UNIVERSIDAD CÉSAR VALLEJO

.”

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

Sistema de gestión de seguridad de la información para la Protección de datos en una inmobiliaria, Lima 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Ponce Cruz, Angel Sabino (orcid.org/0000-0002-4961-4578)

ASESOR:

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

LÍNEA DE INVESTIGACIÓN

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA

Desarrollo Económico, Empleo y Emprendimiento

TRUJILLO – PERÚ

2023

Dedicatoria

A mis Padres por todo su amor y cuidado desde que vine a este mundo.

A mi familia por ser lo mejor en mi vida.

Ángel Sabino

Agradecimiento

A la Universidad César Vallejo por permitirme alcanzar un sueño tan ansiado.

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

A mi Asesor de tesis por su apoyo metodológico para el desarrollo de la investigación.

El autor

Índice de contenidos

Pág.

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

Esta investigación tuvo como objetivo general mejorar la protección de datos en una inmobiliaria de la ciudad de lima en el año 2022 mediante la propuesta de un sistema de gestión de seguridad de la información. El tipo es investigación fue aplicada y de diseño pre experimental. Se determinó una muestra poblacional de 8 instituciones (públicas y privadas), las cuales fueron evaluadas mediante una Encuesta de satisfacción. El desarrollo de la solución tecnológica propuesta fue bajo la aplicación de la norma internacional ISO/IEC 27001. Como resultado principal se puede decir que, para el primer indicador, se logró minimizar el nivel de riesgos de seguridad de la información en 60.00%; para el segundo indicador, se logró maximizar el nivel de salvaguarda de los activos de información en 65.60% y para el tercer indicador, se logró maximizar el grado de satisfacción de los trabajadores en 62.80%. Como conclusión general se tiene que la propuesta de un sistema de gestión de seguridad de la información mejora significativamente la protección de datos en una Inmobiliaria limeña.

Palabras clave: Sistema de gestión, seguridad de la información, protección de datos, inmobiliaria.

Abstract

The general objective of this research was to improve data protection in a real estate company in the city of Lima in the year 2022 by proposing an information security management system. The type of research was applied and of pre-experimental design. A population sample of 8 institutions (public and private) was determined, which were evaluated by means of a satisfaction survey. The proposed technological solution was developed under the application of the international standard ISO/IEC 27001. The main result is that, for the first indicator, it was possible to minimize the level of information security risks by 60.00%; for the second indicator, it was possible to maximize the level of safeguarding of information assets by 65.60%; and for the third indicator, it was possible to maximize the degree of employee satisfaction by 62.80%. As a general conclusion, the proposal of an information security management system significantly improves data protection in a real estate company in Lima.

Key words: management system, information security, data protection, real estate.

I. INTRODUCCIÓN

En la actualidad, una información segura tiene un rol determinante en el desarrollo de una organización, razón por la cual distintas empresas buscan e implementan maneras de cómo proteger dicha información a través del **Sistema de Gestión de Seguridad de la Información (SGSI)**, donde por intermedio de un conjunto de normas y procedimientos, aseguran la integridad de los datos, permitiendo a la organización un desarrollo confiable y seguro en sus procesos, evitando la manipulación de datos que pueda afectar de gran manera a la organización; cabe mencionar que la protección de datos tiene una participación determinante en el desarrollo de una organización para las actividades y procesos que desempeñe y en el mejor desenvolvimiento y protección de datos que pueda afectar tanto a colaboradores internos como externos, por otro lado por ejemplo se puede volver vulnerable a través de un dispositivo móvil nuestra información se encuentra expuesta en cuentas ya sean personales o de trabajo o incluso de tarjetas de crédito y operaciones digitales interbancarias, que son registradas en plataformas o SO móviles quienes exigen estar vinculados a través de una cuenta y usuario para acceder a su uso y si estas cuentas son sustraídas, se volverían un peligro dándole mal uso a dicha información; siendo necesaria y de vital importancia la protección de datos en las organizaciones, es entonces que, se cuenta con el SGSI, el cual resguarda mediante protocolos y mecanismos de información segura de manera acertada, verídica y confiable.

A nivel internacional, Biblioguias (2020) afirmó que el resguardo de la información significa que aquellos cuya información se extraen, almacenan y transforman deben conocer qué data se guarda y usa haciendo una mejora sobre las deficiencias presentadas. Cuando el estudio involucra a seres humanos, se considera las normativas jurídicas y principios éticos de compartir información; la data personal hace referencia únicamente a registros u otros datos, solos o en combinación con otros datos, que pueden descubrir la identidad de alguien vivo. Por ejemplo, puede usar números en vez de nombres como un identificador en las encuestas, sin embargo, si se tiene otro registro que vincule esos números con nombres reales, se cree que cada registro comprende información personal; Se consideran “Datos Personales”

a la información tal como número telefónico, edad, ubigeo de casa o trabajo, entidad educacional de formación académica.

A nivel latinoamericano, Americasistemas (2015) sostuvo que, la Ley de Protección de Data Personal (LPDP) proporciona medidas generales de seguridad, pero también se recomienda a implementar ISO/IEC 27001 cuando la base de datos es compleja y crítica. En cuanto a las salvaguardas, la LPDP sugirió varias generalizaciones. Por otro lado, la APDP hizo propuestas no vinculantes a través de directivas de seguridad que la ley necesita para especificar los mecanismos seguros requeridos para las bases de data personal que procesan data sensible y se clasifican como complejas o críticas. Garantizó que las bases de datos personales que procesan información sensible se identifican por tipos de información procesada y categorías de procesamiento (compleja y crítica son las más exigentes). También sugirieron que toda empresa peruana hiciera todo lo posible para la protección de sus bases de datos, con o sin leyes de cuidado de data personal, pero eso no sucedió. La Ley 29733 ha sido un buen comienzo en el cuidado de la data personal porque atiende a la creciente divulgación de datos procesados por organizaciones en el país", dijeron los encuestados.

A nivel nacional, El Estado Peruano (2021) afirmó que, un SGSI contenía directivas, operaciones, reglas, bienes y tareas vinculadas, manejadas grupalmente por la empresa para proteger sus activos de información. Un SGSI es una orientación metódica que define, construye, maneja, supervisa, examina, sostiene y maximiza el cuidado de la data empresarial y, así alcanza las metas comerciales. Basada en la evaluación de riesgo y el nivel de aceptación de riesgo de la empresa y tiene como objetivo atender y manejar cada riesgo efectivamente. Analizar los requisitos de protección de los bienes de data y aplicación de los mecanismos correctos a fin de asegurar que estos bienes de data estén cuidados cada vez que se requiera contribuyendo a una implantación con éxito de un SGSI.

A nivel regional, Detrujillo.com (2021) señaló que, el ingreso a la data estatal y cuidado de la misma en la Autoridad Nacional de Protección de Datos Personales (ANPDP) durante el 2021, recibió un total de 136 reclamos por infracciones a la LPDP y, en su mayor número estaban relacionadas con el

uso de data para consumidores que ejecutan actividades económicas sin su consentimiento. Dado el auge del e-commerce en plena COVID-19, los medios de adquisición no se limitaron a los sitios de Internet, sino que también se utilizaron las redes sociales para comercializar un bien y/o servicio. Los sitios de Facebook podían generar una ventanilla única para sus bienes, data de los precios y cualidades. Las partes interesadas podían solicitar primero un pedido anticipado de un artículo y después obtener la data de pago para completar su adquisición.

En este contexto, se tuvo a una **empresa Inmobiliaria**, la cual también contaba con inversionistas que colaboraron con fondos en el manejo e implementación de cada proyecto apostando por ser proyectos serios y con lineamientos ya establecidos, es por ello que los procesos involucrados como lo operativo, financiero y de gestión fueron necesarios en una buena administración de la parte gerencial. Como se aprecia, la empresa últimamente ha ido creciendo involucrando un volumen considerable de información que maneja esta inmobiliaria sin embargo ante posibles deficiencias es de suma importancia proteger y resguardar la misma, puesto que se ha detectado manipulación y fuga de cierta información que involucraría el valor comercial de bienes activos como terrenos que se encuentran reservados o viviendas con tratos formales que ante una pérdida de información quedan expuestos a devaluaciones y regateos de distintos corredores o inmobiliarias que perjudica directa e indirectamente a los fines y cumplimientos de las metas propuestas.

Algunas deficiencias (**problemas específicos**) que se pudieron suscitar en el proceso de gestión en la protección de datos fueron: El manejo y apoyo del personal administrativo fue deficiente lo que genera desorientación y mal uso del personal operativo de los expedientes de potenciales clientes debido a la falta de designación de roles; La falta de controles de protección en el manejo de la información interna y externa fue vulnerable debido a la inseguridad en el cuidado de la cartera de clientes lo que podría originar la difusión y perdida de información en la protección de datos; Se contaba con personal poco calificado debido a la falta de capacitación y programas de actualización lo que provoca errores y deficiencias en las tareas

encomendadas; Se disponía de manuales y reglamentos desactualizados a causa de escasa información lo que ocasiona que el personal no tenga un propósito definido en sus actividades.

Se situó la **formulación del problema**: *General:* ¿En qué condición un programa de administración de información segura influye en la protección de datos en una Inmobiliaria de la ciudad de Lima en año 2022? *Específicos:* Deficiencia concreta 1 - ¿En qué condición un programa de administración de información segura influye en los riesgos de seguridad de la información en una Inmobiliaria de la ciudad de Lima en año 2022? Deficiencia concreta 2 - ¿En qué condición un programa de administración de información segura influye en la salvaguarda de los activos de información en una Inmobiliaria de la ciudad de Lima en año 2022? Deficiencia concreta 3 - ¿En qué condición un programa de administración de información segura influye en el grado de satisfacción de los trabajadores en una Inmobiliaria de la ciudad de Lima en año 2022?

Se situó la **justificación de la Investigación**: *Conveniencia:* favoreció a la compañía inmobiliaria proteger la información particular y la de sus clientes permitiendo el resguardo de datos de potenciales clientes, brindando a los clientes seguridad y confianza del cuidado de sus datos; *Relevancia social:* brindó confianza en el tratamiento de la información de sus trabajadores y clientes, siendo protegida por medio de normas y protocolos que permitirán una información real y verídica sin alteraciones que manipulen dicha información, minimizando riesgos o fuga de la integridad y disponibilidad de la misma; *Utilidad metodológica:* fue el soporte para futuras exploraciones en la protección de la data dentro de la compañía buscando evitar la sustracción de data que pudiera impactar en los beneficios de la organización; De esta manera la acertada protección de datos permitirá un estándar de calidad de información segura que proveería de confiabilidad a la gestión de la compañía; *Implicaciones prácticas:* permitió solucionar la administración de información segura; *Valor teórico:* ayudó a entender con mayor ahínco las bases teóricas de un programa de administración de la información y cuidado de la data.

Se situó los **objetivos** de la investigación: *General:* Maximizar el cuidado de la data en una Inmobiliaria de la ciudad de Lima en el año 2022 mediante

el despliegue del programa de administración de información segura; *Específicos:* Fin concreto 1 - Minimizar los riesgos de seguridad de la información; Fin concreto 2 - Maximizar la salvaguarda de los activos de información; Fin concreto 3 - Incrementar el grado de satisfacción de los trabajadores.

Se situó las **hipótesis:** *General:* “El programa de administración de información segura maximiza considerablemente el cuidado de la data de la compañía Inmobiliaria de la ciudad de lima en el año 2022”. *Específicas:* Teoría concreta 1 - “El programa de administración de información segura minimiza los riesgos de seguridad de la información de la compañía Inmobiliaria de la ciudad de lima en el año 2022”; Teoría concreta 2 - “El programa de administración de información segura maximiza la salvaguarda de los activos de información de la compañía Inmobiliaria de la ciudad de lima en el año 2022”; Teoría concreta 3 - “El programa de administración de información segura incrementa el grado de satisfacción de los trabajadores de la empresa Inmobiliaria de la ciudad de lima en el año 2022”.

II. MARCO TEÓRICO

En este estudio se hallaron **antecedentes** (artículos científicos y trabajos investigativos) que permitieron saber de estudios anteriores como:

Valencia y Orozco (2017) en su artículo tuvieron por objetivo implementar un mecanismo de programa de administración de protección de datos sustentado en la normativa ISO/IEC 27000, cuyo tipo de investigación fue descriptiva no experimentalista, donde se resaltó la interrelación que se presenta en cuatro de las metodologías que sostienen y se dio curso a las tareas que cumplía según lo requerido por la normativa ISO/IEC 27001, los determinados monitoreo seguro de la ISO/IEC 27002, la estructura del bosquejo ISO/IEC 27005 y las recomendaciones establecidas en la ISO/IEC 27003. La interrelación estableció como resultado acertado un proceso metódico dando solución al poder hacer frente ante un proyecto de gran nivel de importancia donde predomina la gestión de organizaciones basados en estándares internacionales. Este proceso fue de gran utilidad e importancia por ser de gran aporte para profesionales que incursionen en esta labor y que buscan herramientas hacia un exitoso desarrollo de un programa de gobernanza de cuidado de la data.

Salinas (2015) en su investigación tuvo como fin el prototipo de un programa para gestionar y proteger de manera eficiente los datos de la organización, quien desarrolló un tipo de estudio descriptivo no experimental; el sistema permitió el diseño para una gestión de la información más segura y protegiendo el activo más preciado que es la información, basándose en la normativa de seguridad que maneja la norma ISO 27001:2013, esto permitió como resultado a la empresa tener mejores normas de protección observando cada medida de protección aplicadas para una mejor administración y obtención de los objetivos estratégicos de la empresa.

Villegas y Zamora (2018) en su investigación tuvieron como objetivo la seguridad de cada activo y preservar las normas de Confidencialidad, Integridad y Disponibilidad de estos mediante un periodo de mejora continua en favor de la empresa. El tipo investigativo fue descriptivo no experimental en base al periodo de mejoramiento continuo (Ciclo PDCA) que aplique la Metodología MAGERIT; como resultado, se conoció las ventajas de un SGSI

en una empresa agroindustrial a través del uso de la normativa ISO 27001: 2013, permitiendo elaborar políticas de seguridad para la azucarera.

Cáceda (2021) a través de su investigación tuvo como objetivo usar un modelo dinámico para la mejora del manejo del cuidado de la infraestructura tecnológica. El tipo de investigación que manejó fue descriptiva no experimental adoptando un prototipo de mejora permanente de sistemas con el objeto de manejar la toma de decisiones estratégicas en seguridad de las organizaciones; este modelo permitió la gestión de las vulnerabilidades previniendo ataques de diversas situaciones, lo que se determina en los indicadores por medio de alertas que se puedan producir de ataques y vulnerabilidades.

Además, para entender mejor este tema de estudio propuesto, se situó un grupo de **bases teóricas** como:

Seguridad de la información: Bloque de programas y procedimientos que aseguran la confiabilidad, la integridad y la disposición de toda información (Del Peso Navarro, 2003). La protección de datos se diferencia por la conservación de la confidencialidad, permitiendo estar solo disponible para usuarios autorizados, protegiendo la información exacta en su proceso; y al final, su disposición (Villegas Rivera, y otros, 2018). Confidencialidad: Garantizando que los datos sean de fácil acceso solamente por personal permitido; Integridad: Protegiendo la información exacta en su proceso, también en su edición permitida; Disponibilidad: Garantizando que el personal permitido acceda a los datos y a los activos afiliados cuando sea solicitado.

Sistema de gestión: en cuanto a su *definición* abarca una estructura conteniendo recurso, procesos y procedimientos que permiten poner en práctica políticas y objetivos de una organización (Ruiz Larrocha, 2017).

Sistema de Gestión de Seguridad de Información (SGSI): Denominación basada en la reglamentación de la ISO/IEC 27001, donde dentro de su enfoque le brinda permisos al área de gerencial que determina, construye, ejecuta, supervisa, examina y optimiza el cuidado de los datos ante un riesgo comercial; siguiendo enfocados en operaciones que usan el periodo de Mejoramiento Continuo o el Ciclo Deming o PDCA (Plan-DoCheck-Act).

También, se basó en las normas UNE-ISO/IEC 27002:2009 y proporciona un listado de controles que se necesitan para cumplir con las metas de protección de datos (ISOTools, Excellence, 2020).

Sistema de información: Es un bloque de componentes que procesan, distribuyen y guardan toda información con el objeto de favorecer el proceso de la elección de alternativas y el control de la empresa (Laudon, y otros, 2016). Dentro de los componentes de un sistema informatizado encontramos a: los recursos, los datos, recursos informáticos, reglas de operación y telecomunicaciones.

Protección de datos: Se hace referencia al derecho fundamental de proteger al individuo a través de la decisión de sus propios datos en el uso masivo frente a la exposición de los mismos (Miguel Pérez, 2015).

Empresa: Es la unidad económico-social donde un conjunto de elementos como son el capital, la dirección y el trabajo se integran para lograr una producción útil y en armonía con las exigencias de un bien común. (Hernández y Rodriguez, y otros, 2011)**.**

*Empresa inmobiliaria***:** Es una sociedad que tiene por actividad arrendar, construir, vender y administrar bienes muebles e inmuebles de carácter civil. Las principales actividades de las empresas inmobiliarias son: venta y alquiler de propiedades, publicación de propiedades en diferentes medios de comunicación, asesoramiento legal, etc. (RAE, 2018). En cuanto a sus *Tipos:* se encuentran: *Promotora inmobiliaria*, es la encargada de planificar el desarrollo de realizar un proyecto ya que es la encargada de conseguir una propiedad para llevar a cabo el proyecto. *Constructora Inmobiliaria:* Luego de la adquisición de la propiedad inmueble (terreno), se inicia la construcción del proyecto donde intervienen uno o varios equipos de trabajo (Ingenieros, arquitectos, operarios, etc.); *Agencias Inmobiliarias*: La agencia es la que se encargará de vender las propiedades y bienes inmuebles ofertando a través de promociones y ventas directas a sus posibles compradores. Desarrolladora Inmobiliaria: Son aquellos que ven la oportunidad de negocio y a través de estrategias realizan un seguimiento hasta realizar la venta. Sociedad peruana de bienes raíces (raices, 2018).

Se situó el uso de algunos **enfoques conceptuales** como complementación de las teorías citadas anteriormente:

Riesgo: Definida como poner a una persona en peligro, y en algunas escrituras se refiere a la cercanía del daño. El riesgo, también conocido como probabilidad de pérdida, puede cuantificarse diferente a la probabilidad de riesgo el cual no es cuantificable. El riesgo es la incertidumbre asociada a la sospecha sobre la posibilidad de que suceda algo que podría conducir a una pérdida. El riesgo es una estimación del nivel de exposición a las amenazas que aparecen en uno o más bienes que causan perjuicios a la empresa. El riesgo describe lo sucedería a un activo si no estuviera debidamente protegido sabiendo qué propiedades son importantes en cada activo y qué propiedades si sitúan en riesgo, es importante analizar el programa correspondiente (Mejía Delgado, y otros, 2016).

Identificación de riesgos: Se debe identificar todos los bienes de data que tuvieran importancia para la empresa en lo que compete a un SGSI y sus administradores responsables, llamados dueños. Se debe identificar los peligros referentes a los bienes reconocidos. Se debe identificar las debilidades que pueden ser explotadas por tales peligros, el impacto potencial del detrimento de privacidad, probidad y disposición en cada bien (Mejía Delgado, y otros, 2016)

Análisis y evaluación de riesgos: Es un procedimiento metódico para evaluar el grado de peligro al que se exhibe una empresa. Sabiendo lo que sucederá, se debe tomar decisiones para administrar esos peligros. El estudio y la administración de peligros de los sistemas informatizados son el centro de las medidas referentes con el estudio, la examinación y la administración de riesgos. Los riesgos se pueden analizar de acuerdo con las metodologías de gestión de riesgos para identificar las amenazas y su impacto (Mejía Delgado, y otros, 2016)

Tratamiento del riesgo: Es un grupo de elección de alternativas para los activos de la data. Los fallos para manejar el peligro incluyen las opciones siguientes: *Impedir el riesgo:* La capacidad de impedir el riesgo es toda actividad que implica cambiar la forma en que una empresa opera o realiza negocios para evitar la ocurrencia del riesgo Mejía & Ruiz (2016); *Aceptar el*

*riesgo***,** si no puede ser mitigado, la actividad que lo provocó debe seguir. Las organizaciones a menudo se enfrentan a situaciones en las que faltan los controles o el diseño es inviable o el costo de implementar los controles supera los efectos del peligro. Bajo estas cualidades, puede ser un fallo lógico aceptar los riesgos y las consecuencias si los riesgos se materializan. Visualice las alternativas de 'transferir el peligro o impedir el peligro' cuando surjan situaciones en las que sería demasiado carísimo para la organización disminuir el riesgo mediante controles o los efectos del riesgo sería devastador para la empresa (Mejía Delgado, y otros, 2016); *Reducir el riesgo*, para reducir el impacto de los riesgos se debe implementar controles adecuados con la finalidad de disminuir la influencia en la empresa de los mismos. Los controles se deberían tomar de la norma ISO 270001:2013. Al establecer el grado de monitoreo, es primordial tener en cuenta los requisitos de protección referentes al riesgo, las vulnerabilidades y amenazas anteriormente identificadas. Los controles reducen el riesgo evaluado de muchas formas: Reduzca la probabilidad de que las vulnerabilidades sean explotadas por amenazas; Reduzca la probabilidad de impacto cuando los riesgos se materializan identificando eventos adversos, reaccionando y saliendo de estos; *Transferir el riesgo,* el riesgo es compartido de una u otra manera, según el contexto y la situación lo pueden compartir agentes internos así también como externos, para lo cual es afectada ambas partes (Rojas Viera, y otros, 2019).

Asimismo, con respecto a las **normativas internacionales o nacionales** respecto a seguridad de la información, básicamente se optó desde un inicio por la *norma internacional ISO 27002: 2013*, por lo que no fue necesario recurrir a la elección de la misma usando algún mecanismo de evaluación especializada.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

- **Tipo de investigación:**

  Aplicada debido a que se sostuvo en el uso de mecanismos ya probados y usadas en solución de la problemática planteada.

- **Diseño de investigación:**

  Preexperimental debido a que se basó en la manipulación deliberada de la muestra poblacional.

3.2 Variables y operacionalización

- Variables:
  - Independiente: *Sistema de gestión de seguridad de la información*
    - Definición conceptual: “Es un bloque de directivas, operaciones y tareas asociadas administradas por una entidad con la finalidad de cuidar eficientemente los bienes de data asegurando su confidencialidad, integridad y disponibilidad” (Valencia Duque, 2021).
    - Definición operacional: El SGSI contempla medidas de seguridad como confidencialidad, disponibilidad, integridad, controles de seguridad y políticas de seguridad.
  - Dependiente: *Protección de datos*
    - Definición conceptual: “Representa el cuidado de la data frente al tratamiento de datos masivos salvaguardándolo los intereses o bienes que podrían ser afectados a través de elaboraciones de informaciones malintencionadas dirigidas por terceros” (Miguel Pérez, 2015).

- Definición operacional: Son establecidos procedimientos y políticas permitiendo la implementación de mecanismos técnicas de soporte que serán necesarios para el uso de formalidades con la finalidad de dar protección a los datos alojados en los sistemas de almacenamiento.

- **Operacionalización:**

  En el Anexo 2 se exhibe el cuadro de operatividad de las variables de estudio.

3.3 Población, muestra y muestreo

- **Población (N):**

  La población estuvo definida por los trabajadores a nivel gerencial, administrativo y operativo de la empresa inmobiliaria.

  Tabla 1. *Población*

Cargo / Puesto	Cantidad
Gerente	01
Jefe de Área	02
Supervisor	02
Operario	06
Total	15

$$N = 15\ personas$$

- **Muestra (n):**

  Son los componentes de una población; se exhibe el tamaño muestral y el procedimiento en que se estableció.

  Dado que la Población fue inferior a 30, en consecuencia, la muestra fue semejante a la población:

$$n = 15\ personas$$

- **Muestreo:**

  Representa el mecanismo estadístico usado para la extracción de la muestra, de clase no probabilística.

3.4 Técnicas e instrumentos de recolección de datos

- Encuesta:

  Mecanismo técnico usado por intermedio de un instrumento conocido como Cuestionario, está dirigido a individuos con la finalidad de obtener información a través de sus opiniones o percepciones. Con la encuesta se pueden obtener resultados cualitativos o cuantitativos, la misma que tiene un orden y un sistema escalonado de respuestas, a través de ella se obtienen datos numéricos que servirá para el análisis estadístico Arias (2020).

  Para la investigación, se usó la Encuesta dirigido al personal operativo y administrativo con la finalidad de conocer el manejo y uso de la información que servirá para medir los estándares y directivas de seguridad para el cuidado de la data de la compañía Inmobiliaria.

- Entrevista:

  Esta técnica es considerada mecánica, porque el entrevistado estará disponible a contestar una guía de preguntas que se elaboran con el fin de conocer la situación de una persona, empresa u organización. Las preguntas siguen una secuencia establecida que puede servir como un cuestionario que fue a su vez guiado por el entrevistador Arias (2020).

  La técnica de la entrevista estará dirigida a la parte gerencial de quien a través de una guía de preguntas nos permitirá conocer

las gestiones de seguridad y operativa a las que está expuesta la información de la empresa que podría afectar de distintas maneras exponiéndose de manera importante a vulnerabilidades.

- Validez y confiabilidad

  Para que el uso de las herramientas de absorción de la data como el Cuestionario y la Guía de entrevista fueran válidos y confiables se sometió y tuvo la aprobación de un *Juicio de expertos* integrados por tres miembros los cuales a través de su rúbrica confirmarán y darán fe de la validez y la confiabilidad que garantizarán una correcta y asertiva encuesta (ver Anexo 4).

  Asimismo, el instrumento empleado en la realización de nuestro trabajo de investigación será evaluados analizados a través del método estadístico *Alpha de Cronbach*, este método estadístico será implementado en el software estadístico llamado SPSS para la confiabilidad del instrumento (ver Anexo 5).

3.5 Procedimientos

El despliegue de la vigente investigación conllevo al desarrollo de los tres (3) fines concretos descritos en el primer capítulo como fueron:

- Fin concreto 1: Minimizar los riesgos de seguridad de la información.
- Fin concreto 2: Maximizar la salvaguarda de los activos de información.
- Fin concreto 3: Incrementar el grado de satisfacción de los trabajadores

3.6 Método de análisis de datos

Se empleó el modelo estadístico descriptivo, permitiendo la recolección de los resultados de los instrumentos los que nos permitirá

reflejar los datos recolectados para posteriormente representarlos y analizarlos a través de gráficos estadísticos

Se empleó el modelo inferencial, permitiendo hallar la normalidad de los indicadores establecidos, utilizando distribuciones estadísticas que acordes al tamaño muestral usado.

3.7 Aspectos éticos

Dentro de los elementos morales, se resalta el manual de ética de la Universidad, el cual consta de veintiuno artículos los cuales constan entre objetivos, principios, normas éticas, responsabilidades, políticas de plagio, derechos de autoría, entre otros; los cuales tienen la finalidad de reglamentar los alcances y derechos del investigador a fin de realizar una investigación acorde con los estándares de seguridad y calidad que respalda la entidad universitaria. Asimismo, el trabajo de investigación será realizado en el formato ISO-690 el cual es exigido por la Universidad como requisito para el despliegue de la investigación; De igual manera el trabajo de investigación es de elaboración propia y originalidad por ello es importante resaltar que se debe respetar los derechos de autor a fin de ser realizar una investigación con total legitimidad.

IV. RESULTADOS

- **Análisis descriptivo**

  - Indicador “Nivel de riesgos de seguridad de la información”

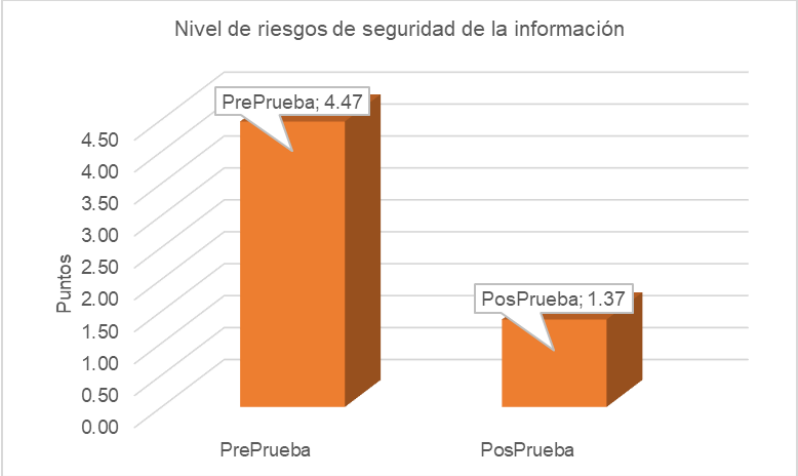


Figura 1. Promedio de preprueba y posprueba del primer indicador.

Se ilustra una minimización del nivel de riesgos de seguridad de la información de 62.00% ulterior al despliegue del SGSI en la compañía inmobiliaria.

  - Indicador “Nivel de salvaguarda de los activos de información”

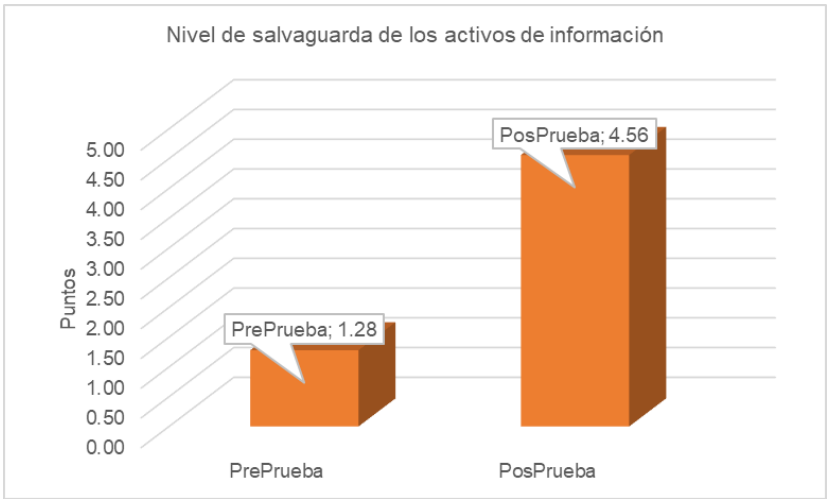


Figura 2. Promedio de preprueba y posprueba del segundo indicador.

Se ilustra una maximización del nivel de salvaguarda de los activos de información de 65.60% ulterior al despliegue del SGSI la compañía inmobiliaria.

- Indicador “Grado de satisfacción de los trabajadores”

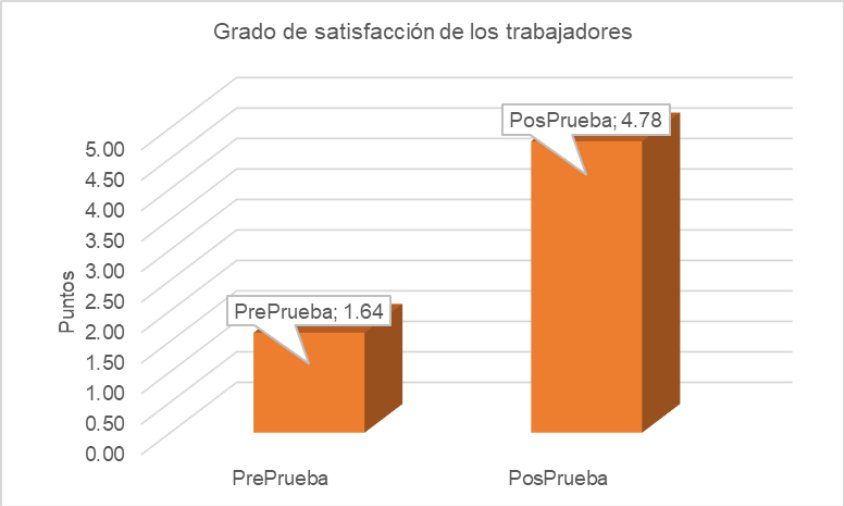


Figura 3. Promedio de preprueba y posprueba del tercer indicador.

Se ilustra un incremento del grado de satisfacción de los trabajadores de 62.80% ulterior al despliegue del SGSI en la compañía inmobiliaria.

- **Análisis inferencial**
  - Indicador “Nivel de riesgos de seguridad de la información”

    H_0: “El nivel de riesgos de seguridad de la información (sin el despliegue del SGSI) si incluye reparto normalizado”.

    H_1: “El nivel de riesgos de seguridad de la información (sin el despliegue del SGSI) no incluye reparto normalizado”.

    H_0: “El nivel de riesgos de seguridad de la información (con el despliegue del SGSI) no incluye reparto normalizado”.

    H_1: “El nivel de riesgos de seguridad de la información (con el despliegue del SGSI) si incluye reparto normalizado”.

    Se optó como valía de significancia: $\alpha = 0.05$

    Valía de significancia > 0.05, acoge la teoría negativa (H_0).

    Valía de significancia ≤ 0.05, coge la teoría positiva (H_1).

Tabla 2. *Prueba de normalidad del primer indicador*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
NRSI-Pre	,817	12	,063
NRSI-Pos	,845	12	,002

Fuente: (Elaboración Propia, 2022)

Según cálculos realizados en las condiciones previa (0.063) y subsiguiente (0.002), se desplegó el examen de Wilcoxon por ser parte de una data inmersa en una distribución normalizada.

- Indicador “Nivel de salvaguarda de los activos de información”

  H_0: “El nivel de salvaguarda de los activos de información (sin el despliegue del SGSI) si incluye reparto normalizado”.

  H_1: “El nivel de salvaguarda de los activos de información (sin el despliegue del SGSI) no incluye reparto normalizado”.

  H_0: “El nivel de salvaguarda de los activos de información (con el despliegue del SGSI) no incluye reparto normalizado”.

  H_1: “El nivel de salvaguarda de los activos de información (con el despliegue del SGSI) si incluye reparto normalizado”.

Se optó como valía de significancia: $\alpha = 0.05$

Valía de significancia > 0.05, acoge la teoría negativa (H_0).

Valía de significancia ≤ 0.05, acoge la teoría positiva (H_1).

Tabla 3. *Prueba de normalidad del segundo indicador*

	Shapiro-Wilk		
	Estadístico	Gl	Sig.
NSAI-Pre	,892	12	,058
NSAI-Pos	,883	12	,004

Fuente: (Elaboración Propia, 2022)

Según cálculos realizados en las condiciones previa (0.058) y subsiguiente (0.004), se desplegó el examen de Wilcoxon por ser parte de una data inmersa en una distribución normalizada.

- Indicador “Grado de satisfacción de los trabajadores”

H_0: “El grado de satisfacción de los trabajadores (sin el despliegue del SGSI) si incluye reparto normalizado”.

H_1: “El grado de satisfacción de los trabajadores (sin el despliegue del SGSI) no incluye reparto normalizado”.

H_0: “El grado de satisfacción de los trabajadores (con el despliegue del SGSI) no incluye reparto normalizado”.

H_1: “El grado de satisfacción de los trabajadores (con el despliegue del SGSI) si incluye reparto normalizado”.

Se optó como valía de significancia: $\alpha = 0.05$

Valía de significancia > 0.05, acoge la teoría negativa (H_0).

Valía de significancia ≤ 0.05, acoge la teoría positiva (H_1).

Tabla 4. *Prueba de normalidad del tercer indicador*

	Shapiro-Wilk		
	Estadístico	Gl	Sig.
GST-Pre	,855	12	,051
GST-Pos	,866	12	,003

Fuente: (Elaboración Propia, 2022)

Según cálculos realizados en las condiciones previa (0.051) y subsiguiente (0.003), se desplegó el examen de Wilcoxon por ser parte de una data inmersa en una distribución normalizada.

- **Contrastación de hipótesis**

  - Teoría concreta 1:

    “El programa de administración de información segura minimiza los riesgos de seguridad de la información de la compañía Inmobiliaria de la ciudad de lima en el año 2022”.

    Se trabajó con las teorías estadísticas negativa y positiva especificando el importe de significancia a 0.05.

    Tabla 5. *Prueba de Wilcoxon para el primer indicador*

	NRSI-Pos - NRSI-Pre
Z	-3,142[b]
Sig. asintótica(bilateral)	,002

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: (Elaboración propia, 2022)

Basado en la tabla anterior, se observa que valía de significancia bilateral del examen de Wilcoxon para el primer indicador “Nivel de riesgos de seguridad de la información” examinado en la condición previa y subsiguiente al despliegue de la solución ofrecida fue 0.002 (≤ 0.05). En tal contexto, se desestima la teoría negativa (H_0) y se acoge la teoría positiva (H_1); por tanto, se infiere: “Se tiene suficiente certidumbre estadística (95%) para sostener que, el despliegue de un SGSI si minimiza el nivel de riesgos de seguridad de la información de una compañía inmobiliaria de la ciudad de Lima en el año 2022 de manera cuantiosa”.

- Teoría concreta 2:

"El programa de administración de información segura minimiza los riesgos de seguridad de la información de la compañía Inmobiliaria de la ciudad de lima en el año 2022".

Se trabajó con las teorías estadísticas negativa y positiva especificando el importe de significancia a 0.05.

Tabla 6. *Prueba de Wilcoxon para el segundo indicador*

	NSAI-Pos - NSAI-Pre
Z	-3,518[b]
Sig. asintótica(bilateral)	,003

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: (Elaboración propia, 2022)

Basado en la tabla anterior, se observa que valía de significancia bilateral del examen de Wilcoxon para el primer indicador "Nivel de salvaguarda de los activos de información" examinado en la condición previa y subsiguiente al despliegue de la solución ofrecida fue 0.003 (≤ 0.05). En tal contexto, se desestima la teoría negativa (H_0) y se acoge la teoría positiva (H_1); por tanto, se infiere: "Se tiene suficiente certidumbre estadística (95%) para sostener que, el despliegue de un SGSI si maximiza el nivel de salvaguarda de los activos de información de una compañía inmobiliaria de la ciudad de Lima en el año 2022 de manera cuantiosa".

- Teoría concreta 3:

"El programa de administración de información segura minimiza los riesgos de seguridad de la información de la compañía Inmobiliaria de la ciudad de lima en el año 2022".

Se trabajó con las teorías estadísticas negativa y positiva especificando el importe de significancia a 0.05.

Tabla 7. *Prueba de Wilcoxon para el tercer indicador*

	GST-Pos - GST-Pre
Z	-3,481[b]
Sig. asintótica(bilateral)	,001

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: (Elaboración propia, 2022)

Basado en la tabla anterior, se observa que valía de significancia bilateral del examen de Wilcoxon para el primer indicador "Grado de satisfacción de los trabajadores" examinado en la condición previa y subsiguiente al despliegue de la solución ofrecida fue 0.001 (≤ 0.05). En tal contexto, se desestima la teoría negativa (H_0) y se acoge la teoría positiva (H_1); por tanto, se infiere: "Se tiene suficiente certidumbre estadística (95%) para sostener que, el despliegue de un SGSI si incrementa el grado de satisfacción de los trabajadores de una compañía inmobiliaria de la ciudad de Lima en el año 2022 de manera cuantiosa.

V. DISCUSIÓN

En lo referente al primer indicador “Nivel de riesgos de seguridad de la información”, los valores conseguidos en los cálculos estadísticos de las condiciones previa y subsiguiente al despliegue de la solución ofrecida (SGSI) fueron 4.47 y 1.37 puntos respectivamente, visualizando un mínimo cuantioso de 62.00%. Estos logros son afines a los conseguidos por (Cáceda, 2021), quien propuso un modelo de mejora continuo de sistemas con la finalidad de manejar la toma de decisiones estratégicas en seguridad de las organizaciones; este modelo permitió la gestión de las vulnerabilidades previniendo ataques de diversas situaciones, lo que se determina en los indicadores por medio de alertas que se puedan producir de ataques y vulnerabilidades. Todo ello, se sostiene en las bases teóricas del SGSI, dentro de su enfoque le brinda permisos al área de gerencial que determina, construye, ejecuta, supervisa, examina y optimiza el cuidado de los datos ante un riesgo comercial (ISOTools, Excellence, 2020).

En lo referente al segundo indicador “Nivel de salvaguarda de los activos de información”, los valores conseguidos en los cálculos estadísticos de las condiciones previa y subsiguiente al despliegue de la solución ofrecida (SGSI) fueron 1.28 y 4.56 puntos respectivamente, visualizando un máximo cuantioso de 65.60%. Estos resutados son afines a los conseguidos por (Valencia Duque, y otros, 2017), quienes en su investigación establecieron como resultado acertado un proceso metódico dando solución al poder hacer frente ante un proyecto de gran nivel de importancia donde predomina la gestión de organizaciones basados en estándares internacionales. Este proceso fue de gran utilidad e importancia por ser de gran aporte para profesionales que incursionen en esta labor y que buscan herramientas hacia un exitoso despliegue de un programa de administración de cuidado de la data. Todo ello, se sostiene en las bases teóricas del SGSI, se enfoca en operaciones que usan el periodo de Mejoramiento Continuo o el Ciclo Deming o PDCA (Plan-DoCheck-Act). También, se basó en las normas UNE-ISO/IEC 27002:2009 (ISOTools, Excellence, 2020).

En lo referente al tercer indicador “Grado de satisfacción de los trabajadores”, los valores conseguidos en los cálculos estadísticos de las

condiciones previa y subsiguiente al despliegue de la solución ofrecida (SGSI) fueron 1.64 y 4.78 puntos respectivamente, visualizando un incremento cuantioso de 62.80%. Estos resultados son afines a los conseguidos por (Salinas, 2015), quien desarrolló un sistema que permitió el diseño para una gestión de la información más segura y protegiendo el activo más preciado que es la información, basándose en la normativa de seguridad que maneja la norma ISO 27001:2013, esto permitió como resultado a la empresa tener mejores normas de protección observando cada medida de protección aplicadas para una mejor administración y obtención de los objetivos estratégicos de la empresa. Todo ello, se sostiene en las bases teóricas del SGSI, proporciona un listado de controles que se necesitan para cumplir con las metas de protección de datos (ISOTools, Excellence, 2020).

VI. CONCLUSIONES

1. Se pudo minimizar el nivel de riesgos de seguridad de la información en 60.00%, donde los valores conseguidos en los cálculos estadísticos de las condiciones previa y subsiguiente al despliegue de la solución ofrecida fueron 4.47 y 1.37 puntos respectivamente. Esto constata que un SGSI maximiza la protección de la data de una compañía inmobiliaria de la ciudad de Lima en el año 2022.
2. Se pudo maximizar el nivel de salvaguarda de los activos de información en 65.60%, donde los valores conseguidos en los cálculos estadísticos de las condiciones previa y subsiguiente al despliegue de la solución ofrecida fueron 1.28 y 4.56 puntos respectivamente. Esto constata que un SGSI maximiza la protección de la data de una compañía inmobiliaria de la ciudad de Lima en el año 2022.
3. Se pudo maximizar el grado de satisfacción de los trabajadores en 62.80%, donde los valores conseguidos en los cálculos estadísticos de las condiciones previa y subsiguiente al despliegue de la solución ofrecida fueron 1.64 y 4.78 puntos respectivamente. Esto constata que un SGSI maximiza la protección de la data de una compañía inmobiliaria de la ciudad de Lima en el año 2022.

VII. RECOMENDACIONES

Al Gerente general:

Se recomienda poner en práctica la propuesta técnica ofertada (SGSI) toda vez que se realice tomando en cuenta la norma internacional ISO 27002:2013.

A los Supervisores:

Se recomienda considerar en sus buenas prácticas laborales el cuidado de la data por intermedio del despliegue del SGSI.

Al Jefe de personal:

Se recomienda promover la educación y formación cultural en seguridad de la información entre los trabajadores de la compañía toda vez que se debe respetar las directivas establecidas en el SGSI.

A los Trabajadores:

Se recomienda respetar de forma integral todas las directivas establecidas en el SGSI.

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 Ingenieria de Sistemas e Informática, 2021. pág. 126.

Del Peso Navarro, Emilio. 2003. *Manual de Outsourcing Informático.* Madrid : Díaz de Santos, 2003. Vol. Segunda Edición.

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/.

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.

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 Ingenieria - 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.

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://bienesraicess.com/.

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.* Universidad Nacional Pedro Ruíz Gallo. Lambayeque : s.n., 2019.

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

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.

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.

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/Iec 27001:2013 para la Empresa Agroindustrial Pomalca S.A.A. - 2016.* Lambayeque : Facultad Ciencias y Mateméticas - Universidad Pedro Ruiz Gallo, 2018.

ANEXOS

Anexo 1 - Matriz de consistencia de la investigación

Título: Sistema de gestión de seguridad de la información para la Protección de datos en una Inmobiliaria, Lima 2022.

Autor: Ponce Cruz, Ángel Sabino.

Problema	Objetivo	Hipótesis	Variable
General: ¿En qué condición un programa de administración de información segura influye en la protección de datos en una Inmobiliaria de la ciudad de Lima en año 2022?	General: Maximizar el cuidado de la data en una Inmobiliaria de la ciudad de Lima en el año 2022 mediante el despliegue del programa de administración de información segura.	General: “El programa de administración de información segura maximiza considerablemente el cuidado de la data de la compañía Inmobiliaria de la ciudad de lima en el año 2022”.	Independiente: Sistema de gestión de seguridad de la información
Específicos: 1. ¿En qué condición un programa de administración de información segura influye en los riesgos de seguridad de la información en una Inmobiliaria de la ciudad de Lima en año 2022? 2. ¿En qué condición un programa de administración de información segura influye en la salvaguarda de los activos de información en una Inmobiliaria de la ciudad de Lima en año 2022? 3. ¿En qué condición un programa de administración de información segura influye en el grado de satisfacción de los trabajadores en una Inmobiliaria de la ciudad de Lima en año 2022?	Específicos: 1. Minimizar los riesgos de seguridad de la información. 2. Maximizar la salvaguarda de los activos de información. 3. Incrementar el grado de satisfacción de los trabajadores.	Específicas: 1. “El programa de administración de información segura minimiza los riesgos de seguridad de la información de la compañía Inmobiliaria de la ciudad de lima en el año 2022”. 2. “El programa de administración de información segura maximiza la salvaguarda de los activos de información de la compañía Inmobiliaria de la ciudad de lima en el año 2022”. 3. “El programa de administración de información segura incrementa el grado de satisfacción de los trabajadores de la empresa Inmobiliaria de la ciudad de lima en el año 2022”.	Dependiente: Protección de datos

<table>
<tr><td colspan="4">Metodología</td></tr>
<tr>
<td>Tipo de investigación:

Aplicada</td>
<td>Población (N):

La población se encuentra determinada por todos los trabajadores de la empresa inmobiliaria.

$N = 15\ personas$</td>
<td>Técnicas de recolección de datos:

• Encuesta</td>
<td>Método de análisis de datos:

• Estadística descriptiva
• Estadística inferencial</td>
</tr>
<tr>
<td>Diseño de investigación:

Preexperimental</td>
<td>Muestra (n):

Dado que la Población es menor que 30, entonces:

$n = 15\ personas$</td>
<td>Instrumentos de recolección de datos:

• Cuestionario</td>
<td>Aspectos éticos:

Se respetará el derecho a la propiedad intelectual (Originalidad de la investigación - Reporte Turnitin).

Se tomará en cuenta el Código de ética de la Universidad César Vallejo.

Adicionalmente, se usará para la redacción de la investigación el Sistema de normas ISO-690.</td>
</tr>
</table>

Anexo 2 - Matriz de operacionalización de variables

Variable	Definición Conceptual	Definición Operacional	Dimensión (Sub variable)	Indicador	Escala de medición
Independiente: Sistema de gestión de seguridad de la información	"Es un bloque de directivas, operaciones y tareas asociadas administradas por una entidad con la finalidad de cuidar eficientemente los bienes de data asegurando su confidencialidad, integridad y disponibilidad" (Valencia Duque, 2021).	El SGSI contempla medidas de seguridad como confidencialidad, disponibilidad, integridad, controles de seguridad y políticas de seguridad.			
Dependiente: Protección de datos	"Representa el cuidado de la data frente al tratamiento de datos masivos salvaguardándolo los intereses o bienes que podrían ser afectados a través de elaboraciones de informaciones malintencionadas dirigidas por terceros" (Miguel Pérez, 2015).	Son establecidos procedimientos y políticas permitiendo la implementación de mecanismos técnicas de soporte que serán necesarios para el uso de formalidades con la finalidad de dar protección a los datos alojados en los sistemas de almacenamiento.	Información	Nivel de riesgos de seguridad de la información	Ordinal
				Nivel de salvaguarda de los activos de información	Ordinal
			Persona	Grado de satisfacción de los trabajadores	Ordinal

Anexo 3 - Instrumentos de recolección de datos

Cuestionario aplicado a los trabajadores de la empresa Inmobiliaria - Lima.

A continuación, se presenta una lista de preguntas contenidas en doce (12) ítems que corresponden a la percepción de la protección de datos por parte de los trabajadores de la empresa.

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
Protección de datos	Información	1. ¿Se cumple el procedimiento de identificación de riesgos de seguridad de la información?					
		2. ¿Se cumple el procedimiento de evaluación de riesgos de seguridad de la información?					
		3. ¿Se cumple el procedimiento de tratamiento de riesgos de seguridad de la información?					
		4. ¿Se cumple el procedimiento de monitoreo de riesgos de seguridad de la información?					
		5. ¿Se cumple el procedimiento de protección del acceso a la información?					
		6. ¿Se cumple el procedimiento de protección del tratamiento de la información?					
		7. ¿Se cumple el procedimiento de protección del respaldo de la información?					
		8. ¿Se cumple el procedimiento de protección de los reportes de información?					
	Persona	9. ¿Se brinda el servicio de protección de datos con alta eficiencia?					
		10. ¿Se brinda el servicio de protección de datos con alta eficacia?					
		11. ¿Se brinda el servicio de protección de datos con alta efectividad?					
		12. ¿Se brinda el servicio de protección de datos con alta confiabilidad?					

Anexo 5 - Validación de los instrumentos de recolección de datos

Hoja de validación del instrumento

I. Datos generales:

Cuestionario

II. II. Instrucciones:

En el siguiente cuadro, para cada ítem del contenido del instrumento que revisa, marque usted con un check (√) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad, Pertinencia o Relevancia*.

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Información							
1. ¿Se cumple el procedimiento de identificación de riesgos de seguridad de la información?	x		x		x		
2. ¿Se cumple el procedimiento de evaluación de riesgos de seguridad de la información?	x		x		x		
3. ¿Se cumple el procedimiento de tratamiento de riesgos de seguridad de la información?	x		x		x		
4. ¿Se cumple el procedimiento de monitoreo de riesgos de seguridad de la información?	x		x		x		
5. ¿Se cumple el procedimiento de protección del acceso a la información?	x		x		x		
6. ¿Se cumple el procedimiento de protección del tratamiento de la información?	x		x		x		
7. ¿Se cumple el procedimiento de protección del respaldo de la información?	x		x		x		
8. ¿Se cumple el procedimiento de protección de los reportes de información?	x		x		x		
Dimensión 2: Persona							
9. ¿Se brinda el servicio de protección de datos con alta eficiencia?	x		x		x		
10. ¿Se brinda el servicio de protección de datos con alta eficacia?	x		x		x		
11. ¿Se brinda el servicio de protección de datos con alta efectividad?	x		x		x		
12. ¿Se brinda el servicio de protección de datos con alta confiabilidad?	x		x		x		

[1]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

[2]**Pertinencia:** Si el ítem pertenece a la dimensión.

[3] **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.

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Dr. Agreda Gamboa, Everson David
Especialidad del evaluador	Redes y Comunicaciones
 **DNI:** 18161457	Trujillo, 29 de mayo del 2022

Hoja de validación del instrumento

I. Datos generales:

Cuestionario

II. II. Instrucciones:

En el siguiente cuadro, para cada ítem del contenido del instrumento que revisa, marque usted con un check (√) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad, Pertinencia o Relevancia*.

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Información							
1. ¿Se cumple el procedimiento de identificación de riesgos de seguridad de la información?	x		x		x		
2. ¿Se cumple el procedimiento de evaluación de riesgos de seguridad de la información?	x		x		x		
3. ¿Se cumple el procedimiento de tratamiento de riesgos de seguridad de la información?	x		x		x		
4. ¿Se cumple el procedimiento de monitoreo de riesgos de seguridad de la información?	x		x		x		
5. ¿Se cumple el procedimiento de protección del acceso a la información?	x		x		x		
6. ¿Se cumple el procedimiento de protección del tratamiento de la información?	x		x		x		
7. ¿Se cumple el procedimiento de protección del respaldo de la información?	x		x		x		
8. ¿Se cumple el procedimiento de protección de los reportes de información?	x		x		x		
Dimensión 2: Persona							
9. ¿Se brinda el servicio de protección de datos con alta eficiencia?	x		x		x		
10. ¿Se brinda el servicio de protección de datos con alta eficacia?	x		x		x		
11. ¿Se brinda el servicio de protección de datos con alta efectividad?	x		x		x		
12. ¿Se brinda el servicio de protección de datos con alta confiabilidad?	x		x		x		

[1]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

[2]**Pertinencia:** Si el ítem pertenece a la dimensión.

[3] **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.

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Dr. Mendoza Rivera, Ricardo Darío
Especialidad del evaluador	Gestión de Proyectos de TIC
 **DNI:** 18070765	Trujillo, 29 de mayo del 2022

Hoja de validación del instrumento

I. Datos generales:

Cuestionario

II. II. Instrucciones:

En el siguiente cuadro, para cada ítem del contenido del instrumento que revisa, marque usted con un check (√) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad, Pertinencia o Relevancia*.

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Información							
1. ¿Se cumple el procedimiento de identificación de riesgos de seguridad de la información?	x		x		x		
2. ¿Se cumple el procedimiento de evaluación de riesgos de seguridad de la información?	x		x		x		
3. ¿Se cumple el procedimiento de tratamiento de riesgos de seguridad de la información?	x		x		x		
4. ¿Se cumple el procedimiento de monitoreo de riesgos de seguridad de la información?	x		x		x		
5. ¿Se cumple el procedimiento de protección del acceso a la información?	x		x		x		
6. ¿Se cumple el procedimiento de protección del tratamiento de la información?	x		x		x		
7. ¿Se cumple el procedimiento de protección del respaldo de la información?	x		x		x		
8. ¿Se cumple el procedimiento de protección de los reportes de información?	x		x		x		
Dimensión 2: Persona							
9. ¿Se brinda el servicio de protección de datos con alta eficiencia?	x		x		x		
10. ¿Se brinda el servicio de protección de datos con alta eficacia?	x		x		x		
11. ¿Se brinda el servicio de protección de datos con alta efectividad?	x		x		x		
12. ¿Se brinda el servicio de protección de datos con alta confiabilidad?	x		x		x		

[1]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

[2]**Pertinencia:** Si el ítem pertenece a la dimensión.

[3] **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.

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Ms. Córdova Otero, Juan Luis
Especialidad del evaluador	Sistemas de información y comunicación
 **DNI:** 18122765 Trujillo, 29 de mayo del 2022	

Anexo 5 - Confiabilidad de los instrumentos de recolección de datos

Resumen de procesamiento de casos

		N	%
Casos	Válido	12	100,0
	Excluido[a]	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
,791	12

Anexo 6 - Solución propuesta

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UN EMPRESA INMOBILIARIA

FASE I: PLANIFICACIÓN

1.1. Introducción a la Norma ISO 27001:2013

Es una normativa que está abocada a la gestión de seguridad de la información donde establece un conjunto de lineamientos a través de una serie de requisitos que permiten implementar, planificar, verificar, analizar, mantener y mejorar un Sistema de Gestión de Seguridad de la información con la finalidad de proteger el principal activo de toda empresa como es la información. Es en base a estos requisitos que se determinará la efectividad o deficiencia de algunos puntos clave en la SGSI. La normativa ISO 27001 es el marco de referencia clave para el desarrollo del proyecto del Sistema de Gestión de Seguridad de la Información para la empresa. porque nos permitirá determinar puntos estratégicos que resguarden el activo de la empresa.

La Norma ISO 27001:2013 está conformada por 14 dominios 35 objetivos de control y 111 controles, además 14 nuevos controles y más de 30 controles actualizados. Uno de los principales cambios radica en el área de evaluación y aprendizaje de los eventos de seguridad de TI.

1.2. Objetivos del SGSI

Establecer el análisis de riesgos, identificando amenazas, factores vulnerables y de impacto en la Empresa motivo de investigación, con el objetivo de proporcionar al SGSI una mejora en la adopción de la norma en cuanto a la forma de trabajo con respecto a la seguridad de la información.

- Personal involucrado en el alcance del SGSI capacitado en aspectos de seguridad de información.
- Garantía de continuidad y disponibilidad del negocio.
- El incremento de los niveles de confianza tanto para sus usuarios como a sus clientes.

FASE II: ANÁLISIS DE LA EMPRESA

2.1. Descripción de la empresa

La empresa que se consideró para el desarrollo de la aplicación de la Norma ISO 27001: 2013, es la empresa Inmobiliaria, la cual es una empresa dedicada al rubro inmobiliario presente en la ciudad de Lima, con ms de 5 años en el sector inmobiliario.

VISIÓN

Ser la mejor alternativa para quienes quieren la ayuda de un profesional inmobiliario, desde una relación cercana y resolutiva, ofreciendo las propuestas más innovadoras. Que nuestros clientes se sientan plenamente acompañados y asesorados durante todo el proceso de compra de una propiedad, para mejorar su calidad de vida.

MISIÓN

Brindar un servicio de asesoría inmobiliaria personalizada orientada a cuidar el patrimonio de nuestros clientes, con ética y profesionalismo, proporcionando a nuestros clientes asesoría inmobiliaria personalizada e integral, con ética, honestidad y discreción, siempre orientados al servicio personalizado en todas las etapas de nuestra intervención en la venta, compra o alquiler, basados en nuestra experiencia y capacitación en el sector.

VALORES

Valor heroico.

Deber y lealtad.

Honradez y justicia.

Compasión.

Honorabilidad.

2.2. Objetivos del Negocio

El objetivo del negocio como empresa privada del sector inmobiliario es el de dar asesoría inmobiliaria y seguimiento en todo el proceso de compra de la propiedad, desde la promoción hasta el cierre de la operación, enlazados al proyecto de gran importancia.

Actividades Principales.

La empresa inmobiliaria ubicada en la ciudad de Lima, desarrolla entre sus actividades comerciales, inversiones y negocios de promoción inmobiliario, administración de centros comerciales y de

habilitación urbana, así como la venta al por menor de productos relacionados a la inmobiliaria y de otras actividades profesionales.

Los productos inmobiliarios que ofrecen son:

- Habilitación Urbana: Promocionan terrenos para posterior venta de lotes que contarán con los servicios básicos como son agua, luz y desagüe. La característica de este producto se maneja bajo un financiamiento directo, es decir con un abono inicial y el saldo financiado en cuotas con un cierto margen de intereses según la elección del número de cuotas. Este producto está dirigido a los niveles socioeconómicos C y D.

Habilitación para condominios: Terrenos que permiten promocionar la venta de departamentos y desarrollar edificaciones con instalaciones amplias con servicios más completos.

Habilitación para vivienda secundaria: Este tipo de productos se desarrolla en terrenos que tienen como enfoque a la venta de lotes con un área determinada para desarrollar proyectos civiles tales como Casas de campo o casas de playa.

Infraestructura de seguridad de la información:

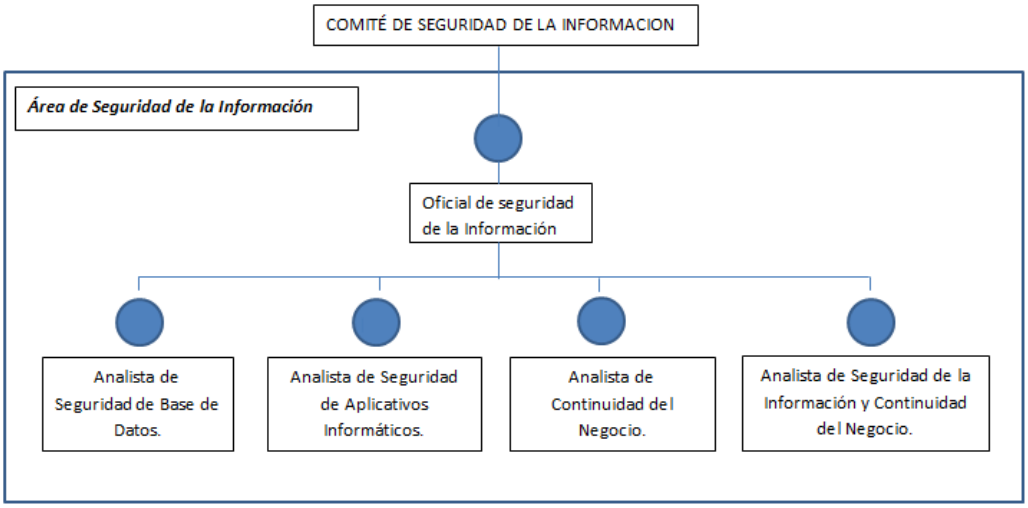


Figura: Cuadro de área de seguridad de la Información

En la figura apreciamos la jerarquía del Comité de Seguridad de la Información, donde es presidida por el departamento oficial de seguridad. La recomendación para este comité es que debe estar apto para revisar el estado de la información de la Institución de manera eficiente contrarrestando percances y situaciones adversas que se puedan presentar.

Alcance:

La Normativa ISO 27001: 2013 se basa en el Sistema de gestión de seguridad de la información que tiene como principal responsable al área comercial y de operaciones, departamento fundamental para el desempeño del negocio; no obstante, su desarrollo es limitado puesto que para una implementación carecería de recursos económicos y humanos por parte de la empresa.

2.3. Definición de la política de Seguridad de la Información.

Se define como un conjunto de reglas y procedimientos de carácter normativo u obligatorio con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información. El estado a través de la Ley 29733 que es la Ley de protección de datos personales establece lineamientos de seguridad estipula la protección de información de datos ya sea en empresas públicas o también privadas, razón por la cual los activos de información de la empresa son protegidos por el estado y garantizado legalmente para la adecuada gestión de la información avalada en este propósito por la Norma ISO 27001:2013. Dichos lineamientos deben ser informados y seguidos por los trabajadores de la organización acatando y ejecutando las políticas vigentes de seguridad.

2.3.1. Objetivos de Políticas de Seguridad de la Información

La política de seguridad de la información busca

- Implementar un marco de referencia con la finalidad de asegurar que los elementos del SGSI sean los necesarios referenciándose como guía y controlando las acciones al momento de la ejecución del proyecto.
- Determinar las reglas de uso de parte del personal con respecto al uso de la información para mejor lineamiento de parte de la gerencia.
- Infundir la concientización del personal con respecto a la importancia de lo que es la seguridad de la información y el grado de responsabilidad que cumplen en el cargo que ocupan o desempeñan.

2.3.2. Alcance de Políticas de Seguridad de la Información

En la Inmobiliaria la preservación y seguridad de una data de información es imprescindible por ello el personal del área comercial y de operaciones se encuentra involucrado dentro del alcance, para tal efecto dichas áreas interactúan con el activo de la información.

2.4. Dominios de la ISO 27001:2013

2.4.1. Política de Seguridad de la Información.

Las políticas de seguridad de la información son 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 empresa como es la información que compete a la compañía.

2.4.2. Organización de la Seguridad de la Información.

En esta parte del 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.

2.4.3. Seguridad en los RR.HH.

Este departamento 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.

2.4.4. Gestión de Activos

En este dominio de la ISO se identifica los activos 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.

2.4.5. Control de Accesos.

Dominio de gran importancia para la empresa por tratarse del control inmediato al acceso de 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.

2.4.6. Criptografía

Se garantiza el uso adecuado de la criptografía con el propósito de proteger la privacidad y confidencialidad de la información manteniendo la integridad de la misma.

2.4.7. Seguridad Física y del entorno

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.

2.4.8. Seguridad en las operaciones

Garantizar que las operaciones 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. Garantizar el óptimo funcionamiento de los Sistemas Operativos

2.4.9. Seguridad en las comunicaciones

Se busca garantizar la protección de los activos de información la red e instalaciones de procesamiento de datos. Proteger la información transferida desde la inmobiliaria con cualquier institución externa.

2.4.10. Adquisición, desarrollo y mantenimiento de sistemas.

Tiene un grado importante entre los dominios ya que de 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.

2.4.11. Relaciones con los proveedores

Proteger los activos de la Empresa 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 los proveedores.

2.4.12. Gestión de los incidentes de seguridad de la información.

Asegurar cualquier intento de vulnerabilidad sobre la seguridad que se encuentren relacionados con los sistemas de información sean reportados de parte de la administración o áreas interesadas con el fin de permitir tomar decisiones correctivas y asertivas sobre el determinado riesgo o evento.

2.4.13. Aspectos de Seguridad de la Información para la gestión de continuidad del negocio.

Se implementará controles que permitan minimizar el riesgo de las interrupciones de actividades funcionales o comerciales críticas para la empresa, 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.

2.4.14. Cumplimiento.

Asegurar el cumplimiento de las obligaciones legales y acuerdos contractuales, derechos de propiedad y privacidad de datos personales relacionados a la seguridad de la información cumpliendo las políticas de seguridad que exige la legislación del estado

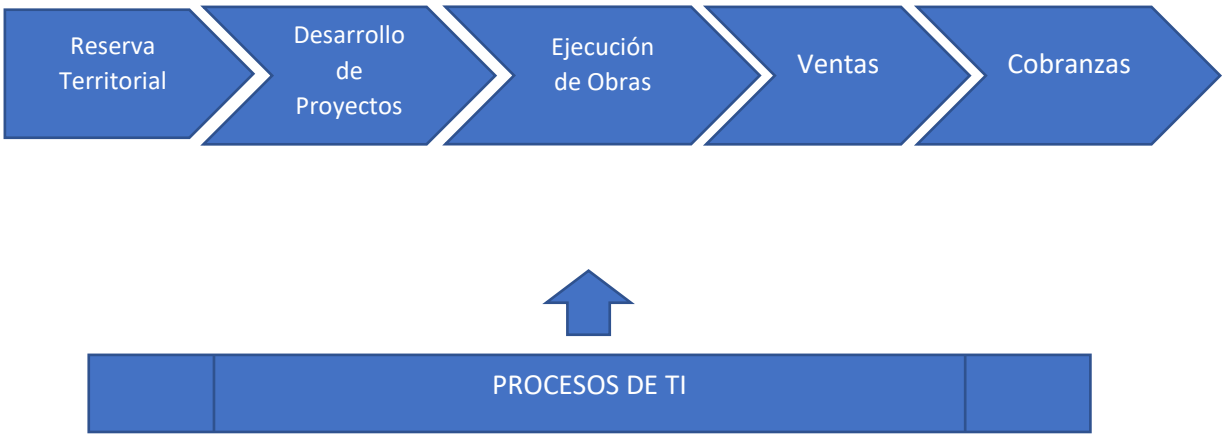
FASE III: ANÀLISIS DE RIESGOS

Se establecen los siguientes procesos que participan dentro del área comercial a fin de determinar el nivel de seguridad de la información con el fin de evitar vulneraciones o exposiciones que puedan alterar su uso apropiado.

Proceso de Área Comercial y de Operaciones	Descripción
Prospectos Clientes	Consulta de prospectos Ingreso de Nuevos prospectos Análisis crediticio del cliente Nueva concesión Análisis de la documentación Establecer acuerdos Financieros con el propietario Firma del contrato (contrato de compra venta-alquiler)
Propiedades	Búsqueda de contactos Realización de tasaciones Seguimiento Negociación Autorización del propietario
Comercialización de propiedades	Publicación de la oferta Visita a las propiedades Seguimiento Negociación

3.1. Procesos de Negocio.

Los principales procesos que involucran al proceso de negocio se registran a continuación para determinar la seguridad de la información y los activos que estos incluyan.



3.1.1. Reserva Territorial.

Es uno de los valores de activos fundamentales de la organización, puesto que es el origen del ciclo del negocio. Dentro de la reserva territorial mencionaremos se suman los subprocesos como son:

- Búsqueda de terreno: La búsqueda del terreno consiste precisamente en ubicar viviendas o algún bien activo con la posibilidad de que el propietario tienda a deshacerse ella, naciendo la posibilidad de un compra o negociación existente.

- Estudio de factibilidad: En el estudio de factibilidad se reúne los requisitos que contribuyan a un alcance donde se registren los pros y contras que puedan favorecer o afectar a la adquisición o desarrollo de un proyecto.

- Negociación del terreno. Ante un interés de una de las parte (tanto comprador como vendedor) nace la posibilidad de una negociación de terreno, donde luego pasa a hacer un

estudio donde se provea de alcances que determinen la fiabilidad del terreno o bien en venta y que no se convierta en una bien que afecte los intereses de la organización.

- Compra de terreno: Es la parte adquisitiva que luego de un estudio sostenible y a su vez de un estudio de factibilidad aprueban los mismos dando paso al contrato de compra de un proyecto o terreno.

- Contrato con opción de compra. Es la parte donde un comprador o cliente muestra el interés por un terreno o bien en venta, pero aún no cumple con todos los requisitos o también el proyecto no se encuentra terminado pero el comprador o cliente desea reservarlo, de esta manera se presenta como opción segura el contrato con opción de compra.

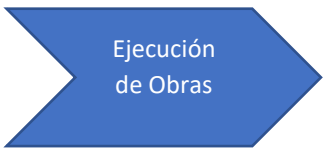
3.1.2. Proceso de Desarrollo de proyectos.

Al igual que el proceso anterior este proceso de Desarrollo de proyectos es de suma importancia. Bajo este proceso encontramos.

Elaboración de Perfil base de proyecto. Básicamente se trata de la elaboración del expediente técnico del perfil base que permitirá la apertura de un expediente para su evaluación de factibilidad y viabilidad del proyecto en mención.

Lanzamiento del proyecto. En esta parte se delimita los lineamientos, condiciones y alcances que permitirán el inicio y promoción de un proyecto inmobiliario. Técnicamente es la oferta que se promocionará al público a través de la venta de viviendas y/o departamentos consistentes en un proyecto inmobiliario.

3.1.3. Proceso de ejecución de obras



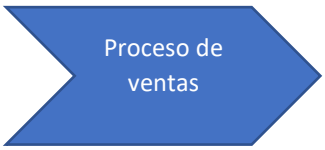
Se pone en marcha los estudios realizados, ya sean factibilidad, viabilidad, entre otros.

Evaluación y aprobación de valorizaciones. El principal objetivo es el de evaluar las valorizaciones y costos presentados para la ejecución de obra, dependiendo de ello se aprobará la valorización de acuerdo al avance del proyecto presentado por el supervisor de la obra a cargo del contratista.

Culminación de obra. Se describen y definen las actividades y el cumplimento de acuerdos establecidos para el desarrollo del proyecto necesarios para la culminación de las obras realizadas en el desarrollo del proyecto,

Carga de plano. Es el registro de los planos finales ejecutados y realizados en el desarrollo del proyecto, donde se establecerá el cumplimiento de los plazos establecidos para el desarrollo del mismo.

3.1.4. Proceso de Ventas

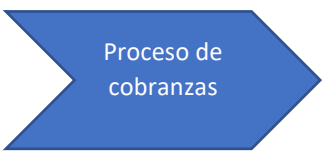


Es la parte administrativa donde ya se lleva a cabo la promoción y venta de terrenos, lotes o inmuebles que estén disponibles para la reserva o para su venta

Prospección de Clientes. Se determina las actividades para promocionar los prospectos inmobiliarios a través de un catálogo que permitirá al cliente según el interés que demuestre, la posibilidad de compra o separación del mismo, ya sea con el compromiso de opción de compra o de compra directa.

Venta de terrenos o inmuebles. Se determina las actividades para la venta o separación de lotes, departamentos o viviendas, donde ante un posible interés del cliente o comprador se le hace llegar la información del inmueble para su evaluación y posible opción de compra.

3.1.5. Proceso de cobranzas



Este proceso determinará la modalidad de pago donde el comprador podrá elegir de acuerdo a sus posibilidades y a través de una evaluación crediticia.

Administración de letras. Esta modalidad se establece a través del pago de cuotas donde se dividirá proporcionalmente el valor de la propiedad y se aplicará el interés en base al número de cuotas que pueda elegir el comprador en un plazo determinado entre la inmobiliaria y el comprador.

Financiamiento Esta modalidad se aplica a través del financiamiento con una entidad bancaria sujeto a evaluación crediticia, quien determinará la manera de pago según sus posibilidades

Compra directa. Es la modalidad conocida como pago en efectivo o a través del pago electrónico donde se abonará directamente a la cuenta de la inmobiliaria con los gastos de gestión y transacción que implique la venta del inmueble, por supuesto previo acuerdo entre las partes participantes.

3.2. Metodología de valorización de activos

Teóricamente los activos de una organización son aquellos que poseen valor y cumplen algún tipo de utilidad o servicio dentro de la empresa, éstos deben de registrarse a través de un inventario para su debido conocimiento y resguardo.

La Norma ISO 27001 precisamente establece que, determinar la gestión de riesgos de la inmobiliaria, primero se debe de identificar los activos de información ya sea tangibles o intangibles que serán necesarios en la participación de la empresa.

3.2.1 Inventario de Activos

El inventario de los activos permitirá la identificación de los activos de información que son indispensables para el área comercial y de operaciones, esta información ayudará a conocer las herramientas, encargados, categorías, responsables del ciclo de vida de la seguridad de la información de la inmobiliaria.

Tabla: *Inventario de activos*

Ítem	Nombre	Descripción	Categoría	Ubicación	Propietario o departamento
01	Microsoft Professional 2010	Microsoft Word, Excel, Power Point, Access.	Programas	Sistema de ordenador	Área de Soporte y departamento de TI
02	Microsoft Professional 2013	Microsoft Word, Excel, Power Point, Access.	Programas	Sistema de ordenador	Área de Soporte y departamento de TI
03	Acrobat Reader X	Adobe PDF	Programas	Sistema de ordenador	Área de Soporte y departamento de TI
04	Antivirus Avast	Avast Premium	Programas	Servidor	Área de Soporte y departamento de TI
05	Sistemas Operativos	Windows 7 Professional	SO	Servidor	Área de Soporte y departamento de TI
06	Dispositivos de Almacenamiento	duros externos, usb, Discos.	Dispositivos	Operaciones y área comercial	Operaciones y área comercial y Logística.
07	Equipos de Usuario	Pc escritorio de usuarios, Impresoras e impresora multifuncional, Copiadoras.	Hardware	Operaciones y área comercial	Área de Soporte y departamento de TI
08	Clientes	Datos de clientes	Datos	Servidor	Operaciones y área comercial

09	Documentos cliente	Registro y expediente de clientes (contratos, propiedades)	Documentación	Operaciones y área comercial	Departamento área Comercial
10	Trabajador	Personal administrativo	Personal	Operaciones y área comercial	RR. HH
11	Correo Electrónico	Correo Electrónico	Herramienta	Servidor	Área de Soporte y departamento de TI
12	Servicios de consumo	Internet, Energía Eléctrica, Cámaras de Videos	Servicios	Operaciones	Departamento de Contabilidad

3.2.2. Valorización de Activos

La valorización de los activos se realizará según la escala de puntuación:

La valorización total será la suma aritmética de los 3 valores.

Tabla: *Valorización de activos*

Criterio	Descripción	Escala de puntuación
Disponibilidad	El activo de información debe estar disponible al menos una cuarta parte de su disponibilidad, por ello no existe riesgo operacional o por alguna razón haya sido eliminado	1
	El activo de información debe estar disponible un 50% de su disponibilidad, en menor porcentaje de disponibilidad podría afectar levemente los intereses de la organización	2
	El activo de información debe estar disponible un porcentaje no menor de 75% de su disponibilidad,	

	en menor porcentaje de disponibilidad podría ocasionar daños considerables en la organización	3
	El activo de información debe estar totalmente disponible, caso contrario podría ocasionar daños catastróficos e irreparables en la inmobiliaria causando pérdidas financieras.	4
INTEGRIDAD	La integridad del activo de información debe ser correcta y estar completa una cuarta parte de su integridad, no hay riesgo ante pérdidas financieras u operacional que se puedan presentar.	1
	La integridad del activo de información debe estar completa al menos un 50% de su integridad, caso contrario los daños que se puedan presentar son leves ante pérdidas financieras u operacionales.	2
	La integridad del activo de información debe estar completa al menos un 75% de su integridad, caso contrario los daños que se puedan presentar son considerables ante pérdidas financieras u operacionales y podrían afectar económicamente a la empresa.	3
	La integridad del activo de información debe estar completa al menos un 100% de su integridad, caso contrario los daños que se puedan presentar son irreparables y peligrosos para los intereses de la inmobiliaria y podrían afectar económicamente a la empresa.	4
Confidencialidad	El activo de información puede ser divulgada o de conocimiento público dicha información no afecta los intereses de la empresa	1
	El activo de información puede ser divulgada sólo si es dirigida bajo ciertas condiciones o restricciones	2
	El activo de información no puede ser divulgada por tratarse de información personal que está reglamentada, su publicación podría involucrar riesgos y problemas para la empresa	3

	El activo de información es de carácter privado y su publicación podría causar daños irreparables para la inmobiliaria e involucrar problemas legales para la empresa.	4

Tabla: *Valoración de activos*

Ítem	Activos	Confidencial	Integridad	Disponibilidad	Total
01	Programas	3	3	4	10
02	Sistemas Operativos	3	3	5	11
03	Dispositivos de Almacenamiento.	4	4	3	11
04	Equipos de Usuario	4	3	5	12
05	Clientes	4	4	5	13
06	Trabajador	3	4	5	12
07	Documentos – Cliente	5	5	5	15
08	Correo Electrónico	4	3	4	11
09	Servicios	3	3	3	9

Tabla: *Descriptiva de tipos de activos*

.	Descripción
Datos	Es la información que se genera, modifica, resguarda, utiliza o destruye dentro de la inmobiliaria
Aplicaciones	Son programas que se emplea en la gestión de la seguridad de la información
Personal	Es el personal operativo que trabaja dentro de la empresa o también los clientes que figuran en la base de datos de la inmobiliaria
Servicios	Están incluidos los servicios básicos además de servicios de internet, de seguridad y video vigilancia
Tecnología	Dispositivos que se utiliza en la gestión de la información y comunicación.

3.2.3. Listado de Valoración de activos de Información

Item	Tipo	Nombre	Descripción	Propietario	Ubicación	Proceso	Confidencial	Integridad	Disponibilidad	Total
01	Datos	Informe búsqueda de terreno	Documento con una lista detallada de las zonas de terreno de interés	Gerente de Reserva territorial	Físico/ Electrónico	Reserva Territorial	3	3	4	10
02	Datos	Informe de zonas de terreno	Documento con una lista detallada de las zonas de terreno con posibilidad de compra, además contiene información de los propietarios	Gerente de Reserva territorial	Físico/ Electrónico	Reserva Territorial	3	3	5	11
03	Datos	Planos de terreno	Plano de levantamiento topográfico del terreno	Gerente de Reserva territorial	Físico/ Electrónico	Reserva Territorial	4	4	3	11
04	Datos	Informe Catastral	Informe descriptivo del plano donde está incluido los planos	Gerente de Reserva territorial	Físico/ Electrónico	Reserva Territorial	4	3	5	12

05	Datos	Expediente del proyecto	Registro de documentación con fines de evaluación para definir la factibilidad del proyecto	Gestor de reserva territorial	Físico/ Electrónico	Reserva Territorial	4	4	5	13
06	Personal	Comité de pre-proyectos	junta de ejecutivos que tiene como objetivo evaluar la viabilidad de nuevos proyectos inmobiliarios	Comité de nuevos proyectos	Físico/ Digital	Reserva Territorial	|1	4	5	12
07	Datos	Documentos – Cliente	Documento que sustenta la no ejecución de compra de un terreno de interés	Gestor de reserva territorial	Digital/ Físico	Reserva Territorial	5	5	5	15
08	Datos	Contrato de compra y venta	Documentos con las cláusulas de compra de un terreno	Representante legal	Digital/ Físico	Reserva Territorial	4	3	4	11
09	Datos	Perfil del proyecto	Documentación de reserva territorial	Gestor de reserva territorial	Digital /Físico	Reserva Territorial				
10	Datos	catálogo de precios	Documento que registra los precios, áreas y alcances de los terrenos de interés.	Gestor de reserva territorial	Físico/ Electrónico	Reserva Territorial				
11	Datos	Precontrato de compra	Contrato con cláusulas que registran la posibilidad de compra de terreno	Representante Legal	Digital/ Físico	Reserva Territorial				
12	Datos	Perfil Base	Registro que está supeditado a evaluación que determina la factibilidad de un proyecto.	Coordinador de proyectos	Digital/ Físico	Desarrollo de proyectos				

13	Datos	Informe de plano de diseño	Información topográfica de terrenos evaluados para venta	Desarrollo de proyectos	Digital/ Físico	Desarrollo de proyectos				
14	Datos	Informe de valorización	Documento que sirve al contratista para el avance de un proyecto	Supervisor de obra	Físico/ Digital	Ejecución de obras				
15	Datos	Informe de alcance de servicios	Documento que se genera a partir de la aprobación del documento de valorización.	Analista de costos	Físico/ Digital	Ejecución de obra				
16	Aplicaciones	Sistema PSAD56	Sistema de información Catastral	Jefe legal territorial	Digital/ Electrónico	Reserva territorial				
17	Aplicaciones	Microsoft Office 2013	Programa de edición de lectura para editar documentos, gráficos, registros, etc.	Soporte de TI	Electrónico	Todos los procesos				
18	Aplicaciones	Acrobat Adobe Reader	Programa que establece el formato PDF para presentación de documentos en general	Soporte de TI	Electrónico	Todos los procesos				
19	Tecnología	Servidor de correo	Servicio con conexión a internet que se utiliza para el medio electrónico con fines de envíos de mensajes en correo y archivos adjuntos	Jefe de TI	Electrónico	Todos los procesos				
20	Servicios	Servicios básicos	Servicio de consumo, internet, energía, cámaras de vigilancia.	Área de operaciones comerciales	Electrónico	Todos los procesos				

4. Metodología de Riesgos.

4.1. Identificación de amenazas

Teóricamente una amenaza es cualquier objeto, acción o acontecimiento que pueda atentar contra la seguridad y el resguardo de la información. Por lo tanto, se identificará las amenazas que de una u otra manera pueden alterar el desenvolvimiento o función de los activos de información.

Podemos determinar los siguientes tipos de amenazas.

- Operacionales. Esta amenaza se puede presentar a través de crisis financiera, perdida de información, fallas en dispositivos u ordenadores.
- Naturales. Se presenta a través de desastres naturales como pueden ser, terremotos, tsunamis, maremotos, tornados, incendios, etc.
- Instalaciones. Se presentan por desperfectos o incidentes como pueden ser explosión, falta de energía, fallas mecánicas, etc.
- Tecnológicas. Vulneración de datos, desperfecto de software, desperfecto de hardware, averías técnicas, etc.
- Humanas. Los más comunes son las epidemias, materiales corrosivos, perdida de información, etc.
- Sociales. También se manifiesta a causa del hombre, a través de protestas, huelgas, manifestaciones, terrorismo.

4.1. 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 acarrean 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*

ASPECTOS DEL RIESGO		
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 mas horas de trabajo y recursos, tal es así que esto ayudaría a intentar cubrir el cumplimiento de las actividades de los procesos.	5-6
	La importancia del impacto es mayor por tal motivo las horas se	

Crítico	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 va 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

4.2. 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

Indicadores

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

Matriz Cualitativa para la evaluación de riesgos

4.3. Valoración de riesgo por activo

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

Programas Informáticos:

Tabla: *Valorización de activo de programas informáticos*

	Amenaza	Impacto	Nivel de Amenazas	Probabilidad	Nivel de Riesgo
Programas Informáticos	Operacionales	5	1	3	15
	Naturales	4	1	1	4
	Instalaciones	6	2	2	24
	Tecnológicas	7	2	4	56
	Humanas	6	2	3	36
	Sociales	3	1	1	3
	Total	31	9	14	VMR= 56

Sistemas operativos:

Tabla: *Valorización de activo de sistemas operativos*

	Amenaza	Impacto	Nivel de Amenazas	Probabilidad	Nivel de Riesgo
Sistemas Operativos	Operacionales	6	2	2	24
	Naturales	5	1	2	10
	Instalaciones	6	2	3	36
	Tecnológicas	7	2	3	42
	Humanas	8	2	2	32
	Sociales	6	1	1	6
	Total	38	10	13	VMR = 42

Dispositivos de almacenamiento:

Tabla: *Valorización de activo de dispositivos de almacenamiento*

	Amenaza	Impacto	Nivel de Amenazas	Probabilidad	Nivel de Riesgo
Dispositivos de Almacenamiento	Operacionales	6	2	3	36
	Naturales	4	1	2	8
	Instalaciones	4	2	2	16
	Tecnológicas	6	3	3	54
	Humanas	5	2	2	20
	Sociales	4	1	1	4
	Total	29	11	13	VMR= 54

Equipos de usuario:

Tabla: *Valorización de activo de equipos de usuario*

	Amenaza	Impacto	Nivel de amenaza	Probabilidad	Nivel de Riesgo
Equipos de usuario	Operacionales	7	3	3	63
	Naturales	5	2	2	20
	Instalaciones	5	2	4	40
	Tecnológicas	7	3	3	63
	Humanas	6	2	2	24
	Sociales	4	1	2	8
	Total	34	13	16	VMR= 63

Clientes:

Tabla: *Valorización de activo de clientes*

	Amenaza	Impacto	Nivel de Amenazas	Probabilidad	Nivel de Riesgo
Clientes	Operacionales	8	2	3	48
	Naturales	4	2	2	16
	Instalaciones	4	2	2	16
	Tecnológicas	5	3	3	45
	Humanas	6	2	3	36
	Sociales	3	2	3	18
	Total	30	13	16	VMR= 48

Trabajador:

Tabla: *Valorización de activo de trabajador*

	Amenaza	Impacto	Nivel de Amenazas	Probabilidad	Nivel de Riesgo
Trabajador	Operacionales	6	2	3	36
	Naturales	4	1	2	8
	Instalaciones	4	1	1	4
	Tecnológicas	6	2	3	36
	Humanas	6	2	4	48
	Sociales	4	2	2	16
	Total	30	10	15	VMR=48

Documentos cliente:

Tabla: *Valorización de activo de documentos cliente*

	Amenaza	Impacto	Nivel de Amenazas	Probabilidad	Nivel de Riesgo
Documentos cliente	Operacionales	8	2	3	48
	Naturales	4	2	2	16
	Instalaciones	4	2	2	16
	Tecnológicas	6	2	3	36
	Humanas	6	3	3	54
	Sociales	4	2	2	16
	Total	32	13	15	VMR=54

Correo Electrónico:

Tabla: *Valorización de activo de correo electrónico*

	Amenaza	Impacto	Nivel de Amenazas	Probabilidad	Nivel de Riesgo
Correo Electrónico	Operacionales	7	2	3	42
	Naturales	4	2	2	16
	Instalaciones	6	2	3	36
	Tecnológicas	8	2	3	48
	Humanas	6	2	2	24
	Sociales	4	2	2	16
	Total	35	12	15	VMR= 48

Servicios:

	Amenaza	Impacto	Nivel de Amenazas	Probabilidad	Nivel de Riesgo
Servicios	Operacionales	6	2	2	24
	Naturales	6	3	2	36
	Instalaciones	7	2	2	42
	Tecnológicas	6	2	3	36
	Humanas	5	2	3	30
	Sociales	4	2	3	24
	Total	34	13	15	VMR= 42

4.1. Tratamiento del riesgo

Para el tratamiento del riesgo se establecerá un valor numérico que permitirá delimitar e identificar los activos que están expuestos a riesgos. La cifra límite será 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 fijaremos el valor máximo del riesgo con las iniciales de VMR representado en el gráfico de cada tabla. Asimismo, se aplicarán el control establecido por la ISO 27001para el presente proyecto.

Ítem	Activos	Amenaza	Nivel de amenaza	Nivel de Riesgo	Total
01	Programas Informáticos	Tecnológica	2	56	10
02	Sistemas Operativos	Tecnológica	2	42	11
03	Dispositivos de Almacenamiento.	Tecnológica	3	54	11
04	Equipos de Usuario	Operacional/ Tecnológica	3	63	12
05	Clientes	Operacional	2	48	13

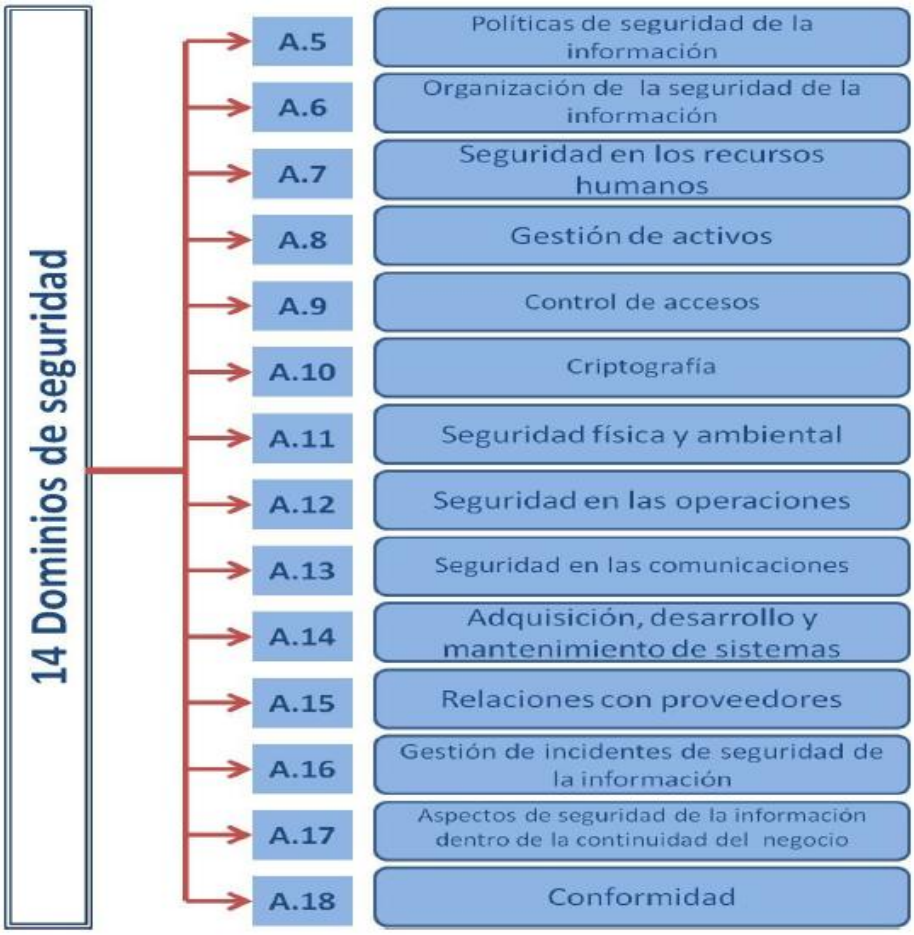
06	Trabajador	Humanas	2	48	12
07	Documentos – Cliente	Humanas	3	54	15
08	Correo Electrónico	Tecnológicas	2	48	11
09	Servicios	Instalaciones	2	42	9

FASE IV. DECLARACIÓN DE APLICABILIDAD

Luego de haber identificado los controles a través de un análisis exhaustivo y al haber encontrado riesgos de nivel superior a lo permitido para la inmobiliaria, en esta cuarta fase se determinarán cual de los controles serán aplicables según el contexto de la empresa. A continuación, se presentan los controles aplicados dentro del sistema de gestión.

4.1 Controles aplicados

Se aplicarán los controles implementados en la metodología de la norma ISO 27001 con el fin de salvaguardar los activos de la empresa.



DECLARACIÓN DE APLICABILIDAD					
ISO 27001 – Controles de seguridad			Es aplicable a la organización		Justificación de aplicabilidad
A.5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN					
Cláusula	Sección	Objetivo de control	¿Se aplica?		Justificación
A.5.1. Dirección de la Alta Gerencia para la seguridad de la información	5.1.1.	Políticas de seguridad de la información	Aplicable	✓	Se tendría que establecer de manera obligatoria una política de seguridad de la información. Esto permitirá la implantación de una gestión de seguridad de la información
	5.1.2.	Revisión de las Políticas de la Seguridad de la Información	Aplicable	✓	No se encontró ninguna política de seguridad en la empresa que se pueda evaluar o podido ser aprobada, por tanto la inmediata política de seguridad que se pueda implantar tendrá que ser observada y revisada antes de ser impuesta y aprobada
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					
A.6.1. Organización Interna	6.1.1.	Roles y Responsabilidad de Seguridad de la información	Aplicable	✓	No se encuentran roles definidos en temas de seguridad de la información, indirectamente los responsables y obligados son el jefe de soporte y de TI. Razón por la cual debe de asignarse de inmediato a fin de sobrecargar las actividades
	6.1.2.	Segregación de deberes	Aplicable	✓	Ante la saturación de actividades que demanda gran responsabilidad del área de soporte y de TI es necesario segregar y aliviar la carga de actividades de los mencionados a fin de que cumplan sus funciones con normalidad.
	6.1.3.	Contacto con autoridades	No aplica	O	A la actualidad no existe un órgano competente que exija la implementación de un SGSI a la inmobiliaria

	6.1.4.	Contacto con grupo de interés especial	No aplica	O	A la actualidad no existe un órgano competente que exija la implementación de un SGSI a la inmobiliaria
	6.1.5.	Seguridad de la información en la gestión	Aplicable	✓	En la inmobiliaria no existe una normativa o metodología de riesgo definida a in de realizar un estudio de riesgos de seguridad en la elaboración de los proyectos. Por tanto, es vital añadir la seguridad de la información en una gestión de los proyectos.
A.6.2. Dispositivos móviles y teletrabajo	6.2.1.	Política de dispositivos móviles	Aplicable	✓	No existe documentación sobre el uso adecuado o determinado de los dispositivos móviles dentro de la empresa, es por ello que se necesita de una documentación que autorice el buen uso de la misma.
	6.2.2.	Teletrabajo	Aplicable	✓	Actualmente existe la modalidad del teletrabajo en esos últimos tiempos, razón por la cual se implementaría una política de seguridad que determine el alcance y las responsabilidades que esta demande. A través del uso de la tecnología se lleva a cabo la modalidad del teletrabajo en la inmobiliaria.
A7. SEGURIDAD EN LOS RECURSOS HUMANOS					
A.7.1. Antes de asumir el empleo	7.1.1.	Verificación de antecedentes	Aplicable	✓	Se revisan los antecedentes penales y policiales de cada postulante a un puesto laboral, Asimismo se tendría que limitar los alcances de cada puesto con mayor precisión.
	7.1.2.	Términos y condiciones del empleo	Aplicable	✓	A través de un contrato elaborado ´por el área de RR.HH. donde se precisan las cláusulas del contrato de trabajo, sin embargo, no se precisa los datos de confidencialidad debiéndose proteger los datos personales de cada empleado o trabajador.

A.7.2. Durante la ejecución del empleo	7.2.1.	Responsabilidades de alta gerencia	Aplicable	✓	La parte de gerencia debería establecer responsabilidades a través de políticas de seguridad a fin de preservar los procedimientos y resguardar la información de la inmobiliaria.
	7.2.2.	Conciencia, educación y formación en S.I.	Aplicable	✓	En la organización no es prescindible la cultura organizacional por tal motivo no se toma muy en cuenta la seguridad de la información. Por tal razón se debería a través de capacitaciones y entrenamientos regular la concientización de la importancia que cumple cada integrante de la inmobiliaria.
	7.2.3.	Proceso Disciplinario	Aplicable	✓	Se deberá establecer sanciones y amonestaciones para el personal que incumpla los reglamentos de seguridad de la información o que irrumpan la política aprobada.
A.7.3. Terminación y cambio de empleo	7.3.1.	Terminación o cambio de responsabilidades de empleo	Aplicable	✓	Después del tiempo de servicio o tiempo de contrato del trabajador, debería extenderse las responsabilidades de la seguridad de la información a fin de resguardas los datos e información personal.
A.8. GESTION DE ACTIVOS					
A.8.1. Responsabilidad de los activos	8.1.1.	Inventario de activos	Aplicable	✓	Se desarrollará una lista de actividades de los activos de información de la organización, que permitirá un control adecuado. Esto estará acompañado de un inventario de activos que posibilitará la correcta unción de los procesos en cuanto al alcance.
	8.1.2.	Propiedad de activos	Aplicable	✓	A través de un inventario se consignará las propiedades y responsabilidad de cada integrante a cargo de los activos de la organización. Todo esto es con el fin de implementar un Sistema de Gestión de Seguridad de la Información íntegro.

	8.1.3.	Uso aceptable de los activos	Aplicable	✓	Para el correcto uso de los activos en la SGSI se debe de elaborar un inventario que permita el control adecuado de los activos de la organización.
	8.1.4.	Devolución de activos	Aplicable	✓	Es necesario elaborar un procedimiento que permita la devolución de algún activo de la empresa que posea algún colaborador cuando finiquite su contrato con la inmobiliaria.
A.8.2. Clasificación de la Información	8.2.1.	Clasificación de la información	Aplicable	✓	Se realizará una clasificación de acuerdo al valor del activo, entre otros criterios para la organización
	8.2.2.	Etiquetado de la información	Aplicable	✓	Se debe definir un esquema que permita la clasificación acorde con su valor para la inmobiliaria
	8.2.3.	Manejo de activos	Aplicable	✓	En la actualidad no se cuenta con un procedimiento para la clasificación de los activos, por lo que se incorporará en el SGSI que será evaluado para su aprobación
8.3. Manejo de Medios	8.3.1.	Gestión de medios removibles	Aplicable	✓	Las herramientas de trabajo para la óptima gestión necesitan de la implementación de una criptografía de seguridad que permita asegurar el uso de los datos e información que pueda llevar consigo el personal.
	8.3.2.	Eliminación de medios	Aplicable	✓	El uso de herramientas informáticas de información es necesario para la oferta de productos de la inmobiliaria por tal motivo se debe de comprobar el uso apropiado y definitivo de la información que ya no se requiera a fin de que no esté expuesta.
	8.3.3.	Transporte de medios físicos	Aplicable	✓	Los medios o herramientas informáticas deben de protegerse para ello se debe de registrar a través de un documento antes de la salida de cada medio o fuente de información y contar con el uso adecuado y evitar la exposición innecesaria.

A.9. CONTROL DE ACCESO					
A.9.1. Requerimientos de negocio para el control de acceso	9.1.1.	Política de control de acceso	Aplicable	✓	NO existe políticas de autorización para el la restricción o prohibición de algún acceso
	9.1.2.	Política en el uso de servicios de red	Aplicable	✓	NO existe políticas de autorización para el cumplimiento de las políticas del acceso a los servicios de red.
9.2. Gestión de accesos de usuario	9.2.1.	Registro y baja de usuario	Aplicable	✓	No existe un procedimiento a cumplir para el registro de baja de algún usuario, por lo que la información quedaría expuesta a riesgos de seguridad.
	9.2.2.	Abastecimiento de usuarios de acceso	Aplicable	✓	No existe un procedimiento que permita el abastecimiento de usuarios de acceso.
	9.2.3.	Gestión de accesos privilegiados	Aplicable	✓	Es necesaria una política que establezca los permisos que brinden los responsables de cada departamento a los colaboradores para cumplir funciones que estos demanden en favor de la organización.
	9.2.4.	Gestión de información, autenticación secreta de usuarios	Aplicable	✓	No existe procedimientos para la gestión y autenticación de los usuarios
	9.2.5.	Revisión de derechos de acceso de usuarios	Aplicable	✓	Es necesario la implementación de una política de seguridad de derecho de acceso a los usuarios a fin de evitar que cualquier tercero pueda tener acceso a la información de la organización.
	9.2.6.	Eliminación o ajuste de derechos de acceso	Aplicable	✓	Para la eliminación de acceso de algún usuario, primero se tendría que implantar una documentación de permisos y accesos, por ello es necesario la implantación de un SGSI donde se detalle estos accesos y sus restricciones hasta el final de la información que consiste en destruir el mismo.

9.3. Responsabilidades del usuario	9.3.1.	Uso de información de autenticación secreta	Aplicable	✓	No se aprecia una cultura de seguridad responsable del colaborador por lo tanto la información se encuentra vulnerable por lo tanto tiene que instalarse una cultura de concientización a fin de que cada trabajador se comprometa y de buen uso del usuario y clave que manejan.
9.4. Control de acceso de sistemas y aplicaciones	9.4.1.	Restricción de acceso a la información	Aplicable	✓	La poca comunicación que se da entre el área de TI y los colaboradores dificulta la ejecución de los procesos, por ello es necesario que se establezcan controles de acceso.
	9.4.2.	Procedimiento de conexión segura	aplicable	✓	Se deberá implementar unos protocolos para la continuidad del¿ la conexión y asegurar el acceso a los sistemas y aplicaciones.
	9.4.3.	Sistema de gestión de contraseñas	Aplicable	✓	Esta política de seguridad deberá ser actualizada a fin de renovar las claves de usuarios donde se establezcan a través de un documento la responsabilidad en no divulgar ni entregar las claves personales de los usuarios de la organización.
	9.4.4.	Uso de programas y utilidades privilegiadas	Aplicable	✓	Es necesario la elaboración de un documento donde se establezca los permisos correspondientes que cada jefe debe de conceder a los colaboradores para cumplir funciones.
	9.4.5.	Control de acceso al código fuente del programa	Aplicable	✓	A falta de un protocolo de seguridad de asignación de código fuente, ésta se ha visto expuesta a vulnerabilidades por lo tanto es necesaria su implementación.
A.10. CRIPTOGRAFIA					
A.10.1. Controles Criptográficos	10.1.1.	Políticas en el uso de controles criptográficos	No aplicable	O	En el alcance realizado para el Sistema de Gestión de Seguridad de la Información no se incluye dicha cláusula
	10.1.2.	Gestión de claves	No aplicable	O	En el alcance realizado para el Sistema de Gestión de Seguridad de la Información no se incluye dicha cláusula

A.11. SEGURIDAD FÍSICA Y DEL ENTORNO					
A.11.1. Áreas Seguras	11.1.1	Perímetro de seguridad físico	Aplicable	✓	Es necesario la instalación de políticas de seguridad con respecto a la implantación de casetas de los puntos de venta de las unidades de viviendas
	11.1.2.	Controles físicos de entrada	Aplicable	✓	Instalar políticas de seguridad con respecto al ingreso de los clientes en las unidades de viviendas
	11.1.3.	Seguridad de oficinas, habitaciones y facilidades	Aplicable	✓	Instalar de políticas de seguridad con respecto a la seguridad de las oficinas y departamentos dentro de las unidades de viviendas con el fin de resguardar la integridad y la información de los clientes.
	11.1.4.	Protección contra amenazas externas y del ambiente	Aplicable	✓	Se deberá establecer lineamientos para el resguardo íntegro frente a desastres que presente la naturaleza.
	11.1.5.	Trabajo en áreas seguras	Aplicable	✓	Instalar de lineamientos de seguridad con respecto al cumplimiento de funciones en las áreas que tengan un grado de riesgo y en general en las unidades de viviendas.
	11.1.6.	Áreas de entrega y carga	Aplicable	✓	Instalar de lineamientos de seguridad con respecto al cumplimiento de funciones en las áreas de entrega y cargo que tengan un grado de riesgo.
11.2. Equipo	11.2.1.	Instalación y protección de equipo	No aplica	O	Existen normas y directrices externas que mantienen una infraestructura segura.
	11.2.2.	Servicios de soporte	Aplicable	✓	Se establecen procedimientos que permitirán entablar el soporte a las áreas solicitantes
	11.2.3.	Seguridad en el cableado	No aplica	O	Existen normas y directrices externas que mantienen una infraestructura de conexiones red segura.
	11.2.4.	Mantenimiento de equipos	Aplica	✓	Establecer protocolos para un mantenimiento preventivo de los equipos de servidores.

	11.2.5.	Retiro de activos	No aplica	✓	Establecer una Política de seguridad que restringe el retiro de los equipos y activos de la empresa.
	11.2.6.	Seguridad del equipo	No aplica	✓	Existe lineamientos que prohíbe que los equipo se sometan a candados con fines de seguridad
	11.2.7.	Eliminación segura o re-uso del equipo	Aplicable	✓	Se establecerá lineamientos que determine el modo de eliminación de los equipos den desuso para evitar la divulgación de la información.
	11.2.8.	Equipo de usuario desatendido	No aplica	O	Se establecerá lineamientos que determine la recuperación de equipos que se encuentren en desuso por algún usuario que no esté en función para evitar la divulgación de la información.
	11.2.9.	Política de escritorio limpio y pantalla limpia	Aplica	✓	Se establece el procedimiento que permita mantener un escritorio y pantalla sin impedimento visual y que no esté ajena a la organización.
A.12. SEGURIDAD EN LAS OPERACIONES					
A.12.1. Procedimientos Operacionales y Responsabilidades	12.1.1.	Documentación de procedimientos operacionales	Aplicable	✓	Garantizar a través de lineamientos correspondientes la disponibilidad de la información, esto implica el mantenimiento de los servidores.
	12.1.2.	Gestión de cambios	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información
	12.1.3.	Gestión de la capacidad	Aplicable	✓	Garantizar a través de lineamientos correspondientes la capacidad y la disponibilidad de la información ´para una adecuada gestión.
	12.1.4.	Separación de los ambientes de desarrollo, pruebas y operación	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información.

A.12.2. Protección de Software Malicioso	12.2.1.	Controles contra software malicioso	Aplicable	✓	Implantar lineamientos de seguridad de correos electrónicos a fin de evitar el tráfico de datos por medio de archivos corruptos o la delincuencia informática
A.12.3. Respaldo	12.3.1.	Respaldo de Información	Aplicable	✓	Establecer procedimientos de resguardo de información a través de los backups para evitar la pérdida de información a través de incidentes informáticos.
A.12.4. Registro y monitoreo	12.4.1.	Registro de eventos	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información
	12.4.2.	Protección de registros de información	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información
	12.4.3.	Registro de administrador y operador	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información
	12.4.4.	Sincronización de relojes	Aplicable	✓	Se tendrá que establecer lineamientos para el correcto funcionamiento del reloj debido a la sincronización de servidores.
A.12.5. Control de Software Operacional	12.5.1.	Instalación de software en sistemas operacionales	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información
A.12.6. Gestión de Vulnerabilidades Técnicas	12.6.1.	Gestión de vulnerabilidades técnicas	Aplicable	✓	Establecer procedimientos por un tema de seguridad para proteger los datos personales de la organización.
	12.6.2.	Restricciones en la instalación de software	No aplicable	O	Cada usuario tiene el acceso a través de su usuario y clave por tal razón las aplicaciones y sus restricciones va a depender del personal autorizado para el uso del software y sus instalaciones.
A.12.7.	12.7.1.	Controles de auditoría de sistemas de información.	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información

A.13 SEGURIDAD EN LAS COMUNICACIONES					
A.13.1. Gestión de Seguridad en Red	13.1.1.	Controles de red	Aplicable	✓	Establecer políticas de control en la red a fin de evitar el tráfico, la navegación lenta, y el robo informático.
	13.1.2.	Seguridad de los servidores en red	Aplicable	✓	Establecer políticas de seguridad a fin de evitar el robo informático, resguardando la información de los servidores y resguardar la información
	13.1.3.	Segregación en redes	Aplicable	✓	Es necesario limitar servicios innecesarios en las redes a fin de evitar el tráfico y la navegación lenta.
A.13.2. Transferencia de información	13.2.1.	Políticas y procedimientos para la seguridad de la información	Aplicable	✓	Establecer lineamientos y procedimientos de seguridad sobre la transferencia de información, donde sea posible hacer un seguimiento de los procesos del sistema.
	13.2.2.	Acuerdos en la transferencia de información	Aplicable	✓	Establecer acuerdos de transferencia de información, donde sea posible hacer un seguimiento de los procesos del sistema.
	13.2.3.	Mensajería electrónica	Aplicable	✓	Establecer lineamientos y procedimientos de seguridad sobre el uso de mensajería electrónica, donde sea posible hacer un seguimiento de los procesos del sistema.
	13.2.4	Acuerdos de confidencialidad o no-revelación	No aplicable	O	Se establecerá políticas de confidencialidad para resguardar la información de la empresa.
A.14.ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO					
A.14.1. Análisis y especificación de requerimientos de seguridad	14.1.1.	Análisis y especificación de requerimientos de seguridad	Aplicable	✓	Se debe garantizar el buen funcionamiento a través de lineamientos establecidos a fin de evitar la intrusión de programas intrusos o virus informáticos.
	14.1.2.	Aseguramiento de	Aplicable	✓	Se debe garantizar el buen funcionamiento a través de lineamientos establecidos a fin

		servicios de aplicación en redes públicas			de evitar la intrusión de programas intrusos o virus informáticos o evitar el acceso a redes públicas que puedan ser puente de un hacking.
	14.1.3.	Protección de transacciones de servicio de aplicación	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información por que no se ha incluido la implementación de un software.
A.14.2. Seguridad en el proceso de desarrollo y soporte	14.2.1.	Política de desarrollo seguro	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información por que no se ha incluido la implementación de un software.
	14.2.2.	Procedimientos de control de cambios	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información por que no se ha incluido la implementación de un software.
	14.2.3.	Revisión técnica de software	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información por que no se ha incluido la implementación de un software.
	14.2.4.	Restricción de cambios a paquetes de software	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información por que no se ha incluido la implementación de un software.
	14.2.5.	Procedimientos de desarrollo de sistemas	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información por que no se ha incluido la implementación de un software.
	14.2.6.	Entorno de desarrollo seguro	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información por que no se ha incluido la implementación de un software.
	14.2.7.	Desarrollo tercerizado	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información por que no se ha incluido la implementación de un software.
	14.2.8.	Pruebas de seguridad del sistema	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información

					por que no se ha incluido la implementación de un software.
	14.2.9.	Pruebas de aceptación del sistema.	No aplicable	O	No aplicable a los alcances del Sistema de Gestión de Seguridad de la Información por que no se ha incluido la implementación de un software.
A.15.RELACIONES CON PROVEEDORES					
A.15.1. Seguridad en relaciones con el proveedor	15.1.1.	Políticas de seguridad de la información con proveedores	Aplicable	✓	Implementar lineamientos ante probables incumplimientos de los servicios
	15.1.2.	Atención de tópicos	Aplicable	✓	Implementar lineamientos ante probables incumplimientos de los servicios
	15.1.3.	Cadena de suministros	No aplicable	✓	No se encuentra estipulado en el alcance del Sistema de Gestión de Seguridad de la Información
15.2. Gestión de entrega se servicios de proveedor	15.2.1.	Monitoreo y revisión de servicios de proveedor	Aplicable	✓	Implementar lineamientos ante monitoreos y revisión o incumplimientos de los servicios del proveedor
	15.2.2.	Gestión de cambios a servicios de proveedor	Aplicable	✓	Implementar lineamientos ante probables incumplimientos por el cambio de los servicios del proveedor
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN					
A.16.1. Gestión de incidentes de seguridad de la información y mejoras	16.1.1.	Responsabilidad y procedimientos	Aplicable	✓	Se implementará un registro de incidencias de seguridad los cuales servirán de evidencia para la mejora y mantener los procesos íntegros y actualizados.
	16.1.2.	Reporte de eventos de S.I.	Aplicable	✓	Se implementará un registro de eventos de los S.I, los cuales servirán de evidencia para la mejora y mantener los procesos íntegros y actualizados,
	16.1.3.	Reporte de debilidades de S.I.	Aplicable	✓	Se implementará un registro de incidencias de seguridad los cuales

					servirán de evidencia para la mejora las debilidades
	16.1.4	Valoración y decisión de eventos de S.I.	Aplicable	✓	Se implementará un registro de incidencias de seguridad los cuales servirán de evidencia para el análisis de tomar acciones en mejora de los S.I.
	16.1.5.	Respuesta a incidentes de S.I	Aplicable	✓	Se implementará un registro de incidencias de seguridad los cuales servirán para dar respuesta y minimizar los incidentes de los S.I.
	16.1.6.	Aprendizaje de incidentes de S.I.	Aplicable	✓	Se implementará un registro de incidencias de seguridad los cuales servirán como evidencia y evitar d esta manera errores y mejorar los S.I.
	16.1.7.	Colección de evidencia	Aplicable	✓	Elaborar un registro de incidencias los cuales a través de una medición se determinarán errores comunes los cuales servirán para evitar incidentes futuros en S.I.
A.17.ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO					
A.17.1. Seguridad de la Información	17.1.1	Planeación de Seguridad de la información en la continuidad	Aplicable	✓	Se determinará los requisitos para la seguridad de la información y la continuidad de la gestión en materia de seguridad de la información en situaciones complejas o durante desastres naturales, lo que permita seguir con la atención a sus clientes,
	17.1.2.	Implementación de Seguridad de la Información en la continuidad	Aplicable	✓	Se establecerá y procedimientos a través de controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
	17.1.3.	Verificación, revisión y evaluación de seguridad	Aplicable	✓	Se implementará políticas que permitan la verificación, revisión y evaluación de la continuidad de los S.I. mediante controles establecidos para la continuidad de la seguridad de la Información.

17.2. Redundancias	17.2.1.	Disponibilidad de procesamientos de información	No aplicable	✓	No se encuentra dentro de los alcances para la implementación del Sistema de Gestión de seguridad de la Información.
A.18. CUMPLIMIENTO					
18.1. Cumplimiento con Requerimientos Legales y Contractuales	18.1.1.	Identificación de legislación aplicable y requerimientos	Aplicable	✓	La inmobiliaria asegura el cumplimiento y legislación de los derechos de propiedad y los requerimientos que se soliciten para el cumplimiento de los acuerdos o contratos establecidos.
	18.1.2.	Derechos de propiedad intelectual	Aplicable	✓	La inmobiliaria asegura el cumplimiento y reglamentación de los derechos de propiedad y el uso de software patentados bajo licencia.
	18.1.3.	Protección de registros	Aplicable	✓	Se implementará lineamientos y protocolos de seguridad con el fin de cuidar y proteger los registros de información que involucre a la empresa e impedir la pérdida, uso indebido o acceso no autorizado.
	18.1.4	Privacidad y protección de información de datos personales	Aplicable	✓	Implementar los controles de seguridad de la información a fin de proteger y salvaguardar los activos de información de la empresa y sus clientes, de manera que el compromiso es la confidencialidad de la información
	18.1.5.	Reglamentación de controles criptográficos	No Aplicable	O	No se estableció dentro de los alcances para el Sistema de Gestión de Seguridad de la información
18.2. Revisiones de Seguridad de la Información	18.2.1.	Revisión independiente de la seguridad de la información	Aplicable	✓	Se establece el compromiso, organización y asignación para su cumplimiento y así mismo establece la revisión del sistema de gestión de seguridad de la información por lo que se deberá actualizar en base a los controles de la norma vigente.
	18.2.2.	Cumplimiento con las	Aplicable	✓	Los trabajadores interactúan permanentemente con los activos de

		políticas y normas de seguridad			información para los cuales se han diseñado políticas y controles en materia de seguridad de la información, es importante establecer controles y políticas de seguridad
	18.2.3.	Revisión del cumplimiento Técnico	Aplicable	✓	Se debe considerar registrar un historial de los informes técnicos los cuales permitirán un conocimiento acertado complementado de recursos informáticos para la revisión de controles y requisitos técnicos de seguridad

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: "Sistema de gestión de seguridad de la información para la Protección de datos en una Inmobiliaria, Lima 2022", cuyo autor es PONCE CRUZ ANGEL SABINO, constato que la investigación tiene un índice de similitud de 22.00%, 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, 12 de Octubre del 2022

Apellidos y Nombres del Asesor:	**Firma**
AGREDA GAMBOA EVERSON DAVID **DNI:** 18161457 **ORCID:** 0000-0003-1252-9692	Firmado electrónicamente por: AGREDA el 12-10-2022 07:59:00

Código documento Trilce: TRI - 0433945

INVESTIGA UCV