ESCUELA DE POSGRADO NEWMAN

Maestría en
Gestión de Tecnologías de la Información

Propuesta de Mejora en la Gestión de la Seguridad Informática de la Empresa KITTON S.A, Guayaquil – Ecuador, 2022

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

Maestro en
Gestión de Tecnologías de la Información

Autores:
Bach. Peña Chávez, Arturo Danilo
Bach. Aguiar Mendoza, Jorge Washington

Docente Guía:
Mg. 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)”

JorgeWashingtonAguiarMendoz

INFORME DE ORIGINALIDAD

11%	11%	0%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

ENCONTRAR COINCIDENCIAS CON TODAS LAS FUENTES (SOLO SE IMPRIMIRÁ LA FUENTE SELECCIONADA)

4%

★ www.veeam.com

Fuente de Internet

Excluir citas	Activo	Exclude assignment template	Activo
Excluir bibliografía	Activo	Excluir coincidencias	< 15 words

Declaración Expresa de Autoría

Ing. **Arturo Danilo Peña Chávez y** el Ing**. Jorge Washington Aguiar Mendoza**, declaran que en el presente trabajo de investigación son responsables del contenido, cuyo tema es "**Mejora en la Gestión de la Seguridad Informática de la Empresa Kitton S.A, Guayaquil – Ecuador, 2022**" es de nuestra auditoria y los derechos patrimoniales únicamente de la Escuela de Postgrado Neumann.

Los derechos que como autores nos corresponde, con excepción de la presente autorización, seguirán a nuestro favor, de acuerdo a lo establecido en los artículos 5,6,8 y entre otros de la Ley de Propiedad Intelectual y su reglamento.

_____	_____
Arturo Danilo Peña Chávez	Jorge Washington Aguiar Mendoza
C.I.0923917470	C.I.1312714544

Índice

DECLARACIÓN EXPRESA DE AUTORÍA **2**

RESUMEN **5**

INTRODUCCIÓN **6**

CAPITULO I: ANTECEDENTES DE ESTUDIO **8**

TÍTULO DEL TEMA 8
PLANTEAMIENTO DEL PROBLEMA 8
1. OBJETIVOS DE LA INVESTIGACIÓN 12
1.1. Objetivo General *12*
1.2. Objetivos Específicos *12*
2. METODOLOGÍA 12
2.1. Tipo y diseño de Investigación *12*
2.2. Fases de la investigación aplicada *13*
4.2.1 Planificación *13*
4.2.2. Ejecución *13*
4.2.3 Publicación de resultados *14*
4. JUSTIFICACIÓN 15
5. PRINCIPALES DEFINICIONES 16
6. ALCANCES Y LIMITACIONES 16

CAPITULO II: MARCO TEÓRICO **18**

7. MARCO TEÓRICO 18
7.2. Seguridad informática *18*
7.3. Estrategias de seguridad informática *19*
7.4. Gestión *20*
7.5. Gestión de riesgo de la seguridad informática. *20*
7.6. Amenazas de la seguridad de la información *21*
7.7. Hacker *21*
7.8. Virus Informático *22*
7.9. Antivirus *22*
7.10. Spam *22*
7.11. Normas y metodologías internacionales *23*
7.12. Gestión de seguridad informática *23*

CAPITULO III: MARCO REFERENCIAL **25**

8. MARCO REFERENCIAL 25
8.2. Reseña Histórica y filosofía organizacional *25*
8.3. Visión *25*
8.4. Misión *25*
8.5. Valores *26*
8.6. Políticas de calidad *26*
8.7. Diseño Organizacional *28*
8.8. Productos y Servicios *31*
8.9. Diagnóstico organizacional o sectorial *33*
9. CRONOGRAMA 35

CAPITULO IV: PROPUESTA DE MEJORA **35**

10. DIAGNOSTICO ..... **¡ERROR! MARCADOR NO DEFINIDO.**
10.1 FUENTE DE INVESTIGACION POR PROYECTO DE MEJORA 35
10.2 VENTAJAS Y DESVENTAJAS DE LAS SOLUCIONES BAAS Y DRAAS. 39

11 DISEÑO DE MEJORA 46
12 CAPITULO V 48
CONCLUSIONES....48
13 ANEXOS 50
Proceso de Mejoramiento de la infraestructura tecnológica 50
14 DOCUMENTACIÓN DEL PROCESO 54
15 ACTA DE ENTREGA Y SALIDA DE EQUIPOS DE LA EMPRESA KITTON S.A 55
ÍNDICE DE ILUSTRACIONES....59
ÍNDICE DE TABLAS....60
16 BIBLIOGRAFÍA....61

Resumen

El avance de los medios tecnológicos y de comunicación han provocado un gran surgimiento de vulnerabilidades y ataques delictivos, donde han transformado al Internet y las nuevas tecnologías en posibles amenazas en los sistemas informáticos presentes en diferentes empresas y organizaciones. Las pequeñas empresas que cuentan con un departamento de informática en su mayoría de sus procesos y manejo de seguridad informática lo resuelven cuando se presentan las incidencias en ese momento, llevándoles tiempo, costo y perdidas a nivel software y hardware. El desconocimiento y poco uso de planes de mejoras, planes de riesgos, inventarios, normas ISO y entre otras, provoca una despreocupación en la gestión de seguridad informática y un ejemplo claro es la empresa Kitton S.A, Guayaquil – Ecuador que presentó varias problemáticas y a pesar de resolverlas inmediatamente no está garantizado que estén preparados para vulnerabilidades grandes y al corregir esto, potenciáramos o redujéramos el grado de inseguridad informática de esta entidad. Lo más importante en una empresa es entender, estudiar y resolver su comportamiento de manera interna y externa para su evolución dentro de la sociedad, mediante este trabajo de investigación diseñaremos un plan de mejora en la gestión de seguridad informática, asegurando y reduciendo algunas situaciones que se presenten en el estudio con estrategias concretas que solo dependerán de la misma adaptarlas para asegurar el patrimonio de todos que lo conforman.

Palabras Clave: seguridad informática, plan de mejora, tecnología.

Introducción

La seguridad informática en las empresas dentro del área o departamento informático necesita estrategias eficientes para estar prevenidos en algún sin número de vulnerabilidades, por eso se realiza este trabajo de investigación para la entidad Kitton S.A, Guayaquil – Ecuador, con la finalidad de realizar un plan de mejora que este basado en un estudio o diagnóstico que nos permita diseñar un plan de riesgo con sus mecanismos de control correspondiente, tomando en cuenta la reglamentación o norma ISO que estén utilizado para el orden de procesos dentro de la organización.

Este plan de mejora permitirá a la empresa aplicar cambios correctivos en el manejo de seguridad informática, estableciendo un proceso guía para los usuarios que forman parte del departamento de tecnologías, dando la facilidad y accesibilidad a pasos a seguir en cada vulnerabilidad o actividad que hay que tener presente, durante un tiempo o etapa del año que ejecuta la empresa dentro de su planificación y sus objetivos.

El diagnóstico y estudio del entorno de la organización es la parte fundamental para poder realizar la propuesta y plan de mejora, conocer la empresa y sus fines, funcionamiento del departamento de diit y sus relaciones entre los demás, inventarios de software y hardware, antecedentes, ayudarán a fortalecer este estudio siendo más confiable y seguro para establecer medidas en la gestión informática.

Las nuevas tendencias o cambios tecnológicos no solo nos orillan a esta propuesta, sino a enfocar y orientar a la organización en la importancia de la seguridad informática y sus procesos establecidos, beneficiando a futuro menos

inversión económica, más rendimiento laboral, hardware y software actualizados, personal altamente capacitados y el bienestar saludable del negocio en el ambiente informático.