OFICINA DE POSTGRADOS

TEMA:

PROPUESTA DE UN PLAN DE SEGURIDAD INFORMÁTICO PARA LA EMPRESA E.P.-E.M.A.P.A.-A.

Proyecto de investigación previo a la obtención del título de Magister en Gerencia Informática

Línea de Investigación:

Sistemas de información y/o nuevas tecnologías de la información y comunicación y sus aplicaciones.

Autor:

Carlos Arturo Moya Gavilanes

Director:

Mg. Santiago Alejandro Acurio Maldonado

Ambato – Ecuador

Marzo 2023

PONTIFICA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

PROPUESTA DE UN PLAN DE SEGURIDAD INFORMÁTICO PARA LA EMPRESA E.P.-E.M.A.P.A.

Línea de Investigación:

Gerencia, planificación, organización, dirección y/o control de sistemas de información

Autor:

Carlos Arturo Moya Gavilanes

Santiago Alejandro Acurio Maldonado, Ing. Mg. f._____

CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. f._____

CALIFICADOR

Galo Mauricio López Sevilla, Ing. Mg. f._____

CALIFICADOR

Juan Carlos Acosta Teneda, P. Ph.D. f._____

OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
DIRECCIÓN CENTRO DE POSGRADOS
Sede Ambato

Pontificia Universidad Católica del Ecuador
SECRETARIA GENERAL
PROCURADURÍA

Ambato – Ecuador

Marzo 2023

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, **CARLOS ARTURO MOYA GAVILANES**, con **CC. 180205519-2**, autor del trabajo de graduación intitulado "PROPUESTA DE UN PLAN DE SEGURIDAD INFORMÁTICO PARA LA EMPRESA E.P.-E.M.A.P.A.-A." previa a la obtención del título profesional de **MAGISTER EN GERENCIA INFORMÁTICA** en el **CENTRO DE POSGRADOS**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENECYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, marzo de 2023

Carlos Arturo Moya Gavilanes
CC. 1802055192

AGRADECIMIENTO

Primeramente, agradezco a Dios por darme la oportunidad de superarme en mi carrera profesional y darme la sabiduría para culminarla.

A mi querida esposa, Lilian Gamboa, quien me ha impulsado a seguir adelante y ha sido mi apoyo en todos estos años juntos.

A mis hijos, Carlos Moya y Ana Moya, quienes me inspiran a seguir adelante y a esforzarme cada día más por mejorar y brindarles un mejor futuro.

DEDICATORIA

Este trabajo se lo dedico a mi esposa Lilian Gamboa y a mis hijos Carlos Moya y Ana Moya. Ellos son mi fuente de inspiración para superarme todos los días, son quienes me brindan su apoyo moral para seguir adelante y mejorar.

Este éxito es gracias a ustedes.

RESUMEN

El presente proyecto tiene como objetivo proponer un plan de seguridad informático para la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Ambato “E.P.–E.M.A.P.A.–A.”, enfocado en sus requerimientos y alineado a los objetivos de la organización. Dicho proyecto se basa en la norma internacional para sistemas de gestión de la seguridad de la información (SGSI) “ISO/IEC 27001:2013”, y en la metodología de análisis y gestión de riesgos de los sistemas de información “MAGERIT”. La necesidad surge debido al crecimiento de incidentes de seguridad de la información a nivel nacional e internacional y, al grado de importancia que tiene la empresa para la ciudad. Utilizando como sustento metodológico la investigación cualitativa, se realiza un estudio de las políticas, procesos, controles, planes y manuales existentes en la Unidad de Tecnologías de la Información (U.T.I.) de la E.P.-E.M.A.P.A.-A., se define una línea base sobre el estado actual de la empresa con respecto a Seguridad de la información y, basado en metodologías de análisis y gestión de riesgos, se determina un proceso crítico para la empresa y sus activos de información. Apoyado en la norma internacional ISO/IEC 27001, se propone un conjunto de buenas prácticas de seguridad de la información. Como resultado, se define una política de seguridad de la información, se asignan roles y responsabilidades, se definen actividades y períodos de ejecución. Mediante métodos estadísticas, se comprueba la veracidad de la hipótesis planteada y de las herramientas utilizadas para conocer el nivel de impacto del proyecto en la E.P.-E.M.A.P.A.-A.

Palabras clave: Seguridad, metodologías, gestión, norma, políticas, MAGERIT.

ABSTRACT

The objective of this project is to propose an information processing security plan for the Public Company – Municipal Potable Water and Sewage Company of Ambato “E.P.–E.M.A.P.A.–A.”, focused on its requirements and aligned with the objectives of the organization. This project is based on the international standard for information security management systems (ISMS) “ISO/IEC 27001:2013”, and on the “MAGERIT” information systems risk analysis and management methodology. The need arises due to the growth of information security incidents at a national and international level and how essential the company is for the city.By using qualitative research as methodological support, a study is carried out on the existing policies, processes, regulations, plans and manuals in the Information Technology Unit (U.T.I.) of the E.P.-E.M.A.P.A.-A., a baseline is defined on the current state of the company with respect to Information Security and, based on risk analysis and management methodologies, a critical process for the company and its information assets is determined. Supported by the international standard ISO/IEC 27001, a set of good information security practices is proposed. As a result, an information security policy is defined, roles and responsibilities are assigned, activities and execution periods are defined. Through statistical methods, the veracity of the hypothesis and the tools used to determine the level of impact of the project on the company E.P.- E.M.A.P.A.-A is verified.

Keywords: Security, methodologies, management, standard, policies, MAGERIT.

ÍNDICE GENERAL DE CONTENIDOS

INTRODUCCIÓN

Comenzando con el uso de tarjetas perforadas, cintas magnéticas, hasta los actuales circuitos integrados, el ser humano ha buscado métodos y herramientas que le permitan almacenar su información por el mayor tiempo posible, y evita que la misma se pierda o quede ilegible. Gracias al constante desarrollo de la tecnología, y desde la creación de Internet, el mundo entero cuenta con acceso a todo tipo de información en cualquier momento y en cualquier lugar del planeta, facilitando de esta manera, la capacidad de aprendizaje y desarrollo intelectual. Hoy en la actualidad, tanto de manera personal, profesional, como empresarial, el mundo se ha transformado a “La era digital” (Jódar,2010).

Hoy en día, Internet se ha convertido en una herramienta tanto de ocio, como de trabajo. Tal es su nivel de influencia, que instituciones gubernamentales, entidades bancarias, empresas públicas y privadas utilizan este servicio de red mundial; sin embargo, debido a que la información generada cuenta con un alto nivel de importancia para la sociedad, requiere protección ante cualquier tipo de amenaza. Personas mal intencionadas, con conocimientos sobre sistemas informáticos, podrían obtener esta información y dar un uso inadecuado a la misma generando, en casos extremos, inestabilidad económica, política o social (Pampín,2016).

Además de las amenazas producidas por expertos informáticos, existen diversos factores que afectan a la disponibilidad, integridad y confidencialidad de la información. Según Solano, Pérez y Bernal (2016), el usuario, los factores tecnológicos y la gestión organizacional contribuyen en el desempeño del sistema de información en pequeñas y medianas empresas.

Utilizar estándares internacionales como marco de referencia, permiten una adecuada administración de los recursos de una organización, se identifican los procesos críticos de la empresa y se realiza una correcta gestión de los riesgos asociadas a los activos de información (Cárdenas, Martínez y Becerra, 2016). La presente investigación tiene como objetivo, analizar los beneficios que brindan los marcos de referencia en seguridad informática en diferentes organizaciones a nivel

mundial y, como replicar dichos resultados en empresas nacionales, para ello, se considera a la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Ambato (E.P.–E.M.A.P.A.–A.) como referente, la misma es una empresa pública, encargada de la administración del servicio de agua potable y alcantarillado en la ciudad de Ambato.

Antecedentes teóricos y prácticos

El objetivo de un sistema de gestión de seguridad de la información, es cumplir con los requerimientos de la empresa, satisfacer sus necesidades en cuanto a seguridad; y, sobre todo, integrarse con los procesos de la organización. El personal requiere concientización sobre la importancia de su rol para la gestión de la información y un sistema, que facilite su uso mediante reglas que brinden seguridad, pero no interrumpan el normal desarrollo de las actividades y funciones de la empresa.

La seguridad de la información, involucra un compromiso tanto de la alta dirección, como del personal de la organización. Prado, Rosón, Marcos y Bueno (2019) realizan un estudio sobre: “Experiencia en la implementación de un Sistema de Gestión de Seguridad de la Información basado en ISO 27000”. Un proceso que comienza en el año 2007 con la implementación de la norma, utiliza la metodología Magerit para análisis y gestión de riesgos y, tras varios años de constantes controles y auditorías, el Sistema Sanitario Público de Galicia, logra la certificación por primera vez en el año 2015. Dicho reconocimiento le permite a la organización, no solo cumplir con el marco legal establecido en España, sino que, facilita la adopción de nuevas normativas para protección de datos.

Situación problemática

El problema, se evidencia en la gestión de la seguridad de la información en la organización. Los departamentos de tecnologías de la información implementan soluciones de acuerdo con los recursos disponibles y los conocimientos adquiridos, basados en su experiencia; sin embargo, las amenazas actuales cuentan con

mayor nivel de complejidad que hace varios años atrás, por lo que la actualización de conocimientos con respecto a seguridad informática, se convierte en un factor indispensable. Crespo (2018) concluye en su estudio realizado en instituciones de educación superior que: “Al no trabajar en prevención, las instituciones arriesgan sus activos de información, estando estos expuestos a amenazas que pueden afectar la confidencialidad, integridad y disponibilidad” (p. 95).

Mediante el uso de un cuestionario como herramienta de investigación, se realizó un diagnóstico y análisis del SGSI de cinco universidades en Colombia. Entre sus resultados se resalta que: “el 40% de las universidades que aquí se están estudiando no cuenten con funcionarios que sean expertos en el tema de la seguridad informática” (Buitrago, 2020, p.100). Este aspecto lo considera como una vulnerabilidad, las instituciones no están preparadas correctamente en el caso de materializarse un riesgo de seguridad informática.

Los factores cibernéticos no son los únicos con influencia sobre la seguridad de la información. Con el surgimiento de la pandemia de COVID-19, el mundo entero tuvo que adaptarse a una nueva realidad, tanto en trabajo como en seguridad (Ospina y Sanabria, 2020). Debido a la inestabilidad económica causada por la pandemia, muchas empresas redujeron sus presupuestos asignados para ciberseguridad en el año 2020; sin embargo, en el año 2021 dicho presupuesto aumentó (ESET, 2022). Incluso con este aumento, el “63% de los encuestados todavía cree que la relación entre el presupuesto recibido y las necesidades de protección cibernética de las mismas sigue siendo dispar” (p4).

Las instituciones ecuatorianas no están exentas en incidentes de ciberseguridad. Entre el año 2021 y 2022, se registra un incremento del 4% en incidentes de seguridad informática en Ecuador (ESET,2022). Según el estudio realizado por Morales y Medina (2021), en su artículo titulado: “Ciberseguridad en Plataformas Educativas Institucionales de Educación Superior de la Provincia de Tungurahua – Ecuador”, debido al incremento en la educación virtual, las instituciones son más propensas a riesgos de ciberseguridad debido a que las plataformas web “tienen un control inadecuado, mala configuración de servidores, falta de administración de

usuarios e ingeniería social, esto ligado a la falta de un personal exclusivo en seguridad de la información" (p69).

La Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Ambato "E.P.–E.M.A.P.A.–A." es la responsable de brindar los servicios de agua potable y alcantarillado en la ciudad de Ambato. La empresa, para demostrar su compromiso con la calidad, ha implementado un sistema de gestión de calidad, el mismo que ha sido certificado mediante la norma ISO 9001 (E.P.-E.M.A.P.A.-A., 2020, p. 3). La empresa cuenta con buenas prácticas relacionadas a la definición de procesos; sin embargo, no se ha suplido correctamente las competencias del personal en cuanto a las necesidades de capacitación y desarrollo laboral (Castro, 2015).

La seguridad informática considera, como parte fundamental, a la gestión de riesgos, donde se realiza el análisis de la probabilidad de que una amenaza explote una vulnerabilidad y el impacto que generaría en la empresa (Baca, 2016). Considerando los incrementos en incidentes de seguridad y la importancia de la E.P.-E.M.A.P.A.-A. para la ciudad de Ambato, se plantea la siguiente pregunta:

Planteamiento del problema

¿De qué manera, se disminuye la probabilidad y el impacto causado por los riesgos de seguridad de la información en la E.P.-E.M.A.P.A.-A.?

Hipótesis

Un plan de seguridad informática, basado en la norma internacional ISO/IEC 27001:2013, genera un impacto positivo en la empresa E.P.-E.M.A.P.A.-A.

Objetivo general

- Elaborar un proyecto de plan de seguridad informática para la empresa E.P-E.M.A.P.A.-A. basado en la norma ISO 27001.

Objetivos específicos

1. Fundamentar teórica del estado del arte de la aplicación de planes de seguridad en instituciones de servicio público.

2. Determinar la situación actual con respecto a seguridad de la información de la Unidad de Tecnologías de la Información de la empresa E.P-E.M.A.P.A.-A.

3. Definir, de acuerdo con la norma ISO 27001, de una política, roles y responsabilidades para la seguridad de la información de la empresa E.P. – E.M.A.P.A. – A.

4. Validar la aplicación de buenas prácticas de la norma ISO 27001 a las actividades de la Unidad de Tecnologías de la Información (U.T.I.) de la empresa E.P-E.M.A.P.A.-A. en una prueba piloto.

Metodología

El sustento metodológico utilizado es la investigación cualitativa. La población con la que cuenta la E.P. – E.M.A.P.A. – A se encuentra conformada por cinco direcciones: Administrativa, Financiera, Gestión de Proyectos e Infraestructura, Operación y Mantenimiento y Comercial, cada una de ellas cuenta con sus diferentes subdirecciones y departamentos. Como muestra, para el caso de estudio, se consideró a la Unidad de Tecnologías de la Información de la Empresa. Como técnica de recolección de información se utilizó una encuesta, mediante la cual, se determinó el nivel actual de la empresa con respecto a seguridad de la información. Posteriormente se analizaron los riesgos asociados a los activos y se propone una solución adaptada al caso de estudio.

Mediante la utilización del Alfa de Cronbach, se determinó el nivel de confiabilidad que presenta el instrumento de recolección de información y, para comprobar la veracidad de la hipótesis planteada, se utilizó el método estadístico de distribución de probabilidad “T de student”.

Justificación de la investigación

El presente proyecto implica el diseño de un plan de seguridad informática orientado a los procesos de la E.P.-E.M.A.P.A.-A., permite que la entidad disminuya el impacto causado por la materialización de un incidente de seguridad. La necesidad del desarrollo del presente proyecto radica en la importancia que tiene la empresa para la sociedad Ambateña, al ser la entidad rectora en la provisión de servicios de agua potable y alcantarillado en la ciudad de Ambato (E.P.-E.M.A.P.A.-A., 2020, pág. 1), cualquier incidente de seguridad, comprometería la continuidad de sus servicios.

CAPÍTULO I. ESTADO DEL ARTE

1.1. Plan de seguridad informática

La seguridad informática ha sido diseñada e implementada en diferentes organizaciones, ya sean estas públicas o privada, con el objetivo de salvaguardar la información contenida en medios digitales. En el estudio realizado por Mujica (2008), se diseña un plan de seguridad informática para la Universidad Nacional Experimental Politécnica Antonio José de Sucre “UNEXPO” en Venezuela. Dentro de la metodología utilizada, se efectúan análisis estadísticos y técnicas de recolección y análisis de información basados en la norma ISO/IEC 27001 e ISO/IEC 17799. Entre los resultados obtenidos, se observa una mejora del 71% en la seguridad informática debido a la implementación de políticas, procedimientos, definición de perfiles, entre otros (Mujica, 2008).

Otro ejemplo de un plan de seguridad informática se lo realizó para el Sistema de Información Misional (SIM) de la Procuraduría General de la Nación en Colombia. Alfaro y Vargas (2016), autores del estudio, inician el proceso con el diagnóstico del estado actual de la organización con respecto a seguridad informática, se realiza un análisis de riesgos al sistema de información misional para finalmente, diseñar un plan de seguridad informática. En el resultado final se evidencian procedimientos para la gestión de vulnerabilidades técnicas, respuestas ante incidentes, concientización, control de acceso, entre otros.

Un sistema informático no es completamente seguro, no es posible garantizar la seguridad total de un sistema porque las amenazas evolucionan constantemente, por lo que no resulta factible implementar medidas de protección dedicadas a cada una de ellas (García, Hurtado, Alegre, 2011); sin embargo, si se identifican y clasifican los tipos de seguridad a implementar, la respuesta ante un incidente es más efectiva. Cuellar (2020), en su tesis de especialización concluye que: “A pesar de que ningún sistema puede garantizar una completa seguridad de la información, es una manera de controlar y prevenir futuros daños a los equipos, al sistema, a la reputación y a la continuidad del negocio” (p. 184).

En el Cuadro 1. se muestran los tipos de seguridad aplicados a sistemas informáticos.

Cuadro 1. Clasificación de la seguridad

Activa	Pasiva	Física	Lógica
Son aquellas medidas que permiten la detección temprana de amenazas. Ejemplos Antivirus, firewall	Son aquellas medidas tomadas después de un incidente de seguridad. Ejemplos Copias de seguridad, redundancias de información	Son aquellas encargadas de proteger la barrera física del sistema informático. Ejemplos UPS, guardias y cámaras de seguridad.	Son aquellas encargadas de asegurar el software del sistema informático. Ejemplo Encriptación de información

Fuente: tomado a partir de (García, Hurtado, Alegre, 2011)

Contexto de la organización

Previo a la ejecución de un plan de seguridad informática, se realiza un análisis de la organización, cuál es su misión, visión y estructura organizacional. En el estudio realizado para la organización Geoconsult Consultoría y Servicios Petroleros y Mineros Ltda., empresa colombiana con operación multinacional, con sedes en Colombia, Ecuador y Perú, Fonseca (2019) indica que:

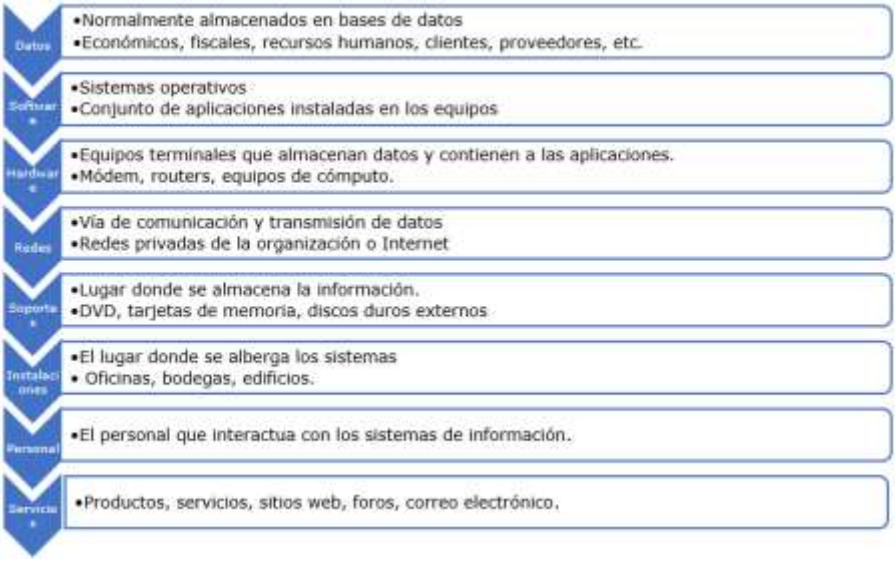
> Un adecuado análisis del contexto de la organización es un aspecto fundamental dentro de las primeras actividades en la implementación de un sistema de gestión de seguridad de la información, debido a que se determinan las cuestiones externas e internas que pueden afectar los resultados previstos del SGSI. (Fonseca, 2019, p. 104)

Un plan de seguridad informática tiene como etapa principal la realización de un análisis de vulnerabilidades y amenazas, seguidamente de la administración del riesgo donde se considera la identificación, análisis y gestión del riesgo y, finalmente, la elaboración del plan.

Análisis de vulnerabilidades y amenazas

Una vulnerabilidad se define como una “Debilidad de un activo o control que puede ser explotada por una o más amenazas” (Organización Internacional de Estandarización [ISO], 2022). Mientras que una amenaza es una “Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización” (ISO, 2022). En la Cuadro 2 se indican los tipos de activos existentes en una organización y varios ejemplos de cada grupo.

Cuadro 2. Activos de información

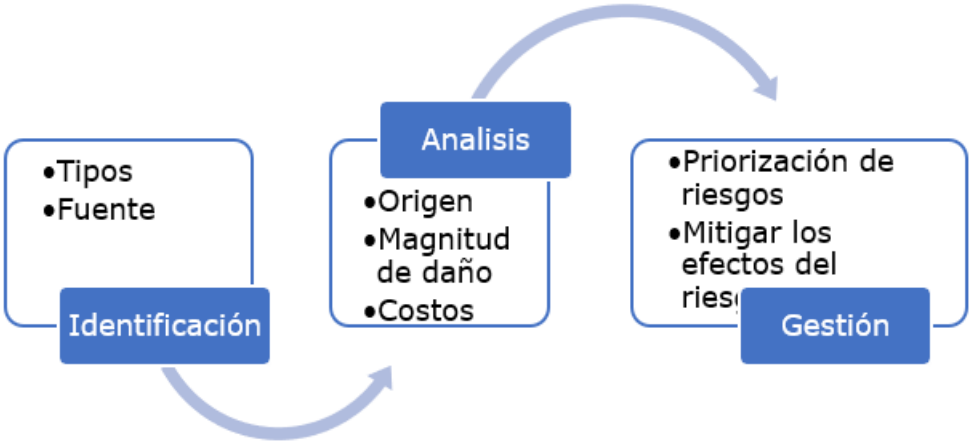


Fuente: tomado de Aguilera (2010).

Administración del riesgo

La administración del riesgo en un plan de seguridad informática considera que riesgos se encuentran expuestos los activos de la organización, que tipos de amenazas afectarían a las vulnerabilidades existentes y cuál sería el impacto y la probabilidad de materializarse un incidente de seguridad en la empresa.

Cuadro 3. Etapas administración de riesgos en proyectos de seguridad informática



Fuente: tomado a partir de Baca (2016)

En la etapa de identificación se determina de donde provienen los riesgos y las fuentes que los provocan. En la etapa de análisis se listan los riesgos, tanto internos como externos. De esta lista se realiza una caracterización del riesgo, donde se definen parámetros como la probabilidad de ocurrencia, el impacto que representa para la empresa y el riesgo que sufriría la misma.

Cuadro 4. Categorización de riesgos

Se originan en cualquiera de las fase del proyecto, la implementación o la operación.	Se originan en cualquiera de los procesos rediseñados en la operación.	Se originan en la tecnología utilizada para aplicar y controlar medidas de riesgo.	Se originan en la forma de administrar el proyecto, su implantación y operación.

Fuente: tomado a partir de Baca (2016)

En la etapa de gestión, de acuerdo con los criterios utilizados para caracterizar el riesgo, se asignan niveles de prioridad conforme al nivel de severidad del riesgo y se determinan indicadores para la ejecución de acciones de mitigación dentro de un plan. Aranzales y Giraldo (2019) concluyen, en su estudio sobre un sistema de gestión de seguridad de la información, que la metodología de gestión de riesgos: “se constituye en su principal soporte, ya que allí se identifican los activos, sus amenazas y vulnerabilidades, para que a partir de ello se elaboren y ejecuten los planes de tratamiento” (p. 75).

Elaboración del plan

Dentro del plan de seguridad informática, se consideran el análisis de las vulnerabilidades y amenazas y la administración del riesgo. De acuerdo con los niveles de prioridad de los riesgos, se establecen una serie de actividades para identificar, analizar y establecer planes para mitigación de riesgos, juntamente con los responsables de su ejecución. Con la finalidad de supervisar los riesgos y tomar decisiones oportunas, se implementan métodos y herramientas para el monitoreo de estos (Baca, 2016).

Un ejemplo de un plan de seguridad informática se lo realizó para la Universidad de las Fuerzas Armadas “ESPE” sede Santo Domingo. Borja y Sánchez (2015) comenzaron con la definición del equipo de trabajo, al cual lo denomina “Comité”, define el alcance del plan de seguridad, clasifica los activos e identifica amenazas, vulnerabilidades y riesgos, realiza un tratamiento de riesgos mediante controles y su madurez de aplicación, define políticas y finalmente, desarrolla el plan. El resultado final permite identificar puntos críticos en la seguridad de la “ESPE”, definir controles y una política bien estructurada basada en estándares internacionales.

1.2. Normas de seguridad informáticas

Existen múltiples normativas, marcos de referencia e información guía con respecto a buenas prácticas relacionadas a seguridad informática tomadas por empresas a nivel nacional e internacional.

COBIT

Este marco de referencia ha sido ampliamente utilizado a nivel nacional e internacional para el gobierno y gestión de TI, en el estudio realizado por Eito-Brun y Calleja (2020), se analiza la gestión documental en el marco de modelo COBIT, concluye que: “Sirve de apoyo a los profesionales encargados de verificar que las

organizaciones han establecido las medidas necesarias para evitar, mitigar y paliar los riesgos y sus efectos" (p. 12).

A nivel nacional, se realizó un modelo de gestión de TICS en la Corporación Financiera Nacional (CFN). Proaño (2012), dentro de su estudio, concluye que COBIT utilizado como modelo de gestión de TICs, "permitiría que la Gerencia de División de Informática de la CFN optimice y mejore la gestión de TICs en aproximadamente un 85%".

En el estudio sobre auditoría de seguridad informática, realizado en la dirección distrital 02D02 en Chimbo se utilizó COBIT 5 como modelo de referencia. Palacios, Bósquez, Palacios y Camacho (2019) se basan en tres fases: Planeación, ejecución y comunicación de resultados. Dentro de los resultados obtenidos, no se detallan hallazgos debido a un acuerdo de confidencialidad; sin embargo, recalcan que la utilización de COBIT 5 "ayudó significativamente en la realización de la auditoría de seguridad informática" (p. 10).

ITIL

ITIL ha sido ampliamente utilizado a nivel mundial en la gestión de servicios de tecnologías de información (TI). En Ecuador, en el estudio realizado por Conde, Quezada y Hernández (2019), proponen utilizar ITIL para la gestión de incidentes en una mesa de servicios tecnológicos, donde brinda soluciones tanto a problemas de hardware, software, redes y varios dispositivos informáticos. En el estudio se concluye: "La meza de servicios basada en ITIL propone llegar a un nivel de eficiencia que se traduzca en una buena prestación de servicios, logrando con ello un alto nivel de eficacia y aceptación del usuario" (p. 5).

El plan estratégico propuesto para la gestión de servicios médicos en Telesalud se basa en las buenas prácticas de gestión de servicios de ITIL V3. Mendoza, Escobar se basan en las buenas prácticas de gestión de servicios de ITIL V3. Las etapas postuladas en su plan consideran: definición del mercado, desarrollo de la oferta, activos estratégicos y preparación para la implementación. Mendoza et al. (2019)

concluyen que: "… la oferta de servicios de salud debe cumplir con parámetros relevantes orientados a prestar un servicio de calidad que cumpla con las demandas y necesidades del cliente, …" (p. 60).

ISO 27001

Esta norma es un marco de referencia a nivel mundial en sistemas de gestión de seguridad de la información (SGSI). En el estudio realizado por Rodríguez, Cruzado, Mejía y Alarcón (2020) sobre la influencia de la norma ISO 27001 en una empresa privada de Lima (Perú), utilizando una metodología cuantitativa, se buscó determinar la influencia en la confidencialidad, integridad y disponibilidad de la información. El estudio concluye que:

> La ISO 27001 brinda políticas que deben implementar con la finalidad de garantizar la confidencialidad de la seguridad de la información […] ISO 27001 ayuda a implementar procedimientos para garantizar la integridad de la información […] la información debe estar disponible permanentemente para dar soporte a la toma de decisiones. (Rodríguez, Cruzado, Mejía y Alarcón, 2020).

Igualmente, en el campo de la seguridad informática, se han realizado múltiples estudios tomando como referencia a la norma ISO/IEC 27001. Solarte, Enríquez y Benavides (2015) presentan: "Los resultados de una experiencia aplicando las fases de auditoría y la metodología de análisis y evaluación de riesgos". Para su estudio utiliza diversos instrumentos como cuestionarios, entrevistas al personal del área informática y usuarios. Los resultados finales muestran que:

> No existe una cultura de seguridad de la información dentro de las organizaciones, tampoco existe sistemas de control de seguridad informática y de información. […] Por tanto, es fundamental que las organizaciones cuenten con un marco normativo de seguridad, que permita aplicar la auditoría basada en la norma ISO/IEC 27002. (p.505).

En la tabla a continuación, se cuenta con un resumen sobre las características de los marcos de referencia estudiados.

Cuadro 5. Comparativa entre COBIT, ITIL e ISO 27001

Área	COBIT	ITIL	ISO 27001
Funciones	Mapeo de procesos IT	Mapeo de la Gestión de Niveles de Servicio de IT	Marco de referencia de seguridad de la información.
Creador	ISACA	OGIC	International Organization for Standarization ISO
Implementación	Auditoría de Sistemas de Información	Gestión de Niveles de Servicio	Cumplimiento del estándar de seguridad
Certificable	NO	NO	SI

Fuente: modificado a partir de Montaño (2011).

Normativas para la gestión de riesgos

ISO 27005

La norma ISO 27005 ha sido ampliamente utilizada en la gestión de riesgos. Montoya (2020) en su tesis realiza la evaluación de riesgos de seguridad de información tomando como referencia a la norma ISO 27005 en el Instituto Nacional de Salud en Perú. Entre los resultados obtenidos, se determina cuáles son los activos con mayor nivel de criticidad para la organización, evaluando procesos, niveles de riesgo e importancia de la información asociada al activo.

La norma fue utilizada dentro de un caso de estudio práctico, validando su aplicabilidad dentro de ámbitos técnicos, económicos, legales y organizacionales. Carrera (2012), en su tesis de maestría, diseña un modelo de gestión de riesgos de seguridad de la información utilizando la norma ISO/IEC 27005 y el método Octave, concluyendo que: "… logran cumplimentarse unas con otras de tal forma que abarcan las actividades requeridas para la gestión de riesgos de seguridad de la información".

MAGERIT

Magerit es la metodología de análisis y gestión de riesgos de Tecnologías de la Información. Esta es utilizada por organizaciones para la ejecución de acciones relacionados con los riesgos tecnológicos (Magerit – Libro 1, como se citó en ÑAÑEZ, 2019). Magerit ha sido ampliamente utilizada en la gestión de riesgos. Molina (2017) realiza un análisis de riesgos en una empresa que brinda servicios de red y sistemas en una Universidad ecuatoriana. Mediante Magerit determinan las vulnerabilidades asociadas a los activos del departamento de informática de la universidad y, utilizando la herramienta Pilar, se obtienen gráficas radiales donde se identifican fácilmente los procedimientos para la protección de los recursos.

En el estudio realizado por Varón (2017) al sistema de información de AGESAGRO S.A.S. aplica la metodología Magerit para analizar amenazas, vulnerabilidad y riesgos asociados al manejo de la información. Varón determina el estado actual de la organización en seguridad de la información, identifica los activos informáticos y el tipo de información que manejan, analiza los riesgos y propone recomendaciones para contrarrestar la fuga de información. Mediante Magerit, Varón concluye que: “[…]los recursos y activos se deben de cuidar en almacenamiento y ambiente que pueda dañar los mismos, la disminución de riesgos puede lograr que la información sea integra, confiable y disponible”.

En el estudio realizado por Ampuero (2022), en su tesis de maestría, realiza la gestión de riesgos de la información basado en la metodología Magerit. Ampuero propone un modelo de gestión de riesgos aplicable a las notarías de la Región Lima. La investigación se basa en un enfoque cualitativo, utilizando entrevistas, observación y análisis documental como instrumento de recolección de datos. Los resultados obtenidos demuestran que Magerit: “… es una herramienta práctica y documentada que permite gestionar adecuadamente los riesgos mediante el análisis y tratamiento respectivo” (p. 7).

1.3. Generalidades ISO 27001

La norma ISO 27001 tiene su origen en Reino Unido, cuando el Instituto Británico de Estandarización (BSI) publica normas con carácter internacional. La norma ISO 27001, previamente BS 7799-1, fue publicada por primera vez en 1995, con el objetivo de proporcionar una serie de mejores prácticas para gestionar la seguridad de la información en empresas británicas. En el año 2000 la Organización Internacional para la Estandarización adopta la norma británica. Después de varias revisiones posteriores y diferentes versiones finalmente, en octubre de 2013, se publican las revisiones de la norma con el nombre ISO/IEC 27001:2013 (Gómez y Fernández, 2018).

Campo de aplicación

La norma ISO/IEC 27001 es aplicable a cualquier tipo de organización, independientemente de su naturaleza, tamaño o sector de actividad. Esta norma detalla los requisitos necesarios para establecer, implementar, mantener y mejorar constantemente un Sistema de Gestión de Seguridad de la información (SGSI), considerando los objetivos y riesgos de la organización. Igualmente, ofrece flexibilidad en el cumplimiento de los requisitos, lo que facilita la utilización de diferentes metodologías (Gómez y Fernández, 2018).

Según la información recopilada de las fuentes citadas en los párrafos anteriores, la norma internacional ISO/IEC 27001:2013 brinda una serie de recomendaciones sobre la protección de activos de información en una organización. Las cláusulas que estipula la norma sirven de guía para el desarrollo e implementación de un sistema de gestión de seguridad de la información; además, al adaptarse a las necesidades de la empresa, permite que la misma implemente medida de seguridad acorde a sus recursos y estructura organizacional.

Mejora continua

La norma ISO/IEC 27001 cuenta con un enfoque basado en el ciclo de Deaming, en el cual, se fomenta la mejora continua. En dicho ciclo se cuenta con cuatro etapas bien definidas y los requisitos necesarios para un SGSI. El proceso comienza con la planificación del sistema de gestión, pasando por la implementación y verificación hasta finalizar con la evaluación y aplicación de medidas correctivas; es en este punto donde se reinicia el ciclo y el proceso vuelve a comenzar (Parra, 2014). En la siguiente tabla se muestran las fases del ciclo de Deming y las actividades correspondientes.

Cuadro 6. Ciclo de mejora continua de Deming.

<table>
<tr><td>1. Plan (Planear)</td><td>En esta fase se planifica la implantación del SGSI</td><td>2. Do (Hacer)</td><td>En esta fase se implementa y pone en funcionamiento el SGSI</td></tr>
<tr><td colspan="2">Identificar objetivos del negocio
Obtener apoyo de la dirección

Definir política
Establecer el alcance
Análisis de riesgos
Seleccionar procesos/procedimientos/controles</td><td colspan="2">Implantar el plan de gestión
Implantar el sistema de gestión
Implantar procesos/procedimientos/controles
Asignar recursos
Formación y concienciación</td></tr>
<tr><td>3. Check (Verificar)</td><td>En esta fase se realiza la monitorización y revisión del SGSI</td><td>4. Act (Actuar)</td><td>En esta fase se mantiene y mejora el SGSI</td></tr>
<tr><td colspan="2">Monitorizar
Auditorías internas
Medir
Revisión por la dirección</td><td colspan="2">Aplicar mejora continua
Acciones correctivas</td></tr>
</table>

Fuente: modificado a partir de Gómez y Fernández (2018).

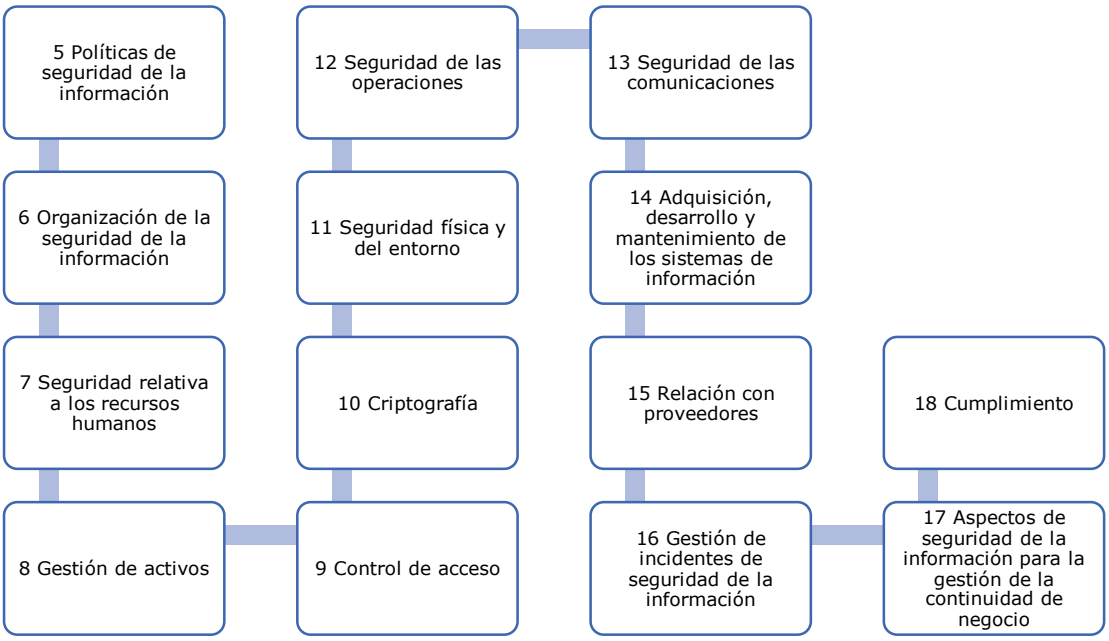
Mediante la utilización del ciclo de Deming, Mahecha y Coello (2016) presentan el desarrollo de un sistema de información basado en la norma ISO 27001:2013 donde implementan, mantienen y mejoran continuamente un sistema de gestión de seguridad de la información. Mahecha y Coello concluyen que: "… un SGSI se mantiene gracias a la mejora continúa sustentada en un ciclo PHVA". Igualmente, Niño (2018) concluye en su estudio realizado en el Instituto Nacional de Estadísticas e Informática INEI en Perú que la metodología PDCA permitió: "realizar un análisis con el fin de identificar los principales problemas como el uso de sus recursos, colaboradores y la información que en ella se opera" (p. 87).

Estructura

En la estructura de la norma se establecen varias secciones donde se indican los requisitos para la gestión de un sistema de seguridad de la información. Comenzado con aspectos relacionados a la norma como: orientaciones sobre el uso, finalidad, modo de aplicación, referencias normativas, términos, definiciones y, clausulas enfocados a la organización como: Contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora. (Yungán y Narváez, 2022).

Al final de la norma ISO 27001 se cuenta con el Anexo A, el mismo es un documento guía para la implementación de controles de seguridad específicos de la norma. Dicho anexo está compuesto por 114 controles, separados en 14 secciones. La variedad de controles brinda un enfoque en seguridad informática, seguridad de la información, ciberseguridad, entre otros (ISO 27001, 2018).

Cuadro 7. Controles Anexo A – ISO/IEC 27001:2013



Fuente: tomado a partir de (Yungán y Narváez, 2022).

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la empresa

Fundada en el año 1967, la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Ambato “E.P.–E.M.A.P.A.–A.”, nace en la ciudad de Ambato como “persona jurídica de derecho público y autonomía administrativa, operativa, financiera y patrimonial” (E.P.-E.M.A.P.A.-A., 2020, p. 4).

Constituida como empresa municipal por el Ingeniero Germán Chacón Bucheli hasta consolidar su autonomía en el año 2010 mediante Ordenanza Sustitutiva (E.P.-E.M.A.P.A.-A., 2020, p. 1). La E.P.–E.M.A.P.A.–A. cuenta con un edificio matriz, donde se desarrollan actividades financieras y administrativas de la empresa. Además, cuenta con varias sucursales de recaudación, estaciones de bombeo y tanques de reserva distribuidos en zonas urbanas y rurales de Ambato.

Misión y visión de la E.P.–E.M.A.P.A.–A.

Misión

Desarrollar, mantener y operar la infraestructura instalada para la dotación de servicios básicos de agua potable y alcantarillado de manera eficiente para contribuir a la salud y bienestar de la ciudadanía ambateña, garantizando el mantenimiento y conservación de las fuentes de agua, apoyando en el cuidado ambiental de la zona de influencia, implementando tecnología adecuada y altos estándares de calidad. (E.P.-E.M.A.P.A.-A., 2020, p. 2).

Visión

Ser reconocida en el año 2022, como una empresa eficiente, rentable e innovadora en la dotación de servicios de agua potable y alcantarillado, con responsabilidad social y ambiental en el desarrollo de obras y proyectos de agua potable y alcantarillado. (E.P.-E.M.A.P.A.-A., 2020, p. 2).

Contexto de la organización

La E.P.-E.M.A.P.A.-A. tiene como finalidad la dotación de servicios de agua potable y alcantarillado, “según el plan de ordenamiento territorial de Ambato” (E.P.-E.M.A.P.A.-A., 2020, p. 4).

Estructura organizativa

La E.P.-E.M.A.P.A.-A. cuenta con el siguiente orgánico estructural (Cuadro 8):

Cuadro 8. Estructura orgánica funcional

Fuente: tomado a partir de E.P.-E.M.A.P.A.-A. (2018, p. 4)

Base legal

La E.P.-E.M.A.P.A.-A. cumple con la base legal, de acuerdo con el Artículo 7 de la Ley Orgánica de Transparencia y Acceso a la Información Pública - LOTAIP.

Certificaciones

La E.P.–E.M.A.P.A.–A., consiente del papel que desempeña y, de la importancia de brindar sus servicios a la comunidad ambateña, ha mantenido la certificación en gestión de la calidad bajo norma ISO 9001:2015 (E.P.-E.M.A.P.A.-A., 2020, p. 3).

2.2. Estructura de la investigación

Este es un diseño de una propuesta bibliográfica, se revisa la bibliografía con relación al tema, se valida la evidencia, se confirma datos importantes y se propone una solución adaptada al caso de estudio. El sustento metodológico utilizado es la investigación cualitativa, donde se recolecta información actual sobre la seguridad de la información en la empresa, se analiza el riesgo en los activos y se propone políticas.

Dentro de la revisión bibliográfica se consideraron tesis de postgrado y artículos científicos referentes a sistemas de gestión de seguridad de la información y seguridad informática, dentro de los cuales, se analizó la metodología utilizada, los marcos de referencia implementados y los resultados obtenidos. Dentro del estudio realizado se determinó que la metodología de análisis y gestión de riesgos Magerit brinda un amplio panorama para el tratamiento de riesgos (Ferruzola et al., 2019) y, al ser complementada con las recomendaciones de la norma ISO 27005, se realiza una gestión de riesgos orientada en los requisitos de la norma ISO/IEC 27001:2013 (Ramírez y Ortiz, 2011).

Dentro de la investigación cualitativa, se realizó una encuesta para determinar el nivel de madurez inicial de la empresa con respecto a seguridad informática, considerando los requisitos y lineamientos establecidos por la norma ISO/IEC 27001:2013; de esta manera se logró comprender como la E.P. – E.M.A.P.A.- A. protege sus activos de información. Con los resultados obtenidos, se plantearon mejoras y se desarrolló la propuesta del plan de seguridad informática.

Para la ejecución de la presente investigación se ocupa la técnica de la encuesta y la entrevista aplicada a los miembros de la Unidad de Tecnologías de la Información (U.T.I.) de la E.P.-E.M.A.P.A.-A. El objetivo es obtener información correspondiente al departamento donde se aplica el presente proyecto. La población total se encuentra conformada por cinco integrantes de la Unidad de Tecnologías de la información, por lo cual, no es necesaria la determinación de una muestra debido al reducido número de empleados que conforman el departamento.

En el caso de estudio se consideró la utilización de varios requisitos establecidos en la norma ISO/IEC 27001:2013 para la elaboración de la propuesta del plan de seguridad informática. A continuación, se describen cuáles fueron los requisitos utilizados, las metodologías implementadas y los resultados esperados.

Liderazgo

En la propuesta se considera el compromiso de la alta dirección para el desarrollo del plan de seguridad informática. Dentro del liderazgo se espera:

- Establecer políticas y objetivos de seguridad.
- Comunicar la importancia de una gestión eficiente de la seguridad informática.
- Asignar los roles y responsabilidades pertinentes a la seguridad informática.

Planificación

Se analizan los riesgos asociados a los activos de información de la empresa de estudio. Utilizando como guía a la norma ISO 27005 y la metodología Magerit se realiza: identificación, análisis y evaluación de riesgos. Asimismo, la metodología Magerit fue utilizada para clasificar los activos de información de la empresa. Se determinaron tres grupos principales de activos, de los cuales, se realizó el análisis de vulnerabilidades y amenazas para analizar el impacto que tendría cada uno de ellos con respecto a la confidencialidad, disponibilidad e integridad de la información. La norma ISO 27005 fue utilizada como guía para determinar los niveles de impacto, probabilidad y severidad para evaluar los riesgos expuestos en los activos de información. Igualmente, se diseñó un mapa de calor para identificar el nivel de severidad de los riesgos, tanto inherentes como residuales.

Soporte

En el caso de estudio se consideraron:

- Capacitación continua del personal en temas de seguridad informática
- Contribución del personal en la eficacia del plan.

No se consideró la información documentada requerida por la norma debido a que el plan se basa únicamente en la seguridad informática.

Operación

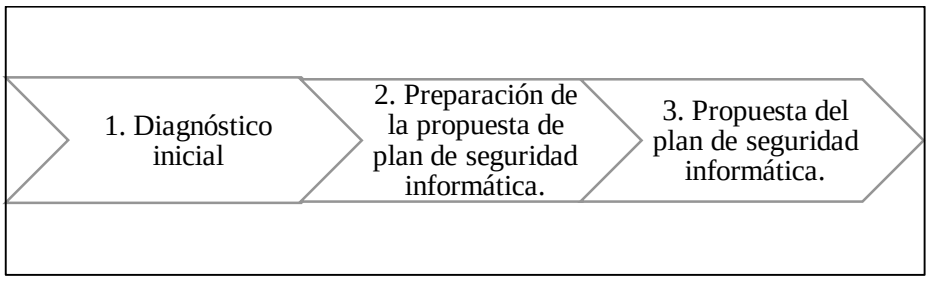
No se considera la implementación y control de los procesos dentro del presente estudio debido a que es una propuesta.

Evaluación del desempeño

Se determina el nivel de fiabilidad del instrumento de investigación utilizando el Alfa de Cronbach y, mediante un modelo estadístico, se evalúa la hipótesis planteada.

Para la investigación se establecieron 3 fases en el desarrollo e implementación de un plan de seguridad informática.

Cuadro 9. Fases del plan de seguridad informática.



Fuente: Elaboración propia.

A continuación, se describen cada una de las etapas en el proceso investigativo.

En la Fase I, conocida como Diagnóstico inicial, se realiza un análisis de la situación actual de la empresa con respecto a seguridad de la información. Para ello se

inspecciona la información existente, se realizan entrevistas, encuestas con el fin de identificar el cumplimiento de la empresa con respecto a la norma.

En la Fase II, conocida como Preparación de la propuesta de plan de seguridad informática, se identifican las partes interesadas, se genera el alcance del sistema, se establece la política general y los objetivos del plan de seguridad.

En la Fase III, conocida como Propuesta del plan de seguridad informática, se identifica y valora los activos de información, se establecen las políticas y los controles necesarios para el plan.

FASE I

Para iniciar con el diagnostico, se realiza un cuestionario a la Unidad de Tecnologías de la Información (U.T.I.) de la empresa (Anexo 1), la misma está conformada por 5 miembros entre jefe, analistas y técnicos.

Tabla 1. Personal U.T.I.

Cargo	Cantidad
Jefe de TI	1
Analista TI	3
Analista técnico	1
Total	5

Fuente: Elaboración propia.

El Cuestionario consta de un total de 31 preguntas, las cuales, se encuentran divididas entre los 14 dominios con los que cuenta el Anexo A de la norma ISO 27001.

Para el análisis, se consideró una escala de valoración y un valor porcentual para cada pregunta, considerado de la siguiente manera:

Tabla 2. Niveles y valoración utilizados en la encuesta.

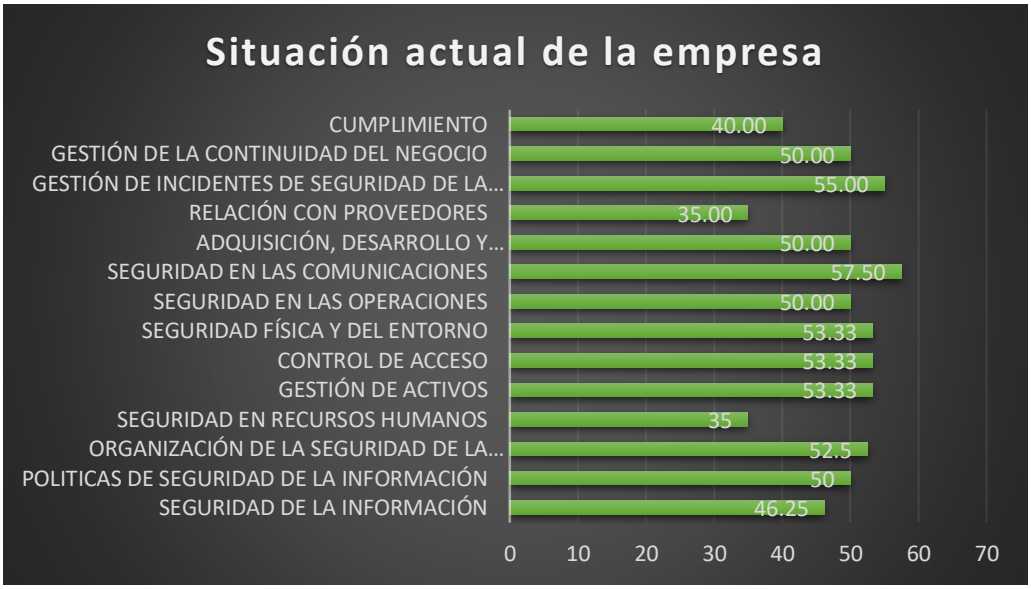
E (Excelente)	MB (Muy Bueno)	B (Bueno)	R (Regular)	D (Deficiente)
100%	75%	50%	25%	0%

Fuente: Elaboración propia.

Dentro de cada dominio se obtiene un valor promedio de las preguntas evaluadas. Este proceso se realiza con cada participante para obtener el resultado total de la Unidad de Tecnologías de la Información por cada dominio.

En la Tabla 3 se describe el porcentaje de cumplimiento con respecto a cada dominio. Se observa que en diversos dominios se cuenta con un cumplimiento igual o mayor que el 50%; sin embargo, en varios de ellos se encuentran valores que oscilan entre el 35% y el 46,25%, lo que denota que existe un sistema de gestión de seguridad, pero el mismo no cubre con los requisitos de la organización

Tabla 3. Nivel de madurez por dominio.

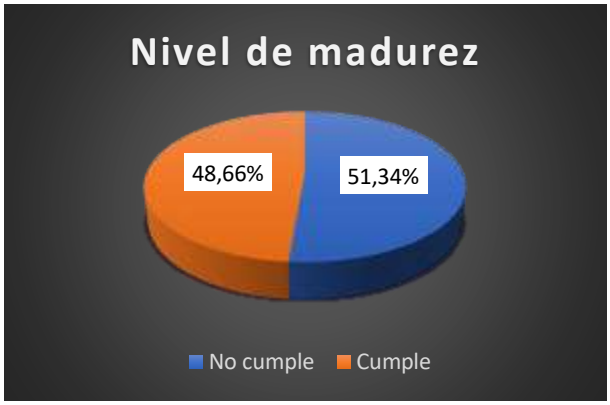


Fuente: Elaboración propia.

En la Tabla 4, se muestra el nivel de madurez general obtenido por la E.P.-E.M.A.P.A. – A. El valor de cumplimiento es del 48,66%, lo que indica cuenta con

buenas prácticas en seguridad; sin embargo, las mismas no satisfacen los lineamientos establecidos en la norma ISO 27001.

Tabla 4. Nivel de madurez general.



Fuente: Elaboración propia.

FASE II

El correcto desarrollo de un Sistema de Gestión de Seguridad de la Información implica que todos los miembros de la empresa se involucren y tomen parte del proceso. Entre las partes interesadas internas se considera a la dirección ejecutiva, la misma proporciona directrices sobre organización y monitoreo del desempeño de las tecnologías de la información, gerente de negocio y gestión de riesgos. En el caso de las partes interesadas externas se reconoce a los socios de negocio y a los proveedores de TI.

Alcance

El alcance se define de acuerdo con el proceso, el seleccionado es “Respaldo, archivo y custodia de la información electrónica”. Este proceso involucra a los departamentos: Comercial, Financiero y Dirección de Operación y Mantenimiento (DOM). Para la definición del alcance se cuenta con el apoyo del jefe de Departamento de Tecnologías de la Información de la empresa, basado en la norma ISO 27001.

Políticas de Seguridad para el SGSI.

La E.P.- E.M.A.P.A. – A. comprometida con la mejora continua, reconoce que la implementación de políticas adecuadas inherentes a la seguridad de la información le permite satisfacer las necesidades tanto de los clientes internos como externos; para ello se establece la siguiente política, alineada al contexto de la seguridad de la información en la empresa.

Promover el uso de buenas prácticas de seguridad de la información dentro de la empresa, garantizando una eficiente administración de los recursos tecnológicos y asegurando continuidad de los procesos de la E.P. - E.M.A.P.A.- A. a través de un Sistema de Gestión de Seguridad de la Información adecuado a sus necesidades, garantizando la confidencialidad, integridad y disponibilidad de la información.

Objetivos del S.G.S.I

Con el fin de cumplir la política establecida, se establecen los siguientes objetivos:

- Proteger la información de mayor importancia mediante respaldos digitales.
- Controlar el acceso inapropiado a los respaldos de información.
- Asegurar la información generada definida como importante.
- Mantener bajo custodia de la Unidad de Tecnologías de la Información.

FASE III

Para realizar una correcta gestión de riesgos se evalúa el grado de impacto hacia la empresa y la probabilidad de ocurrencia determinando si el riesgo es aceptable o buscar procedimientos para mitigarlo. La U.T.I. cuenta con una extensa cantidad de activos de información para los distintos procesos de la empresa. En este caso se consideran los relacionados al proceso de estudio.

Para la gestión de riesgos de activos se utilizó la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Magerit) y la norma ISO/IEC 27005,

ambas guías permiten analizar los riesgos a los que están expuestos los activos informáticos, identificar las amenazas, exponer los activos de información con mayor grado de impacto dentro de la organización y con ello, aplicar los controles adecuados para minimizar el impacto. En la siguiente tabla se describen los tipos de activos presentes dentro de la metodología Magerit.

Cuadro 10. Tipos de activos según Magerit.

Abreviatura	Tipo de activo
D	Datos / Información
K	Claves criptográficas
S	Servicios
SW	Software – Aplicaciones Informáticas
HW	Equipamiento informático (hardware)
COM	Redes de Comunicación
Media	Soportes de Información
AUX	Equipamiento auxiliar
L	Instalaciones
P	Personal

Para el caso de estudio se consideraron los tipos de activos presentes en el proceso que son: hardware, software y personal.

A cada activo de información asociado al proceso se le asignó un código alfanumérico, el mismo está conformado por: el tipo de activo al que pertenece y un número consecutivo. Dentro de cada activo se evaluó el impacto que tiene el mismo con respecto a la confidencialidad, disponibilidad e integridad de la información utilizando una escala numérica (Tabla 5), donde el valor más bajo es 1 y el valor más alto es 5.

Cuadro 11. Valoración numérica de confidencialidad, disponibilidad e integridad.

1	2	3	4	5
Muy poco	Poco	Medio	Alto	Muy Alto

Finalmente, se obtuvo la media de los tres valores por cada activo. En la Tabla 5 se muestra a detalle el análisis realizado.

Tabla 5. Análisis de activos evaluados

Activo	Código	CONFIDENCIALIDAD	DISPONIBILIDAD	INTEGRIDAD	PROMEDIO
"SERVIDORES DE RED P.III,MONITOR COLOR	HW1	5	5	5	5,00
AIRE ACONDICIONADO A/A TIPO SPLIT LG.	AUX1	3	5	4	4,00
ANALIZADOR DE RED EN TIEMPO REAL	HW2	5	5	5	5,00
FIREWALL TIPO SOFTWARE	SW1	4	5	5	4,67
FIREWALL PERIMETRAL TIPO HARDWARE PARA FILTRADO Y BLO	HW3	4	4	5	4,33
FIREWALL TIPO HARDWARE PARA INSPECCIÓN DEL ESTADO DE C	HW4	4	4	5	4,33
FUENTE DE PODER 750 W PARA SERVIDOR TIPO RACK	AUX2	3	5	4	4,00
SERVIDOR DE ALMACENAMIENTO CONECTADO RED	HW5	4	5	5	4,67
SERVIDOR DEDICADO A VIDEO	HW6	3	4	5	4,00
SERVIDOR HP DL 180G6 2.4 GHZ.	HW7	3	4	5	4,00
SERVIDOR HP DL38067 SERIE 2M214300LR	HW8	3	4	5	4,00
SERVIDOR HP PROLIANT DL380PG8 SERIE 2M23060IE0	HW9	4	4	5	4,33
SERVIDOR HP PROLIANT DL380PG8 SERIE 2M232304T8	HW10	4	4	5	4,33
SERVIDOR PROLIANT DL 380 SP CPU USE518A5CR	HW11	4	4	5	4,33
SERVIDOR SISTEMA COMERCIAL #HP PROLIANT DL30080G5 SERIE	HW12	4	4	5	4,33
SERVIDOR: MARCA HP; MODELO ML35Oe Gen 8v2; SERIE MX2511(	HW13	4	4	5	4,33
SWITCH DE ACCESO HP ARUBA 2530 - 24G	HW14	2	4	4	3,33
SWITH ETHERNET 12 PUERTOS ADMINISTRABLE:MARCA NET GEAF	HW15	3	3	4	3,33
SWITH HP 5500 SERIE:CN55B9R0J9	HW16	4	5	5	4,67
SWITH HP 5500 SERIE:CN57V9R00K	HW17	4	5	5	4,67

Fuente: Elaboración propia.

Tomando como referencia las amenazas propuestas por *Magerit*, para cada tipo de activo de información se analizaron las amenazas asociadas y se evaluó individualmente su impacto en cuanto a confidencialidad, disponibilidad e integridad utilizando una escala de 0 a 100 por ciento. En el Anexo 2 se presenta a detalle la ponderación utilizada en cada una de las amenazas de acuerdo con el tipo de activo.

Para el análisis de riesgos se tomaron como referencias las vulnerabilidades presentes en la norma ISO 27005 y se identificaron los niveles de impacto y probabilidad de la empresa basados en los lineamientos establecidos por dicha norma.

Dentro de los niveles de impacto, se estipularon los siguientes criterios en el Cuadro 12:

Cuadro 12. Niveles de evaluación de impacto.

IMPACTO	
Bajo	Paralización de actividades de una o dos personas de un departamento.
Medio	Paralización de actividades de una jefatura.
Alto	Paralización de actividades de una dirección.
Catastrófico	Paralización de dos o más direcciones.

Fuente: Elaboración propia.

Dentro de los niveles de probabilidad, a cada valor se le asignó un color y se estipularon los siguientes criterios como se muestra en la Tabla 6.

Tabla 6. Niveles de evaluación de probabilidad.

PROBABILIDAD	
Baja	1% a 25% de ocurrencia
Media	26% a 50% de ocurrencia
Alta	51% a 75% de ocurrencia
Muy alto	76% a 100% de ocurrencia

Fuente: Elaboración propia.

Para determinar el nivel de severidad del riesgo se desarrolló una escala de evaluación. A cada valor analizado se le asignó un color como se muestra en el Cuadro 13.

Cuadro 13. Niveles de evaluación de severidad.

SEVERIDAD	
Baja	- El impacto y la probabilidad son bajos. - Pueden implementarse remediaciones en un periódo de 12 a 18 meses
Media	- El impacto y la probabilidad son moderados. - Pueden implementarse remediaciones en un período de 6 a 12 meses.
Alta	- El impacto y probabilidad son muy altos. - Deben implementarse remediaciones en un período de 3 a 6 meses.

Fuente: Elaboración propia.

Tomando en cuenta los valores y criterios establecidos para el análisis de riesgos, se desarrolló una herramienta para la visualización de los riesgos que enfrenta la organización, conocida como “Mapa de calor del riesgo” Cuadro 14.

Cuadro 14. Mapa de calor del riesgo.

		IMPACTO			
		Bajo	Medio	Alto	Catastrófico
PROBABILIDAD	Baja	Severidad baja	Severidad baja	Severidad baja	Severidad media
	Media	Severidad baja	Severidad baja	Severidad media	Severidad media
	Alta	Severidad baja	Severidad media	Severidad alta	Severidad alta
	Muy alta	Severidad media	Severidad alta	Severidad alta	Severidad alta

Fuente: Elaboración propia.

La asignación del nivel de severidad según el mapa de calor se describe detalladamente en el Anexo 3. Dentro de la matriz de riesgos desarrollada para la empresa, se analizó la inherencia de cada uno de los riesgos identificados.

Posterior a ello se evaluaron los controles con los que cuenta la empresa para mitigar estos riesgos considerando si dichos controles: se encuentran implementados, son obligatorios, están documentados y son eficientes. Mediante esta evaluación se determinó el riesgo residual considerando los criterios establecidos en la Cuadro 15.

Cuadro 15. Criterio de evaluación de controles.

CONTROLES			
Implementado	Obligatorio	Documentado	Eficiente
Reducción de 1 nivel de impacto	Reducción de 1 nivel de probabilidad	No reduce impacto ni probabilidad	Reducción de 1 nivel de impacto y probabilidad

Fuente: Elaboración propia.

En el Cuadro 16 se muestra un extracto de la matriz de riesgos mientras que, en el Anexo 4, se presenta a detalle la evaluación de cada uno de los riesgos considerado en la organización.

Cuadro 16. Matriz de evaluación de riesgos.

				INHERENTE			CONTROLES				RESIDUAL		
Tipo de activo	Amenaza	Vulnerabilidad	Riesgo	Impacto	Probabilidad	Severidad	Implementado	Obligatorio	Documentado	Eficiente	Impacto	Probabilidad	Severidad
HW	Avería de origen físico o lógico	Falta de mantenimiento a los equipos	Interrupción en las operaciones por equipo no disponible	Catastrófico	Alta	Alta	SI	NO	NO	NO	Alto	Alta	Alta
	Contaminación mecánica												
	Errores en la administración de los equipos.	Falta de documentación formal y actualizada del estado de los equipos	Deterioro y/o pérdida del equipo.	Alto	Alta	Alta	NO	NO	NO	NO	Alto	Alta	Alta
	Ataques cibernéticos	Falta de revisión de vulnerabilidades en el sistema.	Pérdida y/o eliminación de información	Catastrófico	Alta	Alta	SI	NO	NO	NO	Alto	Alta	Alta

Fuente: Elaboración propia.

Análisis de la matriz de riesgos

Mediante el análisis realizado al tipo de activo Hardware se determinó que:

- La falta de mantenimiento a los equipos se presenta como una vulnerabilidad de la organización ante amenazas como las averías de origen físico o lógico y la contaminación mecánica, puede desencadenar en un riesgo para la empresa. La interrupción en las operaciones por equipo no disponible involucra un riesgo inherente alto, su impacto es catastrófico para la organización y su probabilidad de ocurrencia es alta. La empresa cuenta con un control implementado; sin embargo, no es de carácter obligatorio, no se encuentra debidamente documentado por lo que no es eficiente en la institución. El resultado final involucra una reducción en el impacto; sin embargo, su probabilidad se mantiene, dando como resultado un riesgo residual con severidad alta.

- Los errores en la administración de los equipos explotan vulnerabilidades en una organización cuando no cuentan con documentación formal y actualizada, resultando en el deterioro y/o pérdida del equipo. El riesgo inherente presenta un impacto alto para la empresa y su probabilidad de ocurrencia es alta, por lo que resulta en una severidad alta. La empresa no cuenta con controles implementados para este riesgo, por lo que su riesgo residual se mantiene en el mismo nivel de severidad.

Mediante el análisis realizado al tipo de activo Software se determinó que:

- La falta de revisión de vulnerabilidades del sistema facilita la ejecución de ataques cibernéticos a la empresa, tiene como riesgo la pérdida y/o eliminación de información. El riesgo inherente presenta un impacto catastrófico y su probabilidad de ejecución es alta, dando como resultado una severidad alta. La empresa cuenta con controles implementados para este riesgo; sin embargo, no son de cumplimiento obligatorio, no se cuenta con documentación oficial para su ejecución y no es eficiente. El riesgo residual presenta una disminución en su impacto, pero su probabilidad se mantiene al igual que su severidad.

- Los errores en la actualización de programas y mantenimiento presentan un impacto catastrófico para la empresa y su probabilidad de ocurrencia es alta cuando existe una falta de supervisión en la actualización de programas y parches. El riesgo inherente tiene una severidad alta, involucra un sistema inoperable. La empresa cuenta con controles implementados y documentados, no obstante, no son de cumplimiento obligatorio y no son eficientes para la organización. Su impacto residual disminuye, pero al mantenerse su probabilidad de ocurrencia, la severidad residual se mantiene en alta.

Mediante el análisis realizado al tipo de activo Personal se determinó que:

- La falta de asignación y socialización de roles y responsabilidades en seguridad informática abren la puerta a deficiencias en la organización, provocando se comprometa la infraestructura crítica de la empresa en caso de ataques cibernéticos. Su riesgo inherente tiene un impacto catastrófico pero una probabilidad media por lo que su severidad inherente es alta. La empresa cuenta con controles implementado; sin embargo, estos no son de cumplimiento obligatorio, no se encuentran documentados y no son eficientes, dando como resultado un riesgo residual con un impacto alto y una probabilidad media, por lo que su severidad residual es media.

- La falta de concientización en el personal provoca que existan fugas de información, corriendo el riesgo de divulgar información confidencial de clientes. El impacto inherente para la empresa es alto y su probabilidad inherente es media por lo que, su severidad inherente es igualmente media. La empresa no cuenta con controles implementados dando como resultado que el riesgo residual se mantenga en el mismo nivel de severidad.

- La capacitación no permanente, al personal en seguridad informática, hace que sean más propensos a sufrir ataques de ingeniería social, dando como riesgo una defensa débil ante ataques cibernéticos. El riesgo inherente tiene un impacto catastrófico y una probabilidad media por lo que su severidad es

alta. La empresa cuenta con controles implementados, no obstante, no son de cumplimiento obligatorio, no se encuentran documentados y no son eficientes. El riesgo residual cuenta con un impacto alto y una probabilidad media por lo que la severidad residual es media.

La empresa se enfrenta a múltiples riesgos cibernéticos, muchos de los cuales, requieren cuentan con una severidad alta. En base al análisis realizado, se planteó el siguiente plan de seguridad informática.

2.3. Propuesta de plan de seguridad informática

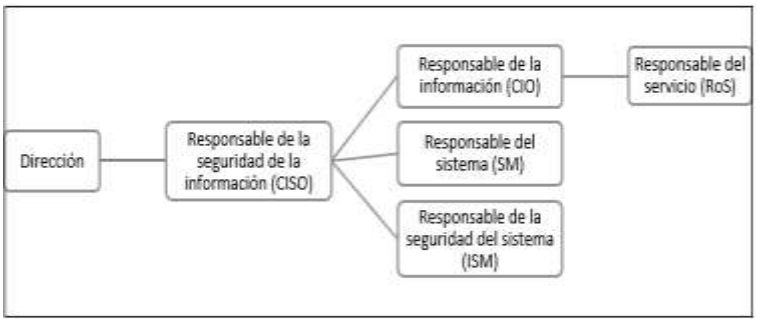
En la presente investigación, se realiza una propuesta de un plan de seguridad informática basado en la norma ISO 27001:2013, para lo cual, se cuenta con las siguientes actividades:

- Difundir la política del S.G.S.I. a los miembros de la organización.
- Asignar roles y responsabilidades al personal involucrado en seguridad de la información.
- Capacitar al personal en temas de seguridad de la información y ciberseguridad.
- Supervisar y mejorar continuamente el S.G.S.I. de la empresa.

Para el cumplimiento de las actividades se cuenta con la duración de un año fiscal. Cada miembro involucrado en la seguridad de la información cuenta con un cargo y responsabilidades designadas dentro del SGSI; donde se cuenta con la siguiente jerarquía.

- La dirección es el organismo líder, quien garantiza que el SGSI cumpla con los objetivos de la empresa.
- El responsable de la seguridad de la información (CISO – Chief Information Security Officer) es el encargado de la seguridad de la información a un nivel ejecutivo.
- El responsable de la información (CIO – Chief Information Officer) es el encargado del estado de la información de la empresa a un nivel técnico.
- El responsable del sistema (SM- System Manager) es el encargado del estado del sistema a un nivel técnico.
- El responsable de la seguridad del sistema (ISM – Information Security Manager) es el encargado de la seguridad de la información a un nivel técnico.
- El responsable del servicio (RoS – Responsable of Service) es el encargado del mantenimiento predictivo, correctivo en la empresa.

Cuadro 17. Jerarquía SGSI.



Fuente: Elaboración propia

Para la difusión de las políticas, se establecen reuniones de comité con los líderes departamentales, los cuales, son los encargados de socializar a cada uno de los miembros de su equipo.

Para la asignación de roles y responsabilidades, la dirección es la encargada de establecer al responsable de la seguridad de la información (CISO). Este por su parte, es el encargado de designar las funciones y cargos a desempeñar a cada miembro de su equipo de trabajo.

En cuanto a capacitación del personal, el responsable de la seguridad de la información (CISO), mediante reuniones con su equipo de trabajo, determinan las necesidades de aprendizaje y se plantean iniciativas. El CISO, expone estas iniciativas ante la dirección, se determina la factibilidad administrativa y financiera y se presentan los resultados al equipo de trabajo.

Para supervisar y mejorar continuamente el S.G.S.I de la empresa, el responsable de la seguridad de la información (CISO), supervisa el cumplimiento de las responsabilidades designadas a cada miembro del equipo, presenta un reporte a la dirección y gestiona los recursos para la mejora continua.

A continuación, se describen las responsabilidades de cada rol del equipo de trabajo. El responsable de la seguridad de la información (CISO) se encarga de las tareas:

- Socializar las políticas, responsabilidades y responsables del SGSI. Esto lo realiza semestralmente y como documento de respaldo cuenta con el reporte de socialización.
- Diseñar el cronograma de mantenimiento, el mismo tiene una duración de un año y cuenta como documento de respaldo al cronograma de trabajo
- Concientizar al personal sobre seguridad de la información. Esto lo realiza bimestralmente y como documento de respaldo cuenta con el informe de capacitación.
- Reportar a la dirección sobre el SGSI de la empresa. Esto se lo realiza bimestralmente y cuenta con el reporte bimestral del SGSI como documento de respaldo.
- Organizar el plan anual de capacitaciones. Esto se lo realiza una vez al año y como documento de respaldo cuenta con el informe de Planificación de capacitaciones.

El responsable de la información (CIO) se encarga de las tareas:

- Reportar al CISO sobre el estado de la información en la empresa, se realiza bimestralmente y cuenta como documento de respaldo el informe de estado de la información.
- Supervisar el mantenimiento de equipos, se realiza trimestralmente y cuenta con el informe de revisión de equipos como documento de respaldo.
- Asistir a todas las capacitaciones planificadas dentro del Plan Anual de Capacitaciones.

El responsable del sistema (SM) se encarga de las tareas:

- Reportar al CISO sobre el estado del sistema de la empresa, se realiza bimestralmente y cuenta con el informe de estado del sistema como documento de respaldo.
- Revisar el funcionamiento de software, se realiza trimestralmente y cuenta con el informe de estado actual de software como documento de respaldo.

- Asistir a todas las capacitaciones planificadas dentro del Plan Anual de Capacitaciones.

El responsable de la seguridad del sistema (ISM) se encarga de las tareas:

- Reportar al CISO sobre el estado de la seguridad de la empresa, se realiza bimestralmente y cuenta con el informe de estado de la seguridad de información como documento de respaldo.
- Analizar vulnerabilidades del sistema se realiza trimestralmente y cuenta con el informe de vulnerabilidades en seguridad de la información como documento de respaldo.
- Asistir a todas las capacitaciones planificadas dentro del Plan Anual de Capacitaciones.

El responsable del servicio (RoS) se encarga de las tareas:

- Realizar el mantenimiento de equipos de manera trimestralmente y cuenta con el Informe de mantenimiento de equipos como documento de respaldo.
- Mantenimiento Switch de core de manera semestralmente y cuenta con el Informe de mantenimiento Switch core como documento de respaldo.
- Asistir a todas las capacitaciones planificadas dentro del Plan Anual de Capacitaciones.

Para la detección y respuesta ante eventos que pongan en riesgo la confidencialidad, disponibilidad e integridad de la información en la empresa, se presenta el siguiente conjunto de medidas:

Detección de incidentes

Técnicas

- El responsable del servicio (RoS) se encarga de identificar el evento de riesgo y aislarlo, presenta un informe sobre los hallazgos identificados y ejecutar las

medidas correctivas asignadas por el responsable de la seguridad de la información (ISM).

- El responsable de la seguridad del sistema (ISM) asigna las medidas correctivas al responsable del servicio (RoS) y presenta un informe al responsable de la seguridad de la información (ISM).

Administrativas

- El responsable de la seguridad del sistema (ISM) informa al responsable de la seguridad de la información (CISO) sobre los hallazgos encontrados y las acciones ejecutadas.
- El responsable de la información (CIO) es el encargado de registrar los eventos suscitados y presentar acciones para evitar se materialice el incidente.

Organizativas

- El responsable de la seguridad de la información (CISO) es el encargado de coordinar la ejecución de actividades para las correcciones necesarias.

Respuesta ante incidentes

Administrativas

- El responsable de la seguridad de la información (CISO) es el encargado de declarar un cese a las actividades involucradas en el incidente y notificar los lineamientos a seguir para mantener el funcionamiento de los procesos.
- El responsable de la seguridad de la información (CISO) informa sobre la situación actual del incidente a la Dirección.
- En caso de que la empresa no cuente con los recursos necesarios, el responsable de la seguridad de la información (CISO) es el encargado de gestionarlos con la Dirección.

Organizativas

- El responsable de la seguridad de la información (CISO) es el encargado de distribuir al personal y los recursos para mitigar el impacto causado.

Físicas

- El responsable de la Seguridad del sistema (ISM) es el encargado de limitar el acceso físico únicamente a personal autorizado hasta que el responsable de la seguridad de la información (CISO) notifique la recuperación del incidente.

Técnicas

- El responsable del servicio (RoS) se encarga de identificar los equipos comprometidos, desconectarlos de la red principal y analizarlos para detectar el punto de partida del incidente.
- El responsable del servicio (RoS) se encarga de informar los hallazgos encontrados al responsable de la seguridad del sistema.
- El responsable de la información (CIO) es el encargado de facilitar las copias de respaldo.

Legales

- El responsable de la seguridad de la información (CISO) reporta a la Dirección sobre el impacto causado en el incidente de seguridad, informando sobre el tipo de información involucrada, el costo monetario y las implicaciones legales existentes.

CAPITULO III. ANÁLISIS DE LOS RESULTADOS

En esta sección se analizan los resultados obtenidos de la encuesta y se validan los mismos utilizando métodos estadísticos.

3.1. Resultados de la propuesta

Para medir el impacto de la propuesta se realizó una socialización en la empresa donde se contó con la colaboración de todos los miembros de la Unidad de Tecnologías de la Información (U.T.I.) y una encuesta, la misma se encuentra conformada por 15 preguntas divididas en cuatro grupos, con el objetivo de determinar:

- El nivel de conocimiento actual con respecto a la norma ISO 27001:2013
- La factibilidad de la propuesta
- La eficiencia de la propuesta
- El beneficio que obtiene la empresa sobre la propuesta

Para cada agrupación se utilizó una escala de cinco niveles: Muy Poco (MP), Poco (P), Neutral (N), Bastante (B), Mucho (M). Cada nivel cuenta con una valoración, la misma va desde 1 a 5 respectivamente.

Para medir el nivel de conocimiento actual con respecto a la norma ISO 27001:2013 se realizó una encuesta Anexo 5 donde se analiza si se logra identificar el nivel de importancia y el criterio de clasificación de un activo según su criticidad dentro del sistema de gestión de seguridad de la información. Igualmente, para medir el nivel de beneficio, factibilidad y eficiencia de la propuesta se realizan varias preguntas, analizando cada uno de los ítems planteados en la propuesta y sí es factible su implementación dentro de la empresa. En la Tabla 7 se observan los resultados obtenidos mediante el instrumento de investigación.

Tabla 1. Resultados de la encuesta.

Fuente: Elaboración propia

3.2. Validación estadística

Coeficiente de Cronbach

Para determinar el nivel de confiabilidad del instrumento de investigación, se efectuó el análisis utilizando el Alfa de Cronbach, utilizando la ecuación:

Ecuación 1 Coeficiente de Cronbach

$$\propto = \left(\frac{K}{K-1}\right)\left[1 - \frac{\sum_{i=1}^{k} S_i}{S_t}\right]$$

Donde:

K = Número de ítems

S_i = Varianza de cada ítem

S_t = Varianza de la suma de los ítems.

Con los valores adquiridos de la encuesta (Tabla 8) se obtiene que:

$$\propto = 0{,}83$$

Tabla 8. Datos obtenidos de la encuesta

Preguntas																
Encuestados	P01	P02	P03	P04	P05	P06	P07	P08	P09	P10	P11	P12	P13	P14	P15	Suma
E1	4	4	5	5	4	5	5	5	5	5	5	5	5	5	4	71
E2	4	4	4	4	3	3	4	5	5	5	5	5	4	5	4	64
E3	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	59
E4	5	5	5	5	3	3	4	4	5	5	5	5	5	5	5	69
E5	5	4	5	2	3	4	2	4	5	5	4	5	4	4	4	60
Varianza	0,2	0,2	0,2	1,2	0,2	0,6	1	0,2	0,2	0,2	0,2	0,2	0,2	0,24	0,2	
Sumatoria de Varianza	5,12															
Varianza de la suma de los Items	22,64															

Fuente: Elaboración propia.

Utilizando la tabla de coeficiente de confiabilidad Tabla 9 se determina que existen una confiabilidad “Muy alta” en la información obtenida de la encuesta realizada (Pinto,2020).

Tabla 9. Interpretación del coeficiente de confiabilidad.

Rangos	Magnitud
0,81 a 1,00	Muy Alta
0,61 a 0,80	Alta
0,41 a 0,60	Moderada
0,21 a 0,40	Baja
0,01 a 0,20	Muy Baja

Fuente: Basado en Pinto (2020).

T de student

Para comprobar la utilidad de la propuesta del plan de seguridad informática en la empresa E.P. – E.M.A.P.A. – A., se realizó una encuesta a los 5 miembros de la Unidad de Tecnologías de la Información. Después de exponer la propuesta del plan de seguridad, se vuelve a realizar una encuesta, donde se obtienen los siguientes resultados:

Tabla 10. Resultados encuesta

Encuestados/ Categoría	1	2	3	4	5
Impacto de la norma ISO/IEC 27001:2013 en la empresa.	48,39%	52,26%	63,23 %	83,23%	49,03 %
	94,67%	85,33%	78,67 %	92,00%	76,00 %

Fuente: Elaboración propia.

A un nivel de confianza del 95% (α =0,05). ¿El nivel de impacto de la norma en la empresa es igual antes que después de la propuesta?

Los sujetos son los mismo en ambas muestras, se trata de un contraste de igualdad de medias con datos emparejados, por consiguiente:

Hipótesis

$H_0 \quad \mu = 0$

$H_I \quad \mu > 0$

Para demostrarlo, se lo realiza mediante la siguiente fórmula en el estadístico de contraste.

Ecuación 2 T de student

$$t = \frac{\bar{X}_D}{\frac{S_D}{\sqrt{n-1}}}$$

Donde:

$\bar{X}_D$ = Media de las diferencias pre y post encuesta

S_D = Desviación estándar.

n = Número de encuestados.

Se obtiene la desviación media:

Tabla 11. Diferencia desviación media

Pre encuesta	**48,39%**	**52,26%**	**63,23%**	**83,23%**	**49,03%**
Post encuesta	94,67%	85,33%	78,67%	92,00%	76,00%
Diferencia	46,28%	33,07%	15,44%	8,77%	26,97%

Fuente: Elaboración propia.

El valor promedio de las diferencias es de 26,11%.

La desviación estándar es de 14,75%.

Reemplazando los valores en la Ecuación 2 se obtiene:

$$t = \frac{26{,}11\%}{\frac{14{,}75}{\sqrt{5-1}}}$$

$$t = 3{,}54$$

Como el contraste es unilateral, se busca en la tabla de T de student (Anexo 6), con 4 grados de libertad, el valor que deja por debajo de sí una probabilidad de 0,95, que resulta ser 2,132.

Tabla 12. Extracto tabla T de student

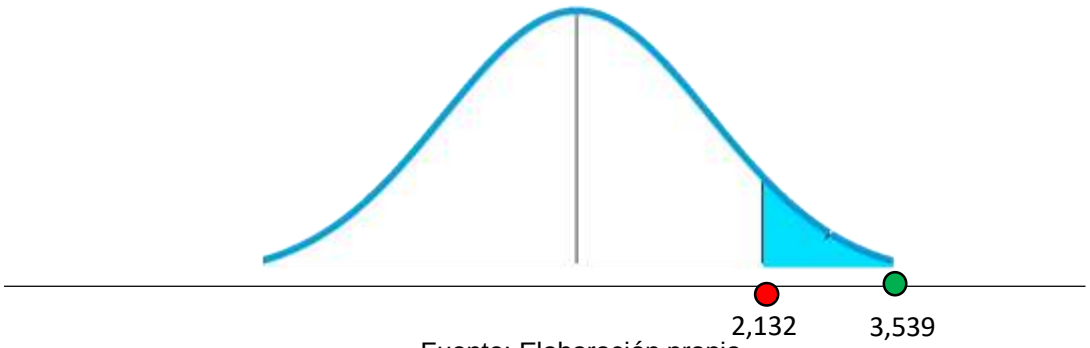
v	**0,6**	**0,75**	**0,9**	**0,95**	**0,975**	**0,99**	**0,995**	**0,9975**	**0,999**	**0,9995**
1	0,325	1,000	3,078	6,314	12,706	31,821	63,656	127,321	318,289	636,578
2	0,289	0,816	1,886	2,920	4,303	6,965	9,925	14,089	22,328	31,600
3	0,277	0,765	1,638	2,353	3,182	4,541	5,841	7,453	10,214	12,924
4	0,271	0,741	1,533	2,132	2,776	3,747	4,604	5,598	7,173	8,610

Fuente: Elaboración propia.

El valor estadístico obtenido es mayor que el valor crítico, por consiguiente, se rechaza la hipótesis nula.

La interpretación sería que la propuesta del plan de seguridad informática es efectiva y tiene un impacto positivo dentro de la organización.

Tabla 13. Interpretación gráfica T de student



Fuente: Elaboración propia.

Mediante la utilización de T de student se pudo demostrar que la empresa tendría un impacto positivo al considerar los lineamientos establecidos en la propuesta de plan de seguridad informática con un 95% de confianza.

CONCLUSIONES

- La fundamentación teórica del estado del arte de la aplicación de planes de seguridad en instituciones de servicio público, permite analizar el uso de la norma ISO 27001:2013, en diferentes organizaciones, brindó parámetros para el desarrollo de un sistema de gestión de seguridad de la información eficaz, adaptado a las necesidades de la empresa y, al ser complementada con la metodología de análisis de riesgos “Magerit”, se enfocó en los lineamientos y requisitos de la organización. Los resultados obtenidos presentan datos favorables, que no son exclusivos para la implementación en la empresa de estudio; sino también, en otras organizaciones similares.

- El conocimiento de la situación actual de la empresa con respecto a la seguridad de la información permitió definir un punto de partida y, el análisis y la selección de los activos de información más importantes para la empresa, se facilita la selección e implementación de controles adecuados y enfocados en la mitigación de los riesgos.

- La determinación de una política de seguridad de la información y la asignación de roles y responsabilidades, acordes a la organización, permitirán, a la empresa detectar incidentes de seguridad antes de que sucedan y dar una respuesta efectiva en caso de materializarse. Las acciones propuestas dentro del plan cubren la necesidad de una mejora dentro de la gestión de seguridad de la información en la empresa.

- La utilización de métodos estadísticos, como el coeficiente de Cronbach y T de student, evidencian que existe coherencia en el planteamiento de las preguntas utilizadas en la encuesta y que las mismas se encuentran alineadas con el plan de seguridad informática propuesto para la organización. La observación de la valoración en cada pregunta es alta y, que la variación existente entre cada encuestado es baja, se demuestra que todo el personal de la Unidad de Tecnologías de la Información valora de manera positiva las iniciativas planteadas en la propuesta de plan de seguridad informática para la empresa.

RECOMENDACIONES

Dentro de las recomendaciones se destaca:

- La necesidad del estudio realizado, toma como referencia los lineamientos establecidos en la norma ISO/IEC 27001:2013. Se recomienda considerando las actualizaciones de la nueva versión de la norma ISO/IEC 27001:2022 para futuros planes de seguridad informática.

- Se recomienda conocer el nivel de madurez, en cuanto a seguridad de una empresa permite determinar un punto de partida para reconocer puntos de mejora. Se recomienda realizar evaluaciones anuales y plantear objetivos para evaluar la eficiencia del sistema de seguridad.

- Sería aconsejable, definir el alcance del sistema de seguridad informática permite delimitar los componentes a ser evaluados y controlados; por lo que, se recomienda expandir el alcance de manera gradual para que los controles implementados sean eficientes.

- Se recomienda la selección de los activos de información más importantes para la empresa facilita la implementación de políticas y controles. Se recomienda expandir el estudio al resto de activos de información y actualizar el análisis de riesgos.

BIBLIOGRAFÍA

Aguilera, P., (2010). *Seguridad informática.* Madrid, España: Editorial Editex, S.A. Recuperado de https://books.google.com.ec/books?id=Mgvm3AYIT64C&printsec=copyright&hl=es&source=gbs_pub_info_r#v=onepage&q&f=false.

Alfaro, I., Vargas, E., (2016). *Diseño del plan de seguridad informática del sistema de información misional de la Procuraduría General de la Nación* (Tesis de Postgrado). Universidad Piloto de Colombia. Disponible en http://repository.unipiloto.edu.co/handle/20.500.12277/2743.

Ampuero, R., (2022). *Gestión de riesgos de la información basado en la metodología MAGERIT para una Notaría de la Región Lima, 2021* (Tesis de Maestría). Universidad César Vallejo. Disponible en https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/85421/Ampuero_HRM-SD.pdf.

Aranzales, R., Giraldo, C., *Documentación de un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa Don Pollo SAS Armenia.* (Tesis de Especialización. Universidad Tecnológica de Pereira. Disponible en https://repositorio.utp.edu.co/items/8fba189c-71a3-43a3-ac5f77e2d3d12d.

Baca, G., (2016). *Introducción a la Seguridad Informática*. Ciudad de México, México: Grupo Editorial Patria. Recuperado de https://books.google.com.ec/books?id=IhUhDgAAQBAJ&lpg=PP1&ots=0XQv2zscFs&dq=plan%20de%20seguridad%20inform%C3%A1tica.

Borja, Y., Sánchez, F., (2015). *Plan de seguridad informática de la ESPE sede Santo Domingo* (Tesis de Maestría). Universidad de las Fuerzas Armadas ESPE. Disponible en http://repositorio.espe.edu.ec/bitstream/21000/12708/1/T-ESPE-049764.pdf.

Buitrago, R., (2020). *Sistemas de Gestión en Seguridad Informática SGSI en Universidades Públicas del Eje Cafetero – Colombia*. (Monografía de especialidad). Universidad Nacional Abierta y a Distancia UNAD. Recuperado de https://repository.unad.edu.co/bitstream/handle/10596/34357/79730104.pdf.

Cárdenas, L., Martínez, H., Becerra, L., (2016). Gestión de seguridad de la información: revisión bibliográfica. *El profesional de la información, 25(6),* 931-948. Doi: https://doi.org/10.3145/epi.2016.nov.10.

Carrera, W., (2012). *Diseño de un Modelo de Gestión de Riesgos de Seguridad de la Información basado en el acoplamiento de la norma ISO/IEC 27005:2008 y el método OCTAVE*. (Tesis de Maestría). Escuela Politécnica Nacional. Disponible en https://bibdigital.epn.edu.ec/bitstream/15000/7942/4/CD-4814.pdf.

Castro, F., (2015). *La Gestión de Capacitación y el Desarrollo de Competencias Laborales en los funcionarios de la Empresa Municipal de Agua Potable y Alcantarillado de Ambato Ep-Emapa-A.* (Tesis de Maestría). Universidad

Técnica de Ambato. Disponible en https://repositorio.uta.edu.ec/jspui/bitstream/123456789/20476/1/T3398M.pdf.

Conde, L., Quezada, P., Hernandez, W., (2019). Propuesta de Arquitectura de mesa de servicios tecnológicos basado en el marco de referencia ITIL V 3.0. *14th Iberian Conference on Information Systems and Technologies* (pág.1-6). Doi: 10.23919/CISTI.2019.8760832.

Crespo, N., (2018). *La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior*. (Tesis de Maestría). Universidad Técnica de Ambato. Disponible en http://repositorio.uta.edu.ec/jspui/handle/123456789/27259.

Cuellar, J., (2020). *Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la institución EDUTEC de los Andes Pitalito, argumentada en la norma ISO/IEC 27001.* (Tesis de Especialización). Universidad Nacional Abierta y a Distancia “UNAD”. Disponible en https://repository.unad.edu.co/handle/10596/34804

Empresa Pública–Empresa Municipal de Agua Potable y Alcantarillado de Ambato “E.P.-E,M,A,P,A,-A”, (2020), *Quiénes Somos*. Ambato. Recuperado de https://www.emapa.gob.ec/nuestra-historia.

Empresa Pública–Empresa Municipal de Agua Potable y Alcantarillado de Ambato “E.P.-E,M,A,P,A,-A”, (2020), Quiénes Somos. Ambato. Recuperado de https://www.emapa.gob.ec/mision-y-vision-2.

Empresa Pública–Empresa Municipal de Agua Potable y Alcantarillado de Ambato “E.P.-E,M,A,P,A,-A”, (2020), Quiénes Somos. Ambato. Recuperado de https://www.emapa.gob.ec/portal/la-ep-emapa-a-mantiene-certificacion-iso-90012015.

Empresa Pública–Empresa Municipal de Agua Potable y Alcantarillado de Ambato “E.P.-E,M,A,P,A,-A”, (2018), Ordenanza Municipal – EP-EMAPA-A. Ambato. Recuperado de https://www.emapa.gob.ec/portal/wp-content/uploads/2018/05/Enero-2018-a36-Ordenanza-creacion.pdf.

Eito-Brun, R.; Calleja Aliaga, C. (2020). La gestión documental en los modelos de gobernanza TIC: presencia y visibilidad de la normativa internacional en el modelo de referencia COBIT. *Revista Española de Documentación Científica*, *43 (3),* 1-14. Recuperado de https://doi.org/10.3989/redc.2020.3.1666.

ESET. (2022). *Security Report Latinoamérica 2022.* Recuperado de https://www.welivesecurity.com/wp-content/uploads/2022/07/ESETsecurity-report-LATAM-2022.pdf.

Fonseca, O., (2019). *Modelo de un sistema de gestión de seguridad de la información en la organización Geoconsult CS*. (Tesis de Maestría). Universidad Ean. Disponible en https://repository.universidadean.edu.co/bitstream/handle/10882/9521/FonsecaOmar2019.pdf?sequence=1

Ferruzaola, E., Duchimaza, J., Ramos, J., & Alejandro, M., (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. *Revista Científica Y Tecnológica UPSE*, 6(1), 34-41. Doi: https://doi.org/10.26423/rctu.v6i1.429.

García, A., Hurtado, C., & Alegre, M., (2011). *Seguridad informática*. Madrid, España: Paraninfo. Recuperado de: https://books.google.com.ec/books?hl=es&lr=&id=c8kni5g2Yv8C&oi=fnd&pg=PA1&dq=tipos+de+seguridad+informa%C3%A1tica&ots.

Gómez, L., Fernández, P., *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad.* Madrid, España: AENOR Internacional.

ISO 27001. (2018), *ISO 27001 todo sobre la norma*. Recuperado de https://normaiso27001.es/.

Jódar, J. (2010). La era digital: Nuevos medios, nuevos usuarios y profesionales. *Razón y Palabra, (71)*. Recuperado de https://www.redalyc.org/pdf/1995/199514914045.pdf.

Mahecha, M., Coello, G., (2016). *Desarrollo de un sistema de información para gestionar la implantación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013*. (Tesis de Maestría). Escuela Superior Politécnica del Litoral. Disponible en https://www.dspace.espol.edu.ec/retrieve/98956/D-106133.pd

Mejía, M., (2022). Software para la Gestión de Riesgos en las Prácticas Forenses de derecho Basado en los Principios de la Norma ISO 31000 e ISO 27005. *Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico, (1)*, 243-257. Disponible en http://doi.org/10.5281/zenodo.6551136.

Mendoza, J., Escobar, L., Caicedo, S., (2019). Actividades de estrategia del servicio de ITIL V3 como lineamientos para la gestión de servicios médicos bajo modalidad de Telesalud. *Revista Colombiana de Tecnologías de Avanzada, 2(34).* 52-61. Disponible en https://ojs.unipamplona.edu.co/ ojsviceinves/index.php/rcta/article/view/63/54.

Molina, M., (2017). Análisis de Riesgos de Centro de Datos basado en la herramienta PILAR de Magerit. *Espirales revista multidisciplinaria de investigación, 1(11).* Disponible en http://dx.doi.org/10.31876/re.v1i11.125.

Montaño, C., (2011). La gestión en la seguridad de la información según COBIT, ITIL e ISO 27000. *Revista Pensamiento Americano, 2(6)*, 21-23. Recuperado de https://dsi.face.ubiobio.cl/sbravo/1-AUDIN/GESTION%20_SEGINF%20.pdf.

Montoya, M., (2020). *Evaluación de riesgo de seguridad de información según ISO 27005, OGITT – Instituto Nacional de Salud*. (Tesis de Maestría). Universidad César Vallejo. Disponible en https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/42553/Montoya_OME.pdf.

Morales, P., Median, P., Ciberseguridad en Plataformas Educativas Institucionales de Educación Superior de la Provincia de Tungurahua – Ecuador. *3 c TIC Cuadernos de desarrollo aplicados a las TIC, 10(2),* 49-75. Recuperado de https://doi.org/10.17993/3ctic.2021.102.49-75.

Mujica, M., (2008). Diseño de un plan de seguridad informática para la UNEXPO. *Publicaciones en Ciencias y Tecnologías, 2(1),* 1-7. Disponible en https://dialnet.unirioja.es/ /servlet/articulo?codigo=6504642.

Niño, N., (2018). *Modelo de un Sistema de Gestión de Seguridad de Información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática – INEI filial Lambayeque*. (Tesis de Maestría). Disponible en https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/5935/BC-TO%20MORANTE.pdf?sequence=1&isAllowed=y

Ñañez, O., (2019). *Modelo de Gestión de Riesgos de TI basados en la norma ISO/IEC 27005 y Metodología Magerit para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza*

– *Chachapoyas Perú.* (Tesis de Maestría). Universidad Nacional Pedro Ruiz Gallo. Recuperado de https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/6110/BC-%20MPOS.pdfsequence=1&isAllowed=y.

Organización Internacional de Estandarización (ISO), (2022). *Glosario*. Recuperado de https://www.iso27000.es/glosario.html.

Ospina, M., Sanabria, P., (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad, 62(2),* 199-217. Recuperado de http://www.scielo.org.co/scielo.php?script= sci_arttext&pid=S1794-31082020000200199.

Palacios, A., Bósquez, V., Palacios, J., Camacho, L., (2019). Auditoría de seguridad informática a la dirección distrital 02D03 Chimbo – San Miguel – Educación, aplicando COBIT 5. *Revista de Investigación, 6(2)*, 1-11. DOI: https://doi.org/10.33789/talentos.6.2.103.

Parra, A., (2014). *ISO 27001 para PYMES*. (Tesis de maestría). Universidad Internacional de La Rioja. Disponible en https://reunir.unir.net/bitstream/handle/123456789/3128/AngelaMaria_Parra_Giraldo.pdf.

Pampín, L. (2016). *Impacto mediático y político del activismo hacker en la sociedad red. Estudio de caso: WikiLeaks.* (Tesis doctoral). Universidad Carlos III de Madrid. Disponible en https://core.ac.uk/download/pdf/ 44311132.pdf.

Pinto, E., (2020). Clima organizacional y su relación con la calidad de servicios de la Empresa IDELCOM S.A.C., Lima, 2019 (Tesis de Maestría). Universidad César Vallejo. Recuperado de: https://hdl.handle.net/20.500.12692/46038.

Prado, J., Rosón, B., Marcos, E., Bueno, P., (2019). Experiencia en la implantación de un Sistema de Gestión de Seguridad de la Información basado en ISO 27000: Sistema Sanitario Público de Galicia. *Revista de la Sociedad Española de Informática y Salud, (134),* 21-23. Disponible en https://seis.es/is-134-abril-2019/.

Proaño, F. (2012). *Modelo de Gestión de TICs para la Gerencia de División de Informática de la Corporación Financiera Nacional, Basado en Gerencia Estratégica de Procesos*. (Tesis de Maestría). Escuela Politécnica Nacional. Disponible en https://bibdigital.epn.edu.ec/bitstream/15000/7815/3/CD-4.pdf

Ramírez, A., Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería*, 16(2), 56-66. Disponible en https://dialnet.unirioja.es/servlet/articulo-codigo=4797252.

Rodríguez, L., Cruzado, C., Mejía, C., Alarcón, M., (2017). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones, 8(3),* e786.

Solano, R., Pérez, D., Bernal, J., (2016). El sistema de información y los mecanismos de seguridad informática en la pyme. *Punto de Vista, 7(11)*, 79-98. Recuperado de https://dialnet.unirioja.es/descarga/articulo/6121657.pdf.

Solarte, F., Enríquez, E., y Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL, 28(5)*, 492-507. Recuperado a partir de http://www.rte.espol.edu.ec/index.php/tecnologica.

Varón, J., (2017). *Estudio de Análisis y Gestión de riesgo al sistema de información de la empresa AGESAGRO S.A.S. utilizando la metodología MAGERIT*. (Tesis de Especialización). Universidad Nacional Abierta y a Distancia UNAD. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/11915/5829971.pdfsequence=1&isAllowed=y.

Velásquez, P., (2018). Comparativa entre las metodologías de análisis y gestión del riesgo NTC-ISO/IEC 27005 y Magerit. *Universidad Piloto de Colombia*. http://repository.unipiloto.edu.co/handle/20.500.12277/8666.

Yungán, J., Narváez, C., (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. *Dominio de las Ciencias*, 8(3), 1025-1041. Recuperado de http://dx.doi.org/10.23857/dc.v8i3.285.

ANEXOS

ANEXO 1 Cuestionario diagnóstico para conocer el nivel de madurez.

ENCUESTA INICIAL

PROPUESTA DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA E.P-E.M.A.P.A.-A.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE - AMBATO

Objetivo: Diagnosticar la situación actual con respecto de la seguridad de la información de la Unidad de Tecnologías de la Información de la empresa E.P-E.M.A.P.A.-A.

Datos demográficos

Nombre: _____ Cargo: _____

Antigüedad en la empresa: _____ Nivel de Educación: _____

Marque con una "X" en la casilla correspondiente a la opción que usted considere pertinente.

[E] Excelente [MB] Muy Bueno [B] Bueno [R]Regular [D] Deficiente

CATEGORIA: SEGURIDAD DE LA INFORMACIÓN					
Pregunta:	E	MB	B	R	D
¿Cuál considera usted que es su nivel de conocimiento actual sobre Seguridad de la información?					
¿Qué nivel de conocimiento tiene usted sobre estándares en Seguridad de la información?					
¿Cuál es su nivel de conocimiento con respecto a los SGSI (Sistema de Gestión de Seguridad de la Información)?					
¿Cuál es su nivel de conocimiento con respecto a la norma ISO 27001?					
CATEGORIA: POLITICAS DE SEGURIDAD DE LA INFORMACIÓN					
Pregunta:	E	MB	B	R	D
¿Qué tan eficientes son las políticas de seguridad de la información que tiene la empresa?					
¿Qué tan eficiente es el proceso de verificación de las políticas de seguridad de la información?					
CATEGORIA: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					
Pregunta:	E	MB	B	R	D
¿Conoce quiénes son los responsables de la seguridad de la información en el departamento?					
¿Conoce cuáles son sus responsabilidades con respecto a la seguridad de la información?					

CATEGORIA: SEGURIDAD EN RECURSOS HUMANOS					
Pregunta:	E	MB	B	R	D
¿Qué tan eficiente es la investigación previa de un trabajador con respecto a su formación académica?					
¿Se indican clausulas relacionadas a la Seguridad de la información en el contrato laboral?					
¿Qué tan eficiente es la capacitación de los empleados con respecto a Seguridad de la información?					
CATEGORIA: GESTIÓN DE ACTIVOS					
Pregunta:	E	MB	B	R	D
¿Qué tan eficiente es el inventario actual de activos relacionados a información de la empresa?					
¿Se han establecido normas con respecto al uso de activos de información?					
¿Se puede identificar claramente los activos por su grado de confidencialidad?					
CATEGORIA: CONTROL DE ACCESO					
Pregunta:	E	MB	B	R	D
¿Existen procesos formales para el registro de usuarios?					
¿Se cuenta con un proceso para la asignación de perfiles de acceso a la información?					
¿El control de acceso a la información cuenta con las limitaciones necesarias?					
CATEGORIA: SEGURIDAD FÍSICA Y DEL ENTORNO					
Pregunta:	E	MB	B	R	D
¿Están definidos controles para el acceso en zonas restringidas?					
¿Se supervisa la actividad del personal en zonas restringidas?					
¿Qué tan eficiente es la protección de los equipos de información con respecto a factores medioambientales?					
CATEGORIA: SEGURIDAD EN LAS OPERACIONES					
Pregunta:	E	MB	B	R	D
¿Existe documentación sobre los procedimientos y responsables con respecto a los recursos de información?					
¿Qué tan eficiente es el sistema de detección de software malicioso?					
¿Se cuenta con medidas de control para vulnerabilidades técnicas "hacking ético"?					
¿Se cuenta con restricciones en la instalación de software en cuanto a personal autorizado?					
CATEGORIA: SEGURIDAD EN LAS COMUNICACIONES					
Pregunta:	E	MB	B	R	D
¿Se establecen controles de acceso a la red tanto para usuarios propios como invitados?					
¿Se establecen políticas para el intercambio de información?					

CATEGORIA: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN					
Pregunta:	E	MB	B	R	D
¿Se establecen requisitos de Seguridad de la información en nuevos sistemas?					

CATEGORIA: RELACIÓN CON PROVEEDORES					
Pregunta:	E	MB	B	R	D
¿Se establece y control requisitos de Seguridad de la información en contratos con terceros?					
CATEGORIA: GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN					
Pregunta:	E	MB	B	R	D
¿Se cuenta con procedimientos de respuesta en caso de incidentes relacionados a la Seguridad de la información?					
CATEGORIA: GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO					
Pregunta:	E	MB	B	R	D
¿Se cuenta con redundancia en los activos críticos de la información?					
CATEGORIA: CUMPLIMIENTO					
Pregunta:	E	MB	B	R	D
¿Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la información?					

ANEXO 2 Análisis de las amenazas de acuerdo con el tipo de activo.

	Amenazas	C	D	I
HW	Fuego		100	
	Daños por agua		100	
	Desastres naturales		100	
	Fuego		100	
	Desastres industriales		100	
	Contaminación mecánica		100	
	Contaminación electromagnética		100	
	Avería de origen físico o lógico		100	
	Corte del suministro eléctrico		100	
	Condiciones inadecuadas de temperatura o humedad		100	
	Errores del administrador	50	80	50
	Errores de mantenimiento / actualización de equipos		100	
	Caída del sistema por agotamiento de recursos		100	
	Pérdida de equipos	50	100	
	Abuso de privilegios de acceso	80	30	100
	Uso no previsto	60	30	60
SW	Avería de origen físico o lógico		100	
	Errores de los usuarios	60	30	80
	Errores del administrador	60	60	60
	Ataques cibernéticos	50	80	50
	Errores de re-encaminamiento	100		
	Errores de secuencia			100
	Alteración accidental de la información			100
	Destrucción de información		100	
	Fugas de información	100		
	Vulnerabilidades de los programas	80	60	30
	Errores de mantenimiento / actualización de programas		80	30
	Suplantación de la identidad del usuario	80		80
	Abuso de privilegios de acceso	70	30	70
	Alteración de secuencia			100
	Acceso no autorizado	80		80
	Modificación deliberada de la información			100
	Destrucción de información		100	
	Divulgación de información	100		
	Manipulación de programas	40	80	60
P	Deficiencias en la organización		100	
	Fugas de información	100		
	Indisponibilidad del personal		100	
	Extorsión	70	70	30
	Ingeniería social	70	20	50

ANEXO 3 Severidad según el nivel de impacto y probabilidad del riesgo.

Severidad	Nivel de impacto	Nivel de probabilidad
Baja	Bajo	Baja
		Media
		Alta
	Medio	Baja
		Media
	Alto	Baja
Media	Bajo	Muy alta
	Medio	Alta
	Alto	Media
	Catastrófico	Baja
		Media
Alta	Medio	Muy alta
	Alto	Alta
		Muy Alta
	Catastrófico	Alta
		Muy Alta

ANEXO 4 Matriz de riesgos E.P. – E.M.A.P.A. – A.

				INHERENTE			CONTROLES				RESIDUAL		
Tipo de activo	Amenaza	Vulnerabilidad	Riesgo	Impacto	Probabilidad	Severidad	Implementado	Obligatorio	Documentado	Eficiente	Impacto	Probabilidad	Severidad
HW	Avería de origen físico o lógico	Falta de mantenimiento a los equipos	Interrupción en las operaciones por equipo no disponible	Catastrófico	Alta	Alta	SI	NO	NO	NO	Alto	Alta	Alta
	Contaminación mecánica.												
	Errores en la administración de los equipos.	Falta de documentación formal y actualizada del estado de los equipos	Deterioro y/o pérdida del equipo.	Alto	Alta	Alta	NO	NO	NO	NO	Alto	Alta	Alta
SW	Ataques cibernéticos	Falta de revisión de vulnerabilidades en el sistema.	Pérdida y/o eliminación de información	Catastrófico	Alta	Alta	SI	NO	NO	NO	Alto	Alta	Alta
	Errores de mantenimiento / actualización de programas	Falta de supervisión en la actualización de programas y parches.	Sistema inoperable	Catastrófico	Alta	Alta	SI	NO	SI	NO	Alto	Alta	Alta
P	Deficiencias en la organización	Falta de asignación y socialización de los roles y responsabilidades en seguridad informática.	Compromiso de la infraestructura crítica de la empresa en ataques cibernéticos	Catastrófico	Media	Alta	SI	NO	NO	NO	Alto	Media	Media
	Fugas de información	Falta de concientización del personal	Divulgación de información confidencial de clientes.	Alto	Media	Media	NO	NO	NO	NO	Alto	Media	Media
	Ingeniería social	Falta de capacitaciones permanente y actualizada en seguridad informática.	Defensa débil ante ataques cibernéticos.	Catastrófico	Media	Alta	SI	NO	NO	NO	Alto	Media	Media

ANEXO 5 Encuesta final E.P. – E.M.A.P.A. – A.

ENCUESTA SOBRE EL ARTICULO CIENTÍFICO

El presente instrumento, se realiza como parte de un trabajo de investigación titulado: "PROPUESTA DE UN PLAN DE SEGURIDAD INFORMÁTICO PARA LA EMPRESA E.P.- E.M.A.P.A.-A.", previa la obtención del título de Magister en Gerencia Informática presentado en la PUCE Sede Ambato.

Objetivo: Determinar el nivel de impacto causado por la propuesta de plan de seguridad informática planteada.

Instrucciones:

Por favor, lea detenidamente las preguntas y responda de acuerdo con la escala indicada.

Se usan los siguientes acrónimos:

UTI: Unidad de Tecnologías de la Información.

Marque con una "X" en la casilla correspondiente a la opción que usted considere pertinente.

[MP] Muy Poco [P] Poco [N] Neutral [B] Bastante [M] Mucho

Pregunta:	MP	P	N	B	M
¿En qué grado puede usted identificar el nivel de importancia de un activo de información dentro del Plan de Seguridad?					
¿En qué nivel puede usted clasificar un activo de información según su nivel de importancia dentro del Plan de Seguridad?					
¿Qué nivel de impacto causaría la implementación de los controles establecidos en la norma ISO 27001:2013 en la empresa?					
En qué nivel considera que es factible para la empresa la implementación de un SGSI adaptado a sus necesidades.					
En qué nivel considera que es factible para la empresa brindar los recursos económicos para capacitar al personal de UTI.					
En qué nivel considera que es factible para la empresa presentar documentación continua sobre el estado actual del Plan de Seguridad.					
¿Considera que una adecuada y periódica socialización del Plan de Seguridad facilitaría la toma de decisiones en caso de materializarse una amenaza?					
¿Considera que un reporte periódico sobre el estado de los activos de información de la empresa puede facilitar la administración de los recursos informáticos?					
¿Considera que es necesario capacitación adecuada en temas relacionados a seguridad de la información?					

¿Considera que es necesario concientizar al personal sobre las amenazas existentes hacia los activos de información de la empresa?					
¿En qué nivel beneficiaria la implementación de procedimientos de respuesta a incidentes informáticos en la seguridad de la información?					
¿En qué grado beneficia a la empresa un Plan de seguridad de la información adaptado a sus necesidades y requerimientos?					
¿En qué grado beneficia a la empresa una correcta definición de roles y responsabilidad dentro del Plan de Seguridad?					
¿En qué grado beneficia a la empresa la socialización de las políticas de seguridad de la información?					
¿En qué nivel beneficia económicamente a la empresa la implementación de un Plan de Seguridad acorde a sus requerimientos?					

ANEXO 6 Tabla T de student

	Intervalo de confianza, *c*					
	80%	90%	95%	98%	99%	99.9%
	Nivel de significancia para una prueba de una cola, α					
gl	0.100	0.050	0.025	0.010	0.005	0.0005
	Nivel de significancia para una prueba de dos colas, α					
	0.200	0.10	0.05	0.02	0.01	0.001
1	3.078	6.314	12.706	31.821	63.657	636.619
2	1.886	2.920	4.303	6.965	9.925	31.599
3	1.638	2.353	3.182	4.541	5.841	12.924
4	1.533	2.132	2.776	3.747	4.604	8.610
5	1.476	2.015	2.571	3.365	4.032	6.869
6	1.440	1.943	2.447	3.143	3.707	5.959
7	1.415	1.895	2.365	2.998	3.499	5.408
8	1.397	1.860	2.306	2.896	3.355	5.041
9	1.383	1.833	2.262	2.821	3.250	4.781
10	1.372	1.812	2.228	2.764	3.169	4.587
11	1.363	1.796	2.201	2.718	3.106	4.437
12	1.356	1.782	2.179	2.681	3.055	4.318
13	1.350	1.771	2.160	2.650	3.012	4.221
14	1.345	1.761	2.145	2.624	2.977	4.140
15	1.341	1.753	2.131	2.602	2.947	4.073
16	1.337	1.746	2.120	2.583	2.921	4.015
17	1.333	1.740	2.110	2.567	2.898	3.965
18	1.330	1.734	2.101	2.552	2.878	3.922
19	1.328	1.729	2.093	2.539	2.861	3.883
20	1.325	1.725	2.086	2.528	2.845	3.850