

ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
GESTION DE TECNOLOGÍAS DE LA INFORMACIÓN



**Propuesta de mejora para el proceso de análisis de riesgo de
activos de información tecnológicos de Cayman Systems**

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

Maestro en
Gestión de Tecnologías de la Información

Autores:

Bach. Jaramillo Vinueza, Carlos Javier
Bach. Jaramillo Vinueza, Michelle Nathaly

Docente Guía:

Mtra. Vargas Fuentes Julissa Alexandra

TACNA – PERÚ

2022

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

MichelleNathalyJaramilloVinuez

INFORME DE ORIGINALIDAD

18%

INDICE DE SIMILITUD

19%

FUENTES DE INTERNET

1%

PUBLICACIONES

10%

TRABAJOS DEL
ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Europea de Madrid Trabajo del estudiante	3%
2	cv.uoc.edu Fuente de Internet	2%
3	www.unp.gov.co Fuente de Internet	1%
4	caymansystems.com Fuente de Internet	1%
5	openaccess.uoc.edu Fuente de Internet	1%
6	hdl.handle.net Fuente de Internet	1%
7	repository.ean.edu.co Fuente de Internet	1%
8	repository.unad.edu.co Fuente de Internet	1%
9	repositorio.epneumann.edu.pe Fuente de Internet	1%

Contenido

RESUMEN.....	5
INTRODUCCIÓN.....	6
CAPITULO I: ANTECEDENTES DE ESTUDIO.....	7
1. Título del Tema.....	7
2. Planteamiento del Problema.....	7
3. Objetivos de la Investigación.....	9
1.1 Objetivo General.....	9
1.2 Objetivos Específicos.....	9
4. Metodología.....	9
1.3 Marco metodológico.....	9
5. Justificación.....	11
5.1 Justificación Teórica.....	11
5.2 Justificación Metodológica.....	13
5.3 Justificación Práctica.....	13
6. Principales definiciones.....	14
7. Alcances y limitaciones.....	15
CAPITULO II: MARCO TEÓRICO.....	16
1. Riesgo.....	16
1.1 Gestión de Riesgos.....	18
1.2 Vulnerabilidad.....	20
1.3 Amenaza.....	21
1.4 Incidente.....	23
1.5 Ataques Informáticos.....	24
2. Activos de información (AI).....	28
2.1 Tipos de activos.....	29
2.2 Atributos de activos.....	30

CAPITULO III: MARCO REFERENCIAL	31
1. Estructura organizacional de Cayman Systems	32
2. Descripción de áreas de Cayman Systems	34
CAPITULO IV: RESULTADOS	39
1. Metodología	39
2. Diagnostico	42
3. Propuestas de mejora.....	55
4. Evaluación de Amenazas y Vulnerabilidades	56
5. Mecanismos de control.....	60
6. Mecanismos de implementación.....	64
CAPITULO V:	66
1. SUGERENCIAS.....	66
2. CONCLUSIONES	71
BIBLIOGRAFÍA.....	73

Tablas

Tabla 1. Principales variables de análisis y sus definiciones.....	14
Tabla 2. Tipos de ataques comunes.....	26
Tabla 3. Identificación de controles actuales	45
Tabla 4. Descripción de proceso	59
Tabla 5. Métricas	61

Figuras

Figura 1. Proceso técnico de la Gestión del Riesgo	19
Figura 2. Etapas de un ataque informático	25
Figura 3. Triangulo de la Intrusión	27
Figura 4. Principios de la seguridad	29
Figura 5. Imagen ubicación Satelital de Cayman Systems.....	31
Figura 6. Diagrama organizacional [10].....	33
Figura 7. Análisis FODA	37
Figura 8. Requisitos ISO 27001.....	40
Figura 9. Periodicidad de eventos	43
Figura 10. Valoración de activos	56
Figura 11. Evaluación de Amenazas y Vulnerabilidades	57
Figura 12. Detección de Mecanismos de Control	57
Figura 13. Diseño de proceso.....	60
Figura 14. Analisis de riesgo	65
Figura 15. Claculo de la evaluación del riesgo	66
Figura 16. Tipos de incidentes.....	67
Figura 17. Valoración del impacto	68
Figura 18. Valoración de la urgencia	68
Figura 19. Matriz de prioridad.....	68
Figura 20. La seguridad Informatica y la gestión de personas	69
Figura 21. Seguridad informática y derecho	70

RESUMEN

Este trabajo de titulación tiene la finalidad de crear una propuesta de mejora para el proceso de análisis de riesgo de activos de información tecnológicos que maneja la empresa Cayman Systems, en base a la realidad de la organización y el proceso actual que manejan, con el objetivo de garantizar que este proceso mejorado ayude a minimizar los riesgos de seguridad que la afectan, mediante el uso de procedimientos adecuados para su debido tratamiento, para de este modo brindar mayor y mejor calidad de atención a sus clientes y usuarios. La metodología usada para llevar a cabo esta propuesta se fundamentó en tres fases: (1) estudio diagnóstico, (2) factibilidad y (3) creación de la propuesta de mejora para el proceso de análisis de riesgo de activos de información tecnológicos, tomando como base las guías que se muestran en la la Norma ISO/IEC 27001:2013 y los lineamientos que se indican en la metodología Magerit, todo esto en base a los requerimientos de la empresa.

Palabras clave: Análisis de riesgo, Activos de información tecnológicos, Cayman Systems, Seguridad de la Información, Magerit, ISO27001.

INTRODUCCIÓN

En la actualidad entendemos por seguridad informática a aquel conjunto de las normas, procesos, procedimientos y herramientas cuyo propósito es mantener siempre la triada de la seguridad de la información, es decir, la integridad, disponibilidad y confidencialidad, así como también se dé el uso correcto a la información que está contenida en los sistemas informáticos de la entidad. Hoy por hoy hay más ciberdelincuentes que pretenden obtener accesos no autorizados a los sistemas informáticos que alojan nuestra información.

Si llegara a darse un acceso no autorizado que ocasione una pérdida de datos, podría llegar a ocasionar en la entidad serios trastornos, y más aún si no contamos con algún sistema de respaldo y backup que ejecute copias de seguridad de nuestros sistemas.

La exfiltración de la información importante para una empresa podría acarrear incluso problemas legales que pueden afectar su reputación institucional que afecte seriamente la confianza de los clientes de la entidad.

Por tal motivo el presente trabajo tiene como objetivo realizar una propuesta de mejora para el proceso de análisis de riesgo de activos de información tecnológicos de Cayman Systems. El presente documento está conformado por cinco capítulos en los cuales se describe a mayor detalle cada uno de los temas que fueron usados para el desarrollo de este trabajo de titulación. Como resultado final de la ejecución de esta propuesta se logró mejorar el proceso que actualmente se maneja, tomando como base los dominios, controles y objetivos que se encuentran del Anexo A de la norma ISO 27001 y su relación con la realidad de la empresa Cayman Systems.