UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Sistema de gestión de seguridad de la información para mejorar la seguridad informática de la Empresa Agrokasa S.A., Ica 2022

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Paucar Espino, Jhonathan Felipe (orcid.org/0000-0001-8521-9121)

Zúñiga Monzón, Dina Rosa (orcid.org/0000-0002-3039-1239)

ASESOR:

Ms. Saavedra Jiménez, Robert Roy (orcid.org/0000-0002-2788-4825)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Apoyo a la reducción de brechas y carencias en la educación en todos sus niveles

LIMA - PERÚ

2022

Dedicatoria

A mis padres que han sabido formarme con buenos sentimientos, hábitos y valores lo cual me ha ayudado a seguir adelante en momentos difíciles.

.

A nuestro Dios que día a día nos cuida y nos guía por el buen camino.

Agradecimiento

A la Universidad César Vallejo por su apoyo.

A la empresa Agrokasa S.A. que nos brindó y compartió la información solicitada.

A nuestro asesor de tesis por su orientación y constante apoyo en el desarrollo de la investigación.

Índice de contenidos

Carátula i
Dedicatoria ii
Agradecimiento iii
Índice de contenidos iv
Índice de tablas v
Índice de figuras vi
Resumen vii
Abstract viii
I. INTRODUCCIÓN 1
II. MARCO TEÓRICO 5
III. METODOLOGÍA 23
3.1. Tipo y diseño de investigación 23
3.2. Variables y operacionalización 23
3.3. Población, muestra y muestreo: 24
3.4. Técnicas e instrumentos de recolección de datos: 25
3.5. Procedimientos 30
3.6. Método de análisis de datos 30
3.7. Aspectos éticos: 30
IV. RESULTADOS 32
V. DISCUSIÓN 47
VI. CONCLUSIONES 49
VII. RECOMENDACIONES 50
REFERENCIAS 51
ANEXOS 54

Índice de tablas

Pág.

Tabla 1. Población 24

Tabla 2. Recolección de datos 26

Tabla 3. Validez por juicio experto del cuestionario del indicador “Nivel de confidencialidad de la información” 26

Tabla 4. Validez por juicio experto del cuestionario del indicador “Nivel de integridad de la información” 27

Tabla 5. Validez por juicio experto del cuestionario del indicador “Nivel de disponibilidad de la información” 27

Tabla 6. Nivel de confiabilidad 42

Tabla 7. Confiabilidad del indicador “Nivel de confidencialidad de la información” 29

Tabla 8. Confiabilidad del indicador “Nivel de integridad de la información” 29

Tabla 9. Confiabilidad del indicador “Nivel de disponibilidad de la información” .. 29

Tabla 10. Análisis descriptivo - Indicador “Nivel de confidencialidad de la información” 32

Tabla 11. Análisis descriptivo - Indicador “Nivel de integridad de la información” 33

Tabla 12. Análisis descriptivo - Indicador “Nivel de disponibilidad de la información” 34

Tabla 13. Prueba de Normalidad - Indicador “Nivel de confidencialidad de la información” 36

Tabla 14. Prueba de Normalidad - Indicador “Nivel de integridad de la información” 38

Tabla 15. Prueba de Normalidad - Indicador “Nivel de disponibilidad de la información” 39

Tabla 16. Prueba t-student para el nivel de confidencialidad de la información ... 41

Tabla 17. Prueba t-student para el nivel de integridad de la información 42

Tabla 18. Prueba t-student para el nivel de disponibilidad de la información 44

Índice de figuras

Pág.

Figura 1. Medias de pre prueba y pos prueba del nivel de confidencialidad de la información 33

Figura 2. Medias de pre prueba y pos prueba del nivel de integridad de la información 34

Figura 3. Medias de pre prueba y pos prueba del nivel de disponibilidad de la información 35

Resumen

Este estudio tuvo como objetivo mejorar la seguridad informática de la empresa Agrokasa S.A. en Ica, 2022 mediante la implementación de un sistema de gestión de seguridad de la información; el tipo fue investigación fue aplicada y de diseño preexperimental. Se utilizó una muestra poblacional de 8 personas, además de la aplicación de la normatividad internacional ISO/IEC 27002 del año 2013 para el desarrollo la solución tecnológica propuesta. Como resultados se tuvo que, para la primera dimensión “Nivel de confidencialidad de la información” hubo un incremento de 63.60% de satisfacción, para la segunda dimensión “Nivel de integridad de la información” hubo un incremento de 66.20% de satisfacción y para la tercera dimensión “Nivel de disponibilidad de la información” hubo un incremento de 65.60% de satisfacción, lo cual permitió un resultado favorable al implementar la solución propuesta. Como conclusión general se tuvo que, la implementación de un sistema de gestión de seguridad de la información mejora significativamente la seguridad informática de la empresa en estudio.

Palabras clave: sistema de gestión, seguridad de la información, seguridad informática, empresa comercial.

Abstract

This study aimed to improve the computer security of the company Agrokasa S.A. in Ica, 2022 through the implementation of an information security management system; the type was applied research and pre-experimental design. A population sample of 8 people was used, in addition to the application of the international standard ISO/IEC 27002 of 2013 for the development of the proposed technological solution. As a result, for the first dimension "Level of confidentiality of information" there was an increase of 63.60% in satisfaction, for the second dimension "Level of information integrity" there was an increase of 66.20% of satisfaction and for the third dimension "Level of availability of information" there was an increase of 65.60% of satisfaction, which allowed a favorable result when implementing the proposed solution. As a general conclusion, the implementation of an information security management system significantly improves the computer security of the company under study.

Keywords: management system, information security, information security, commercial enterprise.

I. INTRODUCCIÓN

Para ISOTools (2021) manifiesta respecto a la seguridad de la información es un estado cambiable o variable debido a las particularidades de cada organización que utiliza un sistema de información, también puede alterarse de acuerdo con los tipos de procesos que realiza, específicamente la economía, cada institución tiene objetivos comunes, estos objetivos se encuentran dentro de un contexto de seguridad relacionado con la información y la defensa y cuidado de activos informáticos, es decir información. La seguridad de la información ha sido normada mediante normas internacionales, Entre ellos, la norma ISO 27000/27002; La cual alcanza un modelo de implementación de seguridad respecto a la información, esta norma da a los principios básicos de cómo asegurar a los activos de información, para ello considera la disponibilidad de equipo de información, considera también a los usuarios respecto a la seguridad que deben brindar al sistema, específicamente, esta norma aborda 3 aspectos fundamentales, estos son la confidencialidad, la integridad y la disponibilidad.

De otra parte, Ayudalay (2019) Los sistemas que han sido creados o diseñados para organizar y direccionar los aspectos de seguridad relacionados con la informática tienen como función cuidar la integridad de los documentos físicos o virtuales, la integridad significa que el documento debe mantenerse completo, que no debe haber perdido ninguna parte de sus elementos, que no se haya extraído ni una palabra de dicho documento. la integridad se conceptúa como a la completitud de la información, es decir sin alteraciones ni cambios, tampoco reducciones de la misma. Los sistemas de gestión de seguridad permiten dar garantía a la transmisión de los datos dentro de un contexto totalmente seguro, para ello utiliza toda la tecnología de seguridad informática. Por su parte la confidencialidad hace referencia a que el acceso hacia una información, documento O registro de datos debe ser accedido por el personal a quién se le ha confiado su acceso, esto significa que son personas debidamente autorizadas para utilizar este tipo de información. Por otro lado, la disponibilidad de la información significa que dicha documentación debes estar accesible en todo momento para el personal que tiene la autorización de acceder a ella.

La espacio de estudio para la presente investigación es la empresa Sociedad Agrícola Drokasa S.A., no obstante, también se utiliza su nombre comercial como Agrokasa, La misma que se encuentra ubicada en la ciudad de Ica, dispone como giro del negocio, la producción, empacado y comercialización de frutas, tales como, uvas de mesa, espárragos, paltas y arándanos, Las frutas se venden en estado fresco, de acuerdo a los requisitos presentados por los clientes, así como también en función a las tareas que configuran el productos valorándolo.

Como empresa exportadora, dispone de un sistema informático en donde se generan gran cantidad de información confidencial, pero en la actualidad no dispone de un sistema de gestión, que le pueda brindar y garantizar la seguridad y la ausencia de peligro y ataques que se configuran en los medios de la informática, por lo que se encuentra actualmente en un estado situacional de riesgo y de falta de protección. Los problemas encontrados consisten en que estos documentos pueden ser atacados y afectados en su integridad, en su confidencialidad y en su accesibilidad. Así mismo, se han encontrado problemas de acceso de los usuarios a la información, considerable riesgo de manipulación de la información por parte de usuarios que no disponen del acceso debidamente aceptado, se evidencian políticas de seguridad deficientes e incompletas, muchas veces la información pasa por personal qué ocupan diversas áreas, en ese sentido la información puede ser divulgada y puede perder las características de confidencialidad, integridad y accesibilidad.

Con el propósito de afrontar las dificultades problemáticas indicadas con anterioridad, se hizo preciso implementar de un **Sistema de Gestión de Seguridad de la Información (SGSI)**, para que se garantice las condiciones seguras los activos informáticos, específicamente de los registros informáticos en donde se guarda información confidencial de los negocios de la empresa en estudio.

Las realidades diagnosticadas líneas arriba, conllevan a plantear la **formulación del problema**: *General:* ¿De qué manera un sistema de gestión de seguridad de la información influye en la seguridad informática de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022?; *Específicos:* ¿De

qué manera un sistema de gestión de seguridad de la información influye en el nivel de confidencialidad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022?; ¿De qué manera un sistema de gestión de seguridad de la información influye en el nivel de integridad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022?; ¿De qué manera un sistema de gestión de seguridad de la información influye en el nivel de disponibilidad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022?

La **justificación de la investigación**: *Conveniencia*, porque va a permitir potenciar la credibilidad y reputación del objeto de estudio mostrándolo como una institución asegurada en su sistema de información; *Relevancia social*, porque el estudio finalizado va a beneficiar al entorno con seguridad informática, específicamente en los archivos y registros de documentos muy importantes para la institución; *Utilidad metodológica*, porque el estudio terminado va a contribuir como investigación antecedentes a futuros estudios en donde aborden temas tratados en este estudio; *Implicancias prácticas*, porque va a permitir utilizarlo cotidianamente en los procesos de protección de la información de posibles ataques internos y externos; *Valor teórico*, ayuda a conocer mejor las teorías basadas en un sistema de gestión de seguridad de la información y la seguridad informática.

Con el propósito de dar respuesta a los problemas formulados, se plantean los siguientes **objetivos**: *General*: Mejorar la seguridad informática de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022 mediante la implementación de un sistema de gestión de seguridad de la información; *Específicos*: Incrementar el nivel de confidencialidad de la información de la empresa; Incrementar el nivel de integridad de la información de la empresa; Incrementar el nivel de disponibilidad de la información de la empresa.

Asimismo, se planteó la siguiente **hipótesis:** *General:* "La implementación de un sistema de gestión de seguridad de la información mejora la seguridad informática de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022"; ***Específicas:*** *"*La implementación de un sistema de gestión de seguridad de la información incrementa el nivel de confidencialidad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022";

“La implementación de un sistema de gestión de seguridad de la información incrementa el nivel de integridad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022”; “La implementación de un sistema de gestión de seguridad de la información incrementa el nivel de disponibilidad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022”.

II. MARCO TEÓRICO

En el estudio, con el propósito de fundamentar y conocer el estado situacional científico de las dos variables de estudio se analizaron varios **antecedentes** pertinentes, tales como, tesis de repositorios conocidos, papers o artículos de investigación científica, trabajos relacionados con la ciencia, etc.; que ayudaron con conocimientos previos ligados a la problemática planteada para la presente investigación:

Como **antecedentes internacionales**, se tiene:

Arias y Botero (2019) Se trazó como objetivo realizar el proceso de comunicar y orientar sobre las buenas prácticas qué se debe de realizar en contenidos con referencia a seguridad de la información, Indicó que los problemas de seguridad en el objeto de estudio aparecieron en función al tiempo, los que ocasionaron la generación de lineamientos que fundamenten a una estructura sistemática de gestión de seguridad de la información, fue necesario aplicar buenas prácticas con la finalidad de asegurar los activos de datos y comunicación, identificando que los beneficios de esta propuesta, incluidos los análisis del problema permitieron contribuir en la solución del estudio. Encontró también que fue importante para el objeto de estudio concientizar a los empleados en la seguridad sobre información, así como el reforzamiento de los procesos de la seguridad informática y su respectivo manejo de la información dentro del objeto de estudio.

Hidalgo (2017) en su investigación de grado se trazó el objetivo de proponer el perfeccionamiento de un modelo de gerencia de los aspectos de la seguridad informática con fines de la protección y resguardo de la información física y virtual dentro de la institución, para ello desarrolló un diagnóstico, así como el análisis FODA de la información en el espacio de estudio, En donde se brindaban servicios de tipo judicial a usuarios del Ecuador en todo el territorio del país haciendo uso de sus unidades judiciales, el estudio tuvo como finalidad elaborar un modelo de gestión que contribuya en la articulación de un plan estratégico para la organización, así como también, Articular a los productos consignados en función a la seguridad informática, concluyó que el modelo de gerencia, pudo contribuir

significativamente con garantizar la seguridad informática en el sistema y en los procesos realizados en la institución.

Yañez (2017) en su investigación se planteó como objetivo desarrollar el proceso de administrar realizar el monitoreo la documentación, así como el mejoramiento sostenido de la seguridad de la información, aplicó metodología basada en ciclos de aprobación, en donde se establecieron acuerdos y conciliaciones en función a un adecuado y potente sentido de trabajo de equipo con la finalidad d facilitar la instalación de las políticas y procesos de seguridad informática. Se fundamentó en la gestión de riesgos, específicamente en la norma ISO31000, Con la cual se clasificó en función a las prioridades y a las exposiciones de riesgos, así como a sus consecuencias. se logró optimizar la asignación de los medios a proyectos de seguridad, se favoreció la creación de equipos preparados y enfocados en los objetivos más importantes y en el objetivo estratégico, posteriormente el estudio implicó la aplicación de auditorías, del tipo interno y externo. se encontró que las auditorías fueron independientes al equipo auditor, se implementó el SGSI como instrumento de política y procesos de seguridad informática, las dos auditorías concluyeron que la seguridad actual de la información se encontró en un nivel medio.

Romo y Valarezo (2016) en su investigación Se planteó como objetivo desarrollar el proceso de administrar realizar el monitoreo la documentación, así como el mejoramiento sostenido de la seguridad sobre la información, aplicó metodología establecida en ciclos de aprobación, en donde se establecieron acuerdos y conciliaciones en función a un adecuado y potente sentido de trabajo de equipo con la finalidad de facilitar la instalación de las políticas y procesos de seguridad informática. Se fundamentó en la gestión de riesgos, específicamente en la norma ISO31000, Con la cual se clasificó en función a las prioridades y a las exposiciones de riesgos, así como a sus consecuencias. se logró optimizar la asignación de los medios a proyectos de seguridad, se favoreció la creación de equipos enfocados y preparados en los objetivos más importantes y en el objetivo estratégico, posteriormente el estudio implicó la aplicación de auditorías, del tipo interno y externo. se encontró que las auditorías fueron independientes al equipo auditor, se

implementó el SGSI como instrumento de política y procesos de seguridad informática, las dos auditorías concluyeron que la seguridad actual de la información se encontró en un nivel medio.

Pérez (2015) en su investigación tuvo como objetivo principal dar mantenimiento a la integridad, confidencialidad y disponibilidad de los medios de información activos en el objeto de estudio, en donde se aplicó y se fundamentó en la norma ISO/ICE 27002, En donde se siguieron todas las etapas de cumplimiento con propósitos de garantizar la seguridad de la información de la empresa estudiada.

Como **antecedentes nacionales**, se tiene:

Ticona (2022) en su investigación Se planteó como objetivo general establecer el efecto que tuvo el modelo de seguridad de información estudiado, cuya función fue menguar los riesgos de los recursos de información en el espacio de estudio, trabajó con un tamaño de población y tamaño de muestra de 32 trabajadores de la empresa investigada, El estudio fue de tipo descriptivo, de enfoque cuantitativo, de diseño no experimental, aplicó métodos de análisis de campo, así como la observación de la fuente de información y los registros de datos, la hipótesis planteada consistió en el establecimiento de un modelo de seguridad de la información fundamentada en la norma internacional ISO 27001, en donde se indicó que tuvo un efecto significativo y la reducción de los riesgos de seguridad de la información concluyó que el estudio Tuvo resultado positivo dado que se redujo los riesgos a los que se encontraba la información de la organización antes de la presente investigación.

Aguinaga (2021) en su trabajo científico se trazó el objetivo general, desarrollar la creación de un sistema de gestión fundamentado en la norma hizo 27001 del año 2013 con propósitos de establecer o calcular la influencia respecto a la seguridad informática en una organización del tipo financiero. en su estudio aplicó la metodología del tipo cuantitativo en el nivel aplicado, trabajo con un enfoque experimental de subtipo pre experimental. trabajo con un tamaño de muestra de 24 registros por cada indicador. encontró como resultado que, en la confidencialidad de la información, los documentos estuvieron en forma confidencial al inicio en 75.52% y después en 87.36%, En

la dimensión integridad de la información se encontró un rendimiento inicial del 58.83% y después un rendimiento del 76.32%, Mientras que en la dimensión disponibilidad de la información, se encontró un incremento considerable por qué pasó d 96.81% al 99 93%. se concluyó que el sistema de gestión cimentado en la norma ISO indicada influyó positiva y considerablemente en la seguridad del objeto de estudio.

Chavarry (2021) en su estudio científico tuvo como objetivo calcular el impacto que se pudo tener como resultado en el caso de la implementación del estándar internacional ISO 27001 y 27002 acondicionadas para dar garantía de seguridad a los activos informáticos pertenecientes al objeto de estudio. Trabajo un estudio de naturaleza aplicada, como estrategia, aplicó un tipo de diseño cuasi experimental, esto indicó que trabajó con dos muestras, control y experimental, concluyó que la implementación de la variable independiente mejoró los objetivos planteados.

Cahuana y Cahuana (2021) en su investigación trabajó sobre el objetivo de aprender sobre el efecto del uso de un sistema web fundamentado en la normativa ISO 27001 con la finalidad de realizar la gestión de seguridad en la empresa indicada, el estudio fue de tipo recado, de diseño pre experimental y de nivel experimental. se trabajó con una muestra de 30 reportes relacionados con la información generados durante un mes. aplicar un proceso de selección de información mediante la indagación, aplicó ficha de registro. Concluyó que la ejecución del sistema web influenció positiva y realmente en la administración sobre seguridad informática, se encontró que los reportes confidenciales fueron admitidos y entregados en las fechas establecidas, los reportes no sufrieron daños en su integridad, tampoco en su confidencialidad, se encontró que la información fue transmitida y reportada de manera normal, y que el flujo de información tuvo incremento que inició en 171 89% y con la aplicación del sistema se incrementó a 96.89%, es decir se incrementó en un 25% en la satisfacción de los usuarios en función al reporte de información confidencial, inicialmente sin la aplicación del software web se tuvo una media de 69 11%, pero con la aplicación del software llegó a 96 44%, en ese sentido la mejora de satisfacción de los usuarios íntegros se incrementó en 27 33%. Mientras que los usuarios que entregaron sus informaciones pasó de una

satisfacción del 79 44% a un nivel de satisfacción del 96.00%, el incremento fue de 16.56%.

Risco (2021) en su investigación se trazó el objetivo de establecer la influencia del sistema de gestión relacionado con la seguridad informática y cimentada en la norma ISO 27001 del año 2013, en el espacio y objeto de estudio, debido a que encontró espacios de vulnerabilidad en la mayoría de procesos de las áreas de la institución, que peligraba las dimensiones o características de las informaciones respecto a su integridad accesibilidad y confidencialidad. la investigación aplicó el método cuantitativo, fue de tipo aplicado, trabajo con un diseño pre experimental, en donde el tamaño de la población y de la muestra estuvo estructurada por 20 regís en cada indicador con propósito de lograr un conjunto de valores favorables relacionados con las dimensiones de seguridad informática. se encontró que el 68 5% de vulnerabilidad disminuyo hasta el 15.40% para la dimensión integridad, la disponibilidad varió de 52 60% a 11.40%, Por su parte la dimensión vulnerabilidad inicio con 47 15% y bajó a 11.95 por 100, concluyó que en las 3 dimensiones se pudo mejorar la seguridad de la información en un promedio general de 80% a 90% de efectividad.

Zapata (2021) en el estudio publicado se trazó como objetivo principal realizar el análisis de ciertos factores críticos de éxito para propósitos de implantar un sistema de gestión de seguridad relacionados con los activos informáticos institucionales estudiados ubicada en Sechura Piura, aplicó metodología de observación y análisis con diseño descriptivo, con el propósito de determinar los factores críticos, el autor aplicó una entrevista con los elementos de muestra, así como también el instrumento denominado checklist. se encontró como resultados que los factores establecidos en el espacio en estudio fueron 5, Estos fueron el compromiso que tuvo la gerencia la cultura organizacional desplegada por la administración, y el alcance o logro de la seguridad de la información aspectos imaginativos del desempeño del recurso humano, así como la sensibilización. Concluyó qué los factores lograron estrategias en la implementación del sistema de gestión de seguridad que la información en la empresa en estudio, concluyó además que el factor más importante fue la sensibilización, la cual tuvo un impacto de 78 8% esto

se explicó porque en la medición de los otros factores se tuvo que sensibilizar y desarrollar adecuada actitud en la implementación del sistema dentro de la institución.

Alarcón y otros (2020) en el artículo científico presentado indicaron que los continuos avances desarrollados por la tecnología a nivel mundial ha configurado que la administración y manejo de la información fue muy importante para los objetivos estratégicos institucionales, este estudio tuvo como meta analizar el impacto del uso o aplicación de la norma ISO 27001 en la seguridad informática en el objeto estudiado en la capital peruana, en el estudio se aplicó metodología del tipo cuantitativo, la investigación manipuló las variables, por lo tanto, fue del tipo experimental, Trabajó con una muestra de 30 participantes de la misma empresa. concluyo que existió influencia positiva como consecuencia de usar la norma ISO 27001 para asegurar la información en las dimensiones de integridad disponibilidad y confidencialidad.

Poicon y Ramírez (2020) en el estudio científico se trazaron el objetivo principal desarrollar la realización de una propuesta que implicaba alcanzar un sistema de gestión de seguridad informática en una municipalidad con la aplicación de una norma técnica peruana y la norma ISO 27001 del año 2014, en el estudio aplicó un diseño no experimental, el tipo aplicada, como metodología aplicó el PDCA de Deming, con propósito de desarrollar el diseño de un sistema en función a los problemas encontrados tales como, amenazas, problemas de vulnerabilidad e impactos de peligros y riesgos que afectaban a los activos informáticos, realizó una propuesta de políticas e indicadores de control. en el proceso investigativo identificaron 113 activos organizados por categorías y que conformaban la información de la institución el; encontraron que la información presentó un nivel de amenaza considerado como alto en un 57.50%, también encontraron que los tipos de amenazas estuvo en el mal funcionamiento de las computadoras, fallos de conectividad, así como también en pérdidas de apoyo. se encontró que las vulnerabilidades estuvieron en un nivel alto en un 49%, Encontraron que los documentos estuvieron desprotegidos, o protección no apropiada respecto a la vulnerabilidad, los riesgos con un impacto dañino estuvieron entre 15% y 30%,

concluyó que el conocimiento de la línea base contribuyó en la identificación de las brechas de seguridad informática.

Cruz y Huamaní (2019) en el estudio científico se trazó como objetivo principal la sistematización de los procesos de seguridad de la información cimentada en la norma ISO 27001 con los propósitos de mejorar la seguridad con referencia al manejo de información, debido a que encontraron problemas relacionadas con una inadecuada gestión y pérdida de datos e información en la empresa en estudio. Los autores se plantearon planeta de analizar y observar el impacto de la automatización de la seguridad informática con los propósitos de corregir los puntos débiles, así como gestionar adecuadamente cada 1 de los riesgos puedan existir en el sistema de información. los resultados indicaron que la implementación de la automatización relacionada con la seguridad de la información y normada por ISO 27001 permitió corregir satisfactoriamente, así como mejorar la información en el sistema tecnológico institucional.

Rojas (2019) en su investigación se trazó como objetivo desarrollar la implementación de la norma de seguridad ISO 27001 2014 con el propósito de perfeccionar la seguridad del adata información en el objeto de estudio, la cual fue la RENIEC, Institución qué produce volúmenes grandes datos e información como consecuencia de los procesos operativos cotidiano como cumplimiento de su función social, en donde se asumen, tratan y procesan la información y cada tiempo se hace más grande y que deben ser cuidadas y gestionadas de acuerdo a normas. La institución en estudio trabaja con grandes volúmenes de información debido a que se encarga de registrar toda la data información de los ciudadanos del país. el estudio presentó un enfoque del tipo cuantitativo, el tipo de estudio fue aplicado y experimental, mientras que el diseño fue pre experimental, como instrumento aplicó pre y post test. Tuvo como resultado de que la aplicación de la norma contribuyó en una gestión adecuada de las confidencialidad, integridad y disponibilidad de información del objeto de estudio. También se encontró que los resultados pudieron propiciar placer digitación posterior en el nivel ISO 27001 a la institución estudiada.

Chuna (2018) en su estudio se trató como objetivo principal revisar una propuesta con referencia hola aplicación de un sistema de seguridad relativo a la información fundamentado en la norma técnica del Perú, primeramente hizo análisis de los activos tecnológicos y del Estado actual de la información en el espacio de estudio, con las encuestas aplicadas y el uso de ficha de registro encontró que existieron 30 exposiciones vulnerables y 20 situaciones de riesgos, aplicó la metodología Magerit, en donde encontró que el 50% de estos riesgos y de un habilidades fueron muy altos, 40% estuvieron en riesgo alto, 5% en situación de medio y solo un 5% en situación de bajo, el investigador planteó controles y políticas relacionados con la seguridad, que permitieron a la institución garantizar el uso adecuado y aceptable de sus instalaciones tecnológicas informáticas, establecieron dispositivos tecnológicos para enfrentare eventos no deseados mediante el uso planificado de tratamiento de riesgos, establecido en roles y responsabilidades con la finalidad de atender rápidamente los problemas de seguridad, establecieron procedimientos y reglas seguras en la protección de la información.

Aguirre (2018) en la tesis de grado se planteó como objetivo desarrollar el estudio de la influencia cuando se implementa un sistema web en los procesos de gestión de la seguridad de la información, todo ello cimentada en la norma internacional ISO 27001, la aplicó a una empresa que brinda servicios de informática, el autor trabajó con un tipo de estudio aplicado, el diseño implicó no manipulación de variables, es decir fue pre experimental, trabajo con una población establecida por 30 reportes al día con copia de seguridad que se realizaba en servidores de la institución durante un mes, aplicó técnica de recopilación de la data a la observación, aplicó ficha de registro como instrumento de recojo de datos. obtuvo resultados que permitieron la confirmación que quiera implementación del sistema web influyó positivamente en los procesos de gestión de seguridad de la información, lo cual contribuyó a que los reportes sean entregados a tiempo y de manera íntegra.

Maquera y Serpa (Maquera & Serpa, 2017) en el artículo que elaboraron señalaron que varias empresas que estudiaron carecieron de controles de seguridad, en donde no se pudieron dar garantía de seguridad de los activos

infórmate, también indicaron que con el avance tecnológico y administración informática generan situaciones y espacios de riesgos y vulnerabilidades que son fuentes detalles y amenazas y qué buscan disminuir los niveles de la prestación de servicios de los activos en los giros de negocios de cada una de las empresas que no disponen de seguridad de la información. El estudio encontró que cuando simplemente utiliza mecanismos de control para la seguridad de la información fundamentada en ISO 27002, y que cuando ésta norma es aplicada mediante métricas adecuadas en función a una guía desde ese empeño enfocada en la seguridad de la información Pueden garantizar de alguna manera que los activos informáticos puedan sostener sus dimensiones de integridad, accesibilidad y seguridad, Indica que con la aplicación de la norma se han logrado reducir los niveles de riesgo y vulnerabilidad de los activos informáticos.

Ayala (2017) en la tesis de grado se planteó el objetivo de realizar una adecuada evaluación sobre la implantación de un sistema de gestión de seguridad relacionado con la información, así como también determinar la influencia en el proceso de la administración del riesgo en una institución dedicada a la salud, trabajo una investigación aplicada, mientras que el diseño se consideró como de tipo pre experimental, de enfoque cuantitativo, trabajo con una población muestra que estuvo conformado por los activos que demostraron criticidad de información y que intervinieron en la gestión de riesgo en el espacio de estudio, aplicó el instrumento ficha de observación, Determinó la normalidad mediante la prueba de Shapiro Wilk, encontró diferencia en los resultados de la pre prueba y post prueba, aplicó prueba estadística de Wilcoxon, y concluyó que la implantación del sistema propuesto mejoro los procesos de gestión de riesgo en el espacio en estudio.

Olaza (2017) en la investigación realizada se trazó el objetivo de la determinación de la influencia o impacto que pudiera generar la implementación de una norma técnica peruana fundamentada en ISO 27001 en la seguridad de la información en un área del Ministerio de educación, trabajó con un tipo de investigación denominada aplicada, el diseño trabajado fue de tipo pre experimental, esto significó que manipuló la variable independiente, los elementos de la población estuvo constituida por 4783

registros procedentes d los datos de los activos de la información de la institución en estudio, trabajó con un tamaño de muestra de 136 registros, aplicó muestreo probabilístico, en el modo d aleatorio simple, como metodología aplicó la observación, el análisis y la síntesis. Validó sus datos mediante la metodología de juicio de expertos, la confiabilidad se llevó a cabo mediante la prueba de Wilcoxon En donde encontró un p valor menor a 0.05. encontró como resultados que la implementación de la propuesta demostró influencia positiva en la seguridad informática, pasando de 182 casos de riesgos y de generalidades a 50 casos de las mismas, Respecto a los accesos y cambios no autorizados, al inicio se encontró 322 casos, pero con la implementación se redujo a 47 de ellos, la disponibilidad del sistema al inicio estuvo en 70.36%, con la aplicación de la propuesta pasó a 98.22%.

Agurto (2017) en su trabajo investigativo se planteó el objetivo principal de realizar una elaboración diagnóstica de los activos informáticos del objeto de estudio, debido a que una unidad en el área de estudio tenía como función la ejecución de procedimientos en donde se generaron un volumen de información considerable y que por el entorno podría deteriorarse o perderse, aplicó metodología ISO 27001 en todas las unidades de la organización, Mediante la aplicación de continuos reuniones de trabajo entre los integrantes responsables del área de logística informática con el propósito de establecer la identificación y valoración de los activos informáticos, aplicaron como instrumento al cuestionario y también a las listas de cotejo, obtuvo como resultado que el 58% de la pérdida de archivos con documentación especializada fueron de tipo mecánico, de tipo procedimental, tipos de documentación tecnológica, mientras que la fuga de documentos debido a incidencias en información personalizada fue el 33%. concluyó que con la aplicación del diagnóstico se pudo proponer la elaboración de una respuesta técnica fundamentada en la realización de controles de seguridad fundamentada en normas ISO 27001.

Salsavilca (2017) realizar la implementación de ISO 27001 como propósitos de administrar y poner a buen recaudo la información y activos informáticos en el espacio de estudio, para ello aplicó la metodología PDCA o ciclo de Deming, con la finalidad de mejorar ciertos aspectos de calidad, La

aplicación de esta norma tuvo como objetivo facilitar un adecuado control de riesgos y obtener como consecuencia la disminución o evitamiento de falencias en las unidades tecnológicas frente a los ataques internos y externos, así como también a desastres naturales y artificiales que se pudieran dar como evento de riesgo, La investigación fue no experimental, descriptivo, aplicó como metodología la observación y el análisis. Encontró como resultados qué las dimensiones de integridad, confidencialidad y disponibilidad fueron óptimos, esto significó que los activos de información en el espacio en estudio no sufrieron alteraciones en sus contenidos, que los documentos siempre estuvieron disponibles para los usuarios autorizados, asimismo los contenidos de estos documentos solo fueron accesibles por usuarios debidamente autorizados, esto debido a que la confidencialidad estuvo en 192 puntos 23% la integridad en 197 42% y la disponibilidad en un 90.95%, concluyó que la implementación de ISO 27001 redujo satisfactoriamente la cantidad de riesgos relacionados con el activo informático del espacio en estudio.

Maldonado (2016) se trazó el objetivo principal y consistió en la determinación de la influencia del uso de ISO 27001 en seguridad informática en la unidad de registros académicos del espacio y objeto de estudio. el estudio desarrollado fue aplicado, con un nivel de manipulación de variables, es decir experimental, diseño pre experimental, trabajo con una población cuyos elementos en cantidad fueron 26 registros que indicaban riesgos y 26 registros que indicaban cambios debidamente autorizados, aplicó muestreo censal. como metodología aplicó la observación, el instrumento utilizado fue la ficha de observación. encontró como resultados que la aplicación de la norma internacional indicada te mostro influencia o impacto positivo en los registros académicos del espacio y objeto de estudio, cuantitativamente se encontró que redujo los riesgos del 80 8% en etapa del pre test a un 19% en la etapa del post test.

Asimismo, la presente investigación, con fines de fundamentación de las dos variables ha revisado **bases teóricas** provenientes de investigaciones de fuentes primarias y secundarias, son los que a continuación se presentan:

Seguridad, se conceptúa la seguridad como un estado en donde existe relativa ausencia de riesgos y peligros, en donde las condiciones que pudieran causar algún tipo de daños, psicológicos, físicos o de tipo material son debidamente controlados y evitados con el propósito de cuidar y garantizar la seguridad del recurso humano involucrado en una determinada actividad. También se considera a la seguridad como un estado que contribuye en el conocimiento de qué debe tenerse en cuenta, en que debe de analizarse y conocerse para qué eventos contrarios no puedan suceder. para que una institución logre un determinado nivel de seguridad, incluso el nivel óptimo, siempre va a requerir de Recursos Humanos, de normas, intervenciones de comunidades y gobiernos en donde se busque la concientización comunitaria respecto a la seguridad, en donde se contribuya en la protección de los estados situacionales físicos y psicológicos de la persona. con garantizar la seguridad se busca prevenir accidentes e incidentes, que para la investigación, se hace referencia a la seguridad de los activos informáticos, los cuales pueden ser archivos, registros, ambos de tipo físico o digital (INSPQ, 2018). Para Foucault (2016 pág. 88), los activos informáticos de cualquier tipo de empresa merecen ser bien resguardados, esto significa que los activos de la información deben tener seguridad, específicamente en sus dimensiones de integridad, accesibilidad Y confidencialidad (Esther, y otros, 2011).

Gestión de seguridad, Se denomina así a la integralidad de las responsabilidades que tiene que desarrollar cualquier tipo de institución con la finalidad de realizar actividades pertinentes en el cuidado, reducción de riesgos, reducción de peligros, reducción de vulnerabilidades; tanto en hardware como en software, así como en las conductas de los usuarios respecto a una determinada función o desempeño laboral cuando hacen uso de la tecnología de la información. también se entiende como que es una función que contribuye en el perfeccionamiento del objeto de estudio porque va a reducir y predecir amenazas internas y externas configurados como ataques informáticos. se considera a la gestión de la seguridad informática como un conjunto de actividades estratégicas enfocados y direccionados hacia el cuidado y aseguramiento de la información, sobre todo información

confidencial. realizar procesos de gestión de seguridad son acciones preventivas para poder enfrentar cualquier tipo de ataque informático y de esta manera garantizar la integridad, accesibilidad y confidencialidad de la documentación que forma parte del activo informático de la empresa (Riquelme, 2022). A pesar de la importancia que se le debe prestar a los aspectos de seguridad informática, todavía existen instituciones que no son conscientes de los problemas que se pueden generar cuando el sistema de información carece de una seguridad adecuada, generalmente esto sucede en pequeñas empresas, mientras que en las grandes empresas, en su gran mayoría, le brindan la importancia necesaria por qué trabajan con documentación bastante sensible y confidencial, en este caso es el valor de la documentación informática la que contribuye a que las empresas brinden la importancia debida a la seguridad de la información (INERCO, 2020). Esta variable generalmente gestionada por un equipo especializado Sin efectos técnicos y aspectos computacionales, presenta muchas veces cierta complejidad debido a que la seguridad de la información puede estar sujeto a ataques provenientes del exterior ir del interior de la empresa, Es por ello que debe valerse de personal adecuado para garantizar al personal idóneo para que garantice la seguridad en el uso y acceso de la información institucional; también debe disponer de personal alternativo en el caso de que los titulares deseen abandonar la institución (Red IRIS, 2020).

Sistema de gestión de seguridad de la información (SGSI), existen programas o software que contribuyen en el apoyo de realizar procesos operativos y administrativos concernientes a la seguridad de la información, estos tipos de sistemas apoyan en las actividades, en las políticas, las actividades y en el uso de recursos con fines de protección de la información institucional. Un SGSI es concebido desde un enfoque sistemático como un software que apoya en el establecimiento, monitoreo, ejecución, implantación, mantenimiento, supervisión, mejoramiento y evaluación de la seguridad de un sistema de información en cualquier espacio, estos pueden ser cualquier tipo de empresa privado o público, este tipo de programa contribuye en el alcance seguro de objetivos, así como en garantizar la seguridad integral del sistema, y específicamente en la documentación, cuidando la integridad, la

accesibilidad y confidencialidad de la documentación informática (INACAL, 2020). Los beneficios de Software de gestión de la seguridad presenta varios beneficios a la empresa que tiene implementado en su sistema, uno de estos beneficios consiste en que acelera reproceso de implantación del sistema de gestión, el beneficio consiste en disminuir el tiempo y los costos, así como también presenta las partes más importantes de las pruebas de la existencia de los riesgos, ayuda en el cumplimiento y optimización de la aplicación de la norma ISO 27001 del año 2013, facilita el trabajo en equipo, así como también reduce el margen de error y perder tiempo en el desarrollo de su propio sistema de seguridad, con este software se logra una integración fácil de la documentación y los procesos correspondientes (Calder y Alan, 2016).

Seguridad de la información, se mide en función a métricas de seguridad relacionados con la información, estas métricas son indicadores qué indican los niveles de seguridad y como tal ayudan a tomar decisiones que, respecto a la misma seguridad, existen 3 métricas bastante conocidas cuando se trata de medir las dimensiones de la seguridad informática de una institución, Estas son la disponibilidad, la integridad y la confidencialidad (Cano, 2018). La métrica de disponibilidad hace referencia aquí la documentación informática debe ser accedida por personal autorizado sin ninguna restricción de tiempo y espacio, es decir, todo usuario autorizado debe acceder cuando lo desea a la información, que por norma y desempeño laboral, le corresponde a acceder; Como se puede observar, la disponibilidad es una dimensión de la seguridad situacional de la informática muy significativo debido a que siempre se hace necesario que el usuario deba acceder oportunamente a los archivos a las cuales tiene acceso y pueda trabajar con ella sin ningún tipo de restricción. La métrica de confidencialidad hace referencia a qué la documentación informática debe ser conocida solo por un conjunto de personas autorizadas, no debe ser conocida por personas quienes no tienen la autorización para saberlo y divulgarlo; esto sucede cuando la documentación es de vital importancia y de mucho valor para la institución, en ese sentido solo pueden Darlo a conocer personal autorizado, Y a que otro tipo de personal puede darlo mal uso o utilizarlo contra la institución. La métrica integridad hace referencia a que un documento informático no ha sido alterado, ni modificado, por lo

tanto, conserva la totalidad de la información. en los ataques informáticos, los atacantes pueden robar toda la información, pueden manipular o alterar el contenido, así como también no permitirle al verdadero usuario a modificar o acceder a la información. tomando en cuenta estas 3 métricas o dimensiones, se hace necesario de toda institución debe desarrollar conciencia de la necesidad y el valor de la seguridad informática (Solano (2020).

Familia de normas internacionales *ISO 27000*, cada norma tiene reservado un número los cuales van desde 27000 hasta 27019 y de 27030 a 27044. Las normas ISO se encuentran estandarizadas, es de aplicación internacional, se aplican en diversas ramas del saber humano, pero las relacionadas con la seguridad informática constituyen una familia de normas dentro del estándar ISO 27000, generalmente es gratuita, pero en ciertos casos implica un costo que tiene que pagar la empresa que desea implementar; la norma ISO 27001 del año 2013 da un conjunto de requisitos sobre la gestión, la ejecución y el mantenimiento de la seguridad de la información en toda empresa, Constitución que desee certificarse en este tipo de norma. Por su parte ISO 27002 está contenido en un manual de buenas prácticas en donde se indican todas las metas relacionadas con el control y evaluaciones recomendadas por esta norma en función a la seguridad informática, Dispone de 33 objetivos de control y 133 controles de forma agrupada en donde contiene 11 dominios distintos, alcanza información necesaria para usar el ciclo PHVA (Planificar, Hacer, Verificar y Actuar) de Deming relacionado con la calidad. ISO 27004 En donde se alcanzan las técnicas métricas que pueden ser aplicadas en el establecimiento de la eficacia de un sistema que garantice la seguridad informática, así como también alcanza los controles pertinentes. Por su parte, ISO 27005; ISO 27005, enfocados en procesos administrativos relacionados con los riesgos de la seguridad informática, apoya las concepciones generales enmarcados dentro del ISO 27001, contribuye en la aplicación de manera satisfactoria en el asentamiento de la información cimentada en gestión de riesgos, para el entendimiento de esta norma se requiere del dominio de los conceptos, procesos, modelos y el conocimiento de los términos indicados en las normas ISO 27002 y 27001 (IsoTools, 2015).

Esta norma también dispone de un conjunto ni conceptos enfocados en la investigación, estos son:

Activo informático, los registros de datos históricos, los documentos escritos o en estado digital, o cualquier otro tipo de información constituyen activos informáticos para cualquier institución, son recursos que se generan como parte del desarrollo de las actividades institucionales, se elaboran para ser difundidos para conocimiento de todo el recurso humano o parte de ella, son requeridos en los procesos de negocios para garantizar su sostenibilidad y competitividad; dada su importancia, es que se hace necesario su protección, sobre todo de la documentación privilegiada para la empresa; la adecuada gestión y administración de estos documentos contribuye en que las autoridades puedan tomar decisiones fundamentales para la buena marcha de estas organizaciones (PJGROUP, 2020).

Control de seguridad, con este proceso, se garantiza la seguridad de los activos, el software, hardware, así como a las instalaciones y la documentación en donde se encuentran los datos, insumo de principal interés en el crecimiento de la organización, estos deben estar totalmente protegidos contra cualquier ataque interno o externo, se debe dar seguridad frente a daños eventuales, así como al uso no legal de los documentos o información (AUDITOOL, 2022).

Dominio de seguridad, cuando los archivos, así como toda la información digital acumulada en el sistema informático o sistema de información de una organización se encuentra debidamente protegida, entonces se indica que se tiene dominio de seguridad. de acuerdo con ISO 27002, el dominio de política de seguridad tiene como finalidad alcanzará la institución el soporte y la gestión administrativa requerida para dotar de seguridad a la información cumpliendo requisitos y requerimientos totalmente legal, el dominio denominado ente de seguridad informática establece un marco referencial desde la dirección con fines de implantar y controlar la seguridad de la información en la institución, el dominio seguridad de los Recursos Humanos quién es la finalidad de establecer medidas requeridas y suficientes para asegurar la vigilancia correspondiente a la seguridad de la información, esto hace referencia al manejo y a los usuarios el sistema de información, el

dominio seguridad física y del ambiente, tiene por finalidad, la protección de las instalaciones e información de tipo sensible, el dominio administración de procesos comunicaciones y operativas con la finalidad de establecer los procesos y responsabilidades en la parte operativa con fines de avalar Los procesos relacionados al aseguramiento de la información; el dominio denominado control de acceso, busca asegurar los procesos de accesibilidad del usuario del sistema de información debidamente autorizado al activo de información, es decir, a los registros, archivos físicos o digitales de la organización; El dominio adquisición desarrollo y mantenimiento, tiene como finalidad a que las organizaciones apliquen y ejecuten un sistema de software de manera interna, o en todo caso puedan convenir a una organización para que desarrolle dicho proceso; el dominio gestión de incidentes, trata de aplicar la mejora continua cuando ocurran incidentes relacionados con la seguridad de la información; el dominio denominado gestión de la sostenibilidad institucional como finalidad asegurar el sostenimiento de la institución haciendo uso de los controles para que de esta manera puedan evitar o reducir cualquier tipo de suspensión en la actividad institucional, los cuales pueden generar impactos negativos, por último, el dominio cumplimiento busca dar garantía a que se cumplan los requisitos legales Respecto a la seguridad informática en función a la aplicación de diseño operatividad y uso en los sistemas informáticos (ISOTools, 2018).

En cuanto a las **metodologías, marcos de trabajo o normas internacionales/nacionales candidatas** para la solución propuesta, se tiene:

Norma ISO/IEC 27002:2013, determina los lineamientos y principios normativos de manera general respecto al inicio, implantación, mantenimiento y perfeccionamiento de las tareas relacionados con la gestión de seguridad informática en cualquier tipo de institución. presenta como objetivos el lineamiento de tipo general enfocados en los objetivos para el logro de la seguridad informática que son aceptados de modo general. esta norma tiene como finalidad su implementación enfocada siempre, en la satisfacción de requerimientos sin necesidades en un proceso de evaluación de peligros y riesgos; esta norma puede ser utilizada como una línea práctica en el desarrollo de estándares relacionados con la seguridad y en la parte operativa

de la gestión para garantizar seguridad efectiva y contribuir en la construcción de confianza en el establecimiento de tareas acordadas por la empresa (ISO, 2013).

Norma nacional NTP-ISO/IEC 17799, considerada como una norma técnica nacional, tiene como finalidad ayudar en los procesos de implementación de la seguridad informática en organizaciones nacionales, busca mejorar e incrementar la generación de valor en dichas organizaciones, busca, direccionar controlar y alcanzar soporte en los procesos de administración de la seguridad informática en coherencia con sus respectivos requisitos, así como también con las normas y regulaciones previamente establecidas. para su aplicación se tienen que establecer claramente las políticas de seguridad de la información a seguir, estas políticas deben ser publicadas para conocimiento de todos los involucrados (ISO, 2005).

Marco de trabajo NIST SP-800, establece un marco referencial de cómo se debe operar frente a los procesos de dar seguridad a la información, contribuye con políticas concernientes con la seguridad de la información, alcanza procesos y direcciones Para asegurar la información, apoyen la gestión y en la praxis operativa para garantizar la seguridad informática. este marco de trabajo ayuda en la evaluación de los riesgos alcanzando 6 fases o etapas para mejorar la seguridad de la información, las cuales son proceso de categorización, selección, puesta en práctica, evaluación, autorización y monitoreo (NIST, 2016).

En base a las tres metodologías/marcos de trabajo, se eligió la aplicación del **método de juicio experto** en la elección de la metodología más conveniente en el objetivo de dar solución, se eligió a la norma internacional ISO/IEC 27002:2013 - ver Anexo 3.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

- **Tipo de investigación**

  Fue de tipo aplicada debido a que se han aplicado los conocimientos científicos relacionados con ambas variables (Euroinnova, 2020).

- **Diseño de investigación**

  Pre experimental porque se ha trabajado con un solo grupo experimental, los elementos de la muestra no sean seleccionados de manera aleatoria, se ha manipulado la variable independiente, y se han tomado dos observaciones o mediciones durante todo el proceso investigativo (QuestionPro, 2021).

3.2. Variables y operacionalización

- **Variables**

  - **Variable independiente:** Sistema de gestión de seguridad de la información

    - **Definición Conceptual:**

      "Cualquier sistema relacionado con la seguridad de la información se entiende como un sistema integrado de elementos que van a ejecutar un conjunto de procesos, aspectos normativos, aplicaciones de normas, desarrollo de actividades, los cuales son debidamente planificados, organizados y administrados por una autoridad competente de la organización que se ha planteado como objetivo garantizar la protección de la información" (INACAL, 2020).

    - **Definición operacional:**

La medición de esta variable implica el uso de normas, políticas, actividades y procesos enfocados en la seguridad de los activos informáticos dentro de las instituciones.

- **Variable dependiente:** Seguridad informática
  - **Definición Conceptual:**

    Hacen referencia a elementos sistémicos mecanizados y dinámicos cuya función es proteger de ataques internos y externos, así como de manipulación de datos hacia los activos de valor e importancia para una determinada institución (Andrade, 2018).

  - **Definición operacional:**

    La medición operacional se desarrolla por el nivel de que el acceso sea confiable, de que la información no haya sido cambiada, y que esté disponible para quienes realmente puedan accederla.

- **Operacionalización**

La tabla matricial de operaciones de las variables se alcanza a nivel de detalle en el Anexo 2.

3.3. Población, muestra y muestreo:

- **Población (N)**

Se estructuró con usuarios de los documentos e información del espacio de estudio.

Tabla 1. *Población*

Cargo / Puesto	Cantidad

Gerente general	1
Jefe de área	3
Operario	4
Total	8

Fuente: (Elaboración propia, 2022)

$$N = 8\, colaboradores$$

- **Muestra (n)**

Porque la población tuvo 30 elementos, por lo tanto, la muestra tuvo la mima dimensión:

$$n = N = 8\, personas$$

- **Muestreo**

Se eligió un tipo de muestreo no probabilístico porque cada elemento de muestra fue seleccionado a conveniencia.

3.4. Técnicas e instrumentos de recolección de datos:

- **Técnicas:**
  - Encuesta.
  - Análisis documental.

- **Instrumentos:**
  - Cuestionario (Encuesta).
  - Ficha de datos (Análisis documental).

Tabla 2. *Recolección de datos*

Dimensión	Indicador	Técnica	Instrumento
Confidencialidad	Nivel de confidencialidad de la información	Encuesta	Cuestionario
Integridad	Nivel de integridad de la información	Encuesta	Cuestionario
Disponibilidad	Nivel de disponibilidad de la información	Encuesta	Cuestionario

Fuente: (Elaboración propia, 2022)

- **Validez y confiabilidad:**

La validez, es conceptuado cómo qué es el nivel en que un instrumento tiene que medir a la variable que necesariamente debe medir, esto significa que el instrumento cumple el objetivo para el cual ha sido diseñado (Arribas, 2014).

Los cuestionarios de ese estudio fueron analizados por el grado de validez, fueron tres expertos quienes validaron el instrumento, las siguientes tablas 3, 4 y 5 evidencian la validez.

Tabla 3. *Validez por juicio experto del cuestionario del indicador "Nivel de confidencialidad de la información"*

N°	Experto	Grado académico	Puntaje	Observación
1	Agreda Gamboa, Everson David	Doctor	85%	Aplicable
2	Mendoza Rivera, Ricardo Darío	Doctor	80%	Aplicable
3	Córdova Otero, Juan Luis	Maestro	90%	Aplicable
	Promedio		85%	Aplicable

Fuente: (Elaboración propia, 2022)

Esta validez se hizo por medio virtual con tres expertos para que puedan validar el instrumento “Nivel de confidencialidad de la información”, se puede constatar en el Anexo 4 - Dimensión “Confidencialidad”, la cual obtuvo un ponderando de 85%, lo que demuestra que el nivel de confianza del instrumento es aplicable.

Tabla 4. *Validez por juicio experto del cuestionario del indicador “Nivel de integridad de la información”*

N°	Experto	Grado académico	Puntaje	Observación
1	Agreda Gamboa, Everson David	Doctor	85%	Aplicable
2	Mendoza Rivera, Ricardo Darío	Doctor	80%	Aplicable
3	Córdova Otero, Juan Luis	Maestro	90%	Aplicable
	Promedio		85%	Aplicable

Fuente: (Elaboración propia, 2022)

Esta validez se hizo por medio virtual con virtual del cuestionario a tres expertos para que puedan validar la ficha del indicador “Nivel de integridad de la información”, se puede constatar en el Anexo 4 - Dimensión “Integridad”, la cual obtuvo un ponderando de 85%, lo que demuestra que el nivel de confianza del instrumento es aplicable.

Tabla 5. *Validez por juicio experto del cuestionario del indicador “Nivel de disponibilidad de la información”*

N°	Experto	Grado académico	Puntaje	Observación
1	Agreda Gamboa, Everson David	Doctor	85%	Aplicable
2	Mendoza Rivera, Ricardo Darío	Doctor	80%	Aplicable
3	Córdova Otero, Juan Luis	Maestro	90%	Aplicable

	Promedio	85%	Aplicable

Fuente: (Elaboración propia, 2022)

Esta validez se hizo por medio virtual con el cuestionario a tres expertos para que puedan validar la ficha del indicador “Nivel de disponibilidad de la información”, como se puede constatar en el Anexo 4 - Dimensión “Disponibilidad”, la cual obtuvo un ponderando de 85%, lo que demuestra que el nivel de confianza del instrumento es aplicable.

La confiabilidad, es conceptuada como el grado instrumento aplicado varias veces hacia un objeto de estudio da el mismo resultado o valor con cierta precisión, la repetición del mismo valor es la que genera confianza en su medición (Arribas, 2014).

El nivel de confiabilidad se alcanza en el anexo 8, en ella se reflejan los valores para describir el nivel de confianza alcanzado por el instrumento de la presente investigación.

En el establecimiento de la confiabilidad, existen varias técnicas para determinar la confiabilidad de un instrumento, no obstante, el más utilizado es Alfa de Cronbach, A la cual se le considera como un método de consistencia interna y que se fundamenta y correlaciones promedio entre las preguntas.

La confiabilidad para el instrumento del indicador *“Nivel de confidencialidad”*, según el coeficiente Alfa de Cronbach en el SPSS v26 es de 0,850, que significa que la viabilidad es *Elevado*; por tanto, el instrumento es confiable, para el presente estudio.

Tabla 6. *Confiabilidad del indicador "Nivel de confidencialidad de la información"*

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,850	8

Fuente: Elaboración propia

La confiabilidad para el instrumento del indicador *"Nivel de integridad de la información"*, según el coeficiente Alfa de Cronbach en el SPSS v26 es de 0,845, que significa que la viabilidad es *Aceptable*; por tanto, el instrumento es confiable.

Tabla 7. *Confiabilidad del indicador "Nivel de integridad"*

Tabla de confiabilidad del instrumento	
Alfa de Cronbach	N de elementos
,845	8

Fuente: Elaboración propia

La confiabilidad para el instrumento del indicador *"Nivel de disponibilidad"*, según el coeficiente Alfa de Cronbach en el SPSS v26 es de 0,848, que significa que la viabilidad es *Aceptable*; por tanto, el instrumento es confiable.

Tabla 8. *Confiabilidad del indicador "Nivel de disponibilidad"*

Tabla de confiabilidad del instrumento	
Alfa de Cronbach	N de elementos
,848	8

Fuente: Elaboración propia

3.5. Procedimientos

El presente estudio científico busca dar respuesta a tres objetivos específicos (Oe):

- Oe_1: Incrementar el nivel confidencial de la información

  Se procedió con el recojo de datos con referencia a la dimensión confidencialidad del objeto de estudio aplicando la encuesta y como instrumento al cuestionario (Anexo 4).

- Oe_2: Incrementar el nivel integro de la información

  Se procedió con el recojo de datos con referencia a la dimensión integridad del objeto de estudio aplicando la encuesta y como instrumento al cuestionario (Anexo 4).

- Oe_3: Incrementar el nivel disponible de la información

  Se procedió con el recojo de datos con referencia a la dimensión disponibilidad del objeto de estudio aplicando la encuesta y como instrumento al cuestionario (Anexo 4).

3.6. Método de análisis de datos

Se ha aplicado la estadística descriptiva e inferencial con la finalidad de procesar y desarrollar y dar tratamiento analítico a la data recabada. Asimismo, se aplicó el método deductivo como parte de la interpretación de la población a lo obtenido, es decir, de lo general hacia lo específico.

3.7. Aspectos éticos:

Los autores declaran la autoría del presente estudio, dejan constancia expresa que es el resultado del trabajo arduo, consciente; sostienen que es un trabajo muy original, en donde se ha respetado los conocimientos de cada uno de los investigadores a quienes se les ha citado teniendo en cuenta la metodología indicada. Los autores se han ceñido al Código de ética de la Universidad para propósitos de cumplir

con lo exigido en lo que respecta a las conductas éticas de la investigación. Se ha cumplido con todo lo exigido en los códigos de ética respecto a la libertad, respeto, integridad; la aplicación del sistema antiplagio prepuesto por la universidad ha dado la garantía de que la presente investigación en todo su contenido confirma la originalidad y pertenencia como trabajo del equipo investigador.

IV. RESULTADOS

De acuerdo con las dimensiones planteadas se presentan los siguientes resultados:

- **Análisis descriptivo**

Con el propósito de demostrar los resultados del presente estudio, Se ha llevado a cabo una descripción analítica de las dimensiones previa medición, para luego aplicar el sistema de gestión de seguridad informática (SGSI).

1. Análisis estadístico descriptivo de la dimensión “Nivel de confidencialidad de la información”

A continuación, se visualiza el análisis estadístico descriptivo de la muestra en la Prueba antes y Prueba después:

Tabla 6. Análisis descriptivo - Indicador “Nivel de confidencialidad de la información”

	N	Mínimo	Máximo	Media	Desv. Desviación
NCI-PrePrueba	8	1,38	1,75	1,6100	,16603
NCI-PosPrueba	8	4,25	5,00	4,5729	,33767
N válido (por lista)	8				

Fuente: Base de datos

Se observa en la tabla 9 que la dimensión confidencialidad previo a la aplicación de la variable independiente, que en este caso es el sistema de gestión aplicado, presentó un promedio de 1.61 respecto a satisfacción, luego de aplicar el sistema de gestión de seguridad o variable independiente, el promedio fue de 4.57 respecto a la satisfacción; los resultados indicaron un aumento de 2.96 en la satisfacción, la variación porcentual fue de 59.20%. Se encontró que el valor mínimo en la prueba antes fue 1.38 y en el después 4.25 ambos en insatisfacción, así mismo, en la prueba después el valor mínimo fue 4.25 y 5.00 respectivamente en el nivel

de satisfacción. Estos resultados indicaron que existió un aumento en la confidencialidad de la información luego de implementar el sistema con la cual se gestionó la seguridad. La siguiente figura gráfica estos resultados.

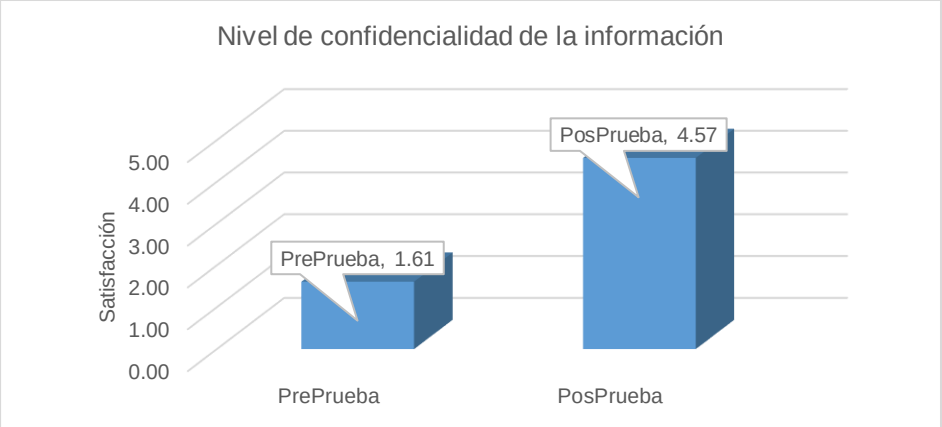


Figura 1. Medias de pre prueba y pos prueba del nivel de confidencialidad de la información

2. Análisis estadístico descriptivo del indicador “Nivel de integridad de la información”

A continuación, se visualiza el análisis estadístico descriptivo elaborado de indicador en función a la Pre Prueba y Pos Prueba en la tabla 11:

Tabla 7. Análisis descriptivo - Indicador “Nivel de integridad de la información”

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
NII-PrePrueba	8	1,38	1,75	1,5650	,19777
NII-PosPrueba	8	4,38	5,00	4,6600	,23652
N válido (por lista)	8				

Fuente: base de datos

Se observa en la tabla 11 que la dimensión integridad previo a la aplicación de la variable independiente, que en este caso es el sistema de gestión aplicado, presentó un promedio de 1.57 respecto a satisfacción, luego de aplicar el sistema de gestión de

seguridad o variable independiente, el promedio fue de 4.66 respecto a la satisfacción; los resultados indicaron un aumento de 3.09 en la satisfacción, la variación porcentual fue de 61.80%. Se encontró que el valor mínimo. En la prueba antes fue 1.38 y el valor máximo 1.75 respecto a satisfacción, así mismo, en la prueba después, el valor mínimo fue 4.38 y 5.00 respectivamente en el nivel de satisfacción. Estos resultados indicaron que existió un aumento en la integridad de la información luego de implementar el sistema con la cual se gestionó la seguridad. La siguiente figura gráfica estos resultados.

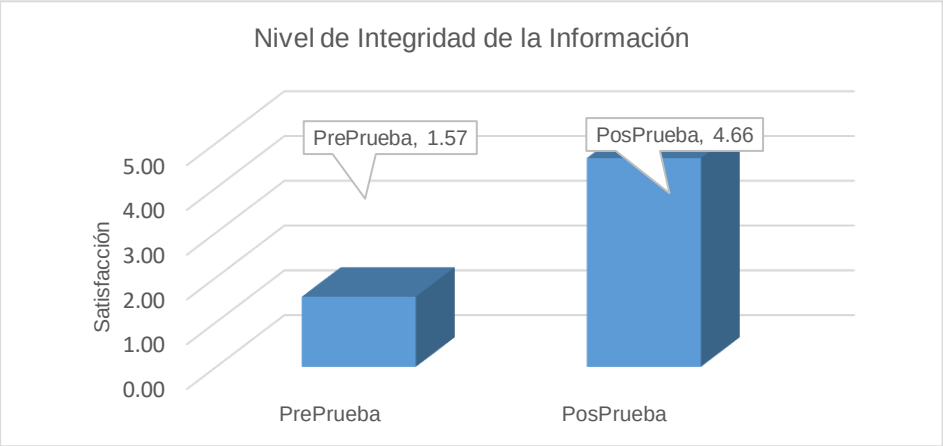


Figura 2. Medias de pre prueba y pos prueba del nivel de integridad de la información

3. Análisis estadístico descriptivo del indicador "Nivel de disponibilidad de la información"

En la tabla 11 se visualiza el análisis estadístico descriptivo elaborado para el indicador en la Pre Prueba y Pos Prueba:

Tabla 8. Análisis descriptivo - Indicador "Nivel de disponibilidad de la información"

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
NDI-PrePrueba	8	1,25	1,88	1,5020	,23520
NDI-PosPrueba	8	4,63	5,00	4,7280	,16069
N válido (por lista)	8				

Fuente: base de datos

Se observa en la tabla 11 que la dimensión disponibilidad previo a la aplicación de la variable independiente, que en este caso es el sistema de gestión aplicado, presentó un promedio de 1.50 respecto a satisfacción, luego de aplicar el sistema de gestión de seguridad o variable independiente, el promedio fue de 4.73 respecto a la satisfacción, lo cual generó un aumento de 64.60%. Se encontró que el valor mínimo en la prueba antes fue 1.25 y el valor máximo 1.88 respecto a satisfacción, así mismo, en la prueba después, el valor mínimo fue 4.63 y 5.00 respectivamente en el nivel de satisfacción. Estos resultados indicaron que existió un aumento en la disponibilidad de la información luego de implementar el sistema con la cual se gestionó la seguridad. La siguiente figura gráfica estos resultados.

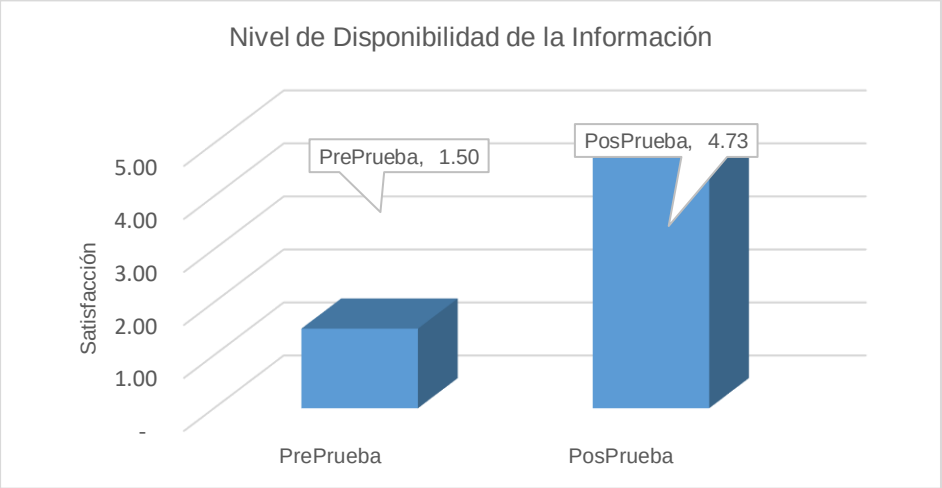


Figura 3. Medias de pre prueba y pos prueba del nivel de disponibilidad de la información

- **Análisis inferencial**

Antes de la comprobación de hipótesis, se debe desarrollar la estadística inferencial, para sello se ha usado el estadístico de prueba de normalidad por cada una de las dimensiones. Se aplicó Shapiro - Wilk porque el tamaño de la muestra fue menos de 30 registros, usó para establecer si los datos presentaron conducta normal.

1. Prueba de normalidad de la dimensión “Nivel de confidencialidad”

En el cálculo de la normalidad de la dimensión confidencialidad, se valoraron los resultados alcanzados con el p valor obtenidos en ambas pruebas. Para ello, se utilizaron las hipótesis de normalidad y se estableció la significancia en 0.05.

H_0: La dimensión “Nivel de confidencialidad” (sin que se implemente el sistema de gestión de seguridad de la información) si tiene distribución normal.

H_1: La dimensión “Nivel de confidencialidad de la información” (con implementación del sistema de gestión de seguridad de la información) no tiene distribución normal.

El nivel de significancia: $\alpha = 0.05$

Sig. > 0.05, se acepta (H_0)

Sig. <= 0.05, se acepta (H_1)

Tabla 9. *Prueba de Normalidad - Indicador “Nivel de confidencialidad”*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Confianza antes	,566	8	,000
Confianza después	,641	8	,000

Fuente base de datos

En la Tabla 12**,** se observa que el p valor de la Pre Prueba o confianza antes es de 0.000, es menor a 0.05; en ese sentido, se rechazó la hipótesis nula pero se aceptó la hipótesis alternativa lo cual indicó que los datos de la dimensión nivel de integridad antes no presentó distribución normal; en los datos de nivel de confianza después se visualiza que el p valor de la dimensión nivel de confianza después es de 0.000, menor a 0.05; en concordancia a estos resultados, se rechazó hipótesis nula que indicó que la dimensión nivel de confianza después si tuvo una distribución normal y se aceptó la hipótesis alternativa en donde se indicó que los datos no presentaron distribución normal, por tanto, se aplicó la prueba de Wilcoxon.

2. Prueba de normalidad de “Nivel de integridad”

En el cálculo de la normalidad de la dimensión integridad, se valoraron los resultados alcanzados con el p valor obtenidos en ambas pruebas. Para ello, se utilizaron las hipótesis de normalidad y se estableció la significancia en 0.05.

H_0: La dimensión “Nivel de integridad” (sin la implementación del sistema de gestión de seguridad de la información) si tiene distribución normal.

H_1: La dimensión “Nivel de integridad” (con la implementación del sistema de gestión de seguridad de la información) no tiene distribución normal.

En estos casos el nivel de significancia: $\alpha = 0.05$

Sig. > 0.05, se acepta (H_0)

Sig. <= 0.05, se acepta (H_1)

Tabla 10. *Prueba de Normalidad - Indicador "Nivel de integridad de la información"*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Integridad antes	,418	8	,000
Integridad después	,566	8	,000

Fuente: base de datos

En la Tabla 13**,** se observa que el p valor de la Pre Prueba o integridad antes fue 0.000, es menor a 0.05; en ese sentido, se rechazó la hipótesis nula pero se aceptó la hipótesis alternativa lo cual indicó que los datos de la dimensión nivel de integridad no presentaron distribución normal; en los datos de integridad después se visualizó que el p valor de la dimensión integridad después fue 0.000, fue menor a 0.05; en concordancia a estos resultados, se rechazó hipótesis nula que indica que la dimensión integridad después si presentó una distribución normal y se aceptó la hipótesis alternativa en donde se indicó que los datos no presentaron distribución normal, por tanto, se aplicó la prueba de Wilcoxon.

3. Prueba de normalidad de la dimensión "Nivel de disponibilidad de la información"

En el establecimiento de la normalidad de la dimensión disponibilidad, se valoraron los resultados alcanzados con el p valor obtenidos en ambas pruebas. Para ello, se utilizaron las hipótesis de normalidad y se estableció la significancia en 0.05.

H_0: La dimensión "Nivel de disponibilidad" (sin la implementación del sistema de gestión de seguridad de la información) si tiene distribución normal.

H_1: El indicador "Nivel de disponibilidad" (con la implementación del sistema de gestión de seguridad de la información) no tiene distribución normal.

En ambos casos se estima el nivel de significancia: α = 0.05

Sig. > 0.05, se acepta (H_0)

Sig. <= 0.05, se acepta (H_1)

Tabla 11. *Prueba de Normalidad - Indicador "Nivel de disponibilidad"*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Disponibilidad antes	,641	8	,000
Disponibilidad después	,641	8	,000

Fuente: base de datos

En la Tabla 14**,** se observa que el p valor de la Pre Prueba o nivel de disponibilidad antes fue 0.000, fue menor a 0.05; en ese sentido, se rechazó la hipótesis nula y se aceptó la hipótesis alternativa, lo cual indicó que los datos de la dimensión nivel de disponibilidad no tuvieron distribución normal; en los datos de nivel de disponibilidad después se visualizó que el p valor de la dimensión nivel de disponibilidad después fue 0.000, fue menor a 0.05; de acuerdo a estos resultados, se rechazó hipótesis nula que indicó que la dimensión nivel de disponibilidad después si tuvo una distribución normal y se aceptó la hipótesis alternativa en donde se indicó que los datos no tuvieron distribución normal, por tanto, se aplicó la prueba de Wilcoxon.

- **Contrastación de hipótesis**

De acuerdo con las pruebas aplicadas para el cálculo de la normalidad para cada una de las dimensiones que sintieron distribución no normal, se aplicó la prueba de Wilcoxon, la cual es una prueba no paramétrica.

Para desarrollar la contrastación de las hipótesis específicas se han desarrollado los siguientes pasos:

1. Hipótesis específica N° 1

"La implementación del sistema de gestión de seguridad de la información incrementa el nivel de confidencialidad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022".

Esta dimensión, al tener datos que no se comportan como datos de una distribución normal tanto en la pre y post prueba, o antes y después, se ha optado por aplicar la prueba de Wilcoxon; por lo tanto, se han formulado ambos tipos de hipótesis, con su respectiva significancia de 0.05.

Hipótesis:

H_0: "El sistema de gestión de seguridad de la información no incrementa el nivel de confidencialidad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022".

$$H_0: NCIa >= NCIp$$

Se puede determinar que no existe incremento de la dimensión.

H_1: "El sistema de gestión de seguridad de la información si incrementa el nivel de confidencialidad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022".

$$H_1: NCIa < NCIp$$

Se puede determinar que si existe incremento de la dimensión.

Nivel de significancia: α = 0.05.

Sig. > 0.05, se acepta (H_0) que es la hipótesis nula

Sig. <= 0.05, se acepta (H_1) que es la hipótesis alternativa

Tabla 12. Prueba Wilcoxon para el nivel de confidencialidad

Estadísticos de prueba [a]

	Confianza después - Confianza antes
Z	-2,549[b]
Sig. asintótica(bilateral)	,011

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Tal como se puede observar en la tabla 15, la contrastación de la hipótesis por medio del estadístico o prueba de Wilcoxon, la significancia o p valor de la diferencia después y antes de los valores de la dimensión nivel de confidencialidad de la información es 0.011, esto es menor a 0.05, esto significa que se rechaza la hipótesis nula y se acepta la alternativa, por tanto, se acepta que el sistema de gestión aplicado incrementa la confidencialidad de la información de la empresa Agrokasa S.A. en el espacio de estudio.

2. Hipótesis específica N° 2

"La implementación del sistema de gestión de seguridad de la información incrementa el nivel de integridad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022".

Esta dimensión, al tener datos que no se comportan como datos de una distribución normal tanto en la pre y post prueba, o antes y después, se ha optado por aplicar la prueba de Wilcoxon; por lo tanto, se han formulado las hipótesis nula y alternativa, con su respectiva significancia de 0.05.

Hipótesis:

H_0: “El sistema de gestión de seguridad de la información no incrementa el nivel de integridad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022”.

$$H_0: NIIa >= NIIp$$

Se puede determinar que no existe incremento de la dimensión.

H_1: “El sistema de gestión de seguridad de la información si incrementa el nivel de integridad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022”.

$$H_1: NIIa < NIIp$$

Se puede determinar que si existe incremento de la dimensión.

Nivel de significancia: α = 0.05.

Sig. > 0.05, se acepta (H_0) que es la hipótesis nula

Sig. <= 0.05, se acepta (H_1) que es la hipótesis alternativa

Tabla 13. Prueba de Wilcoxon para el nivel de integridad

Estadísticos de prueba [a]

	Integridad después - Integridad antes
Z	-2,588[b]
Sig. asintótica(bilateral)	,010

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Tal como se puede observar en la tabla 16, la contrastación de la hipótesis por medio del estadístico o prueba de Wilcoxon, el p valor de la diferencia después y antes de los valores de la dimensión nivel de integridad de la información es 0.010, esto fue

menor a 0.05, esto significa que se rechazó la hipótesis nula y se aceptó la alternativa, que señala que el sistema de gestión aplicado incrementó el nivel de integridad de la información de la empresa Agrokasa S.A. en el espacio de estudio.

3. Hipótesis específica N° 3

"La implementación del sistema de gestión de seguridad de la información incrementa el nivel de disponibilidad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022".

Esta dimensión, al tener datos que no se comportan como datos de una distribución normal tanto en la pre y post prueba, o antes y después, se ha optado por aplicar la prueba de Wilcoxon; por lo tanto, se han formulado las hipótesis nula y alternativa, con su respectiva significancia de 0.05.

Hipótesis:

H_0: "El sistema de gestión de seguridad de la información no incrementa el nivel de disponibilidad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022".

$$H_0: NDIa >= NDIp$$

Se puede determinar que no existe incremento de la dimensión.

H_1: "El sistema de gestión de seguridad de la información si incrementa el nivel de disponibilidad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022".

$$H_1: NDIa < NDIp$$

Se puede determinar que si existe incremento de la dimensión.

Nivel de significancia: $\alpha = 0.05$.

Sig. > 0.05, se acepta (H_0) que es la hipótesis nula

Sig. <= 0.05, se acepta (H_1) que es la hipótesis alternativa

Tabla 14. Prueba de Wilcoxon para el nivel de disponibilidad

Estadísticos de prueba [a]

	Disponibilidad después - Disponibilidad antes
Z	-2,558[b]
Sig. asintótica(bilateral)	,011

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Tal como se puede observar en la tabla 17, la contrastación de la hipótesis por medio del estadístico o prueba de Wilcoxon, la significancia o p valor de la diferencia después y antes de los valores de la dimensión nivel de disponibilidad de la información fue 0.011, esto cual es menor a 0.05, esto significa que se rechazó la hipótesis nula y se aceptó la alternativa, que señala que el sistema de gestión aplicado incrementó el nivel de disponibilidad de la información de la empresa Agrokasa S.A. en el espacio de estudio.

4. Hipótesis general

“La implementación del sistema de gestión de seguridad de la información incrementa el nivel de disponibilidad de la información de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022”.

Esta dimensión, al tener datos que no se comportan como datos de una distribución normal tanto en la pre y post prueba, o antes y después, se ha optado por aplicar la prueba de Wilcoxon; por lo tanto, se han formulado las hipótesis nula y alternativa, con su respectivo nivel de significancia de 0.05.

Hipótesis:

H_0: “La implementación de un sistema de gestión de seguridad de la información no mejora la seguridad informática de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022”.

$$H_0: NDIa >= NDIp$$

Se puede determinar que no existe incremento de la variable.

H_1: “La implementación de un sistema de gestión de seguridad de la información mejora la seguridad informática de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022”.

$$H_1: NDIa < NDIp$$

Se puede determinar que si existe incremento de la variable.

Nivel de significancia: α = 0.05.

Sig. > 0.05, se acepta (H_0) que es la hipótesis nula
Sig. <= 0.05, se acepta (H_1) que es la hipótesis alternativa

Tabla 15. Prueba de Wilcoxon para contrastación de las variables

Estadísticos de prueba [a] sistema de gestión de seguridad de la información y Seguridad informática

	Promedio después - Promedio antes
Z	-2,558[b]
Sig. asintótica(bilateral)	,011

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Tal como se puede observar en la tabla 18, la contrastación de la hipótesis por medio del estadístico o prueba de Wilcoxon, la significancia o p valor de la diferencia después y antes de los valores de las variables implementación de un sistema de gestión de seguridad de la información y seguridad informática fue 0.011, esto es menor a 0.05, esto significa que se rechazó la hipótesis nula y se aceptó la alternativa, que señala que la

implementación de un sistema de gestión aplicado mejoró la seguridad informática de la empresa Agrokasa S.A. en el espacio estudiado.

V. DISCUSIÓN

En la primera dimensión “Nivel de confidencialidad de la información”, se encontró que antes y después de la implementación de un sistema de gestión de seguridad de la información datos de satisfacción de 1.61 a 4.57, ello indicó un aumento de satisfacción de 2.96 con un porcentaje de 59.20%. Resultados fueron similares con los de (Cahuana & Cahuana, 2021) quienes encontraron que los reportes confidenciales presentaron incremento de 71.89 % a 96.89 %. Por otro lado, estos resultados se asemejan a los obtenidos por (Risco, 2021) quien encontró que la confidencialidad de la información inicialmente tuvo 68,85% para luego bajar a 15,40%. Estos resultados concuerdan con los fundamentado en la teoría de la seguridad de la información y sostenida por ISO/IEC 27002:2013, en donde se manifiesta que las dimensiones de la información pueden ser garantizadas en su seguridad cuando se aplican sistemas de seguridad bien efectuados y con la participación de todos los colaboradores (Solano, 2020).

En la segunda dimensión “Nivel de integridad de la información”, se encontró antes y después de la implantación de un sistema de gestión de seguridad de la información datos de satisfacción de1.57 a 4.66, es decir, estos datos presentaron aumento de 3.09, el aumento porcentual fue de 61.80%. Estos resultados fueron similares con los de (Olaza, 2017), en donde se encontró resultados positivos sobre la seguridad informática; sobre el porcentaje de la dimensión accesibilidad a la información, en el antes encontró 322 cuestiones con referencia a la demisión integridad, luego de la implementación los casos se redujeron a 47. Estos resultados encontrados son ligeramente similares a los datos encontrados en la investigación antecedente de (Salsavilca, 2017), en donde se encontró que el nivel de integridad de la información, la cual hizo referencia a que un documento no debe sufrir la falta de sus partes, es decir, debe estar integro o completo, presentó como resultado 97.42%, resultado que indica que existió incremento en los controles y la seguridad.

En la tercera dimensión “Nivel de disponibilidad”, se encontró antes y después de la implantación del sistema de gestión de seguridad de la información datos sobre la satisfacción de 1.50 a 4.73, esto indicó un aumento

en la satisfacción de 3.23, porcentualmente aumentó 64.60%. Los resultados encontrados coinciden ligeramente con los de (Rojas, 2019), en donde se tuvo que la implementación de la NTP ISO/IEC 27001:2014, permitió gerenciar la disponibilidad aplicando mejoras de políticas desde la perspectiva de la misión, visión y objetivos del objeto de estudio. Se encontró que estos datos encontrados fueron ligeramente similares a los encontrados en la investigación de (Aguinaga, 2021) en donde se tuvo que el aumento del nivel de la dimensión disponibilidad se aumentó de 96.81 a 99.93%, lo cual fue significativo.

VI. CONCLUSIONES

1. El sistema de gestión de seguridad de la información de la información de la empresa Agrokasa S.A. incrementó del nivel de confidencialidad de la información con satisfacción de 2.96, esto fue un aumento de 59.20%, la confidencialidad inicial fue 1.61 y después 4.57 en la satisfacción debido a la implementación del sistema propuesto para la empresa.
2. El sistema de gestión de seguridad de la información de la empresa Agrokasa S.A. incrementó el nivel de integridad de la información con satisfacción de 3.09, el incremento porcentual fue 61.80%, la integridad inicial fue de 1.57 y después 4.66 en la satisfacción debido a la implementación del sistema propuesto para la empresa.
3. El sistema de gestión de seguridad de la información de la empresa Agrokasa S.A. incrementó del nivel de disponibilidad de la información con satisfacción de 3.23, el incremento porcentual fue 64.60%, la disponibilidad inicial fue 1.50 y después 4.73 en la satisfacción debido a la implementación del sistema propuesto para la empresa.
4. Debido al incremento en la satisfacción de las tres dimensiones, se concluye que el sistema de gestión de seguridad de la información influyó significativamente en la seguridad informática de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022.

VII. RECOMENDACIONES

Al Gerente general:

Se encarga la implementación de la propuesta del presente estudio para que sobre el uso o aplicación de una plataforma tecnológica que contribuya con el apoyo relacionado con la tecnología beneficiosa y pertinente para la seguridad informática de la empresa.

Al Jefe de TI:

Debe perfeccionar el ciclo de la mejora continua mediante el desarrollo de propuestas en donde se trate de mejorar u optimizar la seguridad informática de la empresa.

Al Jefe de personal:

Debe desarrollar la planificación para ejecutar una capacitación técnica a los colaboradores con el propósito de concientizar en la importancia, conocimientos y enfrentar los retos de seguridad informática.

A los Colaboradores:

Debe llevar a cabo en cada desarrollo de la jornada laboral la ejecución de las buenas prácticas fundamentadas en ISO/IEC 27002 del año 2013, a fin de tener un resguardo y protección sostenible en el tiempo de sus activos informáticos.

REFERENCIAS

Agrokasa. (1 de Enero de 2020). *Página Web Oficial*. Recuperado el 21 de Mayo de 2022, de https://agrokasa.com/

Aguinaga, W. (2021). *"Sistema de gestión alineado a la norma ISO/IEC 27001:2013 para la seguridad de la información en una institución financiera, Chachapoyas-Amazonas, 2021".* Lima: UCV.

Aguirre, M. (2018). *"Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C – La Molina".* Lima: UCV.

Agurto, A. (2017). *"Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001".* Piura: UCV.

Alarcón, M., Cruzado, C., Mejía, C., & Rodríguez, L. (2020). "Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana". *Propósitos y Representaciones*, 1-11.

Arias, M., & Botero, R. (2019). *Estado de la norma técnica de seguridad ISO27002 como soporte para la norma ISO27001 en una empresa de telecomunicaciones de la ciudad de Medellín.* Medellín: TDEA.

AUDITOOL. (10 de Febrero de 2022). Recuperado el 16 de Mayo de 2022, de https://www.auditool.org/blog/auditoria-de-ti/8317-que-son-los-controles-de-seguridad-de-ti

Ayala, Á. (2017). *"Sistema de gestión de seguridad de información para mejorar el proceso de gestión del riesgo en un hospital nacional, 2017".* Lima: UCV.

Ayudalay. (1 de Enero de 2019). *Seguridad de la información: Aspectos a tener en cuenta*. Recuperado el 25 de Mayo de Marzo, de https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/

Cahuana, C., & Cahuana, E. (2021). *"Sistema web basado en la ISO/IEC 27001 para la gestión de la información en la Empresa P.A Perú S.A.C.".* Lima: UCV.

Chavarry, F. (2021). *"Implementación de ISO 27001 y 27002 adaptadas para gestión de seguridad de información en Secretaría Ejecutiva de Policía Nacional del Perú".* Lima: UCV.

Chuna, L. (2018). *"Propuesta de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la DRTPE - Piura".* Piura: UCV.

Cruz, J., & Huamaní, M. (2019). *"Automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la empresa ZEPPELIN INVERSIONES GENERALES S.R.L".* Lima: UCV.

Esther, B., & Orienta, P. (2011). *"Mas allá de la seguridad nacional".* Granada: Comares.

Euroinnova. (1 de Enero de 2020). *Investigación Aplicada*. Obtenido de https://www.euroinnova.pe/blog/que-es-lo-que-caracteriza-a-la-investigacion-aplicada

Foucault, M. (2016). *"El nacimiento de la Biopolítica".* Buenos Aires: FCE.

Hidalgo, V. (2017). *"Diseño de modelo de gestión para el gerenciamiento de la seguridad de la información tecnológica en el Consejo de la Judicatura" – planta central Quito".* Quito: EPG-UQ.

INERCO. (11 de Diciembre de 2020). Recuperado el 10 de Junio de 2022, de https://www.inerco.com/blog/gestion-de-seguridad/

INSPQ. (17 de Agosto de 2018). *Concepto de Seguridad*. Recuperado el 4 de Junio de 2022, de https://www.inspq.qc.ca/es/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad

ISO. (1 de Junio de 2005). *ISO/IEC 17799:2005*. Recuperado el 28 de Mayo de 2022, de Information technology — Security techniques — Code of practice for information security management: https://www.iso.org/standard/39612.html

ISO. (1 de Octubre de 2013). *ISO/IEC 27002:2013*. Recuperado el 28 de Mayo de 2022, de Information technology - Security techniques - Code of practice for information security controls: https://www.iso.org/standard/54533.html

IsoTools. (21 de Enero de 2015). *La Familia de Normas ISO 27000*. Obtenido de https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

ISOTools. (1 de Enero de 2018). *NTP ISO 27002: Los Dominios de la Seguridad de la Información*. Recuperado el 16 de Mayo de 2022, de https://www.isotools.pe/ntp-iso-27001-dominios/

ISOTools. (11 de Marzo de 2021). *¿Qué es la seguridad de la información y cuantos tipos hay?* Recuperado el 23 de Mayo de 2022, de https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Maldonado, E. (2016). *"Norma ISO 27001 para la seguridad de información del área de Registros Académicos del colegio Nuestra Señora del Carmen".* Lima: UCV.

Maquera, H., & Serpa, P. (2017). *Gestión de Activos basados en ISO/IEC 27002 para garantizar Seguridad de la información.* Tacna: UNJBG.

Olaza, D. (2017). *"Implementación de NTP ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin".* Lima: UCV.

Pérez, A. (2015). *"Diseño de un modelo de los controles necesarios asociados a la gestión de activos, bajo el cumplimiento de la norma ISO/IEC 27002 anexo A, en una entidad bancaria".* Bogotá: UCC.

PJGROUP. (1 de Enero de 2020). Recuperado el 16 de Mayo de 2022, de https://peritojudicial.com/activos-informaticos/#:~:text=1.-,Qu%C3%A9%20son%20los%20activos%20inform%C3%A1ticos,ejemplo%20de%20hardware%20y%20software.

Poicon, Á., & Ramírez, Ó. (2020). *"Propuesta de un sistema de gestión de seguridad de la información para la Municipalidad Distrital de Marcavelica, mediante la NTP- ISO/IEC 27001:2014".* Piura: UCV.

QuestionPro. (1 de Enero de 2021). *Investigación experimental*. Obtenido de https://www.questionpro.com/blog/es/investigacion-experimental/

Red IRIS. (1 de Enero de 2020). *Gestión de la seguridad*. Recuperado el 10 de Junio de 2022, de https://www.rediris.es/cert/doc/unixsec/node31.html

Riquelme, M. (6 de Enero de 2022). *Gestión de la seguridad de la empresa*. Recuperado el 10 de Junio de 2022, de https://www.webyempresas.com/la-gestion-de-la-seguridad-en-la-empresa/

Risco, G. (2021). *"Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín,2021".* Lima: UCV.

Rojas, C. (2019). *"Seguridad en los datos e implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC".* Lima: UCV.

Romo, D., & Valarezo, J. (2016). *Analisis e Implementación de la Norma ISO 27002 para el Departamento de Sistemas de la Universidad Politécnica Salesiana de la ciudad de Guayaquil.* Guayaquil: UPS.

Salsavilca, C. (2017). *"Implementación de la norma ISO 27001 en la Gestión de la Seguridad de la Información en la empresa Atento del Perú 2017".* Lima: UCV.

Ticona, R. (2022). *"Modelo de seguridad de la información basado en la normativa ISO/IEC 27001:2013 para mitigar los riesgos de los activos de la información en la entidad privada Severox Perú SAC, Arequipa, 2021".* Arequipa: UCV.

Yañez, A. (2017). *"Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y empresas de menor tamaño".* Santiago de Chile: UCH.

Zapata, S. (2021). *"Análisis de factores críticos de éxito para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa Inversiones Prisco S.A.C – Sechura".* Piura: UCV.

ANEXOS

Anexo 1 - Matriz de consistencia de la investigación

Título: Sistema de gestión de seguridad de la información para mejorar la seguridad informática de la empresa Agrokasa S.A., Ica 2022

Autores: Paucar Espino, Jhonathan Felipe / Zúñiga Monzón, Dina Rosa

Problema	Objetivo	Hipótesis	Variable	Dimensión	Indicador	Instrumento
General: ¿De qué manera un sistema de gestión de seguridad de la información influye en la seguridad informática de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022?	General: Mejorar la seguridad informática de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022 mediante la implementación de un sistema de gestión de seguridad de la información.	General: "La implementación de un sistema de gestión de seguridad de la información mejora la seguridad informática de la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022".	Independiente: Sistema de gestión de seguridad de la información			
Específicos: 1. ¿De qué manera un sistema de gestión de seguridad de la información influye en el nivel de confidencialidad de la información en la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022? 2. ¿De qué manera un sistema de gestión de seguridad de la	Específicos: 1. Incrementar el nivel de confidencialidad de la información de la empresa. 2. Incrementar el nivel de integridad de la información de la empresa. 3. Incrementar el nivel de disponibilidad de la información de la empresa.	Específicas: 1. "La implementación de un sistema de gestión de seguridad de la información incrementa el nivel de confidencialidad de la información en la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022". 2. "La implementación de un sistema de gestión de seguridad de la información incrementa el nivel de integridad de la información en la	Dependiente: Seguridad informática	Confidencialidad	Nivel de confidencialidad de la información	Cuestionario
				Integridad	Nivel de integridad de la información	Cuestionario

información influye en el nivel de integridad de la información en la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022? 3. ¿De qué manera un sistema de gestión de seguridad de la información influye en la disponibilidad de la información en la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022?		empresa Agrokasa S.A. de la ciudad de Ica en el año 2022". 3. "La implementación de un sistema de gestión de seguridad de la información incrementa el nivel de disponibilidad de información en la empresa Agrokasa S.A. de la ciudad de Ica en el año 2022"		Disponibilidad	Nivel de disponibilidad de la información	Cuestionario

Anexo 2 - Matriz de operacionalización de variables

Variable	Definición Conceptual	Definición Operacional	Dimensión (Sub variable)	Indicador	Escala de medición
Independiente: Sistema de gestión de seguridad de la información	"Conjunto de procedimientos, políticas, directrices, actividades y recursos que son organizados y gestionados en forma grupal por una institución que desea proteger la información de su institución. Podemos definir a un SGSI" (INACAL, 2020).	Se puede medir a través de aspectos de políticas y procedimientos de seguridad de la información en las organizaciones.			
Dependiente: Seguridad informática	"Mecanismos de protección de ataques y manipulación de los datos y recursos informáticos considerados como activos primordiales para una organización" (Andrade, 2018).	Se puede medir por el nivel de confidencialidad, integridad y disponibilidad de la información en las organizaciones.	Confidencialidad	Nivel de confidencialidad de la información	Ordinal
			Integridad	Nivel de integridad de la información	Ordinal
			Disponibilidad	Nivel de disponibilidad de la información	Ordinal

Anexo 3 - Método de juicio experto

Apellidos y nombres del experto: Agreda Gamboa, Everson David

Título profesional y/o Grado académico: Ingeniero de Sistemas / Doctor

Fecha: 04/06/2022

Título del proyecto de investigación: "Sistema de gestión de seguridad de la información para mejorar la seguridad informática de la empresa Agrokasa S.A., Ica 2022".

Autores: Paucar Espino, Jhonathan Felipe / Zúñiga Monzón, Dina Rosa

Evaluación de la metodología/marco de trabajo para la implementación del SGSI

Mediante el método de juicio experto, Usted tiene la facultad de calificar las metodologías/marcos de trabajo involucrados, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la metodología/marco de trabajo para implementar la solución propuesta en el presente proyecto de investigación y, también si hubiese algunas sugerencias:

Ítem	Criterios	Norma / Marco de trabajo		
		ISO 27002:2013	NTP-ISO 17799	COBIT 2019
1	Tiempo de implementación	3	3	2
2	Información	3	2	2
3	Requerimientos	3	3	2
4	Complejidad	3	3	2
5	Conocimiento	3	2	2
Total		15	13	10

La escala a evaluar es de: **1** - Malo, **2** - Regular, **3** - Bueno

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las metodologías/marcos de trabajo propuestas

Item	Criterio	Descripción
1	Tiempo de implementación	Es el tiempo que toma la implementación de la solución.
2	Información	Es la cantidad de información disponible sobre la metodología/marco de trabajo.
3	Requerimientos	Es la cantidad de requerimientos que exige la metodología/marco de trabajo.
4	Complejidad	Es el nivel de abstracción del estudio de la metodología/marco de trabajo.
5	Conocimiento	Es la cantidad de conocimiento que el investigador debe tener sobre la metodología/marco de trabajo.

Apellidos y nombres del experto: Mendoza Rivera, Ricardo Darío

Título profesional y/o Grado académico: Ingeniero Industrial / Doctor

Fecha: 04/06/2022

Título del proyecto de investigación: "Sistema de gestión de seguridad de la información para mejorar la seguridad informática de la empresa Agrokasa S.A., Ica 2022".

Autores: Paucar Espino, Jhonathan Felipe / Zúñiga Monzón, Dina Rosa

Evaluación de la metodología/marco de trabajo para la implementación del SGSI

Mediante el método de juicio experto, Usted tiene la facultad de calificar las metodologías/marcos de trabajo involucrados, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la metodología/marco de trabajo para implementar la solución propuesta en el presente proyecto de investigación y, también si hubiese algunas sugerencias:

Ítem	Criterios	Norma / Marco de trabajo		
		ISO 27002:2013	NTP-ISO 17799	COBIT 2019
1	Tiempo de implementación	2	2	2
2	Información	3	2	2
3	Requerimientos	3	3	2
4	Complejidad	2	2	1
5	Conocimiento	3	2	2
Total		13	11	9

La escala a evaluar es de: **1** - Malo, **2** - Regular, **3** - Bueno

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las metodologías/marcos de trabajo propuestas

Item	Criterio	Descripción
1	Tiempo de implementación	Es el tiempo que toma la implementación de la solución.
2	Información	Es la cantidad de información disponible sobre la metodología/marco de trabajo.
3	Requerimientos	Es la cantidad de requerimientos que exige la metodología/marco de trabajo.
4	Complejidad	Es el nivel de abstracción del estudio de la metodología/marco de trabajo.
5	Conocimiento	Es la cantidad de conocimiento que el investigador debe tener sobre la metodología/marco de trabajo.

Apellidos y nombres del experto: Córdova Otero, Juan Luis

Título profesional y/o Grado académico: Ingeniero de Computación y Sistemas / Maestro

Fecha: 04/06/2022

Título del proyecto de investigación: "Sistema de gestión de seguridad de la información para mejorar la seguridad informática de la empresa Agrokasa S.A., Ica 2022".

Autores: Paucar Espino, Jhonathan Felipe / Zúñiga Monzón, Dina Rosa

Evaluación de la metodología/marco de trabajo para la implementación del SGSI

Mediante el método de juicio experto, Usted tiene la facultad de calificar las metodologías/marcos de trabajo involucrados, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la metodología/marco de trabajo para implementar la solución propuesta en el presente proyecto de investigación y, también si hubiese algunas sugerencias:

Ítem	Criterios	Norma / Marco de trabajo		
		ISO 27002:2013	NTP-ISO 17799	COBIT 2019
1	Tiempo de implementación	3	3	2
2	Información	3	2	2
3	Requerimientos	3	3	2
4	Complejidad	3	2	2
5	Conocimiento	3	3	2
Total		15	13	10

La escala a evaluar es de: **1** - Malo, **2** - Regular, **3** - Bueno

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las metodologías/marcos de trabajo propuestas

Item	Criterio	Descripción
1	Tiempo de implementación	Es el tiempo que toma la implementación de la solución.
2	Información	Es la cantidad de información disponible sobre la metodología/marco de trabajo.
3	Requerimientos	Es la cantidad de requerimientos que exige la metodología/marco de trabajo.
4	Complejidad	Es el nivel de abstracción del estudio de la metodología/marco de trabajo.
5	Conocimiento	Es la cantidad de conocimiento que el investigador debe tener sobre la metodología/marco de trabajo.

Anexo 4 - Instrumentos de recolección de datos

Cuestionario aplicado a los usuarios de la empresa Agrokasa S.A.C.

A continuación, se presenta una lista de preguntas contenidas en veinte (20) ítems que corresponden a su percepción sobre la seguridad informática en la empresa. Por favor, indique su apreciación objetiva marcando con una "X" sobre cualquier de los números 1, 2, 3, 4 ó 5, dónde:

1	2	3	4	5
Deficiente	Malo	Regular	Bueno	Excelente

Variable	Dimensión	Ítems	Opción de respuesta				
			1	2	3	4	5
Seguridad informática	Confidencialidad	1. ¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?					
		2. ¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?					
		3. ¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?					
		4. ¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?					
		5. ¿Qué opina Usted sobre el manejo responsable sobre los activos?					
		6. ¿Qué opina Usted sobre la clasificación que se realiza de la información?					
		7. ¿Qué opina Usted sobre el manejo de los soportes de almacenamiento?					
	Integridad	8. ¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?					
		9. ¿Qué opina Usted sobre la protección conveniente contra código malicioso?					
		10. ¿Qué opina Usted sobre el manejo de copias de seguridad?					
		11. ¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?					
		12. ¿Qué opina Usted sobre el control de software de explotación?					
		13. ¿Qué opina Usted sobre la gestión de las vulnerabilidades técnicas?					

		14. ¿Qué opina Usted sobre las consideraciones de la auditorias de los sistemas de información?					
		15. ¿Qué opina Usted sobre el manejo de los controles criptográficos?					
	Disponibilidad	16. ¿Qué opina Usted sobre la gestión de seguridad en redes?					
		17. ¿Qué opina Usted sobre el intercambio seguro de información con partes externas?					
		18. ¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?					
		19. ¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?					
		20. ¿Qué opina Usted sobre la protección de los datos utilizados en pruebas?					

Anexo 4 - Validación de los instrumentos de recolección de datos

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?	x		x		x		
2. ¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?	x		x		x		
3. ¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?	x		x		x		
4. ¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?	x		x		x		
5. ¿Qué opina Usted sobre el manejo responsable sobre los activos?	x		x		x		
6. ¿Qué opina Usted sobre la clasificación que se realiza de la información?	x		x		x		
7. ¿Qué opina Usted sobre el manejo de los soportes de almacenamiento?	x		x		x		
Dimensión 2: Integridad							
8. ¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?	x		x		x		
9. ¿Qué opina Usted sobre la protección conveniente contra código malicioso?	x		x		x		
10. ¿Qué opina Usted sobre el manejo de copias de seguridad?	x		x		x		
11. ¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?	x		x		x		
12. ¿Qué opina Usted sobre el control de software de explotación?	x		x		x		
13. ¿Qué opina Usted sobre la gestión de las vulnerabilidades técnicas?	x		x		x		
14. ¿Qué opina Usted sobre las consideraciones de la auditorias de los sistemas de información?	x		x		x		

15. ¿Qué opina Usted sobre el manejo de los controles criptográficos?	x		x		x		
Dimensión 3: Disponibilidad							
16. ¿Qué opina Usted sobre la gestión de seguridad en redes?	x		x		x		
17. ¿Qué opina Usted sobre el intercambio seguro de información con partes externas?	x		x		x		
18. ¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?	x		x		x		
19. ¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?	x		x		x		
20. ¿Qué opina Usted sobre la protección de los datos utilizados en pruebas?	x		x		x		

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

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

[3] **Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

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

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Dr. Agreda Gamboa, Everson David
Especialidad del evaluador	Tecnologías de la información
 **DNI:** 18161457	Trujillo, 18 de junio del 2022

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?	x		x		x		
2. ¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?	x		x		x		
3. ¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?	x		x		x		
4. ¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?	x		x		x		
5. ¿Qué opina Usted sobre el manejo responsable sobre los activos?	x		x		x		
6. ¿Qué opina Usted sobre la clasificación que se realiza de la información?	x		x		x		
7. ¿Qué opina Usted sobre el manejo de los soportes de almacenamiento?	x		x		x		
Dimensión 2: Integridad							
8. ¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?	x		x		x		
9. ¿Qué opina Usted sobre la protección conveniente contra código malicioso?	x		x		x		
10. ¿Qué opina Usted sobre el manejo de copias de seguridad?	x		x		x		
11. ¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?	x		x		x		
12. ¿Qué opina Usted sobre el control de software de explotación?	x		x		x		
13. ¿Qué opina Usted sobre la gestión de las vulnerabilidades técnicas?	x		x		x		
14. ¿Qué opina Usted sobre las consideraciones de la auditorias de los sistemas de información?	x		x		x		

15. ¿Qué opina Usted sobre el manejo de los controles criptográficos?	x		x		x		
Dimensión 3: Disponibilidad							
16. ¿Qué opina Usted sobre la gestión de seguridad en redes?	x		x		x		
17. ¿Qué opina Usted sobre el intercambio seguro de información con partes externas?	x		x		x		
18. ¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?	x		x		x		
19. ¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?	x		x			x	
20. ¿Qué opina Usted sobre la protección de los datos utilizados en pruebas?	x		x			x	

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

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

[3] **Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

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

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Dr. Mendoza Rivera, Ricardo Darío
Especialidad del evaluador	Gestión de Proyectos
 **DNI:** 18070765	Trujillo, 18 de junio del 2022

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?	x		x		x		
2. ¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?	x		x		x		
3. ¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?	x		x		x		
4. ¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?	x		x		x		
5. ¿Qué opina Usted sobre el manejo responsable sobre los activos?	x		x		x		
6. ¿Qué opina Usted sobre la clasificación que se realiza de la información?	x		x		x		
7. ¿Qué opina Usted sobre el manejo de los soportes de almacenamiento?	x		x		x		
Dimensión 2: Integridad							
8. ¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?	x		x		x		
9. ¿Qué opina Usted sobre la protección conveniente contra código malicioso?	x		x		x		
10. ¿Qué opina Usted sobre el manejo de copias de seguridad?	x		x		x		
11. ¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?	x		x		x		
12. ¿Qué opina Usted sobre el control de software de explotación?	x		x		x		
13. ¿Qué opina Usted sobre la gestión de las vulnerabilidades técnicas?	x		x		x		
14. ¿Qué opina Usted sobre las consideraciones de la auditorias de los sistemas de información?	x		x		x		

15. ¿Qué opina Usted sobre el manejo de los controles criptográficos?	x		x		x		
Dimensión 3: Disponibilidad							
16. ¿Qué opina Usted sobre la gestión de seguridad en redes?	x		x		x		
17. ¿Qué opina Usted sobre el intercambio seguro de información con partes externas?	x		x		x		
18. ¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?	x		x		x		
19. ¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?	x		x		x		
20. ¿Qué opina Usted sobre la protección de los datos utilizados en pruebas?	x		x			x	

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

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

[3] **Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

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

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Ms. Córdova Otero, Juan Luis
Especialidad del evaluador	Sistemas de información
 **DNI:** 18122765	Trujillo, 18 de junio del 2022

Anexo 5 - Tabla de datos

Pre Prueba

	Confidencialidad							Integridad								Disponibilidad				
	Ítem 1	Ítem 2	Ítem 3	Ítem 4	Ítem 5	Ítem 6	Ítem 7	Ítem 8	Ítem 9	Ítem 10	Ítem 11	Ítem 12	Ítem 13	Ítem 14	Ítem 15	Ítem 16	Ítem 17	Ítem 18	Ítem 19	Ítem 20
Persona 1	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	1	2	1	1	1
Persona 2	2	2	1	2	2	2	1	2	1	1	2	2	1	1	2	2	2	1	1	2
Persona 3	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	2	2	1
Persona 4	1	2	2	2	1	2	2	2	1	2	2	2	1	2	2	2	2	2	1	2
Persona 5	1	2	1	2	1	2	1	2	1	1	2	2	1	1	2	1	2	1	1	1
Persona 6	2	2	1	2	2	2	1	2	1	2	2	2	1	2	2	2	2	1	1	2
Persona 7	2	2	1	2	2	2	1	2	2	1	1	2	2	1	1	2	2	1	1	2
Persona 8	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	1	2	2	1
Promedio	1.63	1.75	1.38	1.75	1.63	1.75	1.38	1.75	1.38	1.38	1.75	1.75	1.38	1.38	1.75	1.50	1.88	1.38	1.25	1.50
Prom. Final	1.61							1.56								1.50				

Pos Prueba

	Confidencialidad							Integridad								Disponibilidad				
	Ítem 1	Ítem 2	Ítem 3	Ítem 4	Ítem 5	Ítem 6	Ítem 7	Ítem 8	Ítem 9	Ítem 10	Ítem 11	Ítem 12	Ítem 13	Ítem 14	Ítem 15	Ítem 16	Ítem 17	Ítem 18	Ítem 19	Ítem 20
Persona 1	4	5	5	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Persona 2	5	5	5	4	5	5	5	4	4	4	5	4	4	4	5	4	5	5	4	4
Persona 3	4	4	5	5	4	4	5	4	5	5	5	4	5	5	5	4	4	5	4	4
Persona 4	4	4	5	4	4	4	5	5	4	5	5	5	4	5	5	5	4	5	5	5
Persona 5	4	5	5	4	4	5	5	4	5	4	5	4	5	4	5	4	5	5	4	4
Persona 6	4	5	5	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Persona 7	4	4	5	5	4	4	5	4	5	5	5	4	5	5	5	5	5	5	5	5
Persona 8	5	5	5	4	5	5	5	4	4	4	5	4	4	4	5	5	5	5	5	5
Promedio	4.25	4.63	5.00	4.25	4.25	4.63	5.00	4.38	4.63	4.63	5.00	4.38	4.63	4.63	5.00	4.63	4.75	5.00	4.63	4.63
Prom. Final	4.57							4.66								4.73				

Anexo 6 - Confiabilidad de los instrumentos de recolección de datos

Resumen de procesamiento de casos

		N	%
Casos	Válido	18	100,0
	Excluido[a]	0	,0
	Total	18	100,0

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

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,884	20

Anexo 7 - Solución tecnológica propuesta

(Sistema de Gestión de Seguridad de la Información - SGSI)

ETAPA I: ORGANIZACIÓN EMPRESARIAL

1.1 Descripción de la organización

1.1.1 Breve reseña histórica

Agrokasa Holdings S.A. es una empresa constituida en el Perú como consecuencia de la escisión parcial de Corporación Drokasa S.A., la cual consta en la Escritura Pública de fecha 21 de diciembre de 2011, extendida por el Notario de Lima Dr. Jorge E. Orihuela Ibérico y que entró en vigencia el 1 de diciembre de 2011. Su inscripción registral consta en la Partida Electrónica No. 12793387 del Registro de Personas Jurídicas de Lima.

La referida escisión parcial consistió en la segregación de parte del patrimonio de Corporación Drokasa S.A. (integrado principalmente por las acciones representativas del capital social que ésta tenía en Sociedad Agrícola Drokasa S.A. - Agrokasa) para transferirlo a la nueva sociedad que se constituía denominada Agrokasa Holdings S.A.

Agrokasa Holdings S.A. forma parte del Grupo denominado “Agrokasa Holdings”, el cual opera en el Perú. Las empresas que conforman dicho Grupo son:

(i) Agrokasa Holdings S.A., cuyo objeto social conforme a su Estatuto es realizar directa o indirectamente y disponer de toda clase de inversiones en derechos y valores mobiliarios, siendo que a la fecha su única inversión es en acciones de Sociedad Agrícola Drokasa S.A.; y,

(ii) Sociedad Agrícola Drokasa S.A. (Agrokasa), empresa peruana dedicada a la agro exportación desde 1995, siendo sus principales negocios a la fecha el cultivo, empaque y exportación de espárrago verde, uva de mesa y paltas.

Al 31 de diciembre de 2015, Agrokasa Holdings S.A. tiene un capital social, creado, suscrito y pagado de S/. 66’475,362.

El íntegro del capital social suscrito y pagado de Agrokasa Holdings S.A. está representado por 66’475,362 acciones comunes con derecho a voto, de un valor nominal de S/. 1.00 cada una, todas ellas creadas y emitidas a favor de accionistas nacionales y extranjeros.

Conforme a lo establecido en el artículo cuarto de su Estatuto Social, la duración de Agrokasa Holdings S.A. es indefinida.

1.1.2 Giro del negocio

Agrokasa es una empresa dedicada al cultivo, empaque y exportación de frutas y hortalizas frescas, y forma parte de la cadena logística de comercio internacional.

1.1.3 Ubicación (Google maps)

La empresa tiene sus oficinas administrativas en Jr. Mariscal La Mar 991 – Piso 10. Magdalena Del Mar. Lima, Perú.

Fuente: (Agrokasa, 2020)

Adicionalmente, posee los siguientes fundos:

- Fundo La Catalina

Fuente: (Agrokasa, 2020)

- Fundo Santa Rita

Fuente: (Agrokasa, 2020)

- Fundo Las Mercedes

Fuente: (Agrokasa, 2020)

También, la empresa cuenta con cuatro empacadoras denominadas:

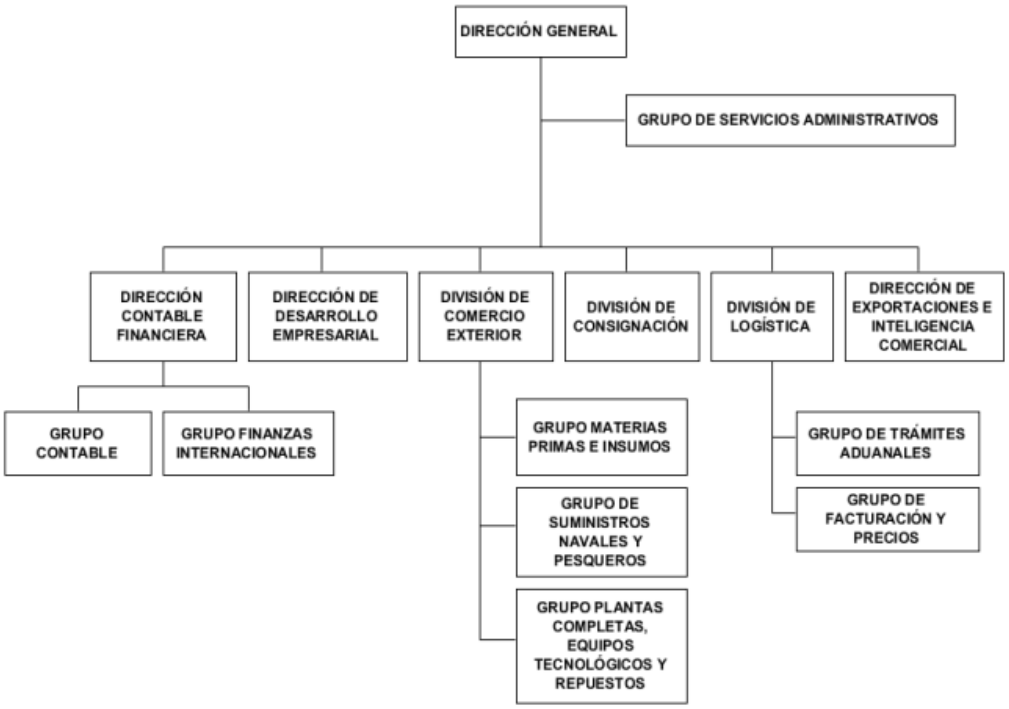
- Pelac: donde se acondiciona espárragos (Packing de Espárragos La Catalina - Ica).
- PESU: donde se acondiciona paltas y arándanos (Planta Empacadora Supe - Barranca).
- PVI y PVII: donde se acondicionan uvas de mesa, ambos ubicados en Ica.

La empresa cuenta con 1.227 hectáreas destinadas al cultivo de palta, 433 ha para uvas, 432 ha enfocadas en espárragos y 147 ha para arándanos.

1.2 Estructura organizacional

1.2.1 Organigrama estructural

La empresa cuenta con el siguiente organigrama estructural:



Fuente: (Agrokasa, 2020)

1.2.2 Principales funciones organizacionales

Por ahora, no se dispone de esta información de forma completa; sin embargo, se considera relevante describir el Departamento de exportación. Las funciones a realizar por el departamento de exportación de la empresa pueden ser tan amplias como se desee. Las funciones básicas son:

- Prospectar y cerrar ventas con clientes internacionales.
- Buscar agentes y distribuidores.
- Realizar un seguimiento administrativo de los pedidos y los pagos.
- Ejecutar las acciones de promoción y publicidad.
- Coordinar todas las actividades de exportación con el resto de departamentos de la empresa.

Por último, también hay que considerar la posibilidad de contratar servicios externos para realizar algunas de estas tareas (estudios de mercado, gestión del transporte, información sobre riesgo comercial de clientes en el exterior, etc.), bien sea de forma parcial o total, aunque siempre bajo las directrices y el control de la empresa.

1.3 Direccionamiento Estratégico

1.3.1 Visión

"Agrokasa será reconocida por sus clientes, por la calidad superior de sus productos y servicios de atención logística y comercial que se brinda" (Agrokasa, 2020).

1.3.2 Misión

"Sociedad Agrícola Drokasa S.A. (cuyo nombre comercial es Agrokasa) produce, empaca y comercializa paltas, uvas de mesa, espárragos y arándanos, en la condición de frescos, cumpliendo con las necesidades de nuestros clientes y llevando a cabo sus actividades en base a las siguientes premisas: Invirtiendo en el desarrollo humano y tecnológico de nuestros colaboradores, asegurándonos de contar con equipos y procesos de vanguardia y promoviendo la mejora continua en todas las fases del negocio; Respetando el Medio Ambiente, velando por la Salud Ocupacional de nuestros colaboradores y manteniendo una relación de apoyo con las Comunidades en las que desarrollamos nuestras actividades; Alineando los intereses de nuestros Clientes y los del Entorno Local con los de nuestros Colaboradores y Accionistas." (Agrokasa, 2020).

1.3.3 Objetivos estratégicos

- Satisfacer las necesidades de los clientes y consumidores finales.
- Suministrar productos agrícolas y servicios logísticos que cumplen con sus requerimientos en los diferentes mercados del mundo poniendo énfasis en la producción de alimentos seguros, legales, auténticos y de calidad.
- Diversificar mercados y desarrollar nuevos productos y presentaciones de acuerdo a las solicitudes de sus clientes. Para lograrlo competitivamente cuenta con personal entrenado y comprometido con la empresa, así como con sus políticas y valores.
- Utilizar la mejora continua y tecnología como herramientas para competitividad.
- Cumplir con la legislación local referida a temas laborales y el cuidado del medio ambiente; privilegia su relación con la comunidad local y está comprometida con la prevención de la contaminación.
- Otorgar transparencia a su relación con clientes, comunidad local e internacional a través de la realización de auditorías externas ejecutadas por otras empresas.
- Contar con un sistema de gestión en control y seguridad diseñado para sus operaciones, contexto y riesgo, y garantiza su mantenimiento y mejora continua.

1.3.4 Principios y valores

- Valores:
  - Compromiso: Se toma como propios el propósito, visión, valores y objetivos de la empresa.
  - Trabajo en equipo: Se colabora para lograr objetivos comunes.
  - Respeto: Se actúa con consideración hacia los demás y todo lo que les rodea; construyendo relaciones de confianza.
  - Honestidad: Se actúa con la verdad en todo momento.
  - Responsabilidad: Se tiene en cuenta tanto el negocio como el medio ambiente.

- Principios:
  - Legalidad en todas las actuaciones: Agrokasa no participa en acciones que comprometan o pongan en peligro la legalidad y los principios éticos fundamentales.
  - Rechazo a cualquier tipo de discriminación: Agrokasa no acepta ningún tipo de discriminación por motivos de edad, raza, color, sexo, religión, opinión política, ascendencia nacional, orientación sexual, origen social o discapacidad.
  - Defensa promoción y difusión de los Derechos: Agrokasa rechaza de cualquier manifestación de acoso físico, psicológico, moral o de abuso de autoridad, o cualquier otra conducta que intimide u ofenda los derechos de las personas. Asimismo, promueve el respeto de los derechos humanos entre aquellas sociedades y comunidades en la que desarrolla su actividad y fomenta interna y externamente un trato digno y respetuoso a todas las personas.
  - Respeto a las personas (rechazo al trabajo forzoso, infantil y falta de libertades): Agrokasa, mediante la adopción de prácticas de empleo compatibles con los convenios de la Organización Internacional del Trabajo, prohíbe el trabajo forzoso en todas sus formas. Agrokasa promueve una infancia segura, erradicando el trabajo infantil mediante sus requisitos de admisión al empleo. Agrokasa defiende la libertad de afiliación, asociación y el reconocimiento efectivo del derecho a la negociación colectiva.

- Compromiso y formalización: Agrokasa a través de su Código de Conducta y de los procedimientos específicos de protección contra el acoso en el trabajo y el acoso sexual, establece los sistemas y procedimientos de detección, denuncia, protección y supresión de actuaciones o comportamientos contrarios a los derechos sociales básicos y a los principios éticos establecidos.
- Compromiso a terceros: Agrokasa impulsa el respeto de estos derechos en su cadena de suministro a través de sus Principios Éticos y las relaciones comerciales con sus proveedores, contratistas y colaboradores.
- Supervisión y colaboración con las autoridades: Agrokasa, vía instrucción de oficio por parte de la Comisión del Código de Conducta, controla y corrige cualquier abuso cometido en detrimento de los Derechos Humanos y, en caso de ser necesario, eleva la cuestión a la autoridad judicial competente, colaborando en cualquier caso con estas.
- Diligencia debida: Agrokasa se realizan con la debida diligencia con el objetivo de no vulnerar y respetar los derechos de terceros y mitigar las consecuencias negativas de sus actividades.

1.4 Productos

La empresa cuenta con los siguientes productos de agro exportación:

- Arándano

Fruto del bosque de color azul oscuro con alto volumen de antioxidantes y bajo en calorías, proporciona múltiples beneficios para el organismo. Variedades: Atlas, Bianca, Biloxi, Emerald, Jupiter y Ventura.

Fuente: (Agrokasa, 2020)

- Espárrago

Es el brote de la planta esparraguera, aporta fibra, vitaminas, potasio, minerales, ácido fólico y glutatión, el cual ayuda al correcto funcionamiento del sistema inmune.

Fuente: (Agrokasa, 2020)

- Palta

Superalimento con propiedades antienvejecimiento, posee un alto contenido de aceite vegetal y vitaminas. Es parte fundamental de cualquier dieta balanceada.

Fuente: (Agrokasa, 2020)

- Uva

Fruta cítrica que posee vitamina K la cual es un elemento primordial para la coagulación de la sangre. Constantemente se renuevan las variedades ofrecidas con la finalidad de satisfacer la demanda por este cultivo.

Fuente: (Agrokasa, 2020)

1.5 Diagnóstico estratégico

1.5.1 Análisis externo

Para el análisis externo, se ha considerado el Análisis PESTEL (Político – Económico – Socio Cultural – Tecnológico – Ecológico – Legal).

A continuación, se muestra una figura con la descripción de cada factor externo correspondiente:

P	POLÍTICO • Nueva reglamentación fitosanitaria "Reglamento (UE) 2018/ 2019". • Acciones fitosanitarias establecidas por Senasa Perú. • El Pacto Verde Europeo – Plan Integral para alcanzar la neutralidad climática.
E	ECONÓMICO • Volatilidad del tipo de cambio debido a la situación actual. • Tensión comercial entre EE. UU. y China. • Aumento de la tasa de desempleo. • Perspectivas favorables para el crecimiento económico del Perú.
S	SOCIOCULTURALES • Creciente demanda de los consumidores de frutas, vegetales y hortalizas. • Mayor preocupación de los consumidores por los productos que compran. • Mayor acceso a tecnología para identificar intereses de consumo.
T	TECNOLÓGICO • La revolución verde – tecnología Smart. • Uso de aplicaciones tecnológicas durante la cadena agrícola. • La agricultura inteligente para lograr la sostenibilidad y mejorar la productividad.
E	ECOLÓGICO • Cosechas afectadas por los climas extremos y fenómenos naturales. • Utilización de productos químicos para la eliminación de plagas. • Cambios en el entorno natural por el calentamiento global.

L	LEGAL • Derogación de la Ley de Promoción Agraria Nº 27360. • Ley N° 30987 que Fortalece la Planificación de la Producción Agraria. • Plan Nacional de Cultivos: Campaña Agrícola 2019-2020 que permite mejorar los planes de siembra y manejar sus precios.

Fuente: (Elaboración propia, 2022)

1.5.2 Análisis interno

Para el análisis externo, se ha considerado el Análisis FODA (Fortalezas – Oportunidades – Debilidades - Amenazas).

A continuación, se describe de cada factor interno correspondiente:

- Fortalezas:
  - Es parte de la Asociación de Productores y Exportadores de Palta Hass del Perú (Pro Hass).
  - Infraestructura de vanguardia (3 fundos, 4 empacadoras), ubicadas en Ica y Barranca.
  - 24 años de experiencia en el sector agro exportador.
  - Personal calificado en el área de logística, inteligencia comercial, control de calidad, entre Otros.
  - Socios estratégicos en el transporte de la fruta y hortalizas y al precio bajo.
  - Cuentan con cliente fidelizados y proveedores confiables que otorgan crédito hasta 3 meses.
  - Marcas propias con prestigio internacional: La Catalina y Santa Rita.
  - Certificaciones internacionales que aseguran la calidad, legalidad y salubridad de los productos.
  - Producción temprana de frutas y hortalizas que aseguran precios altos.

- Oportunidades:
  - Impacto económico de la marca Perú que beneficia al sector agro exportador.
  - Apertura de nuevos mercados (Rusia. Corea del Sur, Asia).
  - Aprovechar la firma de nuevos Tratados comerciales (India, Turquía y El Salvador) y otros por entrar en vigencia, tales como: Guatemala. TPP, Brasil y Reino Unido.

- Capacitación y captación de pequeños productores de palta con la finalidad de obtener productos de calidad.
- Incremento del consumo saludable y orgánico en el mercado internacional.
- Implementación de nuevas plantas de tratamientos residuales, proyecto PETAR.

- Debilidades:
  - Alta rotación de personal que labora en los centros de acopio y empaquetado de paltas.
  - Escasez de clientes para fruta p articular para el calibre 10.
  - Contratación de asesores extranjeros, debido a la falta de asistencia técnica en el país.
  - Falta de sensibilidad en temas de medidas fitosanitarias de algunos proveedores de frutas.
  - Diversas plagas que afectan la producción de paltas (cuaternarias).
  - Disponibilidad de horarios de trabajadores de SENASA en cuanto a las inspecciones de rutina.
  - Falta de promoción en ferias internacionales.

- Amenazas
  - Crisis económica a raíz de pandemia mundial COVID-19.
  - Inserción comercial internacional de nuevos productores y exportadores de palta que afectarían a los precios.
  - Problemas sociales en el Perú, que afecten al transporte de mercadería (Bloqueo de carreteras, paros, entre otros).
  - Fenómenos naturales, cambio climático global.
  - Incremento de plagas que afecten a la producción
  - Incremento de exigencias técnicas para ingreso de mercancía al exterior.
  - Incremento del precio de fertilizantes, insumo importante en el cultivo de frutas y hortalizas.
  - Alta competencia con mercados productos de palta, tales como: Sudáfrica, debido que cosecha en los mismos tiempos de producción de Perú.

ETAPA II: APLICABILIDAD DE LA NORMA INTERNACIONAL ISO/IEC 27002:2013 EN LA ORGANIZACIÓN ACTUAL

2.1. Dominio 8 - Gestión de activos

2.1.1. Objetivo de control 8.1 - Responsabilidad sobre los activos

- Control de seguridad 8.1.1 - Inventario de activos

  No existe un inventario de activos asociados con información e instalaciones de procesamiento de información.

- Control de seguridad 8.1.2 - Propiedad de los activos

  Al no contar con un inventario de activos, no existe mantenimiento.

- Control de seguridad 8.1.3 - Uso aceptable de los activos

  Hace falta de un inventario de activos que permita establecer normas para un uso aceptable de los activos.

- Control de seguridad 8.1.4 - Devolución de activos

  Debido a la coyuntura se ha establecido acuerdos que permiten a los empleados sacar activos de la organización, que posteriormente deben ser devueltos.

2.1.2. Objetivo de control 8.2 - Clasificación de la información

- Control de seguridad 8.2.1 - Directrices de clasificación

  Hace falta clasificar la información en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.

- Control de seguridad 8.2.2 - Etiquetado y manipulado de la información

  Se debe etiquetar los procedimientos desarrollados e implementados en concordancia con el esquema de clasificación de la información a adoptar

- Control de seguridad 8.2.3 - Manipulación de activos

  Se debe establecer un esquema de clasificación de la información a fin de desarrollar y establecer los procedimientos para el manejo de activos.

2.1.3. Objetivo de control 8.3 - Manejo de los soportes de almacenamiento

- Control de seguridad 8.3.1 - Gestión de soportes extraíbles

  Hace falta procedimientos que permita gestionar los medios

- Control de seguridad 8.3.2 - Eliminación de soportes

No existe procedimientos formales para poner a disposición los medios de manera segura.

- Control de seguridad 8.3.3 - Soportes físicos en tránsito

  Hace falta proteger los medios del acceso no autorizado durante su transporte.

2.2. Dominio 9 - Control de accesos

2.2.1. Objetivo de control 9.1 - Requisitos de negocio para el control de accesos

- Control de seguridad 9.1.1 - Política de control de accesos

  Hace falta políticas documentadas y revisadas que establezcan el control de acceso a instalaciones de procesamiento de información.

- Control de seguridad 9.1.2 - Control de acceso a las redes y servicios asociados

  Existen restricciones a servicios de red, pero hace falta especificar más los servicios autorizados a usar.

2.2.2. Objetivo de control 9.2 - Gestión de acceso de usuario

- Control de seguridad 9.2.1 - Gestión de altas/bajas en el registro de usuarios

  Hace falta establecer procesos formales para el registro y baja de usuarios, lo que permite una correcta asignación de derechos de acceso.

- Control de seguridad 9.2.2 - Gestión de los derechos de acceso asignados a usuarios

  Hace falta formalidad en la asignación de acceso a los usuarios, así también al revocar estos.

- Control de seguridad 9.2.3 - Gestión de los derechos de acceso con privilegios especiales

  Los derechos de acceso privilegiados se encuentran controlados por la unidad de sistemas de la organización.

- Control de seguridad 9.2.4 - Gestión de información confidencial de autenticación de usuarios

  La asignación de información de autentificación se controla a través del correo y teléfono personal.

- Control de seguridad 9.2.5 - Revisión de los derechos de acceso de los usuarios

  No existe revisión de derechos de acceso por parte de los propietarios de activos.

- Control de seguridad 9.2.6 - Retirada o adaptación de los derechos de acceso

  Hace falta formalizar la remoción de derechos de acceso a información de los empleados al concluir su empleo.

2.2.3. Objetivo de control 9.3 - Responsabilidades del usuario

- Control de seguridad 9.3.1 - Uso de información confidencial para la autenticación

  No existen prácticas establecidas por la organización para el uso de información de autenticación secreta por parte de los usuarios.

2.2.4. Objetivo de control 9.4 - Control de acceso a sistemas y aplicaciones

- Control de seguridad 9.4.1 - Restricción del acceso a la información

  Hay un control establecido mediante roles para restringir el acceso a la información y funciones del sistema.

- Control de seguridad 9.4.2 - Procedimientos seguros de inicio de sesión

  Hace falta una política de control de acceso, para formalizar el procedimiento de ingreso seguro.

- Control de seguridad 9.4.3 - Gestión de contraseñas de usuario

  Si existe un sistema de gestión de contraseñas, lo cual asegura la calidad de éstas.

- Control de seguridad 9.4.4 - Uso de herramientas de administración de sistemas

  Hace falta establecer un control estricto de programas que sean capaces pasar por alto los controles del sistema.

- Control de seguridad 9.4.5 - Control de acceso al código fuente de los programas

  El acceso al código fuente está restringido por parte de la unidad de sistemas de la organización.

2.3. Dominio 10 - Cifrado

2.3.1. Objetivo de control 10.1 - Controles criptográficos

- Control de seguridad 10.1.1 - Política de uso de los controles criptográficos

  Se debe desarrollar e implementar un método criptográfico a fin de proteger la información sensible.

- Control de seguridad 10.1.2 - Gestión de claves

  Se debe tener una política de tiempo de vida de las claves criptográficas.

2.4. Dominio 11 - Seguridad física y ambiental

2.4.1. Objetivo de control 11.1 - Áreas seguras

- Control de seguridad 11.1.1 - Perímetro de seguridad física

  Los perímetros de seguridad están definidos con pegatinas, avisos, carteles, etc.

- Control de seguridad 11.1.2 - Controles físicos de entrada

  El acceso a las áreas restringidas es sólo a personal autorizado, que son debidamente custodiadas.

- Control de seguridad 11.1.3 - Seguridad de oficinas, despachos y recursos

  Ambientes seguros y acondicionados. Personal de seguridad encargado de resguardar los ambientes.

- Control de seguridad 11.1.4 - Protección contra las amenazas externas y ambientales

  Ambientes acondicionados contra amenazas naturales, externas y accidentes.

- Control de seguridad 11.1.5 - El trabajo en áreas seguras

  No existen procedimientos para realizar trabajos en áreas seguras.

- Control de seguridad 11.1.6 - Áreas de acceso público, carga y descarga

  No existen áreas de despacho y carga.

2.4.2. Objetivo de control 11.2 - Seguridad de los equipos

- Control de seguridad 11.2.1 - Emplazamiento y protección de equipos

  Los equipos están asegurados contra robo (términos de referencia en contrato de vigilancia) y desastres naturales.

- Control de seguridad 11.2.2 - Instalaciones de suministro

  El área cuenta con pozo a tierra que protege a los equipos, así también con reguladores de voltaje en cada uno de estos.

- Control de seguridad 11.2.3 - Seguridad del cableado

  Los equipos de telecomunicaciones están protegidos y debidamente identificados y señalados.

- Control de seguridad 11.2.4 - Mantenimiento de los equipos

  Existe personal asignado a las tareas de servicio y asistencia de equipos.

- Control de seguridad 11.2.5 - Salida de activos fuera de las dependencias de la empresa

  No se puede proceder al retiro de equipos sin autorización de los encargados.

- Control de seguridad 11.2.6 - Seguridad de los equipos y activos fuera de las instalaciones

  Los equipos están identificados por la oficina de control patrimonial.

- Control de seguridad 11.2.7 - Reutilización o retirada segura de dispositivos de almacenamiento

  Cuando se da de baja un equipo, no se asegura que la información sea totalmente eliminada.

- Control de seguridad 11.2.8 - Equipo informático de usuario desatendido

  Debería de establecerse un protocolo de usuarios desatendidos.

- Control de seguridad 11.2.9 - Política de puesto de trabajo despejado y bloqueo de pantalla

  Implementar una política de procedimientos de limpieza de escritorio.

2.5. Dominio 12 - Seguridad operativa

2.5.1. Objetivo de control 12.1 - Responsabilidades y procedimientos de operación

- Control de seguridad 12.1.1 - Documentación de procedimientos de operación

  Es importante disponer de la información a todos los usuarios que necesiten saber sobre los procedimientos operativos.

- Control de seguridad 12.1.2 - Gestión de cambios

  Debe establecerse un control delos cambios en los procesos, instalaciones y sistemas relacionados a la información.

- Control de seguridad 12.1.3 - Gestión de capacidades

  Debe realizarse un monitoreo a las proyecciones de las capacidades del desempeño requerido del sistema.

- Control de seguridad 12.1.4 - Separación de entornos de desarrollo, prueba y producción

  A fin de reducir los riesgos de acceso no autorizado o cambios al entorno operativo.

2.5.2. Objetivo de control 12.2 - Protección contra código malicioso

- Control de seguridad 12.2.1 - Controles contra el código malicioso

  Se debe llevar un control de las incidencias sobre la detección, prevención y recuperación contra código malicioso.

2.5.3. Objetivo de control 12.3 - Copias de seguridad

- Control de seguridad 12.3.1 - Copias de seguridad de la información

  Se hace uso de herramientas en la nube como respaldo.

2.5.4. Objetivo de control 12.4 - Registro de actividad y supervisión

- Control de seguridad 12.4.1 - Registro y gestión de eventos de actividad

  Hace falta el registro de los eventos realizados por el personal, así también como fallas presentadas en los sistemas.

- Control de seguridad 12.4.2 - Protección de los registros de información

  Hace falta mantener la privacidad de la información generada por los eventos.

- Control de seguridad 12.4.3 - Registros de actividad del administrador y operador del sistema

  No existe la necesidad de registrar los eventos realizados por el personal administrativo.

- Control de seguridad 12.4.4 - Sincronización de relojes

  Los relojes están sincronizados de acuerdo a la zona horaria que brinda internet.

2.5.5. Objetivo de control 12.5 - Control del software en explotación

- Control de seguridad 12.5.1 - Instalación del software en sistemas en producción

  Se debería de tener los procedimientos documentados para la instalación de software en sistemas operacionales.

2.5.6. Objetivo de control 12.6 - Gestión de la vulnerabilidad técnica

- Control de seguridad 12.6.1 - Gestión de las vulnerabilidades técnicas

  Se debería tener documentada aquellas vulnerabilidades técnicas que pueden afectar a los sistemas de información.

- Control de seguridad 12.6.2 - Restricciones en la instalación de software

  Se tienen explícitas las reglas para que los usuarios no realicen alguna instalación.

2.5.7. Objetivo de control 12.7 - Consideraciones de las auditorías de los sistemas de información

- Control de seguridad 12.7.1 - Controles de auditoría de los sistemas de información

  Se debería auditar de las actividades que involucran al sistema de información y los procesos del negocio.

2.6. Dominio 13 - Seguridad en las telecomunicaciones

2.6.1. Objetivo de control 13.1 - Gestión de la seguridad en las redes

- Control de seguridad 13.1.1 - Controles de red

  Debe gestionarse el control de las redes, mediante la configuración correcta de los equipos, aplicaciones e información que comprometen.

- Control de seguridad 13.1.2 - Mecanismos de seguridad asociados a servicios en red

  Se debe tener mecanismos de seguridad, niveles de servicio y requisitos de gestión.

- Control de seguridad 13.1.3 - Segregación de redes

  Se debe segregar la información para los usuarios

2.6.2. Objetivo de control 13.2 - Intercambio de información con partes externas

- Control de seguridad 13.2.1 - Políticas y procedimientos de intercambio de información

  Hace falta políticas y/o directivas establecidas para la transferencia formal de información.

- Control de seguridad 13.2.2 - Acuerdos de intercambio

  No existe un acuerdo que dirija la transferencia segura de la información con las partes externas.

- Control de seguridad 13.2.3 - Mensajería electrónica

  Los correos utilizados para mensajería son institucionales, lo cual reduce el riesgo de alteraciones.

- Control de seguridad 13.2.4 - Acuerdos de confidencialidad y secreto

  Al contratar personal para la unidad, se indican los acuerdos de confidencialidad.

2.7. Dominio 14 - Adquisición, desarrollo y mantenimiento de sistemas de información

2.7.1. Objetivo de control 14.1 - Requisitos de seguridad de los sistemas de información

- Control de seguridad 14.1.1 - Análisis y especificación de los requisitos de seguridad

  Hace falta establecer requisitos relacionados a la seguridad cuando se realiza la planificación de un sistema de información.

- Control de seguridad 14.1.2 - Seguridad de las comunicaciones en servicios accesibles por redes públicas

  Se aplica el firewall FORTINET.

- Control de seguridad 14.1.3 - Protección de las transacciones por redes telemáticas

  Se debe tener directivas o protocolos para proteger las transacciones de servicios de aplicaciones.

2.7.2. Objetivo de control 14.2 - Seguridad en los procesos de desarrollo y soporte

- Control de seguridad 14.2.1 - Política de desarrollo seguro de software

  Existen reglas para un desarrollo que software están establecidas por el área de TI.

- Control de seguridad 14.2.2 - Procedimientos de control de cambios en los sistemas

  Hace falta un mejor control del proceso de mejora en los sistemas de información.

- Control de seguridad 14.2.3 - Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

  Hace falta una revisión exhaustiva de los módulos de sistemas desarrollados antes de su despliegue.

- Control de seguridad 14.2.4 - Restricciones a los cambios en los paquetes de software

  Se debe tener un control en las actualizaciones o modificaciones en los paquetes de software.

- Control de seguridad 14.2.5 - Uso de principios de ingeniería en protección de sistemas

  Debería de realizarse un control de gestión.

- Control de seguridad 14.2.6 - Seguridad en entornos de desarrollo

Existe un ambiente designado para el área de TI donde se da atención a los sistemas de comunicación y los sistemas de información.

- Control de seguridad 14.2.7 - Externalización del desarrollo de software

  Los encargados del área de TI, se mantienen monitoreando las actividades de desarrollo de los sistemas contratados.

- Control de seguridad 14.2.8 - Pruebas de funcionalidad durante el desarrollo de los sistemas

  Se debería llevar a cabo pruebas de seguridad durante el desarrollo.

- Control de seguridad 14.2.9 - Pruebas de aceptación

  Se debe tener un esquema donde se tenga mapeado los requerimientos de los sistemas, a fin de tener un Checklist de las implementaciones.

2.7.3. Objetivo de control 14.3 - Datos de prueba

- Control de seguridad 14.3.1 - Protección de datos de prueba

  Existe una política de desarrollo seguro con calidad de software.

ETAPA III: PROPUESTA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

3.1. Objetivo

Presentar las actividades a desarrollar durante en el año 2022, en el marco de la implementación y gestión del Sistema de Gestión de Seguridad de la Información (SGSI) que contribuya al objetivo de mejorar la seguridad informática de la empresa Agrokasa S.A. alineados a la norma internacional ISO/IEC 27002:2013, enmarcado en el ciclo de mejoramiento continuo Planear, Hacer, Verificar y Actuar (PHVA).

3.2. Documentos de referencias

- Norma internacional "ISO/IEC 27002. Estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013".
- Plan de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa Agrokasa S.A.

3.3. Definiciones y Siglas

3.3.1. Definiciones

- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización.
- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.
- Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.
- Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.
- Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

3.3.2. Siglas

- SGSI: Sistema de Gestión de Seguridad de la Información.
- CGSI: Comité de Gestión de Seguridad de la Información.
- ASI: Área de Seguridad de la Información.

3.4. Consideraciones previas

La implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI), se alinea al ciclo de mejora continua de la siguiente forma:

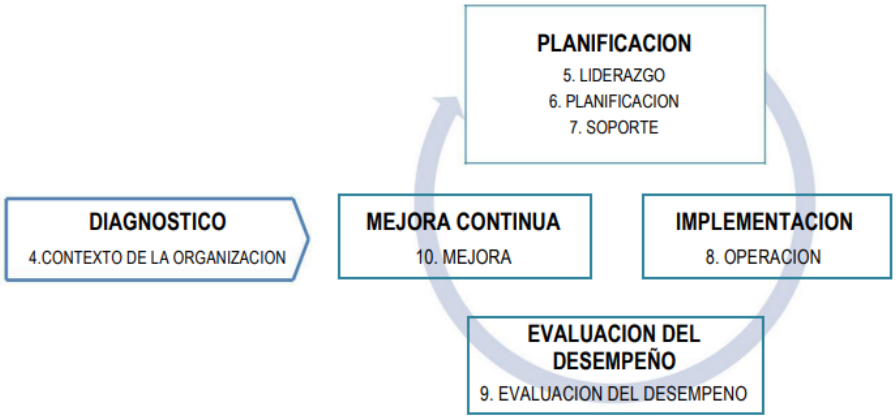


Figura: Norma ISO 27002:2013 alineado al ciclo de mejora continua.

3.5. Situación actual

3.5.1. Diagnóstico de situación actual

De acuerdo con el diagnóstico realizado en la presente investigación sobre la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el año 2022, se obtiene el nivel de implementación para los controles de seguridad de la Etapa II bajo la norma internacional ISO/IEC 27002:2013 como sigue a continuación:

Tabla. Implementación de controles ISO 27002:2013 en la investigación

Dominio	Aplicabilidad (%)
Dominio 8: Gestión de activos	30
Dominio 9: Control de acceso	25
Dominio 10: Criptografía	20
Dominio 11: Seguridad física y del entorno	30
Dominio 12: Seguridad de las operaciones	20
Dominio 13: Seguridad de las comunicaciones	30
Dominio 14: Adquisición, desarrollo y mantenimiento de sistemas	30
Promedio de implementación de controles	26%

De acuerdo a la declaración de aplicabilidad de los controles de la norma internacional ISO/IEC 27002:2013 en la empresa Agrokasa S.A., a la fecha sólo se ha llegado a implementar un 26% de los controles de seguridad.

3.5.2. Fases de implementación del SGSI

En el mes de noviembre y diciembre del año 2022 se desarrollarán las actividades de implementación a mayor detalle de la presente propuesta, puesto que serán evaluadas en las próximas evaluaciones.

En esta fase se persigue los siguientes objetivos:

- Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permita determinar la efectividad de la implantación del SGSI en la empresa.
- Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI en la empresa.

3.6. Cronograma

El cronograma de implementación de la propuesta de la solución planteada (Sistema de Gestión de Seguridad de la Información - SGSI) para el año 2022 se presenta a continuación:

N°	Tarea	Duración	Inicio	Fin
1	Diagnóstico de la situación actual	15 días	15/06/2022	30/06/2022
2	Seguimiento de los resultados de la evaluación 2021-2022	30 días	01/07/2022	30/07/2022
3	Realización de evaluaciones 2022-2023	30 días	01/08/2022	30/08/2022
4	Nivel de implementación de los controles ISO 27002:2013	120 días	01/09/2022	30/12/2022
5	Ejecutar pruebas de ingeniería social	15 días	01/01/2023	15/01/2023

3.7. Desarrollo del SGSI

El resumen de las principales actividades durante la vigencia 2022 se describen a continuación:

Metas	Actividades / Instrumentos / Resultados
1. Conocer situación actual	Se va a realizar la evaluación de la implementación de SGSI para establecer el punto de inicio del desarrollo de la presente propuesta para el año 2022.
2. Seguimiento a los resultados de evaluación 2022	Los informes de resultados de la aplicabilidad de la norma internacional ISO/IEC 27002:2013, nos muestran oportunidades de mejora, observaciones, áreas de preocupación y no conformidades que deben de ser consideradas en la presente propuesta.
3. Aplicación de los controles de la norma internacional ISO/IEC 27002:2013	Se va a realizar los cambios necesarios a fin de cumplir con todos los controles que corresponden a la seguridad informática exigidos por la norma: a. Gestión de activos. b. Control de acceso. c. Criptografía. d. Seguridad física y del entorno. e. Seguridad de las operaciones. f. Seguridad de las comunicaciones. g. Adquisición, desarrollo y mantenimiento de sistemas.
4. Ejecutar pruebas de Ingeniera Social	Ejecutar pruebas anuales de ingeniería social orientadas a verificar aspectos como: a. Los protocoles internos de seguridad. b. El nivel de concientización de los colaboradores de la empresa sobre temas de seguridad de la información. c. El conocimiento y/o cumplimiento de las políticas de seguridad de la información de la empresa. d. El nivel de exposición de la información publicada en internet de la empresa y de sus colaboradores.

Anexo 8 - Carta de autorización de aplicación de instrumentos

Agrokasa

"Año del Fortalecimiento de la Soberanía Nacional"

Ica, 05 de octubre del 2022

CARTA N° 00004-2022-GIM-AGK

A: Dr. Juan Francisco Pacheco Torres
Director de la escuela profesional de ingeniería de sistemas
Universidad Cesar Vallejo S.A.C

Asunto: CARTA DE ACEPTACION PARA EL DESARROLLO DE INVESTIGACION

De mi especial consideración

Es grato dirigirme a Usted, para saludarlo cordialmente y a la vez que la empresa AGROKASA S.A, Acepta el desarrollo del proyecto de investigación "Sistemas de gestión de seguridad de la información para mejorar la seguridad informática de la empresa Agrokasa S.A" realizado por el Sr. Jhonathan Felipe Paucar Espino identificado con DNI 72455276 y la Sra. Rosa Dina Zúñiga Monzón identifica con DNI 45678943, estudiantes del X ciclo de la escuela profesional de Ingeniería de sistemas de la universidad Cesar vallejo, realizando un aporte en mejorar nuestra institución

Se expide la presente carta a solicitud de la parte interesada para los fines que convengan

Atentamente

H. CHACALTANA

ING. HENRY CHACALTANA GARCIA
Jefe de operaciones hidráulica y electricidad

Anexo 9

Nivel de confiabilidad

Escala	Nivel
0.00 < sig. < 0.20	Muy bajo
0.20 < sig. < 0.40	Bajo
0.40 < sig. < 0.60	Regular
0.60 < sig. < 0.80	Aceptable
0.80 < sig. < 1.00	Elevado

Fuente: (Casan, 2017)

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, SAAVEDRA JIMENEZ ROBERT ROY, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Sistema de gestión de seguridad de la información para mejorar la seguridad informática de la empresa Agrokasa S.A., Ica 2022", cuyos autores son ZUÑIGA MONZON DINA ROSA, PAUCAR ESPINO JHONATHAN FELIPE, constato que la investigación tiene un índice de similitud de 22.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 18 de Noviembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
SAAVEDRA JIMENEZ ROBERT ROY **DNI:** 40832175 **ORCID:** 0000-0002-2788-4825	Firmado electrónicamente por: RSAAVEDRAJI el 18-11-2022 09:53:29

Código documento Trilce: TRI - 0444795

INVESTIGA UCV