# ESCUELA DE POSTGRADO NEUMANN

**MAESTRÍA EN**
**GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**


# “Propuesta de mejora de la gestión de seguridad de la información en la empresa mobiliaria PEVISO Ingenieros SAC. Lima – Perú, 2020”

**Trabajo de Investigación**
**para optar el Grado a Nombre de la Nación de:**

Maestro en
Gestión de Tecnologías de la Información

**Autores:**
Bach. Garay Quisbert, Luz Maribel
Bach. Sanchez Seña, Alberto Wilmer

**Docente Guía:**
Mg. Díaz Zelada, Yván Francisco

**TACNA – PERÚ**

**2021**

**Dedicatoria**

A nuestros maestros y familiares que nos brindaron su apoyo y confiaron en nuestro desempeño académico y profesional.

# Índice

## Figuras

**Tablas**

## Resumen

Es para toda empresa Pyme, como Peviso Ingenieros SAC, perceptible la influencia de la Tecnologías de la información y comunicaciones y cada empresa quiere conocer el impacto real, en número y cifras, de su inversión siempre en la búsqueda de alinear todas las inversiones hacia el objetivo del negocio. Cuando se trata de activos informáticos de Hardware y Software percibimos las funcionalidades que nos apoyan en el trabajo día a día, se hace uso del correo electrónico, del software ERP, etc. Sin embargo, cuando hablamos de seguridad la percepción no es tan tangible, por lo menos no en el día a día, es allí donde surge el desconocimiento de la necesidad de un Sistema de seguridad de la información.

Por otro lado, frente a una tendencia mayor de la interconexión y digitalización de la información que a su vez se traduce en un incremento de las amenazas externas hacen fundamental mejorar la protección de la confidencialidad integridad y disponibilidad de la información. El conjunto de medidas para proteger esta información debe estar desarrollado sobre la base de marcos estándar de seguridad que son reconocidos en la región como los estándares de la Organización Internacional de normalización ISO.

Por lo indicado en el Reporte de ciberseguridad de la OEA 2020, muchas empresas, normalmente las empresas pequeñas y medianas, sienten que este esfuerzo requiere de muchos recursos, además que consideran a este tipo de procesos como un accesorio sin un retorno palpable, sin embargo, un trabajo de investigación como éste puede demostrar la facilidad de implementación y los beneficios que apoyan al valor de la empresa.

La propuesta de mejora presentada se desarrolla en cinco capítulos de acuerdo con el siguiente despliegue:

En el Capítulo I se establecen los antecedentes que contiene la problemática interna de la empresa respecto a la seguridad de la información, los objetivos, la justificación, metodología, alcance y límites de esta propuesta.

El Capítulo II, contiene conceptual y teórica, fundamental teóricamente

Contenido: definiciones conceptuales y el uso de modelos metodológicos que apoyan al capítulo IV

El Capítulo III, provee una descripción general de la empresa Peviso Ingenieros SAC con una breve reseña histórica, filosofía organizacional (misión, visión), diseño organizacional y los productos que ofrece la empresa.

El Capítulo IV, comprende el desarrollo de la propuesta iniciando con un diagnóstico situacional para determinar las áreas organizacionales críticas para el negocio para posteriormente efectuar la evaluación y tratamiento de riesgos sobre los activos de información de estas áreas. El tratamiento incluye métricas de seguimiento junto a un cálculo del retorno de inversión de seguridad de la información que presenta la viabilidad de la propuesta.

La presente propuesta finaliza con las conclusiones y sugerencias en el Capítulo V.

## Introducción

La presente propuesta de mejora plantea un Sistema de Gestión de la seguridad de la información para la empresa mobiliaria Peviso Ingenieros SAC con el fin de coadyuvar al logro de sus objetivos estratégicos y como un medio de reestructuración en el actual contexto de pandemia Covid-19 que, debido a la alta digitalización, ha incrementado las amenazas de seguridad de la información sobre vulnerabilidades ya existentes en los activos de información de las empresas.

Para el éxito de este Sistema se reconoció que era fundamental la identificación de las áreas organizaciones críticas de la empresa, por lo que se reunió al grupo de gerentes líderes de cada área a manera de elaborar un primer análisis situacional utilizando las técnicas de PESTEL (Político, económico, social, tecnológico, ambiental y Legal), las 5 fuerzas de PORTER, FODA (Fortalezas, oportunidades, debilidades y amenazas) y la Matriz de análisis estructural o impacto cruzado MICMAC, estableciendo que las áreas críticas corresponden a: i+D, Diseño y Comercial. Luego junto con los gerentes de estas áreas, el Gerente General y el Consultor TI se conformó un grupo de expertos de la empresa con el objetivo de realizar una Medición de capacidad de los procesos de la empresa (CCMI) de los procesos de estas áreas. Como segunda tarea se aprobó la política de seguridad de la información y la metodología de gestión de riesgos alineados a los estándares ISO/IEC 27001:2013, 27004, 27005 y 31000. Con esta metodología se llevó a cabo la evaluación de riesgos iniciando con un relevamiento del inventario de activos de información seguido de la identificación de vulnerabilidades, amenazas, probabilidades y el impacto en la organización que nos conduce a calcular el nivel de riesgo expuesto de cada activo. Por último, se realizó el cálculo del Retorno a la inversión en seguridad (ROSI) utilizando componentes propios a la realidad de la

empresa para el costo total de la pérdida esperada en caso de la materialización del riesgo identificado, así como para el costo de la implementación y adquisición de la solución propuesta para mitigar el riesgo, para éste último se consideraron incluso el costo de la improductividad por la ralentización fruto de la implementación de la solución o herramienta que normalmente no se visualiza pero debe ser considerado por lo menos en una primera iteración.

*Palabras clave*: SGSI, ROSI, MICMAC