UNIVERSIDAD ESTATAL DE MILAGRO

FACULTAD CIENCIAS DE LA INGENIERÍA

PROYECTO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS COMPUTACIONALES

TÍTULO

AUDITORIA DE LA SEGURIDAD INFORMÁTICA BASADO EN LA ISO 27001 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GAD MUNICIPAL DE MILAGRO

Autores:

PAGUAY LEMA CINTHYA KATHERINE

ZAMORA ARANA GABRIEL EDUARDO

Milagro, Septiembre 2017

ECUADOR

ACEPTACIÓN DEL TUTOR

Por la presente hago constar que he analizado el proyecto de grado presentado por los estudiantes **PAGUAY LEMA CINTHYA KATHERINE, ZAMORA ARANA GABRIEL EDUARDO**, para optar al título de Ingeniería en Sistemas Computacionales y que acepto la tutoría del estudiante, durante la etapa del desarrollo del trabajo hasta su presentación, evaluación y sustentación.

Milagro, a los 19 días del mes de Septiembre del 2017

Firma del tutor(a)

Bermeo Almeida Oscar Xavier

C.I 0913960944

DECLARACIÓN DE AUTORÍA DE LA INVESTIGACIÓN

El autor de esta investigación declara ante el Consejo Directivo de la Facultad Ciencias de la Ingeniería de la Universidad Estatal de Milagro, que el trabajo presentado es de nuestra 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 o Grado de una institución nacional o extranjera.

Milagro, a los 19 días del mes de Septiembre de 2017

Firma del estudiante

Nombre: Paguay Lema Cinthya Katherine

CI: 0929132223

Firma del estudiante

Nombre: Zamora Arana Gabriel Eduardo

CI: 0929607471

CERTIFICACIÓN DE LA DEFENSA

El tribunal calificador previo a la obtención del título de Ingeniera en Sistemas Computacionales otorga al presente proyecto de investigación las siguientes calificaciones:

MEMORIA CIENTÍFICA	[45]
DEFENSA ORAL	[47]
TOTAL	[96]
EQUIVALENTE	[5]

PRESIDENTE DEL TRIBUNAL

PROFESOR DELEGADO

PROFESOR SECRETARIO

CERTIFICACIÓN DE LA DEFENSA

El tribunal calificador previo a la obtención del título de Ingeniera en Sistemas Computacionales otorga al presente proyecto de investigación las siguientes calificaciones:

MEMORIA CIENTÍFICA	[45]
DEFENSA ORAL	[47]
TOTAL	[96]
EQUIVALENTE	[5]

PRESIDENTE DEL TRIBUNAL

PROFESOR DELEGADO

PROFESOR SECRETARIO

DEDICATORIA

La presente tesis le dedico a Dios luego mi familia y a mí novio por todo el apoyo que me brindaron para concluir mi carrera.

Se los dedico a mi abuelo Francisco Paguay y a mi abuela María Vargas a mi padre por ayudarme en todo lo que necesitaba y por estar a mi lado siempre, a mi madre por hacerme una mejor persona mediante sus enseñanzas y el amor que me da y a mi hermana por estar siempre presente y darme la confianza que necesitaba.

Y a todos en general que me apoyaron de una u otra forma para poder finalizar la tesis.

Cinthya Katherine Paguay Lema

AGRADECIMIENTO

En especial agradezco a Dios por darme la fuerza y la perseverancia en seguir adelante y poder superar los obstáculos que se presentaron en algún momento y a mi familia que me apoyó incondicionalmente al inicio y fin de la carrera.

También agradezco a mi tutor de tesis el Ing. Oscar Bermeo por toda la ayuda que me brindo en el proyecto de la tesis y durante la carrera contribuyendo con sus conocimientos y experiencias y agradezco a todos mis profesores.

Cinthya Katherine Paguay Lema

DEDICATORIA

Dedico de manera muy especial a Dios y a mis padres pues ellos fueron lo primordial en mi vida brindando el amor y la comprensión de una familia enseñándome la responsabilidad y el deseo de superarme cada día más.

Gabriel Eduardo Zamora Arana

AGRADECIMIENTO

En primer lugar, agradezco a la Universidad Estatal de Milagro por aceptarme de ser parte de ella y haber estudiado la carrera de Ingeniería en Sistemas Computacionales, así como también a mis profesores que me brindaron sus conocimientos y apoyo para seguir avanzando.

También agradezco a mi tutor de tesis Ing. Oscar Bermeo por haberme aceptado a guiarme durante el desarrollo del proyecto de la tesis.

Y agradezco las todas las personas que me ayudaron para cumplir una meta más en mi vida.

Gabriel Eduardo Zamora Arana

CESIÓN DE DERECHOS DE AUTOR

Ingeniero.

Fabricio Guevara Viejó, PhD.

Rector de la Universidad Estatal de Milagro

Presente.

Mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor del Trabajo realizado como requisito previo para la obtención de mi (nuestro) Título de Tercer Nivel, cuyo tema fue "Auditoria de la Seguridad Informática basado en la ISO 27001 sistema de gestión de seguridad de la información para el GAD municipal de Milagro" y que corresponde a la Facultad Ciencias de la Ingeniería.

Milagro, 19 de Septiembre del 2017

Cinthya Paguay.

Firma del Estudiante (a)

PAGUAY LEMA CINTHYA KATHERINE

CI: 0929132223

Firma del Estudiante (a)

ZAMORA ARANA GABRIEL EDUARDO

CI: 0929607471

ÍNDICE GENERAL

INDICE DE CUADROS

INDICE DE FIGURAS

RESUMEN

En el presente proyecto se desarrolla un plan de seguridad de la información basándose en la norma INEN ISO /IEC 27001, para el GAD Municipal de Milagro con la finalidad de mejorar la seguridad de toda la información que maneja aquella entidad, estableciendo políticas, procedimientos y planes de acción para cubrir las brechas que tienen los sistemas de información.

Antes de haber escogido esta norma INEN ISO /IEC 27001 se hizo su debido análisis, ya que se realizó tres propuestas que son las siguientes normas: COBIT, ITIL e ISO 27001, de las cuales la norma ISO 27001 es la que se acoplo a las necesidades que tiene la entidad, ya que esta norma describe cómo gestionar la seguridad de la información de una entidad ya sea tanto pública como privada, además su estructura se adapta a las necesidades que requiere el GAD Municipal de Milagro y los beneficios que le brinda hará que la entidad tenga toda la información que gestiona a diario más segura. También identificara los riesgos que se están cometiendo y a la vez establecer controles para gestionarlos o eliminarlos.

Con la implementación de la norma INEN ISO /IEC 27001 en el GAD Municipal de Milagro, se estableció controles y procedimientos sobre los riesgos identificados, confidencialidad para asegurarnos que solo personas autorizadas puedan acceder a la información, flexibilidad para que los controles y procedimientos se adapten a las áreas de la entidad que lo requieran, además el sistemas de gestión de seguridad de la información que tiene la norma INEN ISO /IEC 27001 permite a la empresa tener la libertad de crecer, innovar y ampliar su base sabiendo que toda la información dada seguirá siendo confidencial.

PALABRAS CLAVE: Seguridad, Información, ISO

LÍNEA DE INVESTIGACIÓN: Tecnologías de la Información y de la Comunicación.

SUBLÍNEA DE LÍNEA DE INVESTIGACIÓN: Seguridad de la Información

CAPÍTULO I: EL PROBLEMA

PLANTEAMIENTO Y JUSTIFICACIÓN DEL PROBLEMA

Uno de los problemas de mayor relevancia en las instituciones es la falta de seguridad informática, hoy en día es una latente preocupación en el campo de las redes especialmente donde se maneja la información confidencial, como correo electrónico, sistemas Informáticos, o páginas gubernamentales, debido al avance tecnológico y a la globalización de las redes de comunicación que van de la mano con la internet. Dadas las condiciones actuales en la red mundial, es imprescindible hacer algo al respecto para, de alguna manera, evitar cualquier tipo de amenazas a los activos de esta entidad.

El departamento de informática del Gobierno autónomo Descentralizado Municipal de Milagro tiene las soluciones tradicionales de firewall y antivirus que son necesarias para evitar la transferencia de programas malintencionados, pero no son suficientes para combatir la nueva generación de amenazas y ataques dirigidos. Tampoco los usuarios y empleados que dan uso a diario de los activos y de la red interna, poseen una cultura de seguridad que pueda salvaguardar la información almacenada en formato electrónico.

La información que maneja GAD Municipal de Milagro es de trascendental importancia para el progreso productivo, económico, social y cultural del cantón debido a que la mayoría de las transacciones se la realizan haciendo uso de sistemas informáticos. Para lo cual se propone el presente proyecto que se encargará de analizar los mecanismos de control que están implantados, determinando si los mismos son apropiados y cumplen los objetivos o estrategias determinadas, de no ser el caso se pretende establecer una serie de recomendaciones estableciendo acciones a emprender, que contribuyan a mejorar el nivel de seguridad de la información.

Debido a los avances de la tecnología, y su naturaleza de las comunicaciones, cada vez es más difícil asegurar la información de tal manera que su integridad esté garantizada. En el entorno actual de las tecnologías de la información, las organizaciones son cada vez más dependientes de sus sistemas de información. La información es un activo que, como otros activos comerciales, es muy importante y esencial para el negocio, por lo tanto necesita ser protegida adecuadamente. Esto es especialmente importante en el entorno empresarial, donde la información está expuesta a un

número cada vez mayor de personas y por tanto a una variedad más amplia de amenazas y vulnerabilidades. Las amenazas, tales como código malicioso, la piratería informática, y ataques de denegación de servicio se han vuelto más comunes, y cada vez son más sofisticadas.

La seguridad de la información a más de ser un problema de Tecnología Informática, también es un asunto de negocios. Si una institución quiere sobrevivir, y mucho más prosperar, es necesario comprender la importancia de la seguridad de la información y poner en práctica medidas y procesos apropiados. Es vital estar preocupado por la seguridad de la información ya que gran parte del valor de una empresa se concentra en el valor de su información. La información es la base de la ventaja competitiva de las empresas. Tanto en el sector privado como en el sector público, se debería tener mayor conciencia de la probabilidad de robo de identidad y en sí de la información. Sin información, ni las empresas privadas ni públicas podrían funcionar. Por tanto, valorar y proteger la información son tareas cruciales para las organizaciones modernas.

La razón básica acerca de los sistemas de seguridad, es que la información confidencial de una empresa debe ser protegida contra la divulgación no autorizada, por motivos ya sea confidencial o competitivo; toda la información que se almacena también debe ser protegida contra la modificación accidental o intencionada y a su vez debe estar disponible de manera oportuna. Además hay que establecer y mantener la autenticidad de los documentos que las organizaciones crean, envían o reciben.

Los Beneficios del presente estudio hacia el GAD Municipal de Milagro es que el sistema de Seguridad de Información establecerá una metodología de gestión de la seguridad clara y estructurada permitiendo la reducción del jus (ISO 9001, ISO 14001, OHSAS 18001etc.) lo que permite un aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

CAPÍTULO II: ANTECEDENTES Y MARCO TEÓRICO

2.1 ANTECEDENTES

Con el desarrollo acelerado del Internet, hoy en día existen amenazas y vulnerabilidades que atentan contra la seguridad informática de las universidades, entre ellas el Data Center de la Escuela Politécnica del Ejército. El presente proyecto se enfoca en el uso de los controles de la Norma ISO 27000, dedicada a especificar requerimientos necesarios para: establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. En este contexto, existe una metodología formal de Análisis y Gestión de Riesgos denominada MAGERIT, que permite recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. Para llevarlo a cabo es necesario complementar con un software denominado PILAR, que permite el análisis de riesgos en Seguridad Informática, de acuerdo a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad y disponga de salvaguardas, normas y procedimientos de seguridad para obtener el riesgo residual en el proceso de tratamiento. Los resultados obtenidos muestran una mejora a nivel de seguridad informática aplicando las salvaguardas, y se reduce el riesgo de la situación actual. Los resultados han permitido técnicamente obtener un informe ejecutivo, definir los lineamientos para el plan de seguridad informático, cara a certificarse en la Norma ISO 27001. [1]

Fideval S.A. Administradora de Fondos y Fideicomisos es una compañía legalmente inscrita en el registro de mercado de valores, constituida con el objetivo de administrar negocios fiduciarios (fideicomisos, encargos fiduciarios de terceros), fondos de Inversión y representar a fondos Internacionales. En ella se maneja información sensible la cual se encuentra alojada en los servidores y sistemas de almacenamiento ubicados en la institución, por lo que es necesario que se garantice su confidencialidad, integridad y disponibilidad de la misma. La presente investigación se orienta a la evaluación o diagnóstico de la seguridad informática en Fideval, porque aparte de verificar las falencias, permitirá implementar controles y políticas en base a las recomendaciones obtenidas para minimizar en el futuro que ocurran estos problemas, y como una forma de prevención para el tratamiento adecuado de datos en riesgos y el cuidado de la información. [2]

En la Universidad Tecnológica Equinoccial basado en la norma internacional ISO/IEC 27000 tiene como objetivo evaluar la seguridad de la información del proceso de admisión de estudiantes de pregrado para determinar el nivel de seguridad y elaborar un plan de tratamiento de riesgos que permita dar respuesta a los riesgos de seguridad de la información asociados a este proceso. En el desarrollo del trabajo se utiliza una metodología de evaluación de seguridad de la información basada en riesgos con su fundamento en la norma NTE INEN-ISO/IEC 27005:2012 elaborada por los autores, en la cual, se establecen los pasos a seguir y las actividades a realizar en cada etapa del proceso hasta obtener los resultados finales sobre la brecha de seguridad respecto a la norma ISO/IEC 27001:2005 y el plan de tratamiento que mitiguen los riesgos priorizados acorde a los criterios de aceptación definidos por el Rector de la UTE. [3]

Para el área de Software de la Procesadora Nacional de Alimentos (PRONACA) se ha enfocado en el desarrollo de un sistema de gestión de seguridad de la información, basada en los dominios de las normas ISO 27001 e ISO 27002. Establecidos en un análisis de las políticas y normas existentes en PRONACA, se ha propuesto que los dominios a ser desarrollados son los siguientes: Control de acceso, que permitirá tener la información de la empresa siempre disponible, confiable y segura a través de la implementación de nuevas políticas. [4]

En la Procesadora Nacional de Alimentos PRONACA se ha enfocado en el desarrollo de un Sistema de Gestión de Seguridad de la Información, establecida en los dominios de Cifrado y Seguridad Física y Ambiental de las normas ISO 27001 e ISO 27002 para el área de Software. Los dominios se expusieron basados en una investigación de las políticas y normas existentes en PRONACA. El dominio de Cifrado permitirá el resguardo de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. Seguridad Física y Ambiental, minimizará las alarmas de daños e interferencias a la información y a las operaciones de la organización. [5]

En el Municipio del Distrito Metropolitana de Quito maneja información sensible de la ciudadanía, como lo es la información catastral, licencia metropolitana única para el ejercicio de actividades económicas, pagos de impuestos prediales, declaración de patente y 1,5 x 1000 en activos, regularización de edificaciones existentes entre otras. Dicha información es crítica la cual se encuentra alojada en los servidores y sistemas

de almacenamiento ubicados en el Data Center, por lo que es necesario que se garantice su confidencialidad, integridad y disponibilidad. El presente trabajo se orienta a la evaluación técnica informática para determinar el cumplimiento de las normas y estándares internacionales que establecen un GAG de la gestión de seguridad de la información, según las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005. [6]

Auditoria de la seguridad informática basado en la ISO 27001

De acuerdo a la Organización Internacional de Normalización (ISO), es una federación de alcance mundial integrada por cuerpos de estandarización nacionales de 157 países, uno por cada país. [7]

La ISO es una organización no gubernamental, establecida en 1947 cuya misión es promover el desarrollo de la estandarización y las actividades relacionadas, con el fin de facilitar el intercambio de servicios y bienes, y promover la cooperación en la esfera del Tl intelectual, científico, tecnológico y económico. Todos los trabajos realizados por la ISO resultan en acuerdos internacionales, los cuales son publicados como Estándares Internacionales.

Un estándar es una publicación que recoge el trabajo en común de los comités de fabricantes, usuario, organizaciones, departamentos de gobierno y consumidores, y que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional, con el objetivo de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología. [8]

Los estándares ayudan a aumentar la fiabilidad y efectividad de materiales, productos, procesos o servicios que utilizan todas las partes interesadas (productores, vendedores, compradores, usuarios y reguladores). En principio, son de uso voluntario, aunque la legislación y las reglamentaciones nacionales pueden hacer referencia a ellos.

Desde 1901 y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas como: BS 5750 publicada en 1979, origen de ISO 9001; BS 7750 publicada en 1992, origen de ISO 14001.

La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información. [8]

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de gestión de seguridad de la información (SGSI) para ser certificable por una entidad independiente. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En el 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión. En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido, así como el año de publicación formal de la revisión.

Esta norma, está constituida por 8 cláusulas y Anexos, de los cuales la parte principal del sistema son desde la cláusula 4 a la 8 y el Anexo A. Las cláusulas indican los procedimientos que deben ser implementados, los documentos que deben ser elaborados y los registros que deben ser mantenidos dentro de la organización. El anexo A indica los controles y objetivos de control a implementar con el fin de ser salvaguardas, los mismos que se encuentran distribuidos en dominios que son:

- Política de seguridad,
- Organización de la seguridad de la información,
- Gestión de activos,
- Seguridad de los recursos humanos,
- Seguridad física y ambiental,
- Gestión de las comunicaciones y operaciones,
- Control de acceso,
- Adquisición, desarrollo y mantenimiento de los sistemas de información,
- Gestión de incidentes en seguridad de la información,
- Gestión de la continuidad del negocio y

- Cumplimiento.

Por lo tanto, ISO 27001, es un estándar que proporciona un modelo para establecer, implementar, utilizar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en un ciclo de vida PDCA (del inglés Plan-Do-Check-Act, cuyo significado en español es Planear, Hacer, Verificar y Actuar; o ciclo de Deming) de mejora continua, al igual que otros sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.). [9]

Es un estándar certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. [10]

Entendiéndose por confidencialidad a la propiedad que impide la divulgación de información a personas o sistemas no autorizados, es decir asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización; así mismo, cuando nos referimos a integridad, es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, es decir trata de mantener la información tal cual fue generada y al hablar de disponibilidad, nos referimos a la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

El aumento de la interconectividad informática y la popularidad del Internet están ofreciendo a las organizaciones todo tipo de oportunidades sin precedentes para mejorar las operaciones, reduciendo significativamente el uso del papel, a su vez reduciendo los costos al compartir información. Sin embargo, el éxito de muchos de esto s esfuerzos depende, en gran parte, de la capacidad de la organización para proteger la integridad, confidencialidad y disponibilidad de los datos y de los sistemas informáticos. [11]

Aunque la seguridad de la información juega un papel importante en la protección de los datos y de los activos de una organización, a menudo oímos noticias sobre delitos informáticos, como la alteración de sitios web o robo de datos. Las organizaciones tienen que ser plenamente conscientes de la necesidad de dedicar más recursos a la protección de los activos de información y seguridad de la información, la seguridad de la información debe convertirse en una de las principales preocupaciones de una empresa.

La seguridad de la información ha sido un área de investigación durante mucho tiempo. Inicialmente los virus y los gusanos se propagaban lentamente a través del intercambio de contenedores magnéticos como los disquetes. Con el desarrollo del internet, los problemas de seguridad se han hecho más frecuentes y han tomado formas muy diferentes, dando lugar al desarrollo de las técnicas nuevas de seguridad. [12]

Los principios básicos clásicos de la seguridad de la información, que son, la confidencialidad, integridad y disponibilidad, constituyen la base para su protección de la TI. Los términos tecnología de información y comunicaciones, y tecnología de información y telecomunicaciones se utilizan con frecuencia como sinónimos. Debido a la longitud de estas expresiones, se han establecido abreviaturas y por lo tanto la gente en general, simplemente se refiere a ella como TI.

Debido a los avances de la tecnología, y su naturaleza de las comunicaciones, cada vez es más difícil asegurar la información de tal manera que su integridad está garantizada. En el entorno actual de las TI, las organizaciones son cada vez más dependientes de sus sistemas de información. La información es un activo que, como otros activos comerciales es muy importante y esencial para el negocio, por lo tanto, necesita ser protegido adecuadamente. Esto es especialmente importante en el entorno empresarial, donde la información está expuesta a un número cada vez mayor de personas y por tanto a una variedad más amplia de amenazas y vulnerabilidades. Las amenazas, tales como código malicioso, la piratería informática, y ataques de denegación de servicio han vuelto más comunes, y cada vez son más sofisticadas. [13]

La seguridad de la información a más de ser un problema de TI, también es un asunto de negocios. Si una empresa quiere sobrevivir, y mucho más prosperar, es necesario

comprender la importancia de la seguridad de la información y poner en práctica medidas y procesos apropiados.

Es vital estar preocupado por la seguridad de la información ya que gran parte del valor de una empresa se concentra en el valor de su información. La información es la base de la ventaja competitiva de las empresas. Tanto en el sector privado como en el sector público, se debería tener mayor conciencia de la probabilidad de robo de identidad y en sí de la información. Sin información, ni las empresas privadas ni públicas podrían funcionar. Por tanto, valorar y proteger la información son tareas cruciales para las organizaciones modernas.

Otro tema de la importancia de la seguridad informática, es el comercio electrónico que se puede ver como parte de la estrategia de desarrollo del mercado. Los consumidores han expresado su preocupación general por la privacidad y la seguridad de sus datos, las empresas con una fuerte seguridad pueden aprovechar su inversión para aumentar el número de compradores y a su vez aumentar su cuota de mercado.

Ya no se tiene que mirar a la seguridad informática únicamente como para evitar la pérdida de la información, la seguridad informática hoy se convierte en una ventaja competitiva que puede contribuir de manera directa a las cifras de ingresos y así el progreso de una empresa.

2.2 MARCO CONCEPTUAL

ISO. - Es una organización que regula una seria de normas para fabricación, comunicación y comercio en empresa y organizaciones internacionales.

COBIT. - Es un modelo que permite auditar la gestión y control de sistemas de información y de tecnología.

ITIL. - También conocida como Biblioteca de Infraestructura de Tecnología de Información, lo cual es una colección de las mejores prácticas observadas en la industria de TI.

Firewall. - Programa informático que controla el acceso de una computadora a la red y sus elementos por seguridad.

BSI. - Son las siglas de La British Standards Institution la cual se fundamenta en la creación de normas para estandarizar los procesos.

SGSI. - Es un Sistema de Gestión de Seguridad de la Información cuya entidad se encarga de los siguientes procesos: diseño, implantación, mantenimiento, confidencialidad, integridad y disponibilidad.

Interconectividad. - Es un proceso de comunicación el cual ocurre entre dos o más redes que están conectadas entre sí.

Métricas. - Es aquello que permite describir la unidad de longitud de una medida.

Holístico. - Algo que se considera como un todo.

Genealógico. - Que contiene un conjunto o parte de algo que pertenece a un documento o libro.

Ofimática. - Es un conjunto de herramientas, técnicas y aplicaciones que se utilizan para las tareas de oficinas.

Traceroute. - Es un pequeño programa de consola de diagnóstico que admite seguir la pista de los paquetes que vienen desde un punto de red.

2.3 CONOCIMIENTO ACADÉMICO

Tabla 1 **Conocimiento Académico**

Nombre de la asignatura	Utilización dentro de la propuesta tecnológica
Gestión de TIC's	Nos ayuda a tener una mejor visión de cómo la entidad manipula toda la información.
Gestión de Proyectos	La gestión de proyectos nos guía en la construcción de esta propuesta tecnológica.
Auditoria de Sistemas	Nos permite verificar todos los procesos que realiza la entidad.
Organización y Métodos	Nos plantea como está estructurada la entidad.
Administración Gerencial	Nos permite verificar si están utilizando adecuadamente los recursos que la entidad tiene a disposición.
Investigación I, II, III, IV	La investigación es un método científico que nos guía a obtener resultados.

Fuente elaboración propia

CAPÍTULO III: ANÁLISIS DE ALTERNATIVAS DE SOLUCIÓN

3.1. TÍTULO DE LA PROPUESTA

3.1.1. PROPUESTA 1

Propuesta del diseño de un Proceso de implementación del Sistema de Seguridad de Información mediante la Norma ITIL en el GAD Municipal de Milagro.

- **Fundamentación teórica:**

En 1980 se impulsó la norma ITIL, pero se adecuo hasta el año de 1990 por Central Computer and Telecommunications Agency (CCTA) del gobierno británico y es de libre manejo. ITIL se define como IT Infrastructure Library, biblioteca de infraestructura de TI con referencia de administración de procesos, pero a través como se desarrollaba se llegó al nombre ITIL.

La norma ITIL está basado en las mejores prácticas de gestión y soporte de servicios de tecnología informática, mediante la correcta definición de los procesos. Los servicios que se entregan a los usuarios deben ser orientadas a la más alta calidad, satisfacer las necesidades de la organización y a los clientes cumpliendo leyes, normas, políticas y reglamentos acorde a la constitución de los países donde se implante esta metodología, su propósito principal es que debe ser entregados de forma eficaz y eficiente, revisarlas y posteriormente tener un plan de acciones correctivas y preventivas para la mejora continua.

Las acciones más trascendentales de la norma ITIL ayuda a respaldar mas no a fijar los procesos de los negocios de una organización teniendo en cuenta los objetivos de la gestión de servicios son:

- Calidad en los servicios
- Aumentar la eficiencia
- Reducir los riesgos asociados a los servicios de la tecnología de la Información

Esta norma no tiene un enfoque hacia la gestión de la seguridad a través de la implementación o mejora de un Sistema de gestión de Seguridad Informática, sin embargo, para poder realizar y aplicar la gestión de servicios y la gestión de seguridad se toma en cuenta la importancia que implica los riesgos para cumplir con los objetivos que se dese alcanzar

La Norma ITIL hace un énfasis en la seguridad de la gestión de servicio con respecto a la seguridad de la Información, para lo cual se fundamenta en la gestión de Incidentes en la cual se rige de una serie de etapas como se muestra en la siguiente figura:

Ilustración 1 Etapas de gestión de incidencias de la norma ITIL

Fuente de la web

Incidencia: es la manera como se comunica el usuario o que se genera automáticamente por las aplicaciones que utilice el usuario.

Service Desk: Son los responsables directos de la gestión de incidencias, son la primera línea de soporte, de aquí parte las demás etapas de forma ordenada para resolver el problema de seguridad de la Información.

Registro y Clasificación: en esta etapa se crea un registro del incidente en el cual se define su prioridad que se calcula como el impacto por la urgencia y se lo categoriza como tipo y personal de soporte que ayudara a dar soluciones de manera más eficientes y eficaz para el usuario.

KDB: Es una etapa de consulta en la base de Datos con la extensión. kdb de conocimiento para verificar si existe una solución preestablecida para solucionar el incidente, primero si se conoce el método de solución se asigna los recursos necesarios para solucionar el incidente, segundo si no se conoce el método solución se escala el incidente a un nivel superior de soporte.

Escalado: Existe dos tipos de escalado en el proceso de resolución de la incidencia, se puede clasificar cono escalado funcional al que recurre a técnicos

de nivel superior, y escalado jerárquico donde se escala la incidencia a un responsable de mayor jerarquía de la organización.

Resolución y Cierre: Este paso cumple cuando se ha logrado resolver satisfactoriamente un incidente, luego se procede a crear un registro en la base de datos de conocimientos o si fuera necesario se genera una petición de cambio.

Esta norma establece un control de responsabilidad y procedimiento en el tratamiento de la gestión de incidentes de la seguridad de la información, guía en la que se define procedimientos a seguir en la gestión de incidentes, la diferencia que tiene esta norma con respecto a otras es la manera de cómo tratar los incidentes que perjudica en la seguridad informática, para ITIL un incidente es " cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o genera una interrupción o una reducción de la calidad del sistema de seguridad de información".

La ITIL considera únicamente aquellos incidentes que tienen relación con la infraestructura tecnológica de la organización y respectivo soporte y provisión de estos servicios que oferte la empresa, mediante esta norma toma como incidente aquellos eventos no solo tecnológicos tales como físicos, ambientales y personas sino a todos los insumos que afectan a la disponibilidad, integridad y confidencialidad de los activos de información.

- **Análisis técnico:**

Entre las características de la norma de Trabajo ITIL:

- La norma de Trabajo ITIL solo respalda a los procesos de negocios de una organización.
- ITIL se centra en la gestión de incidentes, para ITIL un incidente es cualquier evento que no forma parte de la operación estándar de un servicio y que causa o puede causar interrupción o una reducción de calidad del mismo.

3.1.2. PROPUESTA 2

Propuesta del diseño de un Proceso de implementación del Sistema de Seguridad de Información mediante la Norma COBIT en el GAD Municipal de Milagro.

- **Fundamentación teórica**

Los Objetivos de Control para la Información y la Tecnología Relacionadas (COBIT), es un marco de trabajo basados en procesos que reúne por lo general buenas prácticas y estándares internacionales entre ellos la Norma ISO 27000, en estos procesos están enfocados a la gestión de las tecnologías de la información de una información de una organización con el propósito de alinear los objetivos de la tecnología de la Información con los objetivos de la organización basado en las perspectiva de sus necesidades.

COBIT esté compuesto por 4 dominios denominados:

Planear y Organizar (PO) este dominio establece y direcciona parámetros para asegurar que la tecnología de información de un negocio contribuya al cumplimiento de los objetivos organizacionales basados en las estrategias TICS y las de nivel empresarial.

Adquirir e Implementar: la Identificación, desarrollo o adquisición de soluciones de la tecnología de información se basa en las soluciones que están cubiertas por este dominio, además este parámetro establece si es necesario realizar cambio o mantenimiento de los sistemas ya existente en la organización.

Entregar y Dar Soporte: La entrega de los servicios requeridos administración de la seguridad y de la continuidad están cubiertas por este dominio

Monitorear y evaluar este dominio se encarga de la evaluación del desempeño del proceso de la tecnología de la información y asegura que el cumplimiento de los requerimientos y necesidades de la empresa se cumplan.

Los dominios de COBIT contienen 34 procesos genéricos que administran los recursos de la tecnología de la información y para cada proceso se define objetivos de control que son parte para alcanzar las metas definidas para la organización.

Cobit perfecciona las inversiones del TI con esto ayuda a la medición donde se podrá calificar en el momento que algo falle.

- Marco de trabajo de control Cobit asiste a las siguientes necesidades:
- Establece vínculo con los requerimientos del negocio.
- Organiza las actividades de TI en un modelo de procesos.
- Identifica los recursos primordiales de TI.
- Define los objetivos de control gerenciales.

Cobit se enfoca en vincular las metas del negocio con las metas de TI esto aporta a medir los logros e identificar las responsabilidades que se asocian con los propietarios de los procesos de negocio y de TI.

- **Análisis técnico:**

Entre las características técnicas que tiene la norma COBIT en la implementación de un sistema de Seguridad de Información

Enfoque: COBIT está orientado al negocio basado en sus perspectivas de misión y visión organizacional, y además al gobierno de TI, y no se centra en el establecimiento de controles de seguridad seleccionada a partir de estudio de los procesos de gestión de riesgos de la información como otras normas.

Objetivo: COBIT busca ser una solución integral que ayude a las organizaciones a establecer y determinar un gobierno de TI.

Estructura: COBIT posee 4 procesos agrupados en 4 dominios

3.1.3. PROPUESTA 3

Propuesta del diseño de un Proceso de implementación del Sistema de Seguridad de Información mediante la Norma ISO 27001 en el GAD Municipal de Milagro.

- **Fundamentación Teórica:**

El estándar fue publicado en octubre del año 2005 por International Organization for Standartization y por International Electrotechnical Commision para la Gestión de la Seguridad de la Información.

Se publicó una nueva versión de la ISO 27001 en el año 2013 el cambio fue de gran importancia en la estructura, evaluación y tratamiento de los riesgos.

La norma ISO 27001 la conforman una serie de normas denominadas familias de normas SGSI Sistema de Gestión de la Seguridad de la Información cada una de ellas tiene un propósito específico para la creación y mantenimiento de un SGSI dentro de una organización.

La norma ISO 27001 es un marco de trabajo que permite a la organización pequeña, mediana y grande ya sea pública o privada desarrollar e implementar un Sistema de Gestión de la Seguridad de la Información, esta proporciona un modelo para establecer, operar monitorear, revisar, mantener y mejorar la seguridad de los activos de información como hardware, software, documentación etc.

La norma ISO 27001 es la que especifica los requisitos para establecer, operar monitorear, revisar, mantener y mejorar la seguridad de los activos de información, esta norma describe los requisitos generales para la certificación SGSI y los requisitos para las organizaciones certificadoras se establecen en las normas ISO 27001 Y ISO 27006 respectivamente.

La familia de normas Sistema de Gestión de Seguridad de Información facilitan tener una visión clara de lo que se desea alcanzar con la certificación de un Sistema de Gestión por lo cual hay que basarse en el siguiente modelo PHVA (Planear, Hacer, Verificar, Actuar).

En el contexto de un Sistema de Gestión de la Seguridad de la Información abarca la supervisión del proceso y la toma de decisiones con el propósito de alcanzar las metas organizacionales del negocio mediante la protección de los activos de Información, tales activos de información pueden ser datos,

aplicaciones, personas, servicios, hardware y software, es decir toda aquella información considerada de valor para la organización.

- **Análisis técnico:**

Este modelo de norma abarca tres aspectos fundamentales que son:

- Disponibilidad
- Confidencialidad
- Integridad

Basado en esto aspectos se logra asegurar la continuidad del negocio y el prestigio institucional. Para ello la seguridad de la información comprende la selección e implementación de controles de seguridad y la definición de políticas y procedimientos, en base al proceso de gestión de riesgo.

Entre las características que tiene la Norma ISO 27001 frente a otras normas de trabajo se tiene lo siguiente:

- Enfoque hacia la gestión de la seguridad a través de la implementación o mejora de un SGSI.
- Para la mejora de la gestión de servicios informáticos o gestión de seguridad toma en cuenta los riesgos de seguridad para cumplir los objetivos que se desea alcanzar.
- La norma cuenta con controles que hacen mayor énfasis en la seguridad de la información respecto a la gestión de servicios.
- La norma ISO 27001 define a un incidente de seguridad como: uno a varios eventos no deseados que ocurren en un sistema, servicio o red, que indican una violación de la política de seguridad o la falta de un control, llegando esto a comprometer a la seguridad de la información.
- Estructura: Norma ISO 27001 posee 11 dominios, 39 objetivos de control y 133 controles.

3.2. DELIBERACIÓN

Para la deliberación de la mejor propuesta se basó en una matriz de ponderación de criterios en donde se especifica las diferencias notables de las 3 normas propuestas, con el propósito de seleccionar la norma adecuada para la Seguridad de Información en el

GAD Municipal de Milagro. Por tal motivo, para la selección de la norma tenemos: ITIL, COBIT, ISO 27001

La metodología que se utilizó en el modelo de decisión y evaluación de alternativas es basada en las normas ISO 9126-3.

Por consiguiente la fórmula aplicada para los valores finales es:

X=1-A/B

X= Puntuación

A= Requisitos Faltantes de Seguridad

B= Total de requisitos solicitados

La puntuación más cercana a "1" es la mejor opción

Por consiguiente, se tendrá como objetivo facilitar el análisis de la selección de la norma más viable que se vaya a utilizar para la Seguridad de Información en el GAD Municipal de Milagro.

Los criterios de ponderación son los siguientes: "1 = Criterio es aprobado" y "0 = Criterio no aprobado".

Se considera en los criterios para la selección de la norma adecuada para la mejora de la seguridad de Información en el GAD Municipal de Milagro:

- Aspecto Técnico
- Costo
- Estructura
- Enfoque de Gestión
- Disponibilidad
- Confiabilidad
- Integridad

Tabla 2 **Deliberación Para escoger la mejor 0pción**

	ALTERNATIVAS

	ITIL	COBIT	ISO 27001
Aspecto Técnico	1	1	1
Costo	0	0	1
Estructura	1	1	1
Enfoque de Gestión	1	1	1
Disponibilidad	1	1	1
Confiabilidad	0	1	1
Integridad	1	0	1
Total	**0.714**	**0.714**	**1**

Fuente elaboración propia

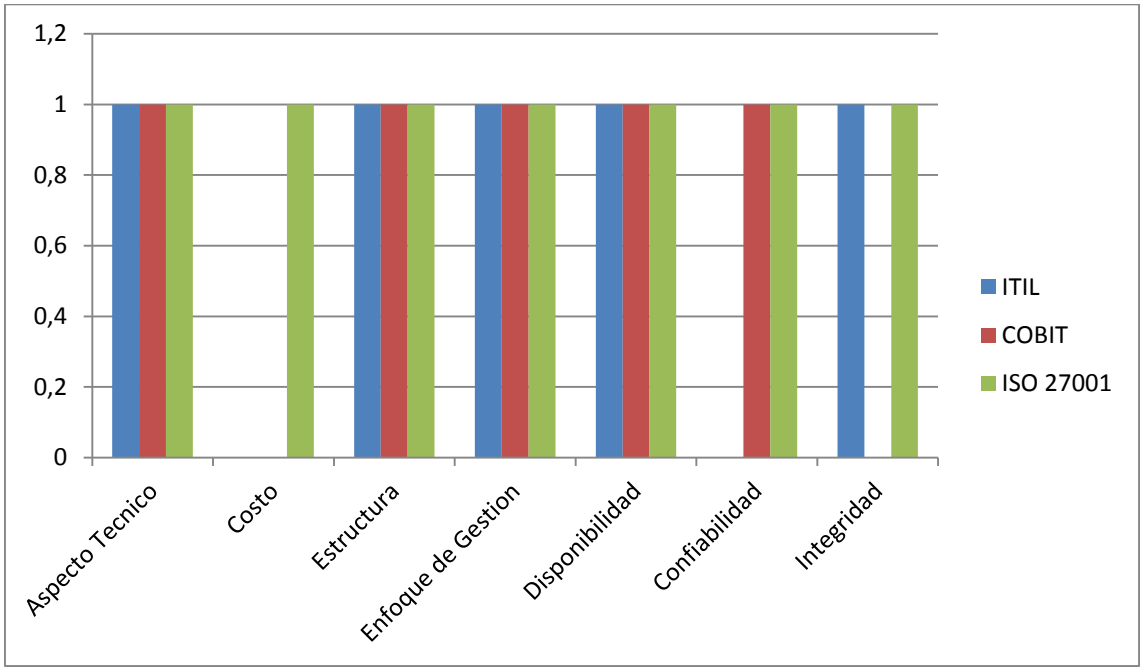

Ilustración 2 Resultados de la deliberación

Fuente elaboración propia

Como se observa en la tabla de valores la Norma ISO 27001 es más rentable ya que es más barata, a su vez cuenta con tres factores de suma importancia que son la disponibilidad, confiabilidad y la integridad, teniendo en cuenta que la Norma ISO 27001 cuenta con las políticas y planes de acciones que ayudaran a tener más segura la información del GAD Municipal de Milagro.

3.3. ELECCIÓN DE LA SOLUCIÓN

Se determinó el título de la propuesta del ítem 3.1.3 con el tema: PROPUESTA DEL DISEÑO DE UN PROCESO DE IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE INFORMACIÓN MEDIANTE LA NORMA ISO 27001 EN EL GAD MUNICIPAL DE MILAGRO.

Luego de la comparativa realizada mediante el estudio planteado y basado en las necesidades se escoge como mejor opción la propuesta antes mencionada, esta propuesta frente a las otras se caracteriza por ser la más viable económicamente y satisfacer las necesidades que requiere la entidad.

Se tiene en cuenta que la Norma ISO 27001 ofrece tres características principales:

Disponibilidad: Se encuentra en todo los campos legales a nivel mundial es referente en temáticas de seguridad de Información.

Confidencialidad: La norma es uno de los referentes en mayor confiabilidad en el campo de la seguridad de la Información, sus procesos de control son de alta seguridad para cualquier organización.

Integridad: Dentro de los procesos de control se protege la información de todos los entes departamentales de la organización desde un punto de vista holístico y de mayor importancia en la cual protege y garantiza el no escape de información.

CAPÍTULO IV: DESARROLLO DE LA PROPUESTA TECNOLÓGICA

4.1. **TÍTULO Y DESCRIPCIÓN DE LA PROPUESTA TECNOLÓGICA**

Auditoria de la Seguridad Informática basado en la ISO 27001 sistema de gestión de seguridad de la información para el GAD Municipal de Milagro.

Este proyecto pretende desarrollar un Plan de Seguridad de la Información basado en las normas INEN ISO/IEC 27001, para el GAD Municipal de Milagro con el fin de establecer las políticas, procedimientos de gestión de la seguridad de la información que utiliza la identidad.

La información de las instituciones públicas de cualquier país, junto a los procesos informáticos y sistemas, son activos muy importantes de toda organización. La confidencialidad, integridad y disponibilidad de información son esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen institucional necesarios para lograr los objetivos de las instituciones.

Con el sistema de seguridad de Información logra asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un Sistema de Gestión de Seguridad de la Información es una herramienta de gran utilidad y de importante ayuda para la gestión de la información en las organizaciones.

El nivel de seguridad informática alcanzado por medios tradicionales es insuficiente por sí mismo. La gestión efectiva de la seguridad informática debe tomar parte activa toda la organización, desde la gerencia, clientes y proveedores. El modelo de gestión de la seguridad contiene procedimientos adecuados que son basados de la planificación organización, y controles basados en una evaluación de riesgos y en una medición de la eficacia de los procesos que implican en el sistema de información.

El Sistema de Gestión de la Seguridad de la Información ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

El presente estudio se enfoca en la seguridad de Información en el GAD Municipal de Milagro basado en esta problemática, donde la población a considerar serán las personas que integran el Departamento de Sistemas. Basado en el contexto del problema tendrá un diseño documental donde el proceso de búsqueda se basara en la recuperación, análisis, crítica e interpretación de datos obtenidos y registrados por otros autores de fuente documentales como libros de herramientas tecnológicas, revistas con artículos relacionados al aprendizaje mediante herramientas TIC's, y de tesis de pregrado aplicado a entes gubernamentales.

Según su finalidad, es básica porque se estará en observación de documentos como libros, revistas y trabajos de grados entorno a la temática de estudio con la finalidad de dar soporte a la información redactada en el presente documento esto permitirá tener un alcance en cuestiones teóricas y prácticas de lo planteado en la problematización.

Según su finalidad, es aplicada porque de acuerdo a los datos obtenidos en los instrumentos de estudio se planteara una solución consistente para poder aportar en el manejo de herramientas tecnológicas ayudando a mejorar la seguridad informática.

Según el objeto genealógico, es descriptivo y se caracteriza un hecho o fenómeno, con el propósito de establecer su comportamiento. A través de este tipo de estudio se miden las variables implícitas en los objetivos de la investigación. Esto se aplicara al presente proyecto debido a que se describirá los factores que inciden en el uso adecuado de las normas de seguridad informática, basado en los instrumentos de investigación que se aplicaran en la obtención de la información.

Según su contexto, es de campo es un método donde se recolectan los datos directamente de la realidad, sin manipular variables y este se lo aplicara porque la obtención de la información se lo aplicara al talento humano de sistemas, aplicando el instrumento de investigación para verificar las premisas planteadas en el estudio observando y analizando las variables por las cuales no se utilizan adecuadamente las herramientas tecnológicas por parte del personal de sistemas y como estas influyen en el aprendizaje de los mismos.

Según el control de las variables, es no experimental en la cual se define los factores que son controlados por el investigador para eliminar o neutralizar cualquier efecto que podrían tener de otra manera en el fenómeno observado.

4.2. OBJETIVO GENERAL Y ESPECÍFICOS

Objetivo General

Diseñar un plan de Gestión de Seguridad de la Información para el GAD Municipal de Milagro implementando la norma ISO-27001.

Objetivos Específicos

- Analizar la seguridad de la información actual de la entidad.
- Determinar el nivel de madurez en el que se encuentra la entidad para su modelo de seguridad de la información.
- Definir los planes de acción orientados a corregir inseguridades que se encuentre en la entidad según la norma a implementar.
- Definir las políticas de la Seguridad de la Información de la entidad tomando como base la norma ISO 27001:2013.

4.3. DESARROLLO EN DETALLE DE LA PROPUESTA TECNOLÓGICA

Antecedentes:

La ilustre Municipalidad del Cantón Milagro, a través de la Señora Alcaldesa Denisse Robles Y EL director de la Dirección de Tecnologías de la Información y Comunicaciones, han brindado la apertura para aplicar el presente proyecto técnico, además han demostrado un gran interés porque se considera esencial para la gestión organizacional en cuanto a la seguridad de la información que maneja el GAD Municipal de Milagro.

Análisis de la Problemática

La problemática del GAD Municipal del Cantón Milagro será analizada mediante un cuadro análisis FODA donde se centra en el enfoque de la gestión de seguridad de la información, para de esta manera determinar la importancia de la implementación del Sistema de Gestión de Seguridad Informática en la organización. Cabe resaltar que las debilidades y amenazas fueron deducidas en base a un análisis de observación mantenidas con los funcionarios.

Tabla 3 **Análisis FODA**

FODA de la Seguridad de la Información en el GAD Municipal de Milagro

FORTALEZAS	OPORTUNIDADES
• El departamento de TICS no depende de otras direcciones para la toma decisiones, es decir las iniciativas con respecto a la adquisición de una nueva infraestructura tecnológica, en el caso de implementación del SGSI pueden ser tratadas de manera directa con la Coordinación Municipal. • La gestión de información del GAD Municipal se encuentra centralizada en el Departamento TICS motivo por el cual resulta más sencillo protegerla mediante controles de seguridad. • Actualmente se ha establecido controles de seguridad Física como es del caso del Circuito cerrado de Cámaras IP, registro de usuarios y visitantes a las instituciones de la Dirección de vigilancia de la policía Municipal.	• Capacitación al personal del Municipio en temáticas de Seguridad Informática. • Definición de nuevas políticas de seguridad e implantación para la protección de los activos de información. • Cumplir con las normativas y leyes establecidas para la protección de derechos de autor.
DEBILIDADES	**AMENAZAS**
• Falta de capacitación de los funcionarios del GAD Municipal. • Falta de controles de seguridad de la Información que se maneja en los departamentos del Municipio. • Sistema inadecuado de respaldo de información que se maneja en los departamentos del Municipio. • Falta de mantenimiento de todos los equipos informáticos. • Resistencia al cambio por parte de algunos funcionarios. • Falta de licencias originales de algunos sistemas operáticos y software ofimática. • No está definido los perfiles de usuarios de algunos departamentos. • Falta de documentación de los sistemas y de las actualizaciones.	• Por el hecho de contar con un sistema web que necesita autenticar su inicio de sesión, existen vulnerabilidades en el sistema actual. • Acceso físico no autorizado a las instalaciones del GAD Municipal. • Fuga o revelación de información en varios departamentos. • Fallas en el suministro de energía eléctrica.

Fuente elaboración propia

Las instituciones públicas del estado ecuatoriano están expuestas a diferentes amenazas de seguridad de información que ha ocasionado una serie de incidentes que han llegado a ser de conocimiento público a nivel nacional en estos años, por tal motivo este proyecto se centra en el GAD Municipal que pueda servir como reflejo de la realidad de la seguridad de información

en todas las entidades públicas del cantón Milagro, generando un beneficio para determinar la importancia y beneficios de la Implementación del Sistema de Gestión de Seguridad de la Información.

Las debilidades identificadas pueden ser cubiertas mediante la implementación de algunos controles de la norma ISO 27001 como se muestra a continuación:

Controles de las debilidades del Análisis FODA

Tabla 4 **Controles de las debilidades del análisis FODA**

DEBILIDADES	CONTROLES
Falta de capacitación de los funcionarios del GAD Municipal.	A.5.2.2 Concientización, Formación y capacitación.
Falta de controles de seguridad de la Información que se maneja en los departamentos del Municipio.	A.5.1.1 Documento de política de seguridad de la información. A.5.1.2 Revisión de la Política de Seguridad de la Información.
Sistema inadecuado de respaldo de información que se maneja en los departamentos del Municipio.	A.10.5.1 Respaldo de la Información. A.15.1.3 Protección de los registros de la Organización.
Falta de mantenimiento de todos los equipos informáticos.	A.9.2.4 Mantenimiento de los Equipos.
Resistencia al cambio por parte de algunos funcionarios.	A.5.2.2 Concientización, formación y capacitación. A.7.1.1 Inventario de activos.
Falta de licencias originales de algunos. Sistemas operáticos y software ofimática.	15.1.2 Derecho de propiedad Intelectual.
Falta de documentación de los sistemas y de las actualizaciones.	A.7.1.1 Inventario de Activos. A.12.4.1 Control de software operativo. A.12.5.1 Procedimiento de control de cambios.
No están definidos los perfiles de usuarios de algunos departamentos.	A.11.1.1 Política de control de acceso.

Fuente elaboración propia

De igual forma para cubrir las amenazas identificadas se puede implementar los controles especificados.

Tabla 5 **Controles de las amenazas del análisis FODA**

Amenazas	Controles
Por el hecho de contar con un sistema web que necesita autenticar su inicio de sesión, existen vulnerabilidades en el sistema actual.	A.5.2.2 Concientización, información y capacitación. A.5.1.1 Documento de Política de Seguridad de la Información. A.5.1.2 Revisión de la Política de Seguridad de la Información. A.12.2.1 Validación de los datos de Entrada. A.12.2.2 Control de procesamiento interno. A.12.8.1 Control de las vulnerabilidades técnicas.
Acceso físico no autorizado a las instalaciones del GAD Municipal.	A.9.1.1 Perímetro de la seguridad física. A.9.1.2 Controles de acceso físico. A.9.1.3 Seguridad de oficinas, recintos e instalaciones.
Fuga o revelación de información en varios departamentos.	A.9.2.1 Ubicación y protección de los equipos. A.12.5.4 Fuga de Información.
Fallas en el suministro de energía eléctrica.	A.15.1.1 Capacidad de generación de reserva. A.15.1.2 Instalación de reguladores de tensión. A.15.1.4 Instalación de circuitos de respaldo.

Fuente elaboración propia

El análisis FODA permitió conocer e identificar las oportunidades que pueden ser explotadas mediante la implementación de un SGSI, así como las fortalezas que permitirán al Departamento TICS, implementar, mantener y mejorar dicho Sistema de Gestión.

Análisis de las seguridades de información en el GAD Municipal

Para el análisis de la seguridad de la información en la institución se hace necesario conocer el modelo de organización donde se destaque los objetivos, y sus actividades empresariales, además de identificar la estructura jerárquica de la organización.

Se proponen métodos de la norma ISO 27001 que servirá para identificar los problemas de la gestión de la Seguridad de La información y definir las posibles soluciones que servirán como base para el proceso de Implementación del SGSI.

GAD MUNICIPAL DEL CANTON MILAGRO

El 17 de septiembre de 1913 en Milagro se eleva a categoría de Cantón San Francisco de Milagro, por la cual está constituida por 4 parroquias urbanas principales tales como: Camilo Andrade Manrique, Chirijos, Coronel Enrique Valdez C., Ernesto Seminario Hans.

MISION

"Contribuir al bienestar de los ciudadanos y ciudadanas del cantón Milagro como facilitador de los esfuerzos de la comunidad en la planificación, ejecución, generación, distribución y uso de los servicios que hacen posible la realización de sus aspiraciones sociales a través de la dotación de obras y servicios públicos; desarrollo humano, social, cultural, económico, ambiental, productivo, para promover el desarrollo integral sostenible y procurar el buen vivir, con participación, equidad e inclusión de sus habitantes".

VISION

El Gobierno Autónomo Descentralizado Municipal del cantón San Francisco de Milagro, se constituirá en un ejemplo del desarrollo local y contará con una organización interna eficiente, generadora de productos y servicios compatibles con la demanda de la sociedad, para convertirse en un centro de desarrollo que crece en forma planificada con aprovechamiento sustentable de sus recursos, dotada de servicios básicos y poseedora de autoridades transparentes, con un gobierno democrático y una ciudadanía solidaria y corresponsable en la Dirección del desarrollo con equidad"

Ubicación

Ilustración 3 Ubicación del GAD Municipal de Milagro

Fuente de la web

Estructura Orgánica

La representación jerarquizada de las Unidades Administrativas que intervienen en la gestión de procesos institucionales.

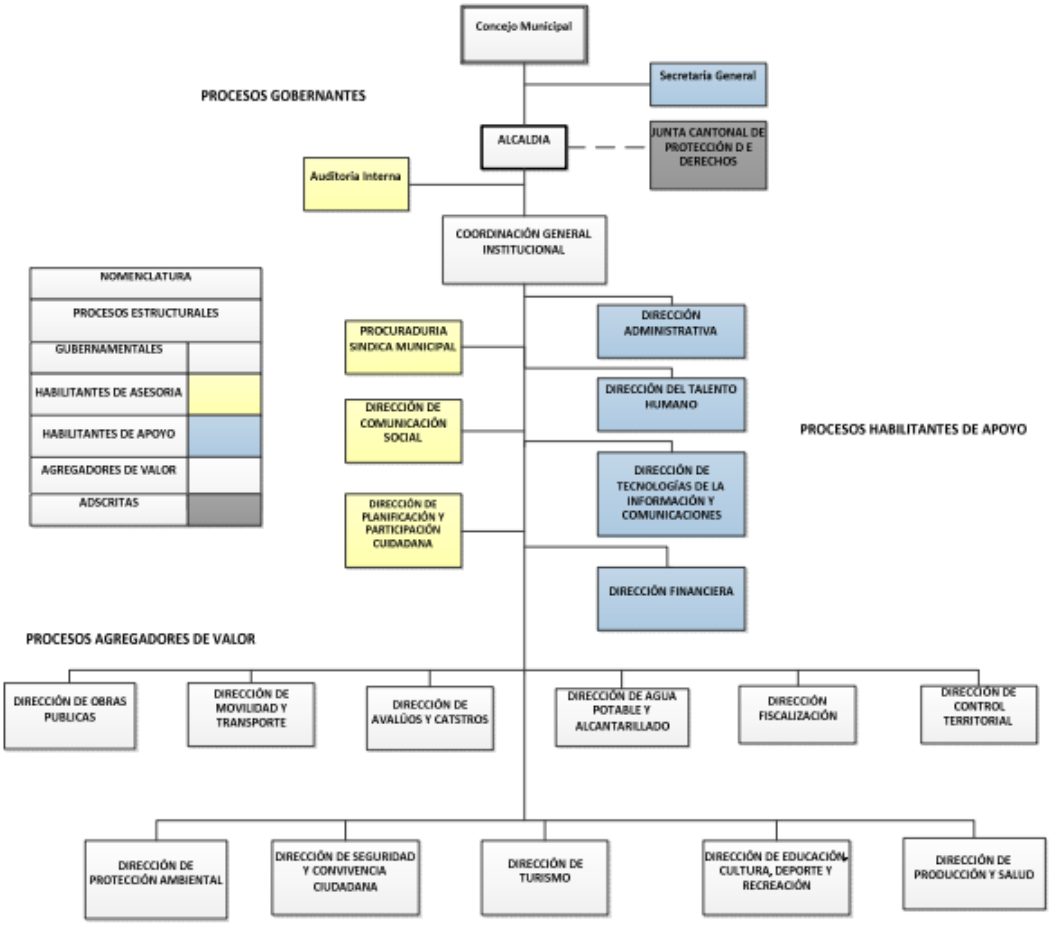

Ilustración 4 Estructura orgánica

Fuente GAD municipal de Milagro

El proceso gobernante direcciona la gestión institucional y organizacional a través de la formulación de políticas y estrategias empresariales, mediante la expedición de ordenanzas municipales, reglamentos, normas e instrumentos para el funcionamiento de la organización.

Los procesos Habilitantes se clasifican en procesos habilitantes de asesoría y procesos habilitantes de apoyo, y su función es de generar productos y servicios para los procesos gobernantes y agregadores de valor por lo cual aporta a la gestión administrativa del GAD Municipal de Milagro.

Los procesos agregadores de valor generan, administran y controlan los productos y servicios primarios destinados a usuarios externos e internos y permiten cumplir con la misión institucional, estos constituyen la razón del ser del Municipio.

Actividades

Las principales actividades del ilustre Municipio del Cantón Milagro se detallan a continuación:

- Gestión de Obras Publicas
- Gestión de Movilidad y Transporte
- Gestión de Avalúos y Catastro
- Gestión de Agua Potable y Alcantarillado
- Gestión de Fiscalización
- Gestión de Control Territorial
- Gestión de Protección Ambiental
- Gestión de Seguridad y Convivencia Ciudadanía
- Gestión de Turismo
- Gestión de Educación, Cultura, Deporte y recreación
- Gestión de Producción y Salud.

El Departamento de Tecnologías de la Información y Comunicación está conformado por la siguiente estructura:

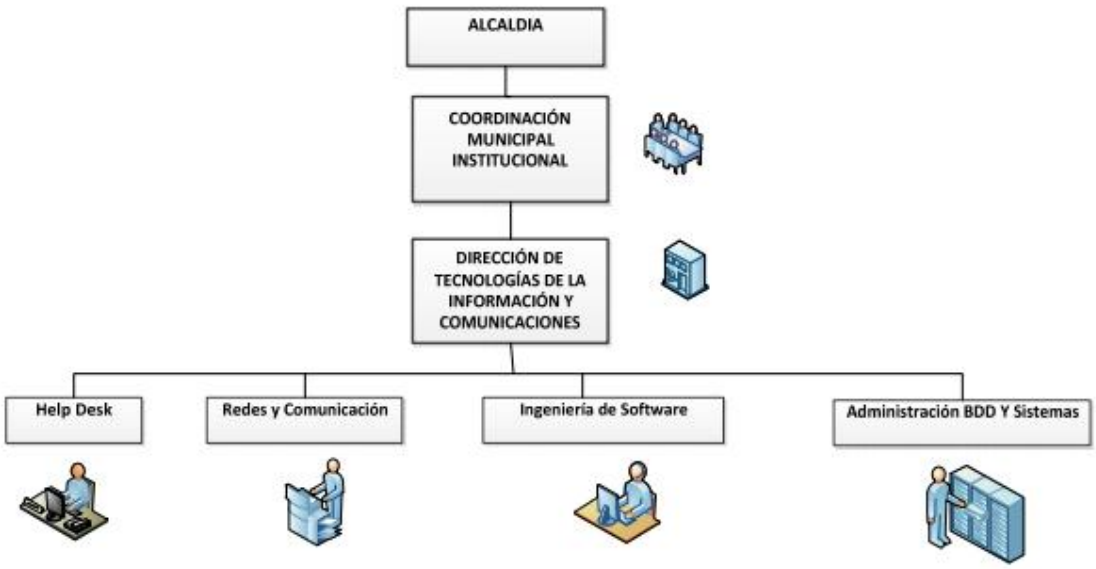

Ilustración 5 Estructura del Departamento de Tecnología de la Información y Comunicación

Fuente GAD municipal de Milagro

El departamento de TICS se compone la Dirección, Help Desk, Redes y Comunicaciones, Ingeniería de Software, Administración de base de Datos y Sistemas, para cumplir con las diferentes obligaciones, la dirección cuenta con un STAFF de analistas y técnicos cuyos perfiles

son idóneos para el puesto. Cada uno de los cargos y sus funciones están formalmente documentados en el Estatuto Orgánico de Gestión Organizacional por Procesos.

Método de evaluación del estado cumpliendo de la Norma ISO 27001 SGSI en el GAD Municipal del Cantón Milagro.

El análisis del estado actual de la seguridad de información se realizó mediante la elaboración de una matriz Check List con técnica de observación que determina el porcentaje de cumplimiento de la norma ISO 27001. Esta matriz considera las características principales de los controles de seguridad detallados en la norma.

- **Nivel de Madurez**

DESPLIEGUE DE CHECK-LIST

Dado los resultados que se serán mostrados mediante el Check-List será en porcentaje.

PARA ENCONTRAR EL VERDADERO

Tabla 6 **Para encontrar el verdadero**

Total de preguntas	100%
Preguntas de Verdadero	✓

Fuente elaboración propia

PARA ENCONTRAR EL FALSO

Tabla 7 **Para encontrar el falso**

Total, de preguntas	100%
Preguntas de Falso	X

Fuente elaboración propia

La puntuación más cercana a “1” es la mejor opción

Los criterios de ponderación son los siguientes: “1 = Criterio de Verdadero” y “0 = Criterio Falso”.

Entonces para encontrar el porcentaje de la ponderación se obtendrá de la siguiente manera:

Suma = La suma de los criterios de verdadero.

Porcentaje = El resultado de la suma y esto multiplicado por 100 luego dividir para la cantidad de preguntas de cada cuestionario

Y Será representado de esta forma:

Check-List para las Políticas de Seguridad:

Tabla 8 **Políticas de seguridad**

Empresa:	GAD Municipal del Cantón Milagro		
Cuestionario de Control de Políticas de Seguridad	C1		
Dominio	Políticas de Seguridad		
Proceso	Control de la Seguridad de la Información		
Objetivo de Control	Seguridad de la Información de las Políticas de Seguridad		
Cuestionario			
Pregunta	**VERDADERO**	**FALSO**	**PONDERACIÓN**
Existen documento(s) de políticas de seguridad de SI	✓		1
Existe normativa relativa a la seguridad de los SI	✓		1
Existen procedimientos relativos a la seguridad de SI	✓		1
Existe un responsable de las políticas, normas y procedimientos		X	0
Existen mecanismos para la comunicación a los usuarios de las normas		X	0
Existen controles regulares para verificar la efectividad de las políticas		X	0
		Suma:	3
		Porcentaje:	50%

Fuente elaboración propia

Recomendación 1

Se puede observar que cumple con lo establecido de este cuestionario el 50% se debe implementar las políticas, normas y procedimientos y mejorar la comunicación de los usuarios tener controles y verificación de las políticas.

Check-List para la Organización de la Seguridad:

Tabla 9 **Organización de la seguridad**

Empresa:	GAD Municipal del Cantón Milagro		
Cuestionario de Organización de la Seguridad	C2		
Dominio	Organización de la Seguridad		
Proceso	Control de la Organización de la Seguridad		
Objetivo de Control	Evaluación de la Información de la Organización		
Cuestionario			
Pregunta	**VERDADERO**	**FALSO**	**PONDERACIÓN**
Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	✓		1
Existe un responsable encargado de evaluar la adquisición y cambios de SI		X	0
La Dirección y las áreas de la Organización participa en temas de seguridad	✓		1
Existen condiciones contractuales de seguridad con terceros y outsourcing		X	0
Existen criterios de seguridad en el manejo de terceras partes		X	0
Existen programas de formación en seguridad para los empleados, clientes y terceros		X	0
Existe un acuerdo de confidencialidad de la información que se acceso	✓		1
		Suma:	3
		Porcentaje:	37.50%

Fuente elaboración propia

Recomendación 2

Se puede observar que cumple con lo establecido de este cuestionario el 37.50% se debe implementar medidas de responsabilidades que se encarguen en la evaluación y cambios de SI. Y tener condiciones de seguridad como también programas en seguridad para empleados, clientes y terceros.

Check-List para la Administración de Activos:

Tabla 10 **Administración de activos**

Empresa:	GAD Municipal del Cantón Milagro		
Cuestionario de Administración de Activos	C3		
Dominio	Administración de Activos		
Proceso	Gestión de Inventarios		
Objetivo de Control	Controles de inventarios y procedimientos de la información		
Cuestionario			
Pregunta	**VERDADERO**	**FALSO**	**PONDERACIÓN**
Existen un inventario de activos actualizado		X	0
El Inventario contiene activos de datos, software, equipos y servicios		X	0
Se dispone de una clasificación de la información según la criticidad de la misma	✓		1
Existe un responsable de los activos	✓		1
Existen procedimientos para clasificar la información		X	0
		Suma:	2
		Porcentaje:	33.33%

Fuente elaboración propia

Recomendación 3

Se puede observar que cumple con lo establecido de este cuestionario el 33.33% no se dispone de información clasificada según la criticidad tampoco existe procedimientos para el mismo.

Check-List para la Seguridad de los RRHH:

Tabla 11 **Seguridad de los RRHH**

Empresa:	GAD Municipal del Cantón Milagro		
Cuestionario de Seguridad de los RRHH	C4		
Dominio	Seguridad de los RRHH		
Proceso	Dirección de responsabilidades		
Objetivo de Control	Definición de roles de seguridad		
Cuestionario			
Pregunta	**VERDADERO**	**FALSO**	**PONDERACIÓN**
Se tienen definidas responsabilidades y roles de seguridad		X	0
Se tiene en cuenta la seguridad en la selección y baja del personal		X	0
Se plasman las condiciones de confidencialidad y responsabilidades en los contratos		X	0
Se imparte la formación adecuada de seguridad y tratamiento de activos		X	0
Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	✓		1
Se recogen los datos de los incidentes de forma detallada		X	0
Informan los usuarios de las vulnerabilidades observadas o sospechadas		X	0
Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades		X	0
Existe un proceso disciplinario de la seguridad de la información		X	0
		Suma:	1
		Porcentaje:	11.11%

Fuente elaboración propia

Recomendación 4

Se observa que cumple con lo establecido de este cuestionario el 11.11% existe fallas en varios aspectos como no tener definidas responsabilidades y roles de seguridad tampoco se tiene en cuenta la baja del personal existen poca información detallada de los incidentes que se recogen y se debe implementar un proceso disciplinario para la seguridad de la información.

Check-List para la Seguridad Física y del Ambiente:

Tabla 12 **Seguridad física y del ambiente**

Empresa:	GAD Municipal del Cantón Milagro		
Cuestionario de la Seguridad Física y del Ambiente	C5		
Dominio	Seguridad Física y del Ambiente		
Proceso	Protección de la Seguridad Física y Ambiental		
Objetivo de Control	Controles Físicas y del Ambiente		
Cuestionario			
Pregunta	**VERDADERO**	**FALSO**	**PONDERACIÓN**
Existe perímetro de seguridad física (una pared, puerta con llave	✓		1
Existen controles de entrada para protegerse frente al acceso de personal no autorizado		X	0
Un área segura ha de estar cerrada, aislada y protegida de eventos naturales		X	0
En las áreas seguras existen controles adicionales al personal propio y ajeno		X	0
Las áreas de carga y expedición están aisladas de las áreas de SI		X	0
La ubicación de los equipos está de tal manera para minimizar accesos innecesarios		X	0
Existen protecciones frente a fallos en la alimentación eléctrica		X	0
Existe seguridad en el cableado frente a daños e intercepciones		X	0
Se asegura la disponibilidad e integridad de todos los equipos		X	0
Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente		X	0
Se incluye la seguridad en equipos móviles		X	0
		Suma:	1
		Porcentaje:	9.09%

Fuente elaboración propia

Recomendación 5

Se observa que sólo cumple con lo establecido de este cuestionario el 9.09% existen demasiadas falencias en los controles, así como el acceso a personal no autorizado y no se dispone de un área segura, aislada y protegida de eventos naturales.

Check-List para la Gestión de Comunicaciones y Operaciones:

Tabla 13 **Gestión de comunicaciones y operaciones**

Empresa:	GAD Municipal del Cantón Milagro		
Cuestionario de Gestión de Comunicaciones y Operaciones	C6		
Dominio	Gestión de Comunicaciones y Operaciones		
Proceso	Protección de los Sistemas de información		
Objetivo de Control	Control de Responsabilidades		
Cuestionario			
Pregunta	**VERDADERO**	**FALSO**	**PONDERACIÓN**
Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados		X	0
Están establecidas responsabilidades para controlar los cambios en equipos		X	0
Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad		X	0
Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas		X	0
Existe una separación de los entornos de desarrollo y producción		X	0
Existen contratistas externos para la gestión de los Sistemas de Información		X	0
Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento		X	0
Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones		X	0
Controles contra software maligno		X	0
Realizar copias de backup de la información esencial para el negocio	✓		1
Existen logs para las actividades realizadas por los operadores y administradores	✓		1
Existen logs de los fallos detectados		X	0
Existen rastro de auditoría		X	0
Existe algún control en las redes		X	0
Eliminación de los medios informáticos. Pueden disponer de información sensible		X	0
		Suma:	10%
		Porcentaje:	10%

Fuente elaboración propia

Recomendación 6

Se observa que sólo cumple con lo establecido de este cuestionario el 10% no existen procedimientos operativos identificados en la política de seguridad han de estar documentados tampoco se establecen acuerdos para intercambio de información y software.

Check-List para el Control de Accesos:

Tabla 14 **Control de accesos**

Empresa:	GAD Municipal del Cantón Milagro		
Cuestionario de Control de Accesos	C7		
Dominio	Control de Accesos		
Proceso	Gestión de Control de Usuarios		
Objetivo de Control	Evaluación y Restricción de Accesos		
Cuestionario			
Pregunta	**VERDADERO**	**FALSO**	**PONDERACIÓN**
Existe una política de control de accesos	✓		1
Existe un procedimiento formal de registro y baja de accesos		X	0
Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario		X	0
Existe una gestión de los password de usuarios		X	0
Existe una revisión de los derechos de acceso de los usuarios		X	0
Existe el uso del password	✓		1
Se protege el acceso de los equipos desatendidos		X	0
Existen políticas de limpieza en el puesto de trabajo		X	0
Existe una política de uso de los servicios de red		X	0
Se asegura la ruta (path) desde el terminal al servicio		X	0
Existe una autenticación de usuarios en conexiones externas		X	0
Existe una autenticación de los nodos		X	0
Existe un control de la conexión de redes		X	0
Existe un control del routing de las redes		X	0
		Suma:	2
		Porcentaje:	12.50%

Fuente elaboración propia

Recomendación 7

Se muestra en el cuestionario que se cumple el 12.50% no existen controles de conexión a redes tampoco se controla el trabajo por la organización entre otras.

Check-List para el Desarrollo y Mantenimiento de los Sistemas:

Tabla 15 **Desarrollo y mantenimiento de los sistemas**

Empresa:	GAD Municipal del Cantón Milagro		
Cuestionario de Desarrollo y Mantenimiento de los Sistemas	C8		
Dominio	Desarrollo y Mantenimiento de los Sistemas		
Proceso	Gestión de Seguridad de la Información		
Objetivo de Control	Controles de Seguridad en los Sistemas de información		
Cuestionario			
Pregunta	**VERDADERO**	**FALSO**	**PONDERACIÓN**
Se asegura que la seguridad está implantada en los Sistemas de Información		X	0
Existe seguridad en las aplicaciones	✓		1
Existen controles criptográficos		X	0
Existe seguridad en los ficheros de los sistemas		X	0
Existe seguridad en los procesos de desarrollo, testing y soporte		X	0
Existen controles de seguridad para los resultados de los sistemas		X	0
Existe la gestión de los cambios en los SO		X	0
Se controlan las vulnerabilidades de los equipos		X	0
		Suma:	1
		Porcentaje:	12.50%

Fuente elaboración propia

Recomendación 8

En el cuestionario se observa que cumple con el 12.50% y no se está cumpliendo con la seguridad en los sistemas de información y no hay control de seguridad para los resultados de los sistemas.

Check-List para la Administración de Incidentes:

Tabla 16 **Administración de incidentes**

Empresa:	GAD Municipal del Cantón Milagro		
Cuestionario de Administración de Incidentes	C9		
Dominio	Administración de Incidentes		
Proceso	Gestión de Daños		
Objetivo de Control	Reporte de Incidentes		
Cuestionario			
Pregunta	**VERDADERO**	**FALSO**	**PONDERACIÓN**
Se comunican los eventos de seguridad	✓		1
Se comunican las debilidades de seguridad		X	0
Existe definidas las responsabilidades antes un incidente		X	0
Existe un procedimiento formal de respuesta		X	0
Existe la gestión de incidentes		X	0
		Suma:	1
		Porcentaje:	20%

Fuente elaboración propia

Recomendación 9

A continuación, se muestra que cumple con el 20% del cuestionario se debe implementar la comunicación a las debilidades de seguridad y también mantener una gestión de incidentes.

Check-List para la Gestión de la Continuidad del Negocio:

Tabla 17 **Gestión de la continuidad del negocio**

Empresa:		GAD Municipal del Cantón Milagro	
Cuestionario de Control de Políticas de Seguridad		C10	
Dominio		Gestión de la Continuidad del Negocio	
Proceso		Gestión de la Continuidad	
Objetivo de Control			
Cuestionario			
Pregunta	**VERDADERO**	**FALSO**	**PONDERACIÓN**
Existen procesos para la gestión de la continuidad		X	0
Existe un plan de continuidad del negocio y análisis de impacto		X	0
Existe un diseño, redacción e implantación de planes de continuidad		X	0
Existe un marco de planificación para la continuidad del negocio		X	0
Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio		X	0
		Suma:	0
		Porcentaje:	0%

Fuente elaboración propia

Recomendación 10

Como tenemos el 0% en la suma del cuestionario, esto quiere decir que existen falencias en los procesos de la planificación para la gestión de la continuidad del negocio, así como también se recomienda diseñar e implantar planes de continuidad.

Check-List para el Cumplimiento:

Tabla 18 **Para el cumplimiento**

Empresa:	GAD Municipal del Cantón Milagro		
Cuestionario de Cumplimiento	C11		
Dominio	Cumplimiento		
Proceso	Gestión de la Seguridad de la Información		
Objetivo de Control	Revisión de Políticas Seguridad		
Cuestionario			
Pregunta	**VERDADERO**	**FALSO**	**PONDERACIÓN**
Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas		X	0
Existe el resguardo de la propiedad intelectual		X	0
Existe el resguardo de los registros de la organización		X	0
Existe una revisión de la política de seguridad y de la conformidad técnica		X	0
Existen consideraciones sobre las auditorías de los sistemas		X	0
		Suma:	0
		Porcentaje:	0%

Fuente elaboración propia

Recomendación 11

Se recomienda que se lleve un control, referente a las políticas del municipio y tener las consideraciones de las auditorias que se han llevado a cabo hasta el momento.

4.4. RESULTADOS ESPERADOS

- **Planes de acción**

  Entre los resultados esperados de la propuesta podemos citar de los aspectos positivos de la implementación del SGSI:

  - Mejora de la Protección de datos de información del GAD Municipal.

Si se alcanza este indicador se evitará interrupciones en el traspaso de información, se asegura la disponibilidad y confiabilidad de los datos y del sistema de información entre departamentos del GAD Municipal.

- Mejora de la competitividad

Si se implementa el sistema de Gestión de Seguridad de Información se incrementa la seguridad e información por lo cual la información estará respaldada para uso exclusivo de información lo que mejoraría las gestiones y actividades departamentales al servicio de la comunidad Milagreña.

- Cumplimiento legal tanto de la norma nacionales e internacionales

A medida que trascurre el tiempo han sido numerosas las leyes y reglamentaciones en materia de seguridad de información por lo cual si se logra la implementación se estará cumpliendo con las normativas de seguridad de información nacionales e internacionales.

- Mantener y mejorar la imagen Corporativa del GAD Municipal

La comunidad Milagreña percibirá las actividades del GAD Municipal como un ente público serio, responsable y comprometida en la mejora de los procesos producto y servicios.

4.5. PLANEACIÓN DE LA PROPUESTA

PLAN DE AUDITORÍA

Objeto de la auditoría

Identificar el nivel de cumplimiento del sistema de la seguridad de la información (SGSI) del GAD municipal de Milagro con respecto a los controles y procedimientos de la norma internacional ISO 27001 versión 2013.

Alcance de la auditoria

El alcance previo del plan de un Sistema de Gestión de Seguridad Informática es aplicable a todos los funcionarios que trabajan en el GAD Municipal de Milagro, además a los diferentes tipos de información, independientemente del formato,

ya sean documentos en papel o electrónicos, aplicaciones y bases de datos, conocimiento de las personas, con la finalidad de garantizar que se proteja la información en un nivel adecuado para el Municipio de la Ciudad de Milagro.

Fecha de la auditoría

Las actividades de auditoria fueron ejecutadas desde el mes de Mayo hasta Agosto del 2017.

Lugar

La auditoría al SGSI fue realizada en las oficinas del GAD municipal de Milagro incluyendo visitas a los centros de cómputo principal y de contingencia.

Áreas auditadas

Se auditaron todas las áreas del GAD municipal de Milagro que están relacionadas con el alcance del SGSI, es decir:

- Administración y Financiera
- Tecnología
- Recursos humanos

Equipo auditor

La auditoría fue ejecutada por los auditores: Paguay Lema Cinthya Katherine, Zamora Arana Gabriel Eduardo.

Personal auditado

Se auditó al siguiente personal del GAD municipal de Milagro

- Gerente General
- Director Administrativo y Financiero
- Director de Recursos Humanos
- Director de Tecnología
- Coordinador de Recursos Humanos
- Coordinador de sistemas

Recopilación de requisitos

- **Definición de las políticas basado en los resultados**

  Para el análisis previo mediante preguntas basadas con Check list del sistema de Gestión de Seguridad de la Información se debe contar con los siguientes requisitos:

  1. Valoración del MODELO PHVA
  2. Establecer el Alcance y las políticas de seguridad de la Información
  3. Constar con un análisis de Riesgo de información
  4. Personal Comprometido
  5. Recursos Económicos para la sociabilización e implementación del Sistema de Seguridad de la Información.
  6. Dirección IP Privadas.

Gestión del tiempo

- Definir las actividades
- Estimar los recursos humanos, técnicos, financieros, materiales por actividad.
- Estimar la duración de las actividades

Entrevista

Se entrevistó a tres personas que laboran en el GAD municipal de Milagro, pero la información recabada no se puede divulgar o dar a conocer a personas que no pertenecen a la entidad, por el cual no podemos ubicar las pertinentes evidencias en este documento.

CAPÍTULO V: ANÁLISIS TÉCNICO ECONÓMICO DE LA PROPUESTA AUDITORIA

Análisis de costos detallado

Para la implementación de la Norma ISO 27001 se utilizó el siguiente recurso material

Recurso Material

- Computadora
- Resmas de Papel
- Norma ISO 27001

Gestión de los recursos humanos

En cuanto a la aplicación se utilizara el personal del GAD Municipal del Cantón Milagro más los autores del presente proyecto.

- Cinthya Paguay
- Gabriel Zamora

Análisis financiero: Retorno de la inversión, VAN, TIR

Tabla 19 **Recursos humanos**

Recursos humanos	**Mes 1**	**Mes 2**	**Mes 3**	**Mes 4**	**Mes 5**	**Mes 6**	**Total**
	Número de Horas	Valor por hora					
Auditor 1	160	5					
Auditor 2	160	5					
Pago mensual Aud. 1	800	800	800	800	800	800	4800
Pago mensual Aud. 2	800	800	800	800	800	800	4800
Total							**9600**

Fuente elaboración propia

Tabla 20 **Recursos financieros**

Recursos financieros	**Mes 1**	**Mes 2**	**Mes 3**	**Mes 4**	**Mes 5**	**Mes 6**	**Total**
2 laptop	0	0	0	0	0	0	2400
Internet	30	30	30	30	30	30	3600
Gastos de transporte y viáticos	80	80	80	100	120	150	1220
Libro de ISO	100	0	0	0	0	0	100
Total							**4080**

Fuente elaboración propia

Tabla 21 **Gestión administrativos**

Gastos administrativos	**Mes 1**	**Mes 2**	**Mes 3**	**Mes 4**	**Mes 5**	**Mes 6**	**Total**
Materiales de oficina y Suministros (Impresiones, Hojas y cartuchos)	5	5	5	15	20	70	120
Total							**120**

Fuente elaboración propia

Tabla 22 **Total de inversión**

Total de inversión	Monto
Recursos humanos	9600
Recursos financieros	4080
Gastos administrativos	120
Total	13800

Fuente elaboración propia

Tabla 23 **Datos para el VAN y TIR**

Año	0	1	2	3	4	5
Inversión final	-13800	7000	7000	7500	7500	7500
VAN	7865,70					
INTERES	20%					
TIR	44%					

Fuente elaboración propia

Tabla 24 **Calculo del VAN y TIR**

TIR	VAN
0%	$ 22.700,00
5%	$ 17.741,37
10%	$ 13.763,13
15%	$ 10.528,31
20%	$ 7.865,70
25%	$ 5.649,60
30%	$ 3.786,30
35%	$ 2.204,99
40%	$ 851,48
45%	($ 316,18)
50%	($ 1.330,86)
55%	($ 2.218,53)
60%	($ 2.999,91)
65%	($ 3.691,69)
70%	($ 4.307,45)
75%	($ 4.858,25)
80%	($ 5.353,24)
85%	($ 5.800,01)
90%	($ 6.204,88)
95%	($ 6.573,17)
100%	($ 6.909,38)

Fuente elaboración propia

Aquí estamos calculando la tasa interna de rentabilidad de la inversión que está definida como la tasa de interés con la cual el valor neto es igual a cero, esto quiere decir el costo en llevar a cabo este plan de auditoria.

CONCLUSIONES

- Al analizar la situación actual de la entidad se recomendó tomar medidas de seguridad para la protección de la información que gestiona el GAD Municipal de Milagro.

- Al determinar el nivel de madurez que tiene el GAD Municipal de Milagro en su modelo de seguridad de información, se recomendó tomar las siguientes medidas de seguridad y control: implantar planes de continuidad, no permitir dispositivos de almacenamiento al personal que manipula información del GAD municipal de Milagro.

- Al definir los controles y procedimientos que contiene la norma ISO 27001:2013, que está dirigida a la seguridad, esto quiere decir que la información que manipula el GAD municipal de Milagro será segura.

RECOMENDACIONES

- Seguir los planes de acciones recomendado como lo describe la norma ISO 27001
- Llevar a cabo las políticas y procedimientos de la norma ISO 27001
- Realizar un seguimiento y control en donde se puso en marcha los controles y procedimientos, para identificar si estos nos están ayudando a mejorar.
- Realizar un análisis después de 6 meses de haber puesto en marcha los controles y procedimientos, para verificar si se han cerrado las brechas de inseguridades.

ANEXOS

Tabla 25 **Proceso Cobit**

Proceso COBIT Versión 4.1	**Incluido en la Norma NTE INEN-ISO/IEC 27001:2009 (si/no/parcialmente)**	**Objetivos de control de COBIT no considerados en la norma NTE INEN-ISO/IEC 27001:2009**
PO 1 Definir un plan estratégico de TI	No	PO1.1 Administración del Valor de TI PO1.2 Alineación de TI con el Negocio PO1.3 Evaluación del Desempeño y la Capacidad Actual PO1.4 Plan Estratégico de TI PO1.5 Planes Tácticos de TI PO1.6 Administración del Portafolio de TI
PO2 Definir la arquitectura de información	Parcialmente	PO2.1 Modelo de Arquitectura de Información Empresarial PO2.4 Administración de Integridad
PO3 Determinar la orientación tecnológica	Parcialmente	PO3.2 Plan de Infraestructura Tecnológica
PO4 Definir los procesos, organización y relaciones de TI	Parcialmente	PO4.1 Marco de Trabajo de Procesos de TI PO4.2 Comité Estratégico de TI PO4.7 Responsabilidad de Aseguramiento de Calidad de TI PO4.12 Personal del TI PO4.13 Personal Clave de TI
PO5 Gestionar la inversión en TI	Parcialmente	PO5.1 Marco de Trabajo para la Administración Financiera

		PO5.2 Prioridades Dentro del Presupuesto de TI PO5.5 Administración de Beneficios
PO6 Comunicar las aspiraciones y la dirección de la gerencia	Si	
PO7 Gestión de los recursos humanos de TI	Parcialmente	PO7.5 Dependencia Sobre los Individuos
PO8 Gestión de la Calidad	Parcialmente	PO8.1 Sistema de Administración de Calidad PO8.2 Estándares y Prácticas de calidad PO8.4Enfoque en el Cliente de TI PO8.5 Mejora Continua PO8.6 Medición, Monitoreo y Revisión de la Calidad
Proceso COBIT Versión 4.1	**Incluido en la Norma NTE INEN-ISO/IEC 27001:2009 (si/no/parcialmente)**	**Objetivos de control de COBIT no considerados en la norma NTE INEN-ISO/IEC 27001:2009**
PO9 Evaluar y gestionar los riesgos de TI	Parcialmente	PO9.5 Respuesta a los Riesgos PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgo
PO10 Gestionar proyectos	No	PO10.1 Marco de Trabajo para la Administración de Programas PO10.2 Marco de Trabajo para la Administración de Proyectos PO10.3 Enfoque de Administración de Proyectos PO10.4 Compromiso de los Interesados PO10.5 Declaración de Alcance del Proyecto

		PO10.6 Inicio de las Fases del Proyecto PO10.7 Plan Integrado del Proyecto PO10.8 Recursos del Proyecto PO10.9 Administración de Riesgos del Proyecto PO10.10 Plan de Calidad del Proyecto PO10.11 Control de Cambios del Proyecto PO10.12 Planeación del Proyecto y Métodos de Aseguramiento PO10.13 Medición del Desempleo, Reporte y Monitoreo del Proyecto PO10.14 Cierre del Proyecto
AI1 Identificar soluciones automatizadas	Parcialmente	AI1.13 Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos
AI2 Adquirir y mantener software aplicativo	Parcialmente	AI2.1 Diseño de Alto Nivel AI2.2 Diseño Detallado AI2.9 Administración de los Requerimientos de Aplicativos AI2.10 Mantenimiento de Software Aplicativo
AI3 Adquirir y mantener la infraestructura tecnológica	Parcialmente	AI3.1 Plan de Adquisición de Infraestructura Tecnológica
Proceso COBIT Versión 4.1	**Incluido en la Norma NTE INEN-ISO/IEC 27001:2009 (si/no/parcialmente)**	**Objetivos de control de COBIT no considerados en la norma NTE INEN-ISO/IEC 27001:2009**
AI4 Facilitar la operación y el uso	Parcialmente	AI4.1 Plan de Soluciones de Operación

		AI4.2 Transferencia de Conocimiento a la Gerencia del Negocio AI4.3 Transferencia de Conocimiento a Usuarios Finales
AI5 Adquirir recursos de TI	Parcialmente	AI5.3 Selección de Proveedores AI5.4 Adquisición de Recursos de TI
AI6 Gestionar cambios	Si	
AI7 Instalar y acreditar soluciones y cambios	Parcialmente	AI7.3 Plan de Implantación AL7.5 Conversión de Sistemas y Datos AI7.8 Promoción a Producción AI7.9 Revisión Posterior a la Implantación
DS1 Definir y gestionar los niveles de servicio	Parcialmente	DS1.4 Acuerdos de Niveles de Operación DS1.6 Revisión de los Acuerdos de Niveles de Servicio y de los Contratos
DS2 Gestionar los niveles de servicios	Si	
DS3 Gestionar el desempeño y la capacidad	Parcialmente	DS3.4 Disponibilidad de Recursos de TI DS3.5 Monitoreo y Reporte
DS4 Garantizar la continuidad de servicio	Si	
DS5 Garantizar la seguridad de los sistemas	Si	
DS6 Identificar y asignar costos	No	DS6.1 Definición de Servicios DS6.2 Contabilización del TI DS6.3 Modelación de Costos y Cargos DS6.4Mantenimiento del Modelo de Costos
DS7 Educar y entrenar a los usuarios	Parcialmente	DS7.3 Evaluación del Entrenamiento Recibido

DS8 Gestionar la mesa de servicios y los incidentes	Si	
DS9 Gestionar la configuración	Si	

Tabla 26 **Proceso COBIT versión 4.1**

Proceso COBIT Versión 4.1	**Incluido en la Norma NTE INEN-ISO/IEC 27001:2009 (si/no/parcialmente)**	**Objetivos de control de COBIT no considerados en la norma NTE INEN-ISO/IEC 27001:2009**
DS10 Gestionar problemas	Parcialmente	DS10.3 Cierre de Problemas DS10.4 Integración de las Administraciones de Cambios, Configuración y Problemas
DS11 Gestionar datos	Si	
DS12 Gestionar el ambiente físico	Si	
DS13 Gestionar las operaciones	Parcialmente	DS13.2 Programación de tareas DS13.3 Monitoreo de la Infraestructura de TI DS13.4 Documentos Sensitivos y Dispositivos de Salida
ME1 Monitorear y evaluar el desempeño de TI	Parcialmente	ME1.1Enfoque del Monitoreo ME1.3 Método del Monitoreo ME1.4 Evaluación del Desempeño ME1.5Reportes al Consejo Directivo y a Ejecutivos ME1.6Acciones Correctivas
ME2 Monitorear y evaluar el control interno	Si	

ME3 Garantizar el cumplimiento de requisitos externos	Parcialmente	ME3.2 Optimizar la Respuesta a Requerimientos Externos ME3.5Reportes Integrados
ME4 Proporcionar gobierno de TI	Parcialmente	ME4.1Establecimiento de un Marco de Gobierno de TI ME4.2Alineamiento Estratégico ME4.3Entrega de Valor ME4.4Administracion de Recursos ME4.5Administracion de Riesgos ME4.6 Medición del Desempeño

REFERENCIAS BIBLIOGRÁFICAS

[1] R. N. Guagalango Vega y P. E. Moscoso Montalvo, «Evaluación técnica de la seguridad informática del Data Center de la Escuela Politécnica del Ejército,» SANGOLQUI / ESPE / 2011, SANGOLQUI, 2011.

[2] V. C. S. Fernando, «Gestión de riesgos informáticos en la empresa FIDEVAL utilizando ISO 27001,» Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería de Sistemas e Informática., SANGOLQUI, 2015.

[3] V. C. R. Patricio, «Artículo Científico - Evaluación de seguridad de la información al proceso de admisión de estudiantes de la UTE basada en ISO /IEC 27000.,» Universidad de las Fuerzas Armadas ESPE. Maestría en Evaluación y Auditoría en Sistemas Tecnológicos., SANGOLQUI, 2014.

[4] R. F. Morales Aréval, «Diseño para la implementación de tres dominios de un sistema de gestión en la seguridad de la información basada en la norma ISO 27001 e ISO 27002, para el área de software de la procesadora nacional de alimentos Pronaca,» Universidad de las Fuerzas Armadas ESPE. Maestría en Gerencia de Redes y Telecomunicaciones., SANGOLQUI, 2015.

[5] R. J. C. Danie y M. Z. R. Mauriciol, «Diseño para la implementación de los dominios de cifrado y seguridad física y ambiental basados en la norma ISO27001 e ISO27002, para el área de TI de la procesadora nacional de alimentos “PRONACA”,» Universidad de las Fuerzas Armadas ESPE. Maestría en Gerencia de Sistemas., SANGOLQUI, 2017.

[6] A. F. D. Santiago y P. C. J. Carlos, «Evaluación técnica de seguridades del data center del Municipio de Quito según las NORMAS ISO/IEC 27001:2005 SGSIE ISO/IEC 27002:2005,» Universidad de las Fuerzas Armadas ESPE. Maestría en Evaluación y Auditoría de Sistemas Tecnológicos, SANGOLQUI, 2014.

[7] «Organización Internacional para la Estandarización (ISO),» [En línea]. Available: http://www.bajacalifornia.gob.mx/registrocivilbc/iso_informa2.htm.

[8] «Norma ISO 27001,» [En línea]. Available: http://www.iso27000.es/iso27000.html.

[9] «Sistema de Gestión de la Seguridad de la Información,» [En línea]. Available: http://www.iso27000.es/download/doc_sgsi_all.pdf.

[10] E. D. Godas, La seguridad de la información digital, Publicaciones Fomento.

[11] A. Á. G. J. M. P. P. M. L. C. Mazariegos Sánchez, «EL CONTROL INTERNO DE UNA ORGANIZACIÓN PRODUCTORA DE CAFÉ CERTIFICADO, EN CHIAPAS, MÉXICO,» *Revista Mexicana de Agronegocios,* vol. XVII, p. 463, 2013.

[12] H. Steffens, «¿Qué son los Gusanos informáticos?,» [En línea]. Available: http://liacolombia.com/2009/12/%C2%BFque-son-los-gusanos-informaticos/.

[13] C. H. T. T., «AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN».