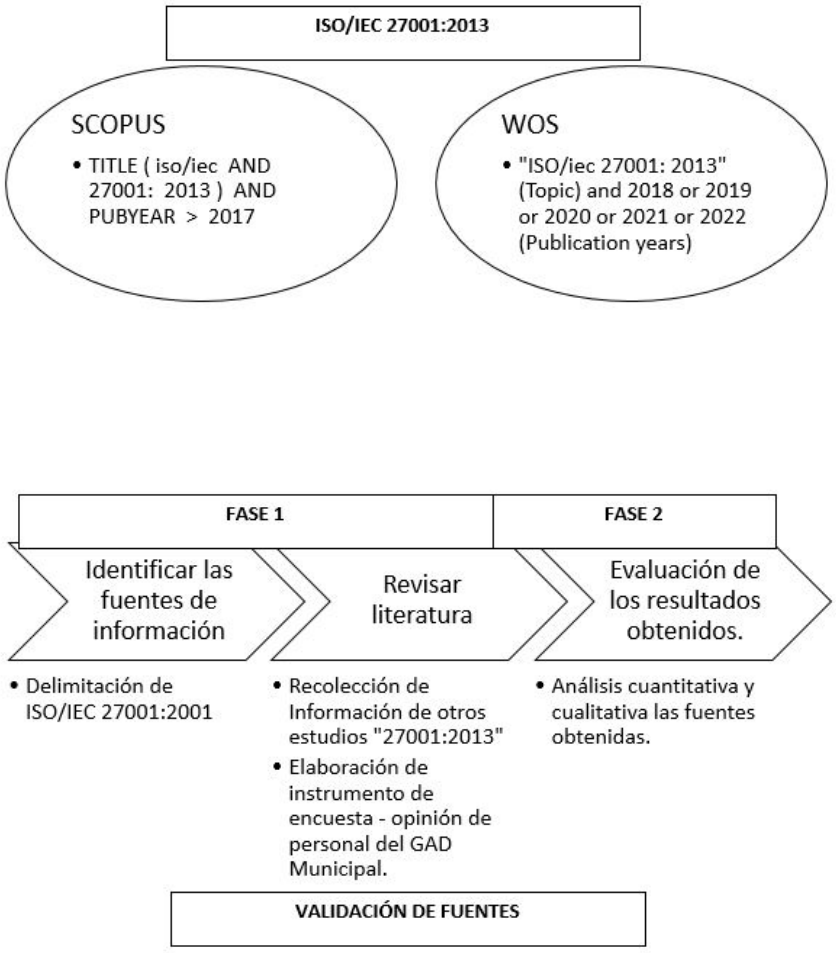
Para (Aqu (2018)) Materializaron un análisis para ascender el nivel de seguridad de la in formación en la Dirección de Tecnologías de la Información (DTI) de la UNAMBA, aplicando el Sistema de Gestión de Seguridad de la Información guiado en el estándar ISO/IEC 27001:2013, para considerar la confidencialidad, disponibilidad e integridad de la información y de los sistemas de información. Con un estudio preexperimental aplicando el criterio Deming PDCA, que fundamento en reconocer los recursos informáticos, análisis y gestión de riesgos, para fijar los controles y mitigarlos adaptándose la metodología MAGERIT III, luego de haberse implantado los controles reducidos a un 75 %, con un inicio de 18 controles y continuar hasta llegar a 65, además ponen en consideración que se realice una capacitación de seguridad a los usuarios internos, para fortalecer conocimientos con nociones de seguridad del 48 % a 95 %.

CAPÍTULO 2

2.1. Metodología

Este estudio investigativo es de carácter exploratorio; pues, primero se revisaron trabajos publicados en bases de datos de SCOPUS y Web Of Science (WOS), y se incluyó una revisión bibliométrica utilizando como término clave ISO/IEC 27001: 2013.

Figura 2.1: Validación de Fuentes



Fuente: Adaptado de (Soto Hernández, Villamar Monserrate, Vinueza Martínez, Astudillo Cobos, Correa Peralta, 2018)

Tabla 2.1: Consulta de Fuentes bibliográficas en SCOPUS y WOS con el término ISO/IEC 27001: 2013 Periodo 2018 - 2022

	TÍTULO	AÑO
	SCOPUS	
TITLE (iso/iec AND 27001: 2013) AND PUB-YEAR >2017	On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations.	2018
	Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs.	2018
	ISMS planning based on ISO/IEC 27001:2013 using analytical hierarchy process at gap analysis phase (Case study: XYZ institute).	2018
	General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance.	2019
	Implementation of an Information Security Management System Based on the ISO/IEC 27001: 2013 Standard for the Information Technology Division.	2021
	WOS	
ISO/IEC 27001: 2013"(Topic) and 2018 or 2019 or 2020 or 2021 or 2022	On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations.	2018
	Decision support for selecting information security controls.	2018
	Information Security Management Practices: Study of the Influencing Factors in a Brazilian AIR FORCE Institution.	2018
	Adapting ISO 27001 to a Public Institution.	2019
	General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance.	2019

Risk Model for Integrated Management System.	2019
A proposal for the management of the information security applied to a Colombian public entity.	2019
Analyzing The Relevance of Inhibiting Factors in Implementing ISO 27001 Using the DEMATEL Method (Case Study: Electronic Procurement Service Center (LPSE) of the Ministry of Finance, Republic of Indonesia).	2019
From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls.	2020
Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ).	2020
From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance.	2020
Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks.	2020
POSSIBILITIES OF ISO 9001: 2015 QMS AND ISO/IEC 27001:2013 ISMS INTEGRATION.	2021
Information Security Assessment On Court Tracking Information System: A Case Study from Mataram District Court.	2021
AUTOMATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON THE ISO/IEC 27001 STANDARD.	2021
Information Security Multiprofile Maturity Model (ISM3).	2022

Adicionalmente, con el uso de la herramienta de Publish or Perish se accedió an Google Scholar, OpenAlex, Semantic Scholar obteniendo como resultado la Tabla 2.

Tabla 2.2: Consulta de Fuentes bibliográficas con el término ISO/IEC 27001: 2013.

SEARCH TERMS	SOURCE	PAPERS	CITES	YEAR
ISO/IEC 27001:2013”[title] from 2021 to 2022, no citations, no patents.	Google Scholar	42	4	4.00
ISO/IEC 27001:2013”[title] from 2020 to 2022.	OpenAlex	27	3	1.50
ISO/IEC 27001:2013”.	Semantic Scholar	12	11	0.38

Adicionalmente, el trabajo se realizó con conocimientos de gestión de la seguridad de la información, al grupo del departamento de Tecnología aplicando una encuesta para receptar la opinión de 55 personas del GAD Municipal de Naranjal validándose este previamente el instrumento por 2 personas: Ing. Vicente Jasmany Franco Peralta, Analista de Sistemas e Ing. Jennifer Patricia

Pérez Parra, Directora de la Gestión Administrativa (E), el procedimiento de investigación se llevó a cabo de la siguiente manera:

a) Recolección de Información de otros estudios previamente investigados que tengan relación a la implementación del SGSI en el estándar ISO/IEC 27001:2013, con su respectiva guía bajo el ciclo PDCA.

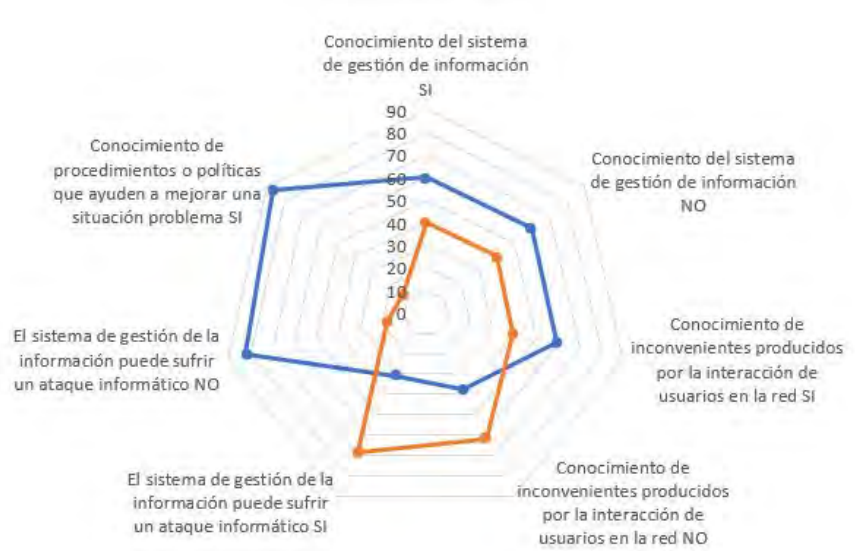
b) Elaboración de instrumento de encuesta para conocer la opinión de personas que laboran en el GAD Municipal de Naranjal.

c) Evaluación de los resultados obtenidos.

Una vez realizado la aplicación de la encuesta se procedió con la tabulación de los datos, utilizando Excel para la presentación de los resultados.

2.2. Análisis descriptivo de los resultados

Figura 2.2: Opinión de personal del GAD Municipal del cantón Naranjal



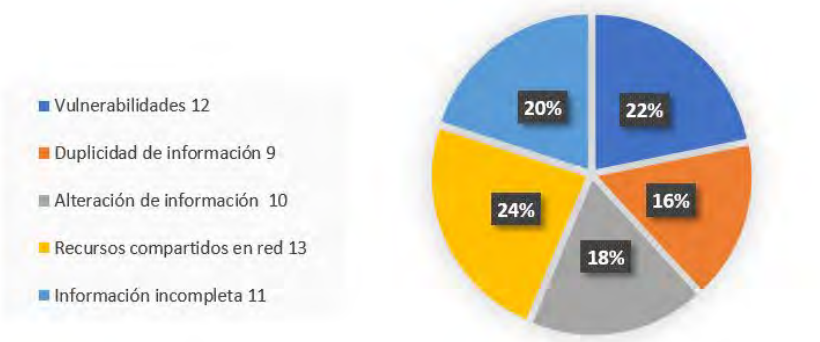
Fuente: Encuesta a usuarios internos del GAD Municipal de Naranjal
Elaborado por: Ing. Alex Ávila

Como se observa en el Gráfico 1 el 40 % desconoce del sistema de gestión de información o interacción de la red y desconocen de los ataques informáticos; además el 62 % no conocen de políticas o procedimientos, así como manuales relacionados a temas tecnológicos, generando que el 82 % considere necesario incluir normativas de seguridad de la información; lo que se infiere que se debe realizar una inducción del proceso de incluir controles y criterios relacionados a seguridad informática, siendo el objeto de estudio de este trabajo de investigación.

Adicionalmente, también se consultó:

- ¿Cuáles de los siguientes tipos de problemas ha tenido en el sistema?

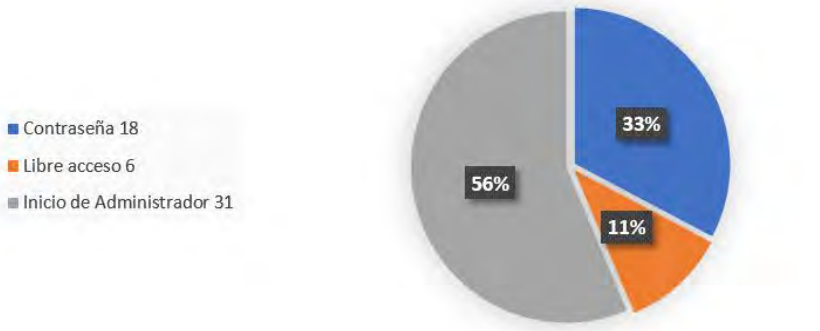
Figura 2.3: Tipos de problemas ha tenido en el sistema



Fuente: Encuesta a usuarios internos del GAD Municipal de Naranjal
Elaborado por: Ing. Alex Ávila

- ¿Para el acceso a la estación de trabajo asignada, requiere lo siguiente?

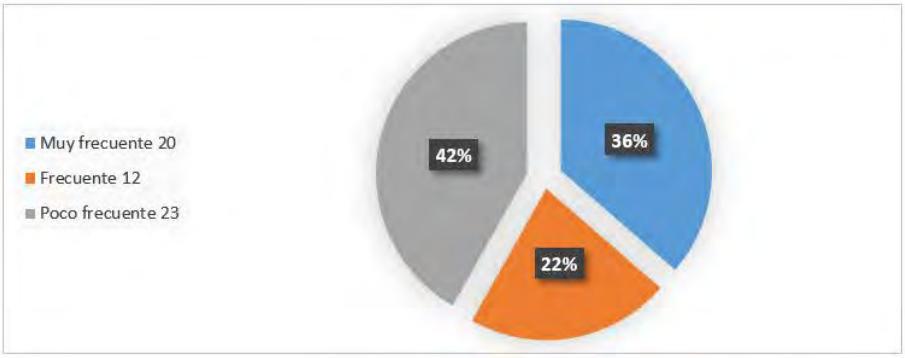
Figura 2.4: Requerimiento para el acceso a la estación de trabajo asignada



Fuente: Encuesta a usuarios internos del GAD Municipal de Naranjal
Elaborado por: Ing. Alex Ávila

- ¿Tipo de frecuencia del ingreso de datos de los contribuyentes en el módulo a cargo?

Figura 2.5: Frecuencia del ingreso de datos de los contribuyentes



Fuente: Encuesta a usuarios internos del GAD Municipal de Naranjal
Elaborado por: Ing. Alex Ávila

Análisis

Como se observa en la Gráfico 2, 3 y 4 se debe planificar desde la gestión tecnológica para reducir problemas relacionados a recursos compartidos; incluso el 56 % de los encuestados indicaron que requieren credenciales con permisos de administrador; en este sentido se identifica la necesidad y sugerencia de realizar una propuesta relacionado a la seguridad de la información.

CAPÍTULO 3

En el este capítulo se realizará el análisis de la situación actual del GAD Municipal de Naranjal, en cuanto a la seguridad de la información. Se empezará con las generalidades y su estructura organizacional, para luego realizar una evaluación del estado actual frente a la seguridad de la información basado en la ISO/IEC 27001:2013. Y, mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 diseñar los controles adecuados.

El GAD Municipal de Naranjal, es una entidad de gobierno seccional que administra el cantón de forma autónoma al gobierno central. La municipalidad está organizada por la separación de poderes de carácter ejecutivo representado por el alcalde, y otro de carácter legislativo conformado por los miembros del concejo cantonal.

La Municipalidad de Naranjal, se rige principalmente sobre la base de lo estipulado en los artículos 253 y 264 de la Constitución Política de la República y en la Ley de Régimen Municipal en sus artículos 1 y 16, que establece la autonomía funcional, económica y administrativa de la Entidad.

Misión

El GAD Municipal de Naranjal, es una organización sin fines de lucro, que cree y participa en el desarrollo cantonal, comprometida con entregar a los y las ciudadanas servicios de calidad y calidez, con un talento humano responsable, competitivo e innovador, empeñado en servir con responsabilidad y puntualidad, para generar productividad y bienestar a la comunidad.

Visión

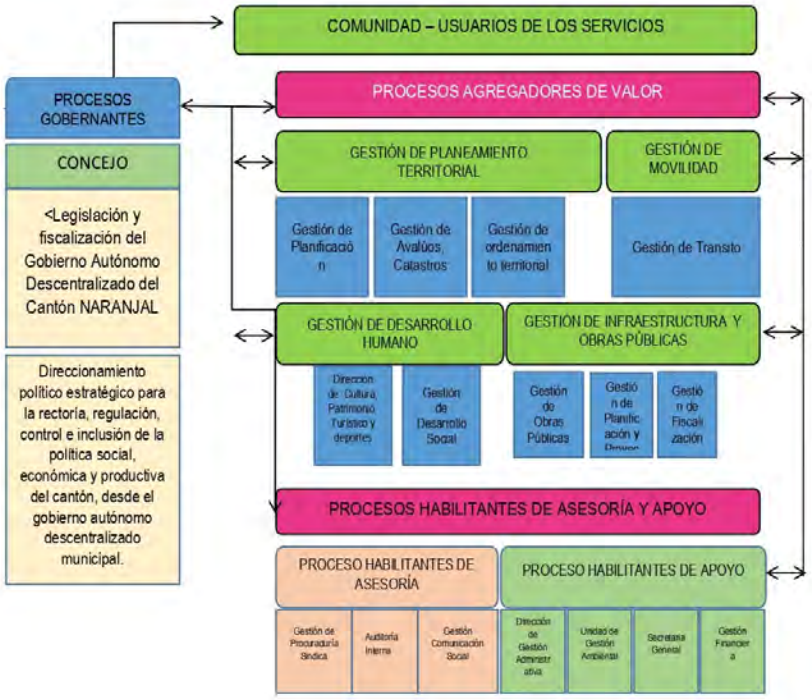
La entidad se constituirá en una organización altamente eficiente capaz de gerenciar productos, procesos, proyectos compatibles con la dinámica estatal y social en forma desconcentrada, descentralizada y con equidad de género.

Estructura organizacional del GAD Municipal de Naranjal

Reformas orgánicas del Ministerio para la gestión de la organización. Para cumplir con su misión y responsabilidades, el Municipio de Naranjal ha adoptado los siguientes procedimientos.

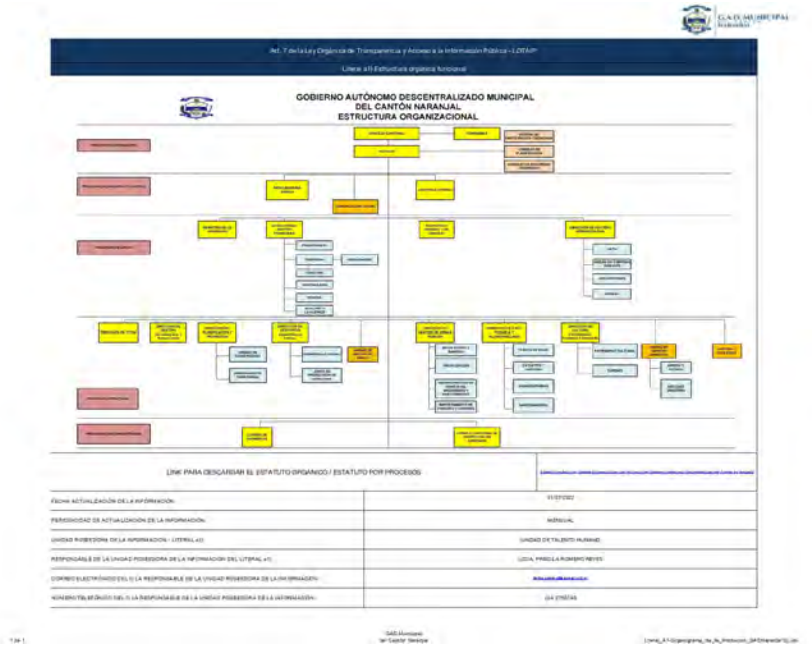
- **Procesos Gobernantes:** Son responsables de establecer las políticas y normas de funcionamiento de la organización en su conjunto.
- **Procesos Habilitantes:** Son responsables de los procesos de gestión y organización y de ellos mismos para crear los productos y servicios que hacen viables las operaciones de la organización.
- **Procesos Agregadores de valor:** Elaboración, gestión y control de productos y servicios para usuarios externos.

Figura 3.1: Mapa de procesos del GAD Municipal de Naranjal



Fuente: GAD Municipal de Naranjal

Figura 3.2: Organigrama del GAD Municipal de Naranjal



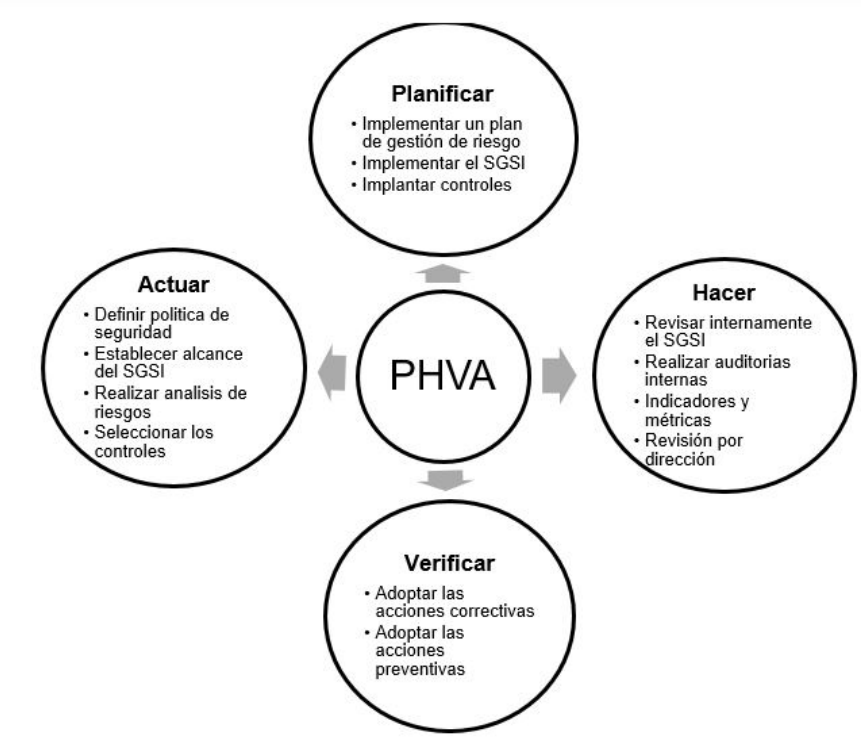
Fuente: Sitio Web del GAD Municipal de Naranjal LOTAIP Literal A1

3.1. Propuesta de solución

El sistema de Gestión de Seguridad de la Información hace referencia a un conjunto de normas y procedimientos para alcanzar un nivel adecuado respecto a la seguridad de la información.

Para el desarrollo de este proyecto se utilizará el ciclo PHVA (Planificar, Hacer, Verificar y Actuar), el cual partirá de la asociación entre las acciones y la ISO/IEC 27001:2013 y la ISO/IEC 27002:2022 como se observa la figura. Se optó por dicha metodología debido a la mejora continua de los servicios y procesos en una organización.

Figura 3.3: Metodología para la propuesta



Elaborado: Ing. Alex Ávila

3.1.1. Fase 1: Definición del alcance y los límites del Protocolo SGSI.

Las necesidades de la organización (en este caso el departamento de TI del municipio) deben determinar el alcance y la idoneidad del sistema de gestión de seguridad de la información.

Alcance del SGSI
Como parte de este proyecto, el departamento de TI del GAD Municipal de Naranjal obtuvo un diseño de SGSI y definió un conjunto de políticas y controles

para proteger los recursos de información del departamento, en vista de los servicios críticos prestados, para la correcta ejecución de las actividades y procesos de la organización.

Objetivos del SGSI

- Protección de los activos de información relacionados con el almacenamiento de información en el departamento de informática del GAD Municipal de Naranjal.
- Definir los controles de seguridad para mantener la confidencialidad, integridad y disponibilidad de los activos de información.

3.1.2. Fase 2: Definición de la política de la seguridad de la información.

Políticas de Seguridad

Ámbito

Esta política de seguridad de la información debe ser divulgada y cumplida por todos los empleados involucrados en el uso de los sistemas de información y equipos tecnológicos.

Objetivo

Custodiar los recursos tecnológicos que son utilizados en la institución Municipal de amenazas (internas o externas y/o intencionales o accidentales), asegurando así que se cumpla con la seguridad, disponibilidad e integridad de la información.

Políticas de los activos de información.

Objetivo
Evitar que se den accidental o deliberadamente los riesgos potenciales de los recursos de información, relacionados con el negocio del día a día que pueden interrumpir las actividades de entidad Municipal.

Acciones

- Se deben definir procedimientos eficaces para el rotulado y manejo de información, los mismos deben contemplar los recursos de información tanto en formatos físicos como electrónicos.
- Todos los activos deben tener una persona responsable, quien será el encargado de la protección de los mismos.
- El custodio de los activos debe definir qué usuarios pueden acceder a los datos que estos contengan.
- Los activos de información deben estar salvaguardados con cables de seguridad en todo momento para evitar pérdidas o robos.

- Las estaciones de trabajo se deben mantener en estricto control, para lo cual se deberá utilizar contraseñas de acceso a su computador y aplicaciones, evitando el acceso indebido a la información cuando el personal no se encuentre físicamente en su estación de trabajo.
- Se debe controlar el mantenimiento preventivo del equipamiento informático de acuerdo a las indicaciones de proveedores, el cual asegurará su disponibilidad e integridad permanentemente.

Políticas del personal

Objetivo

Definir mecanismos para reducir el riesgo de error humano y hacer un uso adecuado de las responsabilidades de los recursos y el personal relacionados con la seguridad de la información.

Acciones

- Asegurar que los usuarios autorizados tengan acceso a la información y sistemas asociados cuando se requiera.
- Los usuarios son responsables de mantener la integridad de sus cuentas y proteger todas las credenciales de acceso.
- No está permitido a los usuarios compartir cuentas o passwords con otras personas, romper seguridades.
- No debe abusar de los recursos disponibles.
- Se prohíbe el acceso a archivos de otros usuarios, a no ser que le sea permitido por parte del responsable del activo.
- Si el usuario identifica que la cuenta y/o clave ha sido violada, debe contactar al departamento de IT, informar el inconveniente y cambiar la contraseña inmediatamente.
- Todo el personal es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.
- Es necesario establecer la responsabilidad sobre el cumplimiento de las normas de seguridad de la información tanto de los empleados como del personal administrativo o de servicio, según corresponda. Los procesos contractuales deberán establecer las responsabilidades de cada empleado en lo que a seguridad de la información se refiere.
- Como parte de sus términos y condiciones iníciales de reclutamiento, los empleados deberán firmar un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información.
- Cada integrante de la institución Municipal deberá recibir una adecuada capacitación y actualización periódica en lo relacionado a la política y normas relacionadas a la seguridad. Esto incluirá los requerimientos de seguridad y las responsabilidades que cada usuario adquiere al iniciar sus labores.

Políticas de seguridad física

Propósito

Prevenir y evitar el acceso no autorizado, daño e intrusión a las instalaciones e información de la institución Municipal, protegiendo así su equipo e información.

Acciones

- Todos los empleados deben contar con una identificación que permita su ingreso a las instalaciones de la institución Municipal.
- En zonas altamente “sensibles” solo deberá transitar el personal autorizado para ese lugar.
- El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas, peligros ambientales, y las oportunidades de acceso no autorizado.
- La protección se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas.
- La institución Municipal debe utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

Políticas de control de acceso e ingreso a los sistemas

Objetivo

Evitar el acceso no autorizado a los sistemas de información, bases de datos y servicios de información en general, y concienciar a los usuarios de sus responsabilidades en el uso de los mismos.

Acciones

- Todos los usuarios deben ser autentificados. Cada usuario debe ser identificado por un nombre y pertenecer a un grupo dentro del sistema operativo o a un rol dentro de la base de datos.
- Cuando un usuario ya no es parte del personal de la institución Municipal, su cuenta debe ser suspendida inmediatamente.
- Los usuarios deben ser capaces únicamente de modificar los datos que les pertenecen, y sólo podrán consultar los datos siempre y cuando estos estén autorizados para hacerlo.
- Sólo el administrador IT debe tener la capacidad de conectarse a los recursos del sistema en modo privilegiado para realizar tareas administrativas.
- Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad, así mismo, será aprobado, controlado y registrado en detalle por los responsables de cada área.

- Se debe definir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a la información, limitando y controlando la asignación, uso de privilegios.
- A fin de mantener un control eficaz de acceso a los datos y servicios de información, el Propietario de la Información llevará a cabo un proceso formal, a intervalos regulares de no más de 6 meses, a fin de revisar los derechos de acceso de los usuarios.
- Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas y deben cumplir las directivas que se impartan a tal efecto.
- El responsable de la administración de los sistemas tiene que asegurar que la información esté disponible cuando sea necesario.
- La información confidencial debe manejarse bajo el criterio de acceso autorizado y no debe estar sujeta a cambios no autorizados.
- Cuando exista la necesidad de otorgar accesos especiales a la información confidencial, se llevará a cabo una evaluación de riesgos para identificar los requerimientos de controles específicos.

Políticas de software

Objetivo

Lograr el nivel adecuado de integridad, confidencialidad y disponibilidad de todos los dispositivos y la información relacionada a través de medidas comunes en cada estación de trabajo. Su objetivo principal es asegurar la continuidad operativa de los procesos y servicios.

Acciones

- Las estaciones de trabajo deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios no están autorizados a deshabilitar este control.
- Los usuarios no deben instalar software en sus estaciones de trabajo, en los servidores de la red, o en otras máquinas, incluso si este software es libre o no licenciado; toda instalación de software debe hacerla un responsable del área de Sistemas.
- No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor.
- Los programas de juegos no son permitidos en las estaciones de trabajo de los usuarios.
- Todo software desarrollado o adquirido debe ser validado previo a su uso.
- Se deberá mantener una base de datos actualizada que contenga un registro del software autorizado para su uso e instalación en la institución Municipal.

Políticas de redes

Objetivo

Almacenar y mantener los datos enviados a través de la red, reducir el riesgo que plantea el acceso indebido a los datos y administrar la entrega de tráfico de datos seguros en la institución Municipal.

Acciones

- Los datos transmitidos sobre redes públicas deben ser encriptados.
- El acceso a redes externas (públicas y privadas) debe hacerse a través de un firewall.
- Se debe identificar y autenticar cualquier sujeto en la red institucional.
- Sólo se permiten habilitar los siguientes servicios de red: SMTP, POP3, HTTP, SSH, SFTP, HTTPS.
- Se debe etiquetar en forma externa las redes disponibles como de acceso abierto, acceso restringido o acceso altamente restringido, de modo que los usuarios o propietarios de los datos estén al tanto de la protección ofrecida.
- Un responsable del área de Sistemas deberá gestionar el acceso a los servicios y recursos de red, de acuerdo a las responsabilidades de cada cargo o por solicitud formal de un empleado aprobado por el Jefe de Área respectivo.
- El camino de las comunicaciones será controlado, es decir se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma. Dichos controles se podrán implementar en los gateways que separan los diferentes dominios de la red.
- Se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino.
- Se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino.

Políticas de correo electrónico

Objetivo

Garantizar la confidencialidad de los mensajes de correo electrónico, su uso adecuado y las obligaciones únicas entre la institución Municipal y sus miembros asociados a este servicio.

Acciones

- Para las operaciones, únicamente se utilizarán los correos electrónicos asignados por la institución Municipal, no se puede emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos de trabajo.

- La información general puede enviarse dentro de la institución Municipal sin encriptación, pero la información confidencial siempre debe ser encriptada. Todos los mensajes de correo electrónico que contengan información concerniente, a números de tarjetas de crédito, claves de acceso, información de investigación y desarrollo e información sensible de entidades externas, debe ser encriptados antes de ser transmitidos.
- Todos los mensajes de correo electrónico deben contener el nombre y apellidos del remitente, su cargo, dirección y número telefónico.
- En todos los mensajes de correo electrónico salientes, debe agregarse un pie de página, en el que se indique que el mensaje puede contener información confidencial, que es para el uso de los destinatarios nombrados, que ha sido registrado para propósitos de archivo.
- El personal no debe abrir archivos adjuntos de correos electrónicos desconocidos, a menos que hayan sido descargados y analizados por el software antivirus aprobado.
- Queda prohibido acceder a mensajes de correo electrónico tipo SPAM, así como también retransmitir este tipo de mensajes.
- No está autorizado enviar mensajes que contengan virus, datos corruptos, texto acosador, difamatorio, obsceno, que atente contra la integridad del personal y/o de la institución Municipal.
- El tamaño permitido de archivos adjuntos no debe exceder de 10MB en un correo electrónico.
- El correo electrónico no debe ser considerado como medio de almacenamiento, por lo que el usuario deberá realizar un mantenimiento constante de su cuenta, archivando la información importante, eliminando correos, etc.
- El responsable de IT deberá monitorizar el uso de correo electrónico del personal, así como también asegurar la eliminación constante de correos con histórico mayor a tres meses.

Políticas de internet

Objetivo

Establecer controles para reducir los riesgos que presenta el acceso a Internet que expone a la institución Municipal directamente a códigos maliciosos que pueden afectar directamente la integridad, disponibilidad y confidencialidad de la información que trata cada elemento de la red.

Acciones

- Tendrán acceso al Internet personal administrativo, y para este caso, los responsables del comercio electrónico en la institución Municipal.
- Los navegadores permitidos deberán establecerse de acuerdo a requerimientos para uso de la web de la institución Municipal.
- No se debe utilizar el Internet para visualizar o descargar música, películas u otros archivos no legales; material pornográfico; descargar software peligroso, no licenciado, o de contenido ilícito; o para uso privado, etc.

- No se deben abrir documentos adjuntos o hacer clic en enlaces de mensajes no solicitados o sospechosos.
- Los usuarios deben abstenerse de visitar sitios restringidos por la institución de manera explícita o implícita, o sitios que afecten la productividad de la institución Municipal.
- Además, no deben brindar cualquier tipo de información institucional en sitios no autorizados o que no cuenten con mecanismos de seguridad que garanticen la confidencialidad de la información en tránsito.
- Tampoco se debe utilizar el Internet para participar en grupos de discusión en Internet, Listas de Correo, chats o cualquier otro foro público, a menos que su participación haya sido expresamente autorizada formalmente por la institución Municipal.
- El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.
- El responsable del área de Sistemas, deberá definir procedimientos eficaces para solicitar y aprobar accesos a Internet. Los accesos serán autorizados por el jefe de Área respectivo.

Políticas de backup

Objetivo

Proporcionar orientación para ayudar a mantener la disponibilidad de información de acuerdo con las necesidades continúas previstas a nivel de operaciones y, por lo tanto, a nivel de la institución Municipal.

Acciones

- Definir el mecanismo y/o programa para realizar respaldos de información.
- El usuario deberá depurar la información previo a realizar un respaldo.
- Debe existir un responsable del área de Sistemas que realice los respaldos y la restauración de los mismos. Solo el encargado puede realizar dichas tareas.
- Los respaldos deben hacerse con regularidad en base a un cronograma preestablecido, se recomienda sean realizados con una frecuencia diaria.
    - Realizar la clasificación de información: frecuente, debe ser información liviana para acceso rápido; histórica, es robusta y pesada, se acceda de manera esporádica a esta información y el respaldo puede ser a un lapso mayor al definido para la información frecuente.
    - Se deben documentar los procedimientos para restaurar el sistema después de fallas serias en los discos u otros componentes de hardware y bajo diferentes tipos de desastres.
    - Será necesario identificar mecanismos que permitan que las actividades de respaldo y recuperación de la información sean las más adecuadas, en lo relativo a costo / beneficio.
    - Establecer procedimiento para sincronización de información vs. backups.

- El responsable de los backups deberá definir procedimientos adecuados para la eliminación segura de los medios de información respetando el cuidado del medio ambiente
- Determinar la ubicación y seguridad donde se colocarán los respaldos.

3.1.3. Fase 3: Identificación de los activos del GAD Municipal de Naranjal en relación a los riesgos.

Los activos de información se protegerán en la medida necesaria para evitar consecuencias negativas que puedan afectar al cumplimiento de sus objetivos.

Identificación de activos

En la tabla siguiente muestra la acumulación de información en el sector de las tecnologías de la información como resultado de la investigación de campo a la que se refiere específicamente el GAD Municipal del cantón Naranjal mediante la observación y la recopilación de información “in situ”.

Para identificar los activos y cualquier factor de riesgo, es necesario hacer una lista de activos, que debe incluir: Activos tangibles (hardware) así como activos intangibles (software e información) involucrados en el comercio electrónico. Para cada activo que se identifica, ISO clasifica los activos de la siguiente manera:

Tabla 3.1: Identificación de activos.

Nº	ID	ACTIVOS	DESCRIPCIÓN	TIPO	RESPONSABLE
1	INFO-001	Físico	Dispositivos de almacenamiento NAS, respaldo de las bases de datos institucional y archivos digitales	Dato	Departamento de TIC
2	INFO-002	Físico	Equipos servidores virtualizados (PROXMOX)	Dato	Departamento de TIC
3	INFO-003	Físico	Dispositivos de comunicaciones, equipos de cómputo, redes e impresión	Dato	Departamento de TIC
4	SW-001	Software	Sistema Integral de Información Multifinalitario siimV6 OpenERP y siim v7 en producción	Aplicación	Departamento de TIC
5	SW-002	Software	Sistema Integral de Información Multifinalitario siimV6 OpenERP y siim v7 en desarrollo o pruebas	Aplicación	Departamento de TIC
6	SW-003	Software	Sitio web y correo institucional en la nube (hosting)	Aplicación	Departamento de TIC
7	SW-004	Software	Firewall MikroTik	Aplicación	Departamento de TIC
8	SW-005	Software	Sistemas operativos, Windows, Linux	Aplicación	Departamento de TIC

Fuente: GAD Municipal de Naranjal, 2022

Valoración de los activos

Una vez identificados los activos, se debe identificar y evaluar la importancia de

cada uno de ellos, teniendo en cuenta los criterios de disponibilidad, integridad y confidencialidad. Se definieron medidas cualitativas para determinar la importancia de cada activo de información identificado por el departamento de TI.

Tabla 3.2: Criterio de validación de los activos

CRITERIO	VALOR	DESCRIPCIÓN
Confidencialidad	0	No es relevante
	1	El acceso a la información sobre los activos no interfiere con las actividades diarias de la unidad de TI.
	2	El acceso a la información sobre los activos sí interfiere con las actividades diarias de la unidad de TI.
	3	El acceso a la información sobre los activos interfiere gravemente con las actividades diarias de la unidad de TI.
Integridad	0	No es relevante
	1	No afecta a la variación de las actividades cotidianas del departamento de informática.
	2	Afecta a la variación de las actividades cotidianas del departamento de informática.
	3	Afecta gravemente a la variación de las actividades cotidianas del departamento de informática.
Disponibilidad	0	No es relevante
	1	La presencia o ausencia de activos no es relevante.
	2	La presencia o ausencia de activos es relevante.
	3	La presencia o ausencia de activos es relevante grave.

Fuente: GAD Municipal de Naranjal, 2022

Tabla 3.3: Nivel de criticidad.

!

Valor	Criticidad
0	No aplica
1	Baja
2	Baja
3	Baja
1	Media
2	Media
3	Media
1	Alta
2	Alta
3	Alta

Fuente: GAD Municipal de Naranjal, 2022

La unidad informática evaluó cada uno de sus activos según los siguientes criterios de evaluación dimensional, que son:

C=Confidencialidad

I=Integridad

D=Disponibilidad

La evaluación de las herramientas informáticas existentes dio como resultado una lista agrupando 8 activos muy importantes, que se presentan en el cuadro 4. En consecuencia, la Agencia debe asignar recursos suficientes para protegerlos y mantener un nivel de riesgo aceptable para evitar la interrupción de las actividades.

Tabla 3.4: Nivel de criticidad.

ID	Activo	C	I	D	Nivel	Valoración
INFO-001	Dispositivos de almacenamiento NAS, respaldo de las bases de datos institucional y archivos digitales	3	3	3	9	Alta
INFO-002	Equipos servidores virtualizados (PROXMOX)	2	3	3	8	Alta
INFO-003	Dispositivos de comunicaciones, equipos de computo, redes e impresión	2	2	3	7	Alta
SW-001	Sistema Integral de Información Multifinalitario siimV6 OpenERP y siim v7 en producción	2	3	3	8	Alta
SW-002	Sistema Integral de Información Multifinalitario siimV6 OpenERP y siim v7 de desarrollo o pruebas	2	3	3	8	Alta
SW-003	Sitio web y correo institucional en la nube (hosting)	2	2	2	6	Media
SW-004	Firewall MikroTik	3	3	3	9	Alta
SW-005	Sistemas operativos, Windows, Linux	1	2	3	6	Media

Fuente: GAD Municipal de Naranjal, 2022

3.1.4. Fase 4: Control de riesgos

Identificación de amenazas

Las organizaciones están expuestas a muchos tipos de amenazas. Hay que identificarlas, analizarlas y determinar su probabilidad de ocurrencia.
Con el fin de la identificación, el propietario del activo determina cómo se han comprometido la confidencialidad, la integridad y la disponibilidad del activo.
La detección, prevención y control oportunos de las situaciones peligrosas identificadas como amenazas es la primera estrategia orientada a la gestión de riesgos.
El riesgo es la probabilidad de que se produzca una amenaza que explote una vulnerabilidad y afecte negativamente a los activos de información de una organización, y viene determinado por los siguientes factores.

Tabla 3.5: Identificación de amenazas.

Inciso	Amenaza
A	Daño físico
B	Eventos Naturales
C	Pérdida de servicios esenciales
D	Perturbación por radiación
E	Compromiso de la información
F	Fallas técnicas
G	Acciones no autorizadas
H	Compromiso de las funciones
I	Errores humanos
J	Fallas en la gestión y la operación del servicio

Elaborado por: Ing. Alex Ávila Coello

Identificación de vulnerabilidades

El siguiente paso fue identificar las vulnerabilidades explotables y su impacto en los activos de información definidos en el SGSI. Cuando una vulnerabilidad es explotada por una amenaza, el impacto puede ser clasificado como alto, medio o bajo, lo que resulta en una situación negativa en el día a día del negocio, la pérdida de la continuidad del negocio y la incompatibilidad con los objetivos y la misión de la organización.

Tabla 3.6: Identificación de vulnerabilidades

ID	Activo	Amenaza	Vulnerabilidad
INFO-001	Dispositivos de almacenamiento NAS, respaldo de las bases de datos institucional y archivos digitales	Perdida de información	Eventos eléctricos, no existe la contratación de hosting dedicado
INFO-002	Equipos servidores virtualizados (PROXMOX)	Daños físicos y lógicos	Eventos eléctricos
INFO-003	Dispositivos de comunicaciones, equipos de computo, redes e impresión	Daños físicos y lógicos	Eventos eléctricos
SW-001	Sistema Integral de Información Multifinalitario siimV6 OpenERP y siim v7 de producción	Mal uso de credenciales de acceso por partes de los usuarios clientes, en los distintos módulos que conforman los sistemas de información	No existen políticas ni controles adecuados, para la seguridad de la información
SW-002	Sistema Integral de Información Multifinalitario siimV6 OpenERP y siim v7 en desarrollo o pruebas	Mal funcionamiento de equipos a causa de averías	Eventos eléctricos
SW-003	Sitio web y correo institucional en la nube (hosting).	Infección con software malicioso	Falta de medidas de detección y prevención contra códigos maliciosos.
SW-004	Firewall MikroTik	Ataques externos contra el sistema, mala administración del servicio de internet	Falta de mecanismos de seguridad
SW-005	Sistemas operativos, Windows, Linux	Daño a causa de código malicioso (virus)	No se posee antivirus con licencia

Fuente: GAD Municipal de Naranjal, 2022

Posibilidad de impacto

La probabilidad de que se produzca un evento refleja la posibilidad de que se produzca una amenaza o se explote una vulnerabilidad, y puede verificarse revi-

sando eventos pasados y solicitando información a los usuarios y administradores sobre su frecuencia.

Este proyecto identificó cinco probabilidades cualitativas a partir de la información proporcionada por el departamento de TI, basándose en eventos de actividades anteriores.

Tabla 3.7: Niveles de probabilidad.

Probabilidad	Descripción
Muy baja	No es probable que la amenaza explote una vulnerabilidad
Baja	No ha ocurrido, es poco probable que la amenaza explote una vulnerabilidad.
Media	Ha ocurrido una vez al año, existe la probabilidad de que la amenaza explote una vulnerabilidad.
Alta	Ha ocurrido una vez al mes, es probable que la amenaza explote una vulnerabilidad.
Muy Alta	Ha ocurrido una vez a la semana, la amenaza explotará una vulnerabilidad.

Elaborado por: Ing. Alex Ávila Coello

Mapa de riesgos

Cuando las vulnerabilidades y amenazas que puedan afectar a los activos del departamento de tecnología de la información, El nivel de riesgo es la relación que existe entre la probabilidad de ocurrencia de un incidente y el impacto resultante del mismo. Los tipos son:

- **Muy bajo:** La materialización de una amenaza podría ser insignificante.
- **Bajo:** La materialización de una amenaza podría tener consecuencias mínimas.
- **Medio:** La materialización de una amenaza puede tener como consecuencia la afectación en las actividades de la unidad, por un periodo de tiempo no mayor a cuatro horas.
- **Alto:** La materialización de una amenaza puede tener como consecuencia la afectación en las actividades de la unidad, por un tiempo no mayor a diez horas.
- **Muy alto:** La materialización de una amenaza puede tener como consecuencia la afectación total en las actividades de la unidad.

Evaluación de riesgo

Partiendo del concepto de utilización del riesgo en términos de pérdidas físicas, económicas y continuas, es necesario definir el riesgo, comprender su naturaleza y cómo afecta a los activos de información y a los distintos procesos y servicios.

El proceso de evaluación de riesgos debe llevarse a cabo con regularidad para validar la calificación asignada al riesgo y para garantizar que el riesgo se ha abordado adecuadamente y se ha minimizado. Por último, se obtiene información para la toma de decisiones y la adopción de nuevas medidas sobre las estrategias de mitigación de riesgos.

3.1.5. Fase 5: Fijación de controles y objetivos de control.

A continuación, se elaboró un cuadro con todos los controles que se establecieron en el GAD Municipal de Naranjal.

Tabla 3.8: Consulta de Fuentes bibliográficas en SCOPUS y WOS con el término ISO/IEC 27001: 2013 Periodo 2018 - 2022

Controles	Objetivos	Estrategias
Política de Seguridad de la Información	Garantizar la idoneidad, la adecuación y la eficacia continuas de la dirección de gestión y el apoyo a la seguridad de la información de acuerdo con los requisitos comerciales, legales, estatutarios, reglamentarios y contractuales.	Custodiar los recursos tecnológicos que son utilizados en la institución Municipal de amenazas (internas o externas y/o intencionales o accidentales), asegurando así el que se cumpla con la seguridad, disponibilidad e integridad de la información.
Roles y responsabilidades de seguridad de la información	Establecer una estructura definida, aprobada y entendida para la implementación, operación y gestión de la seguridad de la información dentro de la organización.	Se definirá y asignará roles para las todas las responsabilidades de la seguridad de la información
Segregación de funciones	Reducir el riesgo de fraude, error y elusión de los controles de seguridad de la información.	Se determinará que deberes y responsabilidades deberán segregarse para evitar problemas en corto, mediano y largo plazo.
Contacto con las autoridades	Garantizar que se produzca un flujo de información adecuado con respecto a la seguridad de la información entre la organización y las autoridades legales, reguladoras y de supervisión pertinentes.	Se definirán diversos protocolos de comunicación con autoridad, como es el caso de determinar quienes podrán contactarse directamente con un superior y de qué manera lo hará, ya que esto garantizará la seguridad de la información y facilitrá la intercomunicación entre entidades.
Contacto con grupos de interés especial	Garantizar que se produzca un flujo adecuado de información con respecto a la seguridad de la información.	El GAD Municipal de Naranjal deberá contacto con grupos de interés especial u otros foros especializados en seguridad.

Seguridad de la información en la gestión de proyectos	Para garantizar que los riesgos de seguridad de la información relacionados con proyectos y entregables se aborden de manera efectiva en la gestión de proyectos a lo largo del ciclo de vida del proyecto.	La seguridad de información debe integrarse en la gestión de proyectos.
Inventario de información y otros activos asociados	Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.	Se deberán identificar los activos asociados con la información y las instalaciones de procesamiento de información.
Uso aceptable de la información y otros activos asociados	Deben identificarse, documentarse e implementarse reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.	Se determinará y socializará requisitos de seguridad de la información que garanticen el correcto manejo de la data y demás activos asociados.
Devolución de bienes	Para proteger los activos de la organización como parte del proceso de cambio o terminación de empleo, contrato o acuerdo.	En caso de terminación de contratos o acuerdos se formalizará la devolución de los activos electrónicos y físicos pertenecientes a la organización.
Clasificación de la información	Asegurar la identificación y comprensión de las necesidades de protección de la información de acuerdo con su importancia para la organización.	Toda información será clasificada de acuerdo a su nivel de importancia dentro de la organización para así evitar inconvenientes con datos críticos o sensibles para la entidad.
Etiquetado de la Información	Facilitar la comunicación de la clasificación de la información y apoyar la automatización del procesamiento y la gestión de la información.	Se deben definir procedimientos eficaces para el rotulado y manejo de información, los mismos deben contemplar los recursos de información tanto en formatos físicos como electrónicos.

Transferencia de la Información	Para mantener la seguridad de la información transferida dentro de una organización y con cualquier parte externa interesada.	Se establecerá y socializará protocolos y acuerdos específicos que garantice sólo las personas interesadas relevantes tengan acceso a la información en caso de una transferencia, por ende, se diseñará controles para salvaguardar la integridad de la data en caso de accesos no autorizados o enrutamientos incorrectos.
Control de acceso	Para garantizar el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.	Se gestionará listas de accesos para que sólo las personas indicadas puedan acceder a la data y demás activos asociados.
Gestión de identidad	Permitir la identificación única de personas y sistemas que acceden a la información de la organización y otros activos asociados y permitir la asignación adecuada de derechos de acceso.	Se le asignará un id que permita identificar a qué información y activos tendrán acceso cada uno de los colaboradores de acuerdo a su rol o jerarquía.
Información de autenticación	Para garantizar la autenticación adecuada de la entidad y evitar fallas en los procesos de autenticación.	Se centralizará los derechos de acceso otorgados a cada uno de los usuarios acordes a sus roles y trabajo y los cuales se modificarán cada vez que sea necesario.
Derechos de acceso	Para garantizar que el acceso a la información y otros activos asociados se defina y autorice de acuerdo con los requisitos comerciales.	Se centralizará los derechos de acceso otorgados a cada uno de los usuarios acordes a sus roles y trabajo y los cuales se modificarán cada vez que sea necesario.

Seguridad de la información para el uso de servicios en la nube	Especificar y administrar la seguridad de la información para el uso de servicios en la nube.	Para servicios en la nube la entidad definirá todos los parámetros de seguridad necesarios para emplear estos recursos sin peligro alguno.
Evaluación y decisión sobre eventos de seguridad de la información	Para asegurar una categorización y priorización efectiva de los eventos de seguridad de la información.	Se categorizará las vulnerabilidades y amenazas de mayor relevancia que puedan comprometer la integridad de los activos de la entidad.
Seguridad de la información durante la interrupción	Para proteger la información y otros activos asociados durante la interrupción.	Se diseñarán controles de seguridad que serán testeados de manera exhausta para garantizar la integridad de la información y demás activos durante cualquier interrupción en operación.
Requisitos legales, estatutarios, reglamentarios y contractuales	Asegurar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la seguridad de la información.	Se desarrollarán políticas para garantizar la seguridad de la información, asimismo, se clasificará la información y demás activos asociados acorde a su función.
Revisión independiente de la seguridad de la información	Asegurar la idoneidad, adecuación y eficacia continuas del enfoque de la organización para gestionar la seguridad de la información.	Se efectuarán políticas y procesos para revisiones independientes periódicas
Cumplimiento de políticas, normas y estándares de seguridad de la información	Para garantizar que la seguridad de la información se implemente y opere de acuerdo con la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos del tema.	Las altas cúpulas de la entidad a tratar deberán asegurarse que se cumplan todos los requisitos de seguridad preestablecidos con la mayor cabalidad posible.

Procedimientos operativos documentados	Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.	Se documentará y socializará los procedimientos necesarios para llevar a cabo todo tipo de actividades operativas dentro de la organización.
Términos y condiciones de empleo	Asegurar que el personal comprenda sus responsabilidades de seguridad de la información para las funciones para las que se le considera.	De forma eventual se dictaminarán capacitaciones básicas sobre seguridad de la información, para así evitar fugas de información o que alguno de los colaboradores caiga en ataques de tipos phishing.
Proceso disciplinario	Asegurar que el personal y otras partes interesadas relevantes entiendan las consecuencias de la violación de la política de seguridad de la información, para disuadir y tratar adecuadamente al personal y otras partes interesadas relevantes que cometieron la violación.	Las políticas de seguridad estipuladas serán diseñadas de manera clara para asegurarse que todos los colaboradores tengan clara las medidas que se puedan tomar en caso de una violación de alguna clausula establecida.
Acuerdos de confidencialidad o no divulgación	Para mantener la confidencialidad de la información accesible por el personal o partes externas.	Se determinarán y formalizará acuerdos de confidencialidad sobre datos críticos de la institución.
Trabajo a distancia	Para garantizar la seguridad de la información cuando el personal está trabajando de forma remota.	Se gestionará protocolos para salvaguardar la información y tareas en casos de la realización de trabajo remoto o teletrabajo.
Reporte de eventos de seguridad de la información	Para respaldar la notificación oportuna, coherente y eficaz de los eventos de seguridad de la información que pueden ser identificados por el personal.	Se llevará a cabo un registro constante de eventos de seguridad de la información.

Perímetro de seguridad física	Para evitar el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados.	Se prohibirá el acceso a personas particulares o no autorizadas a sitios sensibles de la institución, como es el caso de la data center.
Entrada física	Garantizar solo el acceso físico autorizado a la información de la organización y otros activos asociados.	Solo se les permitirá el acceso a ciertos lugares a las personas autorizadas previamente identificadas.
Aseguramiento de oficinas, salas e instalaciones	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados en las oficinas, salas e instalaciones.	Lugares como salas de conferencia y reunión solo podrá ser accedida si el colaborador tiene un permiso previamente autorizado.
Supervisión de la seguridad física	Para detectar y disuadir el acceso físico no autorizado.	Se llevará a cabo un monitoreo constante a lugares de acceso restringido.
Protección contra amenazas físicas y ambientales	Prevenir o reducir las consecuencias de eventos originados por amenazas físicas y ambientales.	La infraestructura contará con sistemas capaces de proteger picos de voltajes que puedan comprometer a la integridad de los equipos. Asimismo, se realizarán inspecciones aleatorias para detectar presencia de explosivos o armas.
Trabajar en áreas seguras	Para proteger la información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas.	En caso de trabajar en lugares ajenos al puesto de trabajo se deberá evitar el trabajo sin supervisión, para así evitar infracciones de seguridad y actividades maliciosas.
Ubicación y protección del equipo	Reducir los riesgos de amenazas físicas y ambientales, y de accesos y daños no autorizados.	Se propone monitorear las condiciones ambientales de lugares de vital importancia como es el caso de la data center.

Seguridad de los activos fuera de las instalaciones	Para evitar la pérdida, el daño, el robo o el compromiso de los dispositivos externos y la interrupción de las operaciones de la organización.	En caso de que el colaborador deba trabajar en lugares fuera de la entidad y con equipos de la organización, el usuario se deberá comprometer a cuidar tales bienes.
Medios de almacenamiento	Para garantizar solo la divulgación, modificación, eliminación o destrucción autorizadas de la información almacenada.	Se evitará el uso de memorias externas ajenos de la compañía para el respaldo de los archivos de la entidad.
Seguridad de cableado	Para evitar la pérdida, el daño, el robo o el compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización relacionadas con el cableado de energía y comunicaciones.	Se mantendrá un control constante del cableado estructurado de la entidad, para así evitar interrupciones en las operaciones cotidianas.
Mantenimiento del equipo	Para evitar la pérdida, daño, robo o compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización causada por la falta de mantenimiento.	El equipo de TIC's realizará de manera periódica un mantenimiento preventivo a todas las oficinas, y del mismo modo realizará un mantenimiento correctivo apenas se lo solicite.
Eliminación segura o reutilización de equipos	Para evitar la fuga de información de los equipos que se desecharán o reutilizarán.	Solo el equipo de TIC's tendrá la autorización de gestionar con los equipos que ya no se estén utilizando.
Derechos de acceso privilegiado	Para garantizar que solo los usuarios autorizados, los componentes y servicios de software reciban derechos de acceso privilegiado.	Restringir y controlar la asignación y uso de derechos de acceso privilegiado de acuerdo con la política y las reglas de control de acceso específica del tema del Municipio.
Restricción de acceso a la información	Para garantizar solo el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados	El acceso a cualquier información solo será permitido al personal autorizado.

Protección contra software malicioso	Para garantizar que la información y otros activos asociados estén protegidos contra malware.	Se instalará y configurará antivirus con licencias originales.
Gestión de vulnerabilidades técnicas	Para prevenir la explotación de vulnerabilidades técnicas.	Obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información utilizados y evaluar si la organización está expuesta a estas vulnerabilidades.
Eliminación de la información	Para evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información.	Se gestionará y formalizará normas para la correcta eliminación de archivos de la entidad.
Prevención de fuga de datos	Para detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.	Se configurará medidas de prevención para evitar ataques de intrusión como hombre en el medio o botnets de tipo backdoor.
Copia de seguridad de la información	Para permitir la recuperación de la pérdida de datos o sistemas	La información crítica de la institución deberá ser respaldada
Redundancia de las instalaciones de procesamiento de información	Asegurar el funcionamiento continuo de las instalaciones de procesamiento de información.	Se diseñará una red robusta y jerarquizada
Instalación de software en sistemas operativos	Para garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas.	Implementación de un programa para controlar la instalación de software en el sistema operativo.
Seguridad de las redes	Para proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo del compromiso a través de la red.	Se deberá instalar herramientas que permitan salvaguardar la integridad de la red, como es el caso de IDS o IPS

Protección de los sistemas de información durante las pruebas de auditoría	Minimizar el impacto de la auditoría y otras actividades de aseguramiento en los sistemas operativos y procesos comerciales.	Se realizará una auditoría constante a nivel de red para evitar posibles ataques a través de puertos.
Codificación Segura	Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguro de software y sistemas.	El área de desarrollo se verá dividida en tres entornos; desarrollo, prueba y producción. Todo proyecto se realizará en primera instancia en dockers o en servidores locales para comprobar su correcto funcionamiento y se evitará usar repositorios públicos.
Filtrado Web	Para proteger los sistemas contra el malware y evitar el acceso a sitios web no autorizados.	Se auditará las páginas utilizadas por cada uno de los departamentos y se bloquearán por ip los sitios que no cumplan con estándares de seguridad (certificados ssl)

Tabla 3.9: Presupuesto

CPC	DESCRIPC	ESPECIF	CANTIDAD	COSTO	TOTAL
831410012	Estudio para una Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO 27002:2022 en el Departamento de Tecnologías de la Información del GAD Municipal del cantón Naranjal.	10 días	10	6.416,07	6.416,07

Fuente: GAD Municipal de Naranjal, 2022

CONCLUSIONES Y TRABAJO FUTURO

Mediante el análisis del estudio investigativo del trabajo se llegó a las siguientes conclusiones:

La propuesta de un Modelo de sistema de gestión de seguridad de la información, permite estandarizar la información mediante el establecimiento de controles basados en la norma ISO/IEC 27001:2013 relacionado al código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado Municipal del cantón Naranjal, de esta manera se obtiene una adecuada seguridad, disponibilidad e integridad de los datos, y por consiguiente facilidad en la toma de decisiones.

La identificación de los componentes para el Modelo de Sistema de Gestión de Seguridad de la Información se la realizo a través de una encuesta efectuada a los usuarios internos del GAD Municipal de Naranjal, permitiendo la evaluación de las estrategias utilizadas y dando seguimiento al procesamiento de los datos, para que con el empleo de los controles adecuados y normados evitar errores y problemas.

Es importante el establecimiento de una metodología de gestión y mejora continua del Modelo de Sistema de Gestión de Seguridad de la Información, garantizando un adecuado tratamiento de la información, donde con el diseño de estrategias ayuden a minimizar los casos de vulnerabilidad y ataques con respecto a la base de datos y el mal uso de las credenciales de acceso a los sistemas de información y demás recursos tecnológicos por parte de los usuarios internos del GAD Municipal de Naranjal.

Mediante la evaluación del Modelo de Sistema de Gestión de Seguridad de la Información de forma continua, y con el empleo de grupos de expertos de seguridad focal se garantiza un adecuado tratamiento de la información, mediante el diseño de una propuesta relacionada al aporte de mejoras en los controles administrativos bajo la norma ISO/IEC 27001:2013

RECOMENDACIONES

De acuerdo con el estudio de investigación realizado es importante considerar las siguientes recomendaciones:

Proponer a las autoridades respectivas la gestión de alternativas que aporten con mejoras en la gestión del control de la información relacionada a la Norma ISO/IEC 27001:2013 en el departamento de Tecnologías de la Información del GAD Municipal de Naranjal.

Gestionar ante el organismo competente la vinculación de nuevas estrategias de participación en los procesos de gestión de seguridad de la información, para ir actualizando nuevas acciones encaminadas al fortalecimiento de la calidad en la seguridad de la información.

Realizar socializaciones del diseño de la propuesta sobre los controles, procesos y medidas preventivas dando paso a capacitaciones para el personal que labora como usuarios dentro del GAD Municipal de Naranjal.

Establecer una cultura de acciones encaminadas para garantizar la seguridad de la información con respecto a los diferentes departamentos de la entidad municipal, permitiendo una confiabilidad, integridad y salvaguardar los datos de manera oportuna.

Gestionar la aplicación de manuales que complementen las actualizaciones de los diferentes comandos relacionada a la Norma ISO/IEC 27001:2013, para la identificación clara y oportuna de la gestión de la información.

BIBLIOGRAFÍA GENERAL

(2018). Assessment of information security management system based on iso/iec 27001:2013 on subdirectorate of data center and data recovery center in ministry of internal affairs. *E3S Web of Conferences*.

(2018). Assessment of information security management system based on iso/iec 27001:2013 on subdirectorate of data center and data recovery center in ministry of internal affairs. *E3S Web of Conferences*.

Benavides Sepúlveda, Alejandra; Blandón Jaramillo, C. (2018). Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. *Scientia et Technica*, page 8.

De León Camelo, J. C. (2019). Diseño de un sistema de gestión de seguridad de la información basado en la norma iso/iec 27001 para entidades del estado.

Hamit, L.C., S. H. M. A. N. . C. S. Y. Y. (2020). Adopting an iso/iec 27005:2011-based risk treatment plan to prevent patients from data theft. *International Journal on Advanced Science, Engineering and Information Technology*, pages 914–919.

ISO (2022). Iso/iec 27001:2013. page https://www.iso.org/standard/54534.html.

ISO.ORG (2022). Iso/iec 27002:2013(en). pages https://www.iso.org/obp/ui/es/iso:std:iso–iec:27002:ed–2:v1:en.

Isotools (2022). https://www.isotools.org/. pages https://www.isotools.org/normas/riesgos–y–seguridad/iso–27001/.

Lema Vinlasaca, Roberto Carlos; Donoso Gallo, D. F. (2018). Implementación de un sistema de seguridad de información basado en la norma iso 27001:2013 para el control físico y digital de documentos aplicado a la empresa lockers s.a.

Lucano Cordones, L. F. (2019). Diagnostico y diseño de un sistema de gestión de seguridad de la información, basado en la norma iso/iec 27001:2013, en un banco público. *Scientia et Technica*.

Nacipucha Cumbe, J. C. (2019). Análisis y diseño para un modelo de gestión de seguridad de la información basados en normas iso/iec 27001:2013 para la empresa artehogar en la ciudad de guayaquil.

Nieves, A. (2017). Diseño de un sistema de gestión de la seguridad de la información basados en la norma iso/iec 27001:2013.

Phirke, A., G.-A. J. (2019). Best practices of auditing in an organization using iso 27001 standard. *International Journal of Recent Technology and Engineering*, pages 691–695.

Tariq, M.I., A.-S. M. N. . B. V. B. M. (2020). Prioritization of information security controls through fuzzy ahp for cloud computing networks and wireless sensor networks. *Sensors (Switzerland)*.

Tigse Moposita, J. L. (2020). Plan de gestión de seguridad informática basado en la norma iso 27001 para el departamento de tecnología de la información de la empresa plasticaucho industrial s.a.

ANEXOS

Anexo 1 Solicitud para levantamiento de información

Figura 4: Solicitud para levantamiento de información

PARA: Abogado. Luigi Rivera Gutiérrez. Msc.
ALCALDE DEL CANTÓN NARANJAL

FECHA: lunes 13 de junio del 2022

22089-A

ASUNTO: SOLICITUD PARA LEVANTAMIENTO DE INFORMACIÓN.

En su despacho. -

De mi consideración:

Yo Ingeniero Alex Armando Ávila Coello, alumno de la MAESTRÍA EN TECNOLOGIAS DE LA INFORMACION de la UNIVERSIDAD ESTATAL DE MILAGRO del actual PROCESO TITULACIÓN - TIC - COHORTE I, periodo académico del 12 de Noviembre 2020 al 05 de Marzo 2022, solicito a usted muy respetuosamente se me conceda los permisos necesarios para ingresar a cada una de las dependencias del GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN NARANJAL, con la finalidad de realizar el respectivo levantamiento de información, el cual me permitirá presentar una PROPUESTA DE UN SISTEMA GESTOR DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013, previo a la obtención del TÍTULO DE MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN.

Por la favorable atención que brinde a la presente, agradezco augurándole muchos éxitos en todas sus valiosas labores a beneficio de la ciudadanía del cantón Naranjal.

Atentamente,

GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN NARANJAL
DPTO. DE SECRETARIA GENERAL
HORA 14:20
FIRMA RECEPCIÓN

Ingeniero
Alex Ávila Coello
MAESTRANTE EN TECNOLOGÍAS DE LA INFORMACIÓN

Elaborado: Ing. Alex Ávila

Anexo 2 Aprobación del GAD Municipal de Naranjal para levantamiento de información

Figura 5: Aprobación del GAD Municipal de Naranjal para levantamiento de información

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL
CANTÓN NARANJAL

Naranjal, 14 de junio de 2022

Oficio GADMCN-AL-LRG-SG-223009-A

Ingeniero
Alex Ávila Coello
MAESTRANTE EN TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD ESTATAL DE MLAGRO.

Ref. Comunicación 13-06-2022
TRAMITE: 222089-A

En virtud a su comunicación señalada en la referencia del 13 de junio de 2022, me permito indicar a usted que cuenta con la **AUTORIZACIÓN** del primer personero municipal para que pueda ingresar a cada una de las dependencias del Gobierno Autónomo Descentralizado Municipal del cantón Naranjal y pueda realizar el levantamiento de información, el cual le permitirá presentar la PROPUESTA DE UN SISTEMA GESTOR DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013, PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN TECNOLOGÍA DE LA INFORMACIÓN.

Particular que comunico para los fines pertinentes.

Cordialmente,

Ab. Gloria Sofía Ramírez Chávez
SECRETARIA GENERAL DEL CONCEJO MUNICIPAL (E)
C. Mora

Con copia: Gestión Administrativa.

14-06-2022
Hora: 15:00 PM

NARANJAL

Av. Olmedo 1201 y Bolívar | 2750 191 - 2750 192 | www.naranjalgob.ec

Elaborado: GAD Municipal del cantón Naranjal

Anexo 3 Constancia del levantamiento de Información en las diferentes dependencias del GAD Municipal de Naranjal.

Figura 6: Dialogo con el alcalde Ab. Luigi Rivera Gutiérrez

Elaborado: Ing. Alex Ávila

Figura 7: Aprobación del levantamiento de información del GAD Municipal de Naranjal.

Elaborado: Ing. Alex Ávila

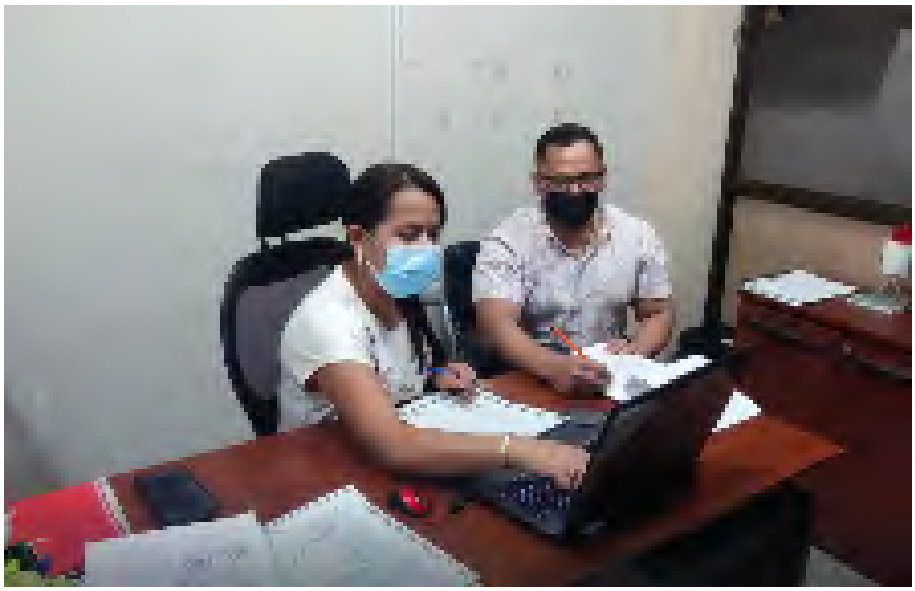
Figura 8: Encuesta realizada al usuario de la Gestión de Tecnología e Informática

Elaborado: Ing. Alex Ávila

Figura 9: Encuesta realizada al usuario de Tesorería Municipal

Elaborado: Ing. Alex Ávila

Figura 10: Encuesta realizada al usuario de Gestión de Dirección Financiera



Elaborado: Ing. Alex Ávila

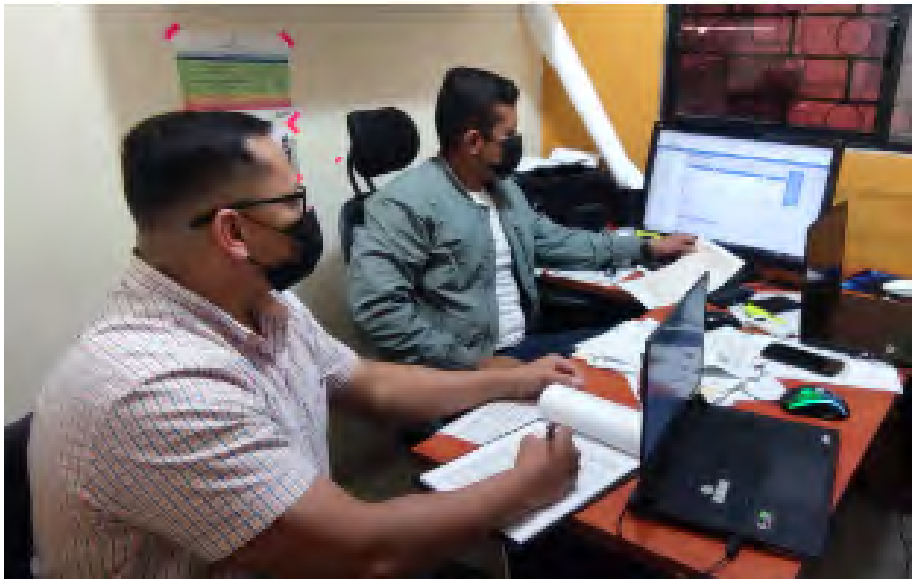
Figura 11: Encuesta realizada al usuario de Directora de Gestión Administrativa (E)

Elaborado: Ing. Alex Ávila

Figura 12: Encuesta realizada al usuario de Presupuesto

Elaborado: Ing. Alex Ávila

Figura 13: Encuesta realizada al usuario de Catastro



Elaborado: Ing. Alex Ávila

Anexo 3 Encuesta

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

Encuesta a usuarios

Estimados:

Este instrumento es de carácter anónimo y de índole académico para la obtención de título de MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN.

Resultados que contribuirán al proyecto de un MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA ESTABLECER CONTROLES BASADOS EN LA NORMA ISO/IEC 27001:2013 MEDIANTE EL CÓDIGO DE PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27002:2022 EN EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN NARANJAL.

Se agradece por su apoyo.

1. **¿Conoce usted del sistema de gestión de información del GAD Municipal de Naranjal?.**

a) Si
b) No

2. **¿Conoce usted de inconvenientes producidos por la interacción de usuarios en la red?.**

a) Si
b) No

3. **¿Usted conoce de procedimientos o políticas que ayuden a mejorar una situación problema?.**

a) Si
b) No

4. **¿Considera usted que el sistema de gestión de la información puede sufrir un ataque informático?.**

a) Si
b) No

5. **¿Tiene conocimientos de manuales de buenas prácticas en el uso del sistema informático?.**

a) Si
b) No

6. **¿Cree usted necesario la aplicación de normativas basadas en la ISO 27001:2013 para mejorar la seguridad de la información?.**

a) SI
b) No

7. **¿Es importante el diseño de un modelo de sistemas de sistema de gestión de seguridad de la información basado en la ISO 27001:2013?.**

a) Si
b) No

Consulta Adicional

1. **Cuáles de los siguientes tipos de problemas ha tenido en el sistema de gestión de información?.**

a) Vulnerabilidades
b) Duplicidad de información
c) Alteración de información
d) Recursos compartidos en red
e) Información incompleta

2. ¿Para el acceso a la estación de trabajo asignada, requiere lo siguiente?

a) Contraseña
b) Libre acceso
c) Inicio de Administrador

3. ¿Tipo de frecuencia del ingreso de datos de los contribuyentes en el módulo a cargo?

a) Muy frecuente
b) Frecuente
c) Poco frecuente

Anexo 4 Informe Técnico

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL
CANTÓN NARANJAL

INFORME TÉCNICO PARA LA CONTRATACIÓN DE UNA CONSULTORIA DE UNA PROPUESTA DE UN MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA ESTABLECER CONTROLES BASADOS EN LA NORMA ISO/IEC 27001:2013 MEDIANTE EL CÓDIGO DE PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27002:2022 EN EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN NARANJAL.

1 ANTECEDENTES

El rápido desarrollo de la tecnología ha creado serios problemas de vulnerabilidad en las organizaciones, con riesgos e inseguridad, así como fraudes informáticos, espionaje, sabotaje, retirada informática e intrusiones o ataques de denegación de servicio. La ISO 27001 es un estándar ISO que establece requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad de la información. Esta norma internacional fue publicada Electrotechnical Commission. ISO 27001 fue publicada como estándar internacional en octubre de 2005, tal como la conocemos hoy, fue el resultado del desarrollo de otras normas relacionadas con la seguridad de la información.

Un sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 tiene como objetivo garantizar que las empresas hayan implementado todos los controles apropiados sobre la seguridad, integridad y disponibilidad de su información, para protegerla de las partes interesadas, socios comerciales y la sociedad en su conjunto. El cumplimiento de la norma ISO 27001 puede ayudar a las empresas a demostrar a sus clientes o socios cuánto se toman en serio la seguridad de la información. La certificación reconocida en la norma ISO 27001 es testimonio del compromiso de la empresa con la gestión de la seguridad de la información.

Las directrices de la OCDE (Organización para la Cooperación y el Desarrollo Económico) tienen como objetivo concienciar sobre los riesgos de los sistemas y redes de información. Deben establecerse políticas, prácticas, medidas y procedimientos para abordar estos riesgos y la necesidad de adopción. Los nueve principios de la guía se aplican a todos los niveles políticos y operativos que rigen la seguridad de los sistemas y redes de información. La norma ISO 27001 proporciona un marco ISMS (Information Security Management Systems) para implementar los principios que rigen el modelo PHVA (Plan, Do, Check, Act) y los procesos del sistema de gestión.

NARANJAL

Av. Olmedo 1201 y Bolívar 2750 191 - 2750 192 www.naranjal.gob.ec

2.2 Objetivos específicos

- Identificar los componentes para el Modelo de Gestión de Seguridad de la Información.

- Establecer una metodología de gestión y mejora continua del Modelo de Gestión de Seguridad de la Información, lo cual garantice un adecuado tratamiento de la información.

- Evaluar el Modelo de Gestión de Seguridad de la Información, mediante grupos de expertos de seguridad focal.

3 JUSTIFICACIÓN

Dado que el Cantón Naranjal ha venido creciendo exponencialmente en los últimos años y de igual forma la municipalidad de naranjal se torna imprescindible la contratación de este tipo de servicios para el cabildo y cantón con la finalidad de proveer seguridad, disponibilidad e integridad de la información histórica y que se genera diariamente reposando en las bases de datos que se gestionan a través de los sistemas de información de esta Municipalidad.

4 ALCANCE

En conformidad con el objetivo, se solicita dar inicio al proceso de contratación para realizar una Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal, con la visión de brindar seguridad, disponibilidad e integridad al recurso almacenado en las bases de datos gestionadas por los sistemas informáticos pertenecientes a esta entidad municipal, y estandarizar la mejora continua.

5 DETALLE DEL PRODUCTO O SERVICIO REQUERIDO

CPC	DESCRIPCION	ESPECIFICACIONES	CANTIDAD	COSTO	TOTAL
831410012	Modelo de Sistema de Gestión de Seguridad de la	10 días	10	6.416,07	6.416,07

El uso inadecuado de los recursos tecnológicos en Instituciones Gubernamentales, hace que tengan serios problemas de seguridad, esto deriva del aumento desmesurado de los índices de delitos informáticos. En la actualidad, uno de los temas de mayor importancia y trascendencia de toda la sociedad, es la seguridad y resguardo de la información, más aún las Instituciones del gobierno que tienen información sensible de todas las transacciones que se realizan y a su vez afectan tanto a los clientes internos como externos.

Según la firma de seguridad Kaspersky en el año 2021, Ecuador lidera la lista de países más vulnerados por los ciberataques, Además, según el reporte, titulado Panorama de Amenazas en América Latina 2021, hay un aumento del 24% en ciberataques en los primeros ocho meses del año, en comparación con el mismo periodo en 2020. Se ha demostrado en la actualidad, que la filtración de documentos e información de Instituciones Gubernamentales ha provocado problemas muy serios, como ejemplo de esto fue el ataque informático a la Agencia Nacional de Tránsito a su sistema AXIS en el 2021; o el ciberataque que recibió el Municipio de Quito el pasado 16 de abril del presente año.

El Gobierno Autónomo Descentralizado Municipal (GAD) del cantón Naranjal una de las dependencias públicas más importantes de esta ciudad, mediante la Gestión de Tecnología e Informática, maneja información crítica y a que su vez se considera sensible correspondiente a todas las transacciones municipales que se realizan a través del Sistema Integral de Información Finalizaría SIIM V7 Comercial y V6 OpenERP Financiero, la cual necesita ser protegida y no existen controles basados en alguna normativa de seguridad de la Información.

2 OBJETIVOS

2.1 Objetivos General

Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal.

	Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal				
				SUBTOTAL	6.416,07

5.1.1 Equipos a utilizar:

Descripción
Dos ordenadores portátiles, para llevar la documentación de manera ordenada y actualizada, durante el proceso de elaboración de la documentación.

6 PLAZO DE EJECUCIÓN

El plazo para presentar la propuesta de un **Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal,** será de 10 días a partir de la firma del contrato de acuerdo al siguiente cronograma:

Tiempo de elaboración de la propuesta: 10 días

NOTA: El planillaje del servicio empezará con el 50% del pago al inicio de la consultoría y el otro 50% será 5 días después de haber presentado la propuesta.

PRODUCTO 1: DOCUMENTACION DEL **MODELO DE** (SGSI).

ETAPA 1: LEVANTAMIENTO DE INFORMACIÓN DEL (SGSI).

Durante esta etapa se procederá a realizar el levantamiento de información en todas las dependencias del GAD Municipal del cantón Naranjal.

DÍAS DE ACTIVIDADES: 10 DÍAS

Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal.										
	DIA 1	**DIA 2**	**DIA 3**	**DIA 4**	**DIA 5**	**DIA 6**	**DIA 7**	**DIA 8**	**DIA 9**	**DIA 10**
Levantamiento de información	X	X	X	X						
Desarrollo de documentación					X	X	X	X	X	X

NOTA: El segundo planillaje para finalizar el servicio del 50% será 5 días después de la entrega conforme de la documentación.

ETAPA 2: VERIFICACIÓN DE LA ENTREGA DE DOCUMENTACIÓN

Una vez verificada la documentación en físico y digital se procederá a realizar el acta de entrega resección de los productos esperados.

- El Contratista debe entregar un informe de haber cumplido su labor
    - Fotos de las dependencias visitadas.
    - Coordenadas o ubicación geográfica de la instalación o instalaciones visitadas.
    - Describir el estándar o norma utilizada para la realización de un Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal.

7.- POBLACIÓN BENEFICIADA

La presente contratación de un **Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal.** Brindará al departamento de tecnologías de la información una herramienta que al ser implantada proveerá seguridad, disponibilidad e integridad de la información histórica y la que se genera diariamente en la institucional Municipal.

8.- RECOMENDACIONES:

Por intermedio de usted señor director ....., solicito derivar al área pertinente la autorización, para la contratación de una consultoría para elaborar un **Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal.**

Atentamente,

.....
NOMBRES
.....
CARGO

Anexo 5 Informe Técnico

Naranjal, julio del 2022

1 ANTECEDENTES:

El rápido desarrollo de la tecnología ha creado serios problemas de vulnerabilidad en las organizaciones, con riesgos e inseguridad, así como fraudes informáticos, espionaje, sabotaje, retirada informática e intrusiones o ataques de denegación de servicio. La ISO 27001 es un estándar ISO que establece requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad de la información. Esta norma internacional fue publicada Electrotechnical Commission. ISO 27001 fue publicada como estándar internacional en octubre de 2005, tal como la conocemos hoy, fue el resultado del desarrollo de otras normas relacionadas con la seguridad de la información.

Un sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 tiene como objetivo garantizar que las empresas hayan implementado todos los controles apropiados sobre la seguridad, integridad y disponibilidad de su información, para protegerla de las partes interesadas, socios comerciales y la sociedad en su conjunto. El cumplimiento de la norma ISO 27001 puede ayudar a las empresas a demostrar a sus clientes o socios cuánto se toman en serio la seguridad de la información. La certificación reconocida en la norma ISO 27001 es testimonio del compromiso de la empresa con la gestión de la seguridad de la información.

Las directrices de la OCDE (Organización para la Cooperación y el Desarrollo Económico) tienen como objetivo concienciar sobre los riesgos de los sistemas y redes de información. Deben establecerse políticas, prácticas, medidas y procedimientos para abordar estos riesgos y la necesidad de adopción. Los nueve principios de la guía se aplican a todos los niveles políticos y operativos que rigen la seguridad de los sistemas y redes de información. La norma ISO 27001 proporciona un marco ISMS (Information Security Management Systems) para implementar los principios que rigen el modelo PHVA (Plan, Do, Check, Act) y los procesos del sistema de gestión.

El uso inadecuado de los recursos tecnológicos en Instituciones Gubernamentales, hace que tengan serios problemas de seguridad, esto deriva del aumento desmesurado de los índices de

Av. Olmedo 1201 y Bolívar ☎ 2750 191 - 2750 192 www.naranjal.gob.ec

delitos informáticos. En la actualidad, uno de los temas de mayor importancia y trascendencia de toda la sociedad, es la seguridad y resguardo de la información, más aún las Instituciones del gobierno que tienen información sensible de todas las transacciones que se realizan y a su vez afectan tanto a los clientes internos como externos.

Según la firma de seguridad Kaspersky en el año 2021, Ecuador lidera la lista de países más vulnerados por los ciberataques, Además, según el reporte, titulado Panorama de Amenazas en América Latina 2021, hay un aumento del 24% en ciberataques en los primeros ocho meses del año, en comparación con el mismo periodo en 2020. Se ha demostrado en la actualidad, que la filtración de documentos e información de Instituciones Gubernamentales ha provocado problemas muy serios, como ejemplo de esto fue el ataque informático a la Agencia Nacional de Tránsito a su sistema AXIS en el 2021; o el ciberataque que recibió el Municipio de Quito el pasado 16 de abril del presente año.

El Gobierno Autónomo Descentralizado Municipal (GAD) del cantón Naranjal una de las dependencias públicas más importantes de esta ciudad, mediante la Gestión de Tecnología e Informática, maneja información crítica y a que su vez se considera sensible correspondiente a todas las transacciones municipales que se realizan a través del Sistema Integral de Información Finalizaría SIIM V7 Comercial y V6 OpenERP Financiero, la cual necesita ser protegida y no existen controles basados en alguna normativa de seguridad de la Información.

2 JUSTIFICACIÓN

Dado que el Cantón Naranjal ha venido creciendo exponencialmente en los últimos años y de igual forma la municipalidad de naranjal se torna imprescindible la contratación de este tipo de servicios para el cabildo y cantón con la finalidad de proveer seguridad, disponibilidad e integridad de la información histórica y que se genera diariamente reposando en las bases de datos que se gestionan a través de los sistemas de información de esta Municipalidad.

3 OBJETIVOS

3.1 OBJETIVO GENERAL:

Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal.

3.2 OBJETIVOS ESPECÍFICOS:

- Identificar los componentes para el Modelo de Gestión de Seguridad de la Información.
- Establecer una metodología de gestión y mejora continua del Modelo de Gestión de Seguridad de la Información, lo cual garantice un adecuado tratamiento de la información.
- Evaluar el Modelo de Gestión de Seguridad de la Información, mediante grupos de expertos de seguridad focal.

4 ALCANCE

En conformidad con el objetivo, se solicita dar inicio al proceso de contratación para realizar una Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal, con la visión de brindar seguridad, disponibilidad e integridad al recurso almacenado en las bases de datos gestionadas por los sistemas informáticos pertenecientes a esta entidad municipal, y estandarizar la mejora continua en los procesos tecnológicos.

SECTOR SELECCIONADO PARA LA PROPUESTA

Gestión de Tecnología e Informática, ubicada en el Palacio Municipal:

N°	UBICACIÓN	TIPO DE SERVICIO	COORDENADAS
1	Palacio Municipal, Gestión de Tecnología e Informática.	Estudio para una Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal.	-2.67518993192, -79.6199091685

5 METODOLOGÍA DE TRABAJO

El departamento de la Gestión de Tecnología e Informática del Gobierno Autónomo Descentralizado del Cantón Naranjal, trabajará en conjunto con el consultor que proveerá la Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal.

La municipalidad de naranjal, tendrá la capacidad para hacer uso del modelo propuesto e iniciar el proceso para su respectiva implantación.

5.1 PRODUCTO 1: DOCUMENTACION DEL MODELO DE (SGSI).

ETAPA 1: LEVANTAMIENTO DE INFORMACIÓN DEL (SGSI).

Durante esta etapa se procederá a realizar el levantamiento de información en todas las dependencias del GAD Municipal del cantón Naranjal.

DÍAS DE ACTIVIDADES: 10 DÍAS

Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal.										
	DIA 1	**DIA 2**	**DIA 3**	**DIA 4**	**DIA 5**	**DIA 6**	**DIA 7**	**DIA 8**	**DIA 9**	**DIA 10**
Levantamiento de información	X	X	X	X						
Desarrollo de documentación					X	X	X	X	X	X

NOTA: El segundo planillaje para finalizar el servicio del 50% será 5 días después de la entrega conforme de la documentación.

ETAPA 2: VERIFICACIÓN DE LA ENTREGA DE DOCUMENTACIÓN

Una vez verificada la documentación en físico y digital se procederá a realizar el acta de entrega resección de los productos esperados.

- El Contratista debe entregar un informe de haber cumplido su labor
    - Fotos de las dependencias visitadas.
    - Coordenadas o ubicación geográfica de la instalación o instalaciones visitadas.
    - Describir el estándar o norma utilizada para la realización de una Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal.

SISTEMA DE CONTROL DE CALIDAD DE SERVICIO A USUARIOS:

- El contratista deberá dar asesoramiento al personal de la Gestión de Tecnología e Informática de como implantar los controles Basados en la ISO 27001:2013.
- El proveedor deberá garantizar que la propuesta presentada se rige a un estándar mundialmente conocido, aceptado y probado.

Observaciones:

- Se pagará una planilla con el 50% del contrato al iniciar la consultoría.
- Al finalizar el contrato el proveedor deberá desmontar haber cumplido y entregado la propuesta documentada en físico y digital, para proceder a pagar el 50% que complete el valor establecido 5 días después de la entrega recepción.

DESCRIPCIÓN	TIEMPO ATENCIÓN*	TIEMPO MÁXIMO RESOLUCIÓN
Levantamiento de información y realización de la respectiva documentación	10 días	10 días

6 PRODUCTOS O SERVICIOS ESPERADOS:

Como resultado de la aplicación del proyecto se espera recibir los productos e informes que se señalan a continuación:

CPC	DESCRIPCION	ESPECIFICACIONES	CANTIDAD	COSTO	TOTAL
831410012	Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranjal.	10 días	10	6.416,07	6.416,07
				SUBTOTAL	6.416,07

6.1.1 Talento Humano que realiza la actividad:

Descripción
Un Profesional con la certificación ISO/IEC 27001:2013 - FORMACIÓN DE AUDITOR INTERNO - SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. Un Analista de Sistemas designado por el departamento de Tecnología e Informática que realizara el acompañamiento, para coordinar las labores de levantamiento de información en las distintas dependencias del GAD Municipal del cantón Naranjal.

6.1.2 Equipos a utilizar:

Descripción
Dos ordenadores portátiles, para llevar la documentación de manera ordenada y actualizada, durante el proceso de elaboración de la documentación.

7 PLAZO DE EJECUCIÓN Y ACTIVIDADES

El plazo para presentar la **PROPUESTA DE UN MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA ESTABLECER CONTROLES BASADOS EN LA NORMA ISO/IEC 27001:2013 EN EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN NARANJAL,** será de 10 días a partir de la firma del contrato de acuerdo al siguiente cronograma:

Tiempo de elaboración de la propuesta: 10 días

NOTA: El planillaje del servicio empezará con el 50% del pago al inicio de la consultoría y el otro 50% será 5 días después de haber presentado la propuesta.

8 DIAGNÓSTICO E INFORMACIÓN QUE DISPONE LA ENTIDAD

A continuación, se detalla cada una de las dependencias con sus respectivos módulos y privilegios de uso dentro del Sistema Informático Municipal:

DEPENDENCIAS DEL GAD MUNICIPAL DEL CANTÓN NARANJAL			
#	**DEPENDENCIAS**	**MODULOS QUE UTILIZAN Y PRIVILEGIOS**	**USUARIOS A ENCUESTAR**
1	Gestión de tecnología e informática	Administración General de todos los módulos del sistema	3
2	Secretaria General del Concejo MM	Gestión Documental	1
3	Gestión Administrativa	Gestión Documental Talento Humano Adquisiciones	3
4	Gestión de Obras Públicas	Gestión Documental	1
5	Gestión Financiera	Gestión Documental Administración Financiera Gestión Financiera Tesorería y Pagos Notas de crédito Coactivas Catastro Urbano Catastro rural Banco del Estado Reportes	3

6	Gestión de Desarrollo Social	Gestión Documental	1
7	Gestión de Cultura, Patrimonio, Turismo y Deporte	Gestión Documental Ferias Licencia Funcionamiento Cliente Espectáculos	1
8	Gestión de Agua Potable y Alcantarillado	Gestión Documental Agua y Alcantarillado Facturación Recaudación	4
9	Gestión de Planificación y Proyectos	Gestión Documental Control Territorial Catastro urbano Catastro Rural	1
10	Gestión De Tránsito, Transporte Terrestre Y Seguridad Vial MM	Gestión Documental Tramite Recaudación	1
11	Unidad de Gestión de Riesgos	Gestión Documental	1
12	Registro de la Propiedad Municipal y Mercantil del cantón Naranjal	Gestión Documental Registro Propiedad Registro Mercantil Cliente	4
13	Tesorera Municipal	Gestión Documental Cliente Depurador Cliente Reportes Tramites Formularios Convenios de Pago Tesorería y pagos Certificaciones	4
14	Jefe de Avalúos y Catastro	Gestión Documental	5

		Catastro urbano Catastro rural Mejoras Cliente Tramites Depurador predial	
15	Procurador Sindico	Gestión Documental	1
16	Jefe de Maquinarias	Gestión Documental	1
17	Guardalmacén Municipal	Activo Fijos Gestión de Inventarios Gestión Documental	2
18	Comunicador Social	Gestión Documental	1
19	Jefa de Rentas	Gestión Documental Alcabalas Arriendos Tramites Plusvalía Patentes Clientes Catastro urbano Catastro Rural Glosas Reintegros Rodaje Agua portable Control Territorial Espectáculos Facturación Ferias Mejoras Pesas Rastro	2
20	Jefa de Contabilidad	Gestión Documental	1

		Administración Financiera Gestión Presupuesto	
21	Jefa de Presupuesto	Gestión de Proyectos Gestión Documental Gestión Presupuesto	1
22	Comisario Urbana Municipal	Gestión Documental Cementerios Comisaria Catastro Urbano Rastro	1
23	Comisario Rural Municipal	Gestión Documental Catastro Rural	1
24	Jefe de Compras Públicas	Gestión Documental Adquisiciones	3
25	Secretaria Ejecutiva de Consejo de Protección de Derechos	Gestión Documental	1
26	Jefe del Relleno Sanitario	Gestión Documental	1
27	Jefe de Recolección y Barrido	Gestión Documental	1
28	Jefe de la Unidad Básica de Rehabilitación	Gestión Documental	1
	Unidad de Talento Humano	Gestión Documental Talento Humano	2
29	Unidad de Coactiva	Clientes Catastro urbano Catastro Rural Gestión Documental Coactivas Reportes	2

En caso de que se requiera mayor información se solicitará al administrador del contrato, para coordinar las actividades correspondientes al proceso.

9 MARCO LEGAL

El proyecto que se presenta está fundamentado legalmente bajo las normativas expedidas por la Contraloría General del Estado y el Estatuto Orgánico de Gestión Organizacional por Procesos del Gobierno Autónomo Descentralizado Municipal del cantón Naranjal.

NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS

410 TECNOLOGÍA DE LA INFORMACIÓN

410-01 Organización informática

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

410-04 Políticas y procedimientos

La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

La Unidad de Tecnología de Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran. Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y

procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información.

Será necesario establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización. Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos.

Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos. La Unidad de Tecnología de Información deberá promover y establecer convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como de programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con la tecnología de información.

500-01 Controles sobre sistemas de información:

Los sistemas de información contarán con controles adecuados para garantizar confiabilidad, seguridad y una clara administración de los niveles de acceso a la información y datos sensibles. En función de la naturaleza y tamaño de la entidad, los sistemas de información serán manuales o automatizados, estarán constituidos por los métodos establecidos para registrar, procesar, resumir e informar sobre las operaciones administrativas y financieras de una entidad y mantendrán controles apropiados que garanticen la integridad y confiabilidad de la información. La utilización de sistemas automatizados para procesar la información implica varios riesgos que necesitan ser considerados por la administración de la entidad. Estos riesgos están asociados especialmente con los cambios tecnológicos por lo que se deben establecer controles generales, de aplicación y de operación que garanticen la protección de la información según su grado de sensibilidad y confidencialidad, así como su disponibilidad, accesibilidad y oportunidad. Las servidoras y servidores a cuyo cargo se encuentre la administración de los sistemas de información, establecerán los controles pertinentes para que garanticen razonablemente la calidad de la información y de la comunicación.

410-04 Políticas y procedimientos:

La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

La unidad de tecnología de información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.

410-06 Administración de proyectos tecnológicos:

La unidad de tecnología de información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad. Los aspectos a considerar son:

1. Descripción de la naturaleza, objetivos y alcance del proyecto, su relación con otros proyectos institucionales, sobre la base del compromiso, participación y aceptación de los usuarios interesados.

2. Cronograma de actividades que facilite la ejecución y monitoreo del proyecto que incluirá el talento humano (responsables), tecnológicos y financieros además de los planes de pruebas y de capacitación correspondientes.

3. La formulación de los proyectos considerará el Costo Total de Propiedad CTP; que incluya no sólo el costo de la compra, sino los costos directos e indirectos, los beneficios relacionados con la compra de equipos o programas informáticos, aspectos del uso y mantenimiento, formación para el personal de soporte y usuarios, así como el costo de operación y de los equipos o trabajos de consultoría necesarios.

4. Para asegurar la ejecución del proyecto se definirá una estructura en la que se nombre un servidor responsable con capacidad de decisión y autoridad y administradores o líderes funcionales y tecnológicos con la descripción de sus funciones y responsabilidades.

5. Se cubrirá, como mínimo las etapas de: inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, así como los entregables, aprobaciones y compromisos formales mediante el uso de actas o documentos electrónicos legalizados.

6. El inicio de las etapas importantes del proyecto será aprobado de manera formal y comunicado a todos los interesados.

7. Se incorporará el análisis de riesgos. Los riesgos identificados serán permanentemente evaluados para retroalimentar el desarrollo del proyecto, además de ser registrados y considerados para la planificación de proyectos futuros.

8. Se deberá monitorear y ejercer el control permanente de los avances del proyecto.
9. Se establecerá un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas.

10. El proceso de cierre incluirá la aceptación formal y pruebas que certifiquen la calidad y el cumplimiento de los objetivos planteados junto con los beneficios obtenidos.

10 MULTAS

Por cada día de retraso en el cumplimiento del plazo de la entrega de los puntos correspondientes, se aplicará la multa del 1 por 1000 del valor pendiente a ejecutar.

11 EXPERIENCIA GENERAL

N	Descripción	TIEMPO	NÚMERO DE PROYECTO	MONTO MÍNIMO	DOCUMENTOS SOLICITADOS
1	Certificación en Auditoria de Sistemas Informáticos o Seguridad de la Información.	1 año	-	-	Acta de Entrega Recepción Definitiva o Facturas con sus retenciones (en el caso de que la experiencia sea en el sector público). Contrato o Facturas con sus retenciones (en el caso de

					que la experiencia sea en el sector privado)

12 EXPERIENCIA ESPECÍFICA MÍNIMA

N	Descripción	TIEMPO	NÚMERO DE PROYECTOS	MONTO MÍNIMO	DOCUMENTOS SOLICITADOS
1	Certificación Norma ISO/IEC 27001:2013 Auditor Interno	-	-	-	Contrato con su respectiva Acta de Entrega Recepción Definitiva o Facturas con sus retenciones (en el caso de que la experiencia sea en el sector público). Contrato o Facturas con sus retenciones (en el caso de que la experiencia sea en el sector privado)

13 PERSONAL TÉCNICO CLAVE

N	FUNCIÓN	NIVEL DE ESTUDIO	TITULACIÓN ACADÉMICA	CANTIDAD	DOCUMENTOS SOLICITADOS
1	Auditor	Título de Cuarto Nivel	Título de Magister en Informática o carreras afines.	1	REGISTRO SENESCYT
2	Analista de Sistemas	Título de Tercer Nivel	Tecnólogo en Informática o carreras afines. Informáticos o carreras a fines	1	REGISTRO SENESCYT

- 1 supervisor de instalación
- 3 técnicos

14 EXPERIENCIA DE PERSONAL TÉCNICO

N	FUNCIÓN	DESCRIPCIÓN	TIEMPO	NÚMERO DE PROYECTOS	MONTO DE PROYECTOS	DOCUMENTOS SOLICITADOS
1	Auditor	Poseer la certificación ISO/IEC 27001:2013 DE AUDITOR INTERNO EN SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	1 años	-	-	Certificado Laboral Cedula identidad Copia de la Certificación ISO/IEC 27001:2013 DE AUDITOR INTERNO EN SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. Avalado por un ente autorizado a nivel mundial.
2	Auxiliar	Experiencia en el área de la Gestión de Tecnología e Informática.	1 año	-	-	Certificado Laboral Cedula identidad

						Título Profesional

15 EQUIPO MÍNIMO

N	EQUIPO	CANTIDAD	CARACTERÍSTICAS	DOCUMENTOS SOLICITADOS
1	Pc Portátil	2	Laptop Dell Inspiron 14" Intel Core i3 Memoria RAM 4GB/Disco Duro 1 TB Silver	FICHA TÉCNICO O CATALOGO

16 FORMA Y CONDICIONES DE PAGO.

El planillaje del servicio empezará con el 50% del pago al inicio de la consultoría y el otro 50% será 5 días después de haber presentado la propuesta, previa revisión de la documentación recibida en físico y digital y entrega la documentación habilitante por parte del proveedor y el informe favorable del administrador del contrato.

- FACTURA – (Esperar solicitud de la Dirección Financiera)
- INFORME DE SATISFACCIÓN,
- ACTA DE ENTREGA-RECEPCIÓN

a) Contra entrega:	
b) Pago por planilla:	X
c) Otra: Especifique:	
d) Anticipo:	X

22 OBLIGACIONES DE LA CONTRATANTE:

- Dar solución a las peticiones y problemas que se presentarán en la ejecución del contrato, en un plazo (15 días) contados a partir de la petición escrita formulada por el contratista.
- Verificar los documentos que el proveedor debe presentar, de conformidad con los intereses institucionales.
- Otorgar al proveedor las facilidades necesarias para la recepción de los bienes.
- Verificar el cumplimiento de las especificaciones técnicas de los bienes.

Elaborado por,

.....

NOMBRES

.....

CARGO

17 MULTAS

Por cada día de retraso en la ejecución de las obligaciones contractuales por parte del contratista, se aplicará la multa del uno por mil (1x1000), las multas se calcularán sobre el porcentaje de las obligaciones que se encuentran pendientes de ejecutarse conforme lo establecido en el contrato.

18 VIGENCIA DE LA OFERTA.

La oferta estará vigente por 3 días, contados a partir de la presentación de la misma, de conformidad a lo dispuesto en el artículo 30 de la Ley Orgánica del Sistema Nacional de Contratación Pública.

19 PUJA:

En el día y hora señalados en la convocatoria, se realizará la puja hacia la baja a través del Portal Institucional del SERCOP, en la cual participarán únicamente los proveedores que hayan enviado su oferta económica inicial.

El porcentaje de variación mínimo durante la puja será del: **0.5%**.

20 NEGOCIACIÓN (EN CASO DE APLICAR):

De existir una sola oferta calificada, o si una sola oferta resultare habilitada, o un solo oferente presentare su oferta económica inicial, se realizará una sesión de negociación de acuerdo a lo establecido en el artículo 47 del RGLOSNCP.

21 OBLIGACIONES DEL CONTRATISTA:

- Garantizar el cumplimiento de porcentaje valor agregado ecuatoriano
- Dar cumplimiento cabal a lo establecido en el presente documento de acuerdo con los términos y condiciones del contrato.
- Previo a la suscripción del contrato, deberá presentar las garantías técnicas.
- Suscribir conjuntamente con los integrantes de la comisión designada por la máxima autoridad o su delegado el acta de entrega – recepción definitiva.
- La entrega de los bienes deben estar en buen estado.

INTRODUCCIÓN

Las amenazas a los sistemas informáticos van en aumento y ponen en peligro uno de los activos más importantes y vulnerables de una empresa, por ejemplo, la información correspondiente al Gobierno Autónomo Descentralizado Municipal del cantón Naranjal. Dado que la integridad de los datos es un servicio que las organizaciones tienen que prestar, los controles de seguridad de la información deben documentarse y aplicarse mediante procedimientos conocidos.

Este trabajo tiene como objetivo desarrollar un plan de seguridad de la información para el Departamento de Tecnologías de la Información del GAD Municipal de Naranjal. Para ello, se realizó un estudio de acuerdo con la norma ISO/IEC 27002:2013 para identificar las vulnerabilidades con el fin de analizar y abordar los riesgos en los procesos mencionados.

Para ilustrar este modelo, el estudio se divide en los siguientes capítulos:

Capítulo 1: se detalla la problemática que presenta el GAD Municipal de Naranjal, así como se establece los objetivos que se van detallando en el transcurso de la tesis y para finalizar se expone el estado del arte tomando como ejemplo investigaciones bibliográfica.

Capítulo 2: se trata de un estudio de mapeo que los artículos publicados en las bases de datos SCOPUS y Web of Science (WOS) se selecciona inicialmente con el fin de utilizar ISO/IEC 27001:2013 para concluir se presenta una encuesta evaluada por dos personas que conforman el departamento de TI.

Capítulo 3: se evalúa un sistema de gestión de la seguridad de la información, el cual es un conjunto de políticas y procedimientos basados en la ISO/IEC 27001:2013 y diseñados mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022, para alcanzar un nivel adecuado de seguridad de la información, . La metodología que se ha desarrollado es utilizando el proceso PHVA (Planificar, Hacer, Verificar, Actuar) .

Por último, se presenta las conclusiones y recomendaciones siguiendo el modelo de SGSI lo cual será muy útil para la implantación del sistema en el GAD Municipal del cantón Naranjal.