



FACULTAD DE CIENCIAS EMPRESARIALES
CARRERA PROFESIONAL DE INGENIERÍA DE
SISTEMAS DE INFORMACIÓN Y GESTIÓN

“MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL
PROCESO DE GESTIÓN DE RIESGOS DE LA FUNDACIÓN PARA
EL DESARROLLO SOLIDARIO EN EL 2020”

Tesis para optar el título profesional de:
Ingeniero de Sistemas de Información

Presentado por:

Elmer Ivan Santisteban Avalos (0000-0003-2249-8391)

Asesor:

Manuel Antonio Pereyra Acosta (0000-0002-2593-5772)

Lima – Perú

2021

ACTA DE SUSTENTACIÓN DE TESIS

Lima, 01 de abril, 2021

Los integrantes del Jurado de tesis:

Presidente	Mg. Luis Alberto Torres Cabanillas
Miembro 1	Mg. Jose Rodriguez Parra Feria
Miembro 2	Mg. Carlos Federico Díaz Sánchez

Se reúnen para evaluar la tesis titulada:

“MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RIESGOS DE LA FUNDACIÓN PARA EL DESARROLLO SOLIDARIO EN EL 2020”

Presentado por el(la) bachiller.

Elmer Ivan Santisteban Avalos

Para optar el Título Profesional de
Ingeniero de Sistemas de Información y Gestión

Asesorado(a) por:

Manuel Antonio Pereyra Acosta

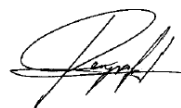
Luego de haber evaluado el informe final de tesis y evaluado el desempeño de(l) (los) estudiantes de la carrera de Ingeniería de Sistemas de Información y Gestión en la sustentación, concluyen de manera unánime (X) por mayoría simple () calificar a:

Tesista:	Elmer Ivan Santisteban Avalos		
Nota (en letras):	14		
Aprobado (X)	Aprobado - Muy buena ()	Aprobado - Sobresaliente ()	Desaprobado ()

Los miembros del jurado firman en señal de conformidad.



Mg. Luis Alberto Torres Cabanillas
Presidente(a) del Jurado



Manuel Antonio Pereyra Acosta
Asesor(a)



Mg. Jose Rodriguez Parra Feria
Miembro 1



Mg. Carlos Federico Díaz Sánchez
Miembro 2

DEDICATORIA

Este trabajo de investigación se lo dedico a mi madre, mis hermanos que me apoyaron y animaron a continuar pese a las dificultades que vive el país.

AGRADECIMIENTOS

Agradecer a la Universidad Científica del Sur por brindarme la enseñanza necesaria para la realización de este proyecto de investigación. Asimismo, a mi asesor el Ing. Manuel Antonio Pereyra Acosta, que me brindó sus conocimientos y el apoyo necesario hasta el término de este proyecto. A la institución Fundación para el Desarrollo Solidario quien me dio la oportunidad de realizar este proyecto en sus instalaciones y a mis compañeros de trabajo. Finalmente, a los ingenieros que aportaron en la validación de los instrumentos que se usaron.

ÍNDICE GENERAL

Dedicatoria	
Agradecimientos	
Índice de figuras	
Índice de tablas	
Índice de anexos	
Resumen	
Abstract	
Introducción.....	1
CAPITULO I PLANTEAMIENTO DEL PROBLEMA	2
1.1. Descripción de la realidad problemática	2
1.2. Formulación del problema	4
1.2.1. Problema general	4
1.2.2. Problemas específicos	4
1.3. Justificación de la investigación	5
1.3.1. Justificación teórica	5
1.3.2. Justificación metodológica	5
1.3.3. Justificación práctica	5
1.3.4. Justificación económica.....	6
1.4. Limitaciones de la investigación	6
1.5. Viabilidad de la investigación	6
CAPITULO II MARCO TEORICO.....	7
2.1. Antecedentes de la investigación	7
2.1.1. Antecedentes nacionales	7
2.1.2. Antecedentes internacionales.....	10
2.2. Bases teóricas	13
2.2.1. Seguridad de la información.....	13
a. Dimensiones de seguridad.....	14
2.2.2. Gestión de riesgo.....	15
a. Valor de un activo	16
2.2.3. Análisis de riesgo	16
2.2.4. Tratamiento de riesgo	18
a. Las salvaguardas	19
2.2.5. Declaración de aplicabilidad.....	20
2.2.6. Metodología Magerit	21
a. Determinación del contexto	23

b. Identificación de los riesgos.....	23
c. La evaluación de los riesgos.....	23
d. El tratamiento de riesgo	24
e. Comunicación y consulta	24
f. Seguimiento y control.....	25
2.2.7. Amenazas	25
a. Identificación de las amenazas	26
2.2.8. La probabilidad de la amenaza.....	26
2.2.9. Vulnerabilidades.....	27
2.2.10. Degradación	27
2.2.11. Control.....	28
2.2.12. Impacto residual.....	28
2.2.13. Metodología	28
2.2.14. Seguridad.....	28
2.2.15. Riesgo	28
2.2.16. Riesgo residual.....	29
2.3. Objetivos de la investigación	29
2.3.1. Objetivo general	29
2.3.2. Objetivos específicos	29
2.4. Formulación de hipótesis	29
2.4.1. Hipótesis general.....	29
2.4.2. Hipótesis específicas.....	29
CAPITULO III: DISEÑO METODOLÓGICO	30
3.1. Diseño de la investigación.....	30
3.2. Tipo.....	30
3.3. Enfoque.....	30
3.4. Población	31
3.5. Muestra.....	31
3.6. Operacionalización de variables	31
3.6.1. Variable dependiente: Gestión de riesgo.....	31
a. Análisis de riesgo.....	32
b. Tratamiento de riesgo	32
3.6.2. Variable independiente: Seguridad de la información.....	33
a. Confidencialidad	33
b. Integridad.....	34
c. Disponibilidad.....	34

3.7. Técnicas para la recolección de datos	34
3.7.1. Descripción de los instrumentos	35
a. Ficha de observación (Valor de riesgo)	35
b. Ficha de observación (Controles)	36
3.7.2. Validez y confiabilidad de los instrumentos	37
a. Validación	37
b. Confiabilidad	37
3.8. Técnica para el procesamiento y análisis de datos	37
3.9. Aspectos éticos	38
CAPITULO IV: RESULTADOS	38
4.1. Estadística descriptiva	40
4.1.1. Gestión de riesgo	40
4.1.2. Evaluación de riesgo	41
4.1.3. Tratamiento de riesgo	43
4.2. Contraste de hipótesis	44
4.2.1. Prueba de hipótesis general	44
4.2.2. Prueba de Hipótesis específica	45
CAPITULO V: DISCUSION, CONCLUSIONES Y RECOMENDACIONES	48
5.1. Discusión	48
5.2. Conclusiones	50
5.3. Recomendaciones	51
REFERENCIAS BIBLIOGRÁFICAS	53
ABREVIATURAS	58
ANEXOS	59
ANEXO 1: MATRIZ DE CONSISTENCIA	59
ANEXO 2: MATRIZ DE OPERACIONALIZACIÓN	60
ANEXO 3: ENCUESTA/INSTRUMENTO DE EVALUACIÓN	61
ANEXO 4: VALIDEZ DE INSTRUMENTOS POR JUECES EXPERTOS	65
ANEXO 5: CONSTANCIA EMITIDA POR LA INSTITUCIÓN DONDE SE REALIZÓ LA INVESTIGACIÓN	71
ANEXO 6. PROCESO DE GESTIÓN DE RIESGO	72
ANEXO 7: IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL EMPLEANDO ISO 27001	116
ANEXO 8: FICHAS DE OBSERVACIÓN	133

ÍNDICE DE FIGURAS

Figura 1. Ciclo PDCA	15
Figura 2. Proceso de riesgo de un activo.....	17
Figura 3. Criterios para el tratamiento de riesgo.	18
Figura 4. Tipos de protección según Magerit.....	20
Figura 5. Activos relevantes según Magerit	22
Figura 6. Proceso de tratamiento de riesgo.	24
Figura 7. Proceso de Gestión de Riesgo.	25
Figura 8. Identificación de las amenazas por Magerit.	26
Figura 9. Gráfico de barras de la gestión de riesgo.....	41
Figura 10. Gráfico de barras de la evaluación de riesgo	42
Figura 11. Gráfico de barras del tratamiento de riesgo.....	43

ÍNDICE DE TABLAS

Tabla 1 Probabilidad de la amenaza	27
Tabla 2 Nivel de vulnerabilidad	27
Tabla 3 Degradación del valor	27
Tabla 4 Variable dependiente	34
Tabla 5 Nivel de Riesgo Pre test y Post test	39
Tabla 6 Muestra descriptiva de la tabla cruzada de la Gestión de riesgo.....	40
Tabla 7 Muestra descriptiva de la tabla cruzada de la Evaluación de riesgo.....	41
Tabla 8 Muestra descriptiva de la tabla cruzada del Tratamiento de riesgo.....	43
Tabla 9 Prueba de Wilcoxon para la Gestión de riesgo.....	44
Tabla 11 Prueba de Wilcoxon para la Evaluación de riesgo.....	45
Tabla 12 Prueba del p-valor en el pre test y post test	45
Tabla 13 Prueba de Wilcoxon para el Tratamiento de riesgo	46
Tabla 14 Prueba del p-valor en el pre test y post test	46

ÍNDICE DE ANEXOS

ANEXO 1: MATRIZ DE CONSISTENCIA	59
ANEXO 2: MATRIZ DE OPERACIONALIZACIÓN	60
ANEXO 3: ENCUESTA/INSTRUMENTO DE EVALUACIÓN	61
ANEXO 4: VALIDEZ DE INSTRUMENTOS POR JUECES EXPERTOS	65
ANEXO 5: CONSTANCIA EMITIDA POR LA INSTITUCIÓN DONDE SE REALIZÓ LA INVESTIGACIÓN	71
ANEXO 6. PROCESO DE GESTIÓN DE RIESGO	72
ANEXO 7: IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL EMPLEANDO ISO 27001.....	116
ANEXO 8: FICHAS DE OBSERVACIÓN	133

RESUMEN

Con el pasar del tiempo vemos un aumento de ataques informáticos, el fácil acceso a la tecnología y el poco conocimiento de algunas personas en seguridad son fuente para causar perjuicio. Por esto, el propósito de la investigación fue implementar una alternativa de solución para el problema de seguridad de la información que existe en la institución Fundación para el Desarrollo Solidario. El objetivo de este estudio es demostrar como la mejora de la seguridad de la información influye en el proceso de gestión de riesgo en la institución. Se propuso la Metodología Magerit con enfoque cualitativo y una población de activos de información para que demuestre como la seguridad mejora con el conocimiento de los riesgos que hay, para esto se dividió en dos fases: pre test y post test. Los resultados que se obtuvieron cuando se propuso las salvaguardas en los activos con riesgo, mostraron que esto tuvo una mejora en seguridad y el riesgo se minimizó; De la misma forma estos resultados se validaron estadísticamente en el SPSS y los instrumentos validados por jueces expertos. De acuerdo con el análisis realizado, se concluye que implementando controles y políticas estas ayudan a mejorar la seguridad de la institución y crear conciencia en cada usuario, manteniendo estable los riesgos y saber cómo actuar frente a cualquier amenaza o incidente, además ellos pueden tomar mejores decisiones en proyectos nuevos y/o actuales en las áreas con respecto a la tecnología.

Palabras clave: Ataques informáticos, seguridad de la información, riesgo, metodología, concientización.

ABSTRACT

Over time we see an increase in computer attacks, easy access to technology and some people's little knowledge of security are a source of harm. For this, the purpose of the research was to implement an alternative solution for the information security problem that exists in the Fundación para el Desarrollo Solidario institution. The objective of this study is to demonstrate how improving information security influences the risk management process in the institution; The Magerit Methodology was proposed with a qualitative approach and information assets for demonstrate how safety improves with knowledge of the risks that exist, for this it's divided this into two phases: pre test and post test. The results that were obtained when I proposed the safeguards in assets with risk, showed that this had an improvement in security and the risk was minimized; The results that were obtained when I proposed the safeguards in assets with risk, showed that this had an improvement in security and the risk was minimized, in the same way, these results were statistically validated in the SPSS and the instruments validated by expert judges. According to the analysis carried out, It is concluded that implementing controls and policies these help to improve the security of the institution and create awareness in each user, risks remain stable and know how to act in the face of any threat or incident, also they will be able to make better decisions on new and / or current projects in areas with respect to technology.

Key words: Computer attacks, information security, risk, methodology, awareness.