VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

MAESTRÍA EN GERENCIA DE SISTEMAS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN GERENCIA DE SISTEMAS

TEMA: EVALUACIÓN TÉCNICA INFORMÁTICA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL GAD PROVINCIAL DE IMBABURA EN BASE DE LA NORMA ISO/IEC 27001:2013

AUTORA: VILLEGAS LIMAICO, JENNY ALEXANDRA

DIRECTOR: RON EGAS, MARIO BERNABE

SANGOLQUÍ

2019

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y

TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "***EVALUACIÓN TÉCNICA INFORMÁTICA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL GAD PROVINCIAL DE IMBABURA EN BASE DE LA NORMA ISO/IEC 27001:2013***", fue realizado por la señorita ***Villegas Limaico, Jenny Alexandra*** el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 23 de agosto de 2019

Firma:

Ron Egas, Mario Bernabe
C.C.: 1704229747

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y

TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORÍA DE RESPONSABILIDAD

Yo, ***Villegas Limaico, Jenny Alexandra***, con cédula de ciudadanía n° **1002850715**, declaro que el contenido, ideas y criterios del trabajo de titulación: ***Evaluación Técnica Informática al Sistema de Gestión de Seguridad de la Información del GAD Provincial de Imbabura en base de la Norma ISO/IEC 27001:2013***, es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 23 de agosto de 2019

Firma:

Villegas Limaico, Jenny Alexandra
C.C.: 1002850715

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN

Yo, ***Villegas Limaico, Jenny Alexandra*** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: ***Evaluación Técnica Informática al Sistema de Gestión de Seguridad de la Información del GAD Provincial de Imbabura en base de la Norma ISO/IEC 27001:2013*** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 23 de agosto de 2019

Firma:

Villegas Limaico, Jenny Alexandra
C.C.: 1002850715

DEDICATORIA

Este trabajo lo dedico a:

Dios por bendecirme durante todo mi camino y darme fuerzas para culminar esta etapa de mi vida,

Mi madre Marthy, por ser mi apoyo en todo momento y celebrar mis triunfos,

Mis herman@s Silvia, Edwin y Ligia por su ejemplo de superación, colaboración y consejos para afrontar los retos que se me han presentado,

Mis sobrin@s Luis Eduardo, Santiago Vladimir, Sofía Alejandra y Belén Estefanía, porque con sus sonrisas me hacen crecer y sentirme muy afortunada de tenerlos conmigo,

Mi padre Eladio que desde el cielo me brinda luz y fuerza para seguir adelante, demostrarle que puede sentirse orgulloso de su última hija.

Jenny Alexandra Villegas L.

AGRADECIMIENTO

"Lo único que se interpone entre ti y tu sueño, es la voluntad de intentarlo y la creencia de que en realidad es posible"

Joel Brown

Mis más sinceros agradecimientos a la Universidad de las Fuerzas Armadas ESPE, por brindarnos la posibilidad de adquirir nuevos conocimientos.

Al personal docente que compartieron sus sabios conocimientos en el aula, en especial al Mgs. Mario Ron por su amable ayuda, apoyo y su valiosa colaboración como director de tesis; al Mgs. Fidel Castro y Mgs. Geovanni Ninahualpa por su apoyo incondicional para culminar el presente trabajo.

A toda la DGTI del GAD provincial de Imbabura por todo su apoyo apertura y colaboración, para realizar el presente trabajo en sus dependencias, en especial al Ing. Jaime Chuga por su colaboración técnica y apoyo incondicional.

A todos mis amig@s porque sin sus bromas y locuras no hubiera sido lo mismo cada día de clases.

Jenny Alexandra Villegas L.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

NOMENCLATURA UTILIZADA

- **EGSI:** Esquema Gubernamental de Seguridad de la Información
- **GAD:** Gobierno Autónomo Descentralizado
- **IEC:** Comisión Electrotécnica Internacional
- **ISO:** Organización Internacional de Normalización
- **SGSI:** Sistema de Gestión de Seguridad de la Información
- **CAAT:** Técnicas de Auditoría asistidas por Computadora
- **CEO:** Chief Executive Officer
- **CIO**: Chief Information Officer
- **CMMI**: Capacity and Maturity Model Integration
- **IEC**: International Electrotechnical Commission
- **INEN:** Instituto Ecuatoriano de Normalización
- **ISO**: International Organization for Standardization
- **NTE:** Norma Técnica Ecuatoriana
- **PDCA:** Plan, Do, Check, Act
- **PHVA:** Planificar, hacer, verificar y actuar
- **APMG:** APM Group, es el instituto de acreditación y examen global de mayor reputación Internacional.
- **ITAF:** Information Technology Assurance Framework, Marco de Garantía de la Tecnología de la Información.

- **ISACA:** Information Systems Audit and Control Association, Asociación de Auditoría y Control de Sistemas de Información.

RESUMEN

El uso del Internet se ha vuelto indispensable en el ámbito educativo, económico y administrativo, tanto en el sector público como privado. Pero así mismo el uso de la tecnología conlleva un mayor riesgo inherente, que conduce a la necesidad de implantar un Sistema de Gestión de la Seguridad de la Información SGSI, conforme a normas internacionalmente aceptadas, que eventualmente deben ser evaluado mediante un proceso técnico de auditoría. Por disposición administrativa emitida para las entidades públicas, el Gobierno Autónomo Descentralizado (GAD) provincial de Imbabura, debe cumplir con la implantación del SGSI, en base de la norma ISO/IEC 27001:2013, en consecuencia es necesario establecer una línea de base mediante una "Evaluación Técnica Informática (ETI)", al SGSI, para elaborar un plan de trabajo eficaz y eficiente que permita certificar en el futuro el cumplimiento de la disposición administrativa y más aún asegurar sus activos de información para brindar a la ciudadanía servicios adecuados. Para conseguir los resultados esperados la ETI, se fundamenta en metodologías, estándares y buenas prácticas publicados por Instituciones de reconocida solvencia como ISACA, APMG, ISO, IEC, INEN. En este caso en forma particular la norma ISO-IEC-NTE-27001-2013. Como resultado de este trabajo se presenta un informe con las observaciones pertinentes y las recomendaciones que deberán ser aplicadas para que el GAD se encuentre preparado para una auditoría de certificación.

PALABRAS CLAVE:

- **EVALUACIÓN TÉCNICA INFORMÁTICA**
- **NORMA ISO 27001**
- **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**

ABSTRACT

The use of the Internet has become indispensable in the educational, economic and administrative spheres, both in the public and private sectors. But likewise, the use of technology entails a greater inherent risk, which leads to the need to implement an Information Security Management System, in accordance with internationally accepted standards, which eventually must be evaluated through a technical audit process by administrative disposition issued for public entities, the Autonomous Decentralized Government (GAD) of Imbabura must comply with the implementation of the Government Information Security Scheme (SGSI), based on the ISO / IEC 27001: 2013 standard, as a consequence must establish a baseline through a "Informatic Technical Assessment (ETI)", the EGSI, to develop an effective and efficient work plan to certify in the future compliance with the administrative provision and even more secure their information assets to provide to the citizenship adequate services. In order to achieve the expected results, the ETI is based on methodologies, standards and good practices published by Institutions of recognized solvency such as ISACA, APMG, ISO, IEC, INEN. In this case, in particular, the ISO-IEC-NTE-27001-2013 standard. As a result of this work, a report is presented with the pertinent observations and the recommendations that must be applied so that the GAD will be prepared for a certification audit.

KEY WORDS:

- **COMPUTER TECHNICAL EVALUATION**
- **ISO 27001 STANDARD**
- **INFORMATION SECURITY MANAGEMENT SYSTEM**

CAPITULO I

INTRODUCCIÓN

1.1 Antecedentes

Figura 1. Logotipo
Fuente: http://www.imbabura.gob.ec/

Conforme se establece en el Plan Estratégico Institucional del Gobierno Autónomo Descentralizado Provincial de Imbabura (GADI), para el período 2014-2019, su rol fundamental radica en la promoción del desarrollo sustentable del territorio provincial para el buen vivir, a través de la implementación de políticas públicas provinciales; elabora y ejecuta el Plan Provincial de Desarrollo y de Ordenamiento Territorial de manera coordinada con la planificación nacional, regional, cantonal y parroquial para el fomento de las actividades provinciales productivas; el desarrollo de la vialidad rural; la gestión ambiental, de riego y desarrollo agropecuario. (Prefectura de Imbabura, 2017).

En el año 2015, el GAD provincial de Imbabura auspició el trabajo de titulación "Hacking Ético para detectar fallas en la Seguridad Informática de la Intranet del Gobierno Provincial de Imbabura e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la Norma ISO/IEC 27001:2005"; que sirve como referencia para el presente proyecto.

1.2 Problema

El GAD provincial de Imbabura, cuenta con un sistema de información destinado a brindar servicios a los ciudadanos de la provincia y realizar una gestión eficaz y eficiente. Es una institución pública que contribuye al desarrollo de la provincia y tiene influencia en cada uno de los GAD Parroquiales, sin embargo, no tiene procesos racionalizados, lo que provoca deficiencias en sus sistemas, por fallas en la disponibilidad, integridad y confidencialidad de la información, degradando así la calidad de los servicios.

1.3 Objetivo

1.3.1. Objetivo General

Realizar una evaluación técnica informática al Sistema de Gestión de Seguridad de la Información del GAD Provincial de Imbabura, mediante procedimientos de auditoría de certificación generalmente aceptados, para validar el cumplimiento de la norma ISO/IEC 27001:2013.

1.3.2. Objetivos específicos

- Realizar una revisión sistemática de literatura de las normas e información relacionada.
- Realizar una evaluación técnica Informática de cumplimiento de la norma ISO/IEC 27001:2013
- Elaborar un informe con las evidencias pertinentes y recomendaciones para que se arbitren las medidas necesarias para la mejora y certificación del SGSI.

1.4 Justificación, importancia y alcance del proyecto

La razón de ser de un SGSI es conseguir seguridad, confidencialidad, disponibilidad de la información que se adquiere, almacena, procesa y distribuye, minimizando los riesgos inherentes y residuales que podrían afectar a la institución, su labor de servicio público, su imagen y relaciones con los usuarios, así como la presencia política de quienes ejercen autoridad en ella, más todavía si la administración ha pretendido ingresar en tendencias modernas como e-government, mejora de servicios a la ciudadanía con eficiencia y eficacia en sus operaciones.

Es importante mantener la confianza de funcionarios y ciudadanos, en el uso y aplicación de sistemas de información que permitan ahorrar tiempo y recursos en los trámites burocráticos, mediante un servicio permanente que tenga resiliencia y seguridad ante las amenazas que actualmente aquejan al uso de la tecnología de la Información.

El servicio público y los entes de control se encuentran preocupados por asegurar el ciberespacio, es por ésta razón que se emite el acuerdo SNAP 166, en el que se dispone el diseño e implantación del Esquema de Gestión de la Seguridad de la Información (EGSI) en todas las instituciones públicas, entre ellas los GAD provinciales; en consecuencia, deberá establecerse una línea de base inicial desde la que pueda proyectarse las acciones pertinentes para su correcta implantación, mediante la ejecución de un proyecto de mejoramiento y una posterior evaluación para finalmente realizar una auditoría de certificación por parte de un organismo independiente, autorizado para tal efecto.

1.5 Nivel, tipo y enfoque de investigación

La investigación que se desarrolla es de nivel Explicativo porque la relación entre las variables es una relación de causa efecto, siendo que la variable independiente: controles de seguridad física y lógica de la ISO/IEC 27002:2013 tiene un efecto sobre la variable dependiente Niveles de Seguridad de la información.

La investigación es de tipo aplicada considerando que consiste en un estudio exhaustivo de la problemática del área de TI y de las posibles soluciones para obtener resultados satisfactorios en el área de TI, que a su vez permitirá mejorar el nivel de seguridad física y lógica de la información.

El enfoque de la investigación es cualitativo porque permite conocer la problemática, los procesos de la organización, el nivel de seguridad del GADI y realizar el planteamiento del problema de manera estructurada.

1.6 Población y recolección de información

Para el presente proyecto de investigación se ha definido como población, al personal del área de TI y los usuarios de los sistemas de información del GAD; la recolección de la información se realizará mediante check list, observación directa, análisis documental, entrevistas, pruebas sustantivas y otras técnicas de auditoría.

1.7 Metodología

Para la ejecución de este proyecto se pretende utilizar la norma ISO-IEC 19000 y que constituye la base del curso de certificación de Auditor Líder de la ISO 27001 por parte de la APMG, se utiliza además buenas prácticas publicadas por los documentos de ITAF de ISACA.

Los instrumentos de investigación de campo y los papeles de trabajo son elaborados de acuerdo a las buenas prácticas de las publicaciones de ISACA y documentos relacionados.

CAPÍTULO II

MARCO TEÓRICO Y ESTADO DEL ARTE

2.1. Marco teórico

En este apartado se presentan los elementos teóricos que fundamentan el estudio que se desarrollará más adelante y comprende las ciencias aplicadas relativas al mismo, los organismos que se encuentran relacionados, las normas que se utilizan como herramientas, el estado del arte y los conceptos inherentes al tema.

2.2. Ciencias Aplicadas relativas al estudio

2.2.1. Análisis de Riesgos

Es un elemento fundamental para determinar las medidas de seguridad que deben ser adoptadas en un activo de información o sistema, identifica los riesgos y estima el impacto potencial que supone la destrucción o pérdida, además de la afectación a la seguridad (disponibilidad, integridad, confidencialidad y no repudio) de la información.

El análisis de riesgos en la organización permite relacionar el costo-beneficio de la implantación de controles, asegura la continuidad operacional de la empresa y permite la mejora continua de la seguridad informática.

El análisis de riesgos pueden ser cualitativo y/o cuantitativo; el cuantitativo es el más utilizado y permite asignar valores de ocurrencia en los riesgos identificados; el cualitativo permite hacer una apreciación referenciada respecto de una buena práctica.

Existen metodologías que cumplen con los criterios mínimos que exige la norma ISO 27001:

- Operationally Critical Threat and Vulnerability Evaluation (OCTAVE): permite desarrollar y aplicar una estrategia de reducción de riesgos en tres fases: perfil de las necesidades en materia de seguridad con respecto a la empresa (disponibilidad, integridad y confidencialidad), estudio de la vulnerabilidad en el desarrollo de la estrategia y plan de seguridad (INCIBE - Instituto Nacional de Ciberseguridad, 2019).
- CCTA Risk Analysis and Method Management (CRAMM): fue creado en 1987 por la Agencia Central de Procesamiento de Datos y Telecomunicaciones del Gobierno del Reino Unido; se realiza en tres fases: definición de valores amenazados, análisis de riesgos y vulnerabilidades, finalmente definición y selección de medidas de seguridad (INCIBE - Instituto Nacional de Ciberseguridad, 2019).
- Methode Harmonisée d'Analyse de Risques (MEHARI): El Método armonizado de análisis de riesgos, fue desarrollada en 1995 por el Club de Seguridad de la Información Francés (CLUSIF), se deriva de los métodos Melissa y Marion. El enfoque general del MEHARI consiste en el análisis de los retos de seguridad y en la clasificación preliminar de las entidades de la Seguridad de la Información en función de tres criterios básicos de seguridad conocidos como la confidencialidad, integridad y disponibilidad. Los retos expresan las disfunciones que tienen un impacto directo sobre la actividad de la empresa. Las auditorías identifican las vulnerabilidades de Seguridad de la Información y el análisis de

riesgo se realiza posteriormente (INCIBE - Instituto Nacional de Ciberseguridad, 2019).

Las fases de un análisis de riesgo de manera general cumplen las etapas presentadas en la Figura 2:

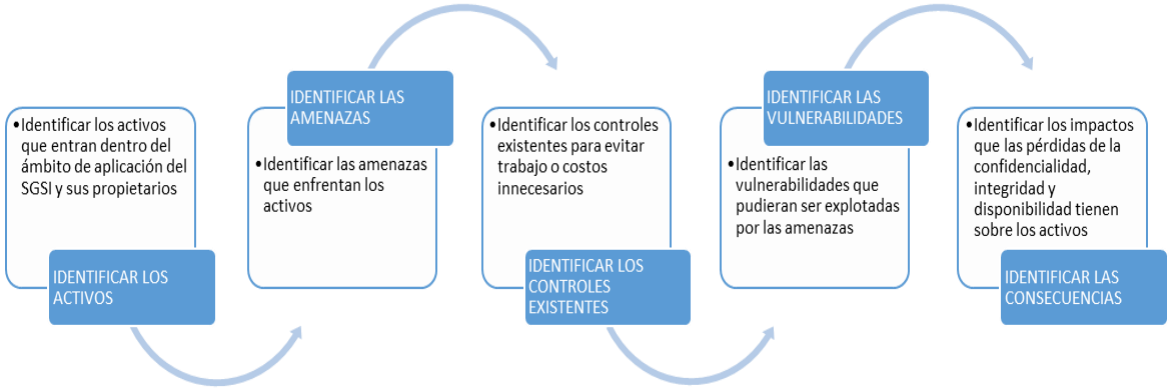

Figura 2. Fases análisis de riesgos
Fuente: Norma ISO/IEC 27001 cláusula 6

En la **Figura 2** se indica las fases del análisis y evaluación de los riesgos dentro de la norma ISO 27001 (Servicio Ecuatoriano de Normalización, 2013) e ISO 27005 (Organización Internacional de Estandarización, 2018):

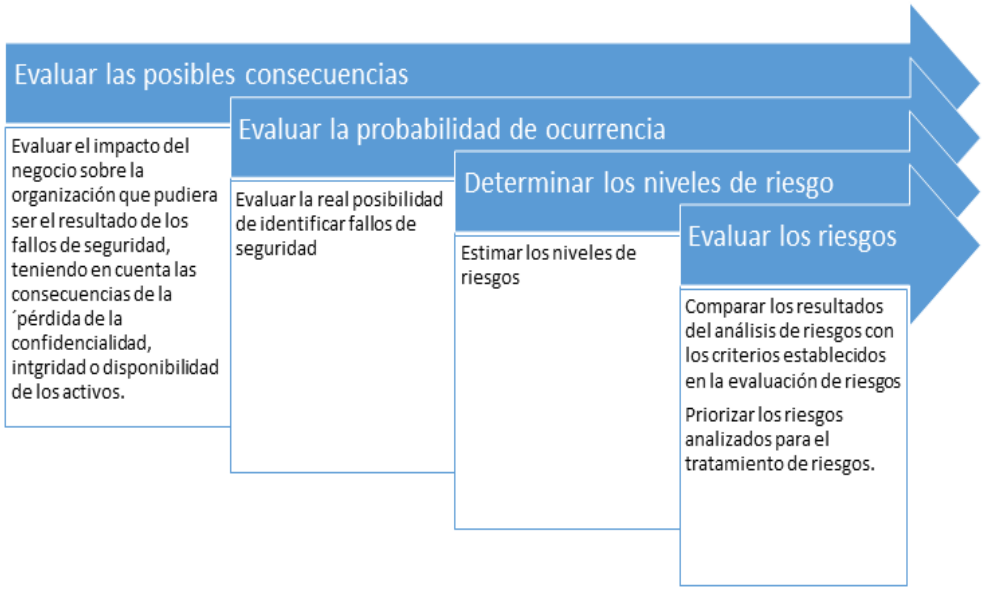

Figura 3. Pasos de desarrollo de análisis de riesgos
Fuente: Norma ISO/IEC 27001 cláusula 6.1.2 d-e

El método de evaluación de riesgos debe permitir la gestión de riesgos de acuerdo las fases de la **Figura 4** (Organización Internacional de Estandarización, 2018):

Figura 4. Opciones de tratamiento del Riesgo
Fuente: Norma ISO/IEC 27001 cláusula 6

- **Reducción:** Selección de controles para reducir el riesgo
- **Retención:** La Dirección decide tomar el riesgo
- **Transferencia:** Decisión de compartir riesgos con las partes externas: seguros y tercerización
- **Evitar riesgos:** Cancelación o modificación de una actividad o conjunto de actividades relacionadas con riesgos.

En la selección de controles, la organización que tiene como objetivo su seguridad, debe tener en cuenta los criterios de aceptación del riesgo que se han definido en la organización, así como los requisitos legales, regulatorios y contractuales.

La declaración de la aplicabilidad debe estar documentada con los controles necesarios, las justificaciones de las inclusiones, si son aplicadas o no y la justificación de las exclusiones de los controles del Anexo A de la ISO 27001 (Servicio Ecuatoriano de Normalización, 2013).

El plan de tratamiento de riesgos de seguridad de la información tiene como finalidad documentar la manera en que se implantaran las opciones de tratamiento elegidas, como mínimo debe incluir las razones que justifican la selección de las opciones de tratamiento, incluyendo los beneficios previstos, las personas responsables, las acciones propuestas, los recursos necesarios, las restricciones, los requisitos en materia de información y un cronograma de trabajo. El riesgo residual es aquel que queda después de la aplicación de los controles con el objetivo de reducir el riesgo inherente, y puede resumirse en la fórmula de la **Figura 5** (Organización Internacional de Estandarización, 2018):

***Riesgo residual*= riesgo inherente - riesgo tratado por controles**

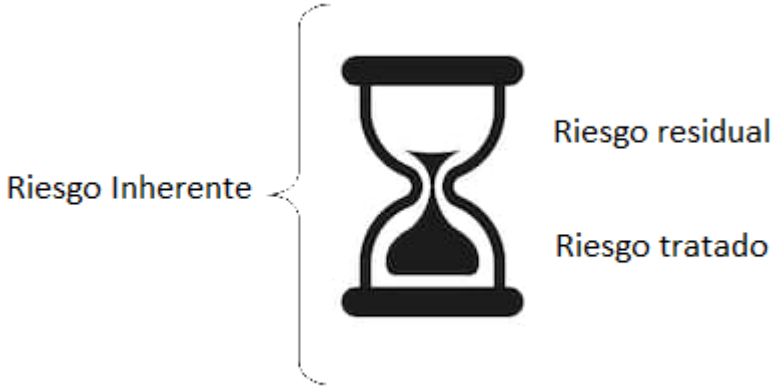

Figura 5. Riesgo Residual
Fuente: Norma ISO/IEC 27005

- **Riesgo inherente:** todos los riesgos sin tener en cuenta controles.
- **Riesgo residual:** riesgos restantes tras el tratamiento del riesgo.
- **Riesgo tratado:** riesgo eliminado con controles.

Los dueños de los riesgos deben estar conscientes de los riesgos residuales y aceptar su responsabilidad respecto de ellos, en todas las circunstancias el riesgo residual debe ser entendido, aceptado y aprobado por la dirección.

2.2.2. Seguridad de la Información

Es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un activo informático. También se ocupa de diseñar los procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y

confiables, para el procesamiento de datos en sistemas informáticos. Es esencial que la organización identifique sus requisitos de seguridad.

Fuentes principales de requisitos de seguridad (Servicio Ecuatoriano de Normalización, 2013):

1. Evaluación de los riesgos para la organización, teniendo en cuenta la estrategia del negocio y objetivos de la organización. A través de una evaluación de los riesgos, se identifican las amenazas a los activos, se evalúa la vulnerabilidad y probabilidad de ocurrencia y se estima el posible impacto;
2. Requisitos legales, estatutarios, reglamentarios y contractuales necesarios que la organización, sus socios comerciales, contratistas y proveedores de servicios han de cumplir y su entorno socio-cultural;
3. Conjunto de principios, objetivos y requisitos de la empresa para el manejo, procesamiento, almacenamiento, comunicación y archivo de la información que una organización ha desarrollado para apoyar sus operaciones.

Dimensiones básicas de la seguridad:

- Disponibilidad: es la propiedad de la información para ser accesible y utilizable por una entidad autorizada. La información debe ser fácilmente accesible para las personas que la necesitan y los servicios pueden ser utilizados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio y afecta directamente a la productividad de las organizaciones. (Dirección General de Modernización Administrativa, 2019)

- Integridad: se trata de proteger la exactitud y completitud de los activos; comprende el mantenimiento de las características de completitud y corrección de los datos. Se afecta a la integridad cuando la información es manipulada, corrupta o incompleta; esto incide en el correcto desempeño de las funciones de una Organización. (Dirección General de Modernización Administrativa, 2019)
- Confidencialidad: Asegura que la información sólo sea accesible a las personas autorizadas. La confidencialidad o secreto puede ser afectada por fugas y filtraciones de información, así como por accesos no autorizados; es una propiedad que puede minar la confianza en la organización causada por quienes no son diligentes en el mantenimiento del secreto. También contempla el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos. (Dirección General de Modernización Administrativa, 2019). Opcionalmente también existen otras propiedades como: la responsabilidad, el no repudio y la fiabilidad.

2.2.3. Auditoría Informática

Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. Así se sustenta y confirma la consecución de los objetivos tradicionales de la auditoría.

Beneficios de realizar una auditoría:

- Mejorar la imagen pública.
- Brindar confianza a los usuarios sobre la seguridad y control de los servicios de TI.
- Optimizar las relaciones internas y el clima de trabajo.

- Minimizar los costos de mala calidad de los productos o servicios ofrecidos por la organización.
- Generar un balance de los riesgos en Tecnologías de la Información.
- Realizar un control de la inversión en un entorno de Tecnologías de la Información.

Tipos de Auditoría (Organización Internacional de Estandarización, 2018):

- Interna: de primera parte, se realizan por la propia organización o en su nombre para la revisión por la dirección y para otros propósitos internos.
- Externa: de segunda (clientes u otras personas en su nombre) o tercera parte (se lleva a cabo por organizaciones auditoras independientes para propósitos legales, reglamentos y similares)
- Combinada: cuando cubren dos o más sistemas de gestión de disciplinas diferentes.
- Conjunta: cuando dos o más organizaciones auditoras cooperan para auditar a un único auditado.

Otros tipos de Auditoría:

- Auditorías de vigilancia.- Se las debe realizar al menos una vez al año y se puede realizar no necesariamente en su totalidad, el tiempo de duración es alrededor del tercio del tiempo dedicado a la auditoría inicial. Las actividades de vigilancia deberán incluir auditorías in situ que evalúen el cumplimiento del sistema de gestión del cliente certificado con respecto de la norma por la que se otorga la certificación.
- Auditorías de seguimiento.- Tomando en cuenta las conclusiones de la auditoría, el auditor puede proceder con una auditoría de seguimiento antes de que la

organización sea recomendada para la certificación. Por lo general una no conformidad alta debería implicar una auditoría de seguimiento.

- Auditoría de recertificación.- Deberá ser planificada y ejecutada como mínimo cada 3 años para evaluar la continuación del cumplimiento de los hitos, además se debe tener en cuenta el rendimiento del sistema de gestión durante el período de certificación y deberá contener el estudio de los informes de auditoría anteriores, su duración es de alrededor de dos tercios del tiempo dedicado a la auditoría inicial.

Fases de la Auditoría:

De acuerdo a las directrices de la norma ISO 19011 y las mejores prácticas de auditoría, existen seis fases como se indica en la **Figura 6** (Organización Internacional de Estandarización, 2018):

Figura 6. Norma ISO 19011 Fases de Auditoría

Existen además tres procesos de soporte muy importantes y que son transversales al modelo: Gestión de Programas de Auditoría, Comunicación durante la auditoría y Gestión de los riesgos de auditoría,

Según los niveles de importancia, la documentación a ser auditada se clasifica como se indica en la figura 7 (Servicio Ecuatoriano de Normalización, 2013):

Figura 7. Clasificación de la información.
Fuente: Norma ISO/IEC 27001

Se debe realizar la verificación del control de la documentación, según el ciclo de vida de la documentación indicado en la **Figura 8**:

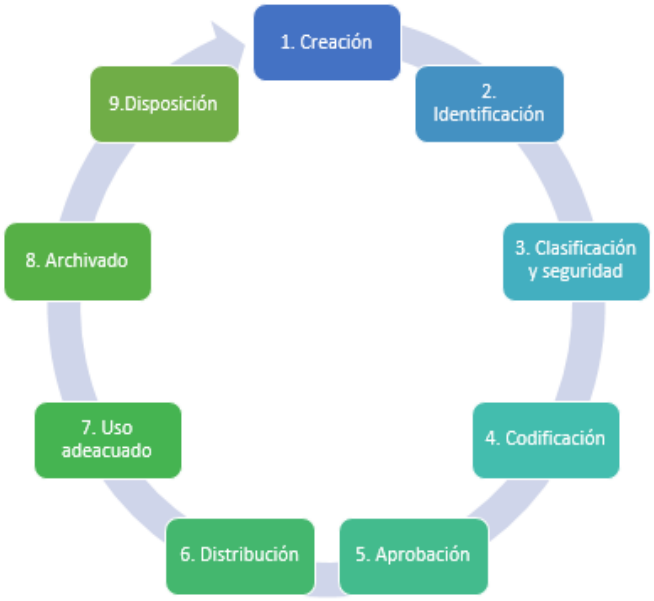

Figura 8. Ciclo de vida de la documentación.
Fuente: Norma ISO/IEC 27001

La auditoría termina cuando se han realizado y aprobado todas las actividades descritas en el plan de auditoría y cuando se ha distribuido el informe de auditoría, es apropiado archivar, devolver o destruir los documentos relacionados con la auditoría, según lo acordado por las partes. El cierre de la auditoría debería incorporarse en el proceso de mejora continua del programa de auditoría las lecciones aprendidas de la misión de la auditoría. (Organización Internacional de Estandarización, 2018).

2.3. Organismos relacionados

2.3.1. International Organization for Standardization (ISO)

Es una red de organismos nacionales de estandarización de más de 160 países. Las normas internacionales publicadas por ISO desde 1947 son alrededor de 19000 y se encuentran relacionados con actividades tradicionales como la agricultura, construcción

de dispositivos, medios de comunicación y el desarrollo más reciente en tecnologías de la información (UNE-ISO/IEC 27000, 2014).

Las ISO no regulan, ni legislan, a pesar de eso pueden ser obligatorias en el mercado, como el caso de la ISO 9001 (Gestión de la calidad) y la 14001 (Gestión Ambiental) ya que se han convertido en un referente internacional. Los ocho principios de gestión de ISO son los que permiten darle valor a las normas ISO ya que cuentan con un enfoque al cliente, liderazgo, participación de las personas, mejora continua, relaciones mutuamente beneficiosas con el proveedor, enfoque en los procesos, toma de decisiones y sistemas para la gestión (UNE-ISO/IEC 27000, 2014).

2.3.2. Information Systems Audit and Control Association (ISACA)

La Asociación de Auditoría y Control de Sistemas de Información, fundada en 1967, es una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información; ISACA tiene más de 110.000 miembros, dos de sus certificaciones más reconocidas profesionalmente a nivel internacional son: CISA (Certified lnformation Systems Auditor) y CISM (Certified lnformation Security Manager) (Asociación de Auditoría y Control de Sistemas de Información, 2019).

2.3.3. National Institute of Standards and Technology (NIST)

El Instituto Nacional de Estándares y Tecnología tiene como misión promover la innovación y la competencia industrial mediante avances en metrología, normas y tecnología para mejorar la economía y la calidad de vida. El progreso e innovación tecnológica de Estados Unidos dependen de las habilidades del NIST en cuatro áreas:

biotecnología, nanotecnología, tecnologías de la información y fabricación avanzada (National Institute of Standards and Technology NIST, 2019).

El sitio web (http://csrc.nist.gov/) permite el acceso a buenas prácticas de seguridad, guías de implementación, políticas de seguridad y otros documentos que se puede utilizar en patrones de seguridad.

2.4. Normas aplicables

2.4.1. ISO 31000

No es una norma certificable. Aborda la Gestión de Riesgos de forma global, es un estándar aplicable a cualquier tipo de organización; establece una serie de principios para la implementación de un SGSI; busca minimizar, gestionar y controlar cualquier tipo de riesgo; se divide en 3 áreas básicas (Organización Internacional de Estandarización, 2018)

Principios de la gestión de riesgos

Son 11 prácticas básicas que debe tener en cuenta cualquier organización dispuesta a implementar un Sistema de Gestión de Riesgos (Organización Internacional de Estandarización, 2018)

Marco de trabajo para la Gestión de riesgos

El objetivo es trazar un marco de acción para saber qué aspectos gestionar y cómo hacerlo, la gestión tiene que ver, con la cuantificación de los riesgos, su objetivo es integrar el proceso de gestión de riesgos en el gobierno, estrategia y planificación, gestión, informes, políticas de toda la organización.

Luego de la etapa de mandato y compromiso. Se establece algunos mandatos en la norma que se requiere por parte de la gerencia (Organización Internacional de Estandarización, 2018).

Proceso de gestión de riesgos

Es el tercer pilar fundamental que debe estar relacionado con los procesos de negocio se detalla en la **Figura 10**.

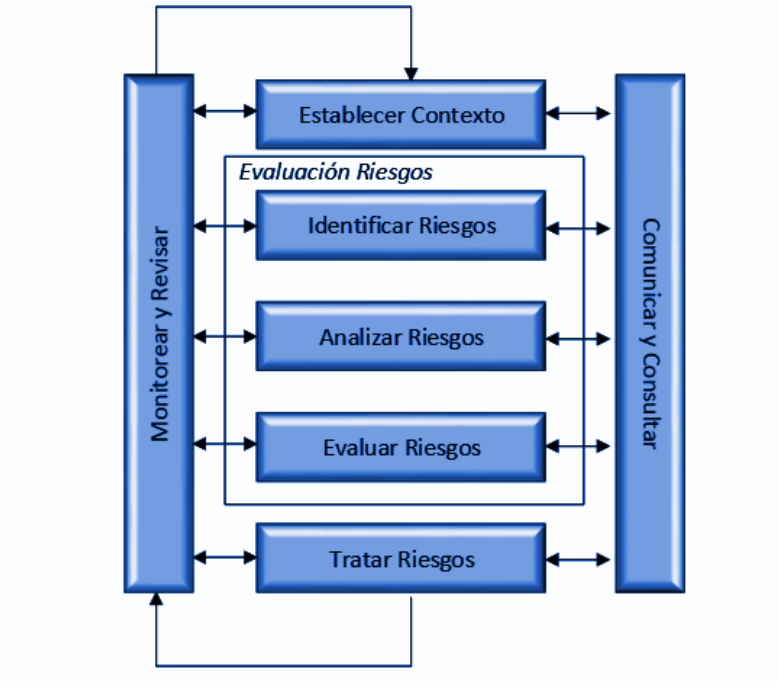

Figura 10. Proceso de gestión de Riesgos
Fuente: Norma ISO/IEC 31000

2.4.2. ISO 27000

La ISO 27000 es una familia de normas exclusiva para el ámbito de seguridad de la información, la única certificable de esta familia es la ISO 27001, las demás son solo directrices, como se indica en la **Figura 11** (UNE-ISO/IEC 27000, 2014):

Figura 11. Familia ISO
Fuente: UNE-ISO/IEC 27000

La familia de normas ISO 27000 ha sido publicada desde el 2005 en forma gradual. Se presenta a continuación una descripción resumida de las normas más conocidas.

- ISO 27000.- Presenta los conceptos básicos de seguridad de la información, el vocabulario y describe el SGSI en una visión de conjunto.
- ISO 27001.- Define los requisitos del SGSI para certificación.
- ISO 27002.- Es una guía de las mejores prácticas para implantar controles de seguridad de la información.
- ISO 27003.- Guía para la implementación de un SGSI.

- ISO 27004.- Guía de indicadores que facilitan la gestión del SGSI.
- ISO 27005.- Gestión de riesgos de seguridad de la información (SI).
- ISO 27006.- Requisitos para entidades que auditan y certifican el SGSI.
- ISO 27007.- Directrices para la auditoría del SGSI.
- ISO 27008.- Guía para los auditores de controles de SI.
- ISO 27010.- Gestión de SI en comunicaciones intersectoriales e inter-organizacionales.
- ISO 27011.- Guía para la gestión de SI para las organizaciones de telecomunicaciones basadas en la Norma ISO/IEC 27002.
- ISO 27013.- Guía para la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1.
- ISO 27014.- Gobernanza de la seguridad de la información.
- ISO TR 27015.- Guía para la gestión de SI para servicios financieros.
- ISO TR 27016.- Gestión de SI, economía organizacional.
- ISO 27031.- Directrices para la continuidad del negocio de la TIC.
- ISO 27799.- Gestión de SI en sanidad utilizando la Norma ISO/IEC 27002.

Las normas ISO de la serie 27009 en adelante estás reservadas para la creación de normas enfocadas en dominios específicos (UNE-ISO/IEC 27000, 2014):

- Para las industrias: Telecomunicaciones, Salud y Finanzas y seguros
- Para sectores específicos relacionada seguridad de la información: Seguridad de las aplicaciones, Seguridad cibernética, Gestión de incidentes de seguridad, Protección de la privacidad.

Norma ISO 27001

Especifica los requisitos para el establecimiento, implementación mantenimiento y mejora continua del SGSI, que asegura la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y otorga a las partes interesadas confianza sobre la adecuada aplicación de controles para SI (Servicio Ecuatoriano de Normalización, 2013).

La norma ISO 27001 no establece controles específicos de seguridad de la información, pero proporciona una lista de los controles que deben ser considerados en el código de prácticas, ISO 27002; fue publicada en el 2005 posteriormente corregida y ampliada en el 2013; su origen es la BS 7799-2:2002. (Spohr, 2019)

La versión 2013 no se vio afectada por la publicación de 2017, en la que solo se añade la aprobación de CEN / CENELEC para la designación EN ("Norma Europea"). (ISMS.online, 2019)

El Servicio Ecuatoriano de Normalización (INEN) adopta la norma internacional ISO/IEC 27001 versión 2013, como una norma que proporciona los requisitos para establecer, implementar, mantener y mejorar de manera continua un SGSI para salvaguardar la integridad, disponibilidad y confidencialidad de la información en una organización. (Servicio Ecuatoriano de Normalización, 2013)

Estructura de la norma ISO 27001

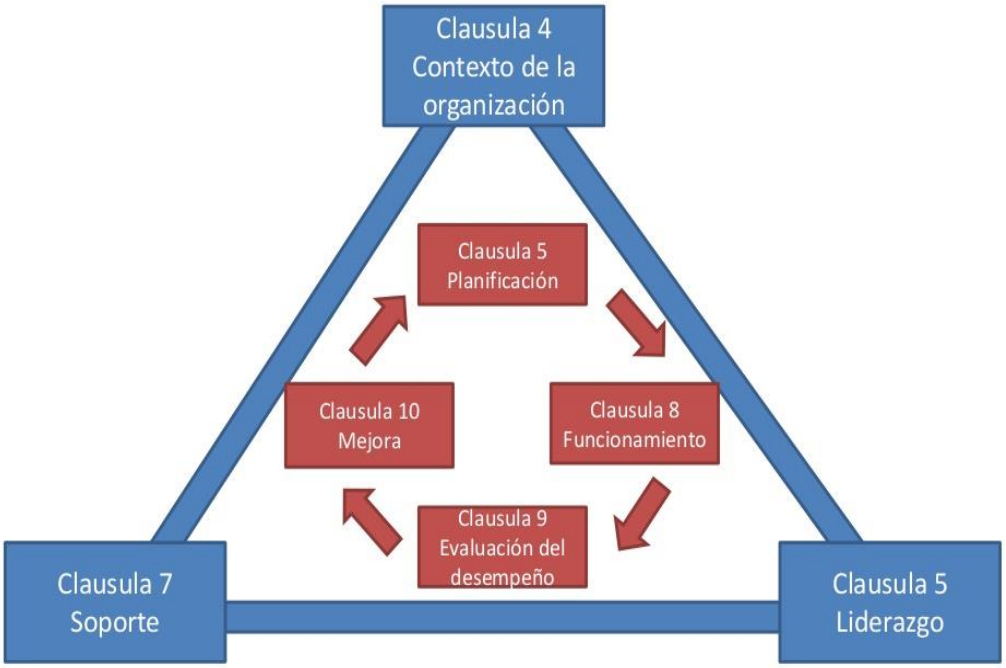

Figura 12. Secciones ISO 27001
Fuente: Norma ISO/IEC 27001

Para certificar la organización debe cumplir con todos los términos definidos en las cláusulas 4 a 10 de la norma como se indica en la **Figura 12**, declarar la aplicabilidad y justificar la inaplicabilidad de los controles del Anexo A.

- Cláusula 4: Contexto de la organización.- Determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su SGSI. El alcance debe estar disponible como información documentada. (Servicio Ecuatoriano de Normalización, 2013).

La organización debe establecer, implementar, mantener y mejorar de manera continua un SGSI, de acuerdo con los requisitos de esta norma internacional. Un SGSI

es un enfoque sistemático para conseguir los objetivos de negocio. Se basa en una evaluación del riesgo y de los niveles de aceptación del riesgo de la organización diseñado para tratar y gestionar los riesgos de manera eficaz (UNE-ISO/IEC 27000, 2014). El SGSI se utiliza para garantizar la selección de controles de seguridad adecuados y equilibrados que protegen los activos y para ofrecer garantías a las partes interesadas, más detalle en se indica en la **Figura 13**.

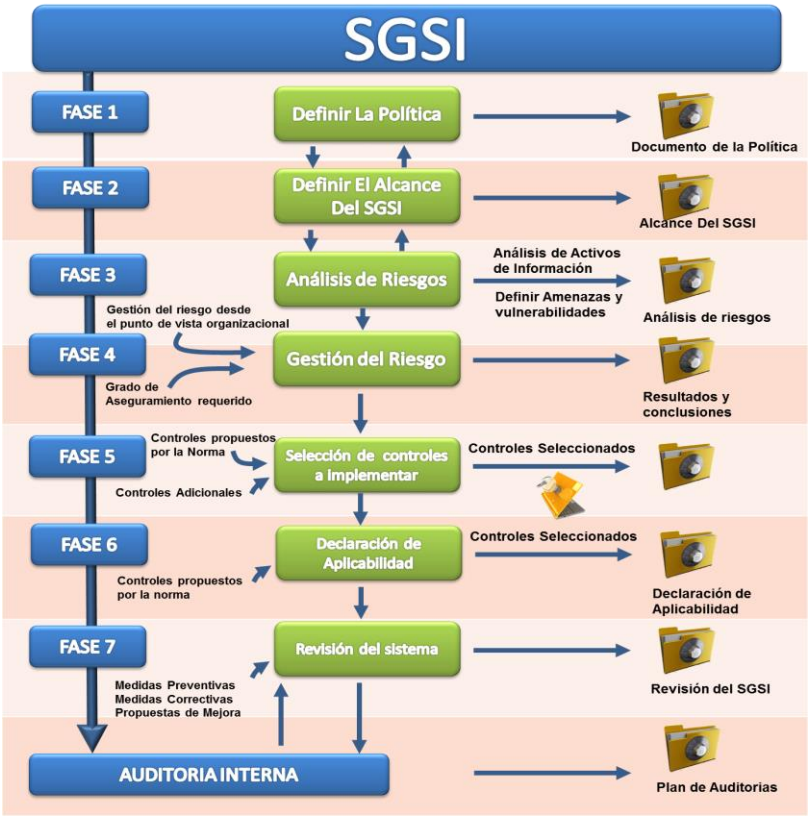

Figura 13. Sistema de Gestión de Seguridad de la Información
Fuente: Norma ISO/IEC 27000

La norma adopta el modelo de proceso PHVA (Planificar, hacer, verificar, actuar) también llamado ciclo de Deming. Se aplica a todos los procesos de un sistema de

gestión, ya que se utiliza como entrada los requisitos y las expectativas de las partes interesadas, cómo se producen, las acciones y procesos necesarios, los resultados de seguridad de la información como se indica en la **Figura 14**.

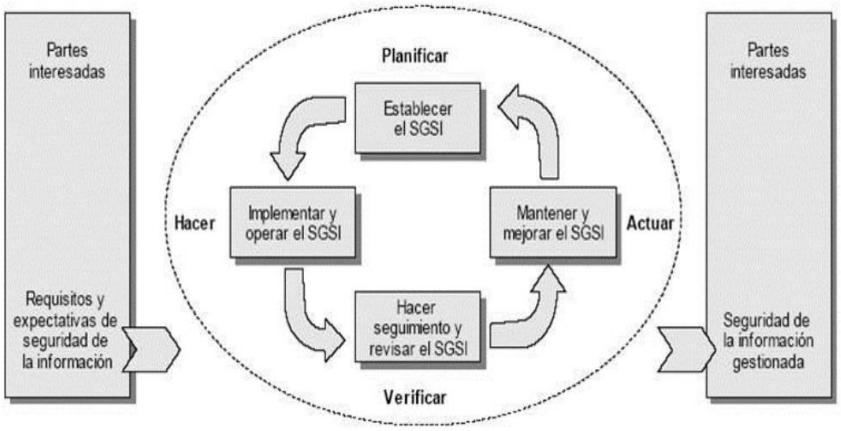

Figura 14. Ciclo de Deming
Fuente: https://q-bo.org/que-es-el-ciclo-pdca-o-deming/. Recuperado: 13 de marzo de 2019

- Cláusula 5: Liderazgo.- Esta sección tiene el objetivo de asegurarse de que el SGSI es compatible con la orientación estratégica de la organización, además integra los requisitos del SGSI en los procesos de negocio de una organización. La Dirección deberá determinar los recursos necesarios para el SGSI, comunicar la importancia de una buena gestión de la seguridad de la información y el cumplimiento de los procesos del SGSI. Los controles de esta cláusula son: Liderazgo y compromiso, Política y Roles, responsabilidades y autoridades en la organización.

- Cláusula 6: Planificación.- La definición del enfoque de evaluación de riesgos y la correcta selección de controles permitirá determinar los necesarios para implementar las opciones de tratamiento de riesgo de seguridad de la información. Los controles de esta cláusula son: las acciones para tratar los riesgos y oportunidades además de los objetivos de seguridad de la información y planificación para su consecución que la organización deberá establecer y alcanzar los objetivos de seguridad de la información en los niveles y funciones pertinentes y deberán ser coherentes con la política de seguridad de la información, deben ser mensurables y ser actualizados según corresponda.
- Cláusula 7: Soporte.- Determinar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI, la concienciación, comunicación y documentación de la misma. Los controles de esta cláusula son: recursos, competencia, concienciación, comunicación, información documentada. Para el control de la información documentada se deberá abordar las siguientes actividades: distribución, protección, almacenamiento, control de cambios y retención de los mismos.
- Cláusula 8: Operación.- La organización deberá planificar, ejecutar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y aplicar medidas para subsanar los riesgos y así alcanzar los objetivos de seguridad de la información establecidos. Los controles de esta cláusula son: planificación y control operacional, apreciación de los riesgos de seguridad de la información, tratamiento de los riesgos de seguridad de la información.

- Cláusula 9: Evaluación del desempeño.- La organización deberá evaluar el rendimiento de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información; mediante auditorías internas y la planificación de un programa de auditorías periódicas, teniendo en cuenta los resultados de cada una con mejora continua.

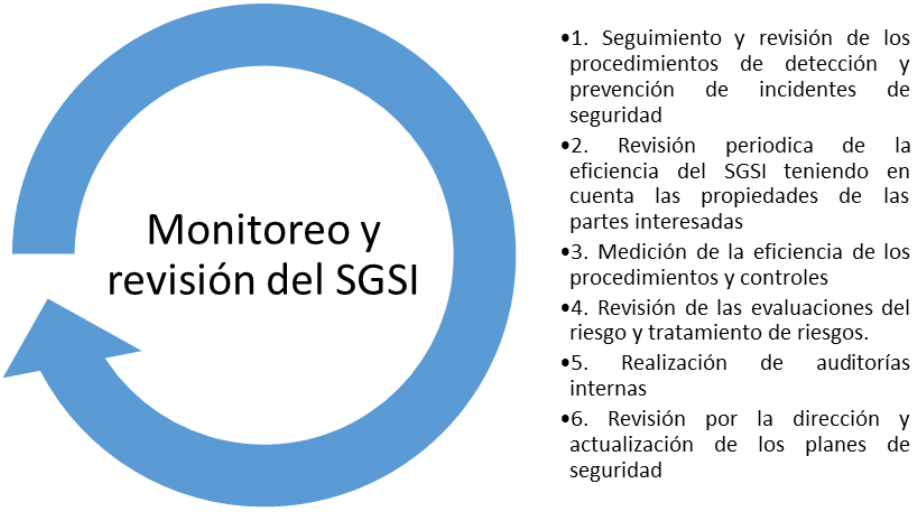

Figura 15. Monitoreo y revisión del SGSI
Fuente: Cláusula 9 ISO 27001

Las revisiones de la Dirección deben ser documentadas, con una frecuencia mínima de una vez al año. Los controles de esta cláusula se indican en la **Figura 15**.

- Cláusula 10: Mejora.- La organización deberá mejorar continuamente la conveniencia, adecuación y eficacia del SGSI y cuando no exista una conformidad la organización deberá, reaccionar incluso realizando algún cambio al SGSI. Los controles de esta cláusula son (Servicio Ecuatoriano de Normalización, 2013): No conformidad y acciones correctivas y, mejora contínua.

- Anexo A.- Los objetivos de control y controles que se enumeran en el anexo A están alineados con los objetivos de seguridad y controles de seguridad que se indican en las cláusulas de la norma ISO 27002, Cláusulas 5 a 18 (Servicio Ecuatoriano de Normalización, 2013).

Tabla 1

Contenido del Anexo A norma ISO 27001.

SECCIÓN	CONTROL
A5	Políticas de seguridad de la información
A6	Organización de la seguridad de la información
A7	Seguridad de los recursos humanos
A8	Gestión de activos
A9	Control de accesos
A10	Criptografía
A11	Seguridad física y medio ambiental
A12	Seguridad de las operaciones
A13	Seguridad de las comunicaciones
A14	Adquisición de sistemas, desarrollo y mantenimiento
A15	Relaciones con los proveedores
A16	Gestión de incidentes de seguridad de la información
A17	Aspectos de seguridad de la información de la gestión de continuidad del negocio
A18	Cumplimiento

Fuente: ISO/IEC 27001

Las listas de objetivos y controles de seguridad que se detallan en la **Tabla 1** en la ISO 27001, Anexo A no son exhaustivos. Una organización puede considerar incluir objetivos adicionales de seguridad y controles de seguridad en caso necesario. La organización debe justificar las razones para la selección de cada control de seguridad incluido en el SGSI. En el caso de exclusión de controles la organización debe justificar las razones de la exclusión de cada control.

Proceso de certificación ISO 27001

El proceso de certificación resumido en 9 pasos se detalla en la **Figura 16**:

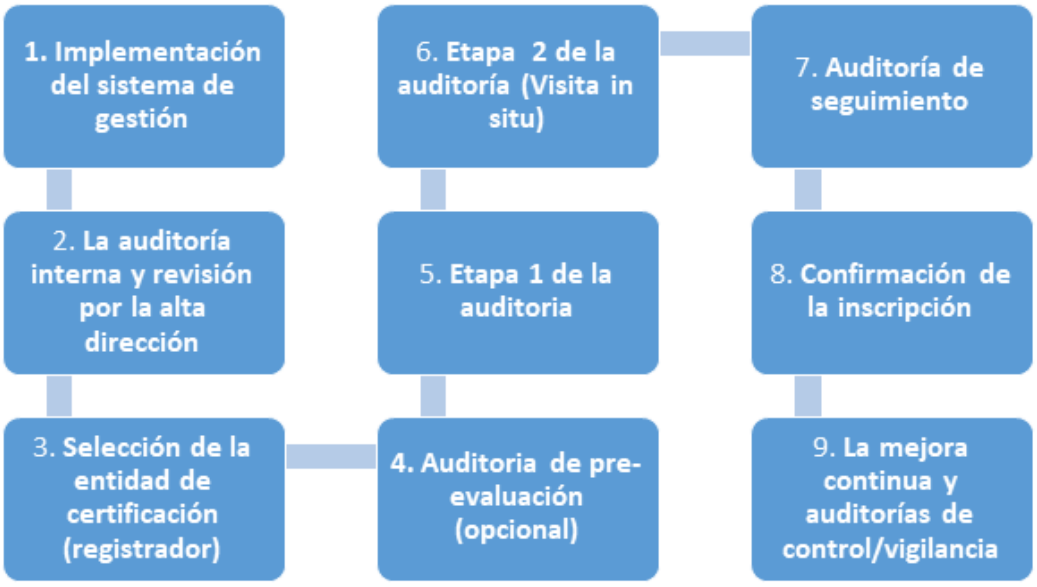

Figura 16. Proceso de certificación ISO 27001
Fuente: https://www2.deloitte.com/ec/es/pages/deloitte-analytics/articles/certificacion-iso-27001-deloitte-ecuador.html

Las actividades de acreditación y certificación no son llevadas a cabo por la ISO, sino por organismos de certificación y acreditación especializados e independientes. La misión de ISO es únicamente el desarrollo de normas (Deloitte, 2019).

2.4.2.1. Norma ISO 27002

Esta norma internacional está diseñada para que las organizaciones la usen como referencia a la hora de seleccionar controles dentro del proceso de implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001 o bien como documento guía para organizaciones que implanten controles de seguridad de la información comúnmente aceptados. Esta norma está pensada también para usarse en el desarrollo de directrices de gestión de la seguridad

de la información en industrias y organizaciones específicas, teniendo en cuenta su entorno específico de riesgo de seguridad de la información (ISO/IEC 27002, 2017).

Proporciona recomendaciones acerca de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como “la preservación de la confidencialidad, integridad y disponibilidad (Spohr, 2019).

Evolución

La Norma (ISO/IEC 27002, 2017) incluyendo Cor 1:2014 y Cor 2:2015 ha sido elaborado por el Comité Técnico ISO/IEC JTC 1 Tecnología de la Información de la Organización Internacional de Normalización (ISO) y de la Comisión Electrotécnica Internacional (IEC) y ha sido adoptada como EN ISO/IEC 27002:2017. Además de que El texto de la Norma ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015 ha sido aprobado por CEN como Norma EN ISO/IEC 27002:2017 sin ninguna modificación.

Secciones norma ISO 27002

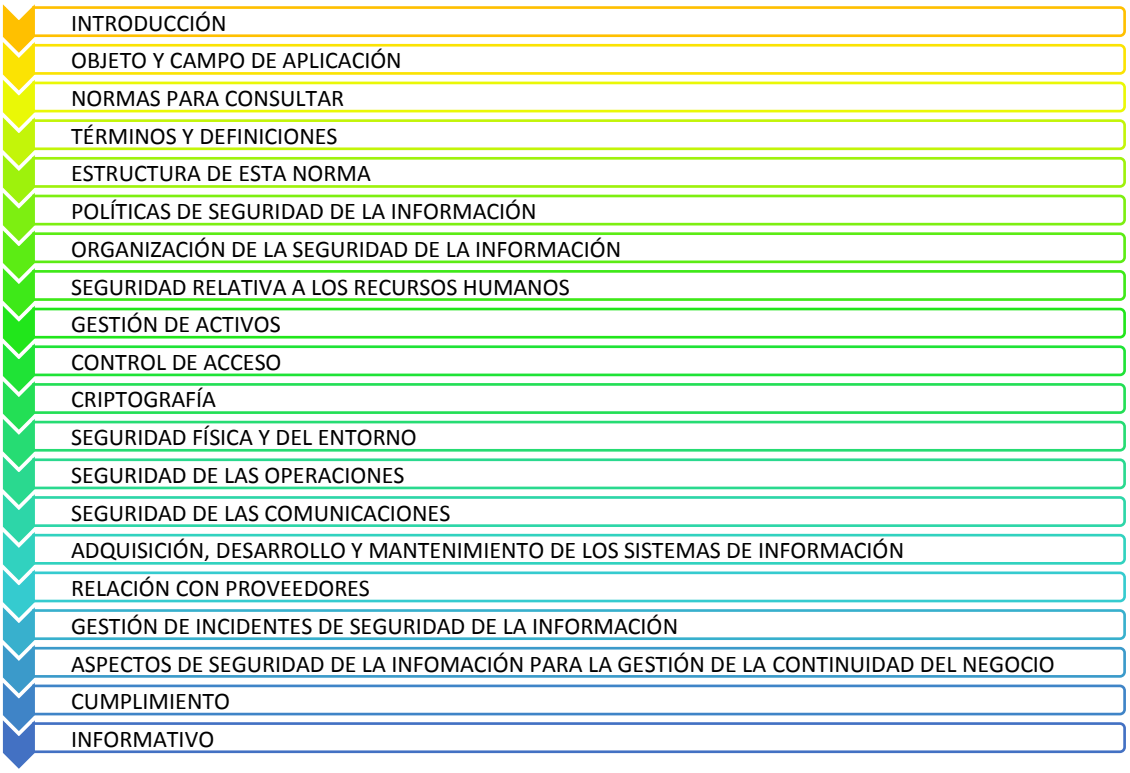

Figura 17. Secciones normativa ISO 27002
Fuente: ISO/IEC 27002

A partir de la sección 5 a la 18 que se presenta en la **Figura 17** un asesoramiento específico y guía para la aplicación de las mejores prácticas para poyar los controles específicos en el Anexo A de la norma ISO 27001.

Estructura de la norma

Esta norma consta de 14 capítulos de controles de seguridad que contienen un total de 35 categorías principales de seguridad y 114 controles.

- **Capítulos.-** Cada capítulo que define controles de seguridad, contiene una o más categorías principales de controles de seguridad. El orden de los capítulos de esta norma no implica un orden de importancia.
- **Categorías de controles.-** Cada categoría principal de controles de seguridad contiene: un objetivo del control que establece qué es lo que se quiere conseguir; y uno o más controles que pueden ser aplicados para conseguir el objetivo del control.

Políticas de seguridad de la información

Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes. (ISO/IEC 27002, 2017)

Seguridad relativa a los recursos humanos

Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran y así proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.

Gestión de activos

Identificar los activos de la organización y definir las responsabilidades de protección adecuadas, asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización y evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.

Control de acceso

Limitar el acceso a los recursos de tratamiento de información y a la información, garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios además de prevenir el acceso no autorizado a los sistemas y aplicaciones.

Criptografía

Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información y evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

Seguridad física y del entorno

Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.

Seguridad de las operaciones

Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información, están protegidos contra el malware, mediante copias de seguridad evitar pérdidas de datos, y registrar eventos generando evidencias.

Seguridad de las comunicaciones

Asegurar la protección de la información en las redes y los recursos de tratamiento de la información y mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.

Adquisición, desarrollo y mantenimiento de los sistemas de información

Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

Relación con proveedores

Asegurar la protección de los activos de la organización que sean accesibles a los proveedores y mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.

Gestión de incidentes de seguridad de la información

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.

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

La continuidad de la seguridad de la información debería formar parte de los sistemas de gestión de la continuidad de negocio de la organización y asegurar la disponibilidad de los recursos de tratamiento de la información.

Cumplimiento

Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos y revisiones de la seguridad de la información. Algunos aspectos legales principales a ser monitoreados son:

- **Protección de datos:** en los países donde las leyes cubren la confidencialidad e integridad de datos, a menudo se limita el control de datos personales.

- **Privacidad:** las organizaciones optan por establecer una política para protección de la privacidad, a menudo diseñada para alcanzar los objetivos como establecer una política empresarial clara y completa para el tratamiento de datos personales.
- **La identificación y el enjuiciamiento de los delitos informático:** una amenaza alta es la ciberdelincuencia a través de internet para los sistemas de información de una organización por lo que el daño puede ser grande y las pérdidas financieras directas o de reputación.
- **El uso de firma digital:** La validez de una firma electrónica hoy en día es legal.
- Propiedad intelectual: tiene potencial en las PYME en materia de protección jurídica, tecnología de la información y la ventaja competitiva.
- **Comercio y pagos electrónicos:** diferencia entre una compra física a un electrónica es más fácil además un consumidor no puede determinar la legislación nacional del producto que se encuentra adquiriendo mediante un sitio web.
- **Gestión de registros:** algunas leyes nacionales propias del país exigen mantener registros actualizados anualmente o hasta pueden obligar a emitir el registro para efectos legales.

Anexo A.- Informativo

Es importante señalar que el Anexo A de la ISO 27001 tiene 14 cláusulas principales de control numeradas de A.5 a A.18, cada una de las cuales identifica uno o más objetivos de control. Cada objetivo cuenta con uno o más controles. Cada control está numerado secuencialmente.

Siendo 114 sub-cláusulas, cada una de las cuales tiene un número de cláusula alfanumérico. El Anexo A está alineado con la ISO 27002; esto significa que se utiliza precisamente los mismos objetivos de control, controles, numeración de la cláusula y redacción en tanto el Anexo A como en la ISO.

2.4.2.2. Norma ISO 27005

Es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información, complementando los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27000, además suministra las directrices para la gestión de riesgos de seguridad de la información en cualquier organización (Organización Internacional de Estandarización, 2018). Cuenta con 12 cláusulas y 6 anexos; de la 1 a las 6 son informativas, de la 7 a la 12 son descriptivas, se indica a continuación en la **Figura 18** :

PREFACIO.

INTRODUCCIÓN.

REFERENCIAS NORMATIVAS.

TÉRMINOS Y DEFINICIONES.

ESTRUCTURA.

FONDO.

DESCRIPCIÓN DEL PROCESO DE ISRM.

ESTABLECIMIENTO CONTEXTO.

INFORMACIÓN SOBRE LA EVALUACIÓN DE RIESGOS DE SEGURIDAD (ISRA).

TRATAMIENTO DE RIESGOS SEGURIDAD DE LA INFORMACIÓN.

ADMISIÓN DE RIESGOS SEGURIDAD DE LA INFORMACIÓN.

COMUNICACIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN.

INFORMACIÓN DE SEGURIDAD SEGUIMIENTO DE RIESGOS Y REVISIÓN.

ANEXO A: DEFINICIÓN DEL ALCANCE DEL PROCESO.

ANEXO B: VALORACIÓN DE ACTIVOS Y EVALUACIÓN DE IMPACTO.

ANEXO C: EJEMPLOS DE AMENAZAS TÍPICAS.

ANEXO D: LAS VULNERABILIDADES Y MÉTODOS DE EVALUACIÓN DE LA VULNERABILIDAD.

ANEXO E: ENFOQUES ISRA

Figura 18. Detalle de normativa ISO 27005
Fuente: ISO/IEC 27005

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su tratamiento, como se indica en la **Figura 19**:

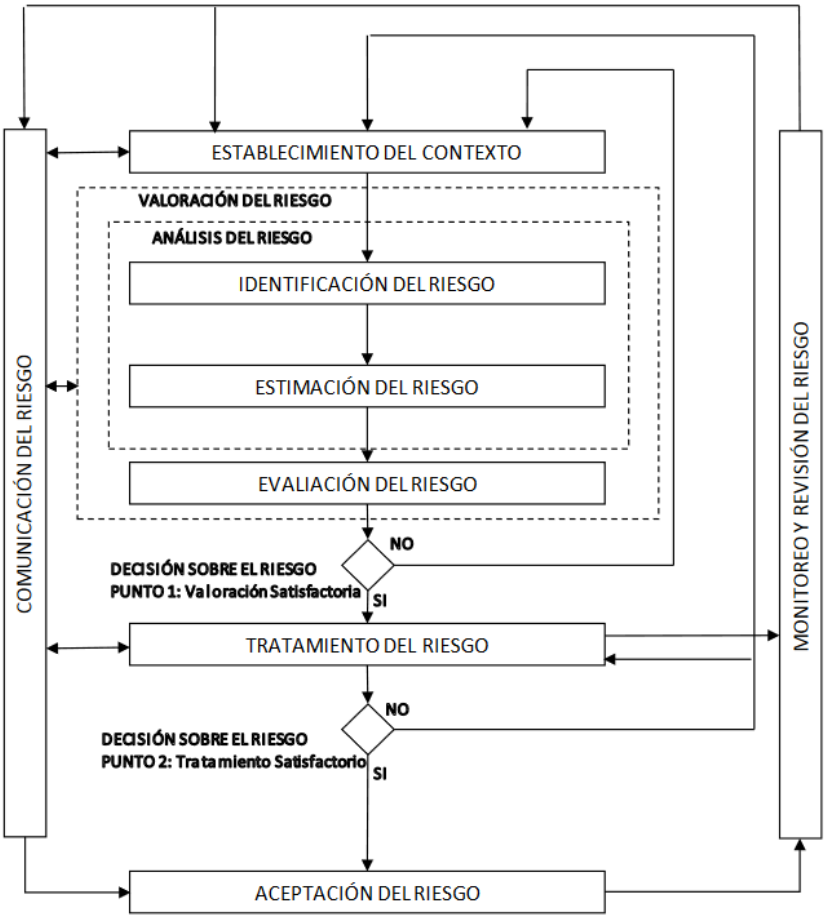

Figura 19. Gestión de Riesgos
Fuente: ISO/IEC 27005

La actualización, mantenimiento y mejora continua de un SGSI ofrece a una organización un enfoque sistemático para la identificación, evaluación y gestión de riesgos de seguridad de la información.

Relación: vulnerabilidad y amenaza

En sí mismo, la presencia de una vulnerabilidad no produce daño, debe existir una amenaza para explotarla. Una vulnerabilidad que no se corresponde con una amenaza puede no requerir la puesta en marcha de un control, pero debe ser identificada y controlada en caso de que se produzcan cambios.

Tener en cuenta que la aplicación incorrecta, el uso o el mal funcionamiento de un control, por sí mismo, podrían representar una amenaza. Un control puede ser eficaz o ineficaz en función del entorno en el que opera. Por otro lado, una amenaza que no es vulnerable no puede representar un riesgo. Como por ejemplo en la **Tabla 2**:

Tabla 2
Ejemplos de vulnerabilidad-amenaza.

VULNERABILIDADES	AMENAZAS
Almacén desprotegido y sin vigilancia	Robo
Complicados procedimientos de proceso de datos	Error de entrada de datos por parte del personal
No hay segregación de tareas	Fraude, uso no autorizado de un sistema
Uso de software pirata	Demanda, virus
No hay revisión de permisos de acceso	Acceso no autorizado a personas que ya no pertenecen a la institución
Procedimientos de backup	Perdida de información

Fuente: ISO/IEC 31000

Anexo A: Definición del Alcance y los límites del proceso de gestión de riesgo de Seguridad de la Información.

Ayuda con la identificación del estudio de la organización con su estructura, valores, misión, su negocio; así como el listado de las restricciones que afectan a la organización, las referencias legislativas y reglamentarias que se aplican a la organización,

Anexo B: Identificación y valoración de los activos y valoración del impacto.

Muestra ejemplos de cómo realizar la valoración de los activos, es necesario que la organización identifique primero sus activos valorar y tener ciertos conceptos claros al momento de aplicar la norma. Por ejemplo:

Impacto: Es la medida del daño sobre el activo derivado de la materialización de una amenaza, o cambio adverso importante en el nivel de los objetivos de negocio logrados. En el anexo B.2 (Organización Internacional de Estandarización, 2018) se puede encontrar una lista de varios impactos potenciales que pueden afectar a la disponibilidad, integridad, confidencialidad o una combinación de ellas:

- Las pérdidas financieras.
- Pérdida de bienes o de su valor.
- La pérdida de clientes, la pérdida de los proveedores.
- Las demandas y sanciones.
- La pérdida de la ventaja competitiva.
- La pérdida de la ventaja tecnológica.
- Pérdida de eficacia y eficiencia.
- Violación de la privacidad de los usuarios o clientes.

- Interrupciones del servicio.
- Incapacidad para proporcionar el servicio.
- Pérdida de la marca o la reputación.
- interrupción de operaciones.
- interrupción de operaciones de terceros (proveedores, clientes, etc.).
- Incapacidad para cumplir con sus obligaciones legales.
- Incapacidad para cumplir con las obligaciones contractuales.
- Peligro a la seguridad del personal y de los usuarios.

Anexo C: se define que una amenaza tiene el potencial de hacer daño a los activos como información, procesos y sistemas y el consiguiente perjuicio a la organización, la naturaleza de la amenaza es siempre indeseable.

Una amenaza es cualquier circunstancia o acontecimiento con el potencial de afectar a un sistema de información como es el acceso desautorizado, la destrucción, la modificación de datos, y/o la negación del servicio (Baquero, 2017). Una amenaza siempre es asociada a un aspecto negativo de riesgo, por lo general una amenaza es indeseable y puede hacer daño a un sistema u organización. Algunos ejemplos de tipología para la clasificación de las amenazas, se detallan en la **Tabla 3**:

Tabla 3
Ejemplo de amenazas.

TIPO DE AMENAZA	EJEMPLO
1 Daño Físico	Fuego
	Daño por agua
2 Desastres naturales	Terremoto
	Inundación
3 Pérdida de servicios esenciales	Falta de aire acondicionado
	Corte de suministro eléctrico
4 Trastornos causados por la radiación	Radiación electromagnética
	Radiación térmica
5 Información comprometida	Escuchas telefónicas
	Robo de documentos
6 Fallas técnicas	Falla de equipo
	Sobrecarga de la red
7 Acción no autorizada	Acceso no autorizado
	Uso de software pirata

Fuente: ISO/IEC 31000

Anexo D: proporciona una tipología para la clasificación de las vulnerabilidades que podría ser utilizada en principio.

Una ***vulnerabilidad*** es una debilidad de un activo o de un control en los procedimientos que puede ser explotada por una o más amenazas, en los procedimientos del sistema de información, de la seguridad del sistema, controles internos, o de implementación que podría ser explotada por una amenaza.

Las vulnerabilidades pueden ser intrínsecas de los activos o extrínsecas están relacionadas con las características de las circunstancias específicas del activo, como por ejemplo se detalla en la **Tabla 4** :

Tabla 4

Ejemplo de catálogo de vulnerabilidades.

TIPO DE VULNERABILIDAD	EJEMPLOS
1 Hardware	Mantenimiento insuficiente
	Portabilidad
2 Software	No hay registros de inscripción
	Interface complicadas
3 Red	Falta de encriptación de las transferencias
	Único punto de acceso
4 Personal	Formación insuficiente
	Falta de supervisión
5 Sitio	Sistema eléctrico inestable
	Sitio en una área susceptible a inundaciones
6 Estructura de la organización	Falta de separación de tareas
	No hay descripción de puestos

Fuente: ISO/IEC 31000

Esta lista de vulnerabilidades debe ser actualizada, pero se usa como una guía o recordatorio para ayudar a organizar y estructurar la recopilación de los datos pertinentes sobre las vulnerabilidades en lugar de una lista para seguir ciegamente.

2.4.3. ISO 19011

Cuando una organización cuenta con un sistema de gestión se debe realizar ciertas auditorías periódicas para asegurarse de que el Sistema de Gestión sigue siendo eficaz por lo que la norma ISO 19011 es útil en estos casos. Esta norma es desarrollada por la ISO en su última revisión 2018, proporciona orientación sobre los elementos de una auditoría, además de las responsabilidades del auditor, su aplicación puede ser para todas las organizaciones que requieran auditorías internas y externas (Organización Internacional de Normalización ISO 19011, 2018).

La ISO 19011 contiene directrices flexibles para que puedan adaptarse fácilmente al tamaño, naturaleza y complejidad de la organización a ser auditada. La responsabilidad recae en cada auditor para aplicar las directrices, según la necesidad y métodos de trabajo.

La norma consta de siete capítulos y dos anexos como se detalla en la Figura 20:

Figura 20. Contenido normativa ISO 19011
Fuente: ISO/IEC 19011

Una auditoría es el proceso sistemático e independiente y documentado para obtener evidencia de auditoría y para evaluarla objetivamente para determinar hasta dónde se cumplen los criterios de la auditoría. Además es una actividad que se ha establecido desde hace mucho tiempo y es muy respetada en el campo de la contabilidad. Los mismos principios básicos y técnicas aplican para las auditorías del sistema de gestión.

- **Auditoría financiera:** Determina si las prácticas de contabilidad de una organización cumplen con principios reconocidos.
- **Auditoría administrativa:** Determina la efectividad de las prácticas de gestión.
- **Auditoría del sistema de información:** Determina si los activos de la información están protegidos correctamente.

Los tipos de auditorías pueden ser internas o externas:

- **Internas:** Son las de denominadas de primera parte, ya que da a la organización una garantía del nivel de control sobre las operaciones, ofrece recomendaciones para mejorar las operaciones y contribuye a la creación de valor agregado. Por lo general son realizadas por la propia organización y revisión de la dirección.
- **Externas:** Se segunda parte: son llevadas a cabo por partes que tiene interés en la organización auditada, tales como clientes u otras personas en su nombre.
- **De tercera parte:** son realizadas por la organización de auditoría externa e independiente, tales como las organizaciones que otorgan el certificado de registro o la certificación de conformidad de los sistemas de gestión.

Según esta norma se debe definir ciertos términos como:

- **Cliente:** persona u organización que solicita la auditoría
- **Auditado:** organización auditada
- **Auditor:** persona competente que realiza la auditoría
- **Experto:** persona que proporciona conocimientos específicos o experiencia de trabajo al equipo auditor
- **Equipo Auditor:** uno o más auditores que realizan el trabajo apoyados, si es necesario por expertos técnicos.

Una auditoría tiene como objetivos:

- **Auditoría de opinión:** recibir consejo y recomendaciones
- **Auditoría de pre-evaluación**: preparar la certificación
- **Auditoría de certificación:** recomendar o no la certificación

Principios de la auditoría:

El objetivo de una auditoría es dar confianza a todas las partes de que un sistema de gestión cumple los requisitos especificados y la certificación es el grado de confianza del público, por ello los principios que debe cumplir una auditoría son (Organización Internacional de Estandarización, 2018):

- **Integridad:** un auditor profesional debe realizar su trabajo con honestidad, responsabilidad y diligencia, la integridad es una conducta profesional que respeta la ética, la ética es un conjunto de principios que constituye un sistema de normas morales e ideales.
- **Presentación razonable:** es obligación del auditor informar con honestidad y precisión, la comunicación deberás ser veraz, exacta, objetiva, oportuna, clara y completa.
- **Debido cuidado profesional:** el auditor debería actuar con cuidado y según los estándares profesionales y las técnicas pertinentes al brindar sus servicios profesionales. Sin olvidar el cuidado profesional en su trabajo es tener la habilidad de hacer juicios razonados en todas las situaciones de la auditoría.
- **Confidencialidad:** no revelar información o utilizar información confidencial adquirida durante tratos profesionales o de negocio para el beneficio personal o el de terceros sin la autorización específica y apropiada, además se debe tener en cuenta el manejo apropiado de información sensible, confidencial o clasificada. Excepciones tales como las permitidas por la ley o autorizadas por las partes interesadas.

- **Independencia:** el auditor frente a la entidad auditada, de aspecto y de hecho, es la base de la imparcialidad y la objetividad de la auditoría así como las conclusiones de la auditoría. Por ejemplo el auditor no deberá suponer no conformidades basado en la apariencia y la actitud de la entidad auditada. Las amenazas a la imparcialidad incluyen lo siguiente:
    - **Interés propio:** las amenazas que surgen de una persona o entidad que actúa en su propio interés.
    - **Autoevaluación:** las amenazas que surgen de una persona o un órgano de revisión del trabajo realizado por ellos mismo.
    - **Familiaridad:** las amenazas que surgen de una persona o cuerpo que es demasiado familiar o confía en otra persona en lugar de buscar la evidencia de la auditoría.
    - **Intimidación:** amenazas que surgen de una persona o un cuerpo que tiene una percepción de ser coaccionado abiertamente o en secreto.
- **Enfoque basado en la evidencia:** es el enfoque racional para poder formular conclusiones de auditoría fiables. Las conclusiones de la auditoría deben ser siempre basadas en suficiente y adecuada evidencia. Para poder presentar evidencia adecuada, se debe reunir evidencias objetivas, estar disponibles y ser verificables, por naturaleza la evidencia puede ser cualitativa o cuantitativa.
    - **Cualitativa:** la evidencia deriva del análisis de una característica no cuantificada de una información relacionada con la determinación de un criterio de auditoría.

- **Cuantitativa:** la evidencia deriva del análisis de la muestra de la información relacionada con la determinación de un criterio de inspección, cuyos resultados cuantificados se proyectan entonces al conjunto de la población estudiada.

Tipos de evidencia (Organización Internacional de Estandarización, 2018)**:**

- **Física:** todo lo que puede ser contado, examinado, observado e inspeccionado, cualquier prueba obtenida mediante observación o inspección directa de los elementos tangibles.
- **Matemática:** consiste en los cálculos matemáticos ejecutados por el auditor, consiste en la validación de la exactitud matemática de ciertos documentos o registros, se utiliza a gran escala en las auditorías financieras.
- **Confirmativa:** es la originada en entidades que tienen una relación externa con el auditado, consiste en obtener la confirmación de uno o más elementos a través de una tercera parte.
- **Técnica:** Los resultados de análisis de pruebas técnicas u observaciones hechas a un sistema de información, consiste en validar el funcionamientos de un sistema de información
- **Analítica**: consiste en los resultados de los análisis y comparaciones de la relación entre los diferentes datos, toda evidencia recolectada por métodos estadísticos es analítica.

- **Documental:** es la evidencia de cualquier expediente o documento la fiabilidad de este tipo de pruebas depende de la naturaleza de los documentos, origen y el proceso de gestión de documentación.
- **Verbal:** es la evidencia recogida durante las interacciones entre el auditor y el personal del auditado, consiste en una entrevista con una persona que tenga conocimientos necesarios y las responsabilidades para llevar a cabo la operación que se está auditando.

Calidad de la evidencia (Organización Internacional de Estandarización, 2018):

- **Adecuada:**
  - ✓ **Relevante:** se refiere al grado de significación con los objetivos de la auditoría señalados, sirve como una entrada para que el auditor pueda evaluar la conformidad con un criterio de auditoría.
  - ✓ **Fiable:** se define como la calidad de la información que garantiza que está razonablemente exenta de errores y que representa fielmente.
- **Suficiente.-** Depende del juicio del auditor ya que es el que determinará con su experiencia si los recursos disponibles son suficientes y fiables.

Enfoque de una auditoría basada en riesgos:

El riesgo de detección aceptable corresponde a qué tan lejos el auditor está dispuesto a llegar en aceptar que sus conclusiones pueden ser sustancialmente erróneas, el riesgo de una auditoría se indica en la **Figura 21** :

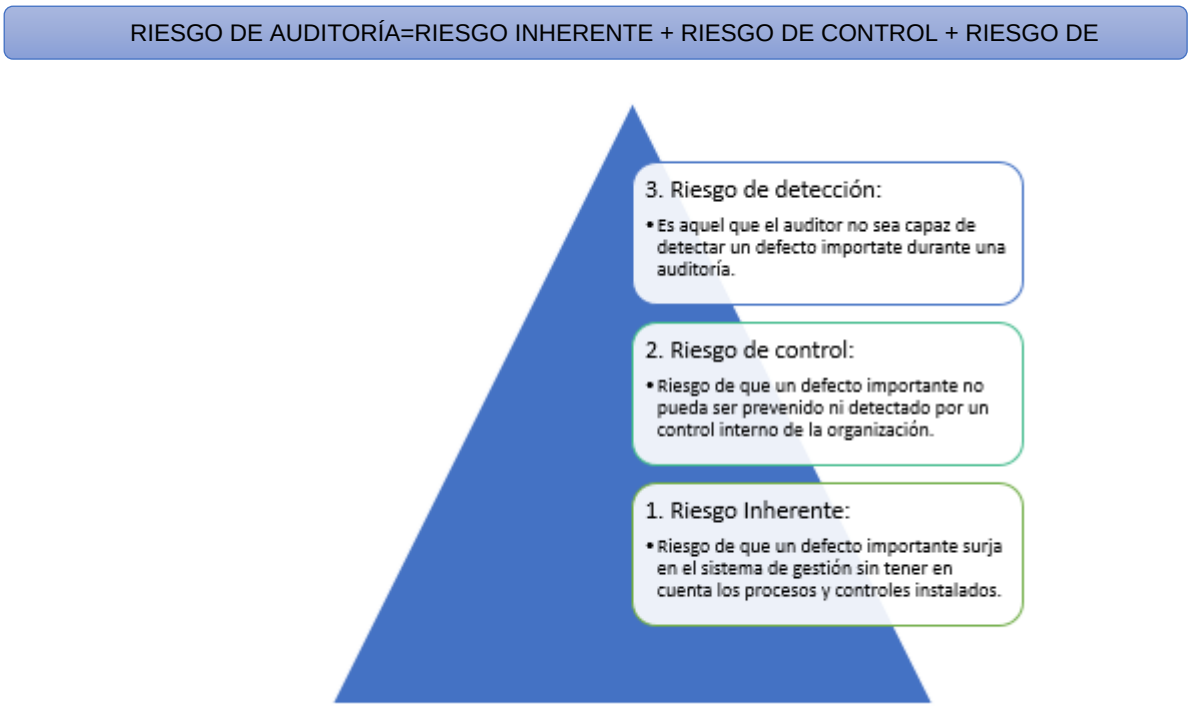

Figura 21. Auditoría basada en Riesgos
Fuente: ISO/IEC 19011

La fórmula de Riesgo de auditoría se puede obtener con el riesgo inherente más el riesgo de control más el riesgo de detección y así obtener resultados finales.

2.4.4. NIST 800-53

El NIST entre todas sus publicaciones, son particularmente relevantes las pertenecientes a la serie SP 800, destinados a la Seguridad de la Información. Esta serie se empezó a publicar en 1990 con la intención de proporcionar una identidad propia a las publicaciones en materia de seguridad, y contiene guías, pautas y propuestas tanto para el ámbito empresarial como industrial, gubernamental o académico. La serie NIST SP 800 es un conjunto de documentos de libre descarga que se facilita desde el gobierno

federal de los Estados Unidos, que describe las políticas de seguridad informática, procedimientos y directrices, que cubren hasta 256 salvaguardas y que las organiza en 18 categorías (National Institute of Standards and Technology NIST, 2019).

SP 800 53 que nos habla sobre los controles de seguridad y privacidad para los sistemas de información federal y organizaciones, que presenta todos los controles de seguridad que se recomiendan por el Instituto Nacional de Estándares y Tecnología, y cómo esta información puede ser utilizada junto con la norma ISO 27002 para diseñar e implantar todos los controles de seguridad especificados en la norma ISO 27001 dentro del Anexo A. Dentro de SP 800 53 tenemos tres capítulos y 10 apéndices, que son los siguientes (National Institute of Standards and Technology NIST, 2019):

- Capítulos: introducción, fundamentos y procesos.
- Apéndices: referencias, glosario, acrónimos, línea base de control de seguridad, seguridad y confiabilidad, catálogo de los controles de seguridad, sistema de gestión de seguridad de la información, plantilla de reposición y privacidad del catálogo de control.

La estructura es similar a la de la ISO 27001 sus 256 controles se encuentran organizados en 18 familias diferentes, cada uno que contiene los controles relacionados con esta norma. NIST SP 800 53 proporciona un mapeo de todos los controles de seguridad que se encuentran en la norma ISO 27001, por ejemplo:

- 1.2 La separación de las funciones asignadas a la CA 5 para la separación de tareas.

- 3.1 Información de copia de seguridad que se asigna al Sistema de Información, CP 9 copia de seguridad.

2.5. Estado del arte

Algunas de las empresas ecuatorianas que se han certificado con la norma ISO/IEC 27001 son Telconet Latam Ecuador, Deloitte Ecuador, Telefónica Ecuador y demás; con dicho certificado el objetivo del Sistema de Gestión de la Seguridad de la Información SGSI, es gestionar y proteger la información confidencial de sus clientes en todas sus formas, a través del cumplimiento de las políticas y procedimientos que garantizan que la información de los clientes se encuentre protegida (Deloitte, 2019) (TELCONET LATAM, 2018) (Telefónica, 2019).

En Ecuador dentro del sector público la única empresa que destaca es la Corporación Nacional de Telecomunicaciones CNT EP, la cual recibió de la Asociación Española de Normalización y Certificación (AENOR) la Certificación ISO 27001, que la reconoce como una empresa que “dispone de un sistema de Seguridad de la Información conforme a la Norma UNE-ISO/IEC 27001:2014” (CORPORACIÓN NACIONAL DE TELECOMUNICACIONES, 2017).

CAPÍTULO III

EVALUACIÓN TÉCNICA INFORMÁTICA AL SGSI DEL GAD PROVINCIAL DE IMBABURA

3.1. Inicio de la Evaluación Técnica Informática

El GAD provincial de Imbabura autorizó la solicitud para realizar el presente trabajo en las instalaciones conjuntamente con la DGTI, el 3 de julio de 2018 (Anexo 1), la persona encargada de realizar la presente evaluación técnica es la Ing. Jenny Alexandra Villegas Limaico siendo líder y auditor de la presente auditoría.

Se realiza la primera reunión con la persona delegada de la Dirección General de Tecnologías de la Información, el Ingeniero Jaime Eduardo Chuga Miño, se trata varios temas de introducción y se queda de acuerdo en los horarios, cronograma de revisión así como las autorizaciones de acceso a la información y demás evidencias.

Se revisa previamente el trabajo de titulación “Hacking Ético para detectar fallas en la Seguridad Informática de la Intranet del Gobierno Provincial de Imbabura e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la Norma ISO/IEC 27001:2005 y si se ha implementado de lo declarado en el mismo.

A. Objetivos

Los objetivos de la presente evaluación técnica son:

a. Determinar el grado de conformidad del SGSI a auditar.
b. Determinar el grado de conformidad de las actividades, procesos y productos con los requisitos y procedimientos del SGSI.

c. Evaluar la capacidad del SGSI para garantizar el cumplimiento de los requisitos legales y contractuales del GAD provincial de Imbabura.
d. Identificación de las áreas de mejora potencial del sistema de gestión.
e. Firma del Acuerdo de confidencialidad (Anexo 2).
f. Recomendar las posibles mejoras a realizar dentro de la institución y posterior certificación.

B. Alcance

El alcance de la evaluación técnica al SGSI, es aplicable en las oficinas del GAD provincial de Imbabura, ubicado en las calles Simón Bolívar y Miguel Oviedo esquina, de la ciudad de Ibarra, contemplando los activos de información conformado por la infraestructura tecnológica como son el sistema de cableado estructurado y los sistemas presentes en el centro de procesamiento de datos o Data Center.

Se especificará requerimientos para planificar, establecer, implementar, operar, monitorear, revisar, probar, mantener y mejorar el SGSI del GAD provincial de Imbabura para controlar los principales riesgos de la organización, basados en la norma ISO 27001, a continuación se detalla el alcance de la auditoría:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información
- Seguridad ligada a los recursos humanos
- Gestión de activos
- Control de accesos
- Cifrado

- Seguridad física y ambiental
- Seguridad operativa
- Seguridad en las telecomunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Relaciones con suministradores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio
- Cumplimiento

La duración prevista será de dos semanas (10 días laborables), el personal técnico de la DGTI está informado y presto para colaborar con la presente evaluación, además se debe tener en cuenta que el GAD provincial es una organización pequeña por lo que se tomará ciertas consideraciones en relación a tareas y funciones.

C. Situación actual GAD provincial de Imbabura

Según el Plan Estratégico Institucional aprobado para el 2014 al 2019 la situación actual es la siguiente:

Objetivos estratégicos *(GAD Provincial de Imbabura, 2019)*

- Gestión Ambiental
- Fomento de las Actividades Productivas y Agropecuarias
- Recursos Hídricos
- Vialidad
- Planificación Territorial

- Cooperación Internacional
- Grupos de Atención Prioritaria
- Participación Ciudadana
- Gestión Institucional

Misión

La Prefectura de Imbabura es la institución encargada de coordinar, planificar, ejecutar y evaluar el Plan de Desarrollo Provincial Participativo; fortaleciendo la productividad, la vialidad, el manejo adecuado de sus recursos naturales y promoviendo la participación ciudadana; a fin de mejorar la calidad de vida de sus habitantes. (GAD Provincial de Imbabura, 2019)

Visión

La Prefectura de Imbabura se consolida como una Institución de derecho público autónoma, descentralizada, transparente, eficiente, equitativa, incluyente y solidaria, líder del desarrollo económico, social y ambiental provincial. (GAD Provincial de Imbabura, 2019)

Orgánico estructural

El GAD provincial de Imbabura cuenta el orgánico estructural que se indica en la **Figura 22**, donde la DGTI forma parte de un proceso habilitante de apoyo el cual a la vez está subdivido en dos áreas.

Figura 22. Organigrama estructural de la Prefectura de Imbabura.
Fuente: http://www.imbabura.gob.ec/

Dirección General de Tecnologías de la Información

Misión.- Proveer y garantizar los servicios de tecnologías de la información de calidad, confiables y con alta disponibilidad en apoyo al cumplimiento de los objetivos estratégicos de la entidad, su representante y responsable es el Director (a) General de Tecnologías de la Información TI (GAD Provincial de Imbabura, 2019). Los subprocesos de nivel táctico dentro de la DGTI son:

Figura 23. Estructura básica DGTI
Fuente: http://www.imbabura.gob.ec/gaceta-oficial/gaceta-oficial/file/461-gaceta-oficial-n-007-2018.html

Atribuciones y Responsabilidades de la Dirección General de Tecnologías de la Información (GAD Provincial de Imbabura, 2019)***.***

a) Asesor a las autoridades, directivos y servidores de la Institución en temas relacionados con sistemas, computación, informática y comunicaciones.
b) Dirigir, evaluar la gestión de la Dirección General de Tecnologías de la Información.
c) Coordinar la implementación de sistemas de información y tecnológicos de las unidades o procesos organizacionales de la entidad.
d) Proponer políticas para la gestión de los recursos tecnológicos.
e) Poner a consideración y aprobaciones de la máxima autoridad los planes tecnológicos y de contingencia institucional.
f) Dirigir, elaborar y evaluar el Plan Operativo Anual y el Plan Anual de compras de la Dirección General de Tecnologías de la Información.

g) Evaluar la calidad de productos y servicios tecnológicos para la generación de un Plan de Mejoramiento Continuo de la Institución.

h) Coordinar la ejecución de los planes tecnológicos de contingencia institucional.

i) Asesorar a los niveles directivos en los procesos de adquisición, mantenimiento y reemplazo de equipos de computación y comunicación.

j) Para todos los bienes tecnológicos identificar y registrar los bienes tecnológicos y de comunicación para la prestación de servicios incluidos los de software de base o de aplicación y versiones de actualización.

k) Las demás funciones delegadas por el Prefecto o Prefecta Provincial.

Productos y servicios (GAD Provincial de Imbabura, 2019)**.**

- Plan Informático Estratégico de Tecnología.
- Políticas y procedimientos de organización de tecnología
- Plan de Contingencia.
- Políticas y reglamentación para el cumplimiento de Normas de Control Interno.
- Servicios de infraestructura, redes y comunicaciones.

3.2. Etapa 1 de Evaluación Técnica Informática.

A. Objetivos de la etapa 1

- Auditar la documentación del sistema de gestión de la Institución.
- Evaluar si las auditorías internas y la revisión por la Dirección están siendo planificadas y llevadas a cabo.

B. Revisión documental del Sistema de Gestión de Seguridad de la Información (SGSI) del GAD provincial de Imbabura.

El trabajo de grado con tema “HACKING ÉTICO PARA DETECTAR FALLAS EN LA SEGURIDAD INFORMÁTICA DE LA INTRANET DEL GOBIERNO PROVINCIAL DE IMBABURA E IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BASADO EN LA NORMA ISO/IEC 27001:2005”, realizado por Fernando Ortiz en el año 2015, diseño e implementación del SGSI basado en la norma ISO/IEC 27001:2005, en su capítulo 5 (Anexo 4).

Los documentos encontrados para realizar la evaluación técnica informática son los siguientes:

- Política se seguridad de la Información (Anexo 5).
- Normativa de acuerdos con terceras partes (Anexo 6).
- Normativa de administración de incidentes de seguridad de la información (Anexo 7).
- Normativa de administración de seguridad de la red (Anexo 8).
- Normativa de buenas prácticas de seguridad de la información (Anexo 9).
- Normativa de control de acceso (Anexo 10).
- Normativa de control de cambios (Anexo 11).
- Normativa de gestión de continuidad del negocio (Anexo 12).
- Normativa de mantenimiento de equipos e instalaciones (Anexo 13).
- Normativa de protección contra software malicioso (Anexo 14).

- Normativa de requisitos de seguridad de la información para nuevas instalaciones y adquisición de software (Anexo 15).
- Normativa de roles y responsabilidades de seguridad de la información (Anexo 16).
- Normativa de segregación de funciones (Anexo 17).
- Normativa de seguridad de la información para la gestión del recurso humano (Anexo 18).
- Normativa de seguridad de la información (Anexo 19).
- Normativa de software licenciado (Anexo 20).
- Normativa de suministro eléctrico (Anexo 21).
- Normativa de uso de internet (Anexo 22).
- Procedimiento de contacto con grupos de interés en materia de seguridad de la información (Anexo 23).
- Procedimiento de disposición de medios de almacenamiento y equipos de cómputo (Anexo 24).
- Procedimiento de generación y almacenamiento de backups (Anexo 25).
- Procedimiento de protección y revisión de registros de auditoría (Anexo 26).
- Procedimiento de seguridad física y ambiental del data center (Anexo 27).
- Procedimiento para la creación, modificación y eliminación de acceso de usuarios en sistemas (Anexo 28).
- Procedimiento para la identificación y clasificación de activos de información (Anexo 29).

- Estándar de contraseñas para usuarios y administradores (Anexo 30).
- Estándar de etiquetado de activos de información (Anexo 31).

C. Declaración de aplicabilidad del SGSI.

Considerando las funciones de la DGTI y sus responsabilidades se describe en el (Anexo 3) los controles implementados en el SGSI del GAD provincial de Imbabura.

D. Resultados del Informe de la etapa 1

Se anexa a detalle el informe completo de la etapa 1 en el (Anexo 37)

3.3. Etapa 2 de la Evaluación Técnica Informática

1. Objetivos de la etapa 2

- Conformidad o no conformidad con todos los requisitos de la norma ISO 27001.
- El SGSI está implementado con eficiencia en la organización.

2. Cronograma

El cronograma que se plantea en las reuniones mantenidas con el encargado para llevar a cabo la evaluación técnica Informática al SGSI de detalla en la **Figura 27**.

N°	ACTIVIDADES	LUGAR	DELEGADO DGTI	RESPONSABLE	MARZO									
					11	12	13	14	15	18	19	20	21	22
1	Revisión capítulo 4 Contexto de la organización (ISO 27001)	DGTI Ibarra	Jaime Chuga	Jenny Villegas										
2	Revisión capítulo 5 Liderazgo (ISO 27001)	DGTI Ibarra	Jaime Chuga	Jenny Villegas										
3	Revisión capítulo 6 Planificación (ISO 27001)	DGTI Ibarra	Jaime Chuga	Jenny Villegas										
4	Revisión capítulo 7 Soporte (ISO 27001)	DGTI Ibarra	Jaime Chuga	Jenny Villegas										
5	Revisión capítulo 8 Operación (ISO 27001)	DGTI Ibarra	Jaime Chuga	Jenny Villegas										
6	Revisión capítulo 9 Evaluación de desempeño (ISO 27001)	DGTI Ibarra	Jaime Chuga	Jenny Villegas										
7	Revisión capítulo 10 Mejora (ISO 27001)	DGTI Ibarra	Jaime Chuga	Jenny Villegas										

Figura 24. Cronograma Evaluación Técnica Informática al SGSI del GAD provincial de Imbabura

3. Evidencias de la evaluación del anexo A ISO 27001

Las evidencias se encuentran en la carpeta *“Anexos”* que se adjuntará en medio magnético a la presente de cada uno de los registros verificables por motivos de confidencialidad de la información.

4. Hallazgos de la evaluación del anexo A ISO 27001

Se adjunta el cuadro con los hallazgos detallado en el (Anexo 38), donde se indica en una tabla los detalles de cada control, los nueve campos que contiene la plantilla utilizada para la ETI son: sección, requerimiento ISO 27001, estado, recurso, preguntas, comentarios, evidencia y conformidad, que se los describe a continuación:

- **Sección:** indica la sección de norma ISO 27001 a evaluar.
- **Requerimientos ISO 27001:** descripción del control ISO 27001 revisión 2013.
- **Estado:** se utilizó la escala indica en la **Figura 25** para determinar el estado de aplicación del SGSI en el GAD provincial de Imbabura.

Estado	Significado
? Desconocido	No ha sido verificado
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO\IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.

Figura 25. Escala de medición ISO 27001 y 27002 para la ETI al SGSI

- **Recurso:** puede ser documentación u observación se puede escoger de la lista desplegable.
- **Preguntas:** son cuestiones que ayudan al control a describir mejor lo que se requiere en la institución.
- **Comentarios:** son las respuestas a las preguntas planteadas.
- **Evidencia:** Anexo de evidencia para cumplir o no con el control.
- **Conformidad:** es la conformidad o no conformidad del control.

- **Recomendación:** son las recomendaciones individuales de cada control a implementar para poder cumplir las conformidades del SGSI institucional.

Los resultados del Check de los controles realizados para indicar el estado de implementación del SGSI son los detallados en la **Figura 26** , para más detalle revisar el (Anexo38).

Proporción de Hallazgos		
Conformidad	26%	7
No conformidad	74%	20

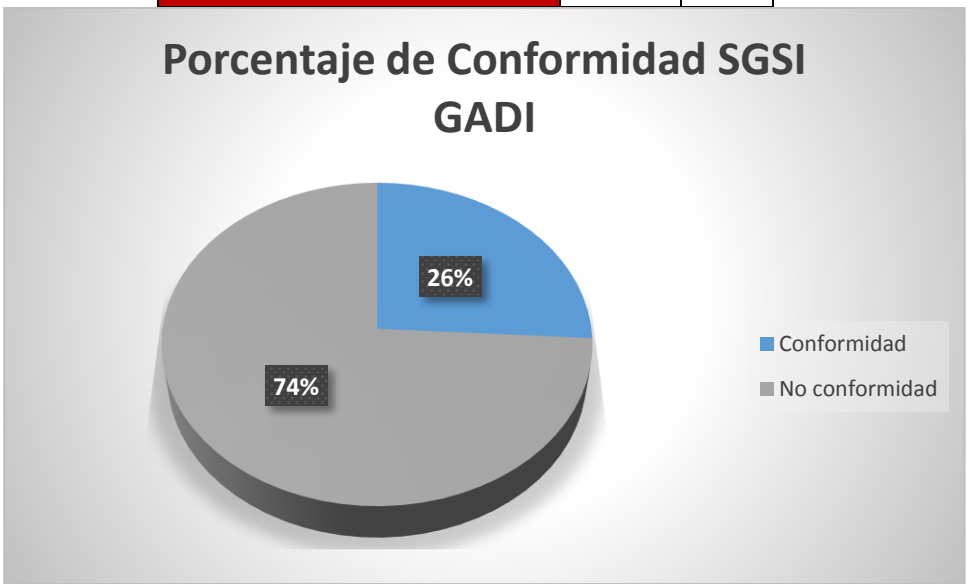

Figura 26. Porcentaje de conformidad del SGSI de GAD provincial de Imbabura

Además se detalla los resultados del estado de implementación del SGSI del GAD provincial de Imbabura en la **Figura 27**, para más detalle revisar el (Anexo38).

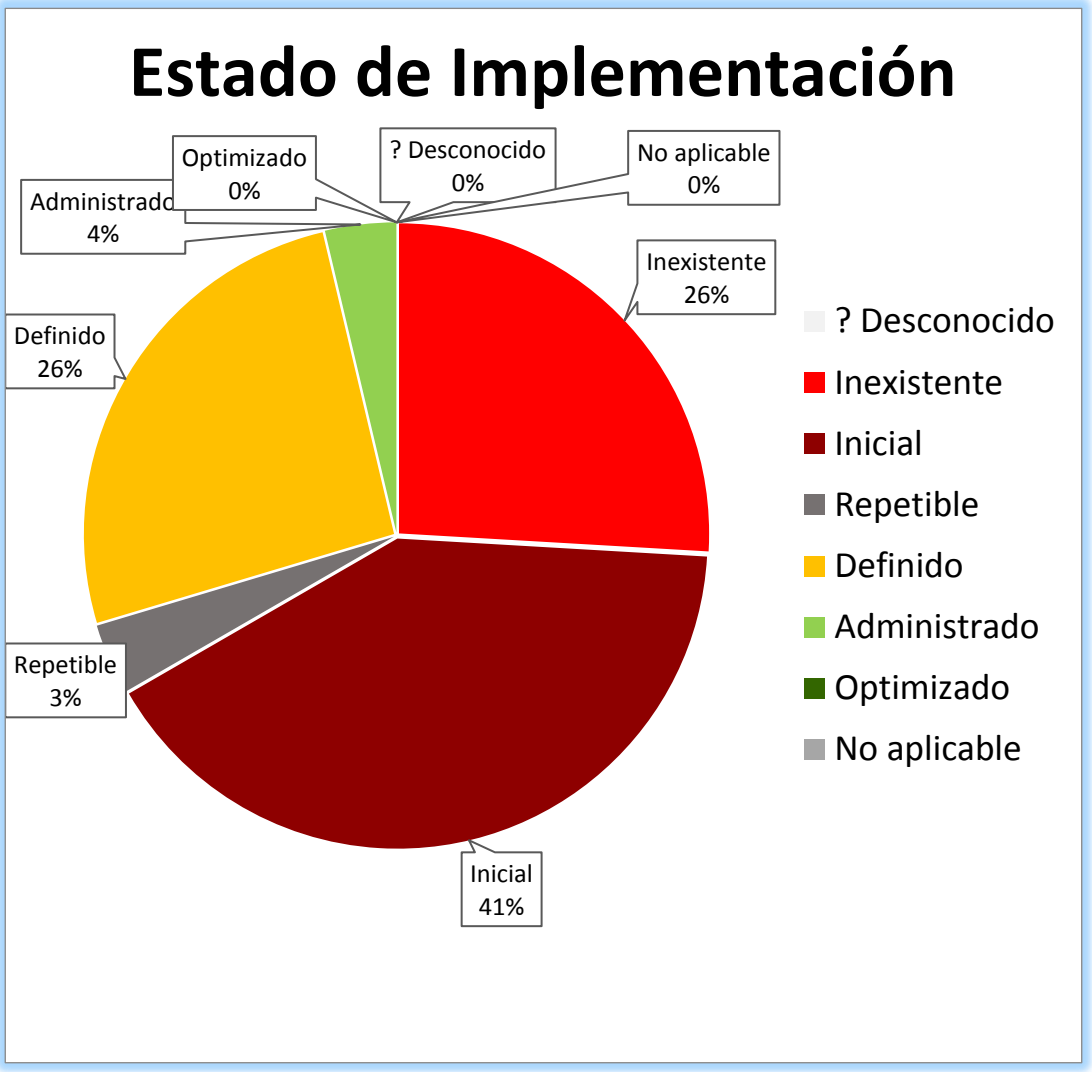

Figura 27. Estado de implementación del SGSI de GAD provincial de Imbabura

CAPÍTULO IV

INFORME FINAL EVALUACIÓN TÉCNICA INFORMÁTICA AL GAD PROVINCIAL DE IMBABURA

REPORTE FINAL

Jenny Villegas

Gobierno Autónomo Descentralizado Provincial de Imbabura

1-29 de Marzo 2019

29 de marzo de 2019

Gobierno Autónomo Descentralizado Provincial de Imbabura

Ibarra-Ecuador

Estamos presentando los resultados de nuestra auditoría de TI "**EVALUACIÓN TÉCNICA INFORMÁTICA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL GAD PROVINCIAL DE IMBABURA EN BASE DE LA NORMA ISO/IEC 27001:2013"** que cubre el período de 1-29 de marzo de 2019. El informe incluye nuestras conclusiones y recomendaciones posteriores a la verificación del cumplimiento de los objetivos de control de la norma ISO 27001:2013 al SGSI institucional. Creemos que la evidencia obtenida proporciona una base razonable para nuestras conclusiones y hallazgos con respecto a los objetivos de la auditoría.

4.1. TABLA DE CONTENIDOS

4.2. INTRODUCCIÓN

Descripción del negocio.

El GAD provincial de Imbabura es la institución encargada de coordinar, planificar, ejecutar y evaluar el Plan de Desarrollo Provincial Participativo; fortaleciendo la productividad, la vialidad, el manejo adecuado de sus recursos naturales y promoviendo la participación ciudadana; a fin de mejorar la calidad de vida de sus habitantes, se encuentra ubicado en la ciudad de Ibarra en las calles Bolívar 7-44 y Oviedo esquina.

Descripción de alto nivel de la infraestructura de TI aplicable

El GAD provincial cuenta desde el año 2013 con nueva infraestructura de TI, que se detalla en el trabajo de grado "OPTIMIZACIÓN DE LA ADMINISTRACIÓN DE LA RED E IMPLEMENTACIÓN DE SERVIDORES DE SERVICIOS PARA EL GOBIERNO PROVINCIAL DE IMBABURA", donde se diseña e implementa un datacenter de tipo TIER I para la institución, la cual es aplicable ahora para la evaluación técnica Informática.

Declaración de propósito de alto nivel

La evaluación técnica Informática se realizó de manera general con todos los controles de la norma ISO 27001 e ISO 27002 al SGSI o Sistema de Gestión de Seguridad de la Información del GAD provincial de Imbabura.

Área de TI que es el objeto de la auditoría

La Dirección General de Tecnologías de la Información

4.3. RESUMEN EJECUTIVO

Una vez analizada y conocida de la situación actual del GAD provincial de Imbabura y, definido el enfoque de auditoría a ser utilizado, así como los responsables de la parte tecnológica y del negocio; se procede con la evaluación técnica informática.

Teniendo como objetivo principal determinar el cumplimiento de los controles del SGSI institucional en base a los controles de la norma ISO 27001.Los resultados son bajos, por lo que la situación en la que se encuentra la institución es crítica se detalla los porcentajes en la **Tabla *5***, para lo cual se debe tomar medidas correctivas urgentes en el ámbito de seguridad de la información detallado en la última columna de la matriz de hallazgos en el campo “Recomendaciones”.

Tabla 5

Ejemplo de catálogo de vulnerabilidades.

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	**0%**	**0%**
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	**26%**	**16%**
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	**41%**	**38%**
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	**4%**	**33%**
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	**26%**	**11%**
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	**4%**	**0%**
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	**0%**	**0%**
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	**0%**	**3%**
	Total	100%	100%

4.4. ALCANCE DE AUDITORÍA

La evaluación técnica informática se basa en la norma ISO 27001, ISO 27002 e ISO 19011, por lo que se debe planificar y aplicar para obtener evidencia suficiente, relevante y válida, obteniendo una base razonable para las conclusiones, opiniones y hallazgos de auditoría.

El alcance de la evaluación técnica al SGSI, es aplicable en las oficinas del GAD provincial de Imbabura, ubicado en las calles Simón Bolívar y Miguel Oviedo esquina, de la ciudad de Ibarra, contemplando los activos de información conformado por la infraestructura tecnológica como son el sistema de cableado estructurado y los sistemas presentes en el centro de procesamiento de datos o Data Center.

Se especificará requerimientos para planificar, establecer, implementar, operar, monitorear, revisar, probar, mantener y mejorar el SGSI del GAD provincial de Imbabura para controlar los principales riesgos de la organización, basados en la norma ISO 27001.

4.5. OBJETIVO DE AUDITORIA

El objetivo de auditoría es determinar las conformidades y no conformidades del SGSI implementado en el GAD provincial de Imbabura para proporcionar una seguridad a sus usuarios y funcionarios.

4.6. METODOLOGÍA DE AUDITORÍA

4.6.1. Pre-auditoría / planificación de la auditoría

Para determinar el alcance y objetivos de la presente evaluación técnica, se realizó previo la planificación de la auditoría, que incluyó la obtención, registro y comprensión del GAD PROVINCIAL DE IMBABURA, tales como la misión, operación, negocio y tecnología de soporte; identificando las necesidades operacionales, legales y reglamentarios de la organización auditada infraestructura de TI 's mediante la revisión de la documentación pertinente. Hemos llevado a cabo visitas en sitio de TI y áreas operativas donde se realizó una evaluación de alto nivel.

La planificación de auditoría incluyó:

- Obtención y revisión de políticas y procedimientos
- Contratos obtenidos y revisados con terceros
- Identificar los factores críticos de éxito para las operaciones de TI de misión crítica.

- Identificar criterios de auditoría, evaluar materialidad y determinar la adecuación de los controles indicados.

Se desarrolló objetivos de auditoría en relación con el control identificado y los objetivos operativos además se desarrolló la estrategia de auditoría en relación con el alcance y los objetivos de la auditoría.

4.6.2. La realización de la auditoría

La evaluación técnica informática se realizó de acuerdo con los controles de la norma ISO 27001, y las buenas prácticas publicadas por los documentos de ITAF de ISACA. La metodología que se utilizó es la indicada en la ISO 19011 como base para realizar el presente proyecto.

4.7. RESULTADOS DE LA AUDITORÍA O HALLAZGOS DE AUDITORÍA

El propósito de esta sección es proporcionar una explicación detallada de los hallazgos de la auditoría, las recomendaciones y las respuestas de la administración.

Tabla 6

Hallazgos Auditoría

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
4	**Contexto de la organización**							
4,1	**Comprensión de la organización y de su contexto**							
4,1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Definido	DOCUMENTACIÓN	¿Están identificados los objetivos del Sistema de Gestión de la Seguridad de la Información? ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información? ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	SI SI SI		CONFORMIDAD	Actualizar, legalizar y difundir el SGSI institucional
4,2	**Comprensión de las necesidades y expectativas de las partes interesadas**							

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Definido	DOCUMENTACIÓN	¿Existe un documento en el que se han determinado cuáles son las partes interesadas para el SGSI?	SI		CONFORMIDAD	Actualizar, legalizar y difundir el SGSI institucional
4.2 (b)	Determinar los requerimientos y obligaciones relevantes de seguridad de la información	Repetible	DOCUMENTACIÓN	¿Existe un documento con el listado de requisitos de las partes interesadas para el SGSI? ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	SI SI		CONFORMIDAD	Actualizar, legalizar y difundir el SGSI institucional
4,3	**Determinación del alcance del SGSI**							
4,3	Determinar y documentar el alcance del SGSI	Definido	DOCUMENTACIÓN	¿Se ha determinado el alcance del SGSI y se conserva información documentada? ¿Dentro del alcance del SGSI se ha considerado las interfaces y dependencias entre las actividades realizadas por la organización y por otras organizaciones (documentado)?	SI SI		CONFORMIDAD	Actualizar, legalizar y difundir el SGSI institucional
4,4	**SGSI**							

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
4,4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estándar	Inicial	DOCUMENTACIÓN	¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	Si está establecido, más no implementado en su totalidad y no se revisa o actualiza de forma planificada.		NO CONFORMIDAD	Actualizar, legalizar y difundir el SGSI institucional además de implementar un plan de actualización al menos anual.
5	**Liderazgo**							
5,1	**Liderazgo y compromiso**							
5,1	La administración debe demostrar liderazgo y compromiso por el SGSI	Inexistente	OBSERVACIÓN	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI? ¿La dirección comunicar la importancia del SGSI ? ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI? ¿La dirección apoya a las personas para contribuir a la eficiencia y mejora continua del SGSI ?	NO NO NO SI		NO CONFORMIDAD	Asignar el recurso material y humano necesario para el cumplimiento del SGSI institucional. Campaña de concienciación sobre la importancia del SGSI y su cumplimiento. Realizar Auditorías Internas para verificar la eficacia del SGSI institucional.
5,2	**Política**							

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
5,2	Documentar la Política de Seguridad de la Información	Administrado	DOCUMENTACIÓN	¿Se ha definido una Política de la Seguridad de la Información? ¿Se ha establecido un marco que permita el establecimiento de objetivos? ¿Se ha establecido un compromiso de cumplir con los requisitos aplicables relacionados con la seguridad de la información? ¿Se mantiene información documentada de la política del SGSI y de sus objetivos? ¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?	SI SI NO SI NO		NO CONFORMIDAD	Se debe actualizar, legalizar y difundir la política de seguridad de la información. Realizar campaña de concienciación sobre la importancia del SGSI y su cumplimiento.
5,3	**Roles, responsabilidades y autoridades en la organización**							
5,3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Inexistente	OBSERVACIÓN	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información? ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?	NO		NO CONFORMIDAD	Asignación legal o contratación de personal exclusivo para el área de Seguridad de la Información, indicando sus responsabilidades. Comunicar a los interesados sobre las responsabilidades y autoridades para la Seguridad de la Información, mediante campaña de concienciación sobre la Seguridad de la

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
								Información u memorando informativos.
6	**Planificación**							
6,1	**Acciones para tratar los riesgos y oportunidades**							
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportunidades	Definido	DOCUMENTACIÓN	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?	SI		CONFORMIDAD	Actualizar, legalizar la metodología y difundir sobre el análisis y gestión de riesgos de los activos.
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Definido	DOCUMENTACIÓN	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?	SI		CONFORMIDAD	Actualizar, legalizar el proceso de análisis de riesgos de la seguridad de la información además de difundirlo.

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Definido	DOCUMENTACIÓN	¿Se ha definido un proceso de tratamiento de riesgos? ¿Se han establecido criterios para elaborar una declaración de aplicabilidad? ¿Se ha definido un plan para el tratamiento de riesgos? ¿Se mantiene información documentada de los puntos anteriores?	SI SI SI SI		CONFORMIDAD	Actualizar, legalizar el proceso de tratamiento o gestión de riesgos de la seguridad de la información además de difundirlo.
6,2	**Objetivos de seguridad de la información y planificación para su consecución**							

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
6,2	Establecer y documentar los planes y objetivos de la seguridad de la información	Definido	DOCUMENTACIÓN	¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio? ¿Se ha tomado en cuenta los requisitos de seguridad de la información aplicables, y los resultados de la apreciación de riesgos y el tratamiento del riesgo? ¿Se ha comunicado y actualizados los objetivos de seguridad de la información? "¿Los objetivos de la Seguridad de la Información están planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación" ¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?	SI SI NO NO NO		NO CONFORMIDAD	Actualizar, legalizar y difundir los objetivos de la seguridad de la información; además de integrarlos en los procesos de la institución.
7	**Soporte**							

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
7,1	**Recursos**							
7,1	Determinar y asignar los recursos necesarios para el SGSI	Inexistente	OBSERVACIÓN	¿Se identifican y asignan los recursos necesarios para el SGSI?	NO		NO CONFORMIDAD	Contratar personal o asignar recurso necesario exclusivo encargado del SGSI institucional.
7,2	**Competencia**							
7,2	Determinar, documentar hacer disponibles las competencias necesarias	Inexistente	OBSERVACIÓN	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad? ¿Se mantiene información actualizada sobre la competencia del personal?	NO		NO CONFORMIDAD	Legalizar y difundir la competencia del personal sobre Seguridad de la Información
7,3	**Concienciación**							
7,3	Implementar un programa de concienciación de seguridad	Inexistente	OBSERVACIÓN	¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información? ¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?	NO SI		NO CONFORMIDAD	Campaña de concienciación sobre seguridad de la información y las consecuencias que puede producir el no seguir tip de seguridad.
7,4	**Comunicación**							
7,4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	Inicial	DOCUMENTACIÓN	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno? ¿Existe un proceso	NO NO		NO CONFORMIDAD	Actualizar, legalizar y difundir la política de seguridad de la información indicando los responsables. Implementar campaña de concienciación sobre Seguridad de la Información.

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
				para comunicar las deficiencias o malas prácticas en la seguridad de la Información?				
7,5	**Información documentada**							
7.5.1	Proveer documentación requerida por el estándar más la requerida por la organización	Inicial	OBSERVACIÓN	¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluyendo? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluyendo registros -Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones técnicas etc.)	NO Solamente el archivo de la secretaría de la DGTI.		NO CONFORMIDAD	Implementar, legalizar y difundir el proceso de control documental incluyendo los de origen externo
7.5.2	Proveer un título, autor, formato consistente, revisión y aprobación a los documentos	Inicial	OBSERVACIÓN	¿Cuándo se crea y actualiza la información documentada, la organización asegura la identificación,	NO Solamente el archivo de la secretaría de la DGTI.		NO CONFORMIDAD	Implementar, legalizar y difundir el proceso de control documental incluyendo los de origen externo

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
				formato, revisiones y aprobaciones?				
7.5.3	Mantener un control adecuado de la documentación	Inicial	OBSERVACIÓN	"¿Existe un control documental donde se verifica? -Quien publica el documento-Quien lo autoriza y como se revisan -Formatos y Soportes de publicación -Su almacenamiento y protección" ¿Se controlan los documentos de origen externo?	SI NO NO NO SI		NO CONFORMIDAD	Implementar, legalizar y difundir el proceso de control documental incluyendo los de origen externo
8	**Operación**							
8,1	**Planificación y control operacional**							
8,1	Planificar, implementar, controlar y documentar el proceso de gestión de riesgos del SGSI (Tratamiento de riesgos)	Inicial	DOCUMENTACIÓN	¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado? ¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad? ¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la	SI SI NO NO		NO CONFORMIDAD	Actualizar, legalizar y difundir el proceso de análisis, evaluación y tratamiento del riesgo en la Seguridad de la Información finalmente documentarlo.(bitácoras)

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
				Información ante cambios realizados? ¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información?				
8,2	**Apreciación de los riesgos de seguridad de la información**							
8,2	Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios	Inicial	DOCUMENTACIÓN	¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique?-El propietario del riesgo-La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia	NO		NO CONFORMIDAD	Actualizar, legalizar y difundir el proceso de análisis y evaluación del riesgo y finalmente documentarlo.(bitácoras)
8,3	**Tratamiento de los riesgos de seguridad de la información**							

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
8,3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Inicial	DOCUMENTACIÓN	¿Se ha implementado un plan de tratamiento de riesgos dónde?-Los propietarios del riesgo están informados y han aprobado el plan-Se documentan los resultados "¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación? ¿Se documenta el nivel de aplicación de todos los controles a aplicar?"	SI NO NO		NO CONFORMIDAD	Actualizar, legalizar y difundir el plan de tratamiento del riesgo y finalmente documentarlo.
9	**Evaluación del desempeño**							
9,1	**Seguimiento, medición, análisis y evaluación**							
9,1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	Inicial	DOCUMENTACIÓN	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información? ¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto	SI NO		NO CONFORMIDAD	Realizar un proceso de monitoreo a los aspectos claves de los controles del SGSI, aplicarlo, tratarlo y documentarlo

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
				de los procesos como de la Seguridad de la Información?				
9,2	**Auditoría interna**							
9,2	Planificar y realizar una auditoría interna del SGSI	Inexistente	OBSERVACIÓN	¿Se ha realizado Auditorías Internas y asignado responsables? ¿Se ha establecido una programación de Auditorías Internas y asignado responsables? ¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría? ¿Se conserva información documentada como evidencia de la implementación del programa(s) de auditoría y de los resultados de esta?	NO NO NO		NO CONFORMIDAD	Se debe planificar las Auditorías Internas al SGSI, mínimo cada seis meses, asignando los responsables, que cuenten con los conocimientos del mismo, y que se cumpla con los procesos y procedimientos de documentación.
9,3	**Revisión por la dirección**							
9,3	La administración realiza una revisión periódica del SGSI	Inicial	OBSERVACIÓN	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica? ¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones	NO NO		NO CONFORMIDAD	Se debe contar con las firmas de las autoridades y se debe mantener al menos una vez al año actualizado el SGSI. Se debe mantener documentada los informes y revisiones del SGSI (bitácoras).

CONTINÚA

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios	Evidencia	Conformidad	Recomendación
				sobre los aspectos cruciales para el SGSI?				
10	**Mejora**							
10,1	**No conformidad y acciones correctivas**							
10,1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	Inicial	OBSERVACIÓN	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento? ¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma? ¿Existe información documentada de evidencia de no conformidad y acciones correctivas?	NO NO NO		NO CONFORMIDAD	Implementar un procedimiento para identificar y registrar las no conformidades y el tratamiento. Implementar un proceso de documentación.
10,2	**Mejora continua**							
10,2	Mejora continua del SGSI	Inexistente	OBSERVACIÓN	¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?	NO		NO CONFORMIDAD	Actualizar, legalizar y difundir el SGSI institucional.

Los resultados del capítulo 3 de los cuales se anexan a este documento y se detallan en el presente informe final de la evaluación técnica informática, destacando de los 114 controles evaluados correspondientes a la norma ISO-IEC 27002:2013 los siguientes detalles:

Tabla 7

Porcentaje de hallazgo ISO 27001

Proporción de Hallazgos		
Conformidad	7%	8
No conformidad	93%	103
No aplicables		3
TOTAL		**114**

Como se indica en la siguiente figura es un porcentaje bajo de cumplimiento:

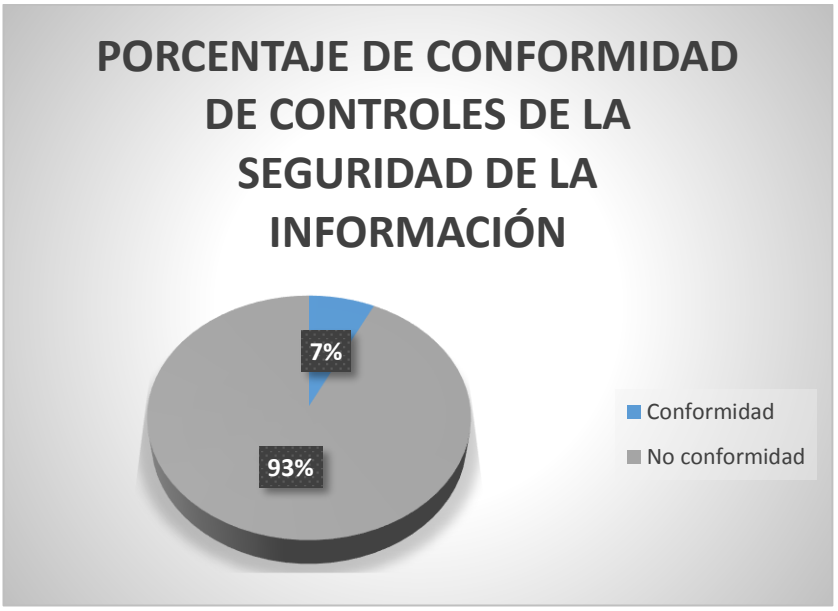

Figura 28. Gráfico del porcentaje de cumplimiento de la norma ISO 27001

4.8. CONCLUSIÓN DE AUDITORÍA

Teniendo como un promedio general del 7% del cumplimiento de los controles, siendo un porcentaje bajo de cumplimiento, cabe indicar que varios de los controles no cumplen, pero varios controles solo cumplen parcialmente ya que existe documentos desactualizados o no difundidos, al momento de realizar la evaluación técnica de pre-certificación, además se pudo constatar que el personal no tiene conciencia de la importancia de la seguridad de la información en la institución.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Se realizó la evaluación técnica informática al sistema de gestión de seguridad de la información del GAD provincial de Imbabura, validando el cumplimiento de la norma ISO/IEC 27001 con satisfacción y colaboración de los funcionarios del GAD.
- Se detalla el informe con los resultados finales de cumplimiento, que son deficiente, denotando la falta de atención a la seguridad de la información en la organización.
- La evaluación técnica informática realizada ha sido el primer paso en la optimización del SGSI institucional, que permitirá en el futuro la certificación frente a un organismo reconocido.
- La falta de personal oficialmente encargado dentro de la estructura organizacional limita la implementación de un SGSI y resta importancia a la seguridad de la información en la institución.
- La norma ISO 27001 proporciona los requisitos para establecer, implementar, mantener y mejorar un SGSI basado en la integridad, disponibilidad y confidencialidad de la información en una organización.

5.2. Recomendaciones

- Es necesario actualizar y documentar regularmente cualquier cambio en lo que se refiere a seguridad de la información, sean procesos, procedimientos, políticas o buenas prácticas.
- Se debe capacitar a los funcionarios del GAD en Seguridad de la Información mediante una campaña que les permita conocer el tema.
- Dentro del presupuesto anual del GAD se debe incluir un rubro que permita cubrir una revisión del funcionamiento del SGSI, si no es posible realizar esta tarea de forma anual se debe considerar realizarlo con frecuencia no mayor a tres años.
- Como se evidenció en los resultados, considerando que el GAD provincial es una institución pública, se debe cumplir con los requisitos de seguridad de la información, por lo que se debería asignar presupuesto para contratar o asignar formalmente una persona como oficial de seguridad y conformar el Comité Técnico Informático.
- Los resultados del presente trabajo son críticos por lo que se sugiere que se oficialice y actualice; los procesos y procedimientos del SGSI en base a las recomendaciones que constan en el informe final.

REFERENCIAS BIBLIOGRÁFICAS

Asociación de Auditoría y Control de Sistemas de Información. (2019). *ISACA- Asociación de Auditoría y Control de Sistemas de Información*. Obtenido de https://www.isaca.org/pages/default.aspx

Baquero, A. (2017). *Libro Informática, Glosario de Términos y Siglas.* Mc. Grow Hill.

CORPORACIÓN NACIONAL DE TELECOMUNICACIONES. (18 de Diciembre de 2017). *Corporación Nacional de Telecomunicaciones*. (Noticias Sala de Prensa) Recuperado el 2019, de CNT: https://corporativo.cnt.gob.ec/la-gestion-de-seguridad-de-la-informacion-de-la-cnt-obtiene-certificacion-internacional/

Deloitte. (2019). *Deloitte Ecuador obtiene Certificación ISO 27001*. Obtenido de https://www2.deloitte.com/ec/es/pages/deloitte-analytics/articles/certificacion-iso-27001-deloitte-ecuador.html

Dirección General de Modernización Administrativa. (2019). *MAGERIT.* Obtenido de Versión 3.0: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

EcuRed. (2019). *Definición Seguridad Informática.* Obtenido de https://www.ecured.cu/Seguridad_Inform%C3%A1tica

Exteriores, S. d. (2019). *Secretarìa de Relaciones Exteriores/Guìa TÈcnica para la Elaboración de Manuales de Procedimientos.* Obtenido de Definición de términos.: https://sre.gob.mx/images/stories/docnormateca/dgpop/guias/guia01.pdf

GAD Provincial de Imbabura. (2019). *GACETA OFICIAL.* Obtenido de http://www.imbabura.gob.ec/gaceta-oficial/gaceta-oficial/file/461-gaceta-oficial-n-007-2018.html

GAD Provincial de Imbabura. (2019). *Prefectura de Imbabura.* Obtenido de http://www.imbabura.gob.ec/institucion/mision-vision.html

INCIBE - Instituto Nacional de Ciberseguridad. (2019). *Metodologías de Análisis de Riesgos*. Obtenido de https://www.incibe.es/extfrontinteco/img/File/empresas/dosieres/plan_director_de_seguridad/plan_director_de_seguridad_metodologias_analisis_de_riesgos.pdf

ISACA Framework. (2018). *COBIT 5* . Obtenido de Introducción: http://www.isaca.org/COBIT/Pages/COBIT-5.aspx

ISO/IEC 27002. (Mayo de 2017). Tecnología de la Información, Técnicas de seguridad, Código de prácticas para los controles de seguridad de. AENOR Internacional, S.A.U. bajo licencia de la Asociación Española de Normalización.

MACHADO LLOREDA, B. J. (2018). *AUDITORIA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS DE INFORMACIÓN BAJO EL ESTÁNDAR COBIT EN LA INSTITUCIÓN EDUCATIVA ESCUELA NORMAL SUPERIOR DE QUIBDÓ.* Obtenido de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18042/4/26274426.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2013). *Gobierno Electrónico de Ecuador.* Obtenido de Esquema Gubernamental de Seguridad de

la Información: https://www.gobiernoelectronico.gob.ec/esquema-gubernamental-de-seguridad-de-la-informacion-egsi/

National Institute of Standards and Technology NIST. (2019). *El Instituto Nacional de Estándares y Tecnología*. Obtenido de https://www.nist.gov/

Organización Internacional de Estandarización. (2018). *Directrices para Auditar Sistemas de Gestión*. Obtenido de ISO/IEC 19011: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0060855

Organización Internacional de Estandarización. (2018). *Gestión del Riesgo - Directrices*. Obtenido de ISO/IEC 31000: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0061478

Organización Internacional de Estandarización. (2018). *ISO/IEC 27005.* Obtenido de ISO/IEC 27005: https://www.iso.org/home.html

Organización Internacional de Normalización ISO 19011. (julio de 2018). *ISO 19011.* Obtenido de https://www.iso.org/obp/ui/es/#iso:std:iso:19011:ed-3:v1:es

Ortiz Beltrán, B. F. (2015). HACKING ÉTICO PARA DETECTAR FALLAS EN LA SEGURIDAD INFORMÁTICA DE LA INTRANET DEL GOBIERNO PROVINCIAL DE IMBABURA E IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BASADO EN LA NORMA ISO/IEC 27001:2005.

Secretaría Nacional de Administración Pública. (2013). *EGSI*. Obtenido de Ministerio de Telecomunicaciones y de la sociedad de la Información: https://www.gob.ec/snap

Servicio Ecuatoriano de Normalización. (2013). Norma NTE INEN ISO/IEC 27001. *TECNOLOGÍAS DE LA INFORMACIÓN -TÉCNICAS DE SEGURIDAD-*

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, Segunda Edición. Quito, Ecuador: INEN. Recuperado el 2019

TELCONET LATAM. (2018). *TELCONET logra certificación 27001*. Obtenido de https://www.telconet.net/index.php/noticias/item/129-telconet-certificacion

Telefónica. (2019). *Certificaciones Telefónica Ecuador*. Obtenido de https://www.telefonica.com.ec/pdf/ISO-27001.pdf

UNE-EN ISO/IEC 27001. (Mayo de 2017). Tecnología de la información, Técnicas de seguridad, Sistemas de Gestión de la Seguridad de la Información.

UNE-ISO/IEC 27000. (2014). Tecnología de la información, Técnicas de seguridad, Sistemas de Gestión de Seguridad de la Información (SGSI). Madrid, España: AENOR.