UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA CON LA NORMA ISO/IEC 27001 EN LA EMPRESA RANSA COMERCIAL S.A - PIURA; 2021.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR

MERINO ROSAS, CÉSAR AUGUSTO

ORCID: 0000-0001-6174-8168

ASESOR

MORE REAÑO, RICARDO EDWIN
ORCID: 0000-0002-6223-4246

PIURA – PERÚ

2021

EQUIPO DE TRABAJO

AUTOR

Merino Rosas, César Augusto

ORCID: 0000-0001-6174-8168

Universidad Católica Los Ángeles Chimbote, Estudiante de Pregrado, Piura, Perú

ASESOR

More Reaño, Ricardo Edwin

ORCID: 0000-0002-6223-4246

Universidad Católica Los Ángeles Chimbote, Facultad de Ingeniería, Escuela Profesional de Sistemas, Piura, Perú

JURADO

Ocaña Velásquez, Jesús Daniel

ORCID: 0000-0002-1671-429X

Castro Curay, José Alberto

ORCID: 0000-0003-0794-2968

Sullón Chinga, Jennifer Denisse

ORCID: 0000-0003-4363-0590

JURADO EVALUADOR DE TESIS Y ASESOR

DR. OCAÑA VELÁSQUEZ, JESÚS DANIEL

PRESIDENTE

MGTR. CASTRO CURAY, JOSÉ ALBERTO

MIEMBRO

MGTR. SULLÓN CHINGA, JENNIFER DENISSE

MIEMBRO

MGTR. MORE REAÑO, RICARDO EDWIN

ASESOR

DEDICATORIA

A mis padres, por brindarme todo su apoyo y ser los principales promotores de mis sueños y de ser la persona que soy en la actualidad.

A mi esposa, por su incondicional apoyo y brindarme el tiempo necesario para realizarme profesionalmente.

A mi hija Danna, por ser mi fuente de motivación e inspiración para poder superarme cada día más y tu afecto y cariño son los detonantes de mi felicidad.

César Augusto Merino Rosas

AGRADECIMIENTO

A Dios, por iluminarme durante este trabajo y por permitirme finalizarlo con éxito, tu amor y tu bondad no tienen fin.

A la Universidad Católica los Ángeles de Chimbote por haberme aceptado y brindarme sus conocimientos y apoyo para seguir adelante cada día.

A la empresa Ransa Comercial S.A que me brindo toda la información necesaria para hacer posible este proyecto.

César Augusto Merino Rosas

RESUMEN

Esta tesis fue desarrollada bajo la línea de investigación: Sistemas de gestión de calidad y seguridad de la información, la problemática de la empresa surge porque ejecuta todos sus procesos en Excel y no lleva un control de todos sus procesos, lo que significa que su información este expuesta a diferentes ataques cibernéticos y posibles pérdidas de información, la investigación tuvo como objetivo general implementar un plan de seguridad informática utilizando la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A – Piura; 2021, para mejorar la seguridad de información de sus clientes. El tipo de la investigación es cuantitativo, el nivel de investigación es descriptivo y el diseño de la investigación es no experimental y de corte transversal. Los resultados de la dimensión 01: Nivel de satisfacción con el sistema actual; el 60.00% de los trabajadores encuestados NO están satisfechos con el sistema actual, mientras que el 40.00% indicaron que SI, en relación a la segunda dimensión, se observó que el 80.00% de los encuestados sostienen que SI creen necesario de una nueva propuesta, mientras que el 20% indicaron que NO, esta investigación tiene como alcance resguardar la confidencialidad de los activos de información en la empresa, se concluyó la implementación de un plan de seguridad informática en la empresa Ransa Comercial S.A, mejoró la seguridad de información de sus clientes.

Palabras Claves: Implementación, Informática, Seguridad, Sistema.

ABSTRACT

This thesis was developed under the research line: Information security and quality management systems, the problem of the company arises because it executes all its processes in Excel and does not keep a control of all its processes, which means that its information It is exposed to different cyber attacks and possible loss of information. The general objective of the investigation was to implement a computer security plan using the ISO / IEC 27001 standard in the company Ransa Comercial SA - Piura; 2021, to improve the information security of its customers. The research type is quantitative, the research level is descriptive, and the research design is non-experimental and cross-sectional. The results of dimension 01: Level of satisfaction with the current system; 60.00% of the workers surveyed are NOT satisfied with the current system, while 40.00% indicated that YES, in relation to the second dimension, it was observed that 80.00% of the respondents say that they believe that a new proposal is necessary, While 20.00% indicated that NO, this investigation aims to protect the confidentiality of the information assets in the company, the implementation of a computer security plan in the company Ransa Comercial SA was concluded, the information security of its companies was improved. customers.

Keywords: Implementation, IT, Security, System.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

I. INTRODUCCIÓN

Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones (1).

En el Perú se ha publicado una ley 30999 de Ciberdefensa, cuyo objetivo principal será proteger la soberanía, los intereses nacionales, los activos críticos y recursos claves para mantener las capacidades frente a amenazas o ataques, frente a este tipo de ataques se buscan herramientas y estrategias que disminuyan al mínimo los riesgos de ser víctimas de la acción de los perpetradores de los ciberdelitos, quienes no tienen una ubicación física definida ni un rostro detectable fácilmente en los archivos policiales (2).

La empresa Ransa Comercial S.A, ejecuta todos sus procesos en Excel, no lleva un control de todos sus procesos, lo que significa que su información este expuesta a diferentes ataques cibernéticos y posibles pérdidas de información. Una parte de la empresa, se encarga de gestionar la información personal de sus clientes, esto conlleva a acreditar la seguridad de información de sus clientes.

De acuerdo a lo expuesto anteriormente, se formula lo siguiente: ¿De qué manera la implementación de un plan de seguridad informática con la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A - Piura, 2021; permitirá mejorar la seguridad de información de sus clientes?

Se planteó como objetivo general proponer la implementación de un plan de seguridad informática con la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A - Piura, 2021, para mejorar la seguridad de información de sus clientes. Se plantearon los siguientes objetivos específicos:

1. Analizar la seguridad actual de la información, en la empresa Ransa Comercial S.A.

2. Determinar el nivel de aceptación respecto a la propuesta de mejora.

3. Evaluar los marcos de referencias que ayuden a mejorar la seguridad de la información en la empresa.

4. Proponer la aplicación de la Norma ISO / IEC 27001, para mejorar la seguridad de la información en la empresa Ransa.

Operativamente se justifica, porque per permitió resguardar la confiabilidad e integridad de los activos de información, en la justificación Económica, se justifica por que mejorará la económica a largo plazo, reduciendo pérdidas de información de sus clientes. En la justificación tecnológica, La nueva tecnología se convierte en el soporte de todas las actividades que se producen en la empresa. En la justificación institucional, la empresa mejorará y destacará ante las demás por brindar una apropiada gestión en los activos de información.

De acuerdo a la encuesta se obtuvo resultados donde; el 60.00% de los encuestados manifestaron que, NO están satisfechos con el sistema actual y el 80,00% de los encuestados manifestaron que, SI están de acuerdo con la propuesta de mejora de la seguridad de información en la empresa para para mejorar la seguridad de información de sus clientes.

La investigación tiene como alcance resguardar la confidencialidad de los activos de información en la empresa, a través de implementación de un plan de seguridad informática con la norma ISO/IEC 27001. La presente investigación fue de tipo cuantitativo nivel descriptivo y diseño no experimental de corte transversal. Por lo tanto, se concluye que existe la necesidad de una propuesta de mejora a través de la implementación de un plan de seguridad informática con el fin, de resguardar la información valiosa de la empresa.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

Pilla (3), en el año 2019 en su tesis de titulación denominada "Diseño de una Política de Seguridad de la Información para el Área de Tecnología de la Información de la Cooperativa de ahorro y crédito Chibuleo LTDA Basado en la Norma ISO/IEC 27002", de Quito-Ecuador; utiliza la metodología de matriz de riesgos de cinco columnas; uno de sus objetivos Diseñar una política de seguridad de información para el área de tecnología de información de la Cooperativa, apoyado en la norma internacional ISO/IEC 27002 mediante la aplicación de los controles de seguridad. El resultado de la investigación arrojó que se debe mitigar posibles vulnerabilidades en los sistemas de información, estableciendo dominios, objetivos y controles para la gestión de la seguridad de la información. En conclusión, A través del diagnóstico y de una revisión profunda de la norma internacional ISO/IEC 27002 se diseñó una política de seguridad de la información para el área de TI de la Cooperativa.

León (4), en el año 2018 en su tesis de titulación denominada "Planificación de un SGSI basado en la Norma ISO 27001; en la empresa Mafelesa", de Guayaquil- Ecuador, utiliza la metodología mixta ya que se utilizó un análisis cuantitativo y cualitativo para el respectivo tratamiento de la información recolectada a través de la encuesta realizada; uno de los objetivos principales es contar con una empresa mejor preparada en el manejo, protección y seguridad de los activos utilizados. El resultado de la investigación arrojó que la

empresa necesita que el sistema sea sometido a mejoras para un funcionamiento correcto y eficaz. En conclusión, en este trabajo de titulación se pudo realizar un análisis de la utilidad e importancia de contar con una planificación de un sistema de gestión de seguridad de la información en la Empresa Mafelesa.

Ararat (5), en el año 2018 en su tesis de titulación denominada "Diseño de un SGSI basado en la Norma ISO 27001 para la Empresa Ma Peñalosa CÍA. S.A.A", de Cúcuta- Colombia; utiliza la metodología de análisis y gestión de riesgos de los sistemas de información; uno de sus objetivos fue plantear lineamientos que permitan mitigar los riesgos en los activos informáticos. El resultado arrojó que se pretende asegurar la integridad, confidencialidad y disponibilidad de los sistemas de la empresa. En conclusión, es importante resaltar que para que el Sistema de Gestión de la Seguridad de la Información tenga éxito, debe tener el respaldo y total apoyo de los directivos de MA PEÑALOSA CÍA. S.A.S, de nada sirve contar con un SGSI y toda la documentación que concierne si ellos no están comprometidos con darle importancia a la seguridad de la información y a todos los activos informáticos.

2.1.2 Antecedentes a nivel nacional

Benites (6) en el año 2019 en su tesis de titulación denominada "Implementación de un sistema de Gestión de Seguridad de la Información- Norma ISO 27001 para la Fábrica Radiadores Fortaleza", de Lima- Perú, se utilizó la metodología de gestión de riesgos bajo el ISO 27001:2013; uno de sus objetivos es realizar la

identificación de activos con alto valor de la empresa Radiadores Fortaleza. El resultado fue satisfactorio, se redujo considerablemente los incidentes técnicos, así como la reducción de tiempo de respuesta en el usuario y en el responsable de TI. En conclusión, el desarrollo del Plan de Implementación de un SGSI requiere de un minucioso trabajo, esfuerzo y gran desempeño de toda la Fábrica de Radiadores Fortaleza, esto incluye desde el más alto nivel jerárquico de la Fábrica de Radiadores Fortaleza hasta los trabajadores de servicios generales.

Dávila (7), en el año 2018 en su tesis de titulación denominada "Evaluación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, en la municipalidad distrital de José Crespo y Castillo", de Aucayacu- Perú, utiliza la metodología de nivel cuantitativo, de diseño no experimental de tipo descriptiva; su objetivo es evaluar la implementación del sistema de gestión de seguridad de la información en la Municipalidad Distrital de José Crespo y Castillo, basado en la norma ISO 27001:2013. El resultado obtenido fue el 80.00% de los trabajadores encuestados NO realizan un correcto uso del Hardware y Software de la empresa. En conclusión, el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC, permitirá una adecuada administración de la información.

Flores (8), en el año 2017 en su tesis de titulación denominada "Diseño del sistema de gestión de seguridad de la información para el grupo SIAS SAC." de Chimbote- Perú, utiliza la metodología de nivel cuantitativo, de diseño no experimental de tipo descriptiva; uno de sus objetivos es realizar el diseño del sistema de gestión de seguridad de la información para el GRUPO SIAS SAC. Con la

finalidad de administrar adecuadamente la información de la empresa. El resultado fue que el problema principal de la institución educativa era la confidencialidad de la información con respecto al control del acceso a la información trayendo como consecuencia la inseguridad en la realización de sus operaciones. En conclusión, se controló los accesos a los recursos informáticos de la institución para aumentar la disponibilidad de la información y se estableció la seguridad en las operaciones del negocio para aumentar confidencialidad de la información.

2.1.3 Antecedentes a nivel regional

Ancajima (9), en el año 2019 en su tesis de titulación denominada "Propuesta de Implementación de Seguridad Informática en la TIC de la I.E San Miguel Arcángel", de Catacaos- Piura; utiliza la metodología cuantitativa, nivel descriptivo, diseño no experimental y de corte transversal; teniendo como objetivo general realizar un estudio de los riesgos que se tiene en la institución, y así brindar una buena propuesta de implementación de Seguridad Informática. El resultado fue que el 75.00% de los encuestado expresó que se encuentran satisfechos con las TIC en el proceso de enseñanza. En conclusión, los docentes para poder utilizar mejor las TIC deben de seguir un módulo dinámico con sus alumnos e interactuar como ellos haciendo un buen uso de los recursos tecnológicos; teniendo como objetivo.

Lara (10), en el año 2018 en su tesis de titulación denominada "Propuesta para la seguridad informática basado en la Norma ISO 27001 en la clínica Simedic Diagnóstica S.A.C", de Piura-Perú,

utiliza la metodología cuantitativa porque que permite recolectar datos para tener resultado y brindar soluciones; teniendo como objetivo general realizar la propuesta para la seguridad informática basada en la norma ISO/IEC. El resultado es que cuenta con la adecuada gestión en los procesos de la clínica que y que si están de acuerdo con la que se debería realizar la propuesta para la seguridad informática para la clínica. En conclusión, queda demostrado que se necesita mejorar la atención al cliente y la seguridad de información en la clínica Simedic Diagnóstica; este resultado es semejante al indicado en la hipótesis general por lo que se concluye que queda aceptada.

Sandoval (11), en el año 2018 en su tesis de titulación denominada "Diseño de un Plan de Seguridad de Información para el Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura", de Piura- Perú, utiliza la metodología de Análisis y Gestión de Riesgos de las Tecnologías de la Información; tiene como objetivo diseñar un plan de seguridad de la información para proteger los activos informáticos que se utilizan por el Centro de Informática y Telecomunicaciones. El resultado es que el CIT está expuesto a una serie de riesgos que son críticos para su funcionamiento, lo cual sustenta la problemática expuesta y la importancia del desarrollo de este proyecto. En conclusión, con el uso del estándar de seguridad de la información ISO 17799, se logra diseñar el Plan de Seguridad de la Información para lograr así una mejor protección de los activos informáticos que se utilizan y generan en cada uno de los procesos de la UNP.

2.2. Bases Teóricas de la investigación

2.2.1. El rubro de la empresa

Es un Operador logístico con más de 78 años en la gestión de cadenas de abastecimientos y diseño de soluciones logísticas integrales y flexibles. (12).

2.2.2. La empresa Investigada

2.2.2.1. Información General

La empresa Ransa Comercial S.A es reconocido como un operador logístico, y cuanta con personal altamente capacitado para atender cualquier requerimiento que solicite el cliente líder en cada sector económico, identifican los costos totales de su actividad logística, simplificamos las operaciones y optimizamos los recursos, mejorando la eficiencia de la cadena de abastecimiento lo que les permite concentrarse en el core del negocio (12).

Gráfico Nro. 1: Ransa Comercial S.A

Fuente: Google Maps (12).

2.2.2.2. Historia

En 1939, la compañía Ransa Comercial fue creada y dedicada al almacenamiento de fardos de algodón para exportación, obteniendo ahorros en flete y almacenamiento. Su objetivo es servicios de almacenamiento simples y cuartos fríos, a los que llamó COLD RANSA. 1978 - Ransa crea Transportes Ransa S.A. Ransa expande sus actividades, proporcionando un servicio nacional de operador de carga. (12).

2.2.2.3. Objetivos Organizacionales.

Nuestro objetivo principal es gestionar operaciones aduaneras que, de acuerdo a la Ley General de Aduanas, permitan cumplir con los requerimientos operativos de nuestros Clientes, brindando un servicio con alto valor agregado (12).

2.2.2.4. Misión

Su misión es brindar servicio logístico y almacenamiento de diferentes productos, manejo de información y documentos (12).

2.2.2.5. Visión

La visión de la empresa es liderar mediante soluciones logísticas, especialmente en la atención de los requerimientos de los clientes, de esta forma los clientes puedan quedar

satisfechos al atender y optimizar los requerimientos específicos de su cadena de abastecimiento en cada sector económico (12).

2.2.2.6. Organigrama

Gráfico Nro. 2: Organigrama de la Empresa

Fuente: Empresa Ransa Comercial S.A (12).

2.2.2.9. Tecnológica existente en la empresa.

Tabla Nro. 1: Equipos Existentes

HARDWARE	
Equipos	**Cantidad**
Equipos portátiles	3
Computador de Escritorio	6
Impresoras Multifunción a tinta	3
Impresoras Matriciales con cinta	02
Proyectores Multimedia	01
Router ZTE-Huawei.	1

Fuente: elaboración propia

Tabla Nro. 2: Aplicativos

SOFTWARE
Antivirus NOD 32
Office 2010, 2013, 2016
Chrome
Windows 7
Windows 8

Fuente: Elaboración propia.

2.2.3. Las tecnologías de la información y comunicaciones (TIC)

2.2.3.1. Definición

Las TIC se han desarrollado a partir de los avances científicos ya que son herramientas para acceder y compartir información por diversos medios tecnológicos como los teléfonos, computadoras, etc. Actualmente las TIC son muy necesarias para la sociedad por que sirven para facilitar la busque de información. (13).

Si hablamos de educación podemos decir que las TIC han facilitado la educación en estos tiempos de pandemia porque son capaces de juntar a las personas a relacionarse mejor aún a distancia, existen diversos instrumentos relacionados a las TIC pero el medio que más se utiliza son los ordenadores que nos permiten utilizar diversas aplicaciones. (14).

2.2.3.2. Historia

La historia de las TIC empieza en la década de los 70 con la caída de los precios de las materias primas y la superioridad de las TIC. Durante la última década hay una carrera contra reloj por la adquisición y generación de información y conocimientos. Podría decirse que las TI han abierto un territorio en el cual la mente humana es la fuerza productiva directa de mayor importancia en la actualidad (15).

2.2.3.3. Evolución de las TIC.

La evolución de las TIC en la tecnología, muestra que los avances realizados en esta área han sido espectaculares y radicales al habilitar información como sonidos, imágenes y las posibilidades que ofrecen las redes fijas y móviles, con la integración de aplicaciones que permiten conectar programas de diferentes tipos. La evolución de las TIC en el desarrollo de software ha permitido la aparición de herramientas avanzadas de software de gestión con nuevas funcionalidades y aplicaciones empresariales (16).

2.2.3.4. Ventajas y Desventajas de las TIC:

Una de las ventajas de las TIC, es que tiene nuevos métodos de comunicación, esto hace de que estemos en comunicación con otras personas y en tiempos de pandemia sea muy utilizado ya sea como un método de enseñanza, por otra parte, es peligroso porque se expone datos personales y podría ser víctima de un ataque cibernético.

2.2.3.5. Las Tic más utilizadas en la RSPNORTE:

- Office 2013
- Correos Corporativos.
- Internet
- Redes Sociales
- Página web
- Bandas anchas

2.2.4. Teoría relacionada con la tecnología de la investigación

2.2.4.1. Seguridad

Si hablamos de seguridad nos referimos a, libres de peligros que pueden ocasionar algún daño tanto físico como psicológico, es decir que uno se sienta protegido contra todo aquello que pueda atentar contra su persona (17).

Para George Beekman, en las empresas la seguridad es un factor muy importante, es un tema muy importante para cualquier empresa, porque no solo es una garantía física, sino también algo más grande que nos permite vivir una vida sin amenazas se recomienda diferentes niveles de seguridad y que dependen solo del usuario para proteger su información. (18).

2.2.4.2. Informática

Según Elizondo (19), en su libro "Informatik 1" menciona a la Organización de las Naciones Unidas para la Educación, la ciencia y la cultura (Unesco), que propone la definición de informática como la ciencia que tiene que ver con los sistemas de procesamiento de información y su economía, política y política e impacto sociocultural. El término informático es el acrónimo de información automática y proviene de la palabra francesa informatique.

La informática es una palabra que implica en su estructura semántica los términos: información y automático. Fue

inventado en Francia hace 40 años con la intención de definir todos los procedimientos, métodos, técnicas y otros aspectos científicos de diferentes campos que se desarrollaron y aplicaron al procesamiento de información utilizando computadoras para resolver problemas económicos, sociales y políticos (20).

2.2.4.3. Seguridad Informática

Es un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo. También se encarga de controlar el acceso al sistema informático, desde el punto de vista software y por usuarios autorizados, ya sea desde dentro del sistema informático o desde una red externa, usando una VPN, la WEB, transmisión de archivos, conexión remota (21).

La tarea principal de la seguridad informática es minimizar los riesgos, en este caso, provienen de muchas partes, puede ser la entrada de datos, el medio que transporta la información, el material utilizado para transmitir y recibir, usuarios mismos e incluso por los mismos protocolos que se implementan, pero la tarea principal sigue siendo minimizar los riesgos para obtener una mayor y mejor seguridad (22).

2.2.4.4. Los Virus Informáticos

Uno de los primeros conceptos cuando se trata de seguridad informática es el virus informático. Las computadoras entienden el código binario solo como ceros y unos. En el mundo de las computadoras y las computadoras hay muchos conceptos como programas, videojuegos, sistemas operativos y todo tipo de software. Un virus informático puede hacer muchas cosas, por ejemplo, eliminar archivos, impedir el acceso a las computadoras, robar información, bloquear las funciones de un sistema operativo o programas en una computadora (22).

2.2.4.5. Seguridad de Información

La seguridad es una necesidad básica ya que se encuentra en la prevención de la vida. Hoy en día, la seguridad puede verse desde dos perspectivas muy definidas, la Legislativa y la Tecnológica. Aunque la tecnología es un elemento indispensable para las organizaciones, se debe utilizar de forma adecuada para evitar riesgos en la información. Por tanto, es importante que se adopten las medidas necesarias antes de que se produzca un incidente de seguridad (23).

2.2.4.6. Activos de Información

Son recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad, son necesarios para que la empresa funcione y alcance los objetivos que se

proponen, como por ejemplo los trabajadores que son esenciales para el fundamentales para el crecimiento de las organizaciones (24).

2.2.4.7. Estándar de gestión de la S.I

- Norma ISO

  La Organización Internacional de Normalización se encarga de la elaboración de estándares que ayudan a resguardar la calidad de productos y servicios, actualmente hay más de 22.000 ISOS diferentes cada una centrada en un elemento de los servicios que brinda las distintas empresas (25).

- ISO

  Es una organización independiente, se encarga de establecer protocolos de internacionales que ayudan a la innovación relevante para el mercado con soluciones a los problemas a los que se enfrenta el mundo, sus expertos son los causantes de realizar estos protocolos, al brindar todos sus conocimientos adquiridos (25).

- Estándar

  Son protocolos o normas que ayudan a dar seguridad y cuidar los servicios de la empresa, uno de sus ventajas es el ordenamiento que ayuda a resolver un problema

potencial o real. El estándar es un nivel de referencia de algún factor de producción que redundará en los beneficios obtenidos por la empresa con el desarrollo de su actividad (25).

2.2.4.8. ISO/IEC 2700

La serie de normas internacionales ISO / IEC 27000 ofrece una serie de recomendaciones de mejores prácticas para la gestión de la seguridad de la información, y esto se puede aplicar en cualquier organización, independientemente de su tamaño, está orientada para que puedan mantener la gestión de la seguridad, compuesto por las siguientes reglas que se pueden observar a continuación (26):

- ISO27000: Es la norma encargada del mantenimiento del SGSI.

- ISO27001: Esta norma puede ser implementada en cualquier tipo de empresa y permite que certifique a la empresa en tema de seguridad de información.

- ISO27002: Se encargar de mejorar el SGSI con buenas prácticas de gestión.

- ISO27003: Esta norma tiene como finalidad implementar un SGSI y puede ser adoptada por los consultores.

- ISO27004: Se encarga de medir el resultado de un SGSI y dar respuestas de las amenazas.

- ISO27005: Puede implementarse en cualquier empresa con la finalidad de gestionar los riesgos de la misma.

- ISO27006: Se encarga de la acreditación y certificación del SGSI.

- ISO27007: Se encarga de auditar a los SGSI que están basados en ISO/IEC 27001,

- ISO27011: Se encarga de la seguridad para las organizaciones de telecomunicaciones.

- ISO27031: Es una norma encargada para determinar los requerimientos para la creación de un plan de Continuidad de las TIC.

- ISO27032: Se encarga de garantizar la seguridad en los intercambios de información en la Red para lograr hacer frente de una manera más efectiva al Cibercrimen.

- ISO27033: Esta norma se encarga de gestionar la seguridad de las redes y a la seguridad de información que se pasa mediante enlaces de comunicaciones.

- ISO27034: Se encarga de brindar seguridad a las aplicaciones creadas por las empresas.

- ISO27799: Está hecha para la industria sanitaria, sirve de apoyo a la aplicación y a la interpretación de la informática en salud.

2.2.4.9. ISO 27001

Es un estándar internacional emitido por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. Puede implementarse en todo tipo de organizaciones, con fines de lucro, privado, público, pequeño o grande. La ISO27001 se ha convertido en el principal estándar mundial de seguridad de la información y varias empresas optan por esta norma. La certificación ISO 27001 es especial para resguardar los activos más importantes de la empresa, al igual que la información de los clientes o trabajadores, la implementación de la ISO 27001 es la respuesta ideal a los requisitos de los clientes (27).

2.2.4.10. ISO 27001 y función

El eje central de ISO27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (leer, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (leer, mitigación o tratamiento del riesgo). (28).

2.2.4.11. La Normativa ISO/IEC 27001:2013

Es una norma enfocada a la seguridad de la información bajo protocolos de administración explícitos, estos protocolos

ayudan a mantener estable y libre de ataques a las organizaciones cumpliendo con numerosas disposiciones reglamentarias y jurídicas relacionadas con la seguridad de la información (29).

2.2.4.12. Metodología de Gestión de Riesgos

Hoy en día las empresas sufren de riesgos informáticos que afecta su funcionamiento, una forma de prevenir estos riesgos es realizando una evaluación de riesgos informáticos. Esta evaluación se puede llevar acabo aplicando algunas de las siguientes metodologías (30):

MAGERIT

Significa Metodología de Análisis y Gestión de Riesgos de los sistemas de información y está relacionada con la generación que utilizan los medios informáticos y minimizar los riegos con protocolos de seguridad adecuados de confianza. MAGERIT se basa en analizar cada violación de seguridad que pueda tener una organización, identificarlas y optar por medidas preventivas y correctivas más apropiadas para mitigar esas amenazas.

OCTAVE

Octave significa Operationally Critical Threat, Asset and Vulnerability Evaluation, es un método de análisi de riesgo que se encarga del riesgo operativo y las prácticas de

seguridad, ayudando a las empresas a la toma de decisiones sobre la seguridad de información, a través de procesos y actividades que ayudan a determinar las necesidades de seguridad en una organización.

CRAMM

Es una metodología orientada a proteger la integridad de los activos existentes en la empresa, con una amplia gama de herramientas que evalúan e identifican las amenazas y vulnerabilidades para la empresa (31).

VALORACIÓN DE LAS AMENAZAS

Para la evaluación de las amenazas, se calcula la probabilidad de que un ataque sea perpetrado contra un objetivo durante un período de tiempo específico, a continuación, se muestra la valoración de dichas amenazas (32):

Tabla Nro.3: Degradación del valor

MA.	Muy alta.	Casi seguro.	Fácil.
A	Alta.	Muy alto.	Medio.
M	Media.	Posible.	Difícil.
B	Baja.	Poco probable.	Muy difícil.
MB	Muy baja.	Muy raro.	Extremadamente Difícil.

Fuente: Libro1 de Margerit (32).

III. HIPÓTESIS

3.1. Hipótesis general

La propuesta de implementación de un plan de seguridad informática con la norma ISO/IEC 27001 en la empresa Ransa comercial S.A – Piura, permitirá mejorar la seguridad de información de sus clientes.

3.2. Hipótesis especificas

1. El análisis de seguridad de la información permite conocer la situación actual de la empresa Ransa Comercial S.A.

2. El determinar el nivel de aceptación respecto a la propuesta de mejora permite implementar un plan de seguridad informática.

3. La evaluación de los marcos de referencia permite una mejor seguridad de la información en la empresa Ransa Comercial S.A.

4. La Propuesta de la aplicación de la Norma ISO/IEC 27001, asegura con seguridad de la información en la empresa Ransa Comercial S.A.

IV. METODOLOGÍA

4.1. Tipo de la investigación

Por las características de la investigación se obtuvo el tipo descriptiva porque permite como su nombre lo indica describir las situaciones, los fenómenos o los eventos que nos interesan, midiéndolos, y evidenciando sus características. Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis (33).

4.2. Nivel de la investigación

Por las características de la investigación se obtuvo de un enfoque cuantitativo porque usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías (33).

4.3. Diseño de la investigación

El diseño de la investigación es no experimental porque según Sampieri, Fernández, Baptista dan a conocer que las variables independientes ocurren y no es posible manipularlas, no se tiene control directo sobre dichas variables ni se puede influir sobre ellas, porque ya sucedieron, al igual que sus efectos (33).

Y de corte transversal según su característica de tiempo ya que el estudio se circunscribe a un momento puntual, recolectándose datos en un tiempo único, describiendo variables y analizando su incidencia (34).

4.4. Población y Muestra

4.4.1. Población

La población es el conjunto de personas u objetos de los que se desea conocer algo en una investigación. El universo o población puede estar constituido por personas, animales, registros médicos, los nacimientos, las muestras de laboratorio, entre otros (35).

La Empresa Ransa Comercial S.A – Piura, cuenta con 27 trabajadores dispersos en las diferentes áreas de la empresa.

4.4.2. Muestra

La muestra es un subconjunto o parte del universo o población en que se llevará a cabo la investigación. Hay procedimientos para obtener la cantidad de los componentes de la muestra como fórmulas. La muestra es una parte representativa de la población (35).

Excluyendo a algunos trabajadores, del cual podremos tomar como muestra la cantidad de 15 trabajadores. La técnica utilizada para la selección de la muestra fue la técnica no probabilística.

4.5. Definición operacional de las variables en estudio

Tabla Nro. 4: Matriz de Operacionalización de las variables

Variable	Definición Conceptual	Dimensiones	Indicadores	Escala medición	Definición Operacional
Implementación de un plan de seguridad informática con la norma ISO/IEC 27001	La implementación de un plan de seguridad informática mejorará la seguridad de información de sus clientes, al garantizar la integridad, disponibilidad y confidencialidad de la información (22).	Nivel de satisfacción con el sistema actual.	-Como usted utiliza el sistema actual. -El proceso de manejo de documentos son confidenciales. -El proceso de copias de seguridad se manejan de la forma correcta. -Usted cree que para manejar el sistema actual solo debe tener una sola clave de acceso. -Tiene conocimiento si las informaciones de sus clientes están seguras.	Ordinal	La seguridad informática se caracteriza por la protección de datos y de comunicaciones en una red asegurando, en la medida de lo posible, los tres principios básicos: La integridad de los datos, la disponibilidad del sistema y la confidencialidad
		Nivel de aceptación de la propuesta de mejora	-Crees que se debe de mejorar la seguridad informática de sus documentos.	Ordinal	

			-Sería adecuado contar con seguridad de información. -Cree usted que la seguridad de información ayudara a la empresa. -Cree usted que si ocurre un incidente de seguridad podrá darle solución. -Cree usted que teniendo una seguridad informática estará segura su información.		

Fuente: elaboración propia

4.6. Técnicas e instrumentos de recolección de datos

4.6.1. Técnica

Se utilizó la técnica de la encuesta y el cuestionario como instrumento, con la finalidad de verificar el cuestionario para medir con los indicadores realizados y seleccionados por medio de las variables en este desarrollo de investigación.

La encuesta es una de las técnicas de investigación social de más extendido uso en el campo de la Sociología que ha trascendido el ámbito estricto de la investigación científica, para convertirse en una actividad cotidiana de la que todos participamos tarde o temprano. Se ha creado el estereotipo de que la encuesta es lo que hacen los sociólogos y que éstos son especialistas en todo (36).

4.6.2. Instrumentos

El cuestionario es un sistema de preguntas ordenadas con coherencia, con sentido lógico y psicológico, expresado con lenguaje sencillo y claro. Permite la recolección de datos a partir de las fuentes primarias. Está definido por los temas que aborda la encuesta. Logra coincidencia en calidad y cantidad de la información recabada. Es el instrumento que vincula el planteamiento del problema con las respuestas que se obtienen de la muestra (36).

4.7. Plan de análisis

Se seleccionará a las personas adecuadas, para poder aplicar los cuestionarios, ya que así obtendremos la información apropiada, por medio de visitas a las diversas instalaciones de la empresa Ransa Comercial S.A.

Asimismo, se entregará los cuestionarios a las personas seleccionadas, para poder resolver cualquier duda en relación a las interrogantes planteadas en los mismos. Se creará un archivo en formato MS Excel 2016 para la tabulación de las respuestas de cada cuestionario en base a cada dimensión de estudio, así se obtendrá rápidamente los resultados y se podrá dar su conclusión a cada una de ellas.

4.8. Matriz de Consistencia

Tabla Nro. 5: Matriz de consistencia

Problema	Objetivo General	Hipótesis General	Variables	Metodología
¿De qué manera la implementación de un plan de seguridad informática con la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A - Piura, 2020; permitirá mejorar la gestión en la seguridad de los	Realizar la propuesta de implementación de un plan de seguridad informática basada en la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A - Piura, 2020; permitirá mejorar la gestión en los activos de información. **OBJETIVO ESPECÍFICO** 1. Analizar la seguridad actual de la información, en la empresa Ransa Comercial S.A.	La implementación de un plan de seguridad informática con la norma ISO/IEC 27001 en la empresa Ransa comercial S.A – Piura, permitirá mejorar la gestión en los activos de información. **HIPÓTESIS ESPECÍFICO** 1. El análisis de seguridad de la información permite conocer la situación actual de la empresa Ransa Comercial S.A.	Implementación de un plan de seguridad informática basada en la norma ISO/IEC 27001	**Nivel:** investigación será de un enfoque cuantitativo. **Tipo:** Descriptivo **Diseño:** Investigación no experimental

activos de información?	2. Determinar el nivel de aceptación respecto a la propuesta de mejora. 3. Evaluar los marcos de referencias que ayuden a mejorar la seguridad de la información en la empresa. 4. Proponer la aplicación de la Norma ISO / IEC 27001, para mejorar la seguridad de la información en la empresa Ransa.	2. El determinar el nivel de aceptación respecto a la propuesta de mejora permite implementar un plan de seguridad informática. 3. La evaluación de los marcos de referencia permite una mejor seguridad de la información en la empresa Ransa Comercial S.A. 4. La Propuesta de la aplicación de la Norma ISO/IEC 27001, asegura con seguridad de la información en la empresa Ransa Comercial S.A.		

Fuente: Elaboración propia

4.9. Principios éticos

Durante la elaboración de esta investigación, teniendo como título: Implementación de un plan de Seguridad Informática de la Empresa Ransa Comercial S.A, Piura; 2021, no se ha descuidado la parte sobre los principios y la ética, como en primer lugar del investigador o indagador y en segundo lugar de la Institución Educativa Emblemática, dando la plena seguridad, la veracidad de una originalidad de toda esta investigación que se ha realizado. Cualquier actividad que se realiza en nuestra Universidad sobre investigación, tiene estos principios (37):

Protección a las personas: Es cuando en la investigación se trabaja con personas voluntarias y estas se ven vulnerables y necesitan de una protección, se debe respetar sus derechos.

Cuidado del medio ambiente y la biodiversidad: En este caso las investigaciones que están involucradas con el medio ambiente deben de protegerlo, tomar medidas para no causar daños.

Libre participación y derecho a estar informado: Toda persona que realiza una investigación tiene derecho a estar bien informado sobre los propósitos y finalidades de la investigación a desarrollar.

Beneficencia no maleficencia: Se debe asegurar el bienestar de los participantes de la investigación.

Justicia: El investigador está obligado a tratar con equidad a aquellas personas que son partícipes en los procesos y servicios asociados a la investigación.

Integridad científica: El investigador deberá mantenerse a la integridad científica, al declarar los conflictos de interés que pudieran afectar el curso de un estudio o la comunicación de sus resultados.

V. RESULTADOS

5.1. Resultados de la encuesta

5.1.1 Dimensión 01: Nivel de satisfacción con el sistema actual.

Tabla Nro.6: Conformidad de seguridad

Conformidad de seguridad, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001 de la empresa Ransa.

Alternativas	n	%
Si	6	40,00
No	9	60,00
Total	15	100,00

Cuestionario aplicado a los trabajadores, respecto a: ¿Se encuentra conforme con la seguridad que ofrece la empresa?

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.6, se aprecia que, el 60.00% de los trabajadores manifestaron que, NO están conforme con la seguridad que ofrece la empresa, mientras que, el 40.00% de los encuestados manifestaron todo lo contrario.

Tabla Nro.7: Seguridad para la información

Seguridad para la información, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.

Alternativas	n	%
Si	4	27,00
No	11	73,00
Total	15	100,00

Cuestionario aplicado a los trabajadores, respecto a: ¿En la empresa, el sistema actual brinda total seguridad, para la información que se maneja?

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.7, se aprecia que, el 73.00% de los trabajadores manifestaron que, el sistema actual NO brinda total seguridad para la información que se maneja en la empresa Ransa Comercial S.A, mientras que, el 27.00% que SI.

Tabla Nro.8: Resguardo de información

Resguardo de información, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.

Alternativas	n	%
Si	6	40,00
No	9	60,00
Total	15	100,00

Cuestionario aplicado a los trabajadores, respecto a: ¿Considera usted que es seguro la manera como resguarda la información la empresa?

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.8, se aprecia que, el 60.00% de los trabajadores manifestaron que, NO es seguro la manera como resguarda la información la empresa en la empresa Ransa Comercial S.A, mientras que, el 40.00% que SI.

Tabla Nro.9: Importancia de una Norma

Importancia de una Norma, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.

Alternativas	n	%
Si	6	40,00
No	9	60,00
Total	15	100,00

Cuestionario aplicado a los trabajadores, respecto a: ¿Considera usted que una norma ISO es de suma importancia para el resguardo de información en la empresa?

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.9, se aprecia que, el 60.00% de los trabajadores manifestaron que, NO es de suma importancia una norma ISO para el resguardo de información en la empresa, mientras que, el 40.00% que SI.

Tabla Nro.10: Procesos de seguridad

Procesos de seguridad, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.

Alternativas	n	%
Si	8	53,00
No	7	47,00
Total	15	100,00

Cuestionario aplicado a los trabajadores, respecto a: ¿Tiene conocimiento sobre los procesos de seguridad para la información de la empresa?

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.10, se aprecia que, el 53.00% de los trabajadores manifestaron que, SI tienen conocimiento sobre los procesos de seguridad para la información de la empresa, mientras que, el 47.00% que NO.

5.1.2. Dimensión 02: Nivel de aceptación de la propuesta de mejora

Tabla Nro.11: Implementación de la norma ISO

Aceptación de la norma ISO, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.

Alternativas	n	%
Si	13	87,00
No	2	13,00
Total	15	100,00

Cuestionario aplicado a los trabajadores, respecto a: ¿Estaría de acuerdo en implementar la norma ISO para la protección de la información de la empresa?

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.11, se aprecia que, el 87.00% de los trabajadores manifestaron que, SI están de acuerdo en implementar la norma ISO para la protección de la información de la empresa, mientras que, el 13.00% que NO.

Tabla Nro.12: Reforzamiento de seguridad

Reforzamiento de seguridad, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.

Alternativas	n	%
Si	12	80,00
No	3	20,00
Total	15	100,00

Cuestionario aplicado a los trabajadores, respecto a: ¿Considera usted que al implementar la norma ISO se reforzará la seguridad de información en la empresa?

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.12, se aprecia que, el 80.00% de los trabajadores manifestaron que, SI se reforzará la seguridad de información al implentar la norma ISO mientras que, el 20.00% que NO.

Tabla Nro.13: Confiabilidad de la empresa

Confiabilidad de la empresa, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.

Alternativas	n	%
Si	6	40,00
No	9	60,00
Total	15	100,00

Cuestionario aplicado a los trabajadores, respecto a: ¿Considera usted que al implementar la norma ISO ayudará a la empresa a ser confiable y a crecer como empresa?

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.13, se aprecia que, el 60.00% de los trabajadores manifestaron que, NO consideran que al implementar la norma ISO ayudará a la empresa a ser confiable, mientras que, el 40.00% que SI.

Tabla Nro.14: Mejora del servicio

Mejora del servicio, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A - Piura, 2020.

Alternativas	n	%
Si	8	53,00
No	7	47.00
Total	15	100,00

Cuestionario aplicado a los trabajadores, respecto a: ¿Considera usted que la implementación de la norma ISO ayudará a mejorar el servicio al cliente y mejorar la imagen de la empresa?

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.14, se aprecia que, el 53,00% de los trabajadores manifestaron que, SI consideran que la implementación de la norma ISO ayudará a mejorar el servicio al cliente y mejorar la imagen de la empresa, mientras que, el 47,00% que NO.

Tabla Nro.15: Disminución de perdida de información

Disminución de pérdidas de información, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.

Alternativas	n	%
Si	9	60,00
No	6	40,00
Total	15	100,00

Cuestionario aplicado a los trabajadores, respecto a: ¿Cree usted que disminuirá las pérdidas de información de contar con la norma ISO para seguridad informática en la empresa?

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.15, se aprecia que, el 60.00% de los trabajadores manifestaron que, SI disminuirá las pérdidas de información de contar con la norma ISO para seguridad informática en la empresa, mientras que, el 40.00% que NO.

5.1.3. Resumen de la Dimensión 1: Nivel de satisfacción del sistema actual.

Tabla Nro.16: Resumen de la Dimensión 1

Distribución de frecuencias de la dimensión N° 1 Nivel de satisfacción del sistema actual, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.

Alternativas	n	%
Si	2	40,00
No	13	60,00
Total	15	100,00

Fuente: Cuestionario aplicado a los trabajadores de la empresa respecto a la Dimensión N° 01.

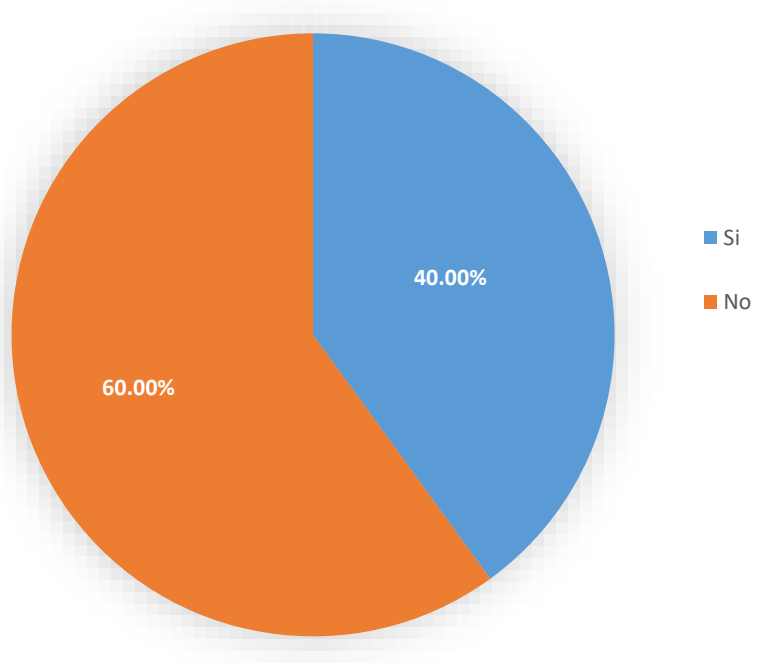
.

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.16, se aprecia que, el 60.00% de los trabajadores manifestaron que, NO están satisfechos con el sistema actual, mientras que, el 40.00% que SI.

Gráfico Nro.3: Resultado general de la dimensión 1

Nivel de satisfacción del sistema actual, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.



Fuente: Tabla Nro. 16

5.1.4. Resumen de la Dimensión 2: Nivel de aceptación de la propuesta de mejora

Tabla Nro.17: Resumen de la Dimensión 2

Distribución de frecuencias de la dimensión N° 2 Nivel de aceptación de la propuesta de mejora, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.

Alternativas	n	%
Si	12	80,00
No	3	20,00
Total	15	100,00

Fuente: Cuestionario aplicado a los trabajadores de la empresa respecto a la Dimensión N° 02.

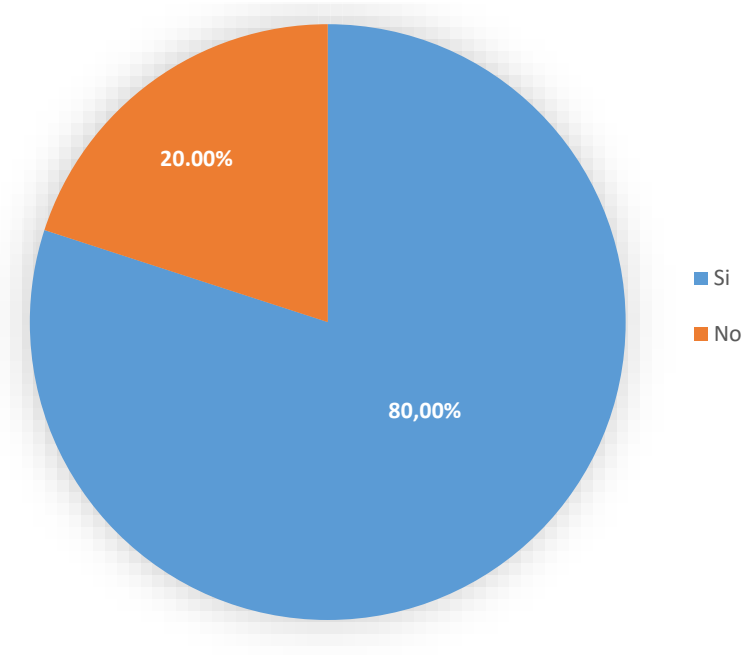
.

Aplicado por: Merino, C.; 2021.

En la Tabla Nro.17, se aprecia que, el 80,00% de los trabajadores manifestaron que, SI existe la necesidad de una propuesta de mejora del sistema actual, mientras que, el 20,00% que NO.

Gráfico Nro.4: Resultado general de la dimensión 2

Nivel de aceptación de la propuesta de mejora, respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001.



Fuente: Tabla Nro. 17

5.1.5. Resumen General

Tabla Nro.18: Resumen General de Dimensiones

Distribución de frecuencias respecto a la implementación de un plan de seguridad informática con la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A - Piura, 2021.

Dimensiones	Alternativas de Respuestas				Muestra	
	Si	%	No	%	n	%
Dimensión 1	2	40.00	13	60.00	15	100,00
Dimensión 2	12	80.00	3	20.00	15	100,00

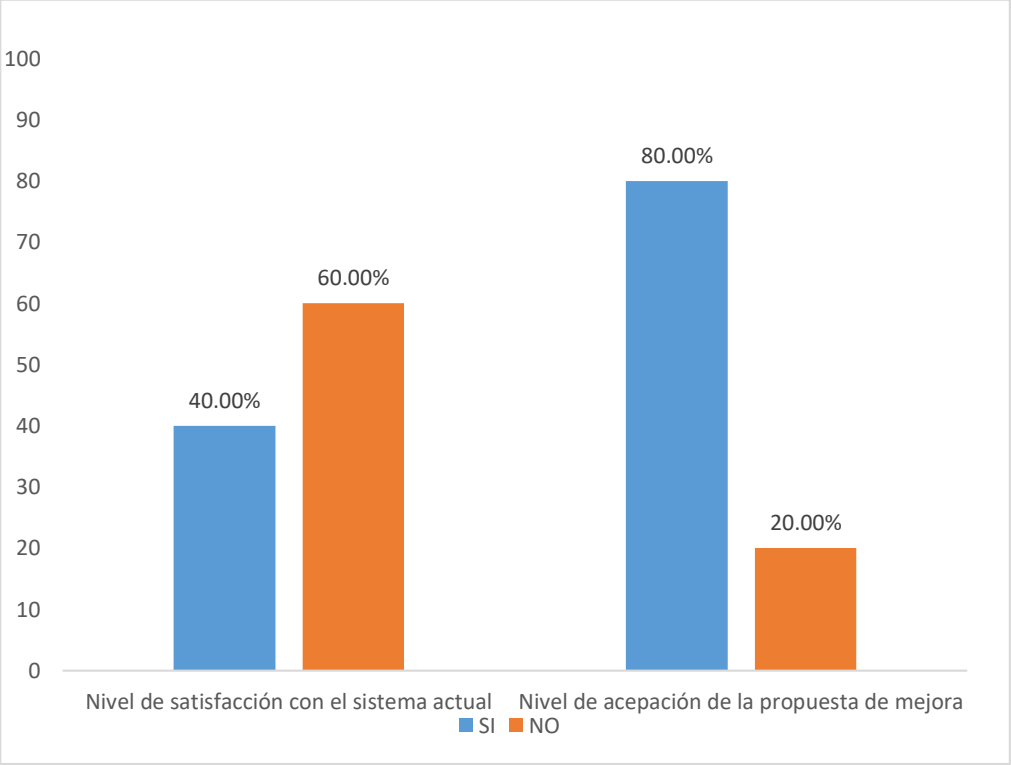
Fuente: Cuestionario aplicado a los trabajadores de la Ransa Comercial, acerca de la aceptación de las dos dimensiones definidas para la investigación en la empresa Ransa Comercial SA

Aplicado por: Merino, C.; 2021.

Una vez obtenidos los resultados, en la Tabla Nro.18, se aprecia que, el 60.00% de los trabajadores manifestaron que, NO están satisfechos con el sistema actual, mientras que, el 40.00% de los encuestados manifestaron que SI, con respecto a la dimensión 2: Propuesta de mejora, se observa que, el 80,00% de los encuestados manifestaron que, SI existe la necesidad de una propuesta de mejora, mientras que, el 20,00% de los encuestados manifestaron lo contrario.

Gráfico N° 5: Resumen General de las Dimensiones

Gráfico porcentual de las encuestas relacionadas con las dos dimensiones definidas para determinar el nivel de satisfacción del sistema actual de la empresa para la Propuesta implementación de un plan de seguridad informática con la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A – Piura; 2021.



Fuente: Tabla N° 17.

5.2. Análisis de Resultados

La presente investigación tuvo como objetivo general: realizar la implementación de un plan de seguridad informática basada en la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A - Piura, 2021, en el cual se ha realizado dos dimensiones que son satisfacción con el sistema actual y propuesta de mejora. Por lo consiguiente una vez interpretado los resultados se proceden a analizarlos detenidamente en los siguientes párrafos:

Respecto a la dimensión 1: Nivel de satisfacción con el sistema actual, en el que se puede observar que el 60,00% de los encuestados manifestaron que, NO están satisfechos con el sistema actual, mientras que, el 40,00% de los encuestados manifestaron que, SI están satisfechos con el sistema actual. Este resultado tiene similitud con los resultados obtenidos por Lara (10), quien en su tesis de investigación titulada: "Propuesta para la Seguridad Informática basado en la Norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018", muestra como resultados que el 61,00% de los empleados encuestados NO cuenta con la adecuada gestión en los procesos de la clínica Simedic Diagnóstica S.A.C. Esto coincide con el autor Gonzales (14), quien menciona que las TIC son utilizadas para la gestión y transformación de la información, y en particular el uso de ordenadores que permiten crear, modificar, almacenar, proteger y recuperar esa información. Estos resultados se obtuvieron porque los procesos se realizan de manera automático, no existen protocolos que aseguren el funcionamiento y seguridad de la información, el contar con la norma ISO nos ayudará a mejorar la gestión de las tecnologías de información.

En relación a la dimensión 2: Nivel de aceptación de la propuesta de mejora, en el que se puede observar que el 80,00% de los encuestados manifestaron que, SI están de acuerdo con la propuesta de mejora de la seguridad de información en la empresa, mientras que, el 20,00% de los encuestados manifestaron que, NO están de acuerdo con la propuesta de mejora de la seguridad de información en la empresa. estos datos mostrados coinciden con Davila (7), quien en su tesis de investigación titulada: "Evaluación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, en la municipalidad distrital de José Crespo y Castillo", muestra como resultados que el 86,00% de los empleados encuestados expresaron que, SI es necesario la implementación de un Sistema de Gestión de la Seguridad de la Información, mientras que un 14,00 %, señalo que SI existen procesos implementados por lo que no es necesario implementar un SGSI, esto coincide con el autor Galdámez (22), quien menciona que la tarea principal de la seguridad informática es minimizar los riesgos para obtener una mayor y mejor seguridad, estos resultados se obtuvieron porque estas empresas no ofrecen la seguridad necesaria, para la documentación de la empresa, esto conlleva a la insatisfacción de los trabajadores por sentirse vulnerables a pérdidas de información, es por eso que es recomendable resguardar la información y minimizar los riesgos.

5.3. Propuesta de mejora

Se eligió la norma ISO 270001 para realizar el SGSI, utilizando el método de análisis de riego porque se estudian la posibilidad y las consecuencias de cada factor de riesgo, con el fin de establecer el nivel de riesgo en que se encuentra la empresa a continuación, mostramos una tabla de comparación de las diferentes metodologías:

Tabla N° 19 Tabla Comparativa entre Metodologías

MAGERIT	CRAMM	OCTAVE
-Ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. -Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.	- Evaluación de impacto empresarial. -Identificación y evaluación de amenazas y vulnerabilidades. -Evaluar los niveles de riesgo entro otras.	-Desmitificar la falsa creencia: la seguridad informática es un asunto meramente. -Octave divide los activos en dos tipos sistemas y personas.

Fuente: Elaboración propia.

5.3.1. Gestión de Riesgos

La gestión de riesgo ayuda a identificar los riesgos existentes en la empresa y la necesidad de gestionarlos, así mismo permitirá a analizar los riesgos sobre el uso de las TIC y preparar a la empresa con los procesos de evaluación, auditorio y certificación o acreditación según corresponde en cada caso.

5.3.2. Inventario de Activos

Un análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado, todos los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

Tabla N° 20 Inventario de los activos

Ámbito	Activo
Instalaciones	Infraestructura
	local eléctrico, telecomunicaciones
Hardware	Servidores
	Computadoras, laptops
	Comunicadores
	Router
	Telefono
Software	Windows 2010
	Office 2013
Aplicaciones	Correos corporativos

	McAfee Antivirus
	Copias de Seguridad McAfee
Datos	Administración y Contabilidad
	Acceso a cuentas
	Registros de operaciones
	Datos de clientes y usuarios
Red	Datos
	Telefonía
	Internet.
Servicios	Luz
	Agua
	internet y Operador Claro.
	Correo Corporativo
Equipos adicionales	Generador de energía
	UPS
	Aire acondicionado
	Control de temperatura
Personal	Gerencia
	Administración
	Fiscalizador de operaciones
	Sistemas
	Almacén
Soportes de información	Discos del servidores.
	Disco de backups
	Memorias.

Fuente: Elaboración propia.

5.3.3 Valoración de Activos

En esta parte detallamos la escala de valoración de activos con el fin de tenerlos en cuenta para una mayor evaluación activos de información.

Las escalas de valoración de los activos son las siguientes categorías muy bajo, bajo, medio, alto y Muy alto.

Tabla N° 21 Valor de los activos.

MA.	Muy alta.
A.	Alta.
M.	Media.
B.	Baja.
MB.	Muy baja.

Fuente: Libro de Magerit (31).

En la siguiente tabla se establecen las abreviaturas que se utilizaran para la valoración de los activos de información, dicha valoración viene a medir la criticidad en las cinco dimensiones de la seguridad de la información manejada por el proceso de negocio. Esta valoración consiste en valorar el impacto que tendrá la materialización de una amenaza sobre la parte de activo expuestos.

Cada activo de información puede poseer un valor diferente en cada una de las diferentes dimensiones para la organización que deseemos analizar. En este caso utilizaremos una escala de valoración de diez valores siguiendo los siguientes criterios:

Tabla N° 22 Escala de valoración

Valor	Criterios
10	Muy grave
7-9	Grave
4-6	Preocupante
1-3	Menor
0	Sin daño

Fuente: Libro de Magerit (31).

A continuación, se detalla la valoración de las dimensiones de seguridad de los activos.

Tabla N° 23 Valoración de seguridad de los activos

Dimensiones de los Activos							
Ámbito	Activo	Valor	Aspectos Críticos				
			A	C	I	D	T
Instalaciones	Localización de la Empresa	Muy Alto				9	
	Local eléctrico	Alto				9	
Ha	Servidores	Alto	7	9	8	8	9
	Pc de escritorio, Portátiles	Alto	8	9	6	8	6

	Equipos de Comunicaciones	Alto	8	8	8	7	8
	Reuter.	Medio	7	7	7	7	8
Aplicaciones	Sistemas Operativos: Windows 2010	Alto	8	8	9	9	7
	Office	Alto	9	7	8	8	8
	Correo corporativo	Medio	8	7	7	7	7
	Antivirus: ESET NOD32	Alto	8	8	7	7	9
	Copias de Seguridad	Medio	8	6	7	8	5
Datos	Información en contabilización	Alto	9	6	9	9	8
	Formatos de acceso	Alto	10	10	7	5	6
	Registros de operaciones	Alto	10	7	9	10	9
	Información de proveedores	Medio	6	6	7	90	8
Red	Red de datos	Muy Alto				9	
	Red de telefonía	Alto				8	
	acceso a Internet	Medio				6	
Servicios	Internet	Medio				6	
	Telefonía	Alto				9	
	Cable de Movistar.	Alto				9	
	Correo	Alto				9	

Equipos adicionales.	Grupo electrógeno	Muy Alto				9	
	UPS	Alto				8	
	Split coge	Medio				7	
	Sistema de control de Temperatura	Alto				9	
Personal.	Gerencia	Alto		7		9	
	Personal de Administración	Alto		8		8	
	Personal para Almacén	Muy Alto		9		9	
	Personal para las atenciones medicas	Muy Alto		10		10	
	Encargado	Medio		7		8	
Soportes de Información.	Discos Servidores.	Alto	8	9	9	9	9
	Discos externos información de backups	Alto	8	8	9	6	8
	Unidades de CD, DVD y Memorias extraíbles	Medio		7	5	6	

Fuente: Elaboración propia.

5.3.4. Análisis de Amenazas

Una vez definidos los activos y su valor para la organización, se debe realizar un análisis que muestre cuales son los activos que siempre están expuestos a amenazas y estas pueden afectar a los distintos aspectos de la seguridad, para posteriormente estimar cuan vulnerable es el activo para dicha amenaza. De acuerdo con lo anterior, se procedió a realizar la clasificación de las amenazas utilizando las tablas existentes en el libro 2: catálogo de elementos de Margerit, el cual seguiré la agrupación de las amenazas en cuatro grupos.

Tabla N° 24 Análisis de amenazas

	Amenazas	Dimensión afectada					Activos Afectados							
		D	I	C	T	A	Hardware.	Red.	Instalaciones.	Aplicaciones.	Información.	Datos.	Servicios.	Personal.
Desastres Naturales.	Fuego.	✓	✓				✓	✓	✓	✓	✓	✓	✓	✓
	Daños por agua	✓					✓	✓	✓	✓	✓	✓		
	Inundación	✓					✓	✓	✓		✓			
	Siniestro mayor	✓					✓	✓	✓		✓			
	Fenómeno sísmico	✓					✓	✓	✓	✓	✓	✓	✓	✓
	Fenómeno meteorológico	✓					✓	✓	✓	✓	✓	✓	✓	✓
Accidentes de origen industrial	Fuego	✓	✓				✓	✓	✓	✓	✓	✓	✓	✓
	Daños por agua	✓					✓	✓	✓		✓			
	Sobrecarga eléctrica	✓					✓	✓	✓		✓			
	Fluctuación eléctrica	✓	✓				✓	✓		✓	✓			
	Contaminación mecánica	✓					✓							
	Contaminación electromagnética	✓					✓		✓					

	Destrucción de información	✓						✓	✓	✓		✓	✓	
	Fugas de información	✓	✓	✓						✓	✓	✓	✓	✓
	Vulnerabilidades de los programas	✓	✓							✓				
	Actualizaciones de software.		✓	✓						✓				
	Actualizaciones de equipos.		✓				✓	✓						
	Caída del sistema por agotamiento de recursos	✓	✓				✓	✓					✓	
	Pérdidas de equipos	✓	✓				✓							
	Indisponibilidad del personal.	✓	✓											✓
Amenazas intencionales presenciales	Manipulación de los registros en actividad.		✓		✓									
	Suplantación de la identidad del usuario.	✓	✓			✓		✓		✓		✓	✓	
	Abusos de privilegios de acceso	✓	✓							✓				
	Re-encaminamiento de mensajes			✓				✓		✓			✓	
	Alteración de secuencias		✓					✓		✓			✓	
	Acceso no autorizado	✓	✓				✓	✓	✓	✓	✓	✓	✓	
	Análisis de tráfico			✓				✓						✓

	Repudio		✓				✓							
	Interceptación de información (Escucha)		✓	✓				✓						
	Modificación deliberada de la información	✓	✓					✓	✓	✓	✓	✓	✓	
	Destrucción de información	✓							✓	✓		✓	✓	
	Divulgación de información		✓						✓	✓	✓	✓	✓	
	Manipulación de programas	✓	✓	✓						✓				
	Manipulación de los equipos	✓		✓			✓							
	Denegación de servicio	✓					✓	✓					✓	
	Robo	✓		✓			✓							
	Ataque destructivo	✓					✓		✓		✓			
	Indisponibilidad del personal	✓												✓
	Extorsión	✓	✓	✓										✓
	Ingeniería social	✓	✓	✓										✓

Fuente: Elaboración propia.

A continuación, se describen los proyectos planteados anteriormente.

5.3.5. Plan de Continuidad de la Empresa

Este plan busca que la empresa cuente con la habilidad para reaccionar de manera inmediata frente a una amenaza y seguir brindando sus servicios de manera normal. A continuación, se presente algunos procedimientos planteados.

- Evaluación del estado actual: En esta parte se realizó un análisis de riesgo para determinar los activos vulnerables de la empresa y determinar los procesos a seguir para protegerlos.

- Estrategia de respaldo: la empresa deberá implementar un respaldo de datos que le permita sobrevivir a cualquier inconveniente con sus instalaciones o su equipo informático.

- Desarrollo del plan: Se debe definir los equipos y procesos adecuados de alerta para un correcto funcionamiento.

- Pruebas: Se utilizarán diferentes pruebas con finalidad de verificar que el plan funciona correctamente.

- Capacitación: Se instruirá al personal a cargo con la finalidad de que obtengan un conocimiento adecuado sobre los nuevos procedimientos a seguir.

- Puesta en marcha del plan, se pone en marcha el implementar el centro de datos considerando los riesgos y soluciones del ambiente físico.

5.3.6. Plan de Capacitación

Este plan es para todo el personal de la empresa, pero con más exigencia al personal administrativo por ser el motor principal del manejo de la seguridad de información.

- Diseño del plan de sensibilización: Se encarga de diseñar estrategias de buenas prácticas de un buen manejo de información.

- Diseño del plan de capacitación: Se diseñarán los procesos de capacitación para el personal encargado de manejar la información en la empresa.

- Consecución de recursos: En esta etapa lo que se busca es financiar los recursos que se necesitan para poner en arranque el plan de sensibilización y capacitación.

5.3.7. Plan de Mitigación de Riesgos

Lo que se busca con el plan de mitigación de riesgos es limitar el impacto de las amenazas a las que se enfrenta la empresa y bloquear cualquier acceso a la información de la empresa. Se aplica una salvaguarda para implementar el plan de gestión de los riesgos existentes, con la finalidad de prevenir

perdidas de almacenamiento y la prevención de acceso no autorizado. A continuación, enumeramos diferentes normas que permitirán disminuir los riesgos en la en la empresa:

1. Confidencialidad de información privilegiado, donde los trabajadores estás prohibidos de bridar cualquier información a externos.

2. Asumir la seguridad y protección de la información de los clientes, cumpliendo con los protocoles dados por la empresa.

3. Brinda información al personal sobre la importancia del SGSI.

4. Utilizar los activos de la empresa con responsabilidad, bajo los principios de ética y moral, para protegerlos.

Por último, se han desarrollado protocolos para la mejora de procesos, aplicando medidas de seguridad con la finalidad de minimizar los riesgos que existen en la empresa. Cabe resaltar que una salvaguarda sirve como medida de emergencia para impedir que la empresa sufra una amenaza. Los resultados ayudaran a la empresa a darse cuenta que es necesario la implementación de un plan de gestión de riesgos que permiten disminuir los riesgos a los que está expuesta la empresa y así evitar pérdidas de información valiosas.

VI. CONCLUSIONES

De acuerdo a los resultados obtenidos en el presente trabajo, se concluye que hay un alto nivel de insatisfacción por parte de los trabajadores encuestados en relación al sistema actual y así mismo existe un alto nivel de aceptación de la propuesta de mejora, respecto a la implementación un plan de seguridad informática que se encargue de reguardas la seguridad de información de la empresa.

Se presentan las siguientes conclusiones:

1. Se evaluó la situación actual de los procesos de seguridad tomando en cuenta la norma ISO 27001 para la empresa, permitiendo identificar los problemas de seguridad en la información.

2. Se logró determinar el nivel de aceptación respecto a la propuesta de mejora en relación a la implementación de un plan de seguridad informática, teniendo en cuenta los resultados obtenidos en la segunda dimensión.

3. Se demostró que la evaluación de los marcos de referencia permitió proponer mejoras en la seguridad de la información en la empresa

4. Se logró realizar la propuesta de la aplicación de la Norma ISO/IEC 27001, la cual mejora la seguridad de la información en las diversas áreas tecnológicas empresa.

El aporte dentro de la investigación para la Implementación de un plan de seguridad informática con la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A - Piura, 2021. Servirá para mejorar la seguridad de información de la empresa, permitiendo llevar un mejor control en la información de la empresa.

El valor agregado para la empresa final fue, identificar las falencias existentes con respecto a la seguridad de información, con el propósito de fortalecer la seguridad y evitar futuras perdidas de información.

RECOMENDACIONES

1. Se recomienda la implementación de un plan de seguridad con la norma ISO/IEC 27001, porque permitirá mejorar la seguridad de información de sus clientes y protegerlos de cualquier amenaza.

2. Se propone que los trabajadores reciban capacitaciones sobre los procesos de seguridad con la finalidad que se adapten rápidamente al nuevo cambio.

3. Es importante que las políticas que se establecieron para mejorar la seguridad informática en la empresa sean cumplidas por todos los trabajadores, esto permitirá evaluar los riesgos y poder prevenirlos.

4. Se plantea utilizar software ISOTools para la implementación de la norma, por que ayuda a las empresas con la calidad y la excelencia a optimizar sus modelos y sistemas de gestión y facilita la aplicación de estos, haciéndolos accesibles, ágiles, medibles y aportando resultados en el corto plazo.

REFERENCIAS BIBLIOGRÁFICAS

1. Clavijo A, La Importancia De Los Sistemas De Información En Las Organizaciones Automatizadas; 2014.
2. Núñez C, Ciberdelincuencia Amenaza Latente ;2021.
3. Pilla J. Diseño de una Política de Seguridad de la Información para el área de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Chibuleo LTDA. Basado en la Norma ISO/IEC 27002; 2019
4. León L. Planificación de un SGSI basado en la Norma ISO 27001 en la Empresa Mafelesa;2008.
5. Ararat J. Diseño de un SGSI basado en la Norma ISO 27001 para la Empresa Ma Peñalosa CÍA. S.A.A; 2018.
6. Benites C. Implementación de un sistema de Gestión de Seguridad de la Información-Norma ISO 27001 para la Fábrica Radiadores Fortaleza;2019.
7. Dávila M, Evaluación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, en la municipalidad distrital de José Crespo y Castillo - Aucayacu; 2018.
8. Flores M, Diseño del sistema de gestión de seguridad de la información para el grupo SIAS SAC. de Chimbote- Perú; 2017.
9. Ancajima M. Propuesta de Implementación de Seguridad Informática en la TIC de la I.E San Miguel Arcángel, Catacaos-Piura;2019.
10. Lara B. Propuesta para la seguridad informática basado en la Norma ISO 27001 en la clínica Simedic Diagnóstica S.A.C;2018.

11. Sandoval J. Diseño de un Plan de Seguridad de Información para el Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura; 2018.

12. Empresa Ransa Comercial S.A, https://www.ransa.biz/quienes-somos/

13. Belloch C. Las Tecnologías de Información y Comunicación (TIC); 208.

14. Gonzales s. Tecnología de la Información y Comunicación; 2015.

15. Bonilla F. Tecnología de la Información y Comunicación; 2012. https://sites.google.com/site/ticsyopal5/assignments

16. Ayala E. Tecnologías de Comunicación y la Comunicación; 2015.

17. Orozco G. El concepto de la seguridad en la Teoría de las Relaciones Internacionales. CIDOB d'Afers Internacionals.

18. Bekman G. introducción a la informática. sexta ed.

19. Elizondo C. Informática 1 Patria GE, editor; 2014.

20. De Pablos H. Informática y comunicacioones en la empresa Madrid: ESIC Editorial; 2004.

21. Alegre R, Garcia. Seguridad Informática Madrid: S.A Ediciones Paraninfo; 2011.

22. Galdámez P. ITI. [Online].; 2003 [cited 2017 Junio 15. Available from: http://web.iti.upv.es/.

23. Tudón J. La medicina del trabajo y la salud ocupacional. Latinoamericana se la Salus y el Trabajo. 2014; 4(2): p. 45.

24. ISO. ISO. [Online]. [cited 2015 10 10. Available from: http://www.iso.org/.

25. Ernesto J. Importancia de la Norma ISO/EIC 27000 en la Implementacion de un sistema de gestión de la seguridad en la Información.

26. López N, Ruiz S. El Portal de ISO 27000 en español. [Online].; 2005 [cited 2017 Junio 15. Available from: http://www.iso27000.es/.

27. ISOTools Excellence. Blog especializado en Sistemas de Gestión. [Online].; 2015 [cited 2017 junio 25. Available from: http://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/.

28. Cuervo S. Implementación ISO 27001; 2017.

29. Talavera A. Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001. pregrado. Lima: Pontificia Universidad Católica del Perú, Ciencias e Ingeniería; 2013.

30. Giménez A. Seguridad en equipos informáticos. IFCT0109. primera ed. IC Editorial 2, editor. Malaga: IC Editorial; 2015.

31. Hernandez S, Fernandez C, Baptista L. Metodología de la Investigación. cuarta ed. Mexico: McGraw Hill; 2004.

32. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madird; 2012.

33. Velásquez. Metodologia de la Investigación Científica limA; 2009.Fachelli S, Metodología de la Investigación Social Cuantitativa; 2015.

34. Rodríguez M, Diseño de Investigación de Corte Transversal; 2018.

35. López P, Población Muestra y Muestreo; 2004.

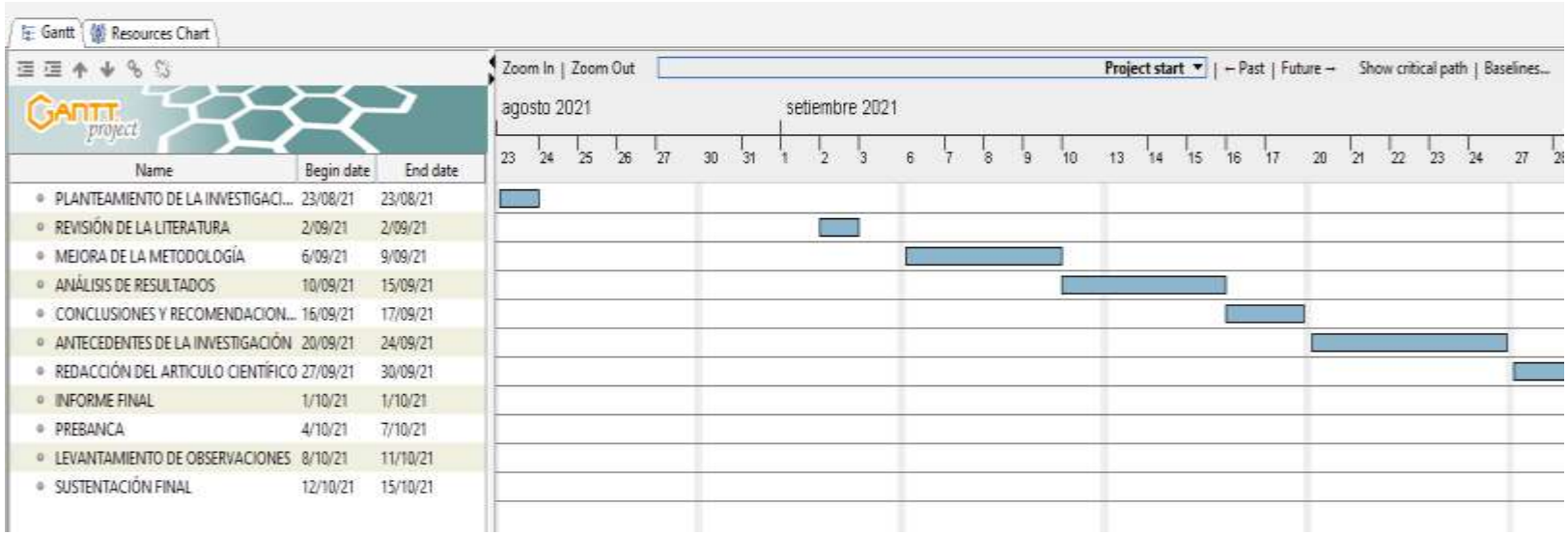
36. García F, Recomendaciones metodológicas para el diseño de cuestionario; 2002.

37. Código de Ética para la Investigación Aprobado por acuerdo del Consejo Universitario con Resolución Nº 0973-2019-CU-ULADECH Católica; 2019

38. Reglamento de investigación V017.

ANEXOS

ANEXO NRO. 1: CRONOGRAMA DE ACTIVIDADES



Fuente: Elaboración propia.

ANEXO NRO. 2: PRESUPUESTO

Presupuesto desembolsable (Estudiante)			
Categoría	**Base**	**% o Número**	**Total (S/)**
Suministros (*)			
• Impresiones			
• Fotocopias			
• Empastado			
• Papel bond A-4 (500 hojas)			
• Lapiceros			
Servicios			
• Uso de Turnitin	50.00	2	100.00
Sub total			
Gastos de viaje			
• Pasajes para recolectar información			
Sub total			
Total de presupuesto desembolsable			
Presupuesto no desembolsable (Universidad)			
Categoría	**Base**	**% ó Número**	**Total (S/.)**
Servicios			
• Uso de Internet (Laboratorio de Aprendizaje Digital - LAD)	30.00	4	120.00
• Búsqueda de información en base de datos	35.00	2	70.00
• Soporte informático (Módulo de Investigación del ERP University - MOIC)	40.00	4	160.00
• Publicación de artículo en repositorio institucional	50.00	1	50.00
Sub total			400.00
Recurso humano			
• Asesoría personalizada (5 horas por semana)	63.00	4	252.00
Sub total			252.00
Total de presupuesto no desembolsable			652.00
Total (S/.)			

Fuente: Reglamento de investigación V017 (38)

ANEXO NRO. 3: CUESTIONARIO

TÍTULO: Implementación de un plan de Seguridad Informática con la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A - Piura; 2021

ESTUDIANTE: Merino Rosas César Augusto

A. PRESENTACIÓN:

El presente instrumento forma parte del actual trabajo de investigación; por lo que se solicita su participación, respondiendo a cada pregunta de manera objetiva y veraz. La información a proporcionar es de carácter confidencial y reservado; y los resultados de la misma serán utilizados solo para efectos académicos y de investigación científica.

B. INSTRUCCIONES:

A continuación, se le presenta una lista de preguntas, agrupadas por dimensión, que se solicita se responda, marcando una sola alternativa con un aspa (“X”) en el recuadro correspondiente (SI o NO) según considere su alternativa

	PREGUNTAS	SI (x)	NO (x)
Dimensión 01: Nivel de satisfacción con el sistema actual			
1	¿Se encuentra conforme con la seguridad que ofrece la empresa?		
2	¿En la empresa, el sistema actual brinda total seguridad, para la información que se maneja?		
3	¿Considera usted que es seguro la manera como resguarda la información la empresa?		

4	¿Considera usted que una norma ISO es de suma importancia para el resguardo de información en la empresa?		
5	¿Tiene conocimiento sobre los procesos de seguridad para la información de la empresa?		
Dimensión 02: Nivel de aceptación de la propuesta de mejora.			
6	¿Estaría de acuerdo en implementar la norma ISO para la protección de la información de la empresa?		
7	¿Considera usted que al implementar la norma ISO se reforzará la seguridad de información en la empresa?		
8	¿Considera usted que al implementar la norma ISO ayudará a la empresa a ser confiable y a crecer como empresa?		
9	¿Considera usted que la implementación de la norma ISO ayudará a mejorar el servicio al cliente y mejorar la imagen de la empresa?		
10	¿Cree usted que disminuirá las pérdidas de información de contar con la norma ISO para seguridad informática en la empresa?		

Fuente: Elaboración propia

ANEXO NRO. 4: FICHAS DE VALIDACIÓN DE INSTRUMENTO

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : JORGE LUIS GUTIERREZ GUTIERREZ
1.2 Cargo e institución donde labore : UNIVERSIDAD CATOLICA LOS ANGELES DE CHIMBOTE
1.3 Nombre del instrumento evaluado : FICHA DE EVALUACION
1.4 Autor del instrumento : CESAR MERINO ROSAS

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si mas del 70% de los ítems cumplen con el indicador).

Aspectos de validación del instrumento		1	2	3	Observaciones
Criterios	Indicadores	D	R	B	Sugerencias
• Pertinencia	Los ítems miden lo previsto en los objetivos de investigación.	☐	X	☐	
• Coherencia	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	☐	X	☐	Algunos ítems deben presentar las alternativas en escala de likert
• Congruencia	Los ítems son congruentes entre si y con el concepto que mide.	☐	☐	X	
• Suficiencia	Los ítems son suficientes en cantidad para medir la variable.	☐	X	☐	
• Objetividad	Los ítems se expresan en comportamientos y acciones observables.	☐	☐	X	
• Consistencia	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	☐	X	☐	
• Organización	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	☐	☐	X	
• Claridad	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	☐	X	☐	
• Formato	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	☐	☐	X	
• Estructura	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	☐	☐	X	
CONTEO TOTAL (Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)		C	B	A	Total

Coeficiente de validez : $\frac{A + B + C}{30} = 0.83$

Intervalos	Resultado
0,00 – 0,49	- Validez nula
0,50 – 0,59	- Validez muy baja
0,60 – 0,69	- Validez baja
0,70 – 0,79	- Validez aceptable
0,80 – 0,89	- Validez buena
0,90 – 1,00	- Validez muy buena

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escribe sobre el espacio el resultado.

Buena

Piura, Noviembre del 2020.

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : Jonathan Joel Purizaca Pingo

1.2 Cargo e institución donde labore : Gerente General - QoriLab

1.3 Nombre del instrumento evaluado : Cuestionario

1.4 Autor del instrumento : Merino Rosas Cesar

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigne a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Aspectos de validación del instrumento		1	2	3	Observaciones
Criterios	Indicadores	D	R	B	Sugerencias
• Pertinencia	Los ítems miden lo previsto en los objetivos de investigación.	☐	☐	☒	
• Coherencia	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	☐	☒	☐	
• Congruencia	Los ítems son congruentes entre sí y con el concepto que mide.	☐	☒	☐	
• Suficiencia	Los ítems son suficientes en cantidad para medir la variable.	☐	☒	☐	
• Objetividad	Los ítems se expresan en comportamientos y acciones observables.	☐	☐	☒	
• Consistencia	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	☐	☒	☐	
• Organización	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	☐	☐	☒	
• Claridad	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	☐	☒	☐	Revisar redacción.
• Formato	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	☐	☒	☐	Revisar redacción.
• Estructura	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	☐	☐	☒	
CONTEO TOTAL (Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)		0	12	12	
		C	B	A	Total

Coeficiente de validez : $\frac{A+B+C}{30} = \frac{0+12+12}{30} = 0.8$

Intervalos	Resultado
0,00 – 0,49	• Validez nula
0,50 – 0,59	• Validez muy baja
0,60 – 0,69	• Validez baja
0,70 – 0,79	• Validez aceptable
0,80 – 0,89	• Validez buena
0,90 – 1,00	• Validez muy buena

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Validez buena

Piura, Noviembre del 2020.

JONATHAN JOEL PURIZACA PINGO
INGENIERO DE SISTEMAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : EDUARDO RAÚL PÉREZ ZAMORA
1.2 Cargo e institución donde labora : DOCENTE TUTOR. ULADECH PIURA
1.3 Nombre del instrumento evaluado : FICHA DE VALIDACIÓN
1.4 Autor del instrumento : MERINO ROSAS CESAR

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Aspectos de validación del instrumento		1	2	3	Observaciones
Criterios	Indicadores	D	R	B	Sugerencias
+ PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	☐	X	☐	
+ COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	☐	X	☐	
+ CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.	☐	X	☐	
+ SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	☐	☐	X	
+ OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	☐	☐	X	
+ CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	☐	☐	X	
+ ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	☐	☐	☐	
+ CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	☐	X	☐	
+ FORMATO	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	☐	X	☐	
+ ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	☐	X	☐	
CONTEO TOTAL (Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)		C	B	A	Total

Coeficiente de validez : $\frac{A + B + C}{30} = 1,4$

Intervalos	Resultado
0,00 – 0,49	- Validez nula
0,50 – 0,59	- Validez muy baja
0,60 – 0,69	- Validez baja
0,70 – 0,79	- Validez aceptable
0,80 – 0,89	- Validez buena
0,90 – 1,00	- Validez muy buena

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Muy buena

Piura, Noviembre del 2020.

EDUARDO RAUL PEREZ ZAMORA
INGENIERO EN COMPUTACIÓN E INFORMÁTICA
Reg. CIP N° 212391

ANEXO NRO. 5: CONCENTIMIENTO INFORMADO

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS

(Ingeniería y Tecnología)

La finalidad de este protocolo en Ingeniería y tecnología es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, el investigador y usted se quedarán con una copia.

La presente investigación se titula Implementación de un plan de seguridad informática con la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A - Piura, 2021 y es dirigido por Cesar Augusto Merino Rosas, investigador de la Universidad Católica Los Ángeles de Chimbote.

El propósito de la investigación es: proponer la implementación de un plan de seguridad informática con la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A - Piura, 2021, para mejorar la seguridad de información de sus clientes.

Para ello, se le invita a participar en una encuesta que le tomará 5 minutos de su tiempo. Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través de su correo electrónico. Si desea, también podrá escribir al correo rosascesar512@gmail.com para recibir mayor información. Asimismo, para consultas sobre aspectos éticos, puede comunicarse con el Comité de Ética de la Investigación de la universidad Católica los Ángeles de Chimbote.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: Arturo

Fecha:

Correo electrónico:

Firma del participante:

Firma del investigador (o encargado de recoger información):