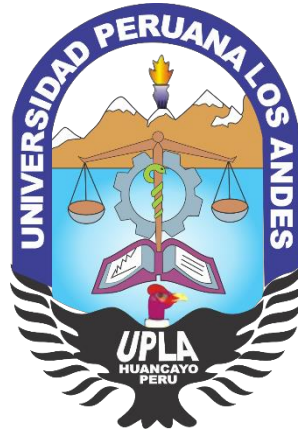


UNIVERSIDAD PERUANA LOS ANDES
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE
INGENIERÍA DE SISTEMAS Y COMPUTACIÓN



TESIS:
SEGURIDAD INFORMÁTICA Y EVALUACIÓN DE RIESGOS EN
LOS ACTIVOS DE INFORMACIÓN DEL INSTITUTO NACIONAL
DE ESTADÍSTICA E INFORMÁTICA – JUNIN

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE
SISTEMAS Y COMPUTACIÓN

Autor:

Bach. HENRY TAIPE ROBLES

Asesores:

Dr. HENRY GEORGE MAQUERA QUISPE

Dr. JHON FREDY ROJAS BUJAICO

Línea de Investigación Institucional:
NUEVAS TECNOLOGÍAS Y PROCESOS

JULIO - DICIEMBRE

HUANCAYO – PERÚ

2020

Dr. HENRY GEORGE MAQUERA QUISPE
ASESOR METODOLÓGICO

Dr. JHON FREDY ROJAS BUJAICO
ASESOR TEMÁTICO

DEDICATORIA

A Nuestro Señor Dios, por cuidarme y bendecirme y protegerme en este recorrido de mi vida.

A mis padres y hermanos, y a toda mi familia por el apoyo y confianza que cada me brindan.

AGRADECIMIENTO

A Dios, por haberme permitido la culminación de este trabajo de investigación y por todas las bendiciones de cada día.

A mis padres, por la confianza que me brindaron y por el apoyo durante toda esta etapa de mi vida personal y académica. A mis hermanos por sus consejos y por todo el apoyo a pesar de las circunstancias.

A cada uno de mis maestros de la Universidad Peruana Los Andes quienes me brindaron su experiencia, conocimientos y enseñanzas. En especial al Dr. Henry George Maquera Quispe por los consejos y asesoría brindada en el desarrollo del presente trabajo de investigación.

Y a todas las personas que influyeron y me apoyaron con sus conocimientos profesionales y que fueron como guías en el desarrollo de la presente Tesis.

HOJA DE CONFORMIDAD DE LOS JURADOS

Dr. CASIO AURELIO TORRES LOPEZ
PRESIDENTE

.....

JURADO 01

.....

JURADO 02

.....

JURADO 03

Mg. MIGUEL ANGEL CARLOS CANALES
SECRETARIO DOCENTE

INDICE

DEDICATORIA	
AGRADECIMIENTO	
INDICE	
INDICE DE TABLAS	
INDICE DE FIGURAS	
RESUMEN	xiv
ABSTRACT	xv
INTRODUCCIÓN	xvi
CAPÍTULO I	18
PLANTEAMIENTO DEL PROBLEMA	18
1.1. Descripción de la Realidad Problemática	18
1.1.1. Identificación de activos de la organización	20
1.1.1.1. Hardware	20
1.1.1.2. Software	21
1.2. Formulación del Problema	24
1.2.1. Problema General	24
1.2.2. Problemas Específicos	25
1.3. Justificación	25
1.3.1. Social	25
1.3.2. Teórica	25
1.3.3. Metodológica	26
1.4. Delimitación del Problema	26
1.4.1. Espacial	26
1.4.2. Temporal	27
1.4.3. Económica	27
1.5. Limitaciones	27
1.6. Objetivos	28
1.6.1. Objetivo General	28
1.6.2. Objetivos Específicos	28
CAPÍTULO II	29
MARCO TEÓRICO	29
2.1. Antecedentes	29
2.1.1. Antecedentes nacionales	29
2.1.2. Antecedentes internacionales	32
2.2. Marco Conceptual	34
2.2.1. Riesgos e Incidencias en la Oficina de la INEI - Junín	34
2.2.2. Seguridad <i>Informática</i> .	34
2.2.3. <i>Plan de seguridad</i> .	34

2.2.4.	<i>Activo de información.</i>	35
2.2.5.	Valoración De Activos	35
2.2.6.	Disponibilidad de los Datos	35
2.2.7.	Autenticidad	35
2.2.8.	Integridad de los datos	36
2.2.9.	Confidencialidad de los datos	36
2.2.10.	Trazabilidad	36
2.2.11.	Amenaza.	36
2.2.12.	Riesgos.	36
2.2.13.	Vulnerabilidad.	37
2.2.14.	Metodología Magerit.	37
2.2.15.	Herramienta PILAR 7.3.3.	37
2.2.16.	Políticas de Seguridad	37
2.3.	Definición de Términos	38
2.4.	Hipótesis	39
2.4.1.	Hipótesis General	39
2.4.2.	Hipótesis Específico	39
2.5.	Variables	39
2.5.1.	Definición Conceptual de la Variable	39
2.5.1.1.	Variable Independiente (X)	39
2.5.1.2.	Variable Dependiente (Y)	39
2.5.2.	Operacionalización de Variables	40
CAPÍTULO III		41
METODOLOGÍA		41
3.1.	Método de Investigación	41
3.2.	Tipo de Investigación	42
3.3.	Nivel de Investigación	42
3.4.	Diseño de la Investigación	42
3.5.	Población	42
3.6.	Muestra	43
3.7.	Técnicas e Instrumentos de Recolección de Datos	43
3.7.1.	<i>Técnicas</i>	43
3.7.2.	<i>Instrumentos</i>	43
a)	<i>[info] Activos Esenciales: Información</i>	44
b)	<i>[info] Activos Esenciales: Servicio</i>	44
c)	<i>[SW] Aplicaciones (Software)</i>	45
d)	<i>[HW] Equipamiento Informático: (Hardware)</i>	46
e)	<i>[COM] Redes de Comunicación</i>	46
f)	<i>[MEDIA] Soporte de Información</i>	47
g)	<i>[AUX] Equipamiento Auxiliar</i>	48

h) [L] Instalaciones	48
i) [P] Personal	49
3.8. Procesamiento de la Información	49
3.9. Aspectos Éticos de la Investigación	49
CAPÍTULO IV	50
RESULTADOS	50
4.1. Planificación	51
4.2. Análisis de Riesgos	52
4.2.1. Tipos de Activos	53
4.2.2. Caracterización de los Activos	53
4.2.2.1. Datos / Información	53
4.2.2.2. Servicio [S]	53
4.2.2.3. Software de Aplicación [SW]	53
4.2.2.4. Equipamiento Informático [HW]	53
4.2.2.5. Redes De Comunicaciones [COM]	54
4.2.2.6. Soporte De Información [MEDIA]	54
4.2.2.7. Equipamiento Auxiliar [AUX]	54
4.2.2.8. Instalaciones [L]	54
4.2.2.9. Personal [P]	54
4.2.3. Valorización de los activos	54
4.2.3.1. Valoración Cualitativa	55
4.2.3.2. Valoración Cuantitativa	55
4.2.4. Criterios de Valoración	56
4.2.5. Valor de la Interrupción del Servicio	57
4.2.6. Dimensiones	57
4.2.7. Nivel de dependencia	59
4.2.7.1. Oficina	60
4.2.7.2. Servicio: Pagina Web	60
4.2.8. Caracterización de las Amenazas	61
4.2.8.1. Frecuencias De Amenazas	62
4.2.8.2. Degradación De Amenazas	62
4.2.8.3. Relación de Frecuencia a Nivel de Impacto	62
4.2.8.4. Componentes involucrados	63
4.2.8.4.1. [EQ-N] Equipos Informáticos (Pc, laptop,	63
4.2.8.4.2. [SO-WIN] Sistema Operativo	64
4.2.8.4.3. [SW-BD] SQL Server 2014	64
4.2.8.4.4. [SW-OFF] Software Ofimático	64
4.2.8.4.5. [SW-ANTI] Antivirus ESET	64
ENDPOINT Security	
4.2.8.4.6. [SW-NAV] Navegadores	64

4.2.8.4.7.	[SOF- PLAT] Plataforma Virtuales	65
4.2.8.4.8.	[RED-n] Redes de Comunicaciones	65
4.2.8.4.9.	[RED- RL] Red LAN.	65
4.2.9.	Estimación del Estado de Riesgos	65
4.2.9.1.	[N] Desastres Naturales	66
4.2.9.2.	[E] Errores y Fallos No Intencionados	66
4.2.9.3.	[A] Ataques Intencionados	66
4.2.10.	Amenazas y vulnerabilidades por activo de información	66
4.3.	Gestión de Riesgos	70
4.3.1.	Valoración de amenazas por cada activo	70
4.3.2.	Identificación y valoración de la salvaguarda	72
4.3.3.	Impacto potencial en cada activo de información	74
4.3.4.	Valoración de riesgos potenciales en activos de información	76
4.4.	Herramienta PILAR 7.3.3	78
4.4.1.	Análisis de Riesgos	78
a)	Datos Del Proyecto	79
4.4.2.	Método de Análisis de Riesgos	79
4.4.3.	Caracterización de los Activos	80
4.4.4.	Identificación de los Activos	81
4.4.5.	Dependencia entre los Activos	82
4.4.6.	Valoración de Activos	83
4.4.6.1.	Dimensiones	84
4.4.6.2.	Criterios de Valoración	84
4.4.7.	Caracterización de las Amenazas.	86
4.4.8.	Identificación de las Amenazas.	86
4.4.9.	Valoración de las Amenazas.	97
4.4.10.	Interpretación de Resultados según la Herramienta Pilar	115
4.4.11.	Gestión de Riesgos	115
4.4.12.	Toma de Decisiones	116
4.4.12.1.	Identificación del Impacto	116
4.4.12.2.	Identificación del Riesgo	116
4.5.	Reglamento de Seguridad	117
4.6.	Control de Seguridad	118
4.7.	Políticas de Seguridad	118
4.8.	Plan De Seguridad Informática basado en las Evaluación de Riesgos de los Activos de Información	120
4.8.1.	Introducción	120
4.8.2.	Verificación y Cumplimiento del Plan de Seguridad	120
4.8.3.	Alcances	121

4.8.4.	Objetivo	121
4.8.5.	Resumen de los Resultados de Análisis de Riesgos de los Activos	121
4.8.6.	Responsabilidades	121
	a) Informática	121
	b) Jefe de Seguridad Informática	122
	c) Director de Sistemas	122
	d) Usuarios	122
4.8.7.	Violación o Incumplimiento de las Políticas de Seguridad	122
4.8.8.	Privilegios Mínimos	123
	a) Identificación de usuarios	123
	b) Seguridad de contraseñas	124
4.8.9.	Niveles de Privilegios	126
	a) Administrador de acceso de usuarios	126
	b) Encriptación de los datos	128
4.8.10.	Seguridad Física	128
	a) Almacenamiento de la información	128
	b) Copiado de información	128
4.8.11.	Seguridad Lógica	128
	a) Distribución de la información	128
	b) Almacenamiento de la información	129
	c) Eliminación de la información	129
4.8.12.	Recuperación frente a un Desastre y Respaldo de la Información	130
	a) Actividades antes al desastre	130
	b) Actividades durante el desastre	131
	c) Actividades después del desastre	132
4.9.	Resultados estadísticos (Pre -Test y Post-Test) de las incidencias y riesgos en los Activos de Información.	133
4.9.1.	Perdida de Información	133
	4.9.1.1. Impacto Potencial de la Perdida de Información:	133
	a) Análisis Descriptivo de Indicador Perdida de Información	134
	b) Prueba de Normalidad de Indicador Perdida de Información	135
	c) Pruebas de Rango de Wilcoxon	136
	4.9.1.2. Validación de la Hipótesis	137
4.9.2.	Robo de Información	137
	4.9.2.1. Impacto Potencial del Robo de Información:	137
	a) Análisis Descriptivo de Indicador Robo de Información	138
	b) Prueba de Normalidad de Indicador Robo de Información	138

c) Pruebas de Rango de Wilcoxon	140
4.9.2.2. Validación de la Hipótesis	140
4.9.3. Modificación de la Información	140
4.9.3.1. Impacto Potencial de la Modificación de la Información:	141
a) Análisis Descriptivo de Indicador Modificación de Información	142
b) Prueba de Normalidad de Indicador Modificación de Información	142
c) Pruebas de Rango de Wilcoxon	144
4.9.3.2. Validación de la Hipótesis	144
4.9.4. Grado de Vulnerabilidad	144
4.9.5. Impacto Potencial:	145
CAPÍTULO V	146
DISCUSIÓN DE LOS RESULTADOS.	146
CONCLUSIONES	152
RECOMENDACIONES	153
REFERENCIAS BIBLIOGRÁFICAS	154
ANEXOS	157
Anexo 1: MATRIZ DE CONSISTENCIA	
Anexo 2: MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES	
Anexo 3: VALIDACIÓN DEL INSTRUMENTO – JUCIO DE EXPERTO	
Anexo 4: INSTRUMENTO – FICHAS DE REGISTRO	
Anexo 5: PRUEBA DE PENETRACIÓN A TRAVÉS DE LA PAGINA DE INTRANET DE LA INEI	

INDICE DE TABLAS

<i>Tabla 01: Cuadro de Activos – Hardware de la Oficina de la INEI – Junín</i>	20
<i>Tabla 02: Cuadro de Activos – Software de la Oficina de la INEI - Junín</i>	21
<i>Tabla 03: Cuadro de Operacionalización de Variables</i>	40
<i>Tabla 04: Cuadro de Población y Muestra</i>	43
<i>Tabla 05: Fichas de Registro de Activos Esenciales - Información</i>	44
<i>Tabla 06: Fichas de Registro de Activos Esenciales - Servicio</i>	44
<i>Tabla 07: Fichas de Registro de Aplicaciones - Software</i>	45
<i>Tabla 08: Fichas de Registro de Equipamiento Informático - Hardware</i>	46
<i>Tabla 09: Fichas de Redes de Comunicación</i>	46
<i>Tabla 10: Fichas de Registro de Soporte de Información</i>	47
<i>Tabla 11: Fichas de Equipamiento Auxiliar</i>	48
<i>Tabla 12: Fichas de Registro de Instalaciones</i>	48
<i>Tabla 13: Fichas de Registro de Personal</i>	49
<i>Tabla 14: Criterios de Valoración de los activos</i>	56
<i>Tabla 15: Valoración de Activos de la Oficina de la INEI - Junín</i>	57
<i>Tabla 16: Frecuencia de Amenazas</i>	62
<i>Tabla 17: Degradación de Amenazas</i>	62
<i>Tabla 18: Relación de Frecuencia del Nivel de Impacto</i>	62
<i>Tabla 19: Amenazas y Vulnerabilidad de los Activos de Información</i>	67
<i>Tabla 20: Frecuencia de Amenazas</i>	70
<i>Tabla 21: Degradación de la Amenazas</i>	71
<i>Tabla 22: Degradación de la Amenazas de la Base de Datos de la Oficina de la INEI - Junín</i>	71
<i>Tabla 23: Nivel de Madurez de Salvaguarda</i>	72
<i>Tabla 24: Nivel de Madurez de Salvaguarda de la Base de Datos</i>	73
<i>Tabla 25: Valor de Impacto Potencial</i>	74
<i>Tabla 26: Degradación de los activos de información</i>	74
<i>Tabla 27: Impacto Potencial de la Base de Datos de la Oficina de INEI</i>	75
<i>Tabla 28: Escala e Impacto, probabilidad de Riesgo</i>	76
<i>Tabla 29: Escala de Riesgo en Relación al Impacto y Frecuencia</i>	76
<i>Tabla 30: Escala de Riesgo de la Base de Datos de la Oficina de la INEI – Junín</i>	77
<i>Tabla 31: Dependencia de activos según el tipo de Activo</i>	82
<i>Tabla 32: Escala detallada de los criterios de valoración</i>	84
<i>Tabla 33: Valoración de los Activos de Información</i>	84
<i>Tabla 34: Identificación de Amenazas a cada uno de los activos de Información</i>	87
<i>Tabla 35: Valoración de las Amenazas</i>	98
<i>Tabla 36: Escala de Degradación en porcentajes</i>	98
<i>Tabla 37: Degradación de Los Activos de Información Proyecto INEI Seguridad Informática</i>	99
<i>Tabla 38: Pre-Test del Indicador Perdida de Información</i>	133
<i>Tabla 39: Post-Test del Indicador Perdida de Información</i>	134
<i>Tabla 40: Pre-Test del Indicador Robo de Información</i>	137
<i>Tabla 41: Post-Test del Indicador Robo de Información</i>	138
<i>Tabla 42: Pre-Test del Indicador Modificación de Información</i>	141
<i>Tabla 43: Post -Test del Indicador Modificación de Información</i>	141

INDICE DE FIGURAS

<i>Figura 01: Croquis de Ubicación del Instituto Nacional de Estadística e Informática</i>	26
<i>Figura 02: Cuadro de Planificación del Proyecto para la Oficina de la INEI – Junín</i>	51
<i>Figura 03: Elementos de Análisis de riesgos</i>	52
<i>Figura 04: Activos de Información</i>	53
<i>Figura 05: Nivel de Dependencia de la Oficina de la INEI</i>	60
<i>Figura 06: Nivel de Dependencia del Servicio Web (Página Web)</i>	61
<i>Figura 07: Herramienta Pilar- Pantalla Principal</i>	79
<i>Figura 08: Datos del Proyecto INEI-SEGURIDAD INFORMÁTICA</i>	79
<i>Figura 09: Análisis de Riesgos – Proyecto INEI Seguridad Informática</i>	80
<i>Figura 10: Caracterización de los activos Riesgos – Proyecto INEI Seguridad Informática</i>	80
<i>Figura 11: Activos de Información – Proyecto INEI Seguridad Informática</i>	81
<i>Figura 12: Tipología de Activos de Información</i>	83
<i>Figura 13: Valoración de Activos – Proyecto INEI Seguridad Informática</i>	83
<i>Figura 14: Caracterización de Amenazas del Proyecto INEI Seguridad Informática</i>	86
<i>Figura 15: Degradación de Los Activos de Información Proyecto INEI Seguridad Informática</i>	99
<i>Figura 16: Identificación de Riesgos de los Activos de Información</i>	115
<i>Figura 17: Identificación del Impacto de los Activos de Información</i>	116
<i>Figura 18: Identificación de riesgos de los Activos de Información</i>	117
<i>Figura 19: Resultados del Análisis Descriptivo – pérdida de información</i>	134
<i>Figura 20: Prueba de Normalidad – pérdida de información</i>	135
<i>Figura 21: Prueba de Normalidad de la pérdida de información (Pre-Test)</i>	135
<i>Figura 22: Prueba de Normalidad de la pérdida de información (Post-Test)</i>	136
<i>Figura 23: Prueba de Rango – pérdida de información</i>	136
<i>Figura 24: Prueba de Significancia – Pérdida de información</i>	136
<i>Figura 25: Resultados del Análisis Descriptivo – Robo de información</i>	138
<i>Figura 26: Prueba de Normalidad – Robo de información</i>	139
<i>Figura 27: Prueba de Normalidad del Robo de información (Pre-Test)</i>	139
<i>Figura 28: Prueba de Normalidad del Robo de información (Post-Test)</i>	139
<i>Figura 29: Prueba de Rango – Robo de información</i>	140
<i>Figura 30: Prueba de Significancia – Robo de información</i>	140
<i>Figura 31: Resultados del Análisis Descriptivo – Modificación de información</i>	142
<i>Figura 32: Prueba de Normalidad – Modificación de información</i>	142
<i>Figura 33: Prueba de Normalidad de Modificación de información (Pre-Test)</i>	143
<i>Figura 34: Prueba de Normalidad de Modificación de información (Post-Test)</i>	143
<i>Figura 35: Prueba de Rango – Modificación de información</i>	144
<i>Figura 36: Prueba de Significancia – Modificación de información</i>	144
<i>Figura 37: Grado de Vulnerabilidad</i>	145
<i>Figura 38: Impacto Potencial</i>	145

RESUMEN

En la actualidad la seguridad informática en las organizaciones es parte importante y fundamental, ya que esto incurre directamente al cumplimiento de sus funciones. En esta investigación se busca identificar los riesgos y vulnerabilidades y establecer controles que inciden en la seguridad de los activos de información.

En primer lugar, se llevará a cabo la identificación y valoración de los activos de información para lo cual se hará uso de la Metodología Magerit para conocer la gestión de Riesgos y las amenazas a los que están expuestos estos activos. Se empleará la Herramienta Pilar para poder graficar la estimación de todos estos resultados y poder así tomar decisiones frente a las amenazas y riesgos.

Los resultados muestran que estos activos de información se encuentran expuestos a riesgos peligrosos, para lo cual se tiene que establecer un plan de seguridad informática para reducir y controlar estos riesgos. Con el plan de Seguridad se pudo optimizar los riesgos y amenazas de los activos de información.

Palabras Claves

Activos, Riesgos, incidencias, Metodología Magerit.

ABSTRACT

Currently, computer security in organizations is an important and fundamental part, since this directly incurs the fulfillment of its functions. This research seeks to identify risks and vulnerabilities and establish controls that affect the security of information assets.

Firstly, the identification and valuation of the information assets will be carried out, for which the Magerit Methodology will be used to know the Risk management and the threats to which these assets are exposed. The Pillar Tool will be used to be able to graph the estimation of all these results and thus be able to make decisions against threats and risks.

The results show that these information assets are exposed to dangerous risks, for which a computer security plan must be established to reduce and control these risks. With the Security plan, the risks and threats of the information assets could be optimized.

Keywords:

Assets, Risks, incidents, Magerit Methodology.

INTRODUCCIÓN

En la actualidad la información es uno de los activos más importantes con los que cuentan las organizaciones y que no necesariamente tienen un gran valor económico y muchos de los que laboran en ellas no le brindan la importancia necesaria para el cuidado o protección, dejándolo así vulnerable a posibles riesgos e incidencias causados por agentes internos o externos y que podría tener un gran impacto, afectando en gran magnitud a las funciones y roles de la organización hasta incluso tener pérdidas irreparables de información y económicas.

En el capítulo I se describe la realidad problemática de la Oficina de la INEI - Junín, y se analiza los activos de información con los que cuenta la Oficina formulando así que estos activos están expuestos a diversos riesgos e incidencias por agentes internos y externos que podrían ser perjudiciales; se establece el análisis en base a la Metodología Magerit para así obtener resultados reales y confiables.

El capítulo II se muestra los conceptos y términos que se utilizarán en el presente trabajo y que están relacionadas a las bases teóricas de la investigación, lo cual sustentan el adecuado desarrollo de la investigación, también se encuentra la hipótesis general y específica planteada en el trabajo de investigación, así como también la Operacionalización de las variables y como estas se relacionan con los indicadores.

El capítulo III se define el método, tipo, nivel y diseño de la investigación, también se define la población y muestra a la cual estará enfocado la investigación. también se muestra las técnicas e instrumentos para la recolección de los datos que nos ayudará al desarrollo del presente trabajo de investigación.

El capítulo IV se muestra la aplicación de la metodología, obteniendo los resultados del análisis de riesgos empezando desde la identificación de los activos de información, caracterización, valorización, dependencias y la gestión de riesgos donde podemos observar la valoración de las amenazas de los activos, así como el impacto y la probabilidad de riesgos e incidencias. Se demuestra los resultados obtenidos del Pre-Test y Post-Test de cada indicador utilizado en la investigación.

En el Capítulo V se desarrolla la discusión de los resultados a manera de explicación, tomando en consideración las variables expuestas y los antecedentes utilizados en el desarrollo del trabajo de investigación.

De los resultados obtenidos se plantearon conclusiones y recomendaciones pertinentes, así como también se adjunta los anexos utilizados en el desarrollo del presente trabajo de investigación.

Bach: Henry Taípe Robles