UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSTGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

SGSI y la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información

AUTOR:

Sanchez Rios, Jefferson (orcid.org/0000-0002-8041-3053)

ASESORES:

Dr. Acuña Benites, Marlon Frank (orcid.org/0000-0001-5207-9353)

Mtro. Aliaga Cerna, Dante (orcid.org/ 0000-0002-5775-3885)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA - PERÚ

2023

DEDICATORIA:

A mis padres Crisanto y Reyna por todo su esfuerzo para ser profesional, mi hermano Cris. A mi esposa Jaqueline, nuestras hijas Yanayra y Yadiel que son mi fortaleza e inspiración de seguir creciendo en lo profesional y personal.

AGRADECIMIENTO:

A Dios por acompañarme en cada paso y saber guiarme.

A los docentes de la escuela de postgrado por compartir sus valiosos conocimientos.

A mis compañeros y ahora amigos del “grupo 1”, por los esfuerzos nocturnos para salir exitosos en los trabajos y exposiciones.

Agradecimiento especial al Dr. Acuña Benites Marlon Frank por su apoyo y gran enseñanza como asesor de esta tesis.

DECLARATORIA DE AUTENTICIDAD DEL ASESOR

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, ACUÑA BENITES MARLON FRANK, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "SGSI en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023", cuyo autor es SANCHEZ RIOS JEFFERSON, constato que la investigación tiene un índice de similitud de 3.00%, 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, 31 de Julio del 2023

Apellidos y Nombres del Asesor:	Firma
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID:** 0000-0001-5207-9353	Firmado electrónicamente por: MACUNABE el 31-07-2023 22:59:29

Código documento Trilce: TRI - 0632282

INVESTIGA UCV

DECLARATORIA DE ORIGINALIDAD DEL AUTOR

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Originalidad del Autor

Yo, SANCHEZ RIOS JEFFERSON estudiante de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "SGSI en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

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

Nombres y Apellidos	Firma
JEFFERSON SANCHEZ RIOS **DNI:** 42722968 **ORCID:** 0000-0002-8041-3053	Firmado electrónicamente por: SSANCHEZRI10 el 31-07-2023 07:29:41

Código documento Trilce: TRI - 0632285

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

Pág.

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación titulada “SGSI y la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023", tuvo como objetivo general determinar la influencia de un SGSI en el área de TI.

La investigación fue de tipo básica, con diseño no experimental, correlacional y transversal con enfoque cuantitativo, la población y muestra de 50 colaboradores, aplicando la técnica “encuesta” y de instrumento “el cuestionario” con escala tipo Likert, que fue validado por juicio de expertos, con una confiabilidad de alfa de Cronbach 0.816 y 0.926 aplicadas a las variables SGSI y gestión de seguridad electrónica.

El tratamiento de datos empleando el software estadístico SPSS en su versión 25, se aplicó la prueba de normalidad Kolmogorov – Smirnov porque la muestra era mayor a 30, con resultado p-valor (0,2) mayor al alfa (0,05) y una prueba paramétrica para contrastar la hipótesis con alcance correlacional R de Pearson con p-valor (0,0).

Concluyendo que la hipótesis de investigación tiene relación positiva y significativa entre las variables de SGSI y gestión de seguridad electrónica y serán utilidad para las recomendaciones mejorando la gestión de los procesos internos en la empresa de servicios aéreos Lima 2023.

Palabras claves: SGSI, seguridad de la información, gestión de riesgos.

ABSTRACT

The present investigation entitled "ISMS and electronic security management of the IT area in an air service company, Lima 2023", had the general objective of determining the influence of an ISMS in the IT area.

The research was of a basic type, with a non-experimental, correlational and cross-sectional design with a quantitative approach, the population and sample of 50 collaborators, applying the "survey" technique and the "questionnaire" instrument with a Likert-type scale, which was validated by trial. of experts, with a reliability of Cronbach's alpha 0.816 and 0.926 applied to the SGSI variables and electronic security management.

The data treatment using the SPSS statistical software in its version 25, the Kolmogorov - Smirnov normality test was applied because the sample was greater than 30, with a result p-value (0.2) greater than alpha (0.05) and a parametric test to test the hypothesis with correlational range Pearson's R with p-value (0,0).

Concluding that the research hypothesis has a positive and significant relationship between the ISMS variables and electronic security management and will be useful for the recommendations to improve the management of internal processes in the air service company Lima 2023.

Keywords: ISMS, information security, risk management.

I. INTRODUCCIÓN

De acuerdo con la estructura de gobierno corporativo actual, el activo que se identifica como el más importante es la información y puede estar en muchas formas, impresa o escrita, electrónicamente, enviada en correo, mostrada en video, o hablar en una conversación. Ladino et al. (2011), argumentan que la expansión de las nuevas tecnologías interrelaciona las organizaciones que manejan información importante para el negocio. La interconexión con clientes de diferentes partes, la posibilidad de comerciar a través de Internet, así como la facilidad general de uso de tecnología y el entorno global de información han ayudado a las empresas a crecer más rápido y mejor. Sin embargo, la proximidad y la facilidad de uso de todas estas tecnologías plantea ciertos desafíos para las empresas y se vuelven más vulnerables a cualquier amenaza ambiental que pueden convertirse en un riesgo real para las empresas. Actividades organizativas normales que afectan al negocio.

López (2018), argumenta que implantar un sistema en la gestión de información, depende estructuralmente como está organizado, incluyendo características como tipo, tamaño, objetivos, razón social, procesos, recursos humanos y seguridad. Los requisitos definidos allí, respaldados por estándares internacionales como ISO/IEC 27001, describen un conjunto de herramientas comerciales que permiten estándares y mejores prácticas para desarrollar un cronograma de acciones detallando los procesos en seguridad.

A nivel internacional, Andrade y Chávez (2018) se enfocan en que el uso de del estándar ISO 27001 que brinda los controles en mejorar los procesos, contribuyendo a la mejora y aseguren la seguridad, integridad y usabilidad de los riesgos que se presentan y comentan que esto se ha logrado a través de una extensa investigación obtenido. Arlenys (2017) realizó un estudio basado en trabajo de campo en tres partes: planificación, preparación y comprensión del entrenamiento. Esta intervención permite disminuir los niveles de riesgos en la empresa. Laudon y Laudon (2016) y Miguel (2015) reconocen que la seguridad y

los controles débiles pueden generar problemas legales. Por ello, es importante que las empresas implementen mecanismos y estrategias para proteger la información no solo de sus clientes, socios comerciales y socios estratégicos. Aguilar-Antonio (2019) explicó que estos incidentes están relacionados con medidas de seguridad inadecuadas que conducen a la pérdida de productividad, reputación y competitividad, lo que resulta en robo de datos o la mayoría de las pérdidas ocurren en el sector comercial amenaza la supervivencia de la organización.

A nivel nacional, Rodríguez et al. (2020), Oficina Nacional de Información de Gobierno Electrónico, registra los tipos o modelos en seguridad de la información publicados en diario El Peruano, y se recomienda al estado el manejo en la información para el sector público. Salvaguardar activos sensibles. Esto también se aplica a las empresas privadas. Como parte de nuestra investigación, pudimos determinar cómo implantar el estándar ISO 27001 afectaría el estado de las empresas participantes. Esto fue determinado por análisis estadístico, y además de estos resultados, existe opinión de expertos sobre la caracterización de este efecto. Las entidades públicas frecuentemente identifican en entornos de riesgo donde las pérdidas pueden ser causadas por procesos, personas o eventos como resultado de las tecnologías de Crespo (2017). Las políticas basadas en el estándar ISO/IEC 27001:2013 pueden mitigar estos riesgos y concientizarlos.

El estudio se realizó para una empresa privada ubicada en Callao con acceso directo al Aeropuerto Internacional Jorge Chávez. Prestación de servicios de manejo de carga aérea, rampa y pasajeros con énfasis en servicios de carga (bodega) con sistemas electrónicos de seguridad en cuanto a acceso y video vigilancia, técnicamente gestionados por el área de TI, pero sin sistemas de procesos y/o procedimientos controles de gestión físicos y el personal concientice con la información sensible en su área de trabajo. Actualmente, el sistema de la aerolínea difiere del utilizado por la cadena de cámaras de vigilancia 24 horas de CCTV: se generan guardias de seguridad y cuentas de usuario, pero el monitoreo se realiza en un software diferente, lo que significa que no hay una trazabilidad efectiva, ya que los derechos de verificación se almacenan en archivos que generar las llamadas "islas". Información sensible sobre estos usuarios, clientes, proveedores, etc. Deben ser protegidos. Además, si es necesario, las imágenes deben protegerse fuera del

sitio, ya que el DVR principal de 91 cámaras está ubicado en el centro de datos, más aún durante una pandemia; la tecnología está involucrada en la operación de sus procesos, pero a la vez procesos que enfrentan los múltiples riesgos y amenazas de TI, (Martínez, 2020).

Todas las empresas permanecen en riesgo y vulnerables a todos los ataques informáticos, Caamaño y Gil (2020). En otras palabras, las amenazas a los activos pueden conducir a la pérdida, alteración o destrucción de datos, Gil y Gil (2017). Por lo tanto, este análisis fue realizado de acuerdo al requerimiento de la aerolínea de implementar un SGSI para proteger los recursos de información del departamento de TI con énfasis en la seguridad electrónica.

Con base del fundamento descrito a la problemática, se propone un problema general y tres específicos. De acuerdo con ello, el problema general propuesto es: ¿En qué medida influye implementar un SGSI en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023? Generando los problemas específicos; PE1: ¿En qué medida el SGSI influye con la confidencialidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023?, PE2: ¿En qué medida el SGSI influye con la integridad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023?, PE3: ¿En qué medida el SGSI influye con la disponibilidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023?

En la siguiente investigación se plantea las justificaciones a fin de sustentar el desarrollo de este estudio, detallando sus clasificaciones teórica, metodológica y práctica.

Esta investigación se justifica teóricamente, porque aplicaremos ISO/IEC 27001:2013 misma brinda controles de como implementar SGSI aplicados a la seguridad de información. Una adecuada implementación del SGSI necesita que el personal tenga conocimiento y aplique las mejoras en el proceso como la identificación, autenticación y autorización de usuarios.

Esta investigación se justifica metodológica, porque se desprenden instrumentos de la recogida de información del SGSI bajo la ISO/IEC 27001:2013 que fortalece y mitiga riegos asegurando la preparación necesaria de los “core” de información. Cumpliendo con los objetivos marcados se han llevado a cabo los estudios pertinentes.

Esta investigación se justifica práctica, porque se plantea porque el activo que se identifica como el más importante es la información, por ello la seguridad electrónica tiene base tecnológica y es importante la necesidad de salvaguardar el activo seguro para limitar el riesgo que ocurra.

Así mismo objetivo general es determinar la influencia de un SGSI en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023. Se propone los siguientes objetivos específicos; OE1: Determinar la influencia del SGSI con la confidencialidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023. OE2: Determinar la influencia del SGSI con la integridad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023. OE3: Determinar la influencia del SGSI con la disponibilidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023.

La hipótesis general de la investigación es el SGSI influye significativamente en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023. Se comenta las siguientes hipótesis específicas; HE1: El SGSI influye significativamente con la confidencialidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023. HE2: El SGSI influye significativamente con la integridad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023. HE3: El SGSI influye significativamente con la disponibilidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023.

II. MARCO TEÓRICO

Sobre el contexto nacional de las siguientes investigaciones sobre el uso de SGSI y cómo contribuyen al control sobre la seguridad de la información. Según López (2022) que tuvo que realizar en una empresa constructora en Lima, existen muchas falencias en los controles y prácticas de seguridad requeridas para proteger los activos de datos en documentos físicos y digitales, así como a las personas. Como resultado, la empresa está expuesta a más riesgos, y el diagrama de Ishikawa se utiliza para ilustrar la solución de seguridad de la información, brindando una tasa de abandono promedio del 15 % por cada 100 usuarios, según el nivel "inicial", la meta será implementar o diseñar pautas en seguridad de información para los colaboradores sean concientizados en un 50%.

De igual forma, Huerta (2020) confirmó el uso de métodos cuantitativos en su trabajo evaluando el desarrollo en gestión de seguridad en información utilizando una población en 24 colaboradores. Después de los resultados la cantidad de dispositivos de control utilizados aumentó de 90.4% a 91.2% y se encontró que seguir los procedimientos y controles establecidos tuvo un impacto positivo para prevenir futuros ataques.

Así mismo Calderón (2019), refiere a la seguridad en la información hacia instituciones porque mejoran procedimientos internos y proteger la información reduciendo riesgos, por lo que su estudio cuantitativo no experimental, tipo básica, utilizando muestra en 83 empleados, utilizando una herramienta de cuestionario con 18 puntos por cada variable para recolectar información, se verifica si existe un vínculo directo entre sus variables, a medida que logra resultados estadísticos, lo hará. Asumiendo que se compara con la correlación Rho de Spearman, tiene una significancia de dos colas de 0,886 y un valor de p de 0,000, que es menor que el nivel de confianza que confirma vínculo positivo y las obtenidas en información seguridad para la entidad del estado en educación, considera que el 40,96% de la población cree bueno, el 48,19% califica medio y 3,61% como malo.

Está en línea con Pizarro (2022), cuyo problema se centró en las variables de gestión de riesgos en las instituciones que buscan relacionarse con seguridad de la información a fin que mejore en sus procesos, y en su trabajo cuantitativo

(utilizando un diseño no experimental) demostró que los tipos definidos, la muestra es de 80 colaboradores y se utiliza una herramienta de cuestionario. Entre ellas, la variable 1 tiene 19 puntos y la variable 2 tiene 24 puntos, indicando la relación entre sus variables existe correlación. Una institución pública porque obtuvo resultados estadísticos comparando sus hipótesis utilizando el coeficiente de Nagelkerke con una significación bilateral de 0,477 y un valor de p inferior a 0,000 (por debajo del nivel de confianza), confirmando correlación en las variables seguridad, el resultado fue 52,50%, de los cuales 42 encuestados consideraron el nivel medio, 33,75% consideraron el nivel demasiado alto y 13,75% consideraron el nivel demasiado bajo.

Además, Huayllani (2020) en su trabajo, cuyos temas están vinculados en la seguridad de información, así como riesgos en institución médica, mejorando evaluación, orientación y seguimiento de la información sensible y concluye en su estudio cuantitativo, no experimental, tipo básico, aplicando 145 colaboradores con cuestionario, su variable 1 con 34 ítems, variable 2 con 14 ítems, lo que demuestra relación entre variables. Aplicó Cronbach resultando 0,907 y 0,942, lo que confirma su excelente confiabilidad y los resultados estadísticos se obtuvieron mediante Rho de Spearman valor igual 0,856, mientras que alfa 0,000, con ello existe una alta correlación y cuyo resultado fue del 0,7% para quienes se encontró erróneo, el 81,4% lo encontró regular, el 17,9% lo encontró incompleto y para el SGR el 1,4% del 79,3% pensó que era rutinario y el 29% pensó que era efectivo.

De igual manera, la pregunta que se hace Tarillo (2016) en su trabajo es el impacto relacionado a los riesgos y seguridad aplicado en una localidad de provincia analiza reducir los incidentes y así garantizar buen servicio al cliente, su estudio cuantitativo no experimental, básico, con muestra aplicada a 50 asociados mediante un instrumento cuestionario que contiene 31 variable 1 en riesgos y 18 variable 2, validando que existe una correlación directa, centrándonos en el registro de Moyobamba, utilizando los resultados estadísticos para comparar este supuesto con el chi-cuadrado de Pearson, la correlación entre las variables es significativa en 15.712, que es mayor que la tabla Chi de (9.48) y rechazó la probabilidad, la hipótesis se acepta con un 95% de confianza y confirma vinculo positivo,

considerando en resultados; baja con un 18%, media con un 30% y entre variables con un 52% como alto.

Se equipara con Castro (2022) en su trabajo, cuyos temas aplican en seguridad y riesgos para en instituciones del sistema electoral, mejora la integridad de la información sensible y concluyó en su estudio cuantitativo, diseño experimenta, básico, una muestra de 45 empleados que utilizaron herramientas de cuestionarios para examinar variables, encontró que existe vínculo en sus variables, centrándose en entidades con sistemas de selección adecuados, con normalidad de Shapiro-Wilk es 0.947 y 0.956, respectivamente, con distribución normal, y se obtuvo estadísticamente usando Rho de S. resultó 0.924 con alfa 0.000 , confirmando positivamente correlación y se obtuvo en una muestra en 45 contribuyentes, con una completitud del 0% considerada pobre, 17.8% moderada y 71.1% alto.

Además, es semejante con Bernaldo (2018) en su trabajo, cuyo tema está relacionado con procesos de registro en institución estatal, generando confianza en su sistema al realizar el trámite a los ciudadanos, ganando así honor en su estudio cuantitativo no experimental, tipo básico, cuya muestra es 175 colaboradores utilizando una herramienta cuestionario, entre los cuales se encuentran 34 ítems para variables 1, y 9 ítems para la variable 1, afirmando relación o vínculo entre las variables y obtuvo el análisis de Cronbach 0,922 y 0,813, lo que confirma su excelente confiabilidad, ya que aplicando el Rho de Spearman de 0,781 con p de 0,000 entre las variables, resultando positivamente vínculos en sus del SGSI, el 72,5 % lo calificó como bajo, el 26,67 % lo calificó como medio y el 0,83 % de personas lo consideró alto.

Por otro lado León (2020) en su trabajo relacionado a la seguridad y riesgos para una institución electoral, concluyó en su estudio cuantitativo que al diseñar experimentos, el tipo básico, con 64 colaboradores en la muestra, utilizando 2 variables, confirmando relación entre ellas, donde el análisis de Cronbach es 0.823 y 0.821, lo que confirma su excelente confiabilidad, aplicando Shapiro-Wilk fue 0,947 y 0,956, respectivamente, lo que confirma su confiabilidad aplicando prueba Rho de Spearman es 0,722 y el valor p es 0,000, que está por debajo del nivel de

confianza, lo que confirma gran correlación en variables. Los resultados en muestra aplicado a 64 asociados sobre la variable seguridad de la información arrojaron 6,3% bajo, 79,7% normal y 14,1% alto; 7% bajo y 65,6% normal en la 12ª dimensión de usabilidad, 17,2% alto.

En el caso de Herrera (2017), la problemática era mejorar los procesos de una oficina de control y reglas digitales en documentos de gestión, concluyó en un estudio cuantitativo con diseño experimental, perteneciente al tipo básico, con una muestra de 60 contribuyentes, utilizando un instrumento cuestionario con 20 item y 19 items en su cuestionario, el análisis de Cronbach fue de 0.848 y 0.813 y 0.813, respectivamente, confirmando su excelente confiabilidad, y aplicando Rho de Spearman con resultado igual 1.0 para seguridad de la información y 0.805 para digitalización de documentos, el valor p es 0.000, que es menor que el nivel de confianza. , confirmando un vínculo positivo en las variables, cuyos resultados consultados fueron de 46,7% de los encuestados cree que es eficaz, el 40% cree que es eficaz y el 13,3% cree que es ineficaz.

Además, en su estudio de los tipos de aplicación, Izquierdo (2021) buscó brindar una alternativa a las implementaciones de SGSI, mediante la cual los investigadores compararon los estándares internacionales y se acordó. Los sujetos de estudio fueron 140 personal de farmacia, la muestra fue de 41 farmacias hospitalarias. Se propone el modelo con 4 etapas, que involucra procesos, subprocesos y herramientas de seguimiento. Se realizó en un hospital y la comparación del antes y el después mostró que la seguridad de la propiedad ha mejorado. Alrededor del 30% de la prueba completada.

De igual forma, Villadesa y Condor (2022) implementaron un SGSI en la ciudad y utilizaron Magerit v3 de gestión de riesgos y análisis aplicativos en su desarrollo cuantitativo, encuestando a una muestra de 47 encuestados. La recopilación de datos es aplicada no empírica. La precisión y seguridad de la herramienta fueron revisadas por tres expertos en la materia, lo que nos permitió evaluar las discrepancias y asegurar que el contenido de la tabla fuera corregido. Contexto del sujeto, variables de estudio, tamaño y resultados del estudio, resultado de confidencialidad con Cronbach. Se analizó el análisis alfa y el puntaje fue de

0,930, lo que se entiende que indica que la herramienta es calificada como excelente en cuanto a privacidad, su conclusión inicial es que el 2% cumple con los requisitos y en la situación actual las organizaciones entienden la importancia y los beneficios del SGSI, pero no se identifican riesgos de procesamiento y se observan amenazas internas y externas mediante el método Magerit y la investigación encontró que el municipio había alcanzado un nivel inaceptable ya que los activos excedieron su tolerancia al riesgo.

Y Benites (2019) cuando trabajaba en una fábrica de radiadores. Utilizó la investigación basada en documentos porque los documentos de la organización y la investigación de expertos sobre cuestiones en seguridad de la información que utilizan para desarrollarlo. Es experimental porque manipula las variables independientes y dependientes de acuerdo con una realidad particular. El total incluía a 50 personas del área de ingeniería y los resultados del análisis de brechas de control a través de entrevistas y cuestionarios estaban incompletos mayormente. Gracias al plan de implementación del SGSI, controles, políticas, métodos y estrategias desarrollados e implementados con la participación de la alta dirección, se ha incrementado en un 50% la concientización de los empleados de la fábrica con el resultado de buenos resultados, así como el Código de Conducta.

De igual manera, Huacasi (2018) en su estudio utilizó un estudio de diseño previo al ensayo para aplicar el SGSI a una unidad nacional cuya población es una unidad militar peruana con sede en la región de San Borja con 350 empleados y modelo TI con 38 empleados. utilizó una encuesta compuesta por 20 preguntas cerradas y utilizó el instrumento cuestionario. Con resultados obtenidos se finiquita a 38 encuestados de la Dirección de Información de las Fuerzas Terrestres del Perú, 12, es decir el 32%, piensan que cuentan con SGSI, 26 personas “sí” representando 68% en profesionales y otros encuestados en la Encuesta 14, cree tener información sobre la gestión de riesgos, es decir, el 37% de la población considera que la gestión de riesgos es gestión; mientras que 24 sintieron que no estaban en riesgo en cuanto al manejo de la información, la proporción fue del 63%. Así, mediante la formación y difusión del SGSI, es posible evaluar y analizar mejor la identificación de activos críticos, mejorando las medidas de seguridad y teniendo en cuenta el factor humano. Los empleados con conocimientos y habilidades en

seguridad de la información deben ser apreciados en puestos clave de TI para evitar la rotación de personal.

Por su parte, Ticona (2022) utilizó el género documental como un proyecto experimental en su investigación aplicada en Arequipa mientras describía las variables de investigación y su estilo expresado. En un entorno real, ya que afecta los activos, la población está determinada por todo lo que todas personas que trabajan en la empresa y todos los medios de comunicación, asumiendo un tamaño de muestra de 32 empleados. El análisis de riesgos se realizó utilizando el método Magerit V3 para estimar el impacto, es decir, medida de riesgo previa al estudio, en una muestra de 32 y una media de 1.00, luego obtenida con una media de 3, 91. Esto muestra una clara diferencia antes y después de implementar seguridad de la información según ISO/IEC27001:2013 a fin de reducir amenazas establecido. Sin embargo, cuando se trata de la puntuación de vulnerabilidad de la prueba previa 32, su puntuación media es 1,50 y la puntuación media de la prueba 32 posterior es 4,53. Esto muestra una diferencia significativa pre y post de implantar un diseño en IA enfocado en ISO/IEC27001:2013, siempre que se logre el objetivo hipotético, es decir, la eliminación de agujeros de seguridad. Los resultados de SGSI de 32 muestras tienen un valor medio de 1,09 y el valor medio después de la prueba de 32 muestras es 3,28. Esto demuestra que existe una diferencia significativa antes y después de implantar seguridad de la información orientada al ISO 27001, teniendo presente las metas asumidas, es decir, identificar el modelo de IA de mitigación del riesgo.

De igual forma Méndez (2022) en su estudio la empresa de administración tributaria en el norte del Perú utilizó un tipo de investigación aplicada caracterizada por la resolución de problemas mediante la aplicación o explotación del conocimiento adquirido, investigación descriptiva; porque la investigación descriptiva le permite definir en detalle una situación o evento, es decir, cómo se ve y cómo se manifiesta el evento. Aplico diseño no experimental con enfoque transaccional ya que se recolectaran los datos específicos. La finalidad fue observar, analizando variables durante un período de tiempo sin manipularlas, y la investigación tiene método deductivo en el sentido de que se extraen conclusiones lógicas de los resultados. El equipo está conformado por 4 colaboradores

responsables de cada sucursal en un área determinada, utilizan técnicas de recolección necesarios en diagnosticar la situación y controlar las etapas de selección para lograr el objetivo propuesto, además de realizar entrevistas y encuestas documental. Esta propuesta de proyecto SGSI ha sido desarrollada bajo el estándar NTP-ISO/IEC 27001:2014, utilizando las 4 fases del ciclo de Deming, que son necesarias para el lanzamiento del SGSI, Plan - Do - Check - Ley; Este estudio se encuentra en la primera fase del "Plan"; Esta fase se aplica solo al diagnóstico, diseño y modelado de SGSI. La información obtenida durante las entrevistas y verificación de documentos sobre asuntos relacionados con el requisito de cumplimiento y medidas de control de NTP-ISO/IEC 27001:2014 esta detallada por el Anexo A; y revisión de documentos con análisis de vulnerabilidad para determinar el estado vigente de la autoridad fiscal en base a seguridad de la información.

Como resultado, se identificaron las vulnerabilidades existentes a través del análisis GAP, donde se fijó el nivel de la norma dando 25%, por ello no cumplía con los requisitos mínimos. La necesidad de gestionar seguridad en la información determina cumplimientos en la organización, detalladas en su anexo en misma norma, lográndose un 30% de cumplimiento si la organización implementa medidas de control, pero no coinciden duplicadas, aprobadas y políticas agnósticas. El desarrollo en gestión en riesgos de una agencia auditada, identificando activos, asi como vulneraciones y amenazas ayuda determinando los niveles de riesgo presentado a la agencia, categorizar 20% de riesgo extremo, 60% de riesgo alto y 20% de riesgo medio; afectando la seguridad de la información.

Según Arias (2020), se han enfocado en la definición de la norma ISO 27001:2013, para optimizar las gestiones, en la fase de metodología se concibió como un proyecto piloto utilizando las estrategias de Uso para crear seguridad para proteger. Las directrices de la empresa son necesarias para que los datos se desarrollen verticalmente, la muestra empleada en el caso incluye 38 empleados, para este propósito, el vacío de información antes de que se complete la adopción de la norma ISO, conduce a una disminución del 49,0% en el próximo - Incremento del 18,0%, muestra impacto del 31,0%, en resumen: custodiar la información

partiendo de los instructivos necesarios. Se garantiza la seguridad de la información.

También Mejía (2020) señala que, en una práctica particular, se presentan violaciones a la seguridad de acceso a la propia base de información, incumplimiento de normas de custodia de la información y permisos a la información encriptaba. Existen otros aspectos como infraestructura por proteger la información, además de ausencia en políticas para asegurar la disponibilidad. Excepto; el estudio considera una aplicación porque proporciona una solución enfocada a las pautas en ISO/IEC 27001:2013; Estuvieron representados en 12 profesionales de tecnología, la muestra fue considerada como población general. De esta forma, se obtendrán los resultados del diseño y gestión del SGSI, las amenazas potenciales y las pruebas de vulnerabilidad, se identificará y documentará la solución óptima, teniendo en cuenta la eficacia de la información que se logró antes de la implementación de ISO. 0 y al final del ciclo la eficiencia es del 91,7%.

Refiriéndose a investigaciones en antecedentes internacionales, Roviralta (2021) señala que lo más importante es el activo de información. Sin este activo, no funcionará porque si no puede comunicarse con su proveedor, no puede acceder a su base de clientes o su sitio web se desconecta, podría estar en un gran problema. La información debe mantenerse confidencial para que nadie externo pueda influir en ella, cambiarla o incluso destruirla. Es importante clasificar la información para encontrar fácilmente quién tiene acceso a esa información ya quién se aplican políticas y/o controles de acceso. Por ello una preocupación importante en muchas organizaciones y urgencia nos muestra signos de disminuir en los próximos años. Resolver esto requiere un enfoque estructurado, y la serie ISO 27000 es uno de los métodos más populares para administrar la seguridad de la información, (Akinyemi et al. 2020).

De igual forma, Dau y Contreras (2022) utilizaron en su estudio un diseño de investigación descriptivo, teniendo en cuenta datos específicos, planificación en seguridad de la información, desarrollaron modelos a partir informaciones obtenida brindado por empleados. Se adoptó un estudio cuantitativo, se adoptó una estrategia basada en encuestas y se adoptó un método de encuesta. La encuesta

se enviará a 100 empleados de la compañía, cualquiera de los cuales esté involucrado en la implementación del modelo en privacidad y seguridad, garantizando la seguridad de la información, Se requiere desarrollar un SGSI que reduzca riesgos, así como vulnerabilidades, aplicando la información recibida de los empleados del Departamento Internacional de Defensa. Realice una encuesta en línea de 100 empleados de la empresa para conocer las vulnerabilidades en privacidad, así como seguridad de la información. Según lo revisado en el conocimiento la relación del estado con el riesgo de seguridad del SGSI. La mayoría (más del 50%) respondió que sí, otro caso de empleados relacionados con la gestión de comunicaciones y operaciones mostró que el 75% de las unidades flash están conectadas, el 70% utiliza dispositivos para almacenar y el 50% se almacena en la computadora, el 95% tiene archivos enviados por correo electrónico y el 95% tiene una conexión a Internet en su lugar de trabajo.

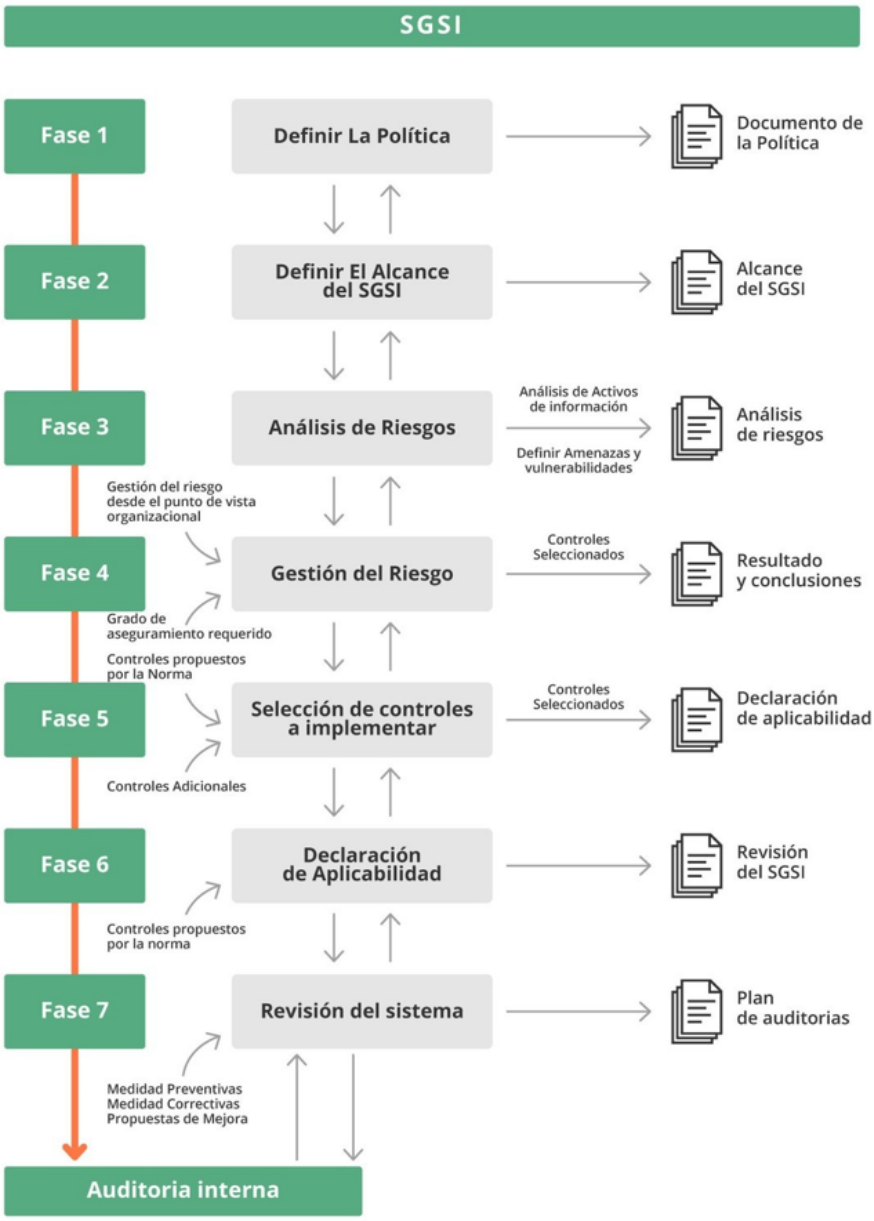
Por lo tanto, Penagos et al. (2016) señalan en su estudio que la implementando políticas y esquemas en seguridad definidos requiere equipos centrales debidamente capacitados, capaces de liderar los procesos de cambio organizacional. Siga las prácticas establecidas. Ararat, (2018) A fin de brindar orientación para la creación de sistemas sólidos en seguridad en la información, se tiene presente las normativas del ISO/IEC 27001:2013 al desarrollar procedimientos más prioritarios que rige todas las etapas en seguridad de información. Teóricamente enfocado a ISO/IEC 27001:2013, la Organización encargada de la estandarización – “ISO”, así como existe una Comisión en Electrónica – “IEC”, que la publicaron y protege “confidencialidad”, además “integridad” finalmente la “disponibilidad”, apoyándose en la gestión de riesgos sistémicos en los que confían las partes interesadas y que se gestionan adecuadamente. Además, Kenyon (2019) menciona en su libro ISO 27001 guía de controles, para implementar que se deben tener consideración los controles en los anexos A, ISO/IEC 27002.

Según Carvalho y Marques (2019), para gestionar mejor las amenazas y los desafíos en el ciberespacio, una empresa pública tomó la decisión de analizar para mejorar los niveles en seguridad de aplicaciones informáticas de acuerdo a las mejores prácticas relevantes. El enfoque adoptado se soporta en la gestión de

riesgos y tiene como fin establecer, así como implementar con desarrollos, mantener los aplicativos, finalmente mejorando frecuentemente el SGSI. Humphreys (2016) define similar a una norma internacional al ISO/IEC 27001: 2013 como grupos en obligaciones para poder establecer, luego implementando, monitoreando, evaluando, manteniendo, actualizando y mejorando un SGSI documentado en relación con los riesgos y oportunidades comerciales generales de la organización. Así mismo Lopes et al. (2019), Comentó que la adopción de la ISO 27001 por parte de las empresas crea un perfil apropiado para establecer, operar, monitorear, revisar, implementar y administrar un SGSI.

Shojaie et al. (2014) En la evaluación realizada en ISO 27001:2013, mencionan sobre los requerimientos principales para crear, implementar, dar mantenimiento y mejora constante en función del estándar examinado se determinan. También indican que han sido escritos de tal manera que dejan la posibilidad de usar varios formularios para su implementación y para que sean borrosos para correlacionar la numeración de puntos; Por lo tanto, podemos ver que las organizaciones estatales que están reguladas por el cumplimiento de los requisitos reglamentarios, así como las empresas de todas los rubros, tamaños y niveles de madurez, pueden estar de acuerdo con ISO/IEC 27001: 2013; En este sentido, a los efectos de este estudio, utilizaremos el término "recetas" para indicar los requisitos del estándar mencionado anteriormente.

Figura 1: Fases de un SGSI según ISO 27001

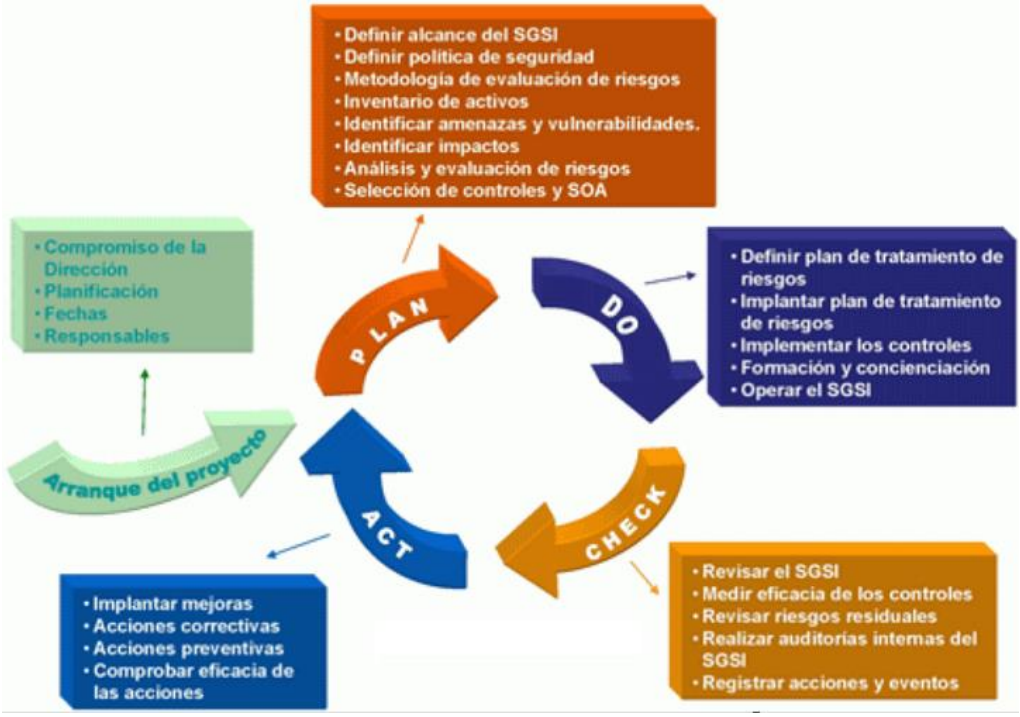


Fuente: piranirisk

De acuerdo al apartado anterior Torres (2018) menciona en su trabajo menciona sobre la implementación del SGSI obviamente es lo más importante en la organización porque brinda muchos beneficios. También mencionar que la información y sus procesos de soporte, los aplicativos de información y las conexiones de redes de las TIC son activos trascendentes y medidas de continuidad del negocio. Por otro lado, Sikman et al. (2019) sugieren que establecer

un SGSI es una decisión que cae dentro del área de planificación estratégica de una organización y de acuerdo con las funciones y requisitos comerciales de la organización. Además, Monev (2020) en su trabajo presenta un método práctico para realizar una evaluación de madurez en seguridad de información aplicada a empresas empleando SGSI, es decir un sistema con las pautas para implantar seguridad, enfocado al ISO 27001:2013. El método utiliza un estudio comparable a COBIT 5 para evaluar la preparación en los controles y regulaciones del ISO 27001:2013 y aplica la guía ISO 27002:2013.

Figura 2: Ciclo de mejora continua de Deming para un SGSI



Fuente: https://www.iso27000.es/

Ciclo Deming: También llamado con las siglas PDCA o PDCA, es un enfoque que consta de cuatro fases: ellas son: (P) Planificación, (H) Ejecución, (V) Verificación y (A) Acción (Córdoba, 2021).

Planificación: Comprende el desarrollo de todos los objetivos, así como los procesos generando soluciones requeridas por la organización. Además, permite una revisión más profunda de las organizaciones que son monitoreadas de forma independiente para lograr resultados positivos para su empresa. (Córdoba, 2021).

Implementación: ISO 27001:2013 requiere en las organizaciones implementen y controlen procesos críticos desde la prevención de amenazas. Además, significa implementar métodos y principios para prevenir ciberataques y pérdidas parciales o totales de información confidencial basados en el conocimiento de amenazas de seguridad (García, 2018).

Descripción general: Según capítulo 9 del estándar ISO 27001:2013 menciona sobre la evaluación continua en los avances en seguridad de la información. También se recalcar sobre implementación de la ISO 27001:2013 tendrá un mayor impacto en los controles de seguridad (Córdova, 2021).

Acción: Trate de eliminar las sorpresas para mejorar el comportamiento del SGSI a través de la innovación y la acción correctiva. Por ello, es importante demostrar que los controles en seguridad de la información están diseñados para custodiar en su totalidad la información. (García, 2018).

Según Aburto (2020), el objetivo cuando se trata de métodos de clasificación descriptivos y cuantitativos es desarrollar herramientas computacionales que trabajen acompañadas durante las etapas de desarrollo en ISO/IEC. Analizo 2 etapas en gestión de seguridad estándar, desarrollando una herramienta de TI para evaluar el estado los servicios y procesos. Lo implementado facilita la gestión centralizada. Los resultados se resaltan a continuación: Se integró una metodología informática para analizar la madurez de las tareas del servicio, así como la seguridad.

Así mismo Von (2019) asegura que la teoría de sistemas en general, se investiga sobre los factores y efectos del aprendizaje. Todos los procesos apuntan al mismo objetivo. una referencia de entrada (García, 2018) donde confirman que el sistema está conectado porque consiste y requiere un proceso lineal. Trate de obtener los productos correctos. De acuerdo con la teoría del sistema, mantiene relación con variables independientes y dependientes, luego se implementará la norma ISO 27001:2013 sobre gestión en información, así mismo los objetivos serán prevenir la pérdida de información, controlar y desarrollar. Entonces, aplicando principios en ISO 27000:2013 para prevenir la pérdida de información, prevenir

ataques cibernéticos, mejorar los controles de seguridad, aumentar la eficiencia, preservar todo lo relacionado con la instalación de investigación.

Como señaló Mero (2017), su investigación sobre métodos destinados a la implantación de SGSI aplica los normado en la ISO 27001. El estudio de riesgo aplicado describe a la empresa enfrenta riesgos de alto potencial para los cuales la empresa no ha sido capacitada. Una vez implementados, finaliza con el visto de la alta dirección de continuar los controles, así como los procesos implementados.

Según Solano (2020), se presentan 3 pilares ISO 27001 en tamaño, esto es muy importante, porque las limitaciones no deben aplicarse a los usuarios externos y al interior desean recibir información de la compañía, pero solo con la licencia inicial para el uso. Detente de manera efectiva. Según el mismo proceso, según la seguridad de un autor, las organizaciones autorizadas tienen prioridad para acceder a la información, porque el uso incorrecto de la información puede ser publicado y creado problemas legales. Con uso ilegal, explicó que es importante que sea importante que sea importante es importante que esto importante es tomar dinero para proteger el acceso al acceso a los usuarios sin autoridad y finalmente. Los autores confirman que la medición de la integridad es responsable de garantizar que la información no se cambie de ninguna manera cuando el último usuario eventualmente recibe y debe ser correcto para determinar. la información está protegida.

En este estudio, los siguientes parámetros ISMS fueron revisados y aplicados a ISO/IEC 27001:

Dimensión 1: Confidencialidad hace referencia a la información que no puede ser obtenida, leída o conocida por desconocidos o personas sin permiso. (Córdoba, 2021).

Dimensión 2: Integridad, Incibe (2019) establece que integridad hace referencia que la información no puede falsearse, ser precisa, no debe ser alterada intencional o indebidamente y las decisiones basadas en esta información no deben ser erróneas.

Dimensión 3: Disponibilidad, hace referencia a la información disponible bajo petición. Soriano (2014) define la accesibilidad a la información bajo demanda, ya que cualquier retraso más allá del nivel de servicio puede considerarse una violación de la accesibilidad.

Figura 3: Dimensiones - Seguridad de la Información

Fuente: kernel.com.mx

Las teorías relacionadas con riesgos de seguridad en información

Enfocado a la ISO/IEC 27005, hace referencia importante sobre el activo, identificando amenazas, así como vulnerabilidades apropiadas, identificar a los sujetos de prevención existentes y afecta el impacto de la divulgación de riesgos, así como identificar posibles consecuencias, y finalmente prioridades sus riesgos y gestión de acuerdo con los criterios para evaluar los riesgos en esta situación, pueden causar daños a una o más organizaciones operativas, pueden ser aleatorias o decididas, creadas por una persona o natural y natural y tener el interior o el exterior están relacionadas con la organización y establece que las pautas que pueden cambiar el riesgo, en todas las actividades, equipos, procesos, políticas y otros. Los controles no siempre proporcionan los resultados de modificación deseados. "El término salvaguarda o contramedida se usa a menudo como sinónimo de control".

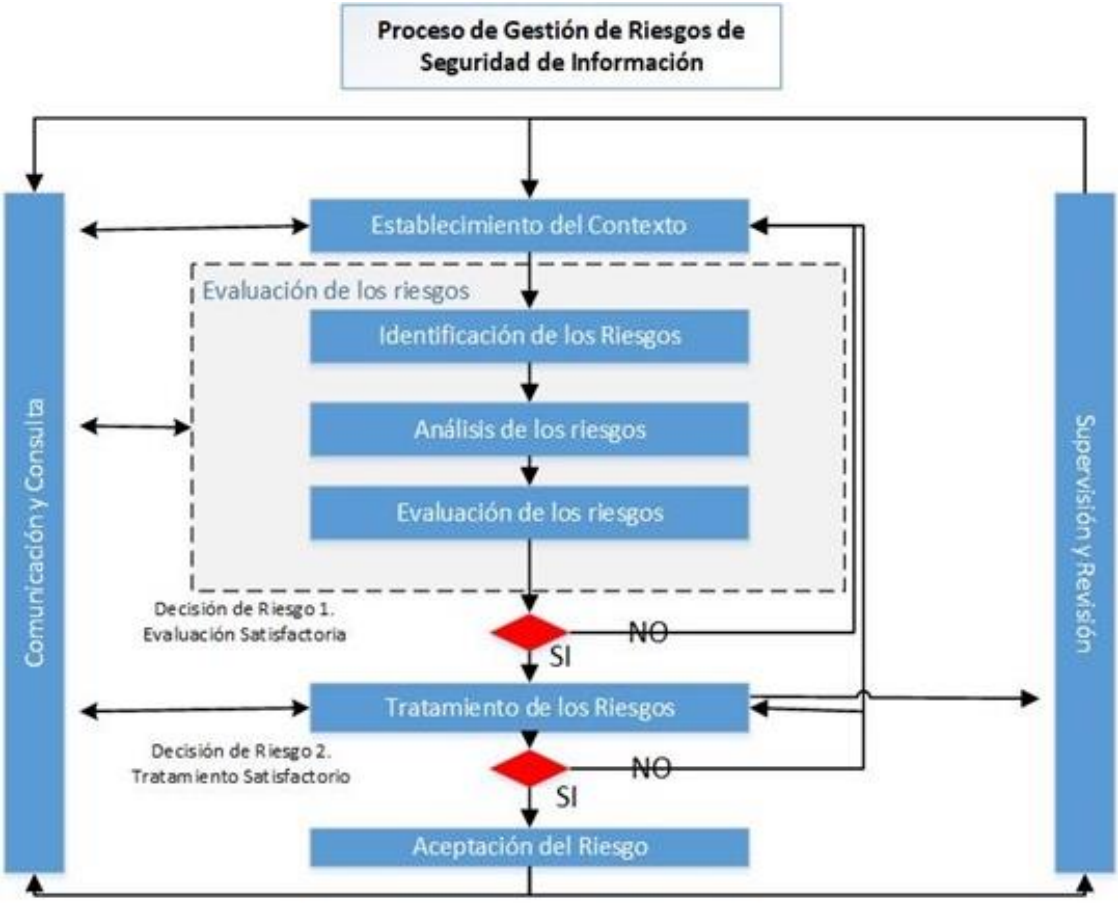
Además, Masso (2020) dice que la gestión de riesgos se enfoca como un grupo de actividades encaminadas para controlar una organización en vinculada al riesgo. También Corda et al. (2017), que establece como objetivo reducir la pérdida de información por falla del sistema que puede afectar el diseño de la empresa, falla natural, accidental o intencional, así como los riesgos legales y de comportamiento, teniendo en cuenta las amenazas potenciales.

Dimensión 1: Identificación de riesgos, ver norma ISO/IEC 27005:2018. identifica riesgos, determinando las pérdidas potenciales y comprender cómo, cuándo y por qué ocurrió un robo.

Dimensión 2: Análisis de riesgos, ver norma ISO/IEC 27005:2018, se define como conocer, derivado que permite analizar riesgos que serán aplicados en las decisiones tomadas.

Dimensión 3: Evaluación de riesgos, ver norma ISO/IEC 27005:2018, Estima importancia del activo y mide los estados maliciosos y vulnerabilidades existentes, identifica medidas de control existentes y su impacto en los riesgos identificados, determinando consecuencias complejas y eventuales. El impacto del riesgo derivado se prioriza y estructura de la evaluación de riesgo. La planificación en gestión humana es basada en resultados con diseño de una evaluación en riesgos que analiza las pautas, las habilidades, así como las competencias organizacionales (Fathurohman y Witjaksono, 2020).

Figura 4: Dimensiones - Gestión de Riesgos



Fuente: hkmexico.com

Según Ramírez y Ortiz (2011), La materialización del riesgo puede significar un impacto comercial significativo en forma de altos costos de cobro de deudas y la ausencia de disponibilidad en los servicios por la organización. Las evaluaciones de riesgos técnicos y su impacto en los activos de información, se tiene presente realizando una evaluación de riesgos en la continuidad gestionada. Haris (2018) apoyó la idea y afirmó que era plan de riesgo de activos críticos información para desarrollar mejores planes seguridad de información. Así es como es Descubrir, categorizar y priorizar es fundamental activos de información.

Además, Aedah y Hoga (2020), comenta que la seguridad son procesos continuos donde se desarrollan, así como implementan políticas, procedimientos que permiten colocar responsables de cada proceso y como solucionarlas, por ello podemos calcular los niveles en madurez. Además, el marco de ISO 27001, parece

lo suficientemente flexible como para ser utilizado para la mejora y maduración de procesos de otras áreas de gestión mediante la definición de controles relevantes. (Rukh y Malik, 2017).

Por lo mencionado, Yoseviano y Retnowardhani (2018), comentan en su trabajo que la información lo importante activo. Con el rápido desarrollo de la tecnología en información, aumentan las opciones o vulnerabilidades de riesgos. A ello las empresas deben implementar políticas adecuadas para proteger y controlar la seguridad en sus activos. Asi mismo los sistemas en gestión de seguridades en información, brindan las pautas o reglas para una buena evaluación de seguridad aplicando las pautas de norma ISO/IEC 27001:2013. (Kurnianto et al. ,2018).

Por otro lado, Podrecca et al. (2022), desarrollaron un conjunto de hipótesis basadas en la teoría y a través de un estudio de eventos a largo plazo complementado con una regresión de 143 empresas que cotizan en EE. UU. Los resultados indican que la certificación ISO/IEC 27001 está asociada con mejoras en la rentabilidad, la productividad laboral y parcialmente el desempeño de las ventas. (Lukitowati y Ramli 2020). Al mantener activos de información, las organizaciones generalmente administran seguridades mediante desarrollos, implementación en políticas que protegen la información, así como de contingencias.,

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Enfoque

Aplicó estudio cuantitativo, fueron observados, así como medidos. Las variables del mismo proceso general a lo específico, lo que da la oportunidad de dividir las variables en partes de acuerdo a la dimensión de medición (Arias, 2021).

Tipo

De tipo básica, Valderrama (2013) define de la siguiente manera: "Investigación que no trata de resolver problemas prácticos, si no aporta conocimiento, otras sectas son básicas o puras, que pretenden recoger información que el investigador ve en realidad, que tiene como objetivo encontrar conceptos regulares"

Diseño

Aplicado no experimental, este proyecto de investigación se trata de "observar fenómenos que ocurren en un contexto natural y luego analizarlos" y es transversal en el sentido de que incluye "recolectar datos a la vez", Hernández et al., (2014).
su propósito es describir variables, analizando sus relaciones en el momento preciso.

3.2. Variables y operacionalización

“SGSI”

Definición conceptual: Significa mantener confidencialidad, integridad y disponibilidad, todo lo asociado a su procedimiento en toda la organización. Según ISO/IEC 27001:2013.

Definición Operacional: El marco integra 14 dominios, 34 entidades y 144 protocolos. “Ellos abarcan a toda la organización que podrían comprometer sus procesos informáticos.” A los efectos de este documento, la medición se refiere al estado actual del cumplimiento del SGSI, así como la aplicación de la custodia.

Tabla 1: Operacionalización: V1 SGSI

Dimensión	Indicador	Ítem	Escala	Niveles o rangos
Confidencialidad	<Políticas_de_seguridad_de la_información> <Clasificación_de_activos_de_información>	1-2 3-6	<Nunca> <Casi_nunca> <A_veces> <Casi_siempre> <Siempre>	<Deficiente> <Regular> <Eficiente>
Integridad	<Protección_de_credenciales> <Incidentes_de_manipulación_de_datos>	7-8 9-12		
Disponibilidad	<Tiempo respuesta> <Respaldo de información>	13-14 15-18		

Fuente: Propia.

“Gestión de Seguridad Electrónica”

Definición Conceptual: Grupo de planteamientos para analizar posibles sucesos, así como pueden ser el efecto antes de decidir qué hacer y cuándo, reducir el riesgo. Además, puede referirse a un grupo de la organización. Según ISO/IEC 27005:2018.

Definición Operacional: Está determinada por una calificación derivada de un cuestionario que mide su impacto en una segunda variable de prueba usando ítems con rangos de respuesta tipo Likert bajo, medio y alto. Necesita el emplear un cuestionario, así como los resultados se aplican a SPSS versión 25.

Tabla 2: Operacionalización: V2 Gestión de Seguridad Electrónica

Dimensión	Indicador	Ítem	Escala	Niveles o rangos
Identificación de Riesgos	<Conocimiento_de_controles> <Conocimiento_de_riesgos>	1-3 3-6	<Nunca> <Casi_nunca> <A_veces> <Casi_siempre> <Siempre>	<Deficiente> <Regular> <Eficiente>
Análisis de Riesgos	<Identificación_de_riesgos> <Monitoreo_de_riesgos>	7-8 9-12		
Evaluación de Riesgos	<Aplicación_y_seguimiento> <Efectividad_en_los_controles y_niveles_de_riesgos>	13-14 15-18		

Fuente: Propia.

3.3. Población, muestra, muestreo

Población

Contó con 50 personas. Así mismo, Hernández et al. (2014) Se conceptualiza en grupo o conjunto de fenómenos en estudio, en el cual los colaboradores tienen igual peso de estudio.

Muestra

Se consideró 50 personas que trabajan en diferentes áreas. Cuando se trata de muestras, especialmente una pequeña fracción de toda la población. Esto quiere decir que es un subconjunto de componentes agregados construidos en sus propiedades, a los que llamamos población, para identificar los elementos que serán analizados es necesario contar con la población para enumerar los parámetros generando resultados, según (Hernández et al., 2018).

Tabla 3: Distribución de personas que conforman la muestra.

ÁREAS	CANTIDAD ENCUESTADOS
Departamento de Atención y Facturación	10
Departamento de Seguridad	9
Departamento de Planeamiento	3
Departamento Comercial	3
Departamento de GDH	4
Departamento de Operaciones Clientes	10
Departamento de Operaciones Aduaneras	6
Departamento Contabilidad	2
Departamento Finanzas	3
Total:	**50**

Fuente: Propia.

Muestreo

Aplicó el total de muestra, según Otzen y Manterola (2017), su propósito en confirmación es comprobar la relación entre distribución en variables.

3.4. Técnicas e instrumentos de recolección de datos.

Técnicas

"Encuesta". Contiene varias preguntas con una serie de respuestas codificadas aplicadas en variables para investigación (Hernández et al., 2014).

Instrumentos

Se empleó el instrumento "cuestionario". Así, estas herramientas se utilizan para obtener datos y son recursos que emplea el investigador registrando datos sobre los fenómenos estudiados (Hernández y Mendoza, 2018).

Tabla 4: Registro de Variable Uno

Técnica:	Encuesta
Instrumento:	SGSI
Autor:	Calderón (2019) adaptado para la investigación
Adaptado:	Jefferson Sanchez Rios (2023)
Escala:	Likert
Significación:	Dim1:Confidencialidad Dim2:Integridad Dim3:Disponibilidad
Extensión:	18 ítems
Administración:	Individual
Aplicación:	Colaboradores internos.
Duración	15 minutos.
Puntuación:	Las respuestas ante cada enunciado son: <<1.Nunca>> <<2.Casi nunca>> <<3.Algunas veces>> <<4.Casi siempre>> <<5.Siempre>>

Fuente: Propia

Tabla 5: Registro de Variable Dos

Técnica:	Encuesta
Instrumento:	Gestión de Seguridad Electrónica
Autor:	Calderón (2019) adaptado para la investigación
Adaptado:	Jefferson Sanchez Rios (2023)
Escala:	Likert
Significación:	Dim1:Identificación_de_riesgo Dim2:Análisis_de_riesgo Dim3:Evaluación_de_riesgo
Extensión:	18 ítems
Administración:	Personal.
Aplicación:	Colaboradores internos.
Duración	15 minutos.
Puntuación:	Las respuestas ante cada enunciado son: <<1.Nunca>> <<2.Casi nunca>> <<3.Algunas veces>> <<4.Casi siempre>> <<5.Siempre>>

Fuente: Propia

Validez

Se aplicó juicio de 3 expertos, mismo que valida confiabilidad en instrumentos del desarrollo de la investigación. (Ventura y Rodríguez, 2017).

Tabla 6: Relación Expertos - Validación de instrumento.

Expertos	Observaciones	Aplicabilidad
Dr. Marlon Frank Acuña Benites	Existe suficiencia	Aplicable
Mtro. Juan Carlos Sernaque Pacheco	Existe suficiencia	Aplicable
Mtro. Guillermo Fidel Vega Mere	Existe suficiencia	Aplicable

Elaborado: Propio.

Confiabilidad

La garantía es consistencia de los resultados proporcionados por una misma persona a diferentes casos, Hernández et al. (2018). Se aplicó el coeficiente Alfa de Cronbach, cuyo análisis fue generado por el software SPSS.

Tabla 7: Prueba de Confiabilidad en variables

Conceptos	Alfa / Cronbach	Cant. de ítems
SGSI	0,816	18
Gestión de Seguridad Electrónica	0,926	18

Fuente: Propia, SPSS v25.

De acuerdo con la información de la Tabla 7, para la variable SGSI resultó 0,816, cuyo valor se interpreta como adecuado. Asimismo, la siguiente variable de Gestión de Seguridad Electrónica, cuyo coeficiente alfa de Cronbach observado fue 0,926, también se encuentra un alcance superior y el instrumento es aceptado.

Tabla 8: Parámetros de interpretación del coeficiente A-C

Parámetros	**Alcance**
>=0.9	Superior
0.8 - 0.89	Adecuado
0.7 – 0.79	Suficiente
0.6 – 0.69	Dudoso
0.5 – 0.59	Escaso
<0.5	Inaceptable

Elaborado: Propio

3.5. Procedimiento

Sobre este punto se necesitó de la carta de presentación que se solicitó a la universidad, mismo fue firmado y aprobado por la empresa de servicios aéreos, Lima 2023, formalizando el pedido de autorización para poder desarrollar el tema de investigación.

La obtención de los datos fue extraída de 2 encuestas diseñadas y propuestas según la empresa de servicios aéreos para comprender la realidad de la variante independiente y dependiente, con sus respectivas dimensiones, a través de 18 preguntas. Los datos fueron tratados en el SPSS que brindó resultados estadísticos.

3.6. Método de análisis de datos

Herramientas utilizadas son considerados confiables cuando 03 expertos dieron los mismos resultados, y se utilizará la aplicación estadística SPSS versión 25 para apoyar el análisis de la información, para probar R de Pearson (coeficiente de correlación), para después comparar hipótesis y recomendaciones.

3.7. Aspectos éticos

Esta investigación se realiza bajo mi autoría, recabando información variada, el procesamiento, así como la interpretación fue realizada bajo mi interpretación, así como la solicitud mediante una carta de presentación a la empresa de servicios aéreos de autorización del desarrollo en la empresa donde se realizaron las encuestas y manteniendo la indicación del anonimato de los participantes.

Las referencias y citas se compilaron utilizando los estándares APA de la 7ª edición de la Asociación Americana de Psicología y el software Turnitin, mediante un trabajo de investigación bajo el código N° 110-2022-VI/UCV.

En relación a recopilación de datos se utilizaron dos encuestas anónimas, la dirección de investigación utilizada para este estudio bajo el código N° 0200-2018/UCV.

IV. RESULTADOS

4.1. Resultados Descriptivos:

Como resultados estadísticos ingresados al software SPSS versión 25 para 50 encuestados que participaron. Se analizó la frecuencia de cada variable y su respectiva dimensión.

Variable Independiente V1: SGSI

Interpretación:

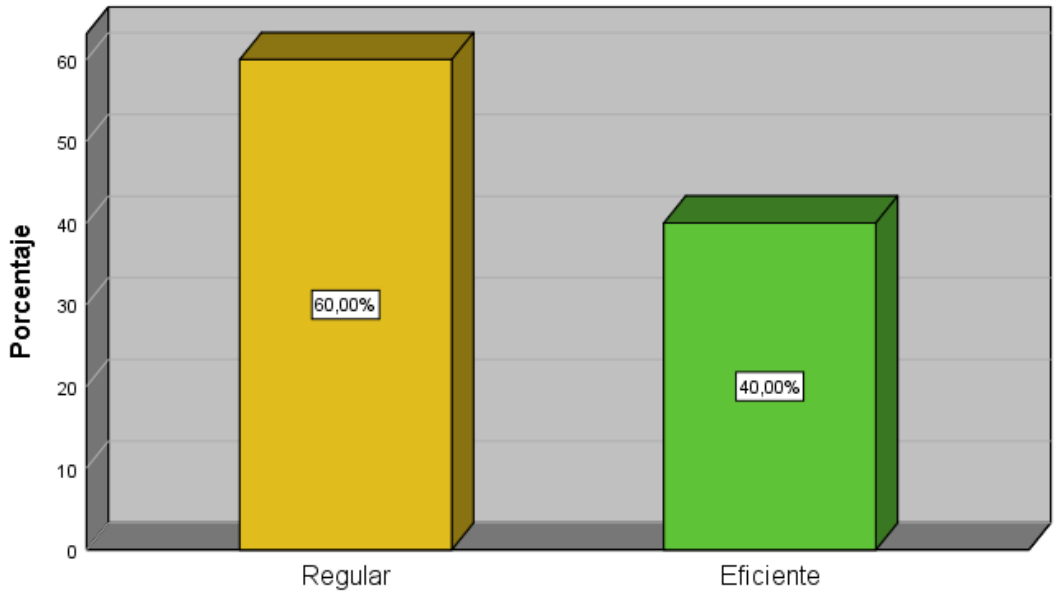
A continuación, en tabla número 8 y figura número 5 una muestra en 50 participantes referido a variable uno, los cuales calificaron 0% como deficiente, 60% como regular y 40% como eficiente.

Tabla 8: Análisis de Frecuencia V1: SGSI

Nivel	Rango	Frecuencia	%	% útil	% final
Deficiente	[5 - 13]	0	0	0	0
Regular	[14 - 22]	30	58,8	60,0	60
Eficiente	[23 - 30]	20	39,2	40,0	100
Suma:		50	98%	100%	

Fuente: Propio, SPSS

Figura 5: Esquema de Barras V1: SGSI



Fuente: SPSS

Variable 1 - Dimensión 1: Confidencialidad

Interpretación:

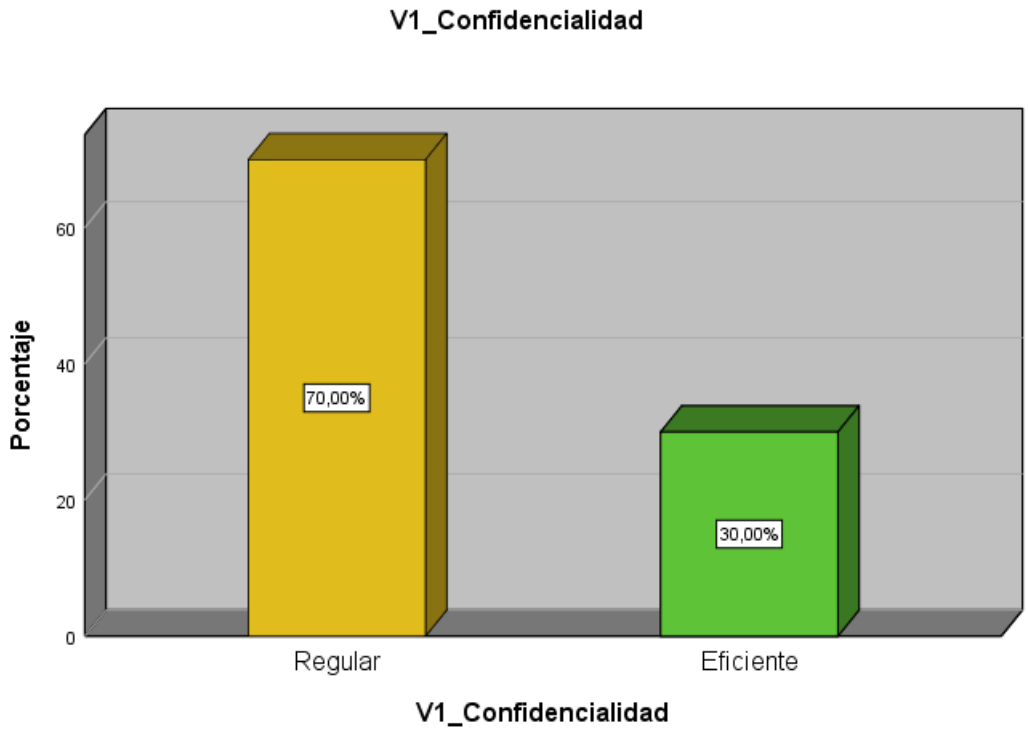
A continuación, en tabla número 9 y figura número 6 una muestra en 50 participantes para la variable uno, aplicado a su dimensión 1 “Confidencialidad”, que el 0% considera deficiente, el 70% considera regular y el 30% considera es eficiente.

Tabla 9: Análisis de Frecuencia V1 Dimensión 1: Confidencialidad

Nivel	Rango	Frecuencia	%	% útil	% final
Deficiente	[5 - 13]	0	0	0	0
Regular	[14 - 22]	35	70,0	70,0	70,0
Eficiente	[23 - 30]	15	30,0	30,0	100,0
Suma:		50	100%	100%	

Elaboración: Propia, SPSS.

Figura 6: Esquema de Barras V1 Dimensión 1: Confidencialidad



Fuente: SPSS v.25

Variable 1 - Dimensión 2: Integridad

Interpretación:

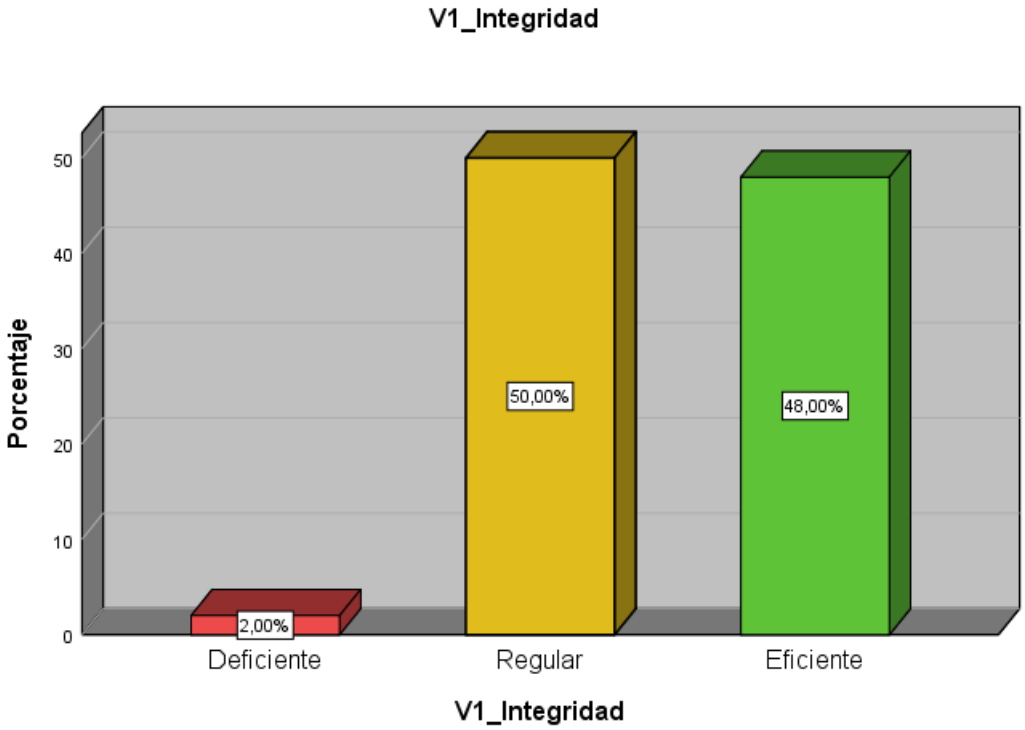
A continuación, en tabla número 10 y figura número 7, una muestra en 50 participantes de variable uno, aplicado a su dimensión 1 “Integridad”, que el 2% considera deficiente, el 50% considera regular y el 48% considera es eficiente.

Tabla 10: Análisis de Frecuencia V1 Dimensión 2: Integridad

Nivel	Rango	Frecuencia	%	% válido	% acumulado
Deficiente	[5 - 13]	1	2,0	2,0	2,0
Regular	[14 - 22]	25	50,0	50,0	52,0
Eficiente	[23 - 30]	24	48,0	48,0	100,0
Suma:		50	100%	100%	

Elaboración: Propia, SPSS.

Figura 7: Esquema de Barras V1 Dimensión 2: Integridad



Fuente: SPSS v.25

Variable 1 - Dimensión 3: Disponibilidad

Interpretación:

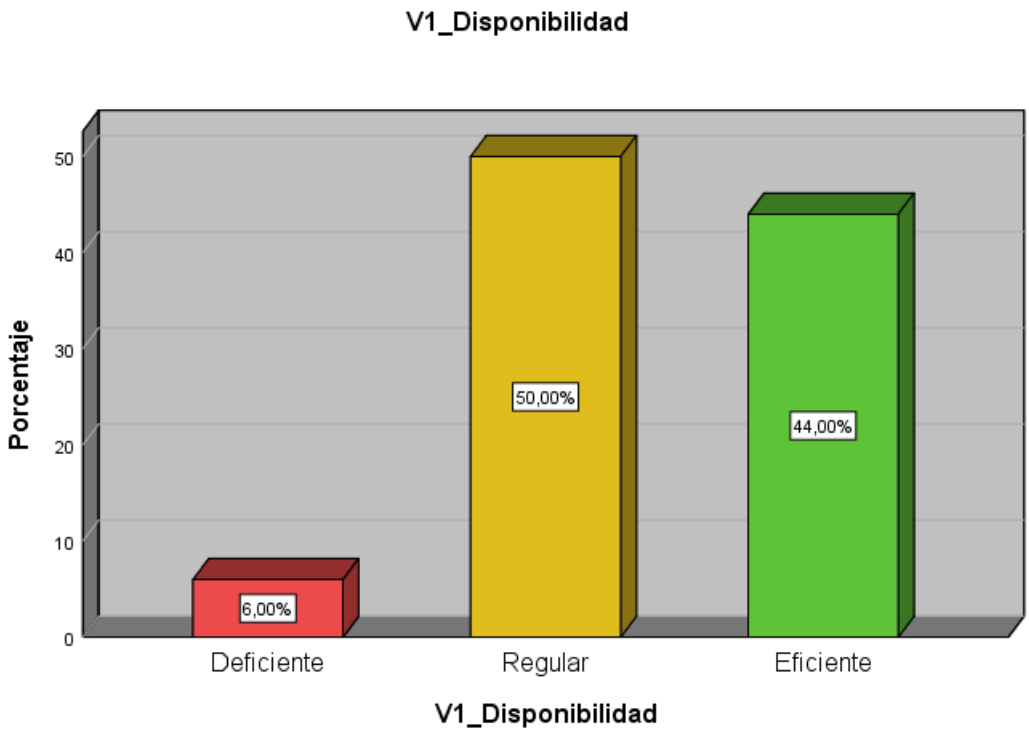
A continuación, en tabla número 11 y figura número 8, una muestra en 50 participantes para la variable uno, aplicado a su dimensión número 1 "Disponibilidad", representa el 6% deficiente, el 50% considera regular y el 44% considera es eficiente.

Tabla 11: Análisis de Frecuencia V1 Dimensión 3: Disponibilidad

Nivel	Rango	Frecuencia	%	% válido	% acumulado
Deficiente	[5 - 13]	3	6,0	6,0	6,0
Regular	[14 - 22]	25	50,0	50,0	56,0
Eficiente	[23 - 30]	22	44,0	44,0	100,0
Suma:		50	100%	100%	

Elaboración: Propia, SPSS.

Figura 8: Esquema en Barras V1 Dimensión 3: Disponibilidad



Fuente: SPSS v.25

Variable dependiente V2: Gestión de Seguridad Electrónica

Interpretación:

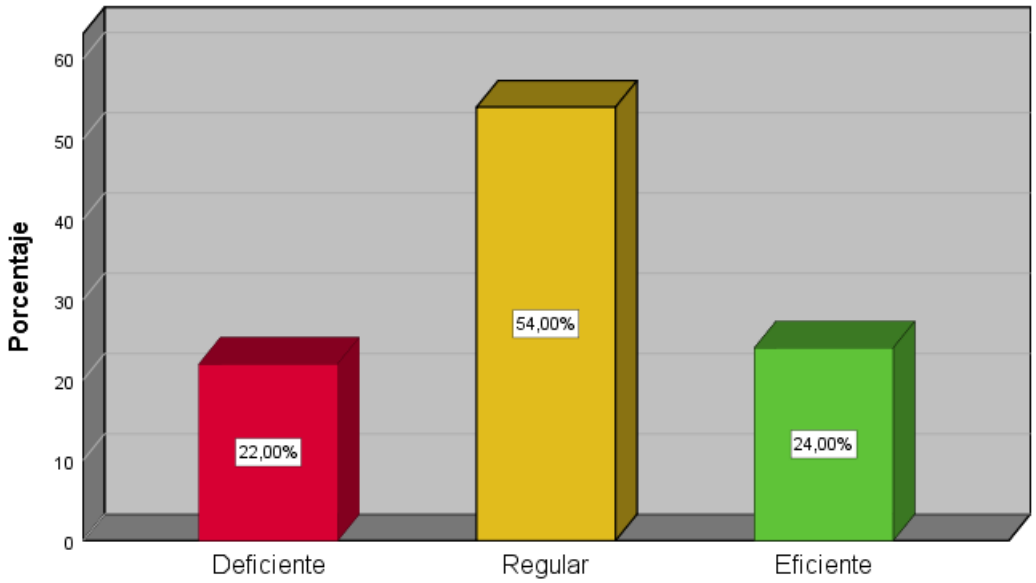
A continuación, en tabla número 12 y figura número 9, una muestra en 50 participantes para variable dos, que considera el 22% es deficiente, el 54% considera regular y el 24% considera es eficiente.

Tabla 12: Análisis de Frecuencia V2: Gestión de Seguridad Electrónica

Nivel	Rango	Frecuencia	%	% válido	% acumulado
Deficiente	[5 - 13]	11	21,6	22,0	22,0
Regular	[14 - 22]	27	52,9	54,0	76,0
Eficiente	[23 - 30]	12	23,5	24,0	100,0
Suma:		50	98%	100%	

Elaboración: Propia, SPSS.

Figura 9: Esquema en Barras V2: Gestión de Seguridad Electrónica



Fuente: SPSS v.25

Variable 2 - Dimensión 1: Identificación de Riesgos

Interpretación:

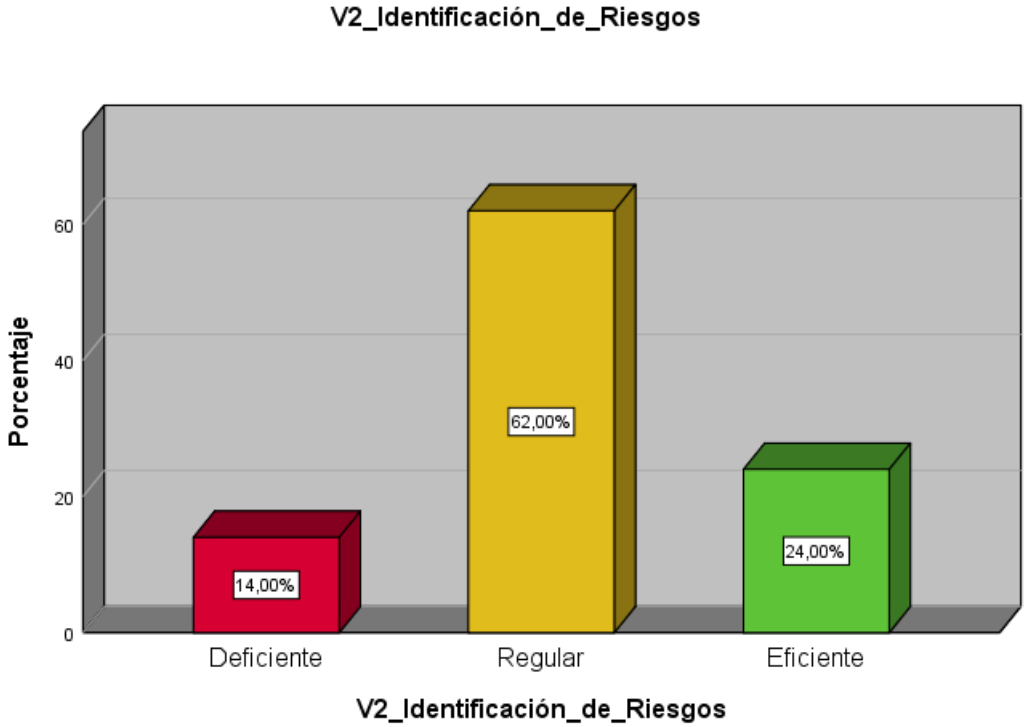
A continuación, en tabla número 13 y figura número 10, una muestra en 50 participantes para la variable dos, aplicado a su dimensión 1 “Identificación de Riesgos”, que el 7% considera deficiente, el 31% considera regular y el 12% considera es eficiente.

Tabla 13: Análisis de Frecuencia V2 Dimensión 1: Identificación de Riesgos

Nivel	Rango	Frecuencia	%	% válido	% acumulado
Deficiente	[5 - 13]	7	14,0	14,0	14,0
Regular	[14 - 22]	31	62,0	62,0	76,0
Eficiente	[23 - 30]	12	24,0	24,0	100,0
Suma:		50	100%	100%	

Elaboración: Propia, SPSS.

Figura 10: Esquema de Barras V2 Dimensión 1: Identificación de Riesgos



Elaboración: SPSS.

Variable 2 - Dimensión 2: Análisis de Riesgos

Interpretación:

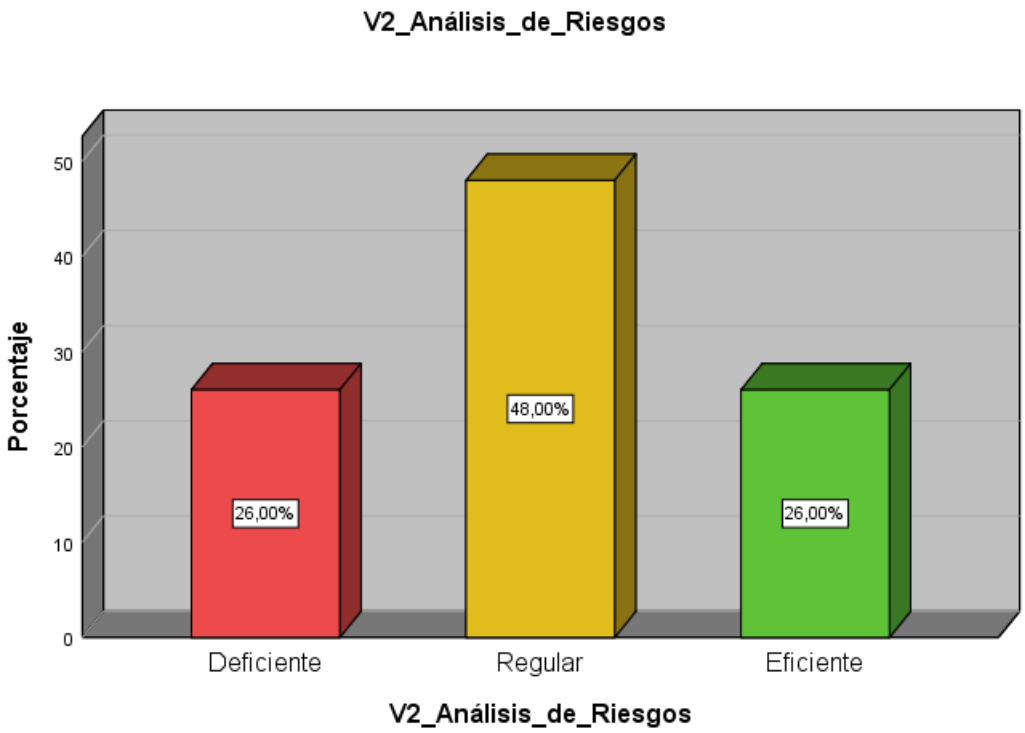
A continuación, en tabla número 14 y figura número 11, una muestra en 50 participantes para variable dos, aplicado a su dimensión 1 “Identificación de Riesgos”, que el 13% considera deficiente, el 24% considera regular y el 13% considera es eficiente.

Tabla 14: Análisis de Frecuencia V2 Dimensión 2: *Análisis* de Riesgos

Nivel	Rango	Frecuencia	%	% válido	% acumulado
Deficiente	[5 - 13]	13	26,0	26,0	26,0
Regular	[14 - 22]	24	48,0	48,0	74,0
Eficiente	[23 - 30]	13	26,0	26,0	100,0
Suma:		50	100,0	100,0	

Fuente: Propia, SPSS v25

Figura 11: Esquema de Barras V2 Dimensión 2: Análisis de Riesgos



Elaboración: SPSS.

Variable 3 - Dimensión 1: Evaluación de Riesgo

Interpretación:

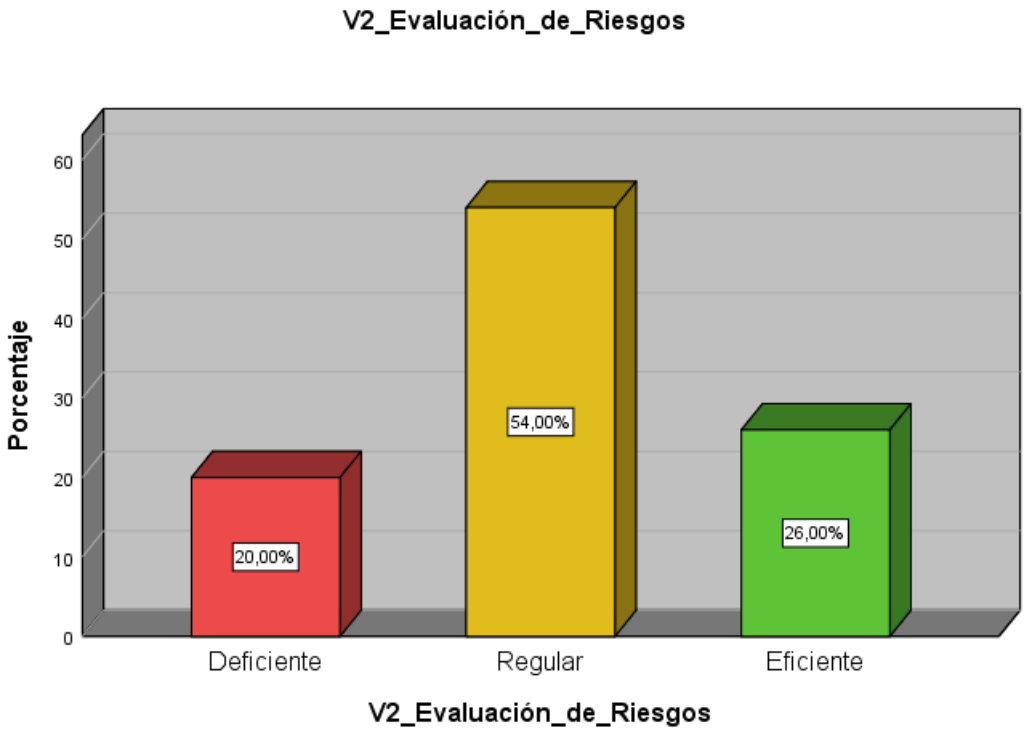
A continuación, en tabla número 15 y figura número 12, una muestra en 50 participantes para la variable dos aplicado a su dimensión 1 “Identificación de Riesgos”, que el 10% considera deficiente, el 27% considera regular y el 13% considera es eficiente.

Tabla 15: Análisis de Frecuencia V2 Dimensión 3: *Evaluació*n de Riesgos

Nivel	Rango	Frecuencia	%	% útil	% final
Deficiente	[5 - 13]	10	20	20	20
Regular	[14 - 22]	27	54	54	74
Eficiente	[23 - 30]	13	26	26	100
Suma:		50	100%	100%	

Elaboración: Propia, SPSS.

Figura 12: Esquema de Barras V2 Dimensión 3: Evaluación de Riesgos



Elaboración: Desde SPSS.

Tabla Cruzada Variable Independiente V1 - Dependiente V2

Interpretación:

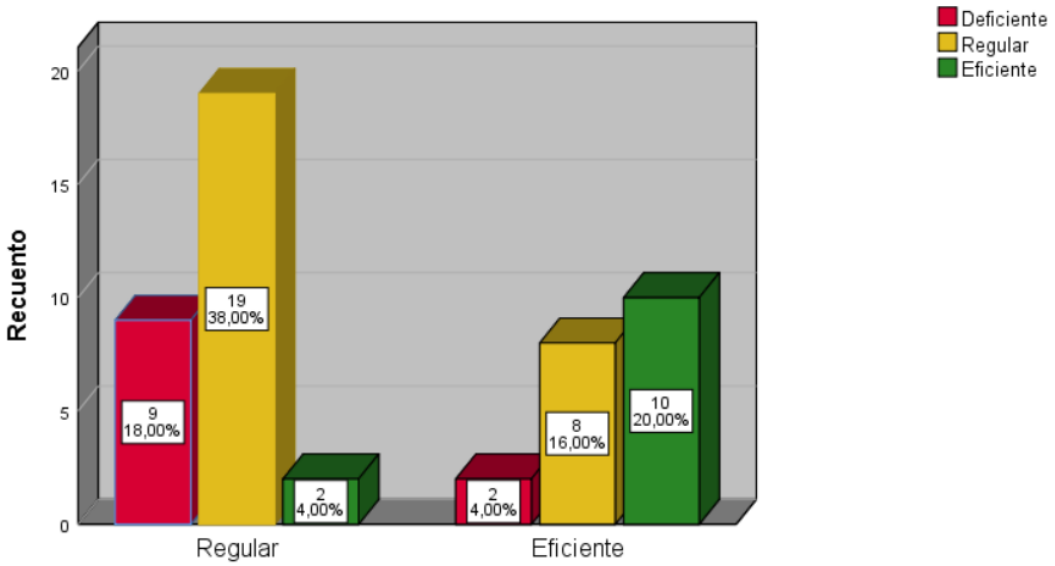
A continuación, información de tabla número 16 y figura número 13, una muestra en 50 participantes con información cruzada sobre conocimiento en las 2 variables, considera 20% eficiente, el 38% considera regular y el 18% considera es deficiente.

Tabla 16: Tabla Cruzada Independiente V1 - Dependiente V2

			V2			
			Deficiente	Regular	Eficiente	Total
V1	Regular		9	19	2	30
		% del total	18%	38%	4%	60%
	Eficiente		2	8	10	20
		% del total	4%	16%	20%	40%
Suma:			11	27	12	50
		% del total	22%	54%	24%	100%

Fuente: Propia, SPSS v25

Figura 13: Esquema de Barras V1 - V2



Fuente: SPSS.

4.2. Resultado Inferencial

4.2.1. Test de Distribución

Se aplicó test utilizando prueba como Kolmogorov-Smirnov (K-S), pues según esta normalidad, la clasificación es superior a 30 y los resultados se derivan de los datos estadísticos ingresados en el software SPSS versión 25.

Hipótesis:

- H0: Aplica distribución normal p-val.> 0,05
- Ha: No aplica distribución normal.

Significancia del p-val.= 0,05 (5%) con 95% de nivel confianza.

Tabla 17: Prueba de normalidad K-S

(K-S)

Variables	Estadístico	gl	Sig.
Seguridad de la Información	,089	50	,200
Gestión de Seguridad Electrónica	,107	50	,200

Fuente: Propia, SPSS v25.

Reglas de decisión:

- N1: Cuando p ≤ 0,05, rechazaremos hipótesis nulo (H0) aceptando Ha (como resultado la información normalmente no se distribuyen, aplicaremos pruebas no paramétricas).
- N2: Cuando p > 0,05, aceptaremos H0, y rechazaremos la Ha (como resultado normalmente se distribuyen, aplicaremos pruebas paramétricas).

Interpretación:

La Tabla 17 muestra que la información estadística del valor p-val. (0.2) es mayor a 0.05, por lo que aceptaremos la regla N2, y aplicaremos Pearson.

4.2.2. Test de Contrastación

A continuación, utilizaremos nuestra prueba R de Pearson ante la validación de (K.S), resultó p (0.2) > alfa (0.05) para ambas variables.

Prueba Hipótesis general:

- Hi: Hipótesis general planteada.
- H0: Negación en la hipótesis general planteada.

Reglas de decisión:

- Cuando p-val ≤ 0,05, rechazaremos hipótesis nulo y aceptamos hipótesis que se investiga.
- Cuando p-val. > 0,05, aprobamos hipótesis nulo, y negamos la Hi,.

Tabla 18: Resultado en Hipótesis – R de Pearson - V1 y V2

			V1	V2
R de Pearson	V1		1	,537
		Sig. (bil.)		,000
		N.	50	50
	V2		,537	1
		Sig. (bil.)	,000	
		N.	50	50

Elaboración: Propio, SPSS v25.

Interpretación:

Según la tabla anterior, cuyo resultado p-val.=0.0 < 0.05, con ello rechazamos la H0, aceptaremos la Hi, validando el vínculo entre las variables de correlación igual a 0,537, con una escala sólida.

Tabla 19: Valores R de Pearson

Rango	Significado Correlación
0.00 <= X < 0.1	Nulo
0.1 <= X < 0.3	Frágil
0.3 <= X < 0.5	Moderado
0.5 <= X < 1	Sólido

Fuente: Propio.

Prueba en primera hipótesis específica:

- Hi: HE uno de la investigación.
- H0: Negación de Hi

Reglas para decisión:

- Cuando p ≤ 0,05, rechazaremos hipótesis nulo y aceptamos hipótesis que se investiga.
- Cuando p > 0,05, aprobamos hipótesis nulo, y negamos la hipótesis que se investiga.

Tabla 20: Prueba de Hipótesis especifica 1

			Confidencialidad	V2
R de Pearson	Confidencialidad		1	,553
		Sig. (bilateral)		,000
		N	50	50
	V2		,553	1
		Sig. (bilateral)	,000	
		N	50	50

Fuente: Propia, SPSS v25.

Interpretación:

Se observa los resultados de tabla número 20, identificando la correlación de (0,553), confirmando una relación sólida de la dimensión confidencialidad con variable dependiente de significancia p=0,000. Por lo tanto, se puede concluir que negaremos hipótesis nulo y aceptaremos hipótesis que se investiga.

Prueba en segunda hipótesis específica:

- Hi: HE dos de la investigación.
- H0: Negación de Hi

Reglas para decisión:

- Cuando p ≤ 0,05, rechazaremos hipótesis nulo y aceptamos hipótesis que se investiga.
- Cuando p > 0,05, aprobamos hipótesis nulo, y negamos la hipótesis que se investiga.

Tabla 21: Prueba de Hipótesis especifica 2

			Integridad	V2
R de Pearson	Integridad		1	,322
		Sig. (bil.)		,023
		N.	50	50
	V2		,322	1
		Sig. (bil.)	,023	
		N.	50	50

Fuente: Propia, SPSS v25.

Interpretación:

Se observa los resultados de tabla número 21, identificando la correlación de (0,322), confirmando una relación moderada de la dimensión integridad con variable dependiente de significancia p=0,023. Por lo tanto, se puede concluir que negaremos hipótesis nulo y aceptaremos hipótesis que se investiga.

Prueba en tercera hipótesis específica:

- Hi: HE tres de la investigación.
- H0: Negación de Hi

Reglas para decisión:

- Cuando p ≤ 0,05, rechazaremos hipótesis nulo y aceptamos hipótesis que se investiga.
- Cuando p > 0,05, aprobamos hipótesis nulo, y negamos la hipótesis que se investiga.

Tabla 22: Prueba de Hipótesis especifica 3

			Disponibilidad	V2
R de Pearson	Disponibilidad		1	,427
		Sig. (bilateral)		,002
		N	50	50
	V2		,427	1
		Sig. (bilateral)	,002	
		N	50	50

Fuente: Propia, SPSS v25.

Interpretación:

Se observa los resultados de tabla número 22, identificando la correlación de (0,477),con ello se confirma que hay correlación afirmativa entre la dimensión disponibilidad con la variable dependiente, con un valor de significancia p=0,002. Por lo tanto, se puede concluir que negaremos hipótesis nulo y aceptaremos hipótesis que se investiga.

V. DISCUSIÓN

Referente a la discusión, este estudio se desarrolló cuantitativamente en lo que refiere a su enfoque, siendo no experimental en su diseño y transversal, se aplicó como básica, asociado con variables en medición, mismas aplicaron una población y muestra de 50 participantes, con estadístico de Kolmogorov - Smirnov con valor de significancia del 0,200 siguiendo una distribución normal ya que es mayor al alfa, se aplica para la contratación de hipótesis, la correlación R de Pearson a la hipótesis general que fue motivo del estudio para una empresa en servicios aéreos, con una correlación de R de Pearson con resultado 0,537, confirmando vínculo existente para V1 y V2, así como valor significancia 0,000.

Presentando similitud con Calderón (2019), cuya problemática enfocada en seguridad de información para los trabajadores de una institución estatal con el fin de mejorar los procesos internos y resguardar la información minimizando riesgos, para ello en su investigación cuantitativa, con diseño no experimental, y es básica, aplicando muestra de 83 miembros, empleando el instrumento cuestionario con 18 ítems para cada variable recopiló información validando que existe varias relaciones similares en seguridad de información así como gestión en riesgos, logrando resultados estadísticos contrastando su hipótesis en correlacionado con Spearman con significancia resultó 0,886 con p-val. de 0,000 que es inferior sobre la confianza y afirmando que hay un grado alto de relación entre sus variables.

Del mismo modo tiene un parecido con Pizarro (2022) cuya problemática enfocada a la variable de gestión de riesgos en una institución del estado buscaba vínculo para la seguridad de información buscando reducir vulnerabilidades en sus procesos y demostró con su trabajo cuantitativo, con diseño no experimental, y es básica, aplicando muestra de 80 colaboradores, empleando el instrumento cuestionario con 19 ítems para su variable en gestión de riesgos y 24 ítems de preguntas en seguridad de la información, que existe relación en su modelos de estudio que fueron aplicados para una entidad pública, porque logró resultados estadísticos contrastando su hipótesis aplicando el coeficiente de Nagelkerke cuya significancia bilateral fue de 0,477 y un el p-valor es menor a 0,000, que es menor

al nivel de confianza, afirmando que hay un grado alto de relación entre sus variables.

Es proporcional con los resultados de las frecuentas por las variables en seguridad de la información, considera que el 0% es deficiente, el 60% considera regular y el 40% considera eficiente. Y tiene mucho en común con los resultados finales de Calderón (2019), evidenciando el análisis de seguridad en información versus los riesgos de una gestión en una institución educativa y el 43.37% considera que tiene nivel bueno el 53.01% considera de nivel regular y solamente el 3,61% considera tener un nivel malo. Y muestra un patrón similar que Pizarro (2022) en su variable seguridad de la información arrojó un resultado de 52,50% con 42 encuestados consideran el nivel medio, el 33,75% aseguran que el nivel es alto y respecto al 13,75% perciben un nivel bajo.

Referente a la hipótesis específica uno, que fue motivo del estudio para una empresa en servicios aéreos. con una correlación de R de Pearson de 0,553, que confirma la presencia positiva en correlación con la confidencialidad con V2 dependiente, cuyo valor en significancia fue de 0,000.

Y no discrepa con Huayllani (2020), en su trabajo cuya problemática fue en presencia aplicada gestionar seguridad en información así como en conjunto a los riesgos en una institución, mejorando la evaluación, orientación y supervisión de la información sensible y concluyó en su investigación cuantitativa, con diseño no experimental, tipo básica, aplicando 145 colaboradores en su muestra, empleando el instrumento cuestionario con 34 ítems para su variable sistema de seguridad de la información, así como 14 ítems para para cada variable, validando que hay presencia directa entre la seguridad de información con los riesgos enfocado al Ministerio de Salud, con un análisis de Cronbach de 0,907 y 0,942 respectivamente afirmando su excelente confiabilidad, porque logro resultados estadísticos de Rho de Spearman con niveles significativa en correlación a de las variables de 0,856, así como p-valor igual a 0,000 que es menor al nivel de confianza, afirmando que hay un grado alto de relación en las variables.

Del mismo lado está en equilibrio con Tarillo (2016) en su trabajo cuya problemática fue como influye la gestión en riesgos y la seguridad en activos en una institución en provincia, con el fin de minimizar las incidencias y riesgos por perdida de información y con ello garantizar la confianza al ciudadano por los servicios que presta, concluyendo en su investigación cuantitativa, aplicó no experimentar como diseño, tipo básica, enfocado a 50 colaboradores, empleando el instrumento cuestionario con 31 ítems para su variable gestión de riesgos y 18 ítems para activos de información, confirmando que hay mucha similitud en las variables mencionadas inicialmente y enfocado a una sede registral de Moyobamba, aplicando resultados estadísticos para contrastar la hipótesis con el Chi-cuadrado de Pearson de nivel de correlación significativa para las variables con 15,712 y mayor Chí tabular de 4° de libertad igual a 9,48 , encontrándose en la probabilidad rechazada, con ello se acepta su hipótesis de 95% en confianza y afirmando los fuertes enlaces entre las variables.

Y es uniforme en los resultados de las frecuencias de dimensión 1 - Confidencialidad, considera el 0% deficiente, el 70% considera regular y el 30% considera eficiente, y se parece con los resultados obtenidos por Huayllani (2020), quien obtuvo de sus encuestados de 145 colaboradores para la variante SGSI un 0,7% opina que es deficiente, el 81,4% que es regular y el 17,9% que es deficiente, referente a la gestión de riesgo 1,4% afirma deficiente, un 79,3% que es regular y el 29% afirma que es eficiente. Por ello es uniforme a los resultados obtenidos por Tarillo (2016) considera que el 18% escala baja, el 30% considera escala media y el 52% considera que es alta, los niveles de la gestión en riesgos y activos de información.

Referente con hipótesis específica dos, que fue motivo del estudio para una empresa en servicios aéreos. con una correlación de R de Pearson de 0,322, que confirma la presencia positiva en correlación para la dimensión integridad y la variable dependiente, y valor en significancia de 0,023.

Se equipara con Castro (2022), en su trabajo cuya problemática enfocado con seguridad de información así como riesgos en una institución con sistema electoral mejorando su integridad en la información sensible y que concluyó en su investigación cuantitativa, con diseño experimental, y es básica, aplicando muestra de 45 colaboradores, empleando el instrumento cuestionario para su variable independiente en seguridad de información así como su otra variable en riesgos enfocado a una entidad del sistema electoral, con una prueba en normalidad de Shapiro-Wilk resultando 0,947 y 0,956 respectivamente, validando que se debe aplicar una distribución normal, dando una muestra no paramétrica y porque logro resultados estadísticos para contrastar la hipótesis aplicando la Rho de Spearman resultando una correlación significativa entre las variables igual a 0,924, con p-valor igual 0,000 que es menor al nivel de confianza, afirmando que hay un grado alto de relación en las variables.

Así también es equivalente a Bernaldo (2018), en su trabajo cuya problemática fue en relación en seguridad de información mejorando sus procesos en la Reniec minimizando los riesgos y mejorando la confianza en sus sistemas al momento de realizar trámites de los ciudadanos por ello concluyó en su investigación cuantitativa, con diseño no experimental, y es básica, aplicando muestra de 175 colaboradores, empleando el instrumento cuestionario con 34 ítems para su variable SGSI y 9 ítems para sus servicios en registro civiles, confirman para el estudio que hay vínculo similar entre sus variables de seguridad de información con los riesgos de gestión enfocado al proceso de registros de una institución pública, con un análisis de Cronbach de 0,922 y 0,813 respectivamente afirmando su excelente confiabilidad, porque logro resultados estadísticos para contrastar su hipótesis aplicando la Rho de Spearman resultando correlación significativa entre las variables igual a 0,781 con p-valor similar a 0,000 que es menor al nivel de confianza, afirmando que hay un grado alto de relación para los diseños de sistemas en información enfocados a la seguridad.

Existe una semejanza con los resultados de las frecuencias de dimensión 2 - Integridad, considera que el 2% es deficiente, el 50% considera regular y el 48% considera eficiente, aproximándose a los resultados obtenidos por Castro (2022), obtuvo de una muestra de 45 colaboradores para el caso de integridad el 0% considera malo, el 17,8% que es medio y el 71,1% que es alto. De forma contrapuesta a los resultados obtenidos por Bernaldo (2018), quien obtuvo 175 colaboradores aplicando al SGSI con 72,5% estima bajo, el 26,67% que es medio y el 0.83% que es alto.

Referente a la hipótesis específica tres, que fue motivo del estudio para una empresa en servicios aéreos con una correlación de R de Pearson de 0427, que confirma existencia de vínculo positivo para disponibilidad con su variable dependiente en riesgo, y con significancia de 0,002.

Existiendo una semejanza evidente con Leon (2020), en su trabajo cuya problemática fue relacionado a la seguridad de información y las gestiones en riesgos de una institución electoral identificando y evaluando las amenazas, así como implementar la mitigación de riesgos concluyendo en su investigación cuantitativa, con diseño experimental, y es básica, aplicando muestra de 64 colaboradores, empleando el instrumento cuestionario para su variables de seguridad de información y procesos en riesgos, validando que existe vínculo directo entre sus variables mencionadas enfocados a una entidad del proceso servicio electoral reniec, con un análisis de Cronbach de 0,823 y 0,821 respectivamente afirmando su excelente confiabilidad, con una prueba de normalidad de Shapiro-Wilk de 0,947 y 0,956 respectivamente, validando una distribución normal, dando una muestra no paramétrica y porque logro resultados estadísticos para contrastar su hipótesis aplicando la Rho de Spearman validando una correlación significativa entre las variables con 0,722, de p-valor igual a 0,000 que es menor al nivel de confianza, afirmando que hay un grado alto de relación en las variables.

Y se aproxima con la investigación de Herrera (2017), cuya problemática fue en relación con seguridad en información para una institución controladora estatal, con propósito de mejorar los procesos, normativas digitales en la documentación que se administra con ello concluyó en su investigación cuantitativa, con diseño experimental, y es básica, aplicando muestra de 60 colaboradores, empleando el instrumento cuestionario de 20 ítems para su variable SGSI y 19 ítems en digitalización de documentos, con un análisis de Cronbach de 0,848 y 0,813 respectivamente afirmando su excelente confiabilidad, con una prueba de normalidad para contrastar su hipótesis Rho de Spearman de 1,0 para seguridad de la información y 0,805 digitalización de documentos respectivamente, y un p-valor similar 0,000 que es bajo por el nivel en confianza, confirmando presencia de un vínculo alto en correlación para sus variables.

Por último se compararon con los resultados de las frecuencias de dimensión 3 - Disponibilidad, considera que el 6% es deficiente, el 50% considera regular y el 44% considera eficiente, estos resultados se aproximan con los obtenidos por Leon (2020), obtuvo de una muestra de 64 colaboradores para arrojar que concierne a seguridad de la información, el 6,3% considera baja, 79,7% es regular y el 14,1% considera como alta, en la dimensión disponibilidad el 12,7% es baja, el 65,6% considera regular y el 17,2 como alta. En contraste con los resultados obtenidos por Herrera (2017), obtuvo el 46,7% como deficiente, el 40% considera regular y el 13.3% considera poco eficiente en referencia con seguridad de información.

VI. CONCLUSIONES

Después de los resultados como sustentos estadísticos, concluí lo siguiente:

Primera:
Se determinó la influencia del SGSI para gestionar la seguridad electrónica en el área de TI para empresa de servicios aéreos, ya que se validó la correlación R de Pearson en 0,537, afirmando la existencia de un vínculo o relación afirmativa para variables V1 y V2 y un valor en significancia en 0,000.

Segunda:
Se determinó la influencia del SGSI con la confidencialidad para gestionar la seguridad electrónica en el área de TI para empresa de servicios aéreos, ya que se validó la correlación R de Pearson en 0,553, afirmando la existencia de un vínculo o relación afirmativa entre confidencialidad y V2 con un valor de significancia de 0,000.

Tercera:
Se determinó la influencia del SGSI con la integridad para gestionar la seguridad electrónica en el área de TI para empresa de servicios aéreos, ya que se validó la correlación R de Pearson en 0,322, afirmando la existencia de un vínculo o relación positiva entre integridad y V2 con un valor de significancia de 0,000.

Cuarta:
Se determinó la influencia del SGSI con la disponibilidad para gestionar la seguridad electrónica en el área de TI para empresa de servicios aéreos ya que se validó la correlación R de Pearson en 0,427, afirmando la existencia de un vínculo o relación afirmativa entre disponibilidad y V2 con un valor de significancia de 0,000.

VII. RECOMENDACIONES

Primero:

Se recomienda al responsable de TI, difundir constantemente a los colaboradores la importancia en seguridad y riesgos en la información mediante normativas que se pueden difundir mensualmente, aplicar auditorias y testing externos para un análisis detallado de vulnerabilidades y finalmente mantener capacitado al personal de TI en nuevas tecnologías.

Segunda:

Se recomienda al encargado del área de TI, sensibilizar en las políticas de seguridad, así como identificar los activos de información en cada área a fin de asegurar la confidencialidad y se apliquen los controles a los riesgos, como pruebas de tráfico.

Tercera:

Se recomienda al encargado del área de TI, aplicar y sensibilizar en políticas de accesos a la información, controlar los cambios como actualizaciones del sistema y que no se dupliquen, así como analizar todo tipo de riesgo que afecte la integridad de la información.

Cuarta:

Se recomienda al encargado del área de TI, asegurar el proceso de contingencias y evaluar los riesgos para asegurar la disponibilidad de la información, así mismo reforzar al personal de TI mediante simulacros de caídas o corte de servicios a fin de mejorar los tiempos en la continuidad de los accesos o sistemas.

REFERENCIAS

Aedah, A. R., & Hoga, S. (2020). *Maturity framework analysis ISO 27001: 2013 on indonesian higher education*. International Journal of Engineering & Technology, 9(2), 429-436.

Aguilar-Antonio, J.-M. (2019). *Hechos ciber físicos: Una propuesta de análisis para ciber amenazas en las estrategias nacionales de ciberseguridad*. *URVIO. Revista Latinoamericana de Estudios de Seguridad, 4299*(25), 24–40. https://doi.org/10.17141/urvio.25.2019.4007

Akinyemi, I., Schatz, D., & Bashroush, R. (2020). *SWOT analysis of information security management system ISO 27001*. International Journal of Services Operations and Informatics, 10(4), 305-329.

Andrade C. y Chávez, C. (2018). *Generación de un plan para la gestión integral de seguridad de la información basado en el marco de la norma ISO 27001 y las mejores prácticas de seguridad de la norma ISO 27002 para la compañía internacional GYM ECUAINTERGYM S.A. de la ciudad de Guayaquil.* Recuperado de http://repositorio.ug.edu.ec/handle/redug/32606

Arias Quispe, Edwin Samuel (2020). *Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao. 2020.* [Tesis de posgrado; Universidad César Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47276/Arias_QES-SD.pdf?sequence=1

Arias, J. y Covinos, M. (2021). *Diseño y metodología de la investigación.* Enfoques Consulting EIRL. http://hdl.handle.net/20.500.12390/2260

Alenys, C. (2017). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013.* Recuperado de http://repository.poligran.edu.co/handle/10823/994

Benites Durand, C. A. (2019). *Implementación de un sistema de gestión de seguridad de la información-Norma ISO 27001 para la fábrica Radiadores Fortaleza.*

Bernaldo Bastidas, Natividad Gladys (2018). *Sistema de gestión de seguridad de la Información en el Proceso de Registros Civiles de RENIEC. San Borja. Lima 2016.* Recuperado por https://repositorio.ucv.edu.pe/handle/20.500.12692/12657

Caamaño, E., & Gil, R. (2020). *Prevención de riesgos por ciberseguridad desde la auditoría forense: Conjugando el talento humano organizacional*. *Novum, 1*(10), 20. https://revistas.unal.edu.co/index.php/novum/article/view/84210/73652

Calderón Sanchez, Jorge Armando (2019), *Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018.* Recuperado de https://repositorio.ucv.edu.pe/handle/20.500.12692/30014

Carvalho, C. y Marques, E. (2019). Adapting ISO 27001 to a Public Institution. 14th Iberian Conference on Information Systems and Technologies. Portugal. https://bit.ly/3iAiPrE

Castro Rios, Henry (2022). *Seguridad de la Información y Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021.* Recuperado por https://repositorio.ucv.edu.pe/handle/20.500.12692/77870

Corda, M. C., Viñas, M., & Coria, M. K. (2017). *Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje*. Palabra clave, 7(1), 00-00.

Córdova, J. (2021). *Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales*

en el departamento de sistemas de una institución universitaria en Colombia. [Tesis doctoral no publicada]. Universidad Peruana Unión.

Crespo, E. (2017). Ecu@Risk, *una metodología para la gestión de riesgo aplicada a las MPYMES.* Enfoque UTE, 8(1), 107–121. https://doi.org/10.29019/enfoqueute.v8n1.140

Dau Janne, J. L., & Contreras Pérez, D. S. (2022) - *Planificación del Sistema de gestión de seguridad de la información (SGSI) de la empresa International Protection.*

Fathurohman, A., & Witjaksono, R. W. (2020). *Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City).* Bulletin of Computer Science and Electrical Engineering, 1(1), 1-11.

Gabriel-Ortega, J. (2017). *Cómo se genera una investigación científica que luego sea motivo de publicación.* Recuperado el 6 de octubre de 2020, a partir de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2072-92942017000200008

García, C. (2018). *Implementación y certificación del SGC bajo la norma ISO 9001:2015 de las áreas de Talleres y Laboratorios y Centro de Documentación y Fondo Editorial de la UC.* Disponible en https://scholar.google.es/scholar?start=10&q=Garc%C3%ADa+2018+iso&hl=es&as_sdt=0,5#d=gs_qabs&t=1673056745757&u=%23p%3D588595z6SX0J

Gil, V., & Gil, J. (2017). *Seguridad informática organizacional: Un modelo de simulación basado en dinámica de sistemas. Scientia et Technica* Año XXII, *22*(2). https://www.redalyc.org/pdf/849/84953103011.pdf

Haris Lukman (2018). *Risk Assessment on Information Asset an academic Application Using ISO 27001.* In 2018 6th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-4). IEEE.

Hernández Sampieri, R., Fernández Collado, C., Baptista Lucio, M. del P., Méndez Valencia, S., y Mendoza Torres, C. P. (2014). *Metodología de la Investigación*. Recuperado el 6 de octubre de 2020, a partir de https://www.uca.ac.cr/wpcontent/uploads/2017/10/Investigacion.pdf

Hernández Sampieri, R., & Mendoza, C. (2018). *La investigación. Las rutas cuantitativa, cualitativa y mixta.* Revista Universitaria Digital de Ciencias Sociales. Retrieved from https://virtual.cuautitlan.unam.mx/rudics/?p=2612

Herrera Castellanos, Erick Vladimir (2017). *Digitalización de documentos y seguridad de la información en la Contraloría General de la República - Lima 2016.* Recuperado por https://repositorio.ucv.edu.pe/handle/20.500.12692/22141

Huacasi Huacasi, J. R. (2018). *Implementación de un sistema de gestión de seguridad de la información aplicando la ntp iso/iec 27001 para mejorar el proceso de seguridad de información en el ejército del perú.*

Huayllani Muñoz, Oscar Yonatan (2020). *Sistema de gestión de seguridad de la información y la gestión riesgo en el Ministerio de Salud, 2019.* Recuperado de https://repositorio.ucv.edu.pe/handle/20.500.12692/97613

Huerta Agurto, C. A. (2020). *Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, 2019.*

Humphreys, E. (2016). *Implementing the ISO/IEC 27001 ISMS Standard. Second* Edition. Artech House. Boston-Londres.

INCIBE. (2019). *Protección de la información.* Colección-Protege tu empresa, 6. Retrieved from https://www.incibe.es/

ISO/IEC 27001:2013 (2013). *Information security management systems.* ISO/IEC — All rights reserved. Retrieved from https://www.iso.org/

ISO/IEC 27005:2018 (2018). *Information technology - Security techniques Information security risk management.* ISO/IEC — All rights reserved. Retrieved from https://www.iso.org/

Izquierdo Cabrera, J. (2021). *Modelo basado en la gestión de seguridad de la información para contribuir en los procesos de las farmacias de los hospitales II-I en la región amazonas.*

Kenyon, B. (2019). *ISO 27001 controls–A guide to implementing and auditing*. IT Governance Ltd.

Kurnianto, A., Isnanto, R., & Widodo, A. P. (2018). *Assessment of information security management system based on ISO/IEC 27001: 2013 on subdirectorate of data center and data recovery center in ministry of internal affairs*. In E3S Web of Conferences (Vol. 31, p. 11013). EDP Sciences.

Ladino A., M. I., Villa S., P. A., & López E., A. M. (2011). *Fundamentos de ISO y su aplicación en las empresas.* Scientia Et Technica, XVII (47), 334-339. https://www.redalyc.org/articulo.oa?id=84921327061

Laudon, K. y Laudon, J. (2016). *Sistemas de información gerencial.* México: Pearson Educación.

Leon Alvarado, Luis Enrique (2020). *Seguridad de la información y gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020.* Recuperado por https://repositorio.ucv.edu.pe/handle/20.500.12692/49738

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). *Implementation of ISO 27001 standards as GDPR compliance facilitator.* Journal of information systems engineering & management, 4(2), 1-8.

López Ramírez Marxela, 2018. *Análisis de riesgos en un sistema de gestión de seguridad informática (SGSI) con metodologías complementarias.* http://repository.unipiloto.edu.co/handle/20.500.12277/2913

Lopez Aguirre, Jasser Ely (2022), *Implementación del sgsi, basado en la iso/iec 27001 para dar tratamiento al riesgo en una empresa constructora*

Lukitowati, R., & Ramli, K. (2020). *Assessing the Information Security Awareness of Employees in PT ABC Against International Organization for Standardization (ISO) 27001: 2013*. Journal of Computational and Theoretical Nanoscience, 17(2-3), 1441-1446.

Martínez, F. (2020). *Ciberseguridad y Estado autonómico.* ICADE. Revista de la Facultad de Derecho, 109, 1–19. https://doi.org/https://doi.org/10.14422/icade.i109.y2020.001

Mariño, S. y Alfonzo, P. (2019). *Evidencias de Accesibilidad Web en la generación de sitios: Propuesta de un método.* Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología, (23), 52-60. Recuperado de https://bit.ly/38mnnMs

Masso Daza, J. E. (2020). *Risk management in the software life cycle: A systematic literature review. Computer Standards & Interfaces*, 10. Retrieved from https://www.researchgate.net/publication/339747572_Risk_management_in_the_software_life_cycle_A_systematic_literature_review

Mero García, A. F. (2016). *Implantación de un sistema de gestión de seguridad de información (SGSI) en el distrito de salud 13d04 24 de mayo–Santa Ana–Olmedo–salud de la provincia de Manabí* (Master's thesis, PUCE).

Mendez Navarro, M. L. (2022). *Diseño de un sistema de gestión de seguridad de información para proteger los activos de información del Servicio de Administración Tributaria de la zona norte del Perú.*

Mejía, B. (2020*). Implementación de los controles de la ISO/IEC 27002: 2013 para la gestión de la base de datos de los registros públicos de la Zona VII – Sede Huaraz, 2019.* [Tesis de maestría, Universidad Peruana de Ciencias e Informática]. http://repositorio.upci.edu.pe/handle/upci/151

Miguel, P. (2015). *Seguridad en los sistemas informáticos.* España: RA-MA

Monev, V. (2020, September). *Organisational information security maturity assessment based on ISO 27001 and ISO 27002*. In 2020 International Conference on Information Technologies (InfoTech) (pp. 1-5). IEEE.

Penagos Granada, E. F., López Echeverry, A. M., & Villa Sánchez, P. A. (2016). *Law on Transparency implementation process, ISO 27001 and Database Reporting on public entities.* Sistemas & Telemática, 14(39),41-56. [fecha de Consulta 22 de Abril de 2023]. ISSN: 1692-5238. Recuperado de: https://www.redalyc.org/articulo.oa?id=411549534005

Pizarro Castro, Ivan Marco Antonio (2022). *Modelo de Gestión de riesgos de TI para la seguridad de la información de una institución del estado, Lima 2022.* Recuperado de https://repositorio.ucv.edu.pe/handle/20.500.12692/97613

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). *Information security and value creation: The performance implications of ISO/IEC 27001*. Computers in Industry, 142, 103744.

Otzen, T., & Manterola, C. (2017). *Técnicas de Muestreo sobre una Población a Estudio.* International Journal of Morphology, 35, 227-232. https://dx.doi.org/10.4067/S0717-95022017000100037

Ramírez Castro, A., & Ortiz Bayona, Z. (2011). *Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios.* Ingeniería, 16(2), 56-66.

Rodriguez Baca, L., Cruzado Puente de la Vega, C., Mejía Corredor, C., & Alarcón Diaz, M. (2020). *Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana.* Propósitos y Representaciones, 8(3), e786. doi: http://dx.doi.org/10.20511/pyr2020.v8n3.786

Roviralta Puente, José Manuel, (2021). *INCIBE. La información, un activo vital para tu empresa* https://www.incibe.es/protege-tu-empresa/blog/informacion-activo-vital-tu-empresa

Ruíz, C. (2002*). Instrumentos de Investigación Educativa: Procedimientos para su Diseño y Validación/Carlos Ruís Bolívar.* Venezuela: CIDEG.

Rukh, L., & Malik, A. A. (2017). *Swiss army knife of software processes generic framework of ISO 27001 and its mapping on resource management*. In 2017 International Conference on Communication Technologies (ComTech) (pp. 12-15). IEEE.

Santana Ormeño, M., & Aspilcueta Loayza, H. (2016). *Prioridades de gestión de tecnologías de información en organizaciones peruanas.* Revista Venezolana De Gerencia, 20(72). https://doi.org/10.37960/revista.v20i72.20926

Solano Méndez, G. E. (2020). *Propuesta mediante la normativa ISO 27001 para la gestión de la seguridad de la información en la empresa Udersol en Costa Rica.* [Proyecto de Graduación de Licenciatura, Universidad Latina de Costa Rica]. Repositorio Institucional de la Universidad Latina de Costa Rica. https://hdl.handle.net/20.500.12411/293

Soriano M. (2014) *Seguridad en redes y seguridad de la información* http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

Sikman, L., Latinović, T., & Paspalj, D. (2019). ISO 27001-Information Systems Security, development, trends, technical and economic challenges. Annals of the Faculty of Engineering Hunedoara, 17(4), 45-48.

Silva, F., Segadas, L. y Kowask, E. (2019). *Gestión de la seguridad de la información.* REDCEDIA. https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI8.pdf

Shojaie, B., Federrath, H. y Saberi, I. (2014). *Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A.* 9th International Conference on Availability, Reliability and Security. Alemania. University of Hamburg. https://bit.ly/391f0IE

Tarrillo Saldaña, Esther Marleni (2016*). Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015.* Recuperado de https://repositorio.ucv.edu.pe/handle/20.500.12692/1286

Torres León, Martin Renzo (2018) *Diseño de un sistema de gestión de la seguridad de la información (SGSI), basada en la norma ISO/IEC 27001:2013, para el proceso de servicio post-venta de un integrador de soluciones en Telecomunicaciones*, https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/624142/Torres_lm.pdf?sequence=12&isAllowed=y

Ticona Bustinza, O. 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.*

Valderrama, S. (2013). Pasos para elaborar proyectos de Investigación Cientifica. Lima:San Marcos.

Ventura-León, J. L., & Caycho-Rodríguez, T. (2017). *El coeficiente Omega: un método alternativo para la estimación de la confiabilidad.* Revista Latinoamericana de Ciencias Sociales, Niñez y Juventud, 15(1), 625-627.

Villadeza Romero, K. L., & Condor Simon, R. D. (2022). *Diseño de un sistema de gestión de seguridad de la información basado en la norma técnica peruana-ISO/IEC 27001: 2014 para la Municipalidad Distrital de Huácar 2022.*

Von, L. (2019). *Teoría general de los sistemas.* Fondo cultura Económico.

Yoseviano, H. F., & Retnowardhani, A. (2018*). The use of ISO/IEC 27001: 2009 to analyze the risk and security of information system assets: case study in xyz, ltd.* In 2018 International Conference on Information Management and Technology (ICIMTech) (pp. 21-26). IEEE.

ANEXOS:

Anexo 1: Matriz de Operacionalización de la Variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	INSTRUMENTO	ITEMS	ESCALA DE MEDICIÓN
Variable Independiente: **SGSI**	Significa mantener confidencialidad, integridad y disponibilidad, todo lo asociado a su procedimiento en toda la organización. Según ISO/IEC 27001:2013.	El marco integra 14 dominios, 34 entidades y 144 protocolos. "Ellos abarcan a toda la organización que podrían comprometer sus procesos informáticos." A los efectos de este documento, la medición se refiere al estado actual del cumplimiento del SGSI, así como la aplicación de la custodia.	**Confidencialidad**	Políticas de seguridad de la información. Clasificación de activos de información.	Cuestionario	1-2 3-6	(1) Nunca (2) Casi nunca (3) A veces (4) Casi siempre (5) Siempre
			Integridad	Protección de credenciales. Incidentes de manipulación de datos.	Cuestionario	7-8 9-12	
			Disponibilidad	Tiempo respuesta. Respaldo de información.	Cuestionario	13-14 15-18	
Variable Dependiente: **Gestión de Seguridad Electrónica**	Grupo de planteamientos para analizar posibles sucesos, así como pueden ser el efecto antes de decidir qué hacer y cuándo, reducir el riesgo. Además, puede referirse a un grupo de la organización. Según ISO/IEC 27005:2018.	Está determinada por una calificación derivada de un cuestionario que mide su impacto en una segunda variable de prueba usando ítems con rangos de respuesta tipo Likert bajo, medio y alto. Necesita el emplear un cuestionario, así como los resultados se aplican a SPSS versión 25.	**Identificación de riesgo**	Conocimiento de controles Conocimiento de riesgos	Cuestionario	1-3 3-6	
			Analisis de riesgos	Identificación de riesgos Monitoreo de riesgos	Cuestionario	7-8 9-12	
			Evaluación de riesgo	Aplicación y seguimiento Efectividad en los controles y niveles de riesgos	Cuestionario	13-14 15-18	

Anexo 2: Ficha Técnica con firma – Juicio de Expertos

RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- **Primera dimensión**: Confidencialidad.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Políticas de seguridad de la información.	1	4	4	4	
	2	4	4	4	
Clasificación de activos de información.	3	4	4	4	
	4	4	4	4	
	5	4	4	4	
	6	4	4	4	

- **Segunda dimensión**: Integridad.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Protección de credenciales	7	4	4	4	
	8	4	4	4	
Incidentes de manipulación de datos.	9	4	4	4	
	10	4	4	4	
	11	4	4	4	
	12	4	4	4	

- **Tercera dimensión**: Disponibilidad.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Tiempo respuesta.	13	4	4	4	
	14	4	4	4	
Respaldo de información.	15	4	4	4	
	16	4	4	4	
	17	4	4	4	
	18	4	4	4	

observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA.

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Acuña Benites, Marlon Frank.

Especialidad del validador: Metodólogos. **29 de mayo del 2023**

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Firma del Experto validador

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2 hasta 20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- **Primera dimensión**: Identificación de riesgos.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Conocimiento de controles	1	4	4	4	
Conocimiento de riesgos	2	4	4	4	

- **Segunda dimensión**: Análisis de riesgos.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Identificación de riesgos	1	4	4	4	
Monitoreo de riesgos	2	4	4	4	

- **Tercera dimensión**: Evaluación de riesgos.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Aplicación y seguimiento	1	4	4	4	
Efectividad en los controles y niveles de riesgos	2	4	4	4	

observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA.

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Acuña Benites, Marlon Frank.

Especialidad del validador: Metodólogos. **29 de mayo del 2023**

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Firma del Experto validador

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

decir debe ser incluido.	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- **Primera dimensión**: Confidencialidad.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Políticas de seguridad de la información.	1	4	4	4	
	2	4	4	4	
Clasificación de activos de información.	3	4	4	4	
	4	4	4	4	
	5	4	4	4	
	6	4	4	4	

- **Segunda dimensión**: Integridad.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Protección de credenciales	7	4	4	4	
	8	4	4	4	
Incidentes de manipulación de datos.	9	4	4	4	
	10	4	4	4	
	11	4	4	4	
	12	4	4	4	

- **Tercera dimensión**: Disponibilidad.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Tiempo respuesta.	13	4	4	4	
	14	4	4	4	
Respaldo de información.	15	4	4	4	
	16	4	4	4	
	17	4	4	4	
	18	4	4	4	

observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA.

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Sernaque Pacheco Juan Carlos.

Especialidad del validador: Ciencias / Seguridad / Salud Ocupacional Internacional.

29 de mayo del 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

Firma del Experto validador

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1003), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- **Primera dimensión**: Identificación de riesgos.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Conocimiento de controles	1	4	4	4	
Conocimiento de riesgos	2	4	4	4	

- **Segunda dimensión**: Análisis de riesgos.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Identificación de riesgos	1	4	4	4	
Monitoreo de riesgos	2	4	4	4	

- **Tercera dimensión**: Evaluación de riesgos.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Aplicación y seguimiento	1	4	4	4	
Efectividad en los controles y niveles de riesgos	2	4	4	4	

observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA.

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Sernaque Pacheco Juan Carlos.

Especialidad del validador: Ciencias / Seguridad / Salud Ocupacional Internacional.

29 de mayo del 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

Firma del Experto validador

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- **Primera dimensión**: Confidencialidad.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Políticas de seguridad de la información.	1	4	4	4	
	2	4	4	4	
Clasificación de activos de información.	3	4	4	4	
	4	4	4	4	
	5	4	4	4	
	6	4	4	4	

- **Segunda dimensión**: Integridad.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Protección de credenciales	7	4	4	4	
	8	4	4	4	
Incidentes de manipulación de datos.	9	4	4	4	
	10	4	4	4	
	11	4	4	4	
	12	4	4	4	

- **Tercera dimensión**: Disponibilidad.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Tiempo respuesta.	13	4	4	4	
	14	4	4	4	
Respaldo de información.	15	4	4	4	
	16	4	4	4	
	17	4	4	4	
	18	4	4	4	

observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA.

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Vega Mere Guillermo Fidel

Especialidad del validador: Ciencias Naviera, Portuaria y Comercial

29 de mayo del

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

Firma del Experto validador

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

decir debe ser incluido.	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- **Primera dimensión**: Identificación de riesgos.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Conocimiento de controles	1	4	4	4	
Conocimiento de riesgos	2	4	4	4	

- **Segunda dimensión**: Análisis de riesgos.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Identificación de riesgos	1	4	4	4	
Monitoreo de riesgos	2	4	4	4	

- **Tercera dimensión**: Evaluación de riesgos.
- Objetivos de la Dimensión: Medir el conocimiento e impresión.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Aplicación y seguimiento	1	4	4	4	
Efectividad en los controles y niveles de riesgos	2	4	4	4	

observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA.

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Vega Mere Guillermo Fidel

Especialidad del validador: Ciencias Naviera, Portuaria y Comercial

29 de mayo del 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

Firma del Experto validador

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

Anexo 3: Instrumentos para la Recolección de Datos

Encuesta 01:

Variable 1: SGSI

Autor: *Pizarro (2022) y Calderón (2019) adaptado para la investigación.*

Instrucciones:

Por favor marque con una "X" su nivel de acuerdo o desacuerdo respecto a los enunciados que se plantean en la siguiente encuesta. La encuesta es anónima.

Niveles de la escala:

Nunca; (2) Casi nunca; (3) Algunas veces; (4) Casi siempre; (5) Siempre

N°		1	2	3	4	5
Ítems	**Dimensión 1: Confidencialidad**					
1	¿Se cuenta o conoce de políticas que administre y controle los accesos a la información?					
2	¿Se realizan capacitaciones o difunden boletines por correo electrónico sobre seguridad de la información?					
3	¿Cuenta con alguna capacitación acerca de la clasificación de los activos de información?					
4	¿Usted protege o resguarda la información en medio seguros como el drive corporativo?					
5	¿Valida la información que desea compartir sea con las personas autorizadas?					
6	¿Se cuenta con tecnología de autenticación de usuario? (biometría)					
Ítems	**Dimensión 2: Integridad**					
7	¿Realiza el bloqueo de su sesión de usuario al retirarse de su ubicación?					
8	¿Realiza el cambio continuo de contraseña?					
9	¿La información física que maneja esta resguardada en lugar seguro y bajo llave?					
10	¿Tiene conocimiento si el antivirus de su equipo es actualizado?					
11	¿Se cuenta o conoce de medidas de contingencia ante un corte eléctrico? (grupo electrógeno)					
12	¿Se difunden boletines acerca de ataques informáticos?					
Ítems	**Dimensión 2: Disponibilidad**					
13	¿La información que requiere, siempre está disponible?					
14	¿Es eficiente y rápido el sistema?					
15	¿El tiempo de restablecimiento del sistema ante un corte de servicio es rápido?					
16	¿Cuándo ha necesitado recuperar información borrada por error, el área de TI logró salvar la información o brindar una copia?					
17	¿Se cuenta en todo momento con el acceso a la información que necesita para realizar sus labores?					
18	¿La página web de la empresa se encuentra activa en todo momento?					

Encuesta 01:

Variable 1: SGSI

Autor: *Pizarro (2022) y Calderón (2019) adaptado para la investigación.*

Instrucciones:

Por favor marque con una "X" su nivel de acuerdo o desacuerdo respecto a los enunciados que se plantean en la siguiente encuesta. La encuesta es anónima.

Niveles de la escala:

(1) Nunca; (2) Casi nunca; (3) Algunas veces; (4) Casi siempre; (5) Siempre

N°		1	2	3	4	5
Ítems	**Dimensión 1: Confidencialidad**					
1	¿Se cuenta o conoce de políticas que administre y controle los accesos a la información?			X		
2	¿Se realizan capacitaciones o difunden boletines por correo electrónico sobre seguridad de la información?				X	
3	¿Cuenta con alguna capacitación acerca de la clasificación de los activos de información?			X		
4	¿Usted protege o resguarda la información en medio seguros como el drive corporativo?				X	
5	¿Valida la información que desea compartir sea con las personas autorizadas?				X	
6	¿Se cuenta con tecnología de autenticación de usuario? (biometría)				X	
Ítems	**Dimensión 2: Integridad**					
7	¿Realiza el bloqueo de su sesión de usuario al retirarse de su ubicación?					X
8	¿Realiza el cambio continuo de contraseña?					X
9	¿La información física que maneja esta resguardada en lugar seguro y bajo llave?					X
10	¿Tiene conocimiento si el antivirus de su equipo es actualizado?		X			
11	¿Se cuenta o conoce de medidas de contingencia ante un corte eléctrico? (grupo electrógeno)		X			
12	¿Se difunden boletines acerca de ataques informáticos?		X			
Ítems	**Dimensión 2: Disponibilidad**					
13	¿La información que requiere, siempre está disponible?					X
14	¿Es eficiente y rápido el sistema?					X
15	¿El tiempo de restablecimiento del sistema ante un corte de servicio es rápido?					X
16	¿Cuándo ha necesitado recuperar información borrada por error, el área de TI logró salvar la información o brindar una copia?				X	
17	¿Se cuenta en todo momento con el acceso a la información que necesita para realizar sus labores?				X	
18	¿La página web de la empresa se encuentra activa en todo momento?					X

Encuesta 02:

Variable 2: Gestión de Seguridad Electrónica

Autor: *Pizarro (2022) y Calderón (2019) adaptado para la investigación.*

Instrucciones:

Por favor marque con una "X" su nivel de acuerdo o desacuerdo respecto a los enunciados que se plantean en la siguiente encuesta. La encuesta es anónima.

Niveles de la escala:

(1) Nunca; (2) Casi nunca; (3) Algunas veces; (4) Casi siempre; (5) Siempre

N°		1	2	3	4	5
Ítems	**Dimensión 1: Identificación de riesgo**					
1	¿Recibió capacitación referente a seguridad de la información?					
2	¿Se implementan capacitaciones sobre la gestión de riesgos en información?					
3	¿Identifica los activos de información críticos o de riesgo?					
4	¿Recomiendan conductas o concientizan en riesgos de la información?					
5	¿Se siente comprometido con la protección de la información crítica que maneja?					
6	¿El personal esta concientizado sobre los riesgos de información?					
Ítems	**Dimensión 2: Análisis de riesgo**					
7	¿Conoce de algún plan de análisis o tratamiento de riesgos para la seguridad de la información?					
8	¿Cuenta o conoce de algún practica de gestión de riesgos?					
9	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?					
10	¿Participó o conoce de la identificación de los riesgos que está expuesta la información en el área que labora?					
11	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?					
12	¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados?					
Ítems	**Dimensión 3: Evaluación de riesgo**					
13	¿Conoce si existen procedimientos o mecanismos tecnológicos que reducen el riesgo?					
14	¿Conoce si el área de TI cuenta con una plataforma virtual en la que actualiza las buenas prácticas de activos de información?					
15	¿Fueron efectivos los controles aplicados a los probables riesgos de información?					
16	¿Se realizan seguimiento a los entornos de seguridad de la información?					
17	¿Cree que la empresa invierte en nuevas tecnologías de información?					
18	¿La empresa renueva los equipos informáticos?					

Encuesta 02:

Variable 2: Gestión de Seguridad Electrónica

Autor: *Pizarro (2022) y Calderón (2019) adaptado para la investigación.*

Instrucciones:

Por favor marque con una "X" su nivel de acuerdo o desacuerdo respecto a los enunciados que se plantean en la siguiente encuesta. La encuesta es anónima.

Niveles de la escala:

(1) Nunca; (2) Casi nunca; (3) Algunas veces; (4) Casi siempre; (5) Siempre

N°		1	2	3	4	5
Ítems	**Dimensión 1: Identificación de riesgo**					
1	¿Recibió capacitación referente a seguridad de la información?	X				
2	¿Se implementan capacitaciones sobre la gestión de riesgos en información?	X				
3	¿Identifica los activos de información críticos o de riesgo?	X				
4	¿Recomiendan conductas o concientizan en riesgos de la información?	X				
5	¿Se siente comprometido con la protección de la información crítica que maneja?					X
6	¿El personal esta concientizado sobre los riesgos de información?				X	
Ítems	**Dimensión 2: Análisis de riesgo**					
7	¿Conoce de algún plan de análisis o tratamiento de riesgos para la seguridad de la información?			X		
8	¿Cuenta o conoce de algún practica de gestión de riesgos?			X		
9	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?					X
10	¿Participó o conoce de la identificación de los riesgos que está expuesta la información en el área que labora?				X	
11	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?			X		
12	¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados?		X			
Ítems	**Dimensión 3: Evaluación de riesgo**					
13	¿Conoce si existen procedimientos o mecanismos tecnológicos que reducen el riesgo?			X		
14	¿Conoce si el área de TI cuenta con una plataforma virtual en la que actualiza las buenas prácticas de activos de información?	X				
15	¿Fueron efectivos los controles aplicados a los probables riesgos de información?		X			
16	¿Se realizan seguimiento a los entornos de seguridad de la información?			X		
17	¿Cree que la empresa invierte en nuevas tecnologías de información?	X				
18	¿La empresa renueva los equipos informáticos?				X	

Anexo 4: Carta de Presentación

UNIVERSIDAD CÉSAR VALLEJO

"Año de la unidad, la paz y el desarrollo"

Lima, 10 de mayo de 2023
Carta P. 0054-2023-UCV-VA-EPG-F01/J

INGENIERO DE SISTEMAS
ARMANDO SUAREZ BERNAOLA
SUB GERENTE DE TI
SERVICIOS AEROPORTUARIOS ANDINOS S.A

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a SANCHEZ RIOS, JEFFERSON; identificado con DNI N° 42722968 y con código de matrícula N° 7002768107; estudiante del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

SGSI en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador SANCHEZ RIOS, JEFFERSON asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

Dra. Helga R. Majo Marrufo
Jefe
Escuela de Posgrado UCV
Filial Lima Campus Los Olivos

saasa
Armando Suárez Bernaola
Sub Gerente de TI

Somos la universidad de los que quieren salir adelante.

ucv.edu.pe

Anexo 5: Carta de Aceptación

saasa
SERVICIOS AEROPORTUARIOS ANDINOS

Lima, 22 de mayo del 2023

CARTA DE AUTORIZACIÓN

Por medio del presente documento el Sub Gerente de TI del área de Tecnología de la Información, autoriza al colaborador, JEFFERSON SANCHEZ RIOS identificado con DNI 42722968, pueda realizar las encuestas necesarias a los colaboradores de la empresa Servicios Aeroportuarios Andinos S.A., salvaguardando la información de los encuestados de forma anónima, los datos obtenidos serán exclusivamente para la elaboración de la Tesis de Maestría que viene desarrollando.

Atentamente,

saasa
Armando Suarez Bernaola
Sub Gerente de TI

Av. Mariscal José De la Mar 1263 Ofic. 604, Urb. Santa Cruz – Miraflores – 15074 – Lima, Perú
Teléfono: +51 13901840

Anexo 6: Aspectos Administrativos

Recursos Humanos

Para el desarrollo humano se necesitó lo mencionado en el cuadro:

Tabla 23: Presupuesto: Recursos Humanos

Ítem	Recurso	Descripción	Inversión
1	Lecturas	Bibliografías	S/ 100
2	Transporte	Movilidad	S/ 50
3	Inversión	Gastos de estudios	S/ 3,000
4	Data	Recolección y procesamiento	S/ 3,000
			S/ 6,150

Fuente: Propia.

Recursos de Hardware

En relación a hardware, se utilizó una laptop, así como una impresora y smartphone:

Tabla 24: Presupuesto: Recursos Hardware

Ítem	Recurso	Descripción	Inversión
1	Equipo	Laptop (Ryzen 7)	S/ 3,000
2	Impresora	Impresora	S/ 500
3	Economato	Tinta y hojas	S/ 500
			S/ 4,000

Fuente: Propia.

Recursos de Software

En relación al software, se consideró utilizar el software SPSS versión 25, así como microsoft project para generar el cronograma.

Tabla 25: Presupuesto: Recursos Software

Ítem	Recurso	Descripción	Inversión
1	Licencias	Project	S/ 100
2	Licencias	Office	S/ 300
3	Licencias	SPSS	S/ 350
4	Antivirus	Uso interno	S/ 80
			S/ 830

Fuente: Propia.

Presupuesto

Finalmente, se realiza en la siguiente tabla se aprecia la suma de todos los recursos anteriores:

Tabla 26: Presupuesto

Sumatoria de recursos	Inversión
Recurso Humano	S/ 6,150
Recurso Hardware	S/ 4,000
Recurso Software	S/ 830
Presupuesto Total	S/ 10,980

Fuente: Propia.

Financiamiento

Fue realizado con la asesoría de la Universidad, en la siguiente tabla se detalle:

Tabla 27: Financiamiento

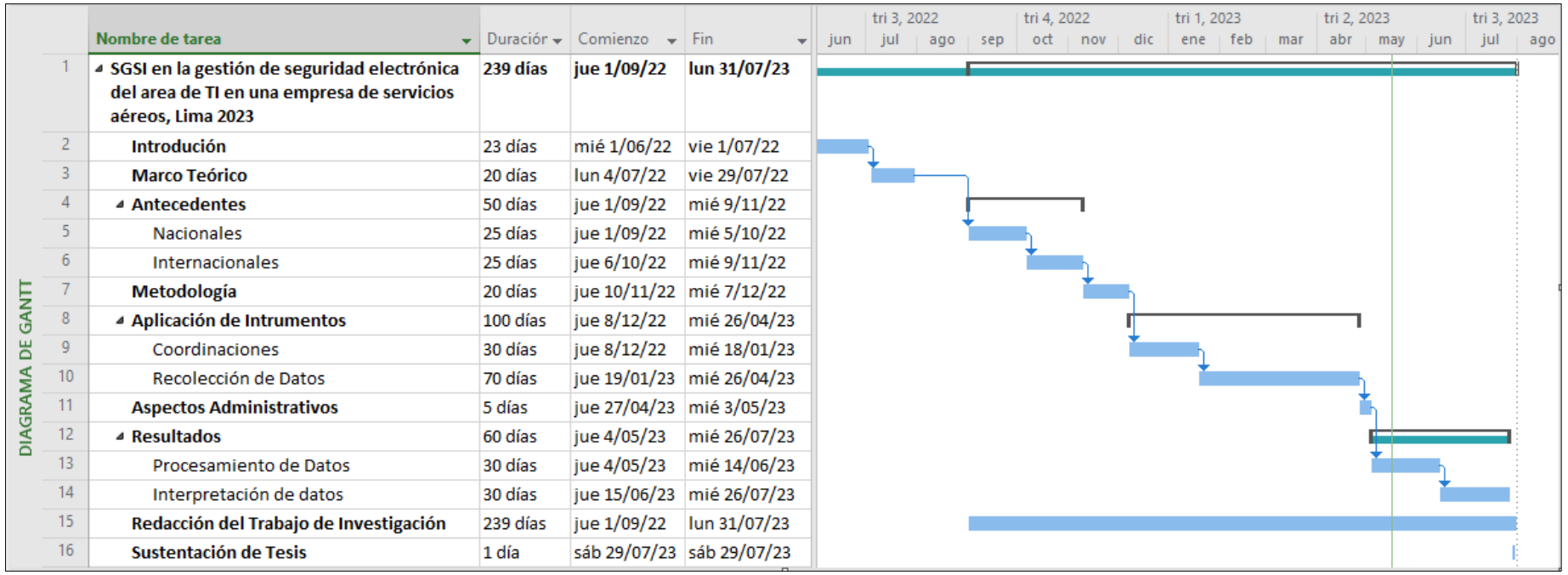
Entidad	Monto	%
Autofinanciado	S/ 10,980	100%

Fuente: Propia.

Cronograma de ejecución

En la siguiente imagen se detallan la estructura con las tareas asignadas.

Figura 14. Cronograma de ejecución



Anexo 7: Fotos de la interfaz del Sistema / Herramienta / Mejoras

1. OBJETIVO

La Gerencia General de SAASA., reconoce como activos estratégicos y vitales a la información y los sistemas que la soportan, por lo que manifiesta su compromiso y determinación en garantizar su protección, asegurando la disponibilidad, confidencialidad e integridad de la misma durante su tratamiento.

El objetivo de la Política de Seguridad de la Información es proporcionar directivas para garantizar la seguridad de información y mejorar la calidad de los servicios ofrecidos a sus clientes.

2. ALCANCE

Esta política abarca a toda la información utilizada para el desarrollo de las actividades y es aplicable a las empresas relacionadas e involucradas en la utilización de la información y los sistemas.

La Política de Seguridad de Información será de aplicación en todas las fases del ciclo de vida de los datos: generación, evaluación, destrucción, almacenamiento, transporte, recuperación, clasificación, análisis, operación, impresión, síntesis y utilización.

3. REFERENCIAS

- Ley 29733 – Ley de Protección de Datos Personales.
- NTP ISO/IEC 27001:2014 - Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.

4. DEFINICIONES

4.1. Custodio:
Gestiona el activo de información por encargo del propietario del activo, de acuerdo con los controles de seguridad definidos por el Responsable de Seguridad de Información. En el concepto de tratamiento se engloban los procesos telemáticos de comunicaciones, almacenamiento y proceso de la información.

4.2. Propietario:
Decide sobre la finalidad, contenido y uso del activo de información. Se responsabiliza del cumplimiento

5. ORGANIZACIÓN Y RESPONSABILIDADES

La función de seguridad de información, es tarea de todos y reside en la Sub Gerencia de Tecnología de la Información, el responsable de seguridad de la información es el Administrador de Seguridad de Información, quien canalizará las directrices y normativas hacia las distintas unidades organizacionales de la empresa.
Los usuarios asumen la responsabilidad de proteger con responsabilidad y de forma congruente con el Código de Conducta y los valores de la empresa, la información interna, de las empresas relacionadas, de sus clientes y de sus proveedores contra los riesgos de destrucción, pérdida, divulgación, malversación, alteración, no disponibilidad y repudio, conforme a los reglamentos internos y/o externos.

Se deberá identificar y asignar las siguientes funciones para los activos de información: Propietario, Custodio, Responsable de Seguridad de Información y Usuario.

Así mismo conforme al artículo 14 de la Ley 29733, la publicación de la presente Política satisface el derecho de información que corresponde a todo titular de datos personales. Al acceder a los servicios (Sociales, sistemas de escritorio y móviles), la presente política se considera aceptada en su totalidad por el Titular de Datos Personales en forma escrita, previa, informada, expresa e inequívoca en los términos en los que lo entiende la Ley 29733, Ley de Protección de Datos Personales y su Reglamento.

SAASA procurará la confidencialidad de los datos personales brindados por el Titular de Datos Personales a través del Servicio y su tratamiento conforme a la legislación vigente sobre protección de datos personales en Perú. Se declara haber adoptado los niveles de seguridad de protección de los datos personales legalmente requeridos, organizativas y legales a su alcance que garanticen la seguridad y eviten la alteración, pérdida, tratamiento o acceso no autorizado a los datos personales.

SAASA procurará el secreto e inviolabilidad de las comunicaciones aplicable a las comunicaciones directas y cualquier otra forma de interacción que el Titular de Datos Personales tenga con el Servicio, así como de los documentos privados que sean proporcionados por o correspondan al usuario. No obstante lo antes mencionado, el usuario debe ser consciente de que las medidas de seguridad en Internet no son

1. OBJETIVO

El objetivo del presente documento es desarrollar un conjunto de reglas básicas que rijan el comportamiento en SAASA con respecto al uso de la información.

Esta normativa define un conjunto de controles de Seguridad de la Información que son de aplicación obligatoria para toda la empresa. Adicionalmente a estos se establece la necesidad de aplicar controles para desarrollar el análisis y gestión de riesgos en los procesos que se indiquen como críticos, con el objetivo de reducir los riesgos mismos a un nivel aceptable para la empresa.

2. ALCANCE

La presente normativa es de aplicación, con carácter obligatorio, en SAASA y aplica también a las empresas relacionadas y entidades colaborativas involucradas en el uso y tratamiento de la información de SAASA .

Esta normativa es de aplicación en todas las fases del ciclo de vida de la información (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción) y de los sistemas que la procesan (análisis, diseño, desarrollo, implantación, explotación y mantenimiento).

El procedimiento **"PRO-INF-01 PROCEDIMIENTO DE SISTEMAS INFORMÁTICOS, CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN"**, define como activos estratégicos la información y los sistemas que la soportan, y manifiesta la determinación que deberá tener la empresa en alcanzar los niveles de seguridad necesarios que garanticen su protección.

3. REFERENCIAS

- NTP ISO/IEC 27001:2014 - Técnicas de seguridad. Sistemas de gestión de Seguridad de la Información. Requisitos.
- Ley 29733 – Ley de Protección de Datos Personales.
- Código de Conducta-SAASA .
- PRO-INF-01 PROCEDIMIENTO DE SISTEMAS INFORMÁTICOS, CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN.
- PRO-INF-XX. Política de Seguridad de la Información

4. DEFINICIONES

saasa SERVICIOS AEROPORTUARIOS ANDINOS	NORMATIVA DE SEGURIDAD DE INFORMACIÓN			
	Fecha: 20.06.23	Versión: 01	Página: 2 de 41	Código: PRO-INF-XX

4.4. Disponibilidad:
La información debe estar disponible en forma organizada para los usuarios autorizados cuando se requiera.

4.5. Evento:
Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

4.6. Evento de Seguridad de Información:
Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la **"PRO-INF-XX. Política de Seguridad de la Información"** o falla en las salvaguardas o una situación previamente desconocida que puede ser relevante para la seguridad.

4.7. Factor de Autenticación:
Información utilizada para verificar la identidad de una persona.

4.8. Incidente de Seguridad de Información:
Evento asociado a una posible falla en la **"PRO-INF-XX. Política de Seguridad de la Información"**, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazan la Seguridad de la Información.

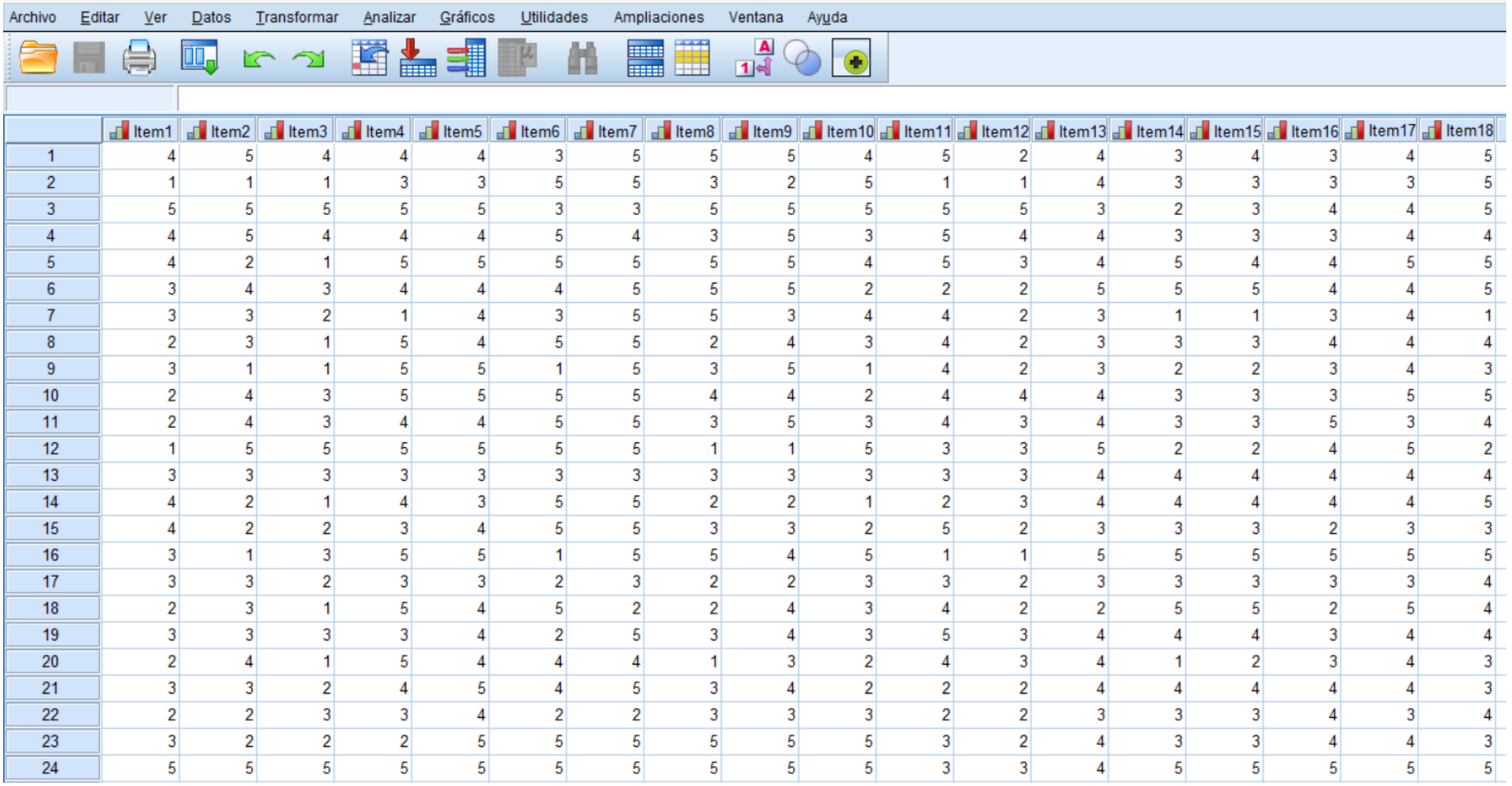
4.9. Información:
Registro físico (Ej. Información en papel) y/o cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

4.10. Integridad:
Preservar la información completa, exacta y válida.

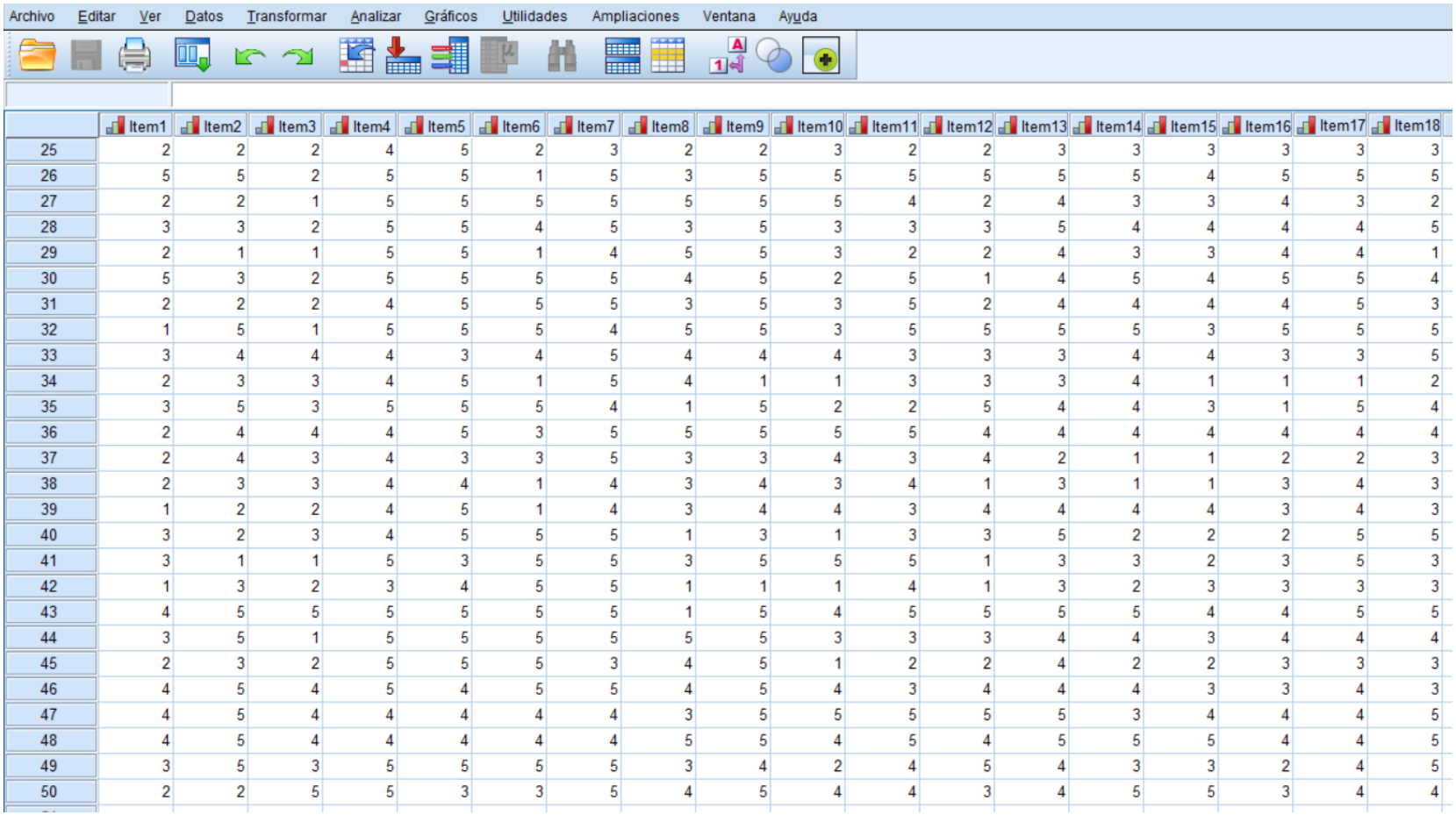
4.11. Monitoreo:
Proceso de medición y evaluación continua del Sistema de Gestión de Seguridad de Información. El monitoreo facilita el proceso de decisión y mejora la performance y la responsabilidad a través de la colección, análisis e informe de datos relevantes del desempeño del SGSI.

Anexo 8: Fotos del SPSS

Variable Independiente: SGSI

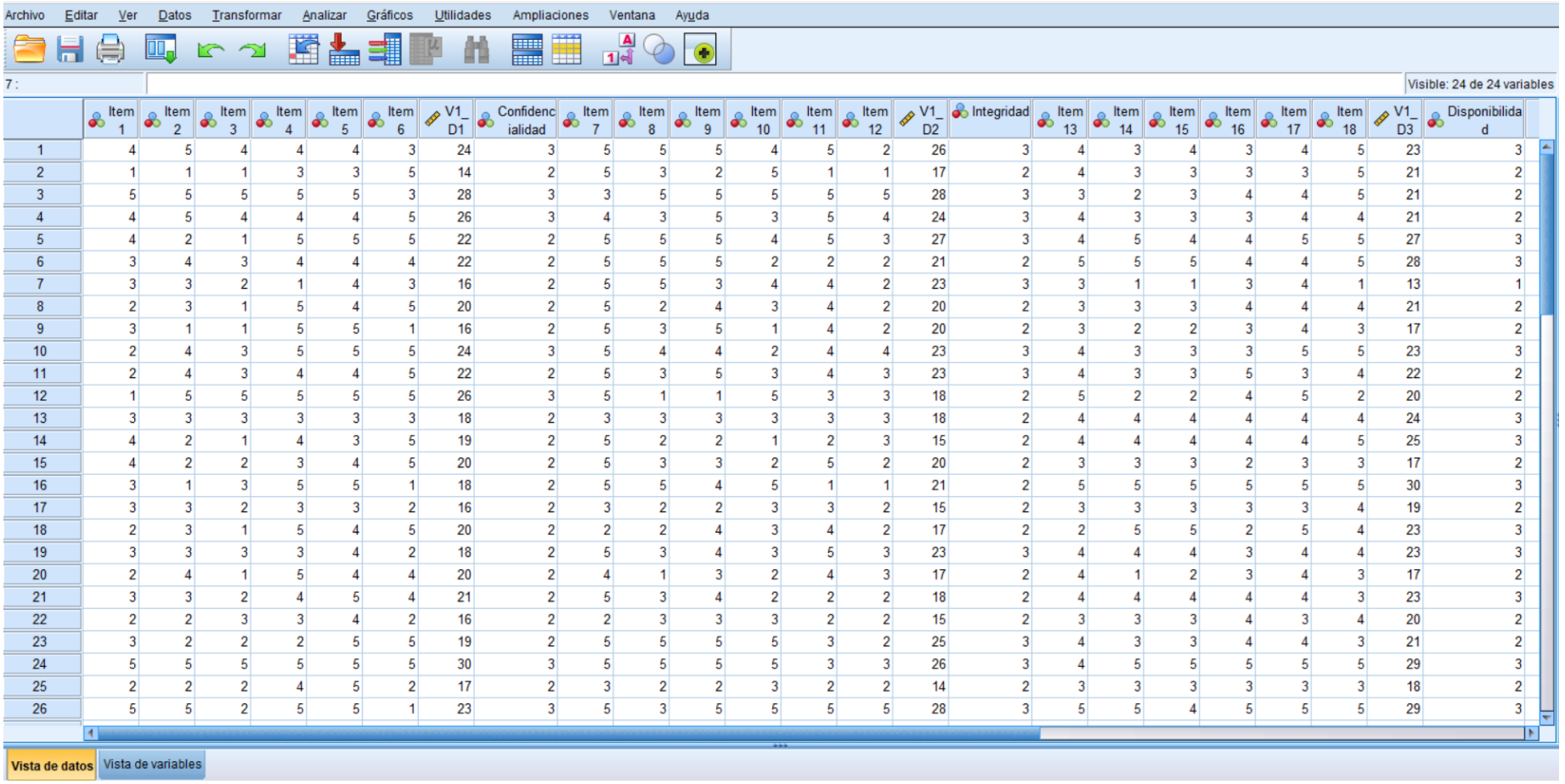


	Item1	Item2	Item3	Item4	Item5	Item6	Item7	Item8	Item9	Item10	Item11	Item12	Item13	Item14	Item15	Item16	Item17	Item18
1	4	5	4	4	4	3	5	5	5	4	5	2	4	3	4	3	4	5
2	1	1	1	3	3	5	5	3	2	5	1	1	4	3	3	3	3	5
3	5	5	5	5	5	3	3	5	5	5	5	5	3	2	3	4	4	5
4	4	5	4	4	4	5	4	3	5	3	5	4	4	3	3	3	4	4
5	4	2	1	5	5	5	5	5	5	4	5	3	4	5	4	4	5	5
6	3	4	3	4	4	4	5	5	5	2	2	2	5	5	5	4	4	5
7	3	3	2	1	4	3	5	5	3	4	4	2	3	1	1	3	4	1
8	2	3	1	5	4	5	5	2	4	3	4	2	3	3	3	4	4	4
9	3	1	1	5	5	1	5	3	5	1	4	2	3	2	2	3	4	3
10	2	4	3	5	5	5	5	4	4	2	4	4	4	3	3	3	5	5
11	2	4	3	4	4	5	5	3	5	3	4	3	4	3	3	5	3	4
12	1	5	5	5	5	5	5	1	1	5	3	3	5	2	2	4	5	2
13	3	3	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4
14	4	2	1	4	3	5	5	2	2	1	2	3	4	4	4	4	4	5
15	4	2	2	3	4	5	5	3	3	2	5	2	3	3	3	2	3	3
16	3	1	3	5	5	1	5	5	4	5	1	1	5	5	5	5	5	5
17	3	3	2	3	3	2	3	2	2	3	3	2	3	3	3	3	3	4
18	2	3	1	5	4	5	2	2	4	3	4	2	2	5	5	2	5	4
19	3	3	3	3	4	2	5	3	4	3	5	3	4	4	4	3	4	4
20	2	4	1	5	4	4	4	1	3	2	4	3	4	1	2	3	4	3
21	3	3	2	4	5	4	5	3	4	2	2	2	4	4	4	4	4	3
22	2	2	3	3	4	2	2	3	3	3	2	2	3	3	3	4	3	4
23	3	2	2	2	5	5	5	5	5	5	3	2	4	3	3	4	4	3
24	5	5	5	5	5	5	5	5	5	5	3	3	4	5	5	5	5	5



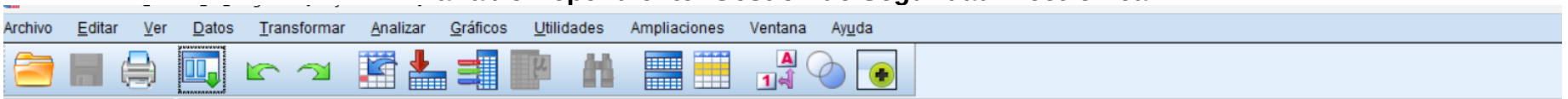
	Item1	Item2	Item3	Item4	Item5	Item6	Item7	Item8	Item9	Item10	Item11	Item12	Item13	Item14	Item15	Item16	Item17	Item18
25	2	2	2	4	5	2	3	2	2	3	2	2	3	3	3	3	3	3
26	5	5	2	5	5	1	5	3	5	5	5	5	5	5	4	5	5	5
27	2	2	1	5	5	5	5	5	5	5	4	2	4	3	3	4	3	2
28	3	3	2	5	5	4	5	3	5	3	3	3	5	4	4	4	4	5
29	2	1	1	5	5	1	4	5	5	3	2	2	4	3	3	4	4	1
30	5	3	2	5	5	5	5	4	5	2	5	1	4	5	4	5	5	4
31	2	2	2	4	5	5	5	3	5	3	5	2	4	4	4	4	5	3
32	1	5	1	5	5	5	4	5	5	3	5	5	5	5	3	5	5	5
33	3	4	4	4	3	4	5	4	4	4	3	3	3	4	4	3	3	5
34	2	3	3	4	5	1	5	4	1	1	3	3	3	4	1	1	1	2
35	3	5	3	5	5	5	4	1	5	2	2	5	4	4	3	1	5	4
36	2	4	4	4	5	3	5	5	5	5	5	4	4	4	4	4	4	4
37	2	4	3	4	3	3	5	3	3	4	3	4	2	1	1	2	2	3
38	2	3	3	4	4	1	4	3	4	3	4	1	3	1	1	3	4	3
39	1	2	2	4	5	1	4	3	4	4	3	4	4	4	4	3	4	3
40	3	2	3	4	5	5	5	1	3	1	3	3	5	2	2	2	5	5
41	3	1	1	5	3	5	5	3	5	5	5	1	3	3	2	3	5	3
42	1	3	2	3	4	5	5	1	1	1	4	1	3	2	3	3	3	3
43	4	5	5	5	5	5	5	1	5	4	5	5	5	5	4	4	5	5
44	3	5	1	5	5	5	5	5	5	3	3	3	4	4	3	4	4	4
45	2	3	2	5	5	5	3	4	5	1	2	2	4	2	2	3	3	3
46	4	5	4	5	4	5	5	4	5	4	3	4	4	4	3	3	4	3
47	4	5	4	4	4	4	4	3	5	5	5	5	5	3	4	4	4	5
48	4	5	4	4	4	4	4	5	5	4	5	4	5	5	5	4	4	5
49	3	5	3	5	5	5	5	3	4	2	4	5	4	3	3	2	4	5
50	2	2	5	5	3	3	5	4	5	4	4	3	4	5	5	3	4	4

Dimensiones

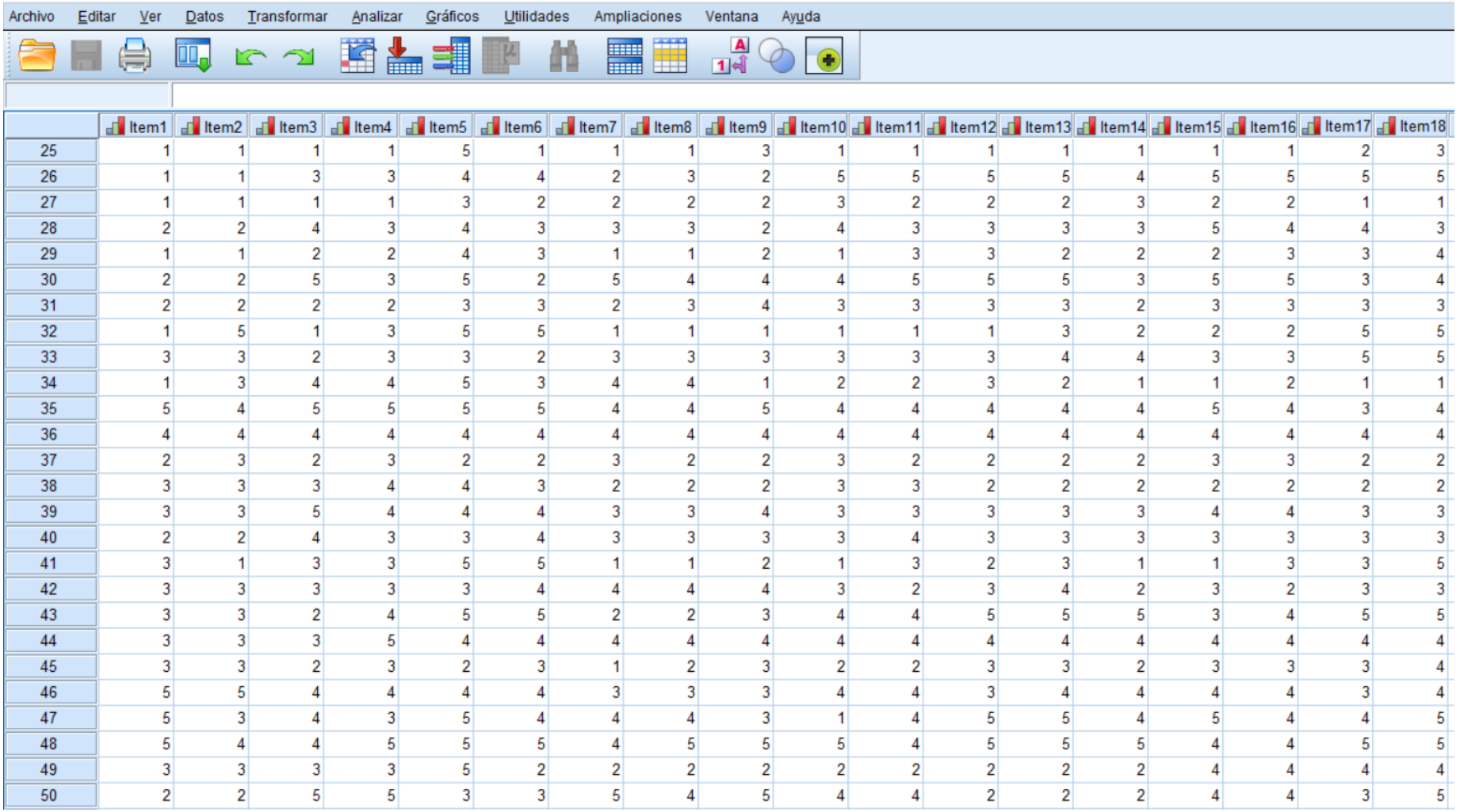


	Item 1	Item 2	Item 3	Item 4	Item 5	Item 6	V1_D1	Confidencialidad	Item 7	Item 8	Item 9	Item 10	Item 11	Item 12	V1_D2	Integridad	Item 13	Item 14	Item 15	Item 16	Item 17	Item 18	V1_D3	Disponibilidad
1	4	5	4	4	4	3	24	3	5	5	5	4	5	2	26	3	4	3	4	3	4	5	23	3
2	1	1	1	3	3	5	14	2	5	3	2	5	1	1	17	2	4	3	3	3	3	5	21	2
3	5	5	5	5	5	3	28	3	3	5	5	5	5	5	28	3	3	2	3	4	4	5	21	2
4	4	5	4	4	4	5	26	3	4	3	5	3	5	4	24	3	4	3	3	3	4	4	21	2
5	4	2	1	5	5	5	22	2	5	5	5	4	5	3	27	3	4	5	4	4	5	5	27	3
6	3	4	3	4	4	4	22	2	5	5	5	2	2	2	21	2	5	5	5	4	4	5	28	3
7	3	3	2	1	4	3	16	2	5	5	3	4	4	2	23	3	3	1	1	3	4	1	13	1
8	2	3	1	5	4	5	20	2	5	2	4	3	4	2	20	2	3	3	3	4	4	4	21	2
9	3	1	1	5	5	1	16	2	5	3	5	1	4	2	20	2	3	2	2	3	4	3	17	2
10	2	4	3	5	5	5	24	3	5	4	4	2	4	4	23	3	4	3	3	3	5	5	23	3
11	2	4	3	4	4	5	22	2	5	3	5	3	4	3	23	3	4	3	3	5	3	4	22	2
12	1	5	5	5	5	5	26	3	5	1	1	5	3	3	18	2	5	2	2	4	5	2	20	2
13	3	3	3	3	3	3	18	2	3	3	3	3	3	3	18	2	4	4	4	4	4	4	24	3
14	4	2	1	4	3	5	19	2	5	2	2	1	2	3	15	2	4	4	4	4	4	5	25	3
15	4	2	2	3	4	5	20	2	5	3	3	2	5	2	20	2	3	3	3	2	3	3	17	2
16	3	1	3	5	5	1	18	2	5	5	4	5	1	1	21	2	5	5	5	5	5	5	30	3
17	3	3	2	3	3	2	16	2	3	2	2	3	3	2	15	2	3	3	3	3	3	4	19	2
18	2	3	1	5	4	5	20	2	2	2	4	3	4	2	17	2	2	5	5	2	5	4	23	3
19	3	3	3	3	4	2	18	2	5	3	4	3	5	3	23	3	4	4	4	3	4	4	23	3
20	2	4	1	5	4	4	20	2	4	1	3	2	4	3	17	2	4	1	2	3	4	3	17	2
21	3	3	2	4	5	4	21	2	5	3	4	2	2	2	18	2	4	4	4	4	4	3	23	3
22	2	2	3	3	4	2	16	2	2	3	3	3	2	2	15	2	3	3	3	4	3	4	20	2
23	3	2	2	2	5	5	19	2	5	5	5	5	3	2	25	3	4	3	3	4	4	3	21	2
24	5	5	5	5	5	5	30	3	5	5	5	5	3	3	26	3	4	5	5	5	5	5	29	3
25	2	2	2	4	5	2	17	2	3	2	2	3	2	2	14	2	3	3	3	3	3	3	18	2
26	5	5	2	5	5	1	23	3	5	3	5	5	5	5	28	3	5	5	4	5	5	5	29	3

Variable Dependiente: Gestión de Seguridad Electrónica

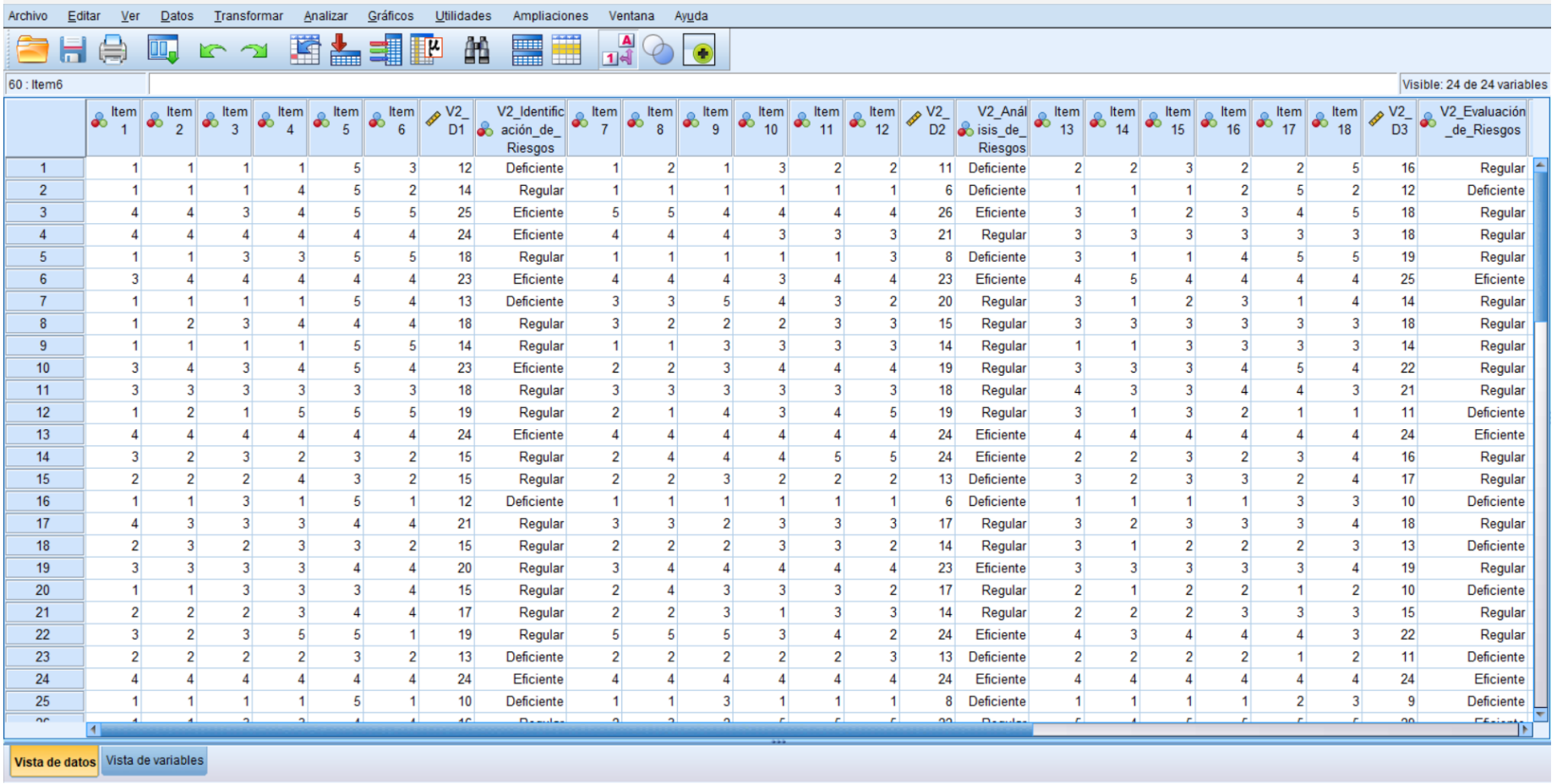


	Item1	Item2	Item3	Item4	Item5	Item6	Item7	Item8	Item9	Item10	Item11	Item12	Item13	Item14	Item15	Item16	Item17	Item18
1	1	1	1	1	5	3	1	2	1	3	2	2	2	2	3	2	2	5
2	1	1	1	4	5	2	1	1	1	1	1	1	1	1	1	2	5	2
3	4	4	3	4	5	5	5	5	4	4	4	4	3	1	2	3	4	5
4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3
5	1	1	3	3	5	5	1	1	1	1	1	3	3	1	1	4	5	5
6	3	4	4	4	4	4	4	4	4	3	4	4	4	5	4	4	4	4
7	1	1	1	1	5	4	3	3	5	4	3	2	3	1	2	3	1	4
8	1	2	3	4	4	4	3	2	2	2	3	3	3	3	3	3	3	3
9	1	1	1	1	5	5	1	1	3	3	3	3	1	1	3	3	3	3
10	3	4	3	4	5	4	2	2	3	4	4	4	3	3	3	4	5	4
11	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	4	4	3
12	1	2	1	5	5	5	2	1	4	3	4	5	3	1	3	2	1	1
13	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
14	3	2	3	2	3	2	2	4	4	4	5	5	2	2	3	2	3	4
15	2	2	2	4	3	2	2	2	3	2	2	2	3	2	3	3	2	4
16	1	1	3	1	5	1	1	1	1	1	1	1	1	1	1	1	3	3
17	4	3	3	3	4	4	3	3	2	3	3	3	3	2	3	3	3	4
18	2	3	2	3	3	2	2	2	2	3	3	2	3	1	2	2	2	3
19	3	3	3	3	4	4	3	4	4	4	4	4	3	3	3	3	3	4
20	1	1	3	3	3	4	2	4	3	3	3	2	2	1	2	2	1	2
21	2	2	2	3	4	4	2	2	3	1	3	3	2	2	2	3	3	3
22	3	2	3	5	5	1	5	5	5	3	4	2	4	3	4	4	4	3
23	2	2	2	2	3	2	2	2	2	2	2	3	2	2	2	2	1	2
24	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4



	Item1	Item2	Item3	Item4	Item5	Item6	Item7	Item8	Item9	Item10	Item11	Item12	Item13	Item14	Item15	Item16	Item17	Item18
25	1	1	1	1	5	1	1	1	3	1	1	1	1	1	1	1	2	3
26	1	1	3	3	4	4	2	3	2	5	5	5	5	4	5	5	5	5
27	1	1	1	1	3	2	2	2	2	3	2	2	2	3	2	2	1	1
28	2	2	4	3	4	3	3	3	2	4	3	3	3	3	5	4	4	3
29	1	1	2	2	4	3	1	1	2	1	3	3	2	2	2	3	3	4
30	2	2	5	3	5	2	5	4	4	4	5	5	5	3	5	5	3	4
31	2	2	2	2	3	3	2	3	4	3	3	3	3	2	3	3	3	3
32	1	5	1	3	5	5	1	1	1	1	1	1	3	2	2	2	5	5
33	3	3	2	3	3	2	3	3	3	3	3	3	4	4	3	3	5	5
34	1	3	4	4	5	3	4	4	1	2	2	3	2	1	1	2	1	1
35	5	4	5	5	5	5	4	4	5	4	4	4	4	4	5	4	3	4
36	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
37	2	3	2	3	2	2	3	2	2	3	2	2	2	2	3	3	2	2
38	3	3	3	4	4	3	2	2	2	3	3	2	2	2	2	2	2	2
39	3	3	5	4	4	4	3	3	4	3	3	3	3	3	4	4	3	3
40	2	2	4	3	3	4	3	3	3	3	4	3	3	3	3	3	3	3
41	3	1	3	3	5	5	1	1	2	1	3	2	3	1	1	3	3	5
42	3	3	3	3	3	4	4	4	4	3	2	3	4	2	3	2	3	3
43	3	3	2	4	5	5	2	2	3	4	4	5	5	5	3	4	5	5
44	3	3	3	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4
45	3	3	2	3	2	3	1	2	3	2	2	3	3	2	3	3	3	4
46	5	5	4	4	4	4	3	3	3	4	4	3	4	4	4	4	3	4
47	5	3	4	3	5	4	4	4	3	1	4	5	5	4	5	4	4	5
48	5	4	4	5	5	5	4	5	5	5	4	5	5	5	4	4	5	5
49	3	3	3	3	5	2	2	2	2	2	2	2	2	2	4	4	4	4
50	2	2	5	5	3	3	5	4	5	4	4	2	2	2	4	4	3	5

Dimensiones



Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

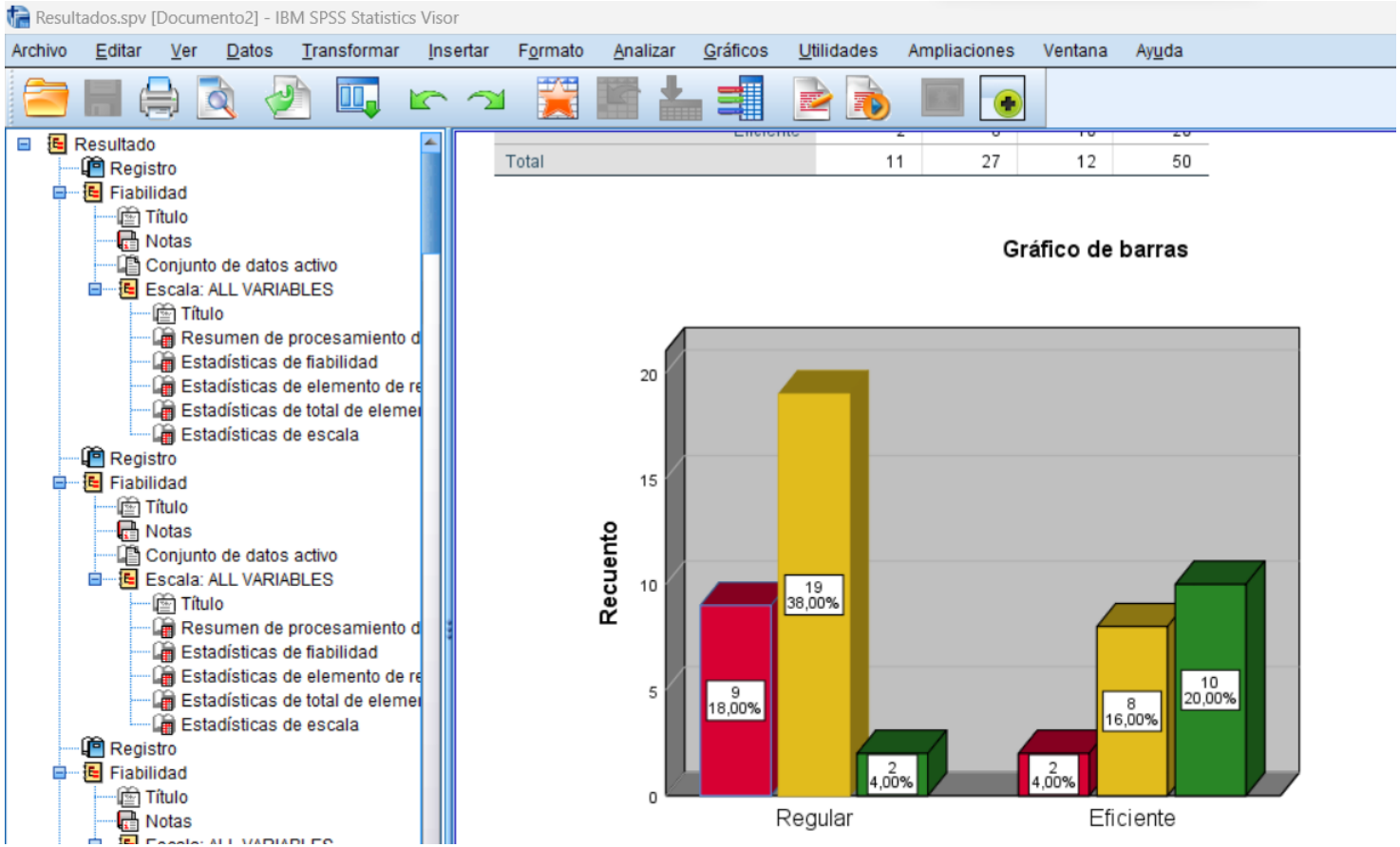
60 : Item6

Visible: 24 de 24 variables

	Item 1	Item 2	Item 3	Item 4	Item 5	Item 6	V2_D1	V2_Identificación_de_Riesgos	Item 7	Item 8	Item 9	Item 10	Item 11	Item 12	V2_D2	V2_Análisis_de_Riesgos	Item 13	Item 14	Item 15	Item 16	Item 17	Item 18	V2_D3	V2_Evaluación_de_Riesgos
1	1	1	1	1	5	3	12	Deficiente	1	2	1	3	2	2	11	Deficiente	2	2	3	2	2	5	16	Regular
2	1	1	1	4	5	2	14	Regular	1	1	1	1	1	1	6	Deficiente	1	1	1	2	5	2	12	Deficiente
3	4	4	3	4	5	5	25	Eficiente	5	5	4	4	4	4	26	Eficiente	3	1	2	3	4	5	18	Regular
4	4	4	4	4	4	4	24	Eficiente	4	4	4	3	3	3	21	Regular	3	3	3	3	3	3	18	Regular
5	1	1	3	3	5	5	18	Regular	1	1	1	1	1	3	8	Deficiente	3	1	1	4	5	5	19	Regular
6	3	4	4	4	4	4	23	Eficiente	4	4	4	3	4	4	23	Eficiente	4	5	4	4	4	4	25	Eficiente
7	1	1	1	1	5	4	13	Deficiente	3	3	5	4	3	2	20	Regular	3	1	2	3	1	4	14	Regular
8	1	2	3	4	4	4	18	Regular	3	2	2	2	3	3	15	Regular	3	3	3	3	3	3	18	Regular
9	1	1	1	1	5	5	14	Regular	1	1	3	3	3	3	14	Regular	1	1	3	3	3	3	14	Regular
10	3	4	3	4	5	4	23	Eficiente	2	2	3	4	4	4	19	Regular	3	3	3	4	5	4	22	Regular
11	3	3	3	3	3	3	18	Regular	3	3	3	3	3	3	18	Regular	4	3	3	4	4	3	21	Regular
12	1	2	1	5	5	5	19	Regular	2	1	4	3	4	5	19	Regular	3	1	3	2	1	1	11	Deficiente
13	4	4	4	4	4	4	24	Eficiente	4	4	4	4	4	4	24	Eficiente	4	4	4	4	4	4	24	Eficiente
14	3	2	3	2	3	2	15	Regular	2	4	4	4	5	5	24	Eficiente	2	2	3	2	3	4	16	Regular
15	2	2	2	4	3	2	15	Regular	2	2	3	2	2	2	13	Deficiente	3	2	3	3	2	4	17	Regular
16	1	1	3	1	5	1	12	Deficiente	1	1	1	1	1	1	6	Deficiente	1	1	1	1	3	3	10	Deficiente
17	4	3	3	3	4	4	21	Regular	3	3	2	3	3	3	17	Regular	3	2	3	3	3	4	18	Regular
18	2	3	2	3	3	2	15	Regular	2	2	2	3	3	2	14	Regular	3	1	2	2	2	3	13	Deficiente
19	3	3	3	3	4	4	20	Regular	3	4	4	4	4	4	23	Eficiente	3	3	3	3	3	4	19	Regular
20	1	1	3	3	3	4	15	Regular	2	4	3	3	3	2	17	Regular	2	1	2	2	1	2	10	Deficiente
21	2	2	2	3	4	4	17	Regular	2	2	3	1	3	3	14	Regular	2	2	2	3	3	3	15	Regular
22	3	2	3	5	5	1	19	Regular	5	5	5	3	4	2	24	Eficiente	4	3	4	4	4	3	22	Regular
23	2	2	2	2	3	2	13	Deficiente	2	2	2	2	2	3	13	Deficiente	2	2	2	2	1	2	11	Deficiente
24	4	4	4	4	4	4	24	Eficiente	4	4	4	4	4	4	24	Eficiente	4	4	4	4	4	4	24	Eficiente
25	1	1	1	1	5	1	10	Deficiente	1	1	3	1	1	1	8	Deficiente	1	1	1	1	2	3	9	Deficiente

Vista de datos Vista de variables

Resultados


Resultados.spv [Documento2] - IBM SPSS Statistics Visor
Archivo Editar Ver Datos Transformar Insertar Formato Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda
Resultado
Registro
Fiabilidad
Título
Notas
Conjunto de datos activo
Escala: ALL VARIABLES
Título
Resumen de procesamiento d
Estadísticas de fiabilidad
Estadísticas de elemento de re
Estadísticas de total de elemer
Estadísticas de escala
Registro
Fiabilidad
Título
Notas
Conjunto de datos activo
Escala: ALL VARIABLES
Título
Resumen de procesamiento d
Estadísticas de fiabilidad
Estadísticas de elemento de re
Estadísticas de total de elemer
Estadísticas de escala
Registro
Fiabilidad
Título
Notas
Total 11 27 12 50
Gráfico de barras
Recuento
20
15
10
5
0
9 18,00%
19 38,00%
2 4,00%
2 4,00%
8 16,00%
10 20,00%
Regular
Eficiente

Anexo 9: Matriz de Consistencia

<table>
<tr><th>PROBLEMA</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th colspan="5">VARIABLES E INDICADORES</th></tr>
<tr><td rowspan="5">Problema general:

¿En qué medida influye implementar un SGSI en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023?

Problemas específicos

PE1: ¿En qué medida el SGSI influye con la confidencialidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023?

PE2: ¿En qué medida el SGSI influye con la integridad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023?

PE3: ¿En qué medida el SGSI influye con la disponibilidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023?</td><td rowspan="5">Objetivo general:

Determinar la influencia de un SGSI en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023

Objetivos Específicos:

OE1: Determinar la influencia del SGSI con la confidencialidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023.

OE2: Determinar la influencia del SGSI con la integridad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023.

OE3: Determinar la influencia del SGSI con la disponibilidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023.</td><td rowspan="5">Hipótesis general:

El SGSI influye significativamente en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023.

Hipótesis específicas:

HE1: El SGSI influye significativamente con la confidencialidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023.

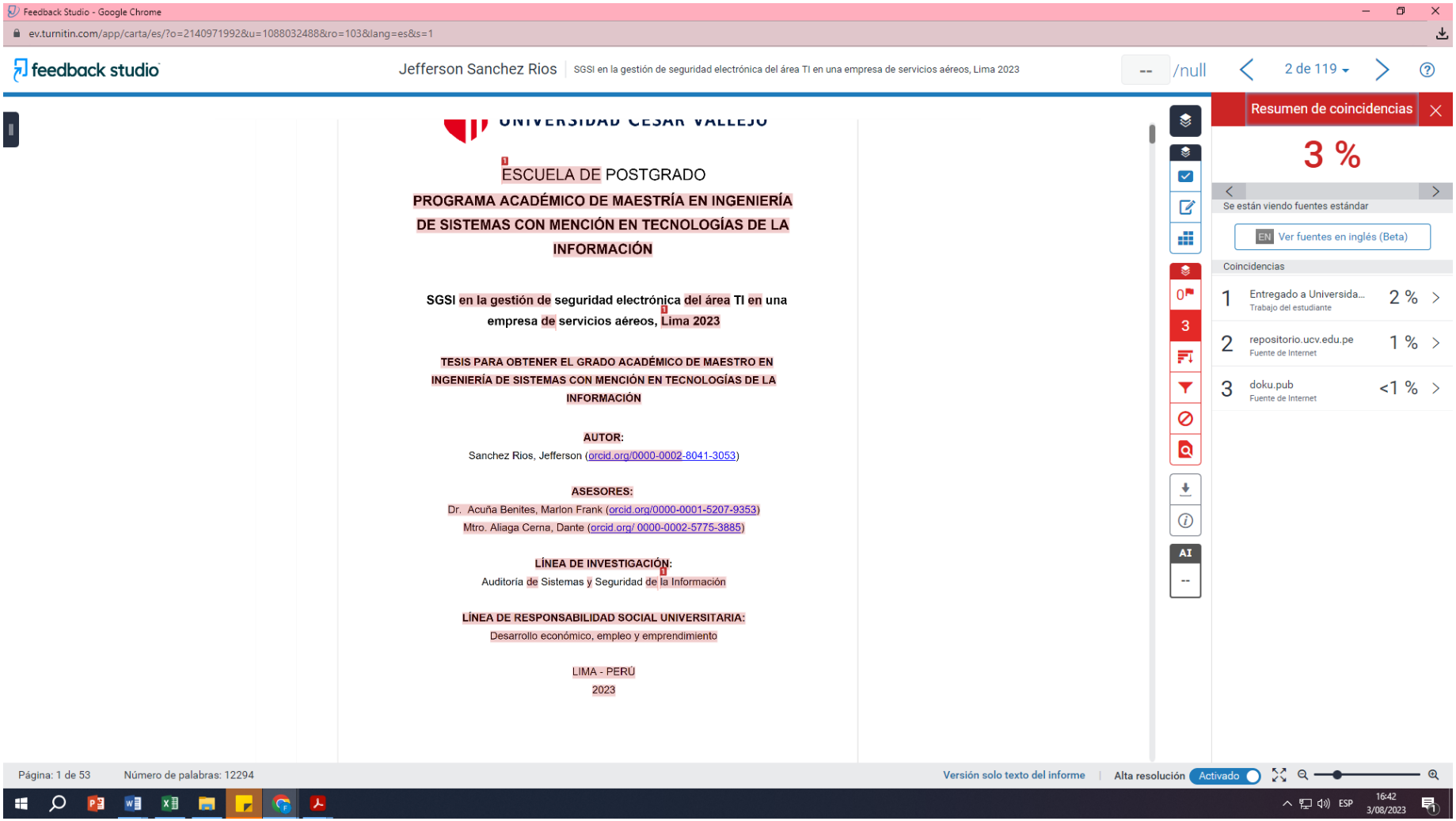
HE2: El SGSI influye significativamente con la integridad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023.

HE3: El SGSI influye significativamente con la disponibilidad en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023.</td><td colspan="5">Variable 1: SGSI</td></tr>
<tr><td>Dimensiones</td><td>Indicadores</td><td>Ítems</td><td>Escala</td><td>Niveles y rangos</td></tr>
<tr><td>Confidencialidad</td><td>Políticas de seguridad de la información.
Clasificación de activos de información.</td><td>1-2
3-6</td><td rowspan="3">(1) Nunca
(2) Casi nunca
(3) A veces
(4) Casi siempre
(5) Siempre</td><td rowspan="3">[1] Deficiente
[2] Regular
[3] Eficiente</td></tr>
<tr><td>Integridad</td><td>Protección de credenciales.
Incidentes de manipulación de datos.</td><td>7-8
9-12</td></tr>
<tr><td>Disponibilidad</td><td>Tiempo respuesta.
Respaldo de información.</td><td>13-14
15-18</td></tr>
<tr><td colspan="5">Variable 2: Gestión de seguridad electrónica</td></tr>
<tr><td>Dimensiones</td><td>Indicadores</td><td>Ítems</td><td>Escala</td><td>Niveles y rangos</td></tr>
<tr><td>Identificación de Riesgos</td><td>Conocimiento de controles
Conocimiento de riesgos</td><td>1-3
3-6</td><td rowspan="3">(1) Nunca
(2) Casi nunca
(3) A veces
(4) Casi siempre
(5) Siempre</td><td rowspan="3">[1] Deficiente
[2] Regular
[3] Eficiente</td></tr>
<tr><td>Análisis de Riesgos</td><td>Identificación de riesgos
Monitoreo de riesgos</td><td>7-8
9-12</td></tr>
<tr><td>Evaluación de Riesgo</td><td>Aplicación y seguimiento
Efectividad en los controles y niveles de riesgos</td><td>13-14
15-18</td></tr>
<tr><th>Nivel – Diseño de la Investigación</th><th>Población y muestra</th><th colspan="3">Técnicas e Instrumentos</th><th colspan="2">Estadística a utilizar</th></tr>
<tr><td>Enfoque: Cuantitativo.
Método: Hipotético - Deductivo.
Diseño: No experimental.
Tipo de estudio: Básica.
Nivel de estudio: Correlacional.
Corte: Transversal o Transeccional.</td><td>Población: 50 colaboradores de diversas áreas.
Tipo de muestreo: No probabilístico.
Tamaño de muestra: 50 colaboradores.</td><td colspan="3">Variable 1: SGSI.
Técnica: Encuesta.
Instrumento: Cuestionario.
Autor: Jefferson Sanchez Rios.
Año: 2023.
Ámbito de Aplicación: Colaboradores de varias áreas.
Forma de Administración: Individual, Única vez.

Variable 2: Gestión de seguridad electrónica.
Técnica: Encuesta.
Instrumento: Cuestionario.
Autor: Jefferson Sanchez Rios.
Año: 2023.
Ámbito de Aplicación: Colaboradores de varias áreas.
Forma de Administración: Individual, Única vez.</td><td colspan="2">Descriptiva:
Estadística descriptiva.

Inferencial:
Para la estadística inferencial se utilizará la prueba estadística R de Pearson para comprobar la asociación entre las variables y sus dimensiones.</td></tr>
</table>

Anexo 10: Resultado de similitud del programa Turnitin



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, ACUÑA BENITES MARLON FRANK, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "SGSI en la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023", cuyo autor es SANCHEZ RIOS JEFFERSON, constato que la investigación tiene un índice de similitud de 3.00%, 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, 31 de Julio del 2023

Apellidos y Nombres del Asesor:	**Firma**
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID:** 0000-0001-5207-9353	Firmado electrónicamente por: MACUNABE el 31-07-2023 22:59:29

Código documento Trilce: TRI - 0632282

INVESTIGA UCV