



**UNIVERSIDAD CÉSAR VALLEJO**

**FACULTAD DE INGENIERÍA Y ARQUITECTURA  
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**Plan de gestión de riesgos de tecnologías de la información para  
la seguridad informática en una empresa inmobiliaria, Casma  
2023**

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:**

Ingeniero de Sistemas

**AUTOR:**

De la Cruz Mejia, Cristhian Paul ([orcid.org/0000-0003-2607-4617](https://orcid.org/0000-0003-2607-4617))

**ASESOR:**

Dr. Agreda Gamboa, Everson David ([orcid.org/0000-0003-1252-9692](https://orcid.org/0000-0003-1252-9692))

**LÍNEA DE INVESTIGACIÓN:**

Sistema de la Información y Comunicaciones

**LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:**

Desarrollo económico, empleo y emprendimiento

TRUJILLO – PERÚ

2023

### **Dedicatoria**

A Dios por acompañarme en todo momento.

A mis Padres por su amor y cuidado desde mi nacimiento.

A mi familia por ser lo más maravilloso que tengo en la vida.

Cristhian Paul

## **Agradecimiento**

A la Universidad César Vallejo por contribuir en lograr una meta tan anhelada.

A la empresa Inmobiliaria por la información compartida en esta investigación.

A mi Asesor de tesis por su orientación metodológica.

El autor

## Índice de contenidos

	Pág.
Carátula .....	i
Dedicatoria .....	ii
Agradecimiento .....	iii
Índice de contenidos .....	iv
Índice de tablas .....	v
Índice de figuras .....	vi
Resumen .....	vii
Abstract .....	viii
I. INTRODUCCIÓN .....	1
II. MARCO TEÓRICO .....	4
III. METODOLOGÍA.....	9
3.1 Tipo y diseño de investigación .....	9
3.2 Variables y operacionalización .....	9
3.3 Población, muestra y muestreo .....	10
3.4 Técnicas e instrumentos de recolección de datos.....	11
3.5 Procedimientos .....	12
3.6 Método de análisis de datos.....	13
3.7 Aspectos éticos .....	13
IV. RESULTADOS .....	14
V. DISCUSIÓN.....	23
VI. CONCLUSIONES.....	25
VII. RECOMENDACIONES .....	26
REFERENCIAS.....	27
ANEXOS .....	31

## Índice de tablas

	Pág.
Tabla 1. Población.....	10
Tabla 2. Examen de normalidad del indicador uno .....	17
Tabla 3. Examen de normalidad del indicador dos.....	18
Tabla 4. Examen de normalidad del indicador tres .....	19
Tabla 5. Examen de Wilcoxon para el indicador uno .....	20
Tabla 6. Examen de Wilcoxon para el indicador dos.....	21
Tabla 7. Examen de Wilcoxon para el indicador tres .....	22

## Índice de figuras

	Pág.
Figura 1. Promedio de preprueba y posprueba del indicador uno.....	14
Figura 2. Promedio de preprueba y posprueba del segundo indicador dos. ....	15
Figura 3. Promedio de preprueba y posprueba del segundo indicador tres. ....	16

## Resumen

Esta investigación tuvo como objetivo general mejorar la seguridad informática en una empresa inmobiliaria de la ciudad de Casma en el año 2023 mediante la propuesta de un plan de gestión de riesgos de tecnologías de la información. El tipo de investigación fue aplicada y de diseño preexperimental. Se determinó una muestra poblacional de 10 colaboradores, los cuales fueron evaluados mediante una Encuesta de satisfacción. El desarrollo de la solución tecnológica propuesta fue bajo la aplicación de las buenas prácticas de gestión de riesgos informáticos. Como resultado principal se tuvo: para el primer indicador, se logró minimizar el nivel de riesgos en seguridad informática por errores humanos en 64%; para el segundo indicador, se logró minimizar el nivel de riesgos en seguridad informática por errores de hardware en 66.00% y; para el tercer indicador, se logró minimizar el nivel de riesgos en seguridad informática por errores de software en 70%. Como conclusión general, se tuvo que, la propuesta de un plan de gestión de riesgos de TI mejora significativamente la seguridad informática en una empresa inmobiliaria casmeña.

Palabras clave: Plan, Gestión de riesgos, Tecnologías de la información, Seguridad informática, Empresa inmobiliaria.

## **Abstract**

The general objective of this research was to improve computer security in a real estate company in the city of Casma in the year 2023 by proposing an information technology risk management plan. The type of research was applied and of pre-experimental design. A population sample of 10 collaborators was determined, which were evaluated by means of a satisfaction survey. The proposed technological solution was developed under the application of good IT risk management practices. The main result was: for the first indicator, the level of computer security risks due to human errors was minimized by 64%; for the second indicator, the level of computer security risks due to hardware errors was minimized by 66%; and for the third indicator, the level of computer security risks due to software errors was minimized by 70%. As a general conclusion, it was found that the proposal of an IT risk management plan significantly improves IT security in a real estate company in Casmeña.

Keywords: Plan, Risk Management, Information Technology, Information Security, Real Estate Company.



## I. INTRODUCCIÓN

En los tiempos recientes, según Gestión (2020), el empleo de las tecnologías de la información (TI) es un factor esencial en el triunfo de la gestión empresarial, y es por este motivo, que se tienen mayormente a empresas que recurren a programas que les permitan administrar y gestionar un valioso recurso, como es el caso de los datos. Sin embargo, la verdad es que existen ciertos riesgos asociados con el uso de TI en un entorno empresarial, ya sea que se trate de daños accidentales por parte de los empleados o intentos deliberados de intrusos de acceder ilegalmente a la información de la empresa para explotarla. Aquí, es donde nuestro negocio puede verse seriamente comprometido, porque después de todo, el valor de la información es enorme hoy en día. Por eso es importante que tengamos una estrategia y herramientas que nos permitan evaluar e identificar todos los riesgos asociados al uso de las TI con el fin de minimizarlos.

Para la Escuela Europea (2022), las compañías actuales adelantan con sus planes de digitalización con favores predecibles, pero además con mayores inquietudes sobre la gestión de riesgos de TI. La alineación oportuna de la administración de peligros de TI con esta nueva atmósfera de intimidaciones es la contestación que buscan las compañías para enfrentar el reto planteado. La gestión de riesgos de TI es más que proteger los datos almacenados en su computadora, dispositivos, redes y hasta medios en línea se sitúan bajo el atento vistazo de planes de riesgo dedicados. La administración de peligros de TI debe identificar, evaluar y clasificar las amenazas, priorizarlas, planificar medidas y tácticas para eliminarlas y, aun cuando ello no sea factible, disminuir o paliar el peligro, o por último asignarlo o concederlo.

En este escenario, se contó con una **compañía Inmobiliaria**, localizada en la provincia de Casma, departamento de Ancash, dedicada al rubro inmobiliario, siendo su actividad principal la búsqueda de terrenos o lotes por medidas delimitantes o hectáreas que, luego pasará por una evaluación a fin de darle un valor agregado mediante la ejecución de obras civiles (edificaciones) destinados a la creación de departamentos y casas para uso doméstico y también para uso ejecutivo como el caso de oficinas.

Se tuvo ciertas deficiencias (**problemas específicos**) que se presentaron como parte del proceso de la administración de los peligros de tecnologías informáticas fueron: Inconvenientes en personas, fundamentalmente del operador informático y especialmente si no cuenta con la necesaria cualificación. Estos inconvenientes se debieron a una mala programación o una mala gestión de los recursos; Accidentes, desastres y robo del hardware, desde la destrucción accidental de discos que contienen datos importantes hasta robos y catástrofes de la naturaleza; Las intimidaciones e intromisiones a nivel de software, los ataques cibernéticos, la intromisión de terceros no autorizados en los programas informáticos de la compañía o la operación de malware han causado daños irreparables.

Se tuvo la **formulación del problema**: *General*: ¿En qué manera un plan de administración de riesgos de TI afecta la seguridad informática en una empresa inmobiliaria de la ciudad de Casma en año 2023? *Específicos*: Deficiencia concreta 1 - ¿En qué manera un plan de gestión de riesgos de TI afecta el nivel de riesgos en seguridad informática por errores humanos en la empresa inmobiliaria de la ciudad de Casma en año 2023? Deficiencia concreta 2 - ¿En qué manera un plan de gestión de riesgos de TI afecta el nivel de riesgos en seguridad informática por errores de hardware en la empresa inmobiliaria de la ciudad de Casma en año 2023? Deficiencia concreta 3 - ¿En qué manera un plan de gestión de riesgos de TI afecta el nivel de riesgos en seguridad informática por errores de software en la empresa inmobiliaria de la ciudad de Casma en año 2023?

Se tuvo la **justificación de la Investigación**: *Conveniencia*: condescendió a la compañía inmobiliaria minimizar los riesgos tecnológicos a nivel de errores humanos, problemas de hardware y de software, otorgando a la empresa confiabilidad en su manejo de información; *Relevancia social*: otorgó confianza en el procesamiento de los datos de los colaboradores, aplicando buenas prácticas de seguridad informática, minimizando riesgos en todo momento; *Utilidad metodológica*: representó la base científica de cercanas investigaciones relacionadas la administración de riesgos tecnológicos sobre todo en el rubro inmobiliario que tiene auge en estos tiempos; *Implicaciones prácticas*: contribuyó a solucionar inconvenientes de

seguridad informáticas vinculados a errores humanos, hardware y software; *Valor teórico:* valió para comprender con detalle las bases teóricas concerniente a planes de gestión de riesgos tecnológicos.

Se tuvo los **objetivos:** *General:* Maximizar la seguridad informática en una empresa inmobiliaria de la ciudad de Casma en el año 2023 mediante la ejecución de un plan de gestión de riesgos de TI; *Específicos:* Finalidad específica 1 - Minimizar el nivel de riesgos en seguridad informática por errores humanos; Finalidad específica 2 - Minimizar el nivel de riesgos en seguridad informática por errores de hardware; Finalidad específica 3 - Minimizar el nivel de riesgos en seguridad informática por errores de software.

Se tuvo las **hipótesis:** *General:* “El plan de gestión de riesgos de TI maximiza cuantiosamente la seguridad informática de la compañía inmobiliaria de la ciudad de Casma en el año 2023”. *Específicas:* Supuesto específico 1 - “El plan de gestión de riesgos de TI minimiza el nivel de riesgos de seguridad informática por errores humanos en la compañía inmobiliaria de la ciudad de Casma en el año 2023”; Supuesto específico 2 - “El plan de gestión de riesgos de TI minimiza el nivel de riesgos en seguridad informática por errores de hardware en la compañía inmobiliaria de la ciudad de Casma en el año 2023”; Supuesto específico 3 - “El plan de gestión de riesgos de TI minimiza el nivel de riesgos en seguridad informática por errores de software en la compañía inmobiliaria de la ciudad de Casma en el año 2023”.

## II. MARCO TEÓRICO

En el vigente estudio se encontraron **antecedentes** concernientes a estudios preliminares como:

Valverde (2022) en su estudio solicitó la implementación de la administración de peligros TI para optimizar la seguridad informática de la empresa anunciante, permitiendo mitigar riesgos, prevenir ataques informáticos y manipulación de datos, por lo que determinó los niveles aceptables de confidencialidad, integridad y disponibilidad. La metodología para llevar a cabo esta gestión de riesgos fue MAGERIT, debido a que se realizaron una serie de ciclos para realizar un análisis de riesgos, y así se pudo recibir respuestas a los riesgos ocasionados por la empresa y así también eliminarlos. gestión de la seguridad de la información. En resumen, se pudo afirmar que durante la implantación de la administración de peligros de TI aplicando la metodología MAGERIT, se logró crear controles que permitieron optimizar la seguridad informática de las compañías, lo que determinó un avance significativo.

Rivera (2019) en su estudio planteó un plan de mitigación de riesgos TI del Hospital de Catacocha para el departamento TIC, que permitió identificar vulnerabilidades que afectan a la seguridad informática, pues la institución estatal maneja gran cantidad de información sensible y confidencial, considerando que los datos solo fueron soportados para los externos. unidades y no se han tomado medidas de seguridad porque depende de una entidad externa que ha dado un presupuesto anual limitado. Se aplicó la metodología MAGERIT con los modelos de empresa de Deloitte para crear una tabla matricial de riesgo inherente y una tabla matricial de peligro residual, para identificar qué tan abierta estaba la institución a los riesgos ante una posible situación y así crear una comparación que muestre el resultado. riesgos que pueden ser evaluados, aceptados, reducidos y transferidos.

Moscoso y otros (2018) en su estudio buscaron contribuye al desempeño de los procesos de gestión empresarial por intermedio del despliegue de un modelo de administración de riesgos TI adecuado para las empresas sanitarias del Norte del Perú. El modelo fue revisado por pares, midiendo su confiabilidad utilizando el alfa de Cronbach y su consistencia de contenido con

base en el de Kendall. El modelo propuesto en esta tesis se aplicó como estudio de caso en una compañía de servicios de alcantarillado en Lambayeque, donde se identificaron 165 riesgos, de los cuales 52 riesgos se clasificaron como prioritarios en base a evaluación de apetito y tolerancia, se propusieron estrategias de manejo para 16 proyectos de implementación a fin de monitorear y examinar que la administración de riesgos tenga éxito en influir en el funcionamiento de los procesos de gestión empresarial.

Además, para comprender aún más la materia de investigación propuesta, se dispuso de un conjunto de **bases teóricas** como:

*Gestión de riesgos de tecnologías de la información:* en cuanto a su *definición*, la administración de peligros de TI es una agrupación de operaciones, tareas y acciones que operan de forma integrada para evitar flujos de datos, arremetidas a la infraestructura tecnológica y bases de datos digitales o maniobra digital o informática incorrecta de los datos capturados, procesados y almacenados. En cuanto a su *importancia*: Favorece el despliegue de los planes en un ambiente de confianza, porque los especialistas responsables conocen que se procedió a la evaluación, calificación y toma de las medidas adecuadas los posibles eventos disruptivos para prevenirlos o daños mucho peor; Coadyuva la reunión de la vivencia esencial para afrontar los desafíos del futuro, lo que es sumamente vital en compañías que optan por avanzar aún un poco más en sus planes de digitalización; Sirve para elaborar presupuestos realistas donde se anticipan todos los eventos inesperados y la planificación se ajusta al contexto real. Esto admite conseguir financiamiento para planes, sobre todo proyectos vinculados con la expansión de la infraestructura tecnológica, sistematización o digitalización de programas, porque las instituciones de finanzas y los inversionistas ven que la compañía mantiene todo con buen control. En cuanto a su *gestión* se tiene: Planificar inspecciones seguras: una plataforma tecnológica con inspecciones seguras adaptados a la compañía perennemente ayuda a prevenir problemas a tiempo; Pruebas de seguridad: el núcleo de la prevención de peligros tecnológicos son las pruebas de seguridad. Es una buena idea implementarlos regularmente y de acuerdo con un cronograma; Gestión de casos: todo riesgo identificado debe ser registrado

y esta información gestionada para responder oportunamente e impedir inconvenientes semejantes en el futuro; Descubrimiento y categorización de debilidades: por encima de la simple administración de la seguridad informática, es necesario poder detectar y clasificar cada vulnerabilidad a la que está expuesto el programa de una compañía. Se cuenta con instrumentales tecnológicos que pueden monitorear estos peligros en línea y de manera continua y brindar informes periódicos. La gestión del riesgo informático requiere que los responsables de la seguridad corporativa tengan un visionamiento total, global y holística de los programas de TI de la compañía que minimice las debilidades (HACKNOID, 2019).

*Seguridad informática:* en cuanto a su *definición:* la seguridad informática es una agrupación de técnicas, operaciones y recomendaciones formuladas para el cuidado de las redes, aparatos, aplicaciones y la data frente a arremetidas cibernéticas, piratería, compromiso o dirección no permitida. En cuanto a sus *características:* Confidencialidad, las medidas de seguridad de la información tienen como objetivo cuidar la reserva de la data; es decir, cuidar aquella información de la dirección no permitida y asegurar que únicamente los usuarios correctos procedan con el direccionamiento a ella; Integridad, esta función es la posibilidad de sostener la exactitud y probidad de la data al asegurar que no se modifiquen o maniobren sin permiso. Lo importante en el manejo actual de ingentes cantidades de datos; Disponibilidad, los mecanismos de aseguramiento de TI deben asegurar la disponibilidad continua de los sistemas y datos y la mitigación y resolución rápida de las interrupciones en la disponibilidad; Autenticidad, parte integral del trabajo de seguridad de la información, es la confirmación de la identidad del usuario o un medio para proteger que dicha identidad no ha sido falsificada; Resiliencia, gracias a la seguridad de los datos, la organización puede recuperarse rápidamente de cualquier interrupción o ataque a la seguridad de los datos, porque la resiliencia del aseguramiento de la data es fundamental para las empresas; Seguridad en capas, significa implementar diversos mecanismos seguros en diversos grados para asegurar un mejor cuidado frente a intimidaciones potenciales; Actualización continua, la seguridad informática es un ámbito en permanente evolución, por lo tanto, las

medidas de aseguramiento informático deben renovarse y mejorarse periódicamente para cuidar adecuadamente frente a nuevas amenazas (Coppola, 2021).

*Empresa inmobiliaria:* es una sociedad dedicada al arrendamiento, construcción, venta y administración de bienes muebles e inmuebles. Las principales áreas de actividad inmobiliaria son: venta y alquiler de inmuebles, publicidad de inmuebles en diversos medios comunicativos, consejo jurídico, etc. (RAE, 2022). Concerniente a sus *Tipos*, se tiene: Agente inmobiliario, responsable de planificar el desarrollo de la ejecución del proyecto, porque su tarea es adquirir la propiedad para la ejecución del proyecto; Construcción de inmuebles, posterior a la adquisición del predio (terreno), empieza la edificación del proyecto, involucrando uno o más equipos laborales (profesionales multidisciplinarios); Agencias inmobiliarias, se encarga de la venta de inmuebles e inmuebles, campañas y venta directa a sus potenciales compradores. Desarrollador Inmobiliario, agente que busca oportunidades de negocio y siguen las tácticas hasta la venta, Asociación Inmobiliaria del Perú (SPBR, 2018).

Se correspondió el empleo de ciertos **enfoques conceptuales** como subsidio de las teorías mencionadas previamente:

*Riesgo:* Se define como situar a un individuo en peligro, y en otras fuentes hace referencia a la proximidad del perjuicio. El riesgo, de por sí conocido como posibilidad de perjuicio, puede ponderarse, a diferencia de la posibilidad de peligro, que no es ponderable. El riesgo es la inseguridad vinculada a la duda de un posible evento que puede resultar en un daño (Delgado, y otros, 2016).

*Identificación de riesgos:* Cada activo de información importantes para la empresa deben ser identificados por el programa de administración de seguridad informática y sus directivos garantes, conocidos como propietarios. Se debe precisar los peligros asociados con la propiedad identificada. Se deben identificar las debilidades que tales amenazas pueden explotar y el impacto potencial de comprometer la privacidad, la integridad y el propósito de cada activo (Delgado, y otros, 2016).

*Análisis y examinación de riesgos:* Es un mecanismo sistemático para examinar el nivel de peligrosidad de las muestras de la empresa. Una vez que sabe lo que está pasando, se deben tomar decisiones para manejar estas amenazas. Identificar y gestionar las amenazas a los sistemas de TI es el núcleo de la investigación comparativa, la investigación y la gestión de riesgos (Delgado, y otros, 2016)

*Tratamiento del riesgo:* Es una agrupación de opciones de recursos de datos. La falta de mitigación de riesgos incluye las siguientes alternativas: Prevención de riesgos, representa cualquier actividad que implica cambiar los procedimientos operativos o las actividades comerciales de una empresa para evitar que ocurran riesgos; Aceptación del riesgo, si es complicado reducirse, la acción que lo generó debe continuar; Reducción de riesgos, se debe desplegar los mecanismos convenientes para reducir su impacto en la empresa; Transferir el riesgo, se comparte por una forma o por otra, dependiendo del escenario y contexto vigente, puede ser compartido tanto por actores internos como externos afectados por ambas partes (Viera, y otros, 2019).

*Sistema de información:* Es una agrupación de elementos que procesa, comparte y almacena toda la data para facilitar la elección de opciones y la gestión de la empresa, de la que disponemos: recursos, data, activos informáticos, reglas de trabajo y comunicación (Laudon, y otros, 2016).

Además, concerniente a la **normatividad internacional o nacional** sobre seguridad informática, esencialmente, se contempló desde el principio del estudio apostar por las *Buenas prácticas de gestión de riesgos TI*, por lo que no fue imprescindible realizar la selección de alguna mediante algún medio de examinación especializado.

En el Anexo 3 se describe de manera meticulosa los pasos que se sigue en el desarrollo de estas recomendaciones para la administración de peligros vinculantes tecnologías informatizadas.



### III. METODOLOGÍA

#### 3.1 Tipo y diseño de investigación

- **Tipo de investigación:**

*Aplicada* porque se apegó a los factores ya probados y utilizados para solucionar el problema planteado.

- **Diseño de investigación:**

*Preexperimental* porque se apegó a la maniobra intencionada de disponer de la muestra de población estimada.

#### 3.2 Variables y operacionalización

- Variables:

- Independiente: *Plan de gestión de riesgos de tecnologías de la información*

- Definición conceptual:

“Es una agrupación de operaciones, tareas y acciones que operan de forma integrada para evitar flujos de datos, arremetidas a la infraestructura tecnológica y bases de datos digitales o maniobra digital o informática incorrecta de los datos capturados, procesados y almacenados” (HACKNOID, 2019).

- Definición operacional:

El plan de administración de peligros de TI incluye la medición de la seguridad en aspectos como la reserva, disposición y probidad.

- Dependiente: *Seguridad informática*

- Definición conceptual:

“Es una agrupación de técnicas, operaciones y recomendaciones formuladas para el cuidado de las redes, aparatos, aplicaciones y la data frente a arremetidas cibernéticas, piratería, compromiso o dirección no permitida” (Coppola, 2021).

- Definición operacional:

La seguridad informática se puede estimar por la mitigación del nivel de riesgos en errores humanos, el nivel de riesgos en errores de hardware y el nivel de riesgos en errores de software.

- **Operacionalización:**

En la sección anexa 2 se ilustra la tabla matricial de operatividad de cada variable de estudio.

### 3.3 Población, muestra y muestreo

- **Población (N):**

La población se conformó por los colaboradores de nivel directivo y operacional de la compañía en estudio.

**Tabla 1.** Población

Cargo / Puesto	Cantidad
Gerente	01
Jefe de área	03
Operario	06
Total	10

*N = 10 personas*

- **Muestra (n):**

Representa los elementos de una población; se detalla la dimensión muestral definida dado que la Población fue bajo 30, entonces, la muestra fue similar a la población:

$$n = 15 \text{ personas}$$

- **Muestreo:**

Se manifiesta como el medio estadístico empleado para la selección de la muestra, en este caso, de categoría *no probabilística*.

### 3.4 Técnicas e instrumentos de recolección de datos

- Encuesta:

Medio técnico empleado para el recojo de la data empleando un instrumental conocido como es el Cuestionario, orientado a individuos cuya opinión o percepción debe ser recolectada de manera objetiva (González, 2020).

Para la investigación, se usó la *Encuesta* a través de un *Cuestionario* dirigido a los colaboradores de la compañía, pues son ellos quienes manejan los activos humanos, de hardware y de software en la inmobiliaria.

- Análisis documental:

Este instrumento es considerado de carácter mecánico, porque permite recoger data de la compañía mediante la revisión documental de artefactos de importancia (González, 2020).

Para la investigación, se usó el Análisis documental a través de una *Ficha de datos* que recolectaba data documental importante de la inmobiliaria.

- Validez y confiabilidad

Con referencia al instrumental de recojo de la data como es el caso del Cuestionario su validación se realizó por la examinación de un *Juicio de expertos* conformados por tres especialistas, quienes mediante su rúbrica y una determinada cantidad de criterios garantizaban una asertiva encuesta (ver Anexo 4).

De otra parte, con referencia a la confiabilidad del instrumental usado para el desarrollo del estudio como es el caso del Cuestionario, se empleó el coeficiente estadístico *Alpha de Cronbach* (ver Anexo 6).

### 3.5 Procedimientos

El despliegue del vigente estudio contrajo la ejecución de tres fines concretos citados en la parte introductoria como:

- Finalidad específica 1: Minimizar el nivel de riesgos en seguridad informática por errores humanos.

Se empleó la *Encuesta* para el recojo de la data en materia de seguridad informática con referencia a errores humanos cometidos por el personal de informática y, sobre todo cuando no exhibe una calificación suficientemente proba. Se usó el *Cuestionario* para este propósito con un bloque de ítems o preguntas correspondientes (ver Anexo 5).

- Finalidad específica 2: Minimizar el nivel de riesgos en seguridad informática por errores de hardware.

Se empleó la *Encuesta* para el recojo de la data en materia de seguridad informática con referencia a errores de hardware software como en el caso de accidentes, desastres y robos. Se usó el *Cuestionario* para este propósito con un bloque de ítems o preguntas correspondientes (ver Anexo 5).

- Finalidad específica 3: Minimizar el nivel de riesgos en seguridad informática por errores de software.

Se empleó la *Encuesta* para el recojo de la data en materia de seguridad informática con referencia a errores de software como en el caso de amenazas e intrusiones. Se usó el *Cuestionario* para este propósito con un bloque de ítems o preguntas correspondientes (ver Anexo 5).

### **3.6 Método de análisis de datos**

Se recurrió al empleo del medio estadístico con enfoque descriptivo y con enfoque inferencial favoreciendo el tratamiento de la data.

Concerniente al medio estadístico descriptivo, se buscó la comparativa ilustrativa y de tabulación de la data recogida previo y posterior al despliegue del programa de administración de riesgos de TI.

Concerniente al medio estadístico inferencial, se planteó determinar la normalidad de cada indicador definido en un escenario previo y posterior al despliegue de la propuesta ofrecida, empleando reparticiones estadísticas según el tamaño de la muestral calculada.

### **3.7 Aspectos éticos**

El aspecto ético no se ha dejado de lado en ningún momento y de ser base fundamental para el desarrollo ético del estudio; de esta manera, se dispone de un reglamento general de cultura ética que la Universidad pone a disposición, cuya conformación está dada por cláusulas con fines, principios, directrices, compromisos, directivas de plagio, autoría, entre otros; donde se buscó el uso de formatos de originalidad del trabajo y autorización de la publicación del mismo.

De otra parte, se usó como norma para la redacción bibliográfica a ISO-690, la cual ha sido un estándar en la elaboración de informes de investigación para la Facultad de Ingeniería.

Asimismo, se trabajó con la plataforma de antiplagio Turnitin para la revisión y cálculo del índice de similitud con el valor permitido.

#### IV. RESULTADOS

- **Análisis descriptivo**

- Indicador uno: “Nivel de riesgos en seguridad informática por errores humanos”

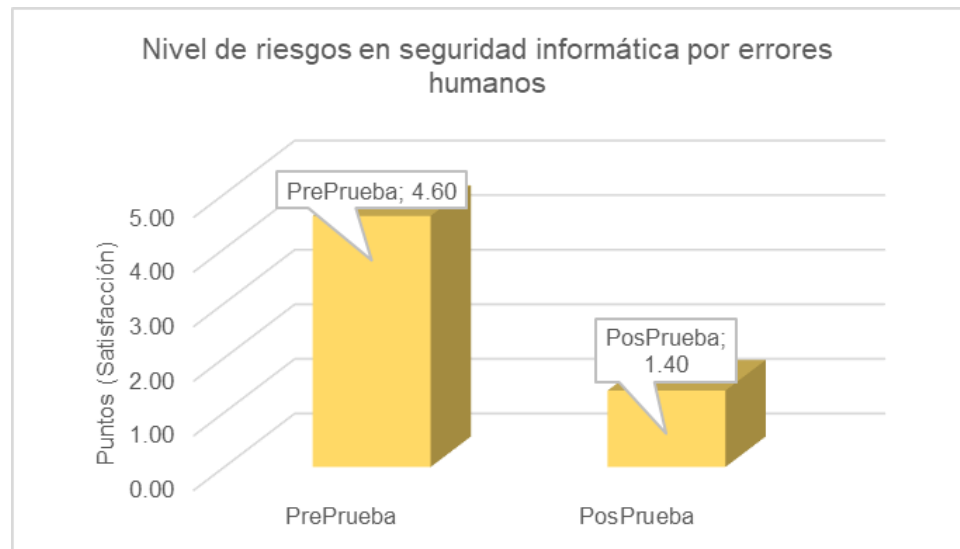


Figura 1. Promedio de preprueba y posprueba del indicador uno.

Se exhibe una minimización del nivel de riesgos en seguridad informática por errores humanos de 4.6 puntos a 1.4 puntos (decremento de 64.00%) por la ejecución del plan de gestión de riesgos de TI en la compañía inmobiliaria.

- Indicador dos: “Nivel de riesgos en seguridad informática por errores de hardware”

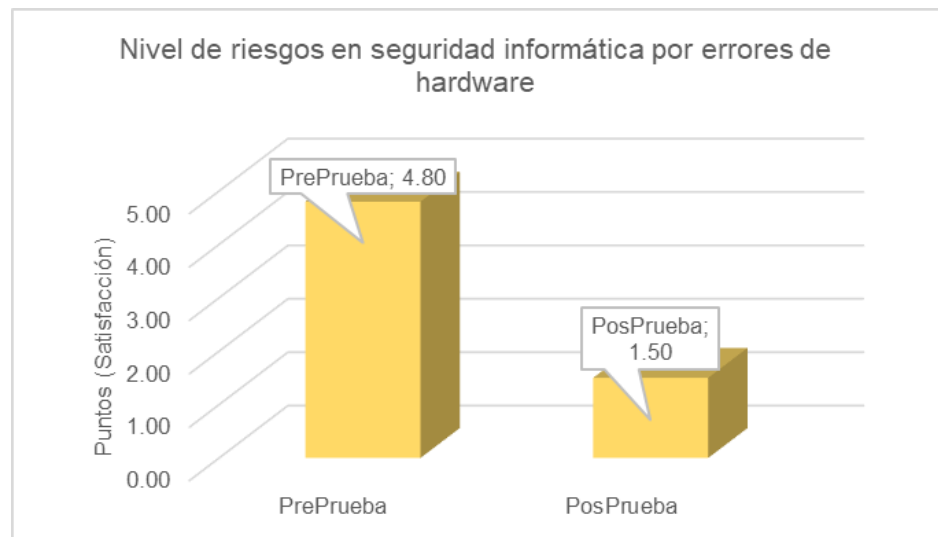


Figura 2. Promedio de preprueba y posprueba del segundo indicador dos.

Se exhibe una minimización del nivel de riesgos en seguridad informática por errores de hardware de 4.8 puntos a 1.5 puntos (decremento de 66.00%) por la ejecución del plan de gestión de riesgos de TI en la compañía inmobiliaria.

- Indicador tres: “Nivel de riesgos en seguridad informática por errores de software”

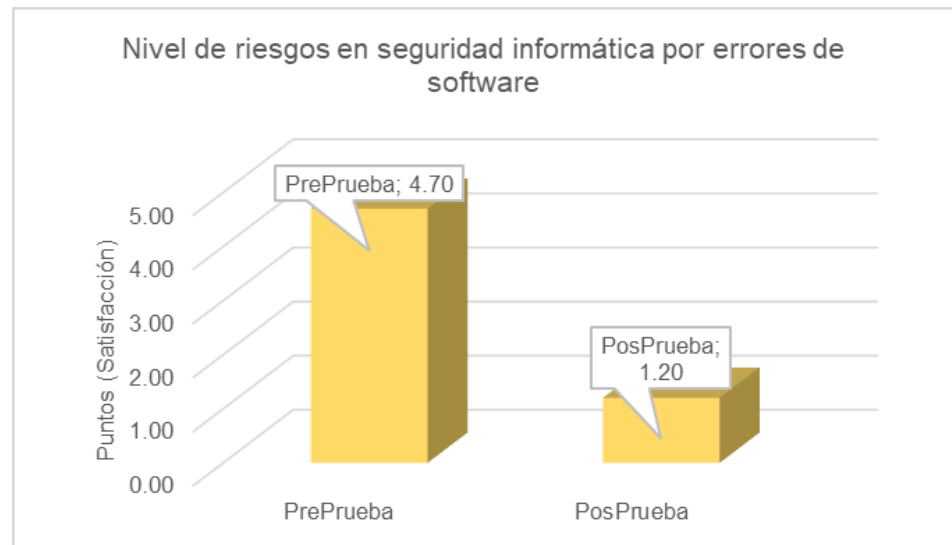


Figura 3. Promedio de preprueba y posprueba del segundo indicador tres.

Se exhibe una minimización del nivel de riesgos en seguridad informática por errores de software de 4.7 puntos a 1.2 puntos (decremento de 70.00%) por la ejecución del plan de gestión de riesgos de TI en la compañía inmobiliaria.



- **Análisis inferencial**

- Indicador uno: “Nivel de riesgos en seguridad informática por errores humanos”

H<sub>0</sub>: “El nivel de riesgos de seguridad informática por errores humanos (sin la ejecución del plan de gestión de riesgos de TI) si posee reparto normalizado”.

H<sub>1</sub>: “El nivel de riesgos de seguridad informática por errores humanos (sin la ejecución del plan de gestión de riesgos de TI) no posee reparto normalizado”.

H<sub>0</sub>: “El nivel de riesgos de seguridad informática por errores humanos (con la ejecución del plan de gestión de riesgos de TI) no posee reparto normalizado”.

H<sub>1</sub>: “El nivel de riesgos de seguridad informática por errores humanos (con la ejecución del plan de gestión de riesgos de TI) si posee reparto normalizado”.

Se tuvo como cuantía de significancia:  $\alpha = 0.05$

Cuantía de significancia  $> 0.05$ , se acoge la teoría negativa (H<sub>0</sub>).

Cuantía de significancia  $\leq 0.05$ , se acoge la teoría positiva (H<sub>1</sub>).

**Tabla 2.** Examen de normalidad del indicador uno

	Shapiro-Wilk		
	Estadístico	gl	Sig.
NRSIEH-Pre	,953	12	,065
NRSIEH-Pos	,942	12	,004

Fuente: (Elaboración Propia, 2023).

Según las operaciones de estimación realizadas en las situaciones previa ( $0.065 > 0.05$ ) y posterior ( $0.004 \leq 0.05$ ), se recurrió al examen de Wilcoxon como un medio estadístico empleado para una distribución no normalizada.

- Indicador dos: “Nivel de riesgos en seguridad informática por errores de hardware”

H<sub>0</sub>: “El nivel de riesgos de seguridad informática por errores de hardware (sin la ejecución del plan de gestión de riesgos de TI) si posee reparto normalizado”.

H<sub>1</sub>: “El nivel de riesgos de seguridad informática por errores de hardware (sin la ejecución del plan de gestión de riesgos de TI) no posee reparto normalizado”.

H<sub>0</sub>: “El nivel de riesgos de seguridad informática por errores de hardware (con la ejecución del plan de gestión de riesgos de TI) no posee reparto normalizado”.

H<sub>1</sub>: “El nivel de riesgos de seguridad informática por errores de hardware (con la ejecución del plan de gestión de riesgos de TI) si posee reparto normalizado”.

Se tuvo como cuantía de significancia:  $\alpha = 0.05$

Cuantía de significancia  $> 0.05$ , se acoge la teoría negativa (H<sub>0</sub>).

Cuantía de significancia  $\leq 0.05$ , se acoge la teoría positiva (H<sub>1</sub>).

**Tabla 3.** Examen de normalidad del indicador dos

	Shapiro-Wilk		
	Estadístico	gl	Sig.
NRSIEW-Pre	,910	12	,060
NRSIEW-Pos	,957	12	,003

Fuente: (Elaboración Propia, 2023).

Según las operaciones de estimación realizadas en las situaciones previa ( $0.060 > 0.05$ ) y posterior ( $0.003 \leq 0.05$ ), se recurrió al examen de Wilcoxon como un medio estadístico empleado para una distribución no normalizada.

- Indicador tres: “Nivel de riesgos en seguridad informática por errores de software”

H<sub>0</sub>: “El nivel de riesgos de seguridad informática por errores de software (sin la ejecución del plan de gestión de riesgos de TI) si posee reparto normalizado”.

H<sub>1</sub>: “El nivel de riesgos de seguridad informática por errores de software (sin la ejecución del plan de gestión de riesgos de TI) no posee reparto normalizado”.

H<sub>0</sub>: “El nivel de riesgos de seguridad informática por errores de software (con la ejecución del plan de gestión de riesgos de TI) no posee reparto normalizado”.

H<sub>1</sub>: “El nivel de riesgos de seguridad informática por errores de software (con la ejecución del plan de gestión de riesgos de TI) si posee reparto normalizado”.

Se tuvo como cuantía de significancia:  $\alpha = 0.05$

Cuantía de significancia  $> 0.05$ , se acoge la teoría negativa (H<sub>0</sub>).

Cuantía de significancia  $\leq 0.05$ , se acoge la teoría positiva (H<sub>1</sub>).

**Tabla 4.** Examen de normalidad del indicador tres

	Shapiro-Wilk		
	Estadístico	gl	Sig.
NRSIES-Pre	,910	12	,055
NRSIES-Pos	,957	12	,002

Fuente: (Elaboración Propia, 2023).

Según las operaciones de estimación realizadas en las situaciones previa ( $0.055 > 0.05$ ) y posterior ( $0.002 \leq 0.05$ ), se recurrió al examen de Wilcoxon como un medio estadístico empleado para una distribución no normalizada.

- **Contrastación de hipótesis**

- **Supuesto específico 1:**

“El plan de gestión de riesgos de TI minimiza el nivel de riesgos en seguridad informática por errores humanos en la empresa inmobiliaria de la ciudad de Casma en el año 2023”.

Se empleó las teorías estadísticas negativa y positiva tomando en consideración la cuantía de significancia de 0.05.

**Tabla 5.** Examen de Wilcoxon para el indicador uno

NRSIEH-Pos - NRSIEH-Pre	
Z	-2,247 <sup>b</sup>
Sig. asintótica(bilateral)	,003

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: (Elaboración propia, 2023).

Concerniente al cuadro preliminar, se plasma que la cuantía de significancia bilateral de la prueba de Wilcoxon para el indicador uno “Nivel de riesgos en seguridad informática por errores humanos” evaluando en la condición anterior y posterior a la ejecución de la solución planteada fue 0.003 ( $\leq 0.05$ ). De este modo, se desecha el supuesto negativo ( $H_0$ ) y se acoge el supuesto positivo ( $H_1$ ); en consecuencia, se afirma que: “Hay abundante seguridad estadística (95%) para evidenciar que, la ejecución de un plan de gestión de riesgos de TI si maximiza la seguridad informática de una compañía inmobiliaria de la ciudad de Casma en el año 2023 de forma cuantiosa”.

- Supuesto específico 2:

“El plan de gestión de riesgos de TI minimiza el nivel de riesgos en seguridad informática por errores de hardware en la empresa inmobiliaria de la ciudad de Casma en el año 2023”.

Se empleó las teorías estadísticas negativa y positiva tomando en consideración la cuantía de significancia de 0.05.

**Tabla 6.** Examen de Wilcoxon para el indicador dos

	NRSIEW-Pos - NRSIEW-Pre
Z	-2,563 <sup>b</sup>
Sig. asintótica(bilateral)	,002

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: (Elaboración propia, 2023).

Concerniente al cuadro preliminar, se plasma que la cuantía de significancia bilateral de la prueba de Wilcoxon para el indicador dos “Nivel de riesgos en seguridad informática por errores de hardware” evaluando en la condición anterior y posterior a la ejecución de la solución planteada fue 0.002 ( $\leq 0.05$ ). De este modo, se desecha el supuesto negativo ( $H_0$ ) y se acoge el supuesto positivo ( $H_1$ ); en consecuencia, se afirma que: “Hay abundante seguridad estadística (95%) para evidenciar que, la ejecución de un plan de gestión de riesgos de TI si maximiza la seguridad informática de una compañía inmobiliaria de la ciudad de Casma en el año 2023 de forma cuantiosa”

- Supuesto específico 3:

“El plan de gestión de riesgos de TI minimiza el nivel de riesgos en seguridad informática por errores de software en la empresa inmobiliaria de la ciudad de Casma en el año 2023”.

Se empleó las teorías estadísticas negativa y positiva tomando en consideración la cuantía de significancia de 0.05.

**Tabla 7.** Examen de Wilcoxon para el indicador tres

NRSIES-Pos - NRSIES-Pre	
Z	-2,389 <sup>b</sup>
Sig. asintótica(bilateral)	,001

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: (Elaboración propia, 2023).

Concerniente al cuadro preliminar, se plasma que la cuantía de significancia bilateral de la prueba de Wilcoxon para el indicador tres “Nivel de riesgos en seguridad informática por errores de software” evaluando en la condición anterior y posterior a la ejecución de la solución planteada fue 0.001 ( $\leq 0.05$ ). De este modo, se desecha el supuesto negativo ( $H_0$ ) y se acoge el supuesto positivo ( $H_1$ ); en consecuencia, se afirma que: “Hay abundante seguridad estadística (95%) para evidenciar que, la ejecución de un plan de gestión de riesgos de TI si maximiza la seguridad informática de una compañía inmobiliaria de la ciudad de Casma en el año 2023 de forma cuantiosa”

## V. DISCUSIÓN

Concerniente al indicador uno: “Nivel de riesgos en seguridad informática por errores humanos”, los importes obtenidos en los cálculos estadísticos de los escenarios anterior y posterior a la ejecución de la propuesta ofrecida (Plan de gestión de riesgos de TI) fueron 4.60 y 1.40 puntos respectivamente, exhibiendo un valor reducido importante de 64.00%. Estos logros son similares a los conseguidos por (Rivera, 2019) quien en su estudio planteó un plan de mitigación de riesgos TI del Hospital de Catacocha para el departamento TIC, que permitió identificar vulnerabilidades que afectan a la seguridad informática, pues la institución estatal maneja gran cantidad de información sensible y confidencial, considerando que los datos solo fueron soportados para los externos. unidades y no se han tomado medidas de seguridad porque depende de una entidad externa que ha dado un presupuesto anual limitado. Lo expuesto previamente, se sostiene en las bases teóricas del Plan de gestión de riesgos de TI, el cual favorece el despliegue de los planes en un ambiente de confianza, porque los especialistas responsables conocen que se procedió a la evaluación, calificación y toma de las medidas adecuadas los posibles eventos disruptivos para prevenirlos o daños mucho peor.

Concerniente al indicador dos: “Nivel de riesgos en seguridad informática por errores de hardware”, los importes obtenidos en los cálculos estadísticos de los escenarios anterior y posterior a la ejecución de la propuesta ofrecida (Plan de gestión de riesgos de TI) fueron 4.80 y 1.50 puntos respectivamente, exhibiendo un valor reducido importante de 66.00%. Estos logros son similares a los conseguidos por (Valverde, 2022) quien en su estudio solicitó la implementación de la administración de peligros TI para optimizar la seguridad informática de la empresa anunciante, permitiendo mitigar riesgos, prevenir ataques informáticos y manipulación de datos, por lo que determinó los niveles aceptables de confidencialidad, integridad y disponibilidad. Se pudo afirmar que durante la implantación de la administración de peligros de TI aplicando la metodología MAGERIT, se logró crear controles que permitieron optimizar la seguridad informática de las compañías, lo que determinó un avance significativo. Lo expuesto previamente, se sostiene en

las bases teóricas del Plan de gestión de riesgos de TI, el cual coadyuva la reunión de la vivencia esencial para afrontar los desafíos del futuro, lo que es sumamente vital en compañías que optan por avanzar aún un poco más en sus planes de digitalización.

Concerniente al indicador tres: “Nivel de riesgos en seguridad informática por errores de software”, los importes obtenidos en los cálculos estadísticos de los escenarios anterior y posterior a la ejecución de la propuesta ofrecida (Plan de gestión de riesgos de TI) fueron 4.70 y 1.20 puntos respectivamente, exhibiendo un valor reducido importante de 70.00%. Estos logros son similares a los conseguidos por (Moscoso, y otros, 2018) quienes buscaron contribuir al desempeño de los procesos de gestión empresarial por intermedio del despliegue de un modelo de administración de riesgos TI adecuado para las empresas sanitarias del Norte del Perú. Se identificaron 165 riesgos, de los cuales 52 riesgos se clasificaron como prioritarios en base a evaluación de apetito y tolerancia, se propusieron estrategias de manejo para 16 proyectos de implementación a fin de monitorear y examinar que la administración de riesgos tenga éxito en influir en el funcionamiento de los procesos de gestión empresarial. Lo expuesto previamente, se sostiene en las bases teóricas del Plan de gestión de riesgos de TI, el cual sirve para elaborar presupuestos realistas donde se anticipan todos los eventos inesperados y la planificación se ajusta al contexto real. Esto admite conseguir financiamiento para planes, sobre todo proyectos vinculados con la expansión de la infraestructura tecnológica, sistematización o digitalización de programas, porque las instituciones de finanzas y los inversionistas ven que la compañía mantiene todo con buen control.



## **VI. CONCLUSIONES**

1. Se consiguió minimizar el nivel de riesgos en seguridad informática por errores humanos en 64.00%, donde los importes obtenidos en las valoraciones estadísticas en los escenarios anterior y posterior a la ejecución de la propuesta plasmada fueron 4.60 y 1.40 puntos correspondientemente. Esto corrobora que un programa de administración de peligros de TI maximiza la seguridad informática de una asociación inmobiliaria de la ciudad de Casma en el año 2023.
2. Se consiguió minimizar el nivel de riesgos en seguridad informática por errores de hardware en 66.00%, donde los importes obtenidos en las valoraciones estadísticas en los escenarios anterior y posterior a la ejecución de la propuesta ofrecida fueron 4.80 y 1.50 puntos respectivamente. Esto corrobora que un programa de administración de peligros de TI maximiza la seguridad informática de una asociación inmobiliaria de la ciudad de Casma en el año 2023.
3. Se consiguió minimizar el nivel de riesgos en seguridad informática por errores de software en 70.00%, donde los importes obtenidos en las valoraciones estadísticas en los escenarios anterior y posterior a la ejecución de la propuesta ofrecida fueron 4.70 y 1.20 puntos respectivamente. Esto corrobora que un programa de administración de peligros de TI maximiza la seguridad informática de una asociación inmobiliaria de la ciudad de Casma en el año 2023.

## **VII. RECOMENDACIONES**

Al Gerente general:

Se pide implantar la propuesta desarrollada (Plan de gestión de riesgos de TI) a fin de establecer mecanismos seguros de reserva, probidad y disposición de la data empresarial.

A los Jefes de área:

Se pide considerar todas las directrices de seguridad informática que contiene el programa de administración de peligros de TI a fin de desarrollar una cultura de protección y cuidado de los activos informáticos.

A los Colaboradores:

Se pide respetar de forma obligatoria todas las recomendaciones vertidas en el plan de gestión de riesgos de TI.

## REFERENCIAS

- americasistemas. 2015.** americasistemas. [En línea] 2015. [Citado el: 02 de abril de 2022.] <https://www.americasistemas.com.pe/ley-de-proteccion-de-datos-personales-y-norma-isoiec-27001/>.
- Areitio Bertolin, Javier. 2008.** *Seguridad de la información. Redes, informática y sistemas de información.* Madrid : Ediciones Parainfo S.A., 2008.
- Arias Gonzáles, José Luis. 2020.** *Técnicas e instrumentos de investigación científica.* Arequipa : Enfoques Consulting E.I.R.L, 2020. Vol. Primera edición.
- biblioguias. 2020.** <https://biblioguias.cepal.org/c.php?g=495473&p=4398118>. [En línea] Cepal-Naciones Unidas, 18 de Diciembre de 2020.
- Cáceda Rodríguez, Carolina Rubí. 2021.** *Modelo dinámico para la gestión de seguridad de la infraestructura de tecnologías de información y comunicación.* Lima : Facultad de Ingeniería de Sistemas e Informática, 2021. pág. 126.
- Coppola, María. 2021.** Seguridad informática: qué es, tipos y características. [En línea] 1 de Enero de 2021. [Citado el: 15 de Diciembre de 2022.] <https://blog.hubspot.es/website/que-es-seguridad-informatica#:~:text=La%20seguridad%20inform%C3%A1tica%20es%20el,da%C3%B1o%20o%20acceso%20no%20autorizado..>
- Del Peso Navarro, Emilio. 2003.** *Manual de Outsourcing Informático.* Madrid : Díaz de Santos, 2003. Vol. Segunda Edición.
- Delgado, César y Huancas, Henry. 2016.** *Influencia de la aplicación de la metodología de gestión de riesgos empresariales en el nivel de riesgos operativos del proceso de gestión de compras en una empresa agroindustrial trujillana.* Trujillo : s.n., 2016.

**Detrujillo. 2021.** detrujillo.com. [En línea] detrujillo.com, 2021. [Citado el: 02 de abril de 2022.] <https://detrujillo.com/quieres-hacer-compras-por-facebook-o-whatsapp-cuida-tus-datos-personales/>.

**Escuela Europea. 2022.** Qué es la gestión de riesgos de TI. [En línea] 14 de Diciembre de 2022. [Citado el: 15 de Diciembre de 2022.] <https://www.escuelaeuropeaexcelencia.com/2022/12/que-es-la-gestion-de-riesgos-de-ti-y-que-competencias-requiere/>.

**Estadoperuano. 2021.** Plataforma Digital del Estado Peruano. [En línea] Gobierno del Perú, 14 de julio de 2021. [Citado el: 02 de abril de 2022.] <https://www.gob.pe/14086-sistema-de-gestion-de-seguridad-de-la-informacion>.

**Hernández y Rodriguez, Sergio y Pulido Martínez, Alejandro. 2011.**  
Fundamentos de gestión empresarial. *Fundamentos de gestión empresarial*. Primera. s.l. : McGRAW-HILL, 2011.

**Gestión. 2020.** La importancia de analizar los riesgos de las TI. [En línea] 1 de Enero de 2020. [Citado el: 15 de Diciembre de 2022.] <https://www.gestion.org/la-importancia-de-analizar-los-riesgos-de-las-ti/>.

**Gonzáles, Luis. 2020.** *Técnicas e instrumentos de investigación científica*. Arequipa : Enfoques Consulting E.I.R.L, 2020. Vol. Primera edición.

**HACKNOID. 2019.** Importancia de la gestión de riesgos informáticos. [En línea] 26 de Agosto de 2019. [Citado el: 15 de Diciembre de 2022.] <https://www.hacknoid.com/hacknoid/importancia-de-la-gestion-de-riesgos-informaticos/>.

**Hernández y Rodriguez, Sergio y Pulido Martínez, Alejandro. 2011.**  
Fundamentos de gestión empresarial. *Fundamentos de gestión empresarial*. Primera. s.l. : McGRAW-HILL, 2011.

**ISOTools, Excellence;. 2020.** Plataforma tecnológica para la gestión de la excelencia. [En línea] 2020. <https://www.normas-iso.com/iso-27001/>.

**Justino Salinas, Zully Isabel. 2015.** *Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013.* Lima. Lima : Facultad de ciencias e Ingeniería - Pontificia Universidad Católica del Perú, 2015.

**Laudon, Kenneth C. y Laudon, Jane P. 2016.** *Sistemas de Información Gerencial. Sistema de información Gerencial.* Décimo cuarta. Ciudad de México : Pearson, 2016, Vol. Décimo cuarta.

**Mejía Delgado, César David y Ruíz Huancas , Henry Miguel. 2016.** *Influencia de la aplicación de la metodología de gestión de riesgos empresariales en el nivel de riesgos operativos del proceso de gestión de compras en una empresa agroindustrial trujillana.* Trujillo : s.n., 2016.

*Metodología para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000.* **Valencia Duque, Francisco Javier y Orozco Alzate, Mauricio. 2017.** 77-88, Colombia : Transformación digital, 2017, Vol. 22.

**Miguel Pérez, Julio César. 2015.** *Protección de datos y seguridad de la información.* cuarta. Madrid : Rama, 2015. pág. 276.

**Moscoso, Lissette, Peña, Edgard y Soto, María del Carmen. 2018.** *"Modelo de gestión de riesgos de TI que contribuye a la Operación de los procesos de gestión comercial de las empresas del sector de saneamiento del norte del Perú".* Chiclayo : USAT, 2018.

**RAE. 2022.** *Diccionario de la Real Academia de la Lengua Española.* [En línea] 1 de Enero de 2022. [Citado el: 15 de Diciembre de 2022.] <https://dle.rae.es/>.

**raices, Sociedad peruana de bienes. 2018.** *Sociedad peruana de bienes raices.* [En línea] Sociedad peruana de bienes raices, 2018. [Citado el: 28 de mayo de 2022.] <https://bienesraices.com/>.

**Rivera, Johanna. 2019.** *"Plan de Gestión de Riesgos de TI en el Hospital de Catacocha".* Loja : UNL, 2019.

**Rojas Viera, Cinthia Katherine y Zavaleta Verona, Tefhany Lisseth. 2019.**

*Sistema de Gestión de Seguridad de Información (SGSI) basado en la Norma ISO/IEC 27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015.* UNPRG. 2019.

**Ruiz Larrocha, Elena. 2017.** Nuevas tendencias en los sistemas de información.

*Nuevas tendencias en los sistemas de información.* Primera. Madrid : Ramón Areces, 2017.

**Salinas, Zully. 2015.** *Diseño de un sistema de gestión de seguridad de*

*información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013.* Lima. Lima : Facultad de ciencias e Ingeniería - Pontificia Universidad Católica del Perú, 2015.

**SPBR. 2018.** Sociedad Peruana de Bienes Raices. [En línea] 1 de Enero de 2018.

[Citado el: 15 de Diciembre de 2022.] <https://bienesraices.com/>.

**Valencia Duque, Francisco Javier. 2021.** *Sistema de gestión de seguridad de la*

*información basado en la familia de normas ISO/IEC 27000.* Primera edición. Manizales : Universidad Nacional de Colombia, 2021. pág. 189.

**Valverde, Diego. 2022.** *"Implementación de una gestión de riesgos de TI para*

*mejorar la seguridad de la información de una empresa de agencia publicitaria - 2021".* Lima : UTP, 2022.

**Viera, Katherine y Verona, Lisseth. 2019.** *Sistema de Gestión de Seguridad de*

*Información (SGSI) basado en la Norma ISO/IEC 27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015.* Universidad Nacional Pedro Ruíz Gallo. Lambayeque.

**Villegas Rivera, César Augusto y Zamora Li, Germán Suishing de Jesús.**

**2018.** *Diseño de un sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001:2013 para Empresa Agroindustrial POMALCA S.A.A. - 2016.* Universidad Nacional Pedro Ruíz Gallo. Lambayeque : s.n., 2018.

## ANEXOS

### Anexo 1 - Matriz de consistencia de la investigación

Título: Plan de gestión de riesgos de tecnologías de la información para la Seguridad informática en una empresa Inmobiliaria, Casma 2023.

Autor: De La Cruz Mejía, Cristhian Paul.

Problema	Objetivo	Hipótesis	Variable
<p>General:</p> <p>¿En qué manera un plan de administración de riesgos de TI afecta la seguridad informática en una empresa inmobiliaria de la ciudad de Casma en año 2023?</p>	<p>General:</p> <p>Maximizar la seguridad informática en una empresa inmobiliaria de la ciudad de Casma en el año 2023 mediante la ejecución de un plan de gestión de riesgos de TI.</p>	<p>General:</p> <p>“El plan de gestión de riesgos de TI maximiza cuantiosamente la seguridad informática de la compañía inmobiliaria de la ciudad de Casma en el año 2023”.</p>	<p>Independiente:</p> <p>Plan de gestión de riesgos de tecnologías de la información</p>
<p>Específicos:</p> <ol style="list-style-type: none"> <li>1. ¿En qué manera un plan de gestión de riesgos de TI afecta el nivel de riesgos en seguridad informática por errores humanos en la empresa inmobiliaria de la ciudad de Casma en año 2023?</li> <li>2. ¿En qué manera un plan de gestión de riesgos de TI afecta el nivel de riesgos en seguridad informática por errores de hardware en la empresa inmobiliaria de la ciudad de Casma en año 2023?</li> <li>3. ¿En qué manera un plan de gestión de riesgos de TI afecta el nivel de riesgos en seguridad informática por errores de software en la empresa inmobiliaria de la ciudad de Casma en año 2023?</li> </ol>	<p>Específicos:</p> <ol style="list-style-type: none"> <li>1. Minimizar el nivel de riesgos en seguridad informática por errores humanos.</li> <li>2. Minimizar el nivel de riesgos en seguridad informática por errores de hardware.</li> <li>3. Minimizar el nivel de riesgos en seguridad informática por errores de software.</li> </ol>	<p>Específicas:</p> <ol style="list-style-type: none"> <li>1. “El plan de gestión de riesgos de TI minimiza el nivel de riesgos de seguridad informática por errores humanos en la compañía inmobiliaria de la ciudad de Casma en el año 2023”.</li> <li>2. “El plan de gestión de riesgos de TI minimiza el nivel de riesgos en seguridad informática por errores de hardware en la compañía inmobiliaria de la ciudad de Casma en el año 2023”.</li> <li>3. “El plan de gestión de riesgos de TI minimiza el nivel de riesgos en seguridad informática por errores de software en la compañía inmobiliaria de la ciudad de Casma en el año 2023”.</li> </ol>	<p>Dependiente:</p> <p style="text-align: center;">Seguridad informática</p>

Metodología			
<p>Tipo de investigación:</p> <p style="text-align: center;">Aplicada</p>	<p>Población (N):</p> <p>La población se encuentra determinada por todos los colaboradores de la empresa inmobiliaria.</p> <p style="text-align: center;"><i>N = 10 personas</i></p>	<p>Técnicas de recolección de datos:</p> <ul style="list-style-type: none"> <li>• Encuesta</li> </ul>	<p>Método de análisis de datos:</p> <ul style="list-style-type: none"> <li>• Estadística descriptiva.</li> <li>• Estadística inferencial.</li> </ul>
<p>Diseño de investigación:</p> <p style="text-align: center;">Preexperimental</p>	<p>Muestra (n):</p> <p>Dado que la Población es menor que 30, entonces:</p> <p style="text-align: center;"><i>n = 10 personas</i></p>	<p>Instrumentos de recolección de datos:</p> <ul style="list-style-type: none"> <li>• Cuestionario</li> </ul>	<p>Aspectos éticos:</p> <p>Se respetará el derecho a la propiedad intelectual (Originalidad de la investigación - Reporte Turnitin).</p> <p>Se tomará en cuenta el Código de ética de la Universidad César Vallejo.</p> <p>Adicionalmente, se usará para la redacción de la investigación el Sistema de normas ISO-690.</p>



## Anexo 2 - Matriz de operacionalización de variables

Variable	Definición Conceptual	Definición Operacional	Dimensión (Sub variable)	Indicador	Escala de medición
Independiente: Plan de gestión de riesgos de tecnologías de la información	“Es una agrupación de operaciones, tareas y acciones que operan de forma integrada para evitar flujos de datos, arremetidas a la infraestructura tecnológica y bases de datos digitales o maniobra digital o informática incorrecta de los datos capturados, procesados y almacenados” (HACKNOID, 2019).	El plan de administración de peligros de TI incluye la medición de la seguridad en aspectos como la reserva, disposición y probidad.			
Dependiente: Seguridad informática	“Es una agrupación de técnicas, operaciones y recomendaciones formuladas para el cuidado de las redes, aparatos, aplicaciones y la data frente a arremetidas cibernéticas, piratería, compromiso o dirección no permitida” (Coppola, 2021).	La seguridad informática se puede estimar por la mitigación del nivel de riesgos en errores humanos, el nivel de riesgos en errores de hardware y el nivel de riesgos en errores de software	Riesgo	Nivel de riesgo en seguridad informática por errores humanos	Ordinal
				Nivel de riesgo en seguridad informática por errores de hardware	Ordinal
				Nivel de riesgo en seguridad informática por errores de software	Ordinal

## Anexo 3 - Metodología de desarrollo del plan de gestión de riesgos de TI

Tan importante como saber qué es un riesgo en informática es entender la importancia de gestionarlo. Llevar a cabo esta tarea siempre será más sencillo desde la visión de un equipo de expertos, sin embargo, existen ciertas prácticas para la prevención de riesgos en informática que todo responsable de una empresa debiera conocer (HACKNOID, 2019).

Se ha considerado los siguientes pasos:

- Paso 1: Diseñar controles de seguridad:

Una plataforma informática con controles de seguridad a la medida de la empresa siempre contribuirá a anticiparse a los problemas de forma oportuna.

- Paso 2: Pruebas de seguridad:

La esencia de la prevención de riesgos informáticos yace en la ejecución de pruebas de seguridad. Una buena idea es realizarlas de forma periódica y calendarizada.

- Paso 3: Gestión de los incidentes:

Se debe mantener un historial con cada uno de los riesgos identificados y gestionar estos datos para ser capaces de reaccionar a tiempo y de evitar problemas similares a futuro.

- Paso 4: Detección y clasificación de vulnerabilidades:

Más allá de la mera gestión de seguridad TI, se debe ser capaz de detectar y clasificar cada una de las vulnerabilidades a que se expone el sistema de la empresa. Existen herramientas informáticas capaces de escanear estos riesgos en tiempo real y continuo, entregando reportes de forma periódica.

En resumen, la gestión de riesgos informáticos exige a los responsables de seguridad de las empresas tener una visión macro, general y completa de los sistemas TI de la empresa, logrando así minimizar las vulnerabilidades.

## Anexo 4 - Instrumentos de recolección de datos

Cuestionario aplicado a los colaboradores de la empresa inmobiliaria - Casma.

A continuación, se presenta una lista de preguntas contenidas en doce (12) ítems que corresponden a la percepción de la seguridad informática por parte de los colaboradores de la empresa inmobiliaria.

Se requiere saber su opinión por cada uno de los ítems presentados. Por favor, indique su apreciación objetiva marcando con una "X" sobre cualquier de los números 1, 2, 3, 4 ó 5, dónde:

1	2	3	4	5
Deficiente	Malo	Regular	Bueno	Excelente

Variable	Dimensión	Ítems	Opción de respuesta				
			1	2	3	4	5
Seguridad informática	Riesgo	1. ¿Se cumple el procedimiento de capacitación del recurso humano en TI?					
		2. ¿Se cumple el procedimiento de programación eficiente del recurso humano en TI?					
		3. ¿Se cumple el procedimiento de administración correcta del recurso humano en TI?					
		4. ¿Se cumple el procedimiento gestión de riesgos con respecto al recurso humano en TI?					
		5. ¿Se cumple el procedimiento de protección de activos de hardware frente a accidentes?					
		6. ¿Se cumple el procedimiento de protección de activos de hardware frente a desastres?					
		7. ¿Se cumple el procedimiento de protección de activos de hardware frente a robos?					
		8. ¿Se cumple el procedimiento gestión de riesgos con respecto al hardware TI?					
		9. ¿Se cumple el procedimiento de protección de activos de software frente a amenazas?					
		10. ¿Se cumple el procedimiento de protección de activos de software frente a intrusiones?					
		11. ¿Se cumple el procedimiento de protección de activos de software frente a ataques?					
		12. ¿Se cumple el procedimiento gestión de riesgos con respecto al software TI?					

## Anexo 5 - Validación de los instrumentos de recolección de datos

Cuestionario aplicado a los colaboradores de la empresa inmobiliaria - Casma.

A continuación, se presenta una lista de preguntas contenidas en doce (12) ítems que corresponden a la percepción de la seguridad informática por parte de los colaboradores de la empresa inmobiliaria.

Se requiere saber su opinión por cada uno de los ítems presentados. Por favor, indique su apreciación objetiva marcando con una "X" sobre cualquier de los números 1, 2, 3, 4 ó 5, dónde:

1	2	3	4	5
Deficiente	Malo	Regular	Bueno	Excelente


Variable	Dimensión	Ítems	Opción de respuesta				
			1	2	3	4	5
Seguridad informática	Riesgo	1. ¿Se cumple el procedimiento de capacitación del recurso humano en TI?					
		2. ¿Se cumple el procedimiento de programación eficiente del recurso humano en TI?					
		3. ¿Se cumple el procedimiento de administración correcta del recurso humano en TI?					
		4. ¿Se cumple el procedimiento gestión de riesgos con respecto al recurso humano en TI?					
		5. ¿Se cumple el procedimiento de protección de activos de hardware frente a accidentes?					
		6. ¿Se cumple el procedimiento de protección de activos de hardware frente a desastres?					
		7. ¿Se cumple el procedimiento de protección de activos de hardware frente a robos?					
		8. ¿Se cumple el procedimiento gestión de riesgos con respecto al hardware TI?					
		9. ¿Se cumple el procedimiento de protección de activos de software frente a amenazas?					
		10. ¿Se cumple el procedimiento de protección de activos de software frente a intrusiones?					
		11. ¿Se cumple el procedimiento de protección de activos de software frente a ataques?					
		12. ¿Se cumple el procedimiento gestión de riesgos con respecto al software TI?					

<sup>1</sup>**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

<sup>2</sup>**Pertinencia:** Si el ítem pertenece a la dimensión.

<sup>3</sup>**Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

**Suficiencia,** se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

<b>Observaciones:</b> Es suficiente	
<b>Opinión de aplicabilidad</b>	
Aplicable [ X ]      Aplicable después de corregir [ ]      No aplicable [ ]	
<b>Apellidos y nombres del juez evaluador</b>	Dr. Agreda Gamboa, Everson David
<b>Especialidad del evaluador</b>	Redes y Comunicaciones
	
DNI: 18161457	Trujillo, 20 de diciembre del 2022

Cuestionario aplicado a los colaboradores de la empresa inmobiliaria - Casma.

A continuación, se presenta una lista de preguntas contenidas en doce (12) ítems que corresponden a la percepción de la seguridad informática por parte de los colaboradores de la empresa inmobiliaria.

Se requiere saber su opinión por cada uno de los ítems presentados. Por favor, indique su apreciación objetiva marcando con una "X" sobre cualquier de los números 1, 2, 3, 4 ó 5, dónde:

1	2	3	4	5
Deficiente	Malo	Regular	Bueno	Excelente


Variable	Dimensión	Ítems	Opción de respuesta				
			1	2	3	4	5
Seguridad informática	Riesgo	1. ¿Se cumple el procedimiento de capacitación del recurso humano en TI?					
		2. ¿Se cumple el procedimiento de programación eficiente del recurso humano en TI?					
		3. ¿Se cumple el procedimiento de administración correcta del recurso humano en TI?					
		4. ¿Se cumple el procedimiento gestión de riesgos con respecto al recurso humano en TI?					
		5. ¿Se cumple el procedimiento de protección de activos de hardware frente a accidentes?					
		6. ¿Se cumple el procedimiento de protección de activos de hardware frente a desastres?					
		7. ¿Se cumple el procedimiento de protección de activos de hardware frente a robos?					
		8. ¿Se cumple el procedimiento gestión de riesgos con respecto al hardware TI?					
		9. ¿Se cumple el procedimiento de protección de activos de software frente a amenazas?					
		10. ¿Se cumple el procedimiento de protección de activos de software frente a intrusiones?					
		11. ¿Se cumple el procedimiento de protección de activos de software frente a ataques?					
		12. ¿Se cumple el procedimiento gestión de riesgos con respecto al software TI?					

<sup>1</sup>**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

<sup>2</sup>**Pertinencia:** Si el ítem pertenece a la dimensión.

<sup>3</sup>**Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

**Suficiencia,** se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

<b>Observaciones:</b> Es suficiente	
<b>Opinión de aplicabilidad</b>	
Aplicable [ X ]      Aplicable después de corregir [ ]      No aplicable [ ]	
<b>Apellidos y nombres del juez evaluador</b>	Dr. Mendoza Rivera, Ricardo Darío
<b>Especialidad del evaluador</b>	Gestión de Proyectos de TIC
	
<b>DNI:</b> 18070765	Trujillo, 20 de diciembre del 2022

Cuestionario aplicado a los colaboradores de la empresa inmobiliaria - Casma.

A continuación, se presenta una lista de preguntas contenidas en doce (12) ítems que corresponden a la percepción de la seguridad informática por parte de los colaboradores de la empresa inmobiliaria.

Se requiere saber su opinión por cada uno de los ítems presentados. Por favor, indique su apreciación objetiva marcando con una "X" sobre cualquier de los números 1, 2, 3, 4 ó 5, dónde:

1	2	3	4	5
Deficiente	Malo	Regular	Bueno	Excelente

Variable	Dimensión	Ítems	Opción de respuesta				
			1	2	3	4	5
Seguridad informática		1. ¿Se cumple el procedimiento de capacitación del recurso humano en TI?					
		2. ¿Se cumple el procedimiento de programación eficiente del recurso humano en TI?					
		3. ¿Se cumple el procedimiento de administración correcta del recurso humano en TI?					
		4. ¿Se cumple el procedimiento gestión de riesgos con respecto al recurso humano en TI?					
	Riesgo	5. ¿Se cumple el procedimiento de protección de activos de hardware frente a accidentes?					
		6. ¿Se cumple el procedimiento de protección de activos de hardware frente a desastres?					
		7. ¿Se cumple el procedimiento de protección de activos de hardware frente a robos?					
		8. ¿Se cumple el procedimiento gestión de riesgos con respecto al hardware TI?					
		9. ¿Se cumple el procedimiento de protección de activos de software frente a amenazas?					
		10. ¿Se cumple el procedimiento de protección de activos de software frente a intrusiones?					
		11. ¿Se cumple el procedimiento de protección de activos de software frente a ataques?					
		12. ¿Se cumple el procedimiento gestión de riesgos con respecto al software TI?					




<sup>1</sup>**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

<sup>2</sup>**Pertinencia:** Si el ítem pertenece a la dimensión.

<sup>3</sup>**Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

**Suficiencia,** se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

<b>Observaciones:</b> Es suficiente	
<b>Opinión de aplicabilidad</b>	
Aplicable [ X ]      Aplicable después de corregir [ ]      No aplicable [ ]	
<b>Apellidos y nombres del juez evaluador</b>	Ms. Córdova Otero, Juan Luis
<b>Especialidad del evaluador</b>	Sistemas de información y comunicación
	
<b>DNI:</b> 18122765	Trujillo, 20 de diciembre del 2022

## Anexo 5 - Confiabilidad de los instrumentos de recolección de datos

### Resumen de procesamiento de casos

		N	%
Casos	Válido	12	100,0
	Excluido <sup>a</sup>	0	,0
	Total	12	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

### Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,805	12

## Anexo 6 - Solución propuesta

### PLAN DE GESTIÓN DE RIESGOS DE TI PARA UN EMPRESA INMOBILIARIA

El plan de gestión de riesgos de TI comprendió el desarrollo de buenas prácticas de gestión de riesgos de tecnologías de la información enmarcados en cuatro (4) pasos como sigue:



Figura: Plan de gestión de riesgos de TI

- **Paso 1: Diseño de controles de seguridad**

Una plataforma informática con controles de seguridad a la medida de la empresa siempre contribuirá a anticiparse a los problemas de forma oportuna.

Para el desarrollo de este paso, se recurrió a la norma internacional ISO/IEC 27002:2013, la cual considera los siguientes dominios de seguridad.

- **Política de seguridad de la información:**

En este dominio, se considera las normas o exigencias que se extiende a los involucrados de manera estricta que alcanza tanto a los trabajadores como a la parte de gerencia con un objetivo en común, el de salvaguardar los intereses y confidencialidad y disponibilidad del activo más importante de la Inmobiliaria como es la información que compete a la compañía.

- **Organización de la seguridad de la información:**

En este dominio, se desarrolla la identificación de puestos y roles que se integrará en el Sistema de Gestión de Seguridad de la Información (SGSI), donde se detalla los responsables y los representativos acuerdos de confidencialidad para la Inmobiliaria en estudio.

- **Seguridad en los recursos humanos:**

En este dominio, este departamento organizacional de la inmobiliaria es el encargado de que los recursos tanto como trabajadores, empleadores y terceros conozcan su participación en el proceso de la seguridad de la información capacitándolos de manera eventual según el rol que desempeñen en la participación de la Inmobiliaria, para de esta manera evitar el riesgo de sustracción del activo de la información.

- **Gestión de activos:**

En este dominio, se identifica los activos de la Inmobiliaria, ya sea de bienes o información para luego clasificarlos de acuerdo a las características, requerimientos, privacidad, confidencialidad, disponibilidad, y valor en este caso sea agregado o determinado que presente la información.

- **Control de accesos:**

En este dominio, la Inmobiliaria al tratarse de un control importante inmediato de acceso a la información; por tanto, debe limitarse el acceso de manera que se asegure

el manejo y manipulación de los sistemas de información a través del acceso seguro y autorizado que haya identificado a los usuarios a través de los permisos de seguridad de la información.

- **Criptografía:**

En este dominio, se garantiza el uso adecuado de la criptografía con el propósito de proteger la privacidad y confidencialidad de la información de la Inmobiliaria manteniendo la integridad de la misma.

- **Seguridad física y del entorno:**

En este dominio, se encarga de prevenir el acceso físico no autorizado, que puedan causar daños e interferencias al activo de información de la Inmobiliaria, asimismo evitando el acceso a las instalaciones donde se puedan tratar, o procesar la información y evitar el robo de los activos que puedan comprometer o interrumpir las operaciones de la organización.

- **Seguridad en las operaciones:**

En este dominio, se garantiza que, las operaciones de la Inmobiliaria se desarrollen de manera segura con la disponibilidad y veracidad en las áreas de procesamiento de información. Haciendo uso de los medios informáticos y aplicaciones para proteger los datos de spyware y malware que intenten vulnerar los medios de seguridad, asimismo hay que resaltar el registro de eventos generando evidencias. Asimismo, se debe garantizar el óptimo funcionamiento de los sistemas operativos.

- **Seguridad en las comunicaciones:**

En este dominio, se busca garantizar la protección de los activos de información de la red e instalaciones de procesamiento de datos de la Inmobiliaria. Se debe proteger la información transferida desde la compañía con cualquier organización externa.

- **Adquisición, desarrollo y mantenimiento de sistemas:**

En este dominio, se tiene un grado importante sobre los demás los dominios, pues éste depende la continuidad de la seguridad de la información evitando pérdidas y errores de los propios sistemas a través del mal uso del activo con aplicaciones licenciadas que protejan la seguridad de información de la Inmobiliaria.

- Relaciones con los proveedores:

En este dominio, se debe proteger los activos de la Inmobiliaria de manera que, sean accesible a los proveedores manteniendo un nivel de seguridad de la información y de contratación de servicios alineado con las cláusulas con éstos.

- Gestión de los incidentes de seguridad de la información:

En este dominio, se debe asegurar cualquier intento de vulnerabilidad sobre la seguridad que se encuentren relacionados con los sistemas de información, ya sean reportados de parte de la administración o áreas interesadas de la Inmobiliaria con el fin de permitir tomar decisiones correctivas y asertivas sobre el determinado riesgo o evento.

- Aspectos de seguridad de la información para la gestión de continuidad del negocio:

En este dominio, se implementa controles que permitan minimizar el riesgo de las interrupciones de actividades funcionales o comerciales críticas para la Inmobiliaria por motivos de desastres o eventos inesperados en los sistemas de información. garantizando la disponibilidad y continuidad para que el debido proceso o procedimiento se cumpla correctamente.

- Cumplimiento:

En este dominio, se asegura el cumplimiento de las obligaciones legales y acuerdos contractuales, derechos de propiedad y privacidad de datos personales relacionados a la seguridad de la información de la Inmobiliaria cumpliendo las políticas de seguridad que exige la legislación del estado.

- **Paso 2: Pruebas de seguridad**

La esencia de la prevención de riesgos informáticos yace en la ejecución de pruebas de seguridad. Una buena idea es realizarlas de forma periódica y calendarizada.

El propósito principal de las pruebas de seguridad es detectar vulnerabilidades y luego repararlas. Ayuda a impulsar el sistema actual de la Inmobiliaria y asegurarse de que el sistema pueda funcionar durante un tiempo prolongado para notar lagunas que provocarán la pérdida de información vital.

Esto incluye lo siguiente:

- Escaneo de vulnerabilidades:

Se realiza mediante software automatizado para examinar el marco frente a exposición.

- Escaneo de seguridad:

Incluye lidiar con la debilidad del sistema y el marco, encontrar respuestas para disminuir la amenaza.

- Pruebas de penetración:

También conocido como "Pruebas de penetración o piratería ética", lo cual, es una práctica de probar sistemas informáticos, redes o aplicaciones web para encontrar vulnerabilidades o debilidades de seguridad que un hacker o atacante podría aprovechar.

Las pruebas de penetración a menudo se realizan con un objetivo particular en mente. Estas metas generalmente caen bajo uno de los siguientes tres objetivos: identificar sistemas hackeables, intentar hackear un sistema específico y llevar a cabo una violación de datos.

Cada objetivo se centra en resultados específicos que los líderes de TI intentan evitar. Por ejemplo, si el objetivo de una prueba de penetración es ver con qué facilidad un pirata informático podría violar la base de datos de la empresa, se instruiría a los piratas informáticos éticos para intentar llevar a cabo una violación de datos.

Los resultados de una prueba de penetración no solo comunicarán la solidez de los protocolos de seguridad cibernética actuales de una organización, sino que también presentarán los métodos de piratería disponibles que se pueden usar para penetrar los sistemas de la organización.

Se puede realizar de forma manual o automatizada con aplicaciones de software.

- Evaluación de riesgos:

Este tipo de prueba incluye un examen de los peligros de seguridad que se ven en la asociación. Los riesgos se denominan de la siguiente manera: Bajo, Medio y Alto.

Esta prueba prescribe controles y medidas para disminuir el riesgo.

- Auditoría de seguridad:

Esta suele ser una investigación interna de aplicaciones y marcos operativos para detectar imperfecciones de seguridad.

La revisión también debería ser posible mediante el examen de código línea por línea.

- Hackeo ético:

Se refiere al acto de vulnerabilidades. y localizar la debilidad del sistema incluye exponer un sitio web para descubrir sus puntos débiles.

Un pirata informático ético intenta eludir el parche de seguridad del sistema que luego puede ser explotado por el pirata informático o atacante.

- Evaluación de la postura:

Esto se une a la comprobación de seguridad, el pirateo ético y las evaluaciones de riesgos para demostrar la postura de seguridad general de una asociación.



- **Paso 3: Gestión de los incidentes**

Se debe mantener un historial con cada uno de los riesgos identificados y gestionar estos datos para ser capaces de reaccionar a tiempo y de evitar problemas similares a futuro.

- **Análisis del riesgo:**

Para el análisis del riesgo se establece la causalidad de probabilidad de un determinado hecho o acción a ocurrir y sus probables consecuencias que acarreen los mismos, dichos probables riesgos se clasificarán según el contexto de la ocurrencia y el factor que impulse a la acción del riesgo.

Los aspectos que determinan el análisis del riesgo son:

- ✓ **Impacto:** Es el grado o nivel de frecuencia que puede ocasionar el riesgo según su contexto en la inmobiliaria.
- ✓ **Probabilidad.** Es la posibilidad que existe de un hecho o acción a ocurrir, la medición la realizaremos a través de una escala que se asignará según el grado de probabilidad.
- ✓ **Nivel de amenazas.** Es el grado de dificultad o de riesgo al cual está expuesto un activo de información interrumpiendo las correctas funciones que se presenta dentro de inmobiliaria.

**Tabla:** *Categorías de aspectos de riesgos en los procesos*

Probabilidad	Descripción	frecuencia
Improbable	Suceso que cuenta con casi ninguna posibilidad de ocurrencia.	1
Remoto	Suceso que tiende a ocurrir extrañamente.	2
Ocasional	Suceso que tiene posibilidad de ocurrir ante un agente causante.	3
probable	Suceso que tiene un grado superior de posibilidad de ocurrencia.	4
Muy probable	Evento que tiene mucha posibilidad de ocurrir con mucha frecuencia	5

Impacto	Descripción	Frecuencia
Minúsculo	El impacto no tiene mayor repercusión dentro de los procesos, los cuales no son afectados en su función ni en el desarrollo de sus actividades.	1-2
Menor	El grado de repercusión es leve pero igual demanda de un esfuerzo extra en el cumplimiento de los procesos.	3-4
Medio	El grado de impacto ya se va volviendo considerable por que se empleará más horas de trabajo y recursos, tal es así que esto ayudaría a intentar cubrir el cumplimiento de las actividades de los procesos.	5-6
Crítico	La importancia del impacto es mayor por tal motivo las horas se convierten en días de trabajo para suplir el incumplimiento de actividades por el grado de impacto presentado.	7-8
Muy crítico	El grado de impacto es definitivo en los procesos ya que se intentaría retomar las actividades de los procesos en los días posteriores, pero no existe la seguridad de que realmente se vaya a retomar la normalidad de los procesos.	9-10

Nivel de amenaza	Descripción	Frecuencia
Leve	Riesgo que se manifiesta de manera leve pero no es de mayor importancia ya que no afecta a los procesos	1
Medio	Gradualmente las amenazas van tomando cierto de grado de importancia y en este nivel el riesgo toma una importancia influyente	2
Alto	El riesgo en este nivel es de suma importancia o hasta decisivo en los procesos ya que se verán afectados por la importancia del mismo en su funcionamiento.	3

- Evaluación del riesgo:

La evaluación de riesgo es el proceso por el cual se analiza la probabilidad de ocurrencia y posibles consecuencias del daño o del evento que surge como resultado de la exposición a determinados riesgos.

Se tiene:

**Tabla: Evaluación del riesgo**

Probabilidad		Impacto			
Improbable	Minúsculo	Menor	Medio	Crítico	Muy crítico
Muy probable	A	A	P	P	P
probable	M	A	A	P	P
Ocasional	I	M	A	A	P
Remoto	I	I	M	A	P
Improbable	I	I	M	M	A

**Tabla: Indicadores del nivel de riesgo**

Mínimo Riesgo	Riesgo Moderado	Alto Riesgo	Riesgo extremo
I	M	A	P

- Valoración del riesgo:

Se hará una valorización en relación de los activos para determinar la importancia y el valor que contribuyen a la Inmobiliaria donde se conocerá los índices de valor que sostienen en la compañía.

**Tabla:** Valorización de activos informáticos

	Amenaza	Impacto	Nivel de Amenazas	Probabilidad	Nivel de Riesgo
Activo informático	Operacionales	5	1	2	10
	Naturales	4	1	1	4
	Instalaciones	5	1	2	10
	Tecnológicas	6	1	3	18
	Humanas	5	1	2	10
	Sociales	3	1	1	3
	Total	28	7	11	VMR = 18

▪ Tratamiento del riesgo:

Para el tratamiento del riesgo se establece un valor numérico que permitirá delimitar e identificar los activos que están expuestos a riesgos. La cifra límite es de 50, por lo que, los valores que superen este índice necesitarían del tratamiento establecido, a diferencia de los que no superen esta cifra se asumiría el riesgo.

También se fija el valor máximo del riesgo con las iniciales de VMR representado en la tabla anterior.

**Tabla:** Tratamiento del riesgo

Ítem	Activos	Amenaza	Nivel de amenaza	Nivel de Riesgo	Total
01	Activo informático	Tecnológica	2	18	30

- **Paso 4: Detección y clasificación de vulnerabilidades**

Más allá de la mera gestión de seguridad TI, se debe ser capaz de detectar y clasificar cada una de las vulnerabilidades a que se expone el sistema de la empresa. Existen herramientas informáticas capaces de escanear estos riesgos en tiempo real y continuo, entregando reportes de forma periódica.

La gestión de vulnerabilidades es un proceso continuo de IT que se encarga de identificar, evaluar, tratar e informar sobre las vulnerabilidades de seguridad en los sistemas y el software que se ejecuta en ellos. La gestión de vulnerabilidades, junto con otras tácticas de seguridad, es vital para que las empresas prioricen las posibles amenazas y minimicen su impacto.

En un proceso de gestión de vulnerabilidades no solo se evalúan los riesgos y amenazas de seguridad, sino que se categorizan los activos IT de la empresa y se clasifican las vulnerabilidades según su nivel de amenaza.

El proceso de gestión de vulnerabilidades es proactivo y cíclico, ya que requiere de una monitorización y corrección continua para garantizar la protección de los recursos IT de una organización.

Las fases de una gestión de vulnerabilidades son:

- **Identificar recursos TI:**

El primer paso para una correcta gestión de vulnerabilidades es identificar cada uno de los recursos TI que forman la infraestructura de la Inmobiliaria, como componentes hardware, aplicaciones y licencias de software, bases de datos, cortafuegos, etc.

- **Recoger información:**

La identificación de vulnerabilidades es un paso esencial en este proceso porque consiste en detectar y exponer todas las vulnerabilidades que pueden existir en la infraestructura IT de la Inmobiliaria ya identificada.

Este proceso se realiza con un escaneo o análisis de vulnerabilidades bajo una visión externa y externa, para garantizar unos resultados los más reales y precisos posibles.

- **Analizar y evaluar:**

Con las vulnerabilidades existentes ya identificadas se debe abordar un proceso de análisis y evaluación de los riesgos y amenazas de las mismas, para poder clasificarlas y priorizarlas según distintos niveles en la Inmobiliaria.

En el proceso de priorización de vulnerabilidades se debe tener en cuenta el riesgo de amenaza a nivel tecnológico, pero también en cuanto a impacto en los procesos y tareas de la empresa.

Se suele utilizar un sistema de puntuación de vulnerabilidades para su priorización, aunque muchas veces este tipo de puntuaciones no son el único factor para priorizar una vulnerabilidad.

- Tratar y corregir:

En esta fase se aplican las medidas necesarias para corregir las vulnerabilidades y para mitigar su impacto en caso de que sucedan en la Inmobiliaria.

La aplicación de parches de seguridad y de corrección de vulnerabilidades, la eliminación de procesos y tareas que comprometen la seguridad o la adopción de nuevas políticas de seguridad, son acciones para tratar y corregir las vulnerabilidades detectadas en la empresa.

Como norma general, para eliminar vulnerabilidades se utilizan tres tipos de acciones:

- ✓ Corrección. Es la opción preferible si puede ser llevada a cabo, y consiste en aplicar un parche o actualización para eliminar por completo la vulnerabilidad y que no pueda ser explotada.
- ✓ Mitigación. Si no puede aplicarse la corrección de una vulnerabilidad debe optarse por mitigar su impacto en el negocio, Para ello hay que aplicar la acción más efectiva para reducir la posibilidad de que sea explotada. Se trata de una medida temporal para ganar tiempo y poder encontrar una solución definitiva que la corrija.
- ✓ Aceptación. Cuando una vulnerabilidad es de bajo riesgo o su coste para eliminarla es mayor que el daño que ocasionaría en caso de ser explotada, se opta por no tomar medidas correctoras para corregirla.



**UNIVERSIDAD CÉSAR VALLEJO**

**FACULTAD DE INGENIERÍA Y ARQUITECTURA  
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

### **Declaratoria de Autenticidad del Asesor**

Yo, AGREDA GAMBOA EVERSON DAVID, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - TRUJILLO, asesor de Tesis titulada: "Plan de gestión de riesgos de tecnologías de la información para la Seguridad informática en una Empresa Inmobiliaria, Casma 2023", cuyo autor es DE LA CRUZ MEJIA CRISTHIAN PAUL, constato que la investigación tiene un índice de similitud de 23.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

TRUJILLO, 22 de Febrero del 2023

<b>Apellidos y Nombres del Asesor:</b>	<b>Firma</b>
AGREDA GAMBOA EVERSON DAVID <b>DNI:</b> 18161457 <b>ORCID:</b> 0000-0003-1252-9692	Firmado electrónicamente por: AGREDA el 27-03- 2023 11:58:20

Código documento Trilce: TRI - 0534757