

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 Señá, Alberto Wilmer

Docente Guía:

Mg. Díaz Zelada, Yván Francisco

TACNA – PERÚ

2021

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del (los) autor (es)”

Dedicatoria

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

Índice

Índice	4
Figuras	8
Tablas	10
Resumen	11
Introducción	13
CAPITULO I: ANTECEDENTES DEL ESTUDIO	15
1.1. Planteamiento del problema	15
1.2. Objetivos	17
1.2.1. Objetivo general	17
1.2.2. Objetivos específicos	17
1.3. Justificación	18
1.4. Metodología	19
1.4.1. Tipo y diseño	19
1.4.2. Población muestra	19
1.4.3. Técnicas, instrumentos y herramientas	20
1.5. Alcances y limitaciones.	21
1.5.1. Alcances	21
1.5.2. Limitaciones.	21
CAPITULO II: MARCO TEÓRICO	23
2.1. Conceptualización	23
2.1.1. Sistema de Gestión de la Seguridad de la Información (SGSI):.	23

2.1.2. Conceptualización de las técnicas para el diagnóstico situacional	28
2.1.3. Retorno de la inversión en Seguridad de la información.	30
2.1.4. Marco normativo en Perú en relación con la Seguridad de la información	34
2.2. Importancia del Sistema de gestión de seguridad de la información	35
2.3. Modelos	36
2.3.1. Estándar ISO/IEC 27001:2013	36
2.3.2. NIST Marco de ciberseguridad	41
2.3.3. COBIT	41
2.4. Análisis comparativo.....	42
2.5. Análisis crítico.....	43
CAPITULO III: MARCO REFERENCIAL.....	44
3.1. Reseña Histórica	44
3.2. Filosofía organizacional	44
3.2.1. Misión	44
3.2.2. Visión.....	45
3.2.3. Valores corporativos	45
3.2.4. ADN Visso	45
3.3. Diseño Organizacional	46
Gerencia General	46
Externos – Outsourcing	49

3.4. Productos y/o Servicios	49
Productos:	49
3.5. Diagnostico organizacional.....	50
CAPITULO IV: RESULTADOS.....	53
4.1. Diagnóstico situacional	53
4.1.1. Identificación de las unidades organizacionales críticas	53
4.1.2. Conformación del Grupo de expertos de Peviso SAC.....	59
4.1.3. Medición de capacidad de los procesos de la empresa CMMI (Capability Maturity Model Integration) respecto a la seguridad de la información	60
4.2. Diseño de la propuesta de mejora.....	69
4.2.1. Evaluación y tratamiento de riesgos.....	69
4.2.2. Declaración de aplicabilidad.....	111
4.3. Análisis del retorno a la inversión en seguridad ROSI de la propuesta de mejora.	119
CAPÍTULO V: SUGERENCIAS.....	132
5.1. Sugerencias.....	132
5.2. Conclusiones	133
Bibliografía	135
Anexos	139
ANEXO 1	139
ANEXO 2.....	143

ANEXO 3 - Cuestionario para la medición de capacidad de los procesos
de Peviso Ingenieros SAC..... 160

Figuras

Figura 1. Procesos de la empresa Peviso Ingenieros SAC.	15
Figura 2 Diagrama Ishikawa de la problemática actual	16
Figura 3 Matriz MICMAC	30
Figura 4 Ciclo PHVA en la ISO 27001:2013	38
Figura 5 ADN Visso	45
Figura 6 Diseño Organizacional	46
Figura 7 Matriz MicMac aplicado a Peviso	57
Figura 8 Cuadrante MicMac de campos-áreas críticas	58
Figura 9 Cuadro resumen medición de capacidad de los procesos de Peviso Ingeniero SAC	68
Figura 10 Resumen medición de capacidad de los procesos de Peviso Ingeniero SAC	68
Figura 11 Matriz de Inventario y valoración inicial de activos del área de i+D	70
Figura 12 Matriz de Inventario y valoración inicial de activos del área de Diseño	76
Figura 13 Matriz de Inventario y valoración inicial de activos del área de Comercial	82
Figura 14 Cuadro resumen de activos según Tipo de activo	88
Figura 15 Cuadro resumen de activos según su valoración inicial	88
Figura 16 Matriz de análisis y valoración de riesgos del área i+D.....	90
Figura 17 Matriz de análisis y valoración de riesgos del área de Diseño	94
Figura 18 Matriz de análisis y valoración de riesgos del área Comercial	95
Figura 19 Cuadro resumen del Nivel de riesgos de los activos	97
Figura 20 Tratamiento del riesgo del área i+D.....	98
Figura 21 Tratamiento del riesgo del área Diseño	105
Figura 22 Tratamiento del riesgo del área Comercial	107

Figura 23 Cuadro resumen por tipo de control a aplicar.....	110
Figura 24 Comparativa entre el riesgo actual y el postratamiento.....	110
Figura 25 Cuadro resumen del Costo de la solución en porcentaje	128
Figura 26 Costo Directo (TSC-IMPR) en porcentaje	129
Figura 27 Costos TSC, TSC-IMPR y ALE en Nuevos Soles.....	130

Tablas

Tabla 1 Componentes de cálculo del ROSI	32
Tabla 2 Criterios de comparación	42
Tabla 3 Diagnóstico organizacional Peviso Ingenieros SAC	50
Tabla 4 Adaptación del análisis Pestel y las 5 Fuerzas de Porter aplicado a Peviso	54
Tabla 5 Fortalezas y Debilidades identificadas de Peviso	56
Tabla 6 Estado de la medición de la capacidad de los procesos de Peviso Ingeniero SAC	62
Tabla 7 Declaración de aplicabilidad de Peviso Ingenieros SAC de acuerdo con el Anexo A de la ISO 27001:2013.....	112
Tabla 8 Cálculo del Retorno a la inversión en seguridad ROSI de la propuesta de mejora para cada riesgo en tratamiento del área de i+D.....	121
Tabla 9 Cálculo del Retorno a la inversión en seguridad ROSI de la propuesta de mejora para cada riesgo en tratamiento del área de Diseño.	125
Tabla 10 Cálculo del Retorno a la inversión en seguridad ROSI de la propuesta de mejora para cada riesgo en tratamiento del área de Comercial.	126
Tabla 11 Tabla resumen del Costo de la solución en Nuevos Soles.....	128
Tabla 12 Tabla resumen del Costo de la solución en porcentaje	128
Tabla 13 Expectativa de pérdida ALE	130

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