UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

DIAGNÓSTICO DE LA SEGURIDAD INFORMÁTICA UTILIZANDO LA NORMA ISO/IEC 27001 DE LA EMPRESA RANSA COMERCIAL S.A- PIURA; 2020.

TRABAJO DE INVESTIGACIÓN PARA OPTAR EL GRADO ACADÉMICO DE BACHILLER EN INGENIERÍA DE SISTEMAS

AUTOR

MERINO ROSAS, CESAR AUGUSTO

ORCID: 0000-0001-6174-8168

ASESOR

CORONADO ZULOETA, OSWALDO GABIEL

ORCID: 0000-0002-0708-2286

PIURA – PERÚ
2021

EQUIPO DE TRABAJO

AUTOR

Merino Rosas, César Augusto

ORCID: 0001-6174-8168

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

ASESOR

Coronado Zuloeta, Oswaldo Gabiel

ORCID: 0000-0002-0708-2286

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

JURADO

Sullón Chinga, Jennifer Denisse

ORCID: 0000-0003-4363-0590

Sernaqué Barrantes Marleny

ORCID: 0000-0002-5483-4997

García Córdova, Edy Javier

ORCID: 0000-0001-5644-4776

HOJA DE FIRMA DEL JURADO YASESOR

MGTR. SULLÓN CHINGA JENNIFER DENISSE

PRESIDENTE

DR. MGTR. SERNAQUÉ BARRANTES MARLENY

MIEMBRO

MGTR. GARCÍA CÓRDOVA EDY JAVIER

MIEMBRO

MGTR. CORONADO ZULOETA OSWALDO GABIEL

ASESOR

DEDICATORIA

A mis padres, por haberme forjado como la persona que soy en la actualidad, por brindarme consejos y todo su apoyo.

A mi esposa, porque tu ayuda ha sido fundamental, has estado conmigo incluso en los momentos más turbulentos y su incondicional apoyo en mi carrera.

A mi hija, tu afecto y cariño son los detonantes de mi felicidad, de mi esfuerzo, de mis ganas de buscar lo mejor para ti. Eres mi motivación más grande para concluir con éxito este proyecto.

César Augusto Merino Rosas

AGRADECIMIENTO

En primer lugar, agradezco a Dios, porque es el único dueño de todo saber y verdad, por iluminarnos durante este trabajo y por permitirnos finalizarlo con éxito.

A la Universidad Católica los Ángeles de Chimbote que nos inculca cada día más en la investigación y el desarrollo de nuevas soluciones.

A la empresa Ransa Comercial S.A por permitir explorar e investigar el área de control de operaciones de la gerencia de construcción.

César Augusto Merino Rosas

RESUMEN

El presente trabajo ha sido desarrollado bajo la línea de investigación: Sistemas de gestión de calidad y seguridad de la información para la mejora continua de las organizaciones del Perú, de la escuela profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote Sede en Piura. Tuvo como objetivo realizar el diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A – Piura; 2020. El tipo de investigación utilizado fue cuantitativo, de nivel descriptivo, el diseño fue de tipo no experimental y de corte transversal. Los resultados obtenidos en la dimensión 01: Nivel de satisfacción con el sistema actual; el 87% de los trabajadores encuestados NO están satisfechos con el sistema actual, en la dimensión 02: Nivel de aceptación de la propuesta de mejora; se observó que el 100% de los encuestados SI necesitan de una propuesta de mejora. Y en la dimensión 03: Nivel de conocimiento de Tecnologías de la Información y la Comunicación; el 67% de los trabajadores encuestados NO tiene conocimiento acerca de las TIC. Se concluyó que el diagnóstico para la seguridad informática basada en la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A – Piura; 2020, mejoró los procesos de seguridad, confiabilidad y disponibilidad de la información.

Palabras Claves: confidencialidad, gestión, información, seguridad.

ABSTRACT

This work has been developed under the research line: Information security and quality management systems for the continuous improvement of Peruvian organizations, from the professional school of Systems Engineering of the Universidad Católica Los Ángeles de Chimbote Headquarters in Piura. Its objective was to carry out the diagnosis of computer security using the ISO / IEC 27001 standard in the company Ransa Comercial S.A - Piura; 2020. The type of research used was quantitative, descriptive, the design was non-experimental and cross-sectional. The results obtained in dimension 01: Level of satisfaction with the current system; 87% of the workers surveyed are NOT satisfied with the current system, in dimension 02: Level of acceptance of the improvement proposal; It was observed that 100% of the respondents DO need an improvement proposal. And in dimension 03: Level of knowledge of Information and Communication Technologies; 67% of the workers surveyed have NO knowledge about ICT. It was concluded that the diagnosis for computer security based on the ISO / IEC 27001 standard in the company Ransa Comercial S.A - Piura; 2020, improved the security, reliability and availability of information processes.

Keywords: confidentiality, management, information, security.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

INTRODUCCIÓN

Los años pasan para todos, incluso para la tecnología. Es por esta razón que evoluciona para mantenerse relevante en un mundo donde el estancamiento implica quedar obsoleta. Lejos ha quedado el siglo XX, aquellos años donde una simple red de par de cobre era suficiente para garantizar servicios a los usuarios por décadas. Un mundo distante donde las redes nómadas y móviles por medio de tecnologías analógicas también tardaron varias generaciones en desaparecer. Ahora las telecomunicaciones requieren una inversión constante, sobre todo si la plataforma utilizada es inalámbrica. Hoy en día la seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas (1).

La empresa Ransa Comercial S.A, ejecuta todos sus procesos en Excel, lo que significa que no tienen control sobre sus clientes y los documentos de gestión que entran y salen de la empresa. Una parte importante del trabajo y el tiempo del personal se dedica a investigar y asimilar información, por lo que no es posible mantener el equilibrio y el control de los diferentes clientes. Por otro lado, la empresa gestiona la información personal de sus clientes, por lo que debe protegerse para garantizar una atención confiable y sin riesgos.

Debido a las inconsistencias encontradas en la empresa se planteó la siguiente pregunta: ¿De qué manera el diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A - Piura, 2020; permite mejorar la gestión en la seguridad de los activos de información?

La Investigación tuvo como objetivo general implementar un diagnóstico de seguridad informática utilizando la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A - Piura, 2020, para mejorar la calidad del servicio. Se plantearon los

siguientes objetivos específicos:

1. Identificar la existencia de los riegos considerando la seguridad de la información en la empresa Ransa Comercial S.A - Piura, 2020.
2. Evaluar los mecanismos de seguridad, después de localizar los riesgos en los activos de información que enfrenta la empresa.
3. Analizar las diferentes normas internacionales basadas en la seguridad de información para la empresa Ransa Comercial S.A - Piura, 2020.
4. Analizar las metodologías de evaluación y riesgos informáticos.

El trabajo se realiza en el área de seguridad informática en la empresa Ransa Comercial S.A – Piura. La investigación es de tipo cuantitativa, nivel descriptivo y diseño no experimental de corte transversal.

Este trabajo se justifica tecnológicamente, por la necesidad de tener una descripción clara del nivel de gestión del proceso, esto permitirá evaluar un Sistema de Gestión de Seguridad aplicando la norma ISO/IEC 27001 en la empresa. Operativamente se justifica, por la necesidad de tener claro los procesos de está, esto permitirá evaluar un sistema de gestión de seguridad aplicando la norma ISO/IEC27001 en la empresa. Se justifica económicamente, para garantizar que los riesgos sean conocidos, asumidos, gestionados y minimizados por la empresa de una forma documentada, sistemática, estructurada, eficiente y adaptada en los cambios que se produzcan.

De acuerdo a la encuesta se obtuvo resultados donde; el 86.67% de los encuestados manifestaron que, NO están satisfechos con el sistema actual y el 100,00% de los encuestados manifestaron que, SI están de acuerdo con la propuesta de mejora de la

seguridad de información en la empresa ya que el 66,67% de los encuestados manifestaron que, NO tienen conocimiento acerca de las tecnologías de la información y la comunicación para para mejorar la gestión en los activos de información.

Se utilizó para la presente investigación, una metodología de tipo descriptiva y un enfoque cuantitativo, además el diseño fue no experimental y de corte transversal.

Se concluye, que existe un alto nivel de insatisfacción respecto al sistema actual de la empresa Ransa S.A, asimismo existe un alto nivel de necesidad de realizar un diagnóstico de seguridad informática utilizando la norma ISO/IEC 27001, permitiendo mejorar los procesos de seguridad, confiabilidad y disponibilidad de la información en la empresa Ransa Comercial S.A, generando de esta manera la satisfacción de los trabajadores con esta propuesta, a partir de ello concluyo indicando que la hipótesis general queda debidamente aceptada.

I. REVISION DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes Internacional

León (2), 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 (3), 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.

Pilla (4), 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.

2.1.2 Antecedentes Nacional

Benites (5) 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 (6), 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 (7), 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 Regional

Ancajima (8), 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 (9), 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 (10), 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

2.2.1. Empresa

2. 2.1.1. Definición

Es un negocio, un conjunto de actividades cuyo propósito es varios. Desde un punto de vista financiero, tiene que ganar dinero para garantizar su vida, pero para ganar dinero no hay límites y las metas deben ser. De esta manera, el beneficio recibido regresa a los propietarios, y a veces también a los gerentes y empleados, en la medida en que logran los objetivos (gestión de objetivos). Las empresas obtienen productos

(bienes y servicios) de los factores de producción (mano de obra, capital y materias primas) que intercambian en el mercado, ya sea por otros productos o por dinero (11).

2.2.2. Información de la empresa Investigada

2.2.2.1. Rubro de la empresa

Operador logístico con más de 80 años en el mercado brindando soluciones logísticas: distribución, almacenamiento (incluso aduanero) y gestión de órdenes y suministro (12).

Gráfico Nro. 1: Ransa Comercial S.A

Fuente: Google Maps (13).

2.2.2.2. Reseña Histórica

Ransa Comercial S.A es un operador logístico líder del Perú con más de 7,000 colaboradores altamente capacitados y especializados para atender los requerimientos específicos de nuestros clientes en cada sector económico, convirtiéndonos en socios estratégicos en la logística de nuestros clientes. 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. Ubicación

La empresa se ubica en la Carretera Piura Sullana km.03-26 de Octubre-Piura

Gráfico Nro. 2: Ubicación de la Empresa Ransa Comercial S.A

Fuente: Google Maps (13).

2.2.2.4. Funciones

La empresa Ransa Comercial S.A- Piura cuenta con las siguientes funciones (12):

- Manejo de inventario
- Almacenes especializados
- Planeamiento de pedidos
- Alquiler de contenedores

2.2.2.5. Misión

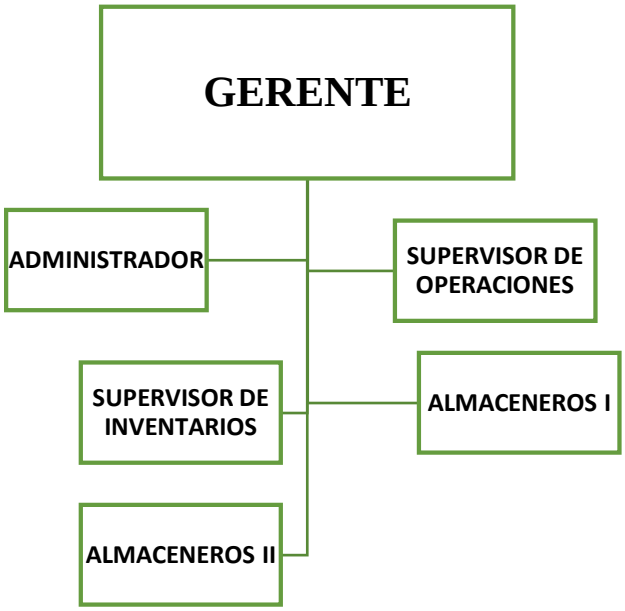
Dar soluciones por sector económico, brindando servicios logísticos secos y refrigerados, también dar servicios de manejo de información, digitalización y documentación de archivos (12).

2.2.2.6. Visión

Su visión es ser la empresa que de líder mediante la gestión de soluciones logísticas creativas diseñadas especialmente para atender y optimizar los requerimientos específicos de su cadena de abastecimiento en cada sector económico (12).

2.2.2.6. Organigrama

Gráfico Nro. 3: Organigrama de la Empresa Ransa Comercial S.A



Fuente: Empresa Ransa Comercial S.A (12)

2.2.2.8. Infraestructura Tecnológica

Tabla Nro. 1: Infraestructura Tecnológica

Departamento	Descripción	Cantidad	Características	S.O	Antivirus	Office
Gerencia	Laptop	3	LENOVO Corel i5-4130 RAM 4GB DD. 1TB	WIN 8	NOD 32	Office 2013
Logística	PC	5	PC Compatible Corel i3-4130 RAM 4GB DD. 1TB	WIN 7	NOD 32	Office 2010
Almacén	PC	2	PC Compatible Corel i3-4130 RAM 4GB DD. 1TB	WIN 7	NOD 32	Office 2010

Fuente: elaboración personal

2.2.3. Tecnologías de la información y comunicaciones (TIC)

2.2.3.1. Definición

Las Tecnologías de la Información y la Comunicación se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las telecomunicaciones. Es el conjunto de tecnologías que permiten el acceso de información presentada en diferentes códigos. El elemento más representativo es el ordenador y más específicamente, Internet. Las TIC están presentes en todos los niveles de nuestra sociedad actual, desde las grandes empresas multinacionales, pymes, gobiernos, administraciones, universidades, etc. Son tecnologías que se han convertido en imprescindibles para muchas personas y empresas (14).

Las TIC, son tecnologías que se utilizan 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 (15).

2.2.3.2. Historia

Iniciada en la década de los 70. Los avances científicos en el campo de la electrónica tuvieron dos consecuencias inmediatas: la caída vertiginosa de los precios de las materias primas y la preponderancia de las Tecnologías de la Información. Desde entonces, los criterios de éxito para una organización dependen cada vez en gran medida de su

capacidad para adaptarse a las innovaciones tecnológicas y de su habilidad para saber explotarlas en su propio beneficio. 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 (16).

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, como en los medios físicos, con mayor velocidad y capacidad de procesamiento y almacenamiento de la información que cualquier tipo de digitalización. 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 (17).

2.2.3.4. Ventajas y Desventajas de las TIC:

- Comunicación inmediata.
- Ahorro de tiempo.
- Acceso de información.
- Ciberseguridad
- Distracción de información.

2.2.3.5. Las Tic más utilizadas en la empresa:

- Office
- Google Chrome
- Facebook
- Portal De Transparencia
- Correos Corporativos.
- Búsqueda de Información
- Internet

2.2.4. Tecnología de la investigación

2.2.4.1. Sistema de Gestión Administrativa

Un Sistema de Gestión Administrativa (SGA) debe proveer información razonada, en base a registros técnicos, de las operaciones realizadas por la empresa con el fin de interpretar sus resultados. Estos datos permitirán conocer la estabilidad y solvencia de la compañía, la situación de cobros y pagos, las tendencias de las ventas, costes y gastos generales, entre otros. De este modo se podrá conocer la capacidad financiera de la empresa y tomar decisiones estratégicas en base a datos reales (18).

2.2.4.2. Seguridad

El concepto de seguridad no se restringe únicamente a la garantía de la existencia física, sino que va más allá y se extiende, también, a la estabilidad social que permite disfrutar

de una vida libre de amenazas. El trabajo conceptual que realiza el autor es un punto de inflexión en la filosofía política, ya que pone a la seguridad como una de las causas del establecimiento del Estado moderno, buscando la protección del individuo y la satisfacción del bienestar general como justificación para su supervivencia (19).

La seguridad es un tema muy importante para cualquier empresa, este o no conectada a una red pública. No solamente es importante, sino que también puede llegar a ser compleja. Los niveles de seguridad que se pueden implementar son muchos y dependerá del usuario hasta donde quiera llegar. La seguridad no solo es una garantía física, sino es algo más grande que nos permitirá tener una vida libre de amenazas, buscando la protección del individuo y la satisfacción del bienestar. Por otro lado, Goerge se enfoca en que la seguridad no es solo un tema importante, sino que es fundamental para el usuario existen diferentes niveles de seguridad que se deben implementar y eso solo depende del usuario para proteger su información (20).

2.2.4.3. Informática

Según Elizondo (21), en su libro titulado "Informática 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 procesamientos de información y sus implicaciones económicas, políticas y socioculturales. El

término informático es el acrónimo de información automática, y proviene del vocablo francés informatique.

Por otro lado, De pablos (22), define la informática como "El conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores".

2.2.4.4. 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 (23).

2.2.4.5. 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 y se pueden clasificar en las siguientes categorías (24).

- Activos de información
- Documentos de papel
- Activos de software
- Personal
- Imagen de la empresa
- Servicios

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. Estándar de gestión de la seguridad de la información

- Norma ISO

Según Hobbes pone la seguridad como uno de las causas del estado moderno, buscando la protección y la satisfacción del bienestar general del individuo como justificación para su supervivencia (25).

- ISO

  Es una organización no gubernamental, independiente, cuyos 163 miembros son los organismos nacionales de normalización. A través de sus miembros, la organización reúne a expertos que ponen sus conocimientos conjuntamente para desarrollar estándares internacionales, apoyo a la innovación relevante para el mercado, basado en el consenso voluntario y que ofrecen soluciones a los problemas mundiales (25).

- Estándar

  Una norma es un documento que proporciona requisitos, especificaciones, directrices o características que pueden ser utilizadas consistentemente para asegurar que los materiales, productos, procesos y servicios son adecuados para su propósito. Hemos publicado más de 19 500 Normas Internacionales que se pueden comprar en la tienda de la ISO o de nuestros miembros (25).

- Beneficios de las normas internacionales

  Normas Internacionales de traer beneficios tecnológicos, económicos y sociales. Ayudan a armonizar las especificaciones técnicas de los productos y servicios que hacen la industria más eficiente y rompiendo las barreras al comercio internacional. Conformidad con las Normas Internacionales de ayuda a tranquilizar a los consumidores

que los productos sean seguros, eficientes y bueno para el medio ambiente (25).

2.2.4.7. 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: Norma que contiene definiciones y términos utilizados en toda la familia de normas ISO 27000.

- ISO27001: El estándar, que contiene y proporciona los requisitos del SGSI, enumera los objetivos de control al implementar el SGSI.

- ISO27002: Incluye un manual de mejores prácticas para gestionar la seguridad de la información. No es un estándar certificable.

- ISO27003: Proporciona una serie de pautas para la implementación del SGSI y es compatible con 27001, no es un estándar certificable.

- ISO27004: Proporciona instrucciones para crear y utilizar métricas y métodos de medición que se

utilizan para determinar la efectividad del SGSI. No es un estándar certificable.

- ISO27005: Proporciona pautas para administrar los riesgos de seguridad de TI, apoyando 27001 en el proceso de administración de riesgos.

- ISO27006: Estándar que proporciona requisitos para la acreditación de organizaciones que acreditan y auditan sistemas de gestión de seguridad de la información.

- ISO27007: Manual con pautas para probar sistemas de gestión de seguridad de la información.

- ISO27011: Guía de administración de seguridad en gestión de telecomunicaciones.

- ISO27031: Norma que describe los procesos y métodos necesarios para resaltar e identificar los aspectos que se utilizan para implementar las TIC a fin de garantizar la continuidad del negocio.

- ISO27032: Proporciona un marco seguro para el intercambio de información, la gestión de incidentes y la coordinación para hacer que los procesos sean más seguros.

- ISO27033: Standard se basa en la gestión de la seguridad de las redes de datos de la organización, teniendo en cuenta las secciones de gestión de su seguridad, el diseño de su arquitectura de seguridad, los marcos de referencia, el uso de la puerta de enlace, el control de acceso remoto y el uso de VPN

y el diseño y La implementación de la seguridad de la red.

- ISO27034: Estándar que proporciona una guía de seguridad de la aplicación.

- ISO27799: Estándar que proporciona un estándar para la gestión de la seguridad de la información en el sector de la salud, el establecimiento de controles y buenas prácticas que deben implementar las empresas del sector de la salud.

2.2.4.8. 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 muchas compañías tienen cumplimiento certificado (27).

2.2.4.9. Funcionamiento de la ISO 27001

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) .Por lo tanto, la filosofía principal de la norma ISO27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente. Las medidas de seguridad (o controles) que se implementarán generalmente se presentan en forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipo). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero lo usan de manera incierta; por lo tanto, la mayor parte de la implementación de ISO27001 estará relacionada con el establecimiento de las reglas de la organización (por ejemplo, redacción de documentos) necesarias para evitar infracciones de seguridad (28).

2.2.4.10. La Normativa ISO/IEC 27001:2013

Es un modelo de gestión de seguridad de la información, que permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos Se basa en la norma ISO 27001 publicada en 2005, corregida y desarrollada en 2013. Su origen se basa en BS 7799-2: 2002 y es la norma de certificación para sistemas de gestión de seguridad. (29).

2.2.4.11. 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:

MAGERIT

Son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico. MAGERIT se encuentra muy relacionada con la generación en la que se utilizan los medios electrónicos, informáticos y telemáticos, lo que genera grandes beneficios para los empleados y los ciudadanos (30).

OCTAVE

Giménez (31), nos da a conocer sobre Octave que significa Operationally Critical Threat, Asset and Vulnerability Evaluation. El método está desarrollado por la universidad de Canegie Mellon, y define un conjunto de criterios, para poder emplear métodos más flexibles según la empresa. Existen tres métodos muy comunes que cumplen esos criterios de compatibilidad: El método de Octave original,

el Octaves-s para pequeñas empresas, y el Octave-Allegro, especialmente centrado en los activos de información. Los criterios son bastantes generales, e incluyen; que las medidas sean adaptables a las necesidades, que el proceso de análisis esté definido, sea continuo y tenga visión de futuro, y que el proceso se centre en un conjunto reducido de riesgos críticos. Los resultados se dividen en diferentes fases: fase organizativa (activos críticos y sus requerimientos, amenazas, y prácticas de seguridad habituales), una fase tecnológica (componentes clave y vulnerabilidades), es una tercera y última fase estratégico, o de desarrollo del plan de riesgo.

CRAMM

Es un método estructurado y coherente para la identificación y la evaluación de riesgos en redes y sistemas de información. Abarca escenarios técnicos y no técnicos, proporciona un método riguroso por etapas que permite programar adecuadamente las revisiones (31).

VALORACIÓN DE LAS AMENAZAS

Para realizar la evaluación de los activos, esta metodología nos brindas como valorizar las amenazas de un activo de la siguiente manera (32):

Tabla Nro.2: 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)

II. HIPOTESIS

3.1. Hipótesis general

El diagnóstico de la Seguridad Informática utilizando la norma ISO/IEC 27001 de la Empresa Randa Comercial S.A- Piura, mejorará la gestión en los activos de información.

3.2. Hipótesis especificas

1. El evaluar las necesidades de la seguridad informática de la empresa Ransa Comercial S.A. permitirá determinar el diagnóstico de la seguridad informática.

2. El determinar las herramientas y métodos permitirá desarrollar la propuesta en la empresa Ransa Comercial S.A.

3. La aplicación de la norma ISO/IEC 27001 permitirá desarrollar la propuesta en la empresa Ransa Comercial S.A.

III. METODOLOGÍA

4.1. Diseño de la investigación

La investigación tiene un diseño de tipo no experimental, de corte transversal.

Según Sampieri, Fernández y Baptista (33), 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.

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, en el año 2015 (34).

El esquema del diseño de la investigación tendrá la siguiente estructura:

M ⟶ O

Dónde:

M = Muestra

O = Observación

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 (35).

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 (35).

4.2. Población y Muestra

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 (36).

La Empresa Ransa Comercial S.A – Piura, cuenta con 17 trabajadores dispersos en las diferentes áreas de la empresa.

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 (36).

Excluyendo a los trabajadores de limpieza, 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.

4.3. Definición operacional de las variables e indicadores

Tabla Nro. 3: Definición y Operacionalización de las variables

Variable	Definición Conceptual	Dimensiones	Indicadores	Escala medición	Definición Operacional
Diagnóstico de la Seguridad Informática utilizando la Norma ISO/IEC 27001 de la empresa Ransa Comercial S.A-Piura; 2020.	La seguridad informática es un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un Sistema informático. La seguridad informática se caracteriza por la protección de datos y de comunicaciones	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	• Si • No
		Nivel de aceptación de la propuesta de mejora	Crees que se debe de mejorar la seguridad informática de sus documentos. -Sería adecuado contar con seguridad de información.		

	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 (22).		-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.	Ordinal	
		Nivel de conocimiento de Tecnologías de la Información y la Comunicación (TIC).	Tiene conocimientos acerca de Norma ISO 27001. -Usted ha recibido alguna capacitación de seguridad Informática. -Usted podrá seguir los protocolos de seguridad informática. -Cree que el sistema de gestión basado en la ISO 27001 ayudara en la seguridad de información en la empresa. -Usted está de acuerdo en recibir capacitación sobre seguridad informática y la Norma ISO27001.		

Fuente: elaboración propia

4.4. Técnicas e instrumentos de recolección de datos

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 (37).

Como instrumento de recolección de datos se usó el cuestionario.

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 (37).

4.5. 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.

4.6. Matriz de Consistencia

Tabla Nro. 4: Matriz de Consistencia

PROBLEMA	OBJETIVO GENERAL	HIPÓTESIS GENERAL	VARIABLES	METODOLOGIA
¿De qué manera el diagnóstico de la seguridad informática basada en la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A - Piura, 2020; permite mejorar la gestión en la seguridad de	Realizar el diagnóstico para la 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. Identificar la existencia de los riegos considerando la seguridad de la información en la empresa Ransa Comercial S.A - Piura, 2020. 2. Evaluar los mecanismos de	El diagnóstico de la Seguridad Informática utilizando la norma ISO/IEC 27001 de la Empresa Ransa Comercial S.A- Piura, permitirá mejorar la gestión en los activos de información **HIPÓTESIS ESPECÍFICO** 1. El evaluar las necesidades de la seguridad informática de la empresa Ransa Comercial S.A. permitirá determinar el diagnóstico de la seguridad informática.	Diagnóstico de la seguridad informática basada en la norma ISO/IEC 27001	**Nivel:** investigación será de un enfoque cuantitativo. **Tipo:** Descriptivo **Diseño:** Investigación no experimental

los activos de información?	seguridad, después de localizar los riesgos en los activos de información que enfrenta la empresa. 3. Analizar las diferentes normas internacionales basadas en la seguridad de información para la empresa Ransa Comercial S.A - Piura, 2020. 4. Analizar las metodologías de evaluación y riesgos informáticos.	2. El determinar las herramientas y métodos permitirá desarrollar la implementación en la empresa Ransa Comercial S.A. 3. La aplicación de la norma ISO/IEC 27001 permitirá desarrollar la propuesta en la empresa Ransa Comercial S.A.		

Fuente: Elaboración propia

4.7. Principios éticos

Durante la elaboración de esta investigación, teniendo como título: Diagnóstico de la Seguridad Informática utilizando la Norma ISO/IEC 27001 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:

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 (38).

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 (38).

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 (38).

Beneficencia no maleficencia: Se debe asegurar el bienestar de los participantes de la investigación (38).

Justicia: El investigador está obligado a tratar con equidad a aquellas personas que son partícipes en los procesos y servicios asociados a la investigación (38).

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 (38).

IV. RESULTADOS

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

Tabla Nro.5: Satisfacción de seguridad

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca de la satisfacción de la seguridad informática brindada, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

Alternativas	n	%
Si	4	26,67
No	11	73,33
Total	15	100,00

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Se encuentra satisfecho con la seguridad brindada para su información en la empresa Ransa Comercial S.A?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.5, se observa que, el 73,33% de los encuestados manifestaron que, NO están satisfechos con la seguridad brindada

para su información en la empresa Ransa Comercial S.A, mientras que, el 26,67% de los encuestados manifestaron todo lo contrario.

Tabla Nro.6: Sistema actual

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca si el sistema actual que beneficia la seguridad de información de sus clientes, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

Alternativas	n	%
Si	2	13,33
No	13	86,67
Total	15	100,00

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿El sistema actual beneficia la seguridad de información de sus clientes en la empresa Ransa Comercial S.A?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.6, se observa que, el 86,67% de los encuestados manifestaron que, el sistema actual NO beneficia la seguridad de información de sus clientes en la empresa Ransa Comercial S.A,

mientras que, el 13,33% de los encuestados manifestó todo lo contrario.

Tabla Nro.7: Manejo de Seguridad

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca del sistema actual que maneja la seguridad de su información de forma segura, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

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

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Considera usted que en empresa Ransa Comercial S.A, el sistema actual maneja la seguridad de su información de forma segura?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.7, se observa que, el 80,00% de los encuestados manifestaron que, en la empresa Ransa Comercial S.A el sistema actual NO se maneja la seguridad de su información de forma segura, mientras que, el 20,00% de los encuestados manifestó todo lo contrario.

Tabla Nro.8: Necesidad de Norma ISO

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca de necesitar una norma ISO para dar seguridad a la información, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

Alternativas	n	%
Si	5	25,00
No	15	75,00
Total	20	100,00

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Cree usted que se necesita una norma ISO para dar seguridad a la información a la empresa Ransa Comercial S.A?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.8, se observa que, el 75% de los encuestados manifestaron que, NO se necesita una norma ISO para dar seguridad a la información a la empresa Ransa Comercial S.A, mientras que, el 25% de los encuestados manifestaron todo lo contrario.

Tabla Nro.9: Pasos de seguridad

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca de cuáles son los pasos para la seguridad de su información, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

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

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Sabe cuáles son los pasos para la seguridad de su información en la empresa Ransa Comercial S.A?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.9, se observa que, el 80% de los encuestados manifestaron que, NO saben cuáles son los pasos para la seguridad de su información en la empresa Ransa Comercial S.A, mientras que, el 20% de los encuestados manifestaron todo lo contrario.

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

Tabla Nro.10: Utilización de norma ISO

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca si están de acuerdo en utilizar una norma ISO para dar seguridad a la información, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

Alternativas	n	%
Si	14	93,33
No	1	6,67
Total	15	100,00

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Estaría de acuerdo en utilizar una norma ISO para dar seguridad a la información de la empresa Ransa Comercial S.A?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.10, se observa que, el 93,33% de los encuestados manifestaron que, SI se necesita una norma ISO para dar seguridad a la información a la empresa Ransa Comercial S.A, mientras que, el 6,67% de los encuestados manifestaron todo lo contrario.

Tabla Nro.11: Mejora de seguridad

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca si están de acuerdo que al utilizar la norma ISO para mejorar la seguridad de información ayudara a la empresa, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

Alternativas	n	%
Si	14	93,33
No	1	6,67
Total	15	100,00

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Está usted de acuerdo que al utilizar la norma ISO para mejorar la seguridad de información ayudara a la Empresa Ransa Comercial S.A?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.11, se observa que, el 93,33% de los encuestados manifestaron que, SI se necesita una norma ISO para dar seguridad a la información a la empresa Ransa Comercial S.A, mientras que, el 6,67% de los encuestados manifestaron todo lo contrario.

Tabla Nro.12: Confiabilidad y Productividad

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca que la norma ISO en la seguridad informática ayudara a la confiabilidad y productividad, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

Alternativas	n	%
Si	15	100,00
No	0	0
Total	15	100,00

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Considera usted que la seguridad

informática ayudara a la confiabilidad y productividad dentro de la Empresa Ransa Comercial S.A?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.12, se observa que, el 100% de los encuestados manifestaron que, SI consideran que la norma ISO en la seguridad informática ayudara a la confiabilidad y productividad dentro de la Empresa Ransa Comercial S.A

Tabla Nro.13: Mejora de servicio

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca que la nueva seguridad de información permitirá mejorar el servicio a los clientes y mejorar la imagen, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

Alternativas	n	%
Si	15	100,00
No	0	0
Total	15	100,00

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta. ¿Considera usted que la nueva seguridad de información permitirá mejorar el servicio a los clientes y mejorar la imagen de la empresa Ransa Comercial S.A?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.13, se observa que, el 100% de los encuestados manifestaron que, SI consideran que la nueva seguridad de información permitirá mejorar el servicio a los clientes y mejorar la imagen de la empresa Ransa Comercial S.A.

Tabla Nro.14: Reducción de perdida de información

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca de reducir la pérdida de información de contar con la seguridad informática, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

Alternativas	n	%

Si	15	100,00
No	0	0
Total	15	100,00

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Cree usted que se reduciría la pérdida de información de contar con la seguridad informática en la empresa Ransa Comercial S.A?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.14, se observa que, el 100% de los encuestados manifestaron que, SI reduciría la pérdida de información de contar con la seguridad informática en la empresa Ransa Comercial S.A.

5.3. Dimensión 03: Nivel de conocimiento de las tecnologías de información.

Tabla Nro.15: Conocimiento

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca si tiene conocimiento de que son las Normas ISO/IEC 27001, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

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

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Tiene conocimiento de que son las Normas ISO/IEC 27001?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.15, se observa que, el 60,00% de los encuestados manifestaron que, NO tienen conocimiento de que son las Normas ISO/IEC 27001, mientras que, el 40,00% de los encuestados manifestaron todo lo contrario.

Tabla Nro.16: La ISO/IEC 27001

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca de tener conocimiento si la norma ISO/IEC 27001 es necesaria para la seguridad de su información, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

Alternativas	n	%
Si	5	33,33
No	10	66,67
Total	15	100,00

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Tiene conocimiento si la norma ISO/IEC 27001 es necesaria para la seguridad de su información?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.16, se observa que, el 66,67% de los encuestados manifestaron que, NO tienen conocimiento que la norma ISO/IEC 27001 es necesaria para la seguridad de su información, mientras que, el 33,33% de los encuestados manifestaron todo lo contrario.

Tabla Nro.17: Aceptación de la NORMA ISO/IEC 27001

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca si accederían a recibir la norma ISO/IEC 27001 para la protección de información, respecto al diagnóstico de la seguridad

informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

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

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Usted accedería a recibir la norma ISO/IEC 27001 para la protección de información en la empresa Ransa Comercial S.A?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.17, se observa que, el 80,00% de los encuestados manifestaron que, SI accederían a recibir la norma ISO/IEC 27001 para la protección de información en la empresa Ransa Comercial S.A, mientras que, el 20,00% de los encuestados manifestaron todo lo contrario.

Tabla Nro.18: Seguridad informática

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca si tienen conocimientos acerca de seguridad informática, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

Alternativas	n	%
Si	2	13,38
No	13	86,67
Total	15	100,00

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Tiene conocimientos acerca de seguridad informática?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.18, se observa que, el 86,67% de los encuestados manifestaron que, NO tienen conocimientos acerca de seguridad informática, mientras que, el 13,33% de los encuestados manifestaron todo lo contrario.

Tabla Nro.19: Tipo de seguridad

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca si conocen que tipo de seguridad de información maneja la empresa, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

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

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para responder a la siguiente pregunta: ¿Usted conoce que tipo de seguridad de información maneja la empresa Ransa Comercial S.A?

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.19, se observa que, el 60,00% de los encuestados manifestaron que, NO conocen que tipo de seguridad de información maneja la empresa Ransa Comercial S.A, mientras que, el 20,00% de los encuestados manifestaron todo lo contrario.

5.4. Resultado General Dimensión 1

Tabla Nro.20: Nivel de satisfacción con el sistema actual

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca de la dimensión 1, en donde se aprueba o desaprueba la satisfacción con el sistema actual, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

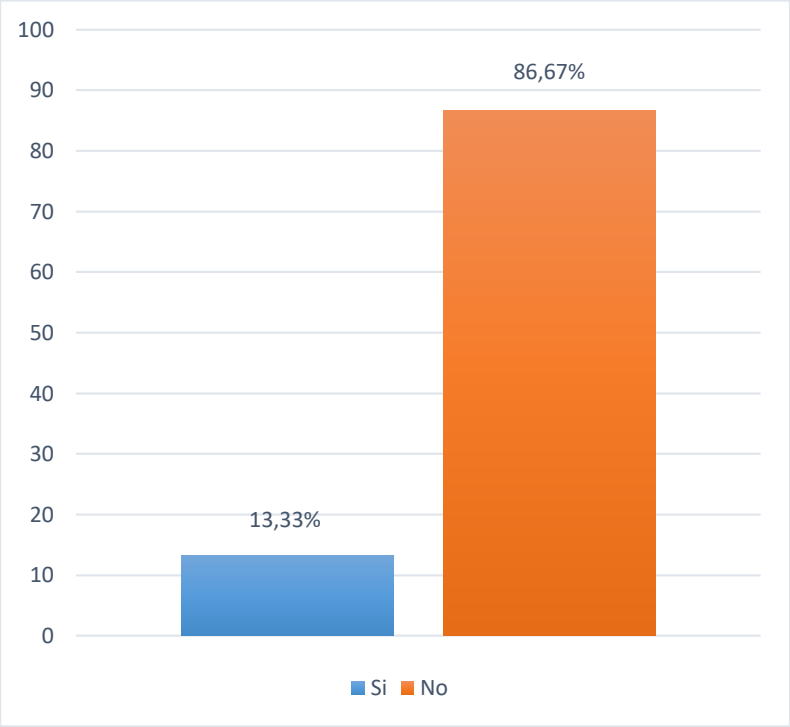
Alternativas	n	%
Si	2	13,33
No	13	86,67
Total	15	100,00

Fuente: Instrumento de recolección de datos para medir la dimensión 1: Nivel de satisfacción con el sistema actual, basado en 5 preguntas, aplicado a los trabajadores de la Ransa Comercial S.A-Piura.

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.20, se observa que, el 86,67% de los encuestados manifestaron que, NO están satisfechos con respecto al sistema actual, mientras que, el 13,33% de los encuestados manifestaron que, SI están satisfechos con el sistema actual.

Gráfico Nro.4: Resultado general de la dimensión 1



Fuente: Tabla Nro.20: Nivel de satisfacción con el sistema actual

5.5. Resultado General Dimensión 2

Tabla Nro.21: Nivel de aceptación de la propuesta de mejora

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca de la dimensión 2, en donde se evidencia la propuesta de mejora del sistema actual, respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

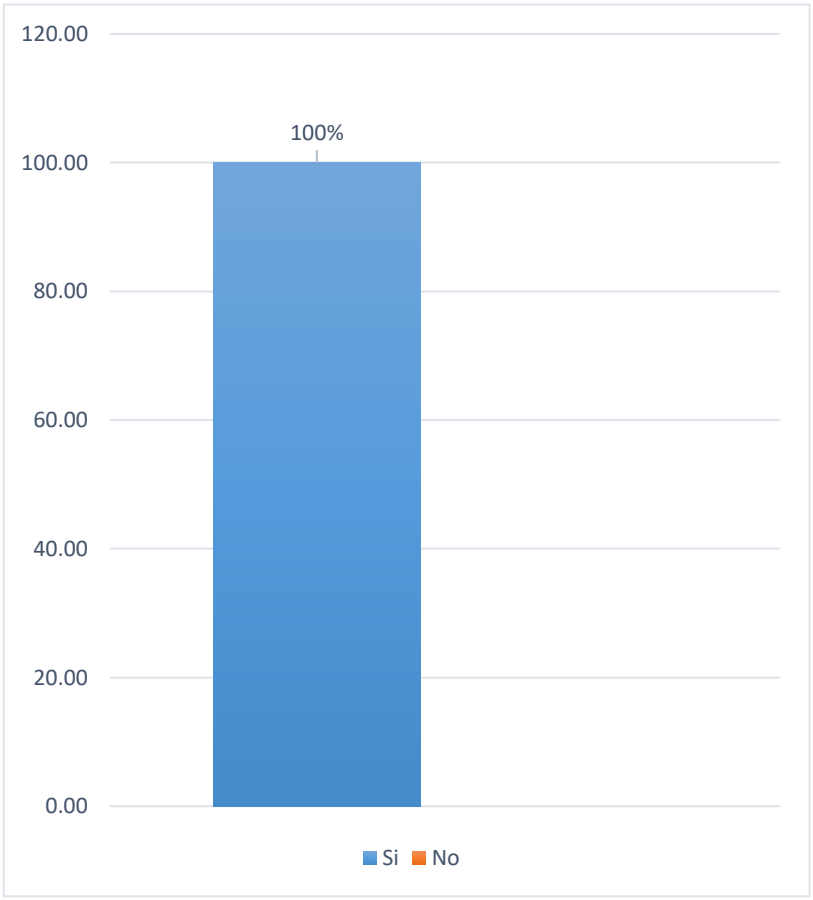
Alternativas	n	%
Si	15	100,00
No	0	0
Total	15	100,00

Fuente: Instrumento de recolección de datos para medir la dimensión 2: Necesidad de propuesta de mejora del sistema actual, basado en 5 preguntas, aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura.

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.21, se observa que, el 100% de los encuestados manifestaron que, SI existe la necesidad de una propuesta de mejora del sistema actual.

Gráfico Nro.5: Resultado general de la dimensión 2



Fuente: Tabla Nro.22: Nivel de aceptación de la propuesta de mejora

5.6. Resultado General Dimensión 3

Tabla Nro.22: Nivel de conocimiento de las tecnologías de información.

Frecuencias y respuestas distribuidas de los trabajadores encuestados, acerca de la dimensión 3, en donde se evidencia el nivel de conocimiento de las tecnologías de información., respecto al diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

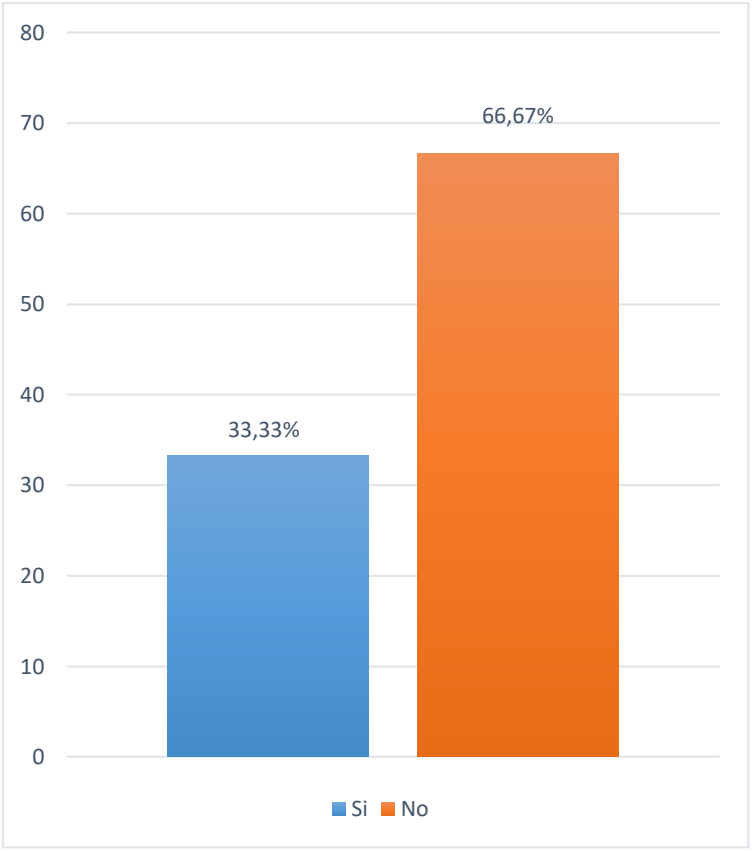
Alternativas	n	%
Si	5	33,33
No	10	66,67
Total	15	100,00

Fuente: Instrumento de recolección de datos para medir la dimensión 3: Nivel de conocimiento de las tecnologías de información., basado en 5 preguntas, aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura.

Aplicado por: Merino, C.; 2020.

En la Tabla Nro.22, se observa que, el 66,67% de los encuestados manifestaron que, NO tienen conocimiento con respecto a la Norma ISO/IEC 27001 en la seguridad informática, mientras que, el 33,33% de los encuestados manifestaron que, SI tienen conocimiento con respecto a la Norma ISO/IEC 27001 en la seguridad informática.

Gráfico Nro.6: Resultado general de la dimensión 3



Fuente: Tabla Nro.23: Nivel de conocimiento de las tecnologías de información.

5.7. Resumen General por Dimensiones

Tabla Nro.23: Resumen general de dimensiones Frecuencias y respuestas distribuidas, para determinar los niveles correspondientes a la dimensión 1: Nivel de satisfacción con el sistema actual. 2: Propuesta de mejora. 3: Nivel de conocimiento de las tecnologías de información, aplicado a los trabajadores de la empresa Ransa Comercial S.A- Piura, para el diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

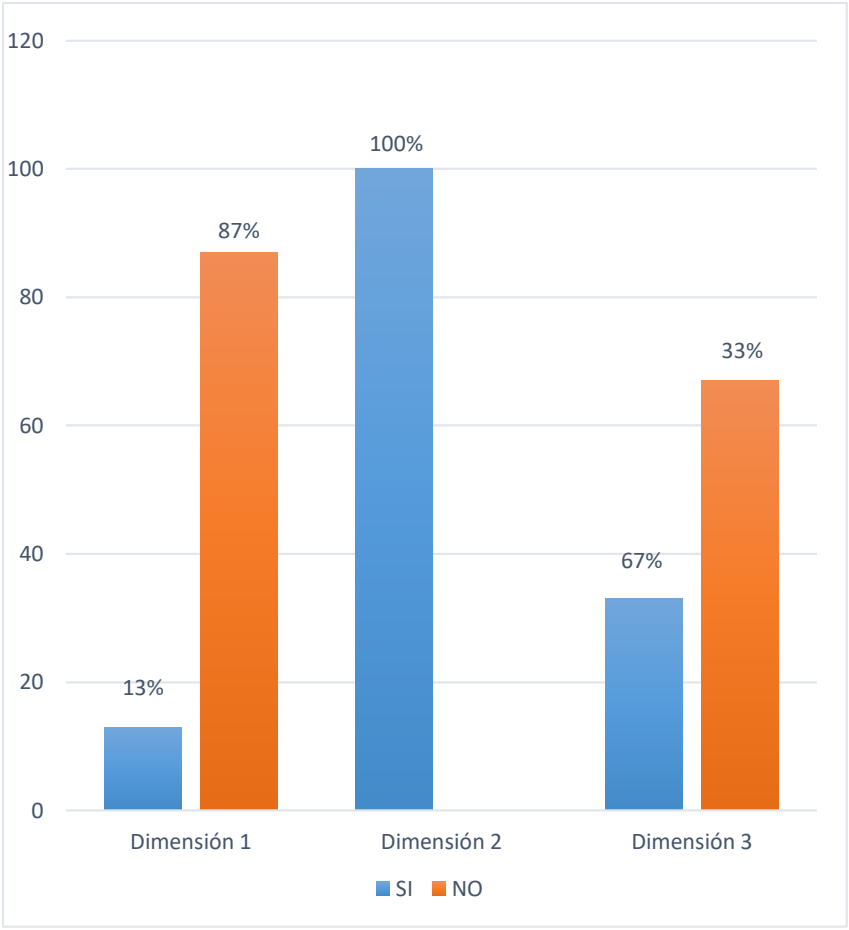
Dimensiones	Alternativas de Respuestas				Muestra	
	Si	%	No	%	n	%
Nivel de satisfacción con respecto a la norma ISO/IEC 27001 en la seguridad informática	2	13,33	13	86,67	15	100,00
Nivel de aceptación de la propuesta de mejora	15	100	0	0	15	100,00
Nivel de conocimiento de las tecnologías de información.	5	33,33	10	66,67	15	100,00

Fuente: Instrumento de recolección de datos aplicado a los trabajadores de empresa Ransa Comercial S.A- Piura, para medir la dimensión 1, la dimensión 2 y la dimensión3, las cuales fueron definidas para esta investigación.

Aplicado por: Merino, C.; 2020.

Una vez obtenidos los resultados, en la Tabla Nro.23, se puede observar que, en lo que respecta a la dimensión 1: Nivel de satisfacción con el sistema actual, el 86,67% de los encuestados manifestaron que, NO están satisfechos con el sistema actual, mientras que, el 13,33% de los encuestados manifestaron que, SI están satisfechos con el sistema actual, con respecto a la dimensión 2: Propuesta de mejora, se observa que, el 100% de los encuestados manifestaron que, SI existe la necesidad de una propuesta de mejora en el sistema actual y respecto a la dimensión 3: Nivel de conocimiento de las tecnologías de información, el 66,67% de los encuestados manifestaron que, NO tienen conocimiento con respecto a la Norma ISO/IEC 27001 en la seguridad informática, mientras que, el 33,33% de los encuestados manifestaron que, SI tienen conocimiento.

Gráfico Nro.6: Resumen general de las dimensiones



Fuente: Tabla Nro.24: Resumen general de dimensiones

5.7. Análisis de Resultados

La presente investigación tuvo como objetivo general: realizar un diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001, con el fin de mejorar el control de la seguridad informática de la empresa Ransa Comercial S.A- Piura, 2020, en el cual se ha realizado tres dimensiones que son satisfacción con el sistema actual, propuesta de mejora y conocimiento de las tecnologías de información. 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 86,67% de los encuestados manifestaron que, NO están satisfechos con el sistema actual, mientras que, el 13,33% de los encuestados manifestaron que, SI están satisfechos con el sistema actual. Este resultado tiene similitud con los resultados obtenidos por Dávila (6), 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 100,00% de los empleados encuestados NO están satisfechos con el sistema e actual. Esto coincide con el autor Sánchez (14), quien menciona que las TIC están presentes en todos los niveles de nuestra sociedad actual, desde las grandes empresas multinacionales, pymes, gobiernos, administraciones y universidades. Estos resultados se obtuvieron porque los procesos se realizan de manera intuitiva, sin seguir protocolos o estándares que aseguren el funcionamiento y seguridad de la información, al utilizar correos corporativos debería contar con un control de seguridad a través de la norma ISO que mejorará 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 100,00% de los encuestados manifestaron que, SI están de acuerdo con la propuesta de mejora de la seguridad de información en la empresa, estos datos mostrados coinciden con Lara (9), 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", muestra como resultados que el 68,00% de los empleados encuestados están de acuerdo que se debería realizar la propuesta de mejora para la seguridad informática en la clínica Simedic Diagnóstica S.A.C, mientas que el 32,00% indicaron que NO es importante la propuesta de mejora, esto coincide con el autor Alegre (22), quien menciona que la 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, estos resultados se obtuvieron porque ambas empresas no brindan la protección necesaria para la documentación interna y esto hace que los trabajadores, como los clientes estén descontentos con el servicio que les brindan, porque su información está expuesta a los peligros por tener la documentación en forma manual, es por eso que se debería asegurar la integridad de la seguridad informática.

En relación a la dimensión 3: Nivel de conocimiento de Tecnologías de la Información y la Comunicación, en el que se puede observar que el 66,67% de los encuestados manifestaron que, NO tienen conocimiento acerca de las tecnologías de la información y la comunicación, mientras que, el 33,33% de los encuestados manifestaron que, SI tienen conocimiento acerca de las tecnologías de la información y la comunicación, esto coincide con el autor Flores (7), quien en su tesis de investigación titulada. "Diseño del sistema de gestión de seguridad de la información para el grupo SIAS SAC", muestra como resultado que el 98,00% de los empleados encuestados no tienen

conocimiento de políticas de seguridad de la información en la gestión administrativa para el GRUPO SIAS SAC, mientras que el 12,00% indicaron que SI tienen conocimiento, esto coincide con el autor Galdámez (24), quien menciona que la tecnología es un elemento indispensable para las organizaciones, se debe utilizar de forma adecuada para evitar riesgos en la información, estos resultados se obtuvieron por que las empresas no prestan atención en mantener la integridad de la información y no se dan cuenta que están vulnerables a pérdidas de información e incidentes de seguridad, ya que la tecnología es un elemento indispensable para las organizaciones y se debe utilizar de forma adecuada con el fin de garantizar la seguridad de los sistemas.

5.8. Propuesta de mejora

Habiéndose realizado el análisis de los resultados obtenidos en la presente investigación, se ha detectado que no existen planes de acción y contingencias para mitigar los riesgos y vulnerabilidades de la seguridad de la información.

La norma ISO 27001:2013 fue elijada para realizar el sistema de gestión de seguridad de información, porque se permitirá ver la información tanto interna y externa de la empresa como un activo valioso, para que los trabajadores puedan trabajar con confianza. Así mismo al implementar esta norma permitirá minimizar los riesgos, por otro lado, se podrá evaluar los diferentes riesgos y establecer una serie de estrategias, controles oportunos para asegurar la protección y defender la información.

5.8.1. Análisis diferencial del estado actual con la ISO/IEC 27001 y 27013

El trabajo se enfoca en analizar los controles y requerimientos de seguridad con los procesos de la empresa Ransa Comercial S.A , por lo cual se detalla cada capítulo, empezando por el numeral 5– Políticas de Seguridad de la información y terminando con el 18- Cumplimiento. En cada capítulo hay controles que se deben implementar. Este análisis nos permitirá conocer de manera específica el estado de la empresa, en relación de la seguridad de la información.

Se agrega un valor a cada control en base al estado en el que se encuentra:

0.- No implementado.
1.- Parcialmente implementado.
2- Si implementado.

Tabla N° 24 Análisis diferencial

Norma	Sección	N°	Descripción	Hallazgos positivos	Hallazgos negativos	Valor
27001 - A.5	5.Políticas de Seguridad de información	5.1	Orientación de la dirección para la gestión de la seguridad de la información			
		5.1.1	Políticas para la seguridad de la información	Existe un Documento de políticas	No está incluido la política de seguridad.	1
		5.1.2	Revisión de las políticas de seguridad de la información.		las políticas se encuentran desactualizada.	0
	Organización De la Información	6.1	Organización Interna			
		6.1.1	Funciones de seguridad de la Información y las responsabilidades	Si están los roles documentados en la empresa.	No cuentan con roles para los responsables del sistema de gestión de seguridad.	1
		6.1.2	La segregación de funciones	existen roles y cargos definidos		2
		6.1.3	Ponerse en contacto con autoridades.		No cuentan con procesos para recaudar información.	0
		6.1.4	Ponerse en contacto con los grupos especial		No cuenta con información referente a los grupos de interés.	0

	Organización De la Información	6.2	Dispositivos móviles y teletrabajo			
		6.2.1	Política de dispositivo móvil		No existen procedimientos sobre la utilización de celulares.	0
		6.2.2	Trabajo remoto		No cuentan con procedimientos de trabajo remoto.	0
	Seguridad de los Recursos Humanos	7.1	Antes de la contratación laboral			
		7.1.1	Proyección		No cuentan con inventarios de proveedores.	0
		7.1.2	Términos y condiciones de empleo	Cuentan con una regla de confidencialidad de información.	La regla no dice el tiempo de confidencialidad de información.	1
	Seguridad de los Recursos Humanos	7.2	Durante la contratación laboral			
		7.2.1	Responsabilidades de gestión	Cuentan con una regla de confidencialidad de información.	La regla no dice el tiempo de confidencialidad de información.	1

		7.2.2	Concienciación sobre la seguridad de la información, la educación y la formación		Los trabajadores no reciben capacitaciones sobre políticas de seguridad de información.	0
		7.2.3	Proceso disciplinario		En la evaluación obvian los incidentes de seguridad de información.	0
		7.3	Renovación de contrato			
		7.3.1	Culminación o renovación de contratos.		No existen procedimientos para retiro del personal.	0
	Gestión de activos	8.1	Responsabilidad por los Activos	Hallazgo positivo	Hallazgos negativos (Que Falta)	Valor
		8.1.1	Inventario de activos	Los inventarios se manejan manualmente.	No existe un proceso documentado para el inventario de activos.	1
		8.1.2	Propiedad de los bienes	Cuentan con un inventario físico	No existen protocolos para la asignación de activos en la empresa	1
		8.1.3	Uso aceptable de los activos	Se induce al personal sobre el cuidado de cada equipo asignado.	No existe un compromiso firmado sobre la entrega de equipos.	1

		8.1.4	Retorno de los activos	Cuentan con un procedimiento de retiro de activos que utilizan como evidencia para Auditorías internas y externas.		1
		8.2	Clasificación de la Información	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		8.2.1	Clasificación de la información		No cuenta con un proceso de clasificación de información.	0
		8.2.2	Etiquetado de la información		No se tiene clasificación de la información de los cliente.	0
		8.2.3	Manejo de activos	Existe un código a cada equipo asignado.	No existe un monitoreo de equipos asignados.	1
		8.3	Manipulación de Medios	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		8.3.1	Gestión de soportes extraíbles		No se tiene control de los soporte.	0
		8.3.2	Cancelación de medios de comunicación	Realizan una revisión antes de dar de baja a la información.	No existen protocolos de seguridad al eliminar información.	1
		8.3.3	Transferencia de medios físicos	Las informaciones son manejados por un solo personal.	No existe claves de seguridad para acceder a la información de la	0

					empresa.	
	Control de accesos	9.1	Control de Acceso de requerimientosdel Negocio	Hallazgo positive	Hallazgos negativos (Que Falta)	valor
		9.1.1	Política de acceso	Si cuentan con procedimientos para el acceso de la información.	No Se tiene clasificación de la información ni clasificaciones de perfiles de acceso	1
		9.1.2	El acceso a servidores	Si cuentan con el ingreso de un usuarios a la red.	Implementar protocolos de seguridad a la red.	1
		9.2	Gestión de Acceso de Usuarios	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		9.2.1	Ingreso de usuarios	Cuentan con procedimientos para acceder a la VPN.	Actualizar los procedimientos incorporando el sistema de gestión de la seguridad de información.	1
		9.2.2	Provisión de acceso al usuario	Existe procedimiento para acceso de usuarios.	Se tiene que implementar seguridad de acceso a información importante.	1
		9.2.3	Acceso privilegiado	Cuentan con protocolos de acceso a la empresa.	Se tiene que implementar protocolos para la actualización de usuarios.	1

		9.2.4	autenticación de usuarios	Se maneja contraseñas para la seguridad de información.	Se debe implementar el uso de caracteres especiales en las contraseñas.	1
		9.2.5	Revisión de los derechos de acceso de usuario	Realizan inventarios semanales de los activos de la empresa.	No cuenten con documentación las actividades de sistema de gestión de la seguridad informática.	1
		9.3	Responsabilidad de los Usuarios	Hallazgo positivo		valor
		9.3.1	El uso de la información secreta de autenticación	Establecen las buenas prácticas para el manejo de la contraseña se tiene controles de directorio activo para la creación de contraseñas	Se debe definir una política de manejo de contraseñas y buenas prácticas para el uso de estas que incluyan un límite de historia de contraseñas se deben generar controles que garanticen la no reutilización de un límite de contraseña.	1
		9.4	Control de acceso a Sistemas y aplicaciones	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		9.4.1	Restricción de acceso Información		No hay un proceso integral que maneje toda la trazabilidad de un usuario.	0

		9.4.2	Procedimientos seguros de inicio de sesión		no se tiene clasificada y documentada la información, las estrategias de autenticación y los procesos de solicitud de permisos a los diferentes sistemas de información	0
		9.4.3	Sistema de gestión de contraseñas	En las políticas de seguridad se describe el manejo de contraseñas creación de contraseñas seguras; se tienen políticas de grupo de dominio en cuanto a seguridad de contraseñas longitud mínima de 8 caracteres, bloqueo de contraseña 3 intentos fallidos, cambio de contraseña cada 3 meses.		2
		9.4.4	El uso de programas de utilidad privilegiados	Existen políticas de grupo a nivel de dominio que restringe el acceso a utilidades del sistema operativo, existen grupos de dominio para acceso a internet restringido, e tienen reportes de	Se debe actualizar el procedimiento de "revisión de seguridad" ya que no contiene todas las actividades de monitoreo semanal de redes, firewall no están documentadas, no hay	1

				seguimiento y control de servicios de internet, uso de red local.	un documento que especifique los grupos creados en directorio activo sus privilegios y roles.	
		9.4.5	Control de acceso al código fuente del programa		No existen los documentos "Doc Guía -Etapa Implementación" y "Doc Guía - Etapa Desarrollo; " No tiene un sistema para especificar donde se guarda el código, no se menciona control de versiones, no se menciona manejo de cambios de estas fuentes.	0
	Criptografía	10.1	Controles criptográficos	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		10.1.1	Política sobre el uso de controles criptográficos		No se tiene una política de controles criptográficos y en qué caso son necesarios, , para discos externos que salen con información sensible de la empresa	0

		10.1.2	Gestión de claves		No se tiene una política de controles criptográficos y en qué caso son necesarios, para discos externos que salen con información sensible de la empresa	0
	Seguridad física y ambiental	11.1	Áreas Seguras	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		11.1.1	Perímetro de seguridad física	Se tiene controles a nivel de hardware como a nivel de personas los procesos están documentados y existen registros que lo evidencian		2
		11.1.2	Controles de entrada físicas	Se tiene controles a nivel de hardware como a nivel de personas los procesos están documentados y existen registros que lo evidencian.	Los archivos físicos que tienen información sensible e historia de la compañía no tienen control de acceso por carnet ni cámara cercana, el centro de cómputo no tiene control de acceso ni cámara de seguridad	1

		11.1.3	Asegurar oficinas, salas e instalaciones		No se menciona en el proceso seguridad física el manejo del control de llaves (cómo se maneja), quien es el responsable, por cuanto tiempo se almacena este formato, que personas pueden reclamar las llaves.	0
		11.1.4	La protección contra amenazas externas y ambientales		No se menciona ningún proceso para la seguridad contra las amenazas externas y ambientales.	0
		11.1.5	Trabajar en zonas seguras		No se menciona en el proceso de seguridad física el uso de sistemas seguridad cámaras	0
		11.1.6	Zonas de entrega y carga	Se tiene controles a nivel de hardware como a nivel de personas los procesos están documentados y existen registros que lo evidencian	No se tiene un proceso para el manejo de planilla de control ingreso.	1
		11.2	Equipos	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		11.2.1	Emplazamiento y Protección del equipo		No existen procesos, ni alineados que existen análisis de riesgos ambientales documentados.	0
		11.2.2	Apoyo a los servicios públicos	Se tiene incorporado una documentación con las UPS y una vez por año el proceso de mantenimiento con proveedor externo.	No se tiene registro de los mantenimientos de UPS en el proceso, No se menciona en el proceso de instrumentación y electricidad el sistema del centro de cómputo, sus revisiones y mantenimiento	1
		11.2.3	Seguridad del cableado		No hay cableado certificado en la empresa. Se detectó falta de canaletas y separación de cables eléctricos y de datos. No hay un documento o plano de la compañía que apoye las rutas de cableado estructurado.	0

		11.2.4	El mantenimientodel equipo	Se tiene un programa de mantenimientos de equipos tanto lógico como físico. Se tiene un indicador de mantenimiento que se evidencia cada mes.	El proceso de mantenimientos preventivos esta desactualizado hace falta incorporar el indicador de mantenimiento. No se menciona del programa de mantenimientos	1
		11.2.5	La eliminación de los activos	Se tiene incorporado un proceso de registro de dar de baja un equipo. Se tiene incorporado un proceso de desecho tecnológico	El proceso de dar de baja un equipo y que registros se deben realizar no está documentado	1
		11.2.6	Seguridad de los equipos y de los activos fuera del establecimiento	se tiene un proceso de control de salida de equipos de la empresa	No se tiene un sistema en los equipos portátiles. Las personas de seguridad no tienen claridad de cuales son.	1

		11.2.7	La eliminación segura o la reutilización de los equipos	se hace una disposición adecuada de los activos de información y se elimina todo tipo de información corporativa antes de esto los equipos dados de bajo y considerados desechos tecnológicos se les realiza un proceso adecuado	En el proceso "Actualización de usuarios - Ingreso o Retiro" se debe especificar el borrado de la información segura	1
		11.2.8	Equipos de usuario desatendida	Se tienen tips de seguridad educando al usuario con tema equipo desatendidos	Se debe crear una política de equipo desatendido. Se debe implementar un control para el tiempo de inactividad del equipo de cómputo.	1
		11.2.9	Política de escritorio y pantalla clear despejado	Se tienen tips de seguridad educando al usuario con escritorio despejado	Se debe crear una política de escritorio y pantalla despejadas, se debe monitorizar periódicamente la aplicación de la política de escritorio y pantalla despejada	1
	Seguridad en las operaciones	12.1	12. Procedimientos Operacionales y Responsabilidades	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		12.1.1	Procedimientos operacionales, adecuadamente documentados	Se tienen procesos diarios, semanales, mensuales, de todo el SI que soportan la operación	Se debe actualizar el documento "Manual de seguridad" colocando las tareas operativas y Periodicidad	1
		12.1.2	Gestión del cambio	Existe un proceso de gestión de cambios para desarrollo de software. Existe proceso de gestión de cambios para infraestructura. Existe un proceso incorporado en manejo de versiones de aplicaciones de software	No se tiene estandarizado el proceso de Actualización de usuario. Se encuentra información desactualizada.	1
		12.1.3	Gestión de la capacidad	A nivel de desarrollo de software tienen procesos establecidos que les permiten manejar indicadores de calidad y reporte de defectos.	Se debe en el proceso de desarrollo de software detallar el cómo se realiza. No se tiene un proceso estandarizado que especifique la gestión de capacidades.	1
		12.1.4	Separación de desarrollo, prueba y entornos operativos	Se hacen entrenamiento sobre las buenas prácticas de desarrollo	No se evidencia el seguimiento del proceso en cuento los controles de calidad.	1
		12.2	Protección contra código Malicioso	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		12.2.1	Controles contra malware		Se debe ampliar la política de antivirus de las políticas de seguridad de la empresa se debe actualizar procesos relacionados con los monitoreos de la seguridad.	0
		12.3	Copias de Respaldo	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		12.3.1	Copia de seguridad de la información		Los procesos de copias de seguridad no están unificados	0
		12.4	Registro y Seguimiento	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		12.4.1	El registro de eventos	Se tiene un proceso de revisiones diarias, semanales y mensuales de seguridad y estado de salud de la plataforma.	El procedimiento de revisión de la seguridad se encuentra desactualizado. No se tiene protegida la información en cuanto a la manipulación de Registros	1

		12.4.2	Protección de la información de registro	Dentro de los controles establecidos las personas no tienen acceso a la información de diferentes áreas.	No se tiene especificado en el procedimiento revisiones de seguridad quienes son los responsables del acceso, ni la protección a los mismos.	1
		12.4.3	Registros de administrador y operador	Se tiene un proceso incorporado de monitoreo diario, semanal por parte del administrador y el operador de los servicios críticos de la compañía.		2
		12.4.4	Sincronización de reloj	Se tiene un proceso incorporado para la sincronización de la hora de todos los equipos.		2
		12.5	Control de Software Operacional	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		12.5.1	La instalación del software en los sistemas operativos	Se tiene incorporado controles de instalación de aplicaciones en equipos de usuarios. Se tiene incorporado un sistema de actualización de aplicaciones Microsoft.	No se tiene control de instalación de aplicaciones para el área administrativa desde medios extraíbles. No se tiene implementado un sistemade actualización de parches para programas distintos de Microsoft	1
		12.6	Gestión de Vulnerabilidades técnicas	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		12.6.1	Gestión de vulnerabilidades técnicas	Se tiene incorporado en el mantenimiento del servidor chequeo de vulnerabilidades con el software de Microsoft.		2
		12.7	Consideraciones sobre auditorias de Sistemas de Información	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		12.7.1	Controles de auditoría de sistemas de información	Se tiene incorporada la periodicidad de auditoria.	No se tiene documentado el manualdel administrador de seguridad la periodicidad de las auditorias.	1
		13.1	Gestión de la Seguridad de las redes	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		13.1.1	Controles de red	Se tiene un proceso incorporado para las revisiones de todos los servicios de plataforma. Se realizan monitoreos mensuales	El documento Manual del administrador de seguridad informática esta desactualizado las revisiones de los dispositivos.	1
		13.1.2	Seguridad de los servicios de red	Se tiene para los dispositivos de red configurados los roles de acceso a los dispositivos administrador, operador a nivel de dominio se tiene unos grupos creados y determinados accesos para los servicios de plataforma como internet.	No se tiene documentado como se configuran las seguridades de switch. No se tiene dentro del grupo de soporte técnico limitación de acceso al directorio.	1
		13.1.3	La segregación en las redes	Se tiene una documentación completa de la red de la empresa por cada switch e instalado y que dispositivos están conectados a él.		2
		13.2	Transferencia de Información	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		13.2.1	Las políticas y los procedimientos de transferencia de información	Se tiene incorporado en los procesos de inducción y entrenamiento del personal nuevo explicar las buenas prácticas para el uso del correo electrónico, la transferencia de archivos, el uso de la red inalámbrica de visitantes y producción.	Se debe crear una política para el manejo y transferencia de la información a clientes, proveedores, y empleados se debe divulgar la política de transferencia de información a clientes.	1
		13.2.2	Los acuerdos sobre la transferencia de información	Dentro de los contratos proveedores se tienen cláusulas de confidencialidad	Se debe establecer acuerdos de confidencialidad y manejo de la información de acuerdo con la ley con los empleados.	1
		13.2.3	La mensajería electrónica		Se deben establecer para el servicio de correo electrónico metodologías de	0
					encriptados. Se debe para el servicio de mensajería instantánea una política adecuada para el manejo de la información	

		13.2.4	Los acuerdos de confidencialidad o de no divulgación	Se tiene una cláusula de confidencialidad de la información en el contrato.	No se tiene acuerdos de confidencialidad donde se especifique el manejo adecuado, tiempo de retención y normalización de la Información	1
		14.1	Requerimientos de seguridad de los SI	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		14.1.1	Análisis de los requisitos de seguridad de la información y especificación	Dentro de la metodología de desarrollo del proyecto de software se estables los requerimientosno funcionales de la seguridad, se elaboran estrategias de tratamiento a los riesgos según la criticidad del proyecto.		2
		14.1.2	Asegurar los servicios de aplicaciones en las redes públicas	Se tiene a nivel de Firewall protección IDS Las carpetas web server tienen seguridades	se deben fortalecer las políticas de firewall contra ataques Se debe implementar estrategias y protecciones hacia web server a nivel interno.	1
		14.1.3	La protección de las transacciones de servicios de aplicación		se debe establecer para las aplicaciones que manejan y trasmiten	0

					información sensible el	
					uso de códigos criptográficos, certificados, firmas digitales	
		14.2	Seguridad en desarrollo y procesos de soporte	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		14.2.1	Políticas de desarrollo seguro.	Se tienen procesos establecidos para el desarrollo de software las personas del área de desarrollo son entrenadas en buenas prácticas de desarrollo seguro.		2
		14.2.2	Procedimientos de control de cambios del sistema	Se tiene procedimientos de cambios en las aplicaciones y son documentados en actas de entrega de proyectos	Se deben realizar análisis de riesgos de aplicaciones de cada proyecto, donde se identifiquen las amenazas.	1

		14.2.3	Revisión técnica de las aplicaciones después de operar cambios de plataforma	Se tiene incorporado dentro de un proceso de actualización de plataforma realizar reuniones de planeación donde se establecen las actividades, responsables y pruebas.	Se debe crear un procedimiento para la actualización de plataforma donde describa unos lineamientos a seguir se debe actualizar el proceso de pruebas.	1
		14.2.4	Restricciones en los cambios a los paquetes de software	En las aplicaciones que son necesaria se establecen bloqueos para aplicaciones como antivirus en los equipos de los usuarios, sistema operative	de debe establecer un proceso estándar donde se establezca los lineamientos para elegir las aplicaciones que deben tener bloqueos.	1
		14.2.5	Uso de principios de ingeniería en protección de sistemas	Se tiene para la etapa de implementación unos entregables en la etapa de		2
				desarrollo que confirman requerimientos.		

		14.2.6	Seguridad en entornos de desarrollo	Se tienen incorporado prácticas de revisión de seguridad de micros para el área de informática y desarrollo.	Se debe tener una estrategia de seguridad para los entornos de desarrollo y estaciones de trabajo para proteger la información de estos Equipos	2
		14.2.7	Desarrollo Outsourced	no aplica		
		14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	se tiene dentro de la metodología de desarrollo de software una etapa de pruebas funcionales	Se debe incorporar dentro del proceso de pruebas, pruebas de seguridad.	1
		14.2.9	Pruebas de aceptación del sistema		Se debe dentro de la documentación clasificar los tipos de prueba los documentos	0
		14.3	Datos de prueba	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		14.3.1	Protección de los datos de prueba	Los datos de pruebas no contienen información sensible para la compañía, sin embargo de requerirse, estos datos son alterados y no reflejan los reales	Se debe revisar el ambiente de desarrollo y pruebas en cuanto accesos, registros de seguridad	1
		15.1	Seguridad de la Información en la relación con los proveedores	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		15.1.1	Política de seguridad de la información para las relaciones con proveedores	En el contrato se estipulan las condiciones para confidencialidad y política de la información	Se debe incluir en los contratos las formas de tratamiento, retención y transmisión de información, y estas deben acordarse con los proveedores.	1
		15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Existen un proceso de para la compra de servicios con proveedores, y se establecen los requerimientos del servicio brindado.	Se deben establecer acuerdos de confidencialidad donde se estipulen la forma para el tratamiento de la información, para los proveedores.	1
		15.2	Gestión de la prestación de servicios del proveedor	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		15.2.1	El seguimiento y la revisión de los servicios de proveedores	Se hacen un proceso de selección de proveedor y se evidencia en estudio de las cotizaciones y el análisis costo beneficio al final de cada contrato se hace evaluación de servicio a los proveedores.		2

		15.2.2	Gestión de cambios en los servicios de proveedores	Se siguen las buenas prácticas para el cambio de servicios por terceros.	No se tiene documentado los procesos y buenas prácticas para el control de cambios.	1
		16.1	Gestión de Incidentes y Mejoras en la SI	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		16.1.1	Responsabilidades y procedimientos	Se tiene un informe físico donde se ingresan todos los incidentes que afectan la disponibilidad, integridad y confidencialidad. Dentro de los roles se tiene especificado la función de quienes ingresan y clasifican los incidentes de seguridad.		2
		16.1.2	Informar sobre los eventos de seguridad de información	En el entrenamiento inicial de los empleados se les informa el procedimiento a		2
				seguir para el reporte de incidente		

		16.1.3	Presentación de informes de información debilidades de seguridad	Se tiene un proceso de reporte de incidentes tanto para empleados como proveedores.	Los proveedores externos no conocen el proceso y pueden reportar incidentes	1
		16.1.4.	Valoración de eventos de seguridad de la información y toma de decisiones	Se tiene incorporado en los grupos primarios de informática mensuales el análisis de resultados de las solicitudes atendidas y los reproceso a través de indicadores.	No se tiene clasificación en el sistema de ingreso de incidentes para seguridad, ni la criticidad.	1
		16.1.5	Respuesta a incidentes de seguridad de la información	Se tienen informes de gestión sobre el incidente los cuales son reportados a la dirección mensualmente con un acta de resultados.	No se tiene documentado el proceso donde se definen los tiempos de revisión y línea de mando.	1
		16.1.6	Aprendiendo de los incidentes de seguridad de la información	En cada uno de los incidentes se registra la solución y tratamiento, en caso de requerirse se hacen acciones correctivas, preventivas y de mejoramiento	En cada uno de los incidentes se registra la solución y tratamiento, en caso de requerirse se hacen acciones correctivas, preventivas y de mejoramiento	1

		16.1.7	El acopio de pruebas		No se tiene establecido un proceso para la recolección de evidencia formal	0
		17.1	Continuidad SI	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		17.1.1	Información de planificación de continuidad de seguridad		Los documentos del plan de continuidad de negocios se encuentran desactualizado, no se tiene un documento donde se estipulen los tiempos aceptables de recuperación de cada proceso crítico.	0
		17.1.2	Implantación de la continuidad de la seguridad de la información	S	No se tiene establecido un procedimiento que reúna toda la esfera de seguridad en cuanto a información de la clínica, no hay un comité de seguridad para velar las revisiones.	1
		17.1.3	Verificar, revisar y evaluar la información de seguridad de continuidad	El departamento realiza una vez al año como mínimo un simulacro para verificar que los procesos si sean efectivos la información.	No se tiene documentado el plan de simulacros y su periodicidad	1
		17.2	Redundancias	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		17.2.1	Disponibilidadde instalaciones para el procesamiento de la información		No se tiene documentado en el plan de continuidad de negocios los servidores redundantes y su tiempo de activación en caso de incidentes.	1
		18.1	Información			
		18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	Existe clausula confidencial; términos legales entre las partes tanto para empleados como para proveedores se tiene clausulas en los contratos para el cuidado de la propiedad intelectual	No se tiene un documento donde se definan y estipulen las leyes aplicables en tema de seguridad informática en la empresa.	1
		18.1.2	Derechos de propiedad intelectual	Se tiene en los contratos una cláusula hacia la propiedad intelectual, cláusula de confidencialidad y manejo de la información. Dentro de las políticas existen secciones para la instalación de software.	No se tiene un documento donde se defina la periodicidad del monitoreo de software.	1
		18.1.3	Protección de los registros	Se tiene controles de acceso a la información que garantizan la confidencialidad, integridad	La información no tiene ninguna clasificación. no se tiene documentación .	1

				y disponibilidad. Se tiene dos archivos físicos de manejo de documentos los cuales son controlados por uso de llave y autorización de personas solo autorizadas.	los procesos de clasificación de y tipos de protección y cuidados que se tiene para cada tipo de información.	
		18.1.4	Privacidad y protección de datos personales	Se tiene controles de acceso a la información que garantizan la confidencialidad, integridad y disponibilidad. los documentos físicos están bajo llave en zonas seguras y solo pueden ser accedidos por personal autorizado.	No se tiene documentación de los procesos de clasificación de y tipos de protección y cuidados que se tiene para cada tipo de información las personas.	1
		18.1.5	Regulación de los controles criptográficos	Se tiene controles criptográficos establecidos para los servicios de comunicación	No se tiene documentados los procesos criptográficos	1
				transferencia de información.	de la clínica y en qué casos estos aplican.	
		18.2	Revisiones de SI			

		18.2.1	Revisión independiente de la seguridad de la información	Se tienen procesos de revisiones diarias, semanales y mensuales en cuanto a seguridad y salud de la plataforma; se tiene dentro del proceso de plataforma auditorías internas a los procesos de seguridad, 2 veces al año. Se hacen auditorías externas las áreas de informática a los diferentes procesos de plataforma se tiene planes de auditorías a los procesos.	Se debe incorporar en la programación de auditorías internas el sistema de gestión de seguridad de la información se debe actualizar el procedimiento de revisiones de seguridad agregando los reportes de servicios y vulnerabilidades técnicas y demás generalidades de SGSI	1
		18.2.2	El cumplimiento de las políticas y normas de seguridad		Se debe establecer una política donde se defina el tratamiento de la información segura y buenas prácticas se deben establecer controles para monitorizar y reportar todo uso indebido de los sistemas de información.	0
		18.2.3	Revisión de cumplimiento técnico		No se tiene defin ido el proceso formal para la revisión de actividades diarias de los servicios de infraestructura.	0

Fuente: Elaboración propia.

Tras el análisis completo de los diferentes dominios se encontró que, de un total de 114 ítems, 32 de estos no se cumplen, 68 se cumplen parcialmente y 14 se cumplen satisfactoriamente. En lo que respecta a las políticas de seguridad no se cuenta con la documentación necesaria a los procedimientos y controles que ayuden a garantizar la seguridad de información, por otro lado, se realizó el análisis de la seguridad de la información en la organización se cuenta con acuerdos de confidencialidad, sin embargo, no tiene la documentación adecuada y clara en los roles para el control adecuado de la operación de la seguridad. Asimismo, se observa que la seguridad de los recursos humanos no se cuenta con un control adecuado para los procesos referentes a la terminación de contratos, tampoco tiene un control de los equipos que serán devueltos a la culminación del contrato de los empleados. Por otro lado, en la gestión de activos se puede observar, que, aunque se ha trabajado en el inventario de activos, este no se encuentra actualizado en su totalidad, así mismo no se tiene procedimientos para las clasificaciones de la información. En el control de accesos se cuenta con el uso de contraseñas, sin embargo, no se cuenta con documentación formal, mientras que en lo que respecta a la criptografía se observa que no existe procedimientos en todo lo relacionado al uso de las llaves criptográficas.

En la seguridad física y ambiental no se cuenta con una protección completa en la alimentación eléctrica, lo que evidencia falta de seguridad en el cableado y la restricción en el uso de los equipos móviles: así mismo se detectan errores en la seguridad en las operaciones, puesto que no se cuenta con logs y/o carteles en la gestión de medios informativos.

En relación con los proveedores no se cuentan con un control adecuado referente a los requisitos de seguridad, tiendo en cuenta toda la comunicación, para el aseguramiento de la protección de los activos; así como en la gestión de incidentes de seguridad no se cuenta con una correcta gestión, para la recolección de evidencia. Según el análisis realizado, se observa a nivel general, que se requiere una intervención inmediata a nivel de los dominios relacionados con políticas de seguridad, continuidad del negocio, control de accesos, criptografía y relación con los proveedores, puesto que son los que tiene mayor índice de incumplimiento con la norma y afectan la seguridad de la información que se requiere.

5.8.1.1. Gestión de Riesgos

La realización del análisis de riesgos tiene como fin identificar de manera clara los riesgos a los cuales está expuesta la empresa y basados en esta identificación de los riesgos determinar cuáles son las medidas de seguridad adecuadas para los diferentes activos de seguridad de la información, de igual manera permite establecer los planes de contingencia, para este caso realizaremos un análisis de riesgo, que es un tipo de análisis que se realiza teniendo en cuentas las medidas de seguridad que la empresa ya tienen planteadas. Por otro lado, describe la metodología a utilizar para la gestión de riesgos, derivados de las tecnologías de la información, así como el inventario de los activos de la empresa Ransa Comercial y la valorización de estos. Se tendrá en cuenta la confidencialidad, integridad y disponibilidad de la información, realizando de esta forma el análisis de amenazas y la valorización de los riesgos. La metodología para realizar para la gestión de riesgos es MARGERIT que permitirá la implementación en el

proceso de gestión de riesgos dentro de un marco de trabajo, que ayudará a la toma de decisiones teniendo en cuenta los riesgos derivados del uso de las tecnologías de la información.

Por otro lado ayudara a concientizar a los responsables de la empresa, de la existencia de riesgos y de la necesidad de gestionarlos, así mismo permitirá a analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones, por otro lados ayudara a descubrir y planificar el tratamiento oportuno para los riegos bajo control y finalmente ayudará a preparar a la empresa Ransa Comercial con los procesos de evaluación, auditorio y certificación o acreditación según corresponde en cada caso.

5.8.1.2 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° 25 Inventario de los activos

Ámbito	Activo
Instalaciones	Ubicación local de infraestructura y Comunicaciones
	sala eléctrica, telecomunicaciones
Hardware	Servidores
	PC de escritorio, portátiles
	Equipos de comunicaciones

	Reuter inalámbrico
	Telefonía
Software	Windows 2008/ 2010 PRO
Aplicaciones	Paquete de office
	Correo empresarial
	Antivirus: ESET NOD32
	Sistema de backups: ESET NOD32
Datos	Información contable y administrativa
	Formatos documentales (manuales y acceso)
	Registros de operación: informes y Monitoreo
	Datos de clientes y usuarios
Red	Red de datos
	Red de telefonía
	acceso a Internet
Servicios	Internet
	Telefonía
	Servicio de internet y telefonía Movistar.
	Correo
Equipos adicionales	Generadores de energía
	Sistema de alimentación UPS
	Sistema de aire acondicionado
	Equipos de control de temperatura
Personal	Gerente
	Personal administrativo
	Personal para atención al cliente
	Personal para despacho.
	Jefe de informática

Soportes de información	Discos duros de servidores.
	Discos externos información de backups
	Unidades de CD, DVD y Memorias extraíbles

Fuente: Elaboración propia.

5.8.1.3 Valoración de Activos

Siguiendo la metodología se define una tabla de valoración de activos con el fin de utilizarla para la evaluación de los activos de información.

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

Tabla N° 26 Valor de los activos.

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

Fuente: Libro de Magerit (32).

En esta tabla quedan establecidas las abreviaturas que se utilizaran para la valoración de los activos de información. Desde el punto de vista de la seguridad, junto a la valoración en sí de los activos debe

indicarse cuál es el aspecto de la seguridad más crítico. Identificados los activos se realiza entonces la valoración ACIDA de los mismos. 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 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° 27 Escala de valoración

Valor	Criterio
10	Daño muy grave de la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Fuente: Libro de Magerit (32).

A continuación, la valoración de las dimensiones de seguridad de los activos que incluyen aspectos como Autenticidad, Criticidad, Integridad, Disponibilidad y trazabilidad.

Tabla N° 28 Valoración de seguridad de los activos

Valoración Dimensiones de Seguridad de los Activos							
Ámbito	Activo	Valor	Aspectos Críticos				
			A	C	I	D	T
Instalaciones	Ubicación local de infraestructura y comunicaciones	Muy Alto				10	
	sala eléctrica, ups, telecomunicaciones	Alto				7	
Hardware	Servidores	Muy Alto	10	10	10	8	10
	Pc de escritorio, Portátiles	Alto	8	6	7	7	7
	Equipos de Comunicaciones	Muy Alto	10	9	9	10	9
	Reuter inalámbrico	Alto	9	9	9	8	9
Aplicaciones	Sistemas Operativos: Windows 2010	Muy Alto	10	9	8	10	10
	Paquete de office	Medio	5	6	6	7	7
	Correo empresarial	Alto	9	8	8	7	8
	Antivirus: ESET NOD32	Alto	9	6	8	6	8
	Sistema de backups: ESET NOD32	Alto	9	9	8	6	8
Dat	Información contable y Administrativa	Muy Alto	10	10	10	10	10

	Formatos documentales (manuales y acceso)	Muy Alto	9	9	9	10	9
	Registros de operación: informes y monitoreo	Alto	9	8	8	9	8
	Datos de proveedores y Usuarios	Alto	9	9	9	10	9
Red	Red de datos	Muy Alto				10	
	Red de telefonía	Medio				7	
	acceso a Internet	Alto				9	
Servicios	Internet	Alto				9	
	Telefonía	Medio				7	
	Cable de Movistar.	Medio				7	
	Correo	Muy Alto				10	
Equipos adicionales	Generadores de energía	Muy Alto				10	
	Sistema de alimentación UPS	Muy Alto				10	
	Sistema de aire Acondicionado	Alto				9	
	Equipos de control de Temperatura	Medio				8	
P e	Gerente	Muy alto		10		10	
	Personal administrativo	Muy alto		10		10	

	Personal para atención al Cliente	Alto		8		8	
	Personal para las atenciones medicas	Muy Alto		10		10	
	Jefe de informática	Alto		9		9	
Soportes de Información	Discos duros de servidores.	Muy Alto	10	10	10	10	10
	Discos externos información de backups	Muy Alto	9	7	10	8	10
	Unidades de CD, DVD y Memorias extraíbles	Alto		6	8	7	

Fuente: Elaboración propia.

5.8.1.4. 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:

Desastres naturales, de origen industrial, errores y fallos no interconectados, y amenazas intencionales presenciales. Realizándose la siguiente tabla de amenazas:

Tabla N° 29 Análisis de amenazas

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

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

	Destrucción de información	X	X					X	X	X		X	X	
	Fugas de información			X						X	X	X	X	X
	Vulnerabilidades de los programas	X	X	X						X				
	Errores de mantenimiento/ actualizaciones de programas (software)	X	X							X				
	Errores de mantenimiento/ actualizaciones de equipos (hardware)	X					X	X						
	Caída del sistema por agotamiento de recursos	X					X	X					X	
	Pérdidas de equipos	X		X			X							
	Indisponibilidad del personal	X												X
Amenazas intencionales presenciales	Manipulación de los registros en actividad		X		X									
	Suplantación de la identidad del usuario		X	X		X		X		X		X	X	
	Abusos de privilegios de acceso	X	X	X						X				
	Re-encaminamiento de mensajes			X				X		X			X	
	Alteración de secuencias		X					X		X			X	
	Acceso no autorizado		X	X			X	X	X	X	X	X	X	
	Análisis de tráfico			X				X						X
	Repudio		X				X							
	Interceptación de información (Escucha)			X				X						
	Modificación deliberada de la información		X					X	X	X	X	X	X	
	Destrucción de información	X							X	X		X	X	

	Divulgación de información		X						X	X	X	X	X	
	Manipulación de programas	X	X	X						X				
	Manipulación de los equipos	X		X			X							
	Denegación de servicio	X					X	X					X	
	Robo	X		X			X							
	Ataque destructivo	X					X		X		X			
	Indisponibilidad del personal	X												X
	Extorsión	X	X	X										X
	Ingeniería social	X	X	X										X

Fuente: Elaboración propia.

A continuación, se describen los proyectos planteados anteriormente.

5.8.1.5. plan de Continuidad de la Empresa

El plan de continuidad busca generar las pautas que permitan restablecer en el menor tiempo posible la operatividad de la empresa a causa de eventos que impidan su funcionamiento de manera parcial o total. Los procedimientos planteados en este documento son las acciones por realizar en relación con el hardware, software y equipos activos involucrados en los procesos críticos definidos en este plan. A continuación, se describe cada paso:

- Evaluación del estado actual: Se realizó un análisis de riesgo para identificar los activos con que cuenta, activos críticos a ser protegidos y el estado de los controles actuales y la definición de los equipos que deben ser adquiridos, los procesos y procedimientos que deben ser desarrollados. Esto se ha desarrollado a lo largo del documento.

- Estrategia de respaldo: la empresa deberá implementar un centro de datos que permita la seguridad de todos los activos de información. Así mismo evaluar los recursos técnicos y humanos para dicha operación.

- Desarrollo del plan: En esta etapa se definirán los equipos necesarios para un desarrollo adecuado del plan, además de sus responsabilidades y funciones, También se hará una

descripción de los procedimientos de aleta y actuación ante los eventos que pueden llegar a activar el plan.

- Pruebas: Se realizarán las pruebas pertinentes para verificar que el plan funciona correctamente.

- Capacitación: se realizará la capacitación y el entrenamiento respectivo al personal a cargo del plan de contingencia y se realiza un plan de concientización entre todo el personal.

- Puesta en marcha del plan, adicionalmente se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos del área de informática principal para implementar el centro de datos.

5.8.1.6. Plan de Capacitación

El plan de capacitación involucra al personal administrativos, atención al cliente y encargados de almacén. Así mismo para el personal administrativo deberá recibir capacitaciones de nivel medio y jurídico de modo que se mejore el manejo de la seguridad de la información. El plan de concienciación está orientado a disminuir el nivel de riesgo presente con resto a deficiencias en la empresa y fugas de información que fueron identificados en todo el personal de la empresa.

- Diseño del plan de sensibilización: En esta etapa se diseñarán estrategias para sensibilizar a todo el personal de la empresa. Para ello se utilizarán diferentes estrategias.

- Diseño del plan de capacitación: En esta fase se revisará y diseñará los cursos relacionados con seguridad de la información para personal clave, así como talleres prácticos para todo el personal.

- Consecución de recursos: En esta etapa se realizará la gestión de recurso financiero y de personal que se necesitan para poner en funcionamiento el plan de sensibilización y capacitación.

5.8.1.7. Plan de Mitigación de Riesgos

El plan de mitigación de riesgos busca establecer acciones y recursos que restrinjan de la mejor forma posible la propagación de software autoejecutable o que intercambiar información tanto en los equipos de cómputo, como en las aplicaciones y las redes utilizadas por la empresa. Así mismo se busca con este plan restringir el acceso a la información contenida en los discos duros de los equipos de cómputo, de acuerdo con los niveles de acceso del personal.

A continuación, se aplica salvaguardas para implementar el plan de gestión de los riesgos existentes. En primera instancia se deberá aplicar las salvaguardas en niveles con prioridad mayor es decir medidas preventivas y luego las salvaguardas con niveles superiores que conforman las medidas correctoras. Entre las

salvaguardas de mayor prioridad se encuentran la prevención contra incendios y terremotos, prevención de la fuga de información, prevención de perdida de almacenamiento y la prevención de acceso no autorizado. Por otro lado, numeramos algunas normas que permitirán disminuir los riesgos en la en la empresa:

1. Brindar confidencialidad a los trabajadores y proveedores, por la información que tiene la empresa, así mismo los trabajadores deberán asumir una responsabilidad individual respecto a los criterios de confidencialidad, integridad y disponibilidad de los sistemas y tecnologías, así como del uso de información privilegiada.

2. Cumplir con los requerimientos legales en cuento a la protección de la información de los clientes.

3. Dar a conocer a los trabajadores sobre la importación del SGSI, así como su responsabilidad sobre el cumplimiento de los dispuestos por el SGSI.

4. La información y los recursos de vital importancia como activos en la empresa, debe ser utilizados con responsabilidad, bajo los principios de ética y moral, para protegerlos.

Finalmente se ha desarrollado un plan de ejecución que conlleva la participación del personal de varias área e implementación y mejorar de procesos aplicando medidas preventivas correctoras

para reducir los niveles de riesgo existentes. Es importante mencionar que las salvaguardas sugieren permitir minimizar los riesgos, pero cada una tiene un costo por lo que en cada caso en particular se debe evaluar el valor de la información a proteger y los costos que implicaría la pérdida o el sufrimiento de un ataque y en este sentido planificar las acciones pertinentes para la protección de tal información.

Los resultados ayudaran a la organización a reconocer la necesidad de iniciar la implementación de un plan de gestión de riesgos que permiten mitigar los riesgos más críticos, hasta que decidan desarrollar un plan de tratamiento de riesgo en el que se considera la contratación del personal especializado en seguridad, análisis de documentos y registros de incidente.

V. CONCLUSIONES

Teniendo en cuenta los resultados obtenidos en el presente trabajo de investigación se evidencia la necesidad de implementar un diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001, la misma que tiene como finalidad permitir mejorar los procesos de seguridad, confiabilidad y disponibilidad de la información en la empresa Ransa Comercial S.A, generando de esta manera la satisfacción de los trabajadores con esta propuesta. La interpretación realizada concuerda con la hipótesis general propuesta para la investigación donde se indicó que el diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la Empresa Ransa Comercial S.A-Piura; permitirá mejorar la gestión en los activos de información. De acuerdo a lo indicado concluyo que la hipótesis general queda adecuadamente aceptada.

Respecto a las conclusiones específicas se puede concluir lo siguiente:

1. Se identificó la existencia de los riegos considerando la seguridad de la información en la empresa Ransa Comercial S.A - Piura, 2020.

2. Se evaluó los mecanismos de seguridad, después de localizar los riesgos en los activos de información que enfrenta la empresa.

3. Se analizó las diferentes normas internacionales basadas en la seguridad de información para la empresa Ransa Comercial S.A - Piura, 2020.

4. Se analizó las metodologías de evaluación y riesgos informáticos.

Como principal aporte es mejorar la seguridad de información y por ende impedir la pérdida y eliminación de información que le pertenecen a la empresa Ransa Comercial S.A- Piura.

El valor agregado es utilizar la norma ISO/IEC 27001 para verificar el nivel de seguridad de información de todas las áreas tecnológicas de la empresa Ransa Comercial S.A- Piura.

VI. RECOMENDACIONES

1. Implementar la norma ISO/IEC 27001 que le permitirá brindar seguridad en los activos de información y protegerlos en caso de alguna vulnerabilidad de información.

2. Capacitar sobre la seguridad de información para que se puedan adaptar al nuevo cambio con la implementación de la ISO/IEC 27001.

3. Cumplir las políticas establecidas para mejorar la seguridad informática en la empresa, esto permitirá evaluar los riesgos y poder prevenirlos.

4. 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. Evolución Tecnológica
   . https://www.eleconomista.com.mx/opinion/Evolucion-tecnologica-20180412-0029.html; 2018

2. León L. Planificación de un SGSI basado en la Norma ISO 27001 en la Empresa Mafelesa;2008.

3. Ararat J. Diseño de un SGSI basado en la Norma ISO 27001 para la Empresa Ma Peñalosa CÍA. S.A.A; 2018.

4. 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.

5. Benites C. Implementación de un sistema de Gestión de Seguridad de la Información-Norma ISO 27001 para la Fábrica Radiadores Fortaleza;2019.

6. 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.

7. Flores M, Diseño del sistema de gestión de seguridad de la información para el grupo SIAS SAC. de Chimbote- Perú; 2017.

8. Ancajima M. Propuesta de Implementación de Seguridad Informática en la TIC de la I.E San Miguel Arcángel, Catacaos-Piura;2019.

9. Lara B. Propuesta para la seguridad informática basado en la Norma ISO 27001 en la clínica Simedic Diagnóstica S.A.C;2018.

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

11. La Organización en la empresa. Disponible: https://www.mheducation.es/bcv/guide/capitulo/8448146859.pdf

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

13. Google. Google Maps. [Online].; https://www.google.com/maps/place/RANSA+Piura/

14. Sánchez E. Las Tecnologías de Información y Comunicación (TIC) desde una Perspectiva Social; 208.

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

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

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

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

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

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

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

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

23. Romero M, Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades;2018

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

25. 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.

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

27. Cuervo S, Implementación ISO 27001; 2017.

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

29. Gorriti I, Plan de Implementación de la ISO/IEC27001:2013; 2014.

30. 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/.

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

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. Metodología de la Investigación Cientifíca limA; 2009.Fachelli S, Metodología de la Investigación Social Cuantitativa; 2015.

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

35. Fachelli S, Metodología de la Investigación Social Cuantitativa; 2015.

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

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

38. Código de Ética para la Investigación [Internet]. Uladech.edu.pe.2020 [cited 26 June 2020]. Available from: https://www.uladech.edu.pe/images/stories/universidad/documentos/2019/coddigo-de-etica-para-la-investigacion-v002.pdf

39. Reglamento de investigación V015.

ANEXOS

ANEXO NRO. 1: CRONOGRAMA DE ACTIVIDADES

CRONOGRAMA DE ACTIVIDADES																	
N°	Actividades	Año 2008				Año 2020								Año 2021			
		Semestre I				Semestre I				Semestre II				Semestre I			
		Mes				Mes				Mes				Mes			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Elaboración del Proyecto	X															
2	Revisión del proyecto por el jurado de investigación		X														
3	Aprobación del proyecto por el Jurado de Investigación			X													
4	Exposición del proyecto al Jurado de Investigación				X												
5	Mejora del marco teórico					X											
6	Redacción de la revisión de la literatura.						X										
7	Elaboración del consentimiento informado (*)							X									
8	Ejecución de la metodología								X								
9	Resultados de la investigación									X	X						
10	Conclusiones y recomendaciones											X					
11	Redacción del pre informe de Investigación.												X				
12	Reacción del informe final													X			
13	Aprobación del informe final por el Jurado de Investigación														X		
14	Presentación de ponencia en jornadas de investigación															X	
15	Redacción de artículo científico																X

Fuente: Reglamento de investigación V015 (39)

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 V015 (39)

ANEXO NRO. 3: CUESTIONARIO

TITULO: Diagnóstico de la Seguridad Informática utilizando la Norma ISO/IEC 27001 de la empresa Ransa Comercial S.A- Piura; 2020.

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 satisfecho con la seguridad brindada para su información en la empresa Ransa Comercial S.A?		
2	¿El sistema actual beneficia la seguridad de información de sus clientes en la empresa Ransa Comercial S.A?		
3	¿Considera usted que en la empresa Ransa Comercial S.A el sistema actual maneja la seguridad de su información de forma segura?		
4	¿Cree usted que se necesita implementar una norma ISO para dar seguridad a la información en empresa Ransa Comercial S.A?		
5	¿Sabe cuáles son los pasos a seguir para la seguridad de su información en		

	la empresa Ransa Comercial S.A?		
Dimensión 02: Nivel de aceptación de la propuesta de mejora.			
6	¿Estaría de acuerdo en implentar una norma ISO para dar seguridad a la información en la empresa Ransa Comercial S.A?		
7	¿Está usted de acuerdo que al utilizar la norma ISO mejorara la seguridad de información en la empresa Ransa Comercial S.A?		
8	¿Considera usted que la seguridad informática ayudara a la confiabilidad y productividad dentro de la empresa Ransa Comercial S.A?		
9	¿Considera usted que la nueva seguridad de información permitirá mejorar los servicios a los clientes y mejorar la imagen de la empresa Ransa Comercial S.A?		
10	¿Cree usted que se reduciría la pérdida de información de contar con la seguridad informática en la empresa Ransa Comercial S.A?		
Dimensión 03: Nivel de conocimiento de Tecnologías de la Información y la Comunicación (TIC).			
11	¿Tiene conocimiento de que son las Normas ISO/IEC 27001?		
12	¿Tiene conocimiento si la norma ISO/IEC 27001 es necesaria para la seguridad de su información?		
13	¿Usted accedería a implementar la norma ISO/IEC 27001 para la protección de información en la empresa Ransa Comercial S.A?		
14	: ¿Tiene conocimientos acerca de seguridad informática?		
15	¿Usted conoce que tipo de seguridad de información maneja la empresa Ransa Comercial S.A?		

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 labora : 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 más del 70% de los ítems cumplen con el indicador).

Aspectos de validación del instrumento		1	2	3	Observaciones Sugerencias
Criterios	Indicadores	D	R	B	
• 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 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.	☐	☐	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 escriba 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 labora : 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 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.	☐	☐	☒	
• 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
Reg. CIP N° 170291

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 labore : 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 : $\frac{A + B + C}{80} = 1{,}4$

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 INFORMATICA
Reg. CIP N° 212389

ANEXO NRO. 5: CONSENTIMIENTO INFORMADO

Consentimiento Informado

Investigador principal del proyecto: César Augusto Merino Rosas **Consentimiento informado**

Estimado participante,

El presente estudio tiene el objetivo Realizar el Diagnóstico de la Seguridad informática utilizando la Norma ISO 27001 de la empresa Ransa Comercial S.A- Piura 2020, mejorará la gestión en la seguridad de los activos de información.

La presente investigación informará sobre una empresa comercial que se encarga de brindar soluciones logísticas: distribución, almacenamiento y suministro al público en general.

Toda la información que se obtenga de los análisis será confidencial y sólo los investigadores y el comité de ética podrán tener acceso a esta información. Será guardada en una base de datos protegidas con contraseñas. Tu nombre no será utilizado en ningún informe. Si decides no participar, no se te tratará de forma distinta ni habrá prejuicio alguno. Si decides participar, eres libre de retirarte del estudio en cualquier momento.

Si tienes dudas sobre el estudio, puedes comunicarte con el investigador principal de Piura, Perú César Augusto Merino Rosas al celular: 968165054, o al correo: rosascesar512@gmail.com. Si tienes dudas acerca de tus derechos como participante de un estudio de investigación, puedes llamar a la Mg. Zoila Rosa Limay Herrera presidente del Comité Institucional de Ética en Investigación de la Universidad Católica los Ángeles de Chimbote, Cel: (+51043) 327-933, Email: zlimayh@uladech.edu.pe

Si tienes dudas acerca de tus derechos como participante de un estudio de investigación, puedes llamar a la Mg. Mario Nizama Reyes coordinador de la escuela de sistemas de la filial Piura Institucional de Ética en Investigación de la Universidad Católica los Ángeles de Chimbote, Cel: 927116376, Email: mnizamar@uladech.edu.pe

Obtención del Consentimiento Informado

Me ha sido leído el procedimiento de este estudio y estoy completamente informado de los objetivos del estudio. El (la) investigador(a) me ha explicado el estudio y absuelto mis dudas. Voluntariamente doy mi consentimiento para participar en este estudio:

Nombres y apellidos del participante	Nombres y Apellidos del encuestado