UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Norma ISO 27001 para el Control de la Seguridad de Información en una Consultoría Privada, Lima 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:
MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR:
Aleman Balladares Fernando Yasmani (orcid.org/0000-0002-1780-5775)

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

CO-ASESOR:
Dr. Flores Zafra David (orcid.org/0000-0001-5846-325X)

LÍNEA DE INVESTIGACIÓN:
Sistemas de Información y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:
Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ
2023

Dedicatoria

Dedicar la presente investigación de tesis a mi familia por el apoyo constante para lograr mis metas trazadas.

Agradecimiento

A Dios por la darme la oportunidad de fortaleza y perseverancia en lograr los objetivos.

A mi familia por estar siempre a mi lado y darme las fuerzas necesarias en cada momento de mi vida.

Mi agradecimiento al Dr. Acuña Benites Marlon Frank y al Dr. Flores Zafra David, por sus asesorías en esta tesis

Índice de contenido

Pág.

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

La problemática de la presente investigación, surgió con la propagación de la COVID-19, que conllevó a que varias instituciones públicas como privadas de los rubros empresariales se reinventen, empezando la era tecnológica, que trajo como consecuencia los ciberataques; he aquí la importancia de la presente investigación que tuvo como objetivo determinar en qué medida influye la implementación de la norma ISO 27001:2013 en el control de seguridad de la información en una consultoría privada, para ello se aplicó un tipo de investigación aplicada, con diseño preexperimental bajo un enfoque cuantitativo-correlacional. Seguidamente el análisis de resultados se realizó a través de mediciones con las dimensiones definidas para la variable dependiente; se utilizó como instrumentos cuestionarios, validado por el juicio de 03 expertos. Los resultados obtenidos del post test en comparación al pretest fueron menor a 0.5 de nivel de significancia, teniendo en cuenta una prueba no paramétrica de distribución no normal, lo que evidenció que la norma ISO 27001:2013 mejorará en el control de seguridad de la información en la consultoría privada.

Palabras Clave: Seguridad de la información, riesgos informáticos, Norma ISO 27001, control de seguridad.

Abstract

The problem of the present investigation arose with the spread of COVID-19, which led to several public and private institutions in business areas reinventing themselves, beginning the technological era, which resulted in cyber-attacks; Here is the importance of this research that aimed to determine to what extent the implementation of the ISO 27001:2013 standard influences the control of information security in a private consultancy, for this a type of applied research was applied, with pre-experimental design under a quantitative-correlational approach. Next, the analysis of results was carried out through measurements with the dimensions defined for the dependent variable; Questionnaires were used as instruments, validated by the judgment of 03 experts. The results obtained from the post-test compared to the pre-test were less than 0.5 of significance level, taking into account a non-parametric test of non-normal distribution, which showed that the ISO 27001:2013 standard will improve the security control of the information in private consulting.

Keywords: Information security, computer risks, ISO 27001 Standard, security control.

I. INTRODUCCIÓN

Aproximadamente hace no más de 03 años, cuando la pandemia ocasionada por la COVID-19 empezó a propagarse por el mundo; todas las instituciones privadas y públicas de todos los rubros empresariales se vieron en la obligación de reinventarse, crear nuevas estrategias tecnológicas; esto conllevó a que la transformación digital en los últimos años se acelere considerablemente; al igual que el crecimiento en aspectos negativos como son los ciberataques.

En el 2020, según el estudio realizado por la universidad de Maryland señalo que, los dispositivos móviles y computadores, cada 39 segundos son atacados cibernéticamente bajo las técnicas de Phishing, Correo SPAM, Malware y Ransomware y dominios malignos, esto debido a la falta de políticas de seguridad informática (Repositorio Institucional Universidad Piloto de Colombia, 2022).

Por otro lado, en una encuesta realiza por Microsoft sobre ciberseguridad a las grandes empresas de América latina en el año 2022, el 31% de las empresas evidenciaron un crecimiento de ciberataques a lo largo de la pandemia, específicamente en el rubro bancario y consultorías; asimismo se especificó que solamente el 27% de empresas suministra equipos tecnológicos configurados bajo políticas de seguridad a sus trabajadores. En este último aspecto, se genera una gran preocupación, ya que las actividades laborales se realizan con equipos personales, y la empresa acepta el riesgo informático al que puedan ser vulnerados (Morales, 2022).

A nivel nacional, hasta antes de la pandemia, la gran mayoría de empresas PYMES descuidaban la seguridad de su información ya que no eran blanco constante de ciberataques, por tal consideraban como innecesario invertir en estrategias o políticas de seguridad; actualmente esta situación ha cambiado, ya que ante la implementación y automatización apresurada de los procesos internos a raíz de la pandemia, los ciberdelincuentes han encontrado diversas vulnerabilidades y oportunidad para los delitos informáticos (Rossi, 2021).

Los riesgos de ciberataques a través de suplantación de identidad en el Perú entre los años 2020 y 2021 tuvieron un crecimiento de 49%, el phishing como es conocido este tipo de ataques fue realizado a 600 empresas de las cuales la en su mayoría resaltaron los rubros financieros y consultorías, asimismo solamente un 20% de estas empresas tomaron la iniciativa de aumentar su presupuesto en ciberseguridad (Seguridad América, 2022).

La empresa privada, lugar donde se desarrollará la investigación, realiza servicios de consultoría Contable. Según la entrevista realizada al nuevo jefe de sistemas, manifiesta que actualmente existe un total de 293 clientes, de los cuales son atendidos y distribuidos entre 78 profesionales (trabajadores), durante su instancia en la consultora ha detectado diversos déficits, de los cuales en conjunto con la gerencia general han priorizado y coincidido que la organización no cuenta con políticas en seguridad de la información, lo que impide en mejorar la disponibilidad de la misma en base a una correcta accesibilidad; la mayoría de trabajadores cometen desorden de la información almacenándolas en diferentes ubicación, también no existe una adecuada forma de distribuir el acceso a la información perteneciente a la empresa; asimismo existe un déficit en el crecimiento de la información la cual está siendo almacenada de manera improvisada en discos reutilizados y en su mayoría la información se encuentra dividida en diversas unidades por que la capacidad no es suficiente; por otro lado el retraso para acceder a la información histórica se debe a que la información se encuentra almacenada en unidades externas de almacenamiento, esto dificulta el acceso a la información con urgencia; finalmente el resguardo de información está expuesta amenazas externas y climáticas, ya que los dispositivos o unidades están almacenados inapropiadamente en cajas o reubicadas en diferentes unidades.

Es preciso indicar que los nuevos clientes están solicitando con más frecuencia contratos o clausulas donde se garantice la protección de la información para la manipulación de datos que se entreguen a la consultora; por tal se requiere con suma urgencia la implementación de políticas en seguridad de la información que permita mejorar y seguir creciendo la empresa consultora ante la competencia de mercado actual.

La definición de activos de información dentro de las organización o empresas abarca desde la documentación física o digitalizada, así como los servicios, softwares o aplicaciones, también comprende a todo equipamiento tecnológico como servidores, portátiles, equipos estaciones y móviles; a través de su identificación permitirán una óptima gestión en la seguridad de información (Guerrero, 2022).

Se determina que, dentro de los diversos problemas identificados, a través de la utilización del árbol de problemas (ver Anexo 9). Los problemas que han sido identificados en la consultoría privada son: (a) la falta de una norma ISO 27001:2013 para un correcto control de la seguridad de información; (b) la desinformación por parte del personal; (c) la poca eficacia de los trabajadores para poder atender sucesos que ponen en riesgo el control de la seguridad. Es preciso mencionar que uno de los incidentes reportados en marzo del 2022, donde un virus encripto y borro archivos, equivalentes a 15 días de información, generando un retraso de 4 días para la entrega de resultados mensuales a los clientes. Asimismo, no se pudo detectar a los responsables sobre el filtro de dicha amenaza, lo cual trajo como consecuencia la inconformidad del cliente.

Ante el contexto mencionado sobre la realidad problemática, se tiene la siguiente formulación del problema general: ¿cómo influye la implementación de la norma ISO 27001:2013 en el control de seguridad de la información en la consultoría privada? Los problemas específicos son: (a) ¿cómo influye la implementación de la norma ISO 27001:2013 en la disponibilidad de la información?; (b) ¿cómo influye la norma ISO 27001:2013 en la adaptabilidad de la información?; (c) ¿cómo influye la norma ISO 27001:2013 en la accesibilidad de la información?; (d) ¿cómo influye la norma ISO 27001:2013 en el resguardo de la información?

Como justificación práctica, es importante implementar la norma ISO 27001:2013, permitirá controlar la seguridad de información en la consultora privada, desde la identificación de amenazas, vulnerabilidades e impacto que exista sobre los activos de información, con ello se podrá prevenir, afrontar y mejorar

continuamente los riesgos informáticos existentes; por otro lado como justificación teórica, desde la indagación de casos de éxito de otras investigaciones en el marco de gestionar la seguridad de la información, se logrará fortalecer los conceptos técnicos para la implementación de norma ISO 27001:2013 en las consultorías peruanas, permitiendo así una documentación especifica como base para la mejora de otras futuras investigaciones; también se tiene, como justificación metodológica, se basa a partir de la recolección de información y experiencia en el ámbito que se encuentra la empresa en relación a seguridad y gestión de tecnologías de información, la norma ISO 27001:2013 permite ser aplicada en cualquier rubro empresarial, solo se debe mantener el enfoque de mejora continua basada en: Planificar – Hacer – Verificar – Actuar; ante la última justificación referida esta permitirá argumentar la siguiente justificación social, en la cual señala que los riesgos informáticos ya verificados y monitoreados pueden ser señalados como redundantes para otras empresas, por tal pueden ser estandarizados como una política a la cual se añadirían solamente nuevas casuísticas (Gaviria, 2019).

Para la investigación, se tiene el siguiente objetivo general, determinar en qué medida influye la implementación de la norma ISO 27001:2013 en el control de seguridad de la información en una consultoría privada. Como objetivos específicos se hace referencia; (a) determinar en qué medida influye la disponibilidad de la información para el control de la seguridad de información; (b) determinar en qué medida influye la adaptabilidad de la información para el control de la seguridad de información; (c) determinar en qué medida influye en la accesibilidad de la información para el control de la seguridad de información; (d) determinar en qué medida influye en el resguardo de la información para el control de la seguridad de información.

Finalmente, para el análisis de hipótesis general, se realizó el siguiente planteamiento, la norma ISO 27001:2013 mejorará en el control de seguridad de la información en la consultoría privada. Como hipótesis especificas se hace referencia; (a) la norma ISO 27001:2013 gestiona correctamente la disponibilidad de la información para el control de la seguridad de información; (b) la norma ISO 27001:2013 gestiona correctamente la adaptabilidad de la información para el

control de la seguridad de información; (c) la norma ISO 27001:2013 gestiona correctamente la accesibilidad de la información para el control de la seguridad de información; (d) la norma ISO 27001:2013 gestiona correctamente el resguardo de la información para el control de la seguridad de información.

II. MARCO TEÓRICO

Como primer antecedente internacional, según la investigación de Córdova, (2022), señaló en su problemática que una institución universitaria en Colombia adolece de un modelo de gestión en seguridad de la información, ya que los procesos fueron creados autónomamente por el departamento de sistemas y se controlan manualmente para brindar respuesta a los inconvenientes que se presenten por falta de protección en la información. Por consiguiente, el tipo de investigación se consideró aplicada la cual busca dar soluciones a las necesidades a raíz de los formatos brindados por la norma ISO 27001:2013. Además, los resultados de la investigación, permitió identificar los requerimientos de la ISO 27001:2013 para orientar lineamientos de calidad y gestionar los riesgos, asimismo se obtuvo un 43% de aceptación con el desarrollo de los procedimientos bajos la Norma ISO 27001. Finalmente, como conclusión se determina que, bajo el diseño de un SGSI, se abrirá nuevas oportunidades de mejora, como es el análisis para la integración de softwares libres agiles y óptimos, esto traerá el cumplimiento de objetivos a bajo costo.

En un segundo antecedente se hace referencia a Vivanco y Quintana, (2019), el cual indicó que la problemática de la Universidad Iberoamericana de Ecuador no contaba con una gestión en seguridad de información, partiendo de que no existía la documentación correspondiente que guiara a brindar optimas soluciones que eviten perdidas o se altere la información tanto financieramente como académicamente. Por consiguiente, se consideró como tipo de investigación descriptiva, porque se identificaron los riesgos de los activos de información y a partir de ello se estableció el tratamiento correspondiente. Además, el tipo de población finita se consideró a un total de 44 personas referentes a la unidad administrativa, de los cuales bajo un muestreo convencional o intencional se obtuvieron 27 personas que comprenden en el uso de activos de información. Por su parte, los resultados de la información se logró determinar las debilidades y fortalezas que influyen en la implementación de un SSI (Sistema de seguridad de información), para ello se partió desde la cultura empresarial en seguridad informática por parte de los trabajadores y el impacto que existiría al consolidarse una amenaza en los activos de información. En cuanto a, los porcentajes de los

resultados se obtuvo un 81 % de conocimiento en temas de seguridad de información sobre un 19 % que existía inicialmente y se logró mitigar en un 100% las amenazas existentes de acuerdo con los casos de vulnerabilidad detectados. Finalmente, se concluyó que el diseño de un SGSI aumenta en la calidad y competitividad de los procesos en base a los riesgos expuestos.

Como tercer antecedente internacional, para Chicaiza, (2019) el cual indicó que, la realidad problemática fue expuesta por el riesgo latente ante ataques internos o externos a los activos de información lo cual ha traído considerables pérdidas económicas a la pequeña empresa. Por consiguiente, el tipo de investigación fue correlacional porque se permitió a la variable independiente medir de acuerdo con su compatibilidad con la variable dependiente. En cuanto, al tipo de investigación empleado fue finito, ya que se consideró a 10 profesionales los cuales están distribuidos a 7 pequeñas empresas. Por lo tanto, los resultados de la investigación obtenidos bajo encuestas logro planificar y crear procesos idóneos para la implementación de controles en seguridad con relación a la categorización de riesgos. Con respecto a, los resultados se indicaron que el 66% ha obtenido conocimientos sobre seguridad de la información, y se ha tenido una mejora de 60% en los controles de seguridad de la información desde la aplicación de un diseño de gestión. Finalmente, como conclusión el planteamiento de un modelo de gestión en seguridad de la información genérico permitirá a las pequeñas empresas formalizas sus procesos y documentar correctamente las soluciones e incidencias reportadas.

Finalmente, como cuarto antecedente internacional, para Nacipucha, (2019) señaló que, como realidad problemática la empresa Arte Hogar no presente una gestión de información basado en normas de seguridad para el resguardo de información, porque hace vulnerable a cualquier amenaza existente, por tal se formula el siguiente problema: ¿Cómo diseñar un modelo de SGSI a través de la aplicación de la norma ISO 27001?; el tipo de investigación fue de campo, ya que se fundamenta por la obtención de información mediante la observación donde se desenvuelve cada proceso con la interacción con los trabajadores. Además, el tipo de población se consideró finita, asimismo fueron 40 colaboradores considerados

como muestra. Por lo tanto, el resultado de la investigación sobre las encuestas se detectó que la compañía es vulnerable por la desinformación de los trabajadores en temas de seguridad informática y mediante una entrevista al coordinador de TI se detectó la falta de políticas de seguridad. Cabe resaltar, que el porcentaje de resultados se obtuvo porque un 75% reconoció como primordial la seguridad de información. Finalmente, se indica que la empresa Arte Hogar debe permanentemente asegurar todo activo referente a la información a través de la definición de procesos de seguridad.

Luego de señalar los antecedentes internacionales que fundamenten la actual investigación, es necesario precisar algunos antecedentes nacionales, por tal se detallaran 4 de los más importantes y relacionados.

En primer lugar, se menciona el antecedente del autor Guardia, (2020) señaló que la secretaría de educación pública no tiene mecanismos como políticas, enfoques y planes para la adquisición de una cultura que se base en la seguridad entre sus funcionarios, por lo que las actividades que se realizan son basándose en estrategias temporales. Además, la investigación es de carácter aplicada, ya que el diseño de un modelo seguridad de información permitirá analizar los riesgos para iniciar con soluciones y tratamientos. Por lo que, el tipo de población es finita, se empleó el método no aleatorio ya que se observó a 20 colaboradores correspondientes del área de secretaria académica. Asimismo, el resultado de su investigación fue facilitar un modelo de seguridad de información a prueba de cualquier riesgo informático, pero basándose en la NTP-ISO/IEC 27001:2014, y la metodología MARGERIT, con ello facilitara la identificación de los activos informáticos de manera sencilla, dentro de los resultados se logró que lo indicadores alcanzaran en seguridad física un 95%, seguridad lógica 94%, seguridad en red 95%, gestión del modelo de seguridad de la información 100%, cumplimiento de políticas de seguridad por los colaboradores 90%, control de activos de información 93%. Finalmente, existen diferencias estadísticamente notables sobre la importancia de un diseño de un modelo de seguridad de información ya que se redujeron los riesgos informáticos, asimismo es necesario

mantener en una mejor continua las políticas establecidas para prevenir nuevas amenazas y detectar vulnerabilidades.

En segundo lugar, según, Mejía, (2020) señalo que, dentro de la realidad problemática existe un déficit con la seguridad en el acceso a su base de información, la falta de cumplimiento de las políticas de protección de la información y el acceso de los empleados a información segura. En este contexto, se suman otros aspectos como la falta de equipos que les permitan proteger la información, así como la falta de protocolos que garanticen la disponibilidad de los datos. Además; la investigación se consideró de tipo aplicada, ya que proporciona soluciones a partir de la implementación de la ISO/IEC 27001:2013; como población se representó bajo 12 profesionales del área de Tecnología e Informática y la muestra se consideró al total de la población. Por lo que, los resultados de la investigación a partir del diseño y administración de un SGSI, se logró la verificación de posibles riesgos y vulnerabilidades, con ello se definirá la mejor toma de decisiones la cual será documentada, y en donde se señala que la eficiencia en la seguridad de información fue nula antes de la implementación de la ISO, mientras que al término de la implementación se obtuvo una eficiencia en 91.7 %. Finalmente, se concluye que la efectividad de la ISO 27001 sobre la gestión de base datos, mejoró considerablemente en la disponibilidad y accesibilidad de la información.

Como tercer antecedente, según Atencio (2019) señaló que, el cambio tecnológico y su aplicación en la Dirección General de Informática y Estadística, se ha visto afectada por programas maliciosos e incluso usuarios internos que desconocen de la seguridad informática, por lo que su información está expuesta a riesgos y amenazas que afectarán directamente la transferencia de información en las redes informáticas (datos) de la institución. El tipo de investigación es no experimental, por lo que se recolectó la información en base a encuestas a 8 colaboradores de la dirección general de informática, considerados como la población y muestra. Asimismo, los resultados indicaron que el conocimiento de seguridad de información antes de la aplicación de un SGSI era de un 9.1 %, a lo que posteriormente a la implementación, se obtuvo un 90% debido

a que se crearon la documentación donde se dictaminan las normas de seguridad para la institución. Finalmente, se concluye que al desarrollar un sistema o modelo de gestión en seguridad de la información debe cumplirse el objetivo de reducir la incertidumbre y la complejidad de determinar situaciones de seguridad de la información, asimismo, los activos de información no deben solamente enfocarse en factores que influyen en ella, por lo contrario, también en la administración, análisis de gestión de riesgos, planificación estratégica y cultura organizacional.

Para finalizar, como cuarto antecedente nacional, el autor Solano, (2020) señaló que como realidad problemática la gestión de datos de los registros públicos en la Zona VII – Huaraz, se debe a la falta de equipamiento que resguarde la información y protocolos que garanticen la disponibilidad de esta; por tal identificó el problema general: ¿De qué manera la implementación de los controles de la ISO 27002:2013 favorece a la gestión de la base de datos de los registros públicos? El tipo de investigación se enmarco bajo el carácter de aplicada, siguiendo el diseño experimental, en el tipo de población de estudio se consideró finita con un total de 58 trabajadores entre los profesionales que conforman la empresa, asimismo se consideró la misma cantidad para la muestra. Por lo tanto, los resultados de la investigación que se obtuvo son un 91.7% impacto positivamente la implementación de los controles ISO, por otro lado, la disponibilidad y accesibilidad de la información aumento en un 83.3% y 66.7 %; respectivamente. Finalmente, en conclusiones se indica la importancia de capacitaciones constantes por parte del personal Tecnología e Informática a las áreas administrativas, inspecciones constantes y mantenimientos planificados para evadir daños y perdida de información.

Como parte de las **bases teóricas** que tienen como fin brindar el soporte a las variables de investigación, se optó por utilizar los aportes de Aladra (2015) sobre la teoría de la información al afirmar que, es una disciplina que permite el estudio de los procesos informativos, profesionales y sociales que buscan un solo fin. Además, indica que debemos adaptarnos a diversos puntos enfocados en la interacción y constantes cambios producto de la situación. Siguiendo la línea de la

teoría de la información en relación con la variable independiente que la norma ISO 27001:2013, tiene como fin mejorar los procesos que se presente, disminuyendo costos y control en la seguridad de información.

Los aportes de Von, (2019) menciona que, la teoría general de sistemas tiene la influencia de la búsqueda de elementos, así como también el conocimiento de los procesos internos y externos en búsqueda del mismo fin. Lo mencionado tiene relación con el aporte de (García, 2018), donde afirman que, la teoría de sistemas guarda relación, ya que es integradora y conlleva un proceso lineal con el propósito de obtener un producto adecuado. Se afirma que la teoría de sistemas mantiene una relación con la variable independiente y dependiente, debido a que la norma ISO 27001:2013 se implementará para el control de la seguridad de información, tiene como fin el evitar alguna perdida de información, mejorar el control de la seguridad de información y aumentar la eficacia de los trabajadores en los sucesos de riesgo en la seguridad. Por tanto, la implementación de la norma ISO 27000-2013 tiene como fin evitar pérdidas de información, evitar ciberataques, mejorar el control de la seguridad y aumentar la eficiencia, por lo que todo guarda relación con la base del estudio.

La teoría de control tiene como prioridad proporcionar un enfoque metódico para diseñar controladores estables y evitando desviaciones. Por lo que, se afirma que esta teoría mantiene una relación con la variable control de la seguridad de información porque implementa sistemas controlados y dirigidos de manera autónomo a través, de modelos informáticos que evitan causar errores. Para Fermín (2015) afirman que la teoría de control proporciona un esquema fundamentado para plasmarlo a sistemas controlados y gestionados de manera coordinada bajo la esquematización de modelos de control de seguridad en base a parámetros establecidos, el cual busca integrar todos los temas de seguridad. Toda teorías base conceptualizada vienen a ser el soporte de las variables de estudio, que va a permitir tener una perspectiva amplia y que se basa en el presente estudio sobre el control de la seguridad de información.

Continuando con la estructura de investigación, se procede con los **enfoques teóricos generales**, para ello se definirán los conceptos bases que respaldarán el tema central:

Sistemas: se describen como un conjunto de componentes que se integran entre sí, con la finalidad de cumplir los objetivo a través de soluciones simplificadas y automatizadas. Asimismo, en su mayoría los sistemas son alternativas de problemas empíricos y alternativas poco viables como la manualidad o mecanizada (Fernández, 2006).

Normas técnicas ISO, ITIL y CMMI: para la infraestructura y servicios TI, es necesario contar con los siguientes criterios: alcance, restricciones, partes interesadas, tipo de tecnología de la información, la comunicación y el tipo de organización. Asimismo, son importante su implementación en organizaciones orientadas a servicios TI u Outsourcing y sus dimensiones mayormente se basan en lineamientos para la planificación, diseño, desarrollo, implementación y mejora continua (Vela et al., 2019).

Sistemas de información: se define como la información procesada en el entorno de una aplicación o software, todos los sistemas de información deben ser eficaces para lograr lo que la empresa propone como objetivos y también debe ser eficientes para lograr dichos objetivos bajo la optimización de recursos ya sea tecnológicos, económicos y humanos (Heredero, 2006). Por otro lado, los sistemas de información para su buen desempeño y adecuación a diferentes áreas de una organización dependen de otros softwares y hardware que permiten el almacenamiento adecuado de dicha información (Guachi, 2012).

Seguridad de la información: se conceptualiza a partir del conjunto de procedimientos, medidas, técnicas y herramientas que deben asegurar y reaccionar ante cualquier atentado en contra de la información (Agé, 2013). La seguridad de información según la ISO 27001, cuenta con tres aspectos primordiales enfocados a proteger: la integridad, disponibilidad y la confidencialidad de la información, de igual modo hace mención que toda organización debe clasificar la información en

3 tipos: critica, valiosa y sensible. En base a lo mencionado se podrá establecer las mejores alternativas y prácticas para administrar y salvaguardar la información de una organización (Mendoza, 2016). Finalmente, la adecuación de técnicas y medidas para el resguardo de información es primordial en la actualidad, ya que una organización sin controles en la seguridad de su información se verá vulnerable ante cualquier amenaza o exposición a cualquier riesgo (Solarte, et al., 2015).

Riesgo informático: son catalogados como sucesos en realización a una amenaza de daño que dificulta el logro de las metas de una organización (Silva et al., 2019). Los riesgos informáticos dentro de las organizaciones están divididos en 4 tipos: riesgo a la integridad, acceso, utilidad e infraestructura, a partir de identificación y clasificación será posible la ejecución de una óptima medida para gestionar la seguridad de la información (Téllez, 1988). Asimismo, los riesgos informáticos son afrontados por normativas (ISO) o manuales de buenas prácticas (ITIL) que ayudan a las organizaciones a identificar y analizar las amenazas, para exponer las vulnerabilidades (Aguilera, 2010).

Plúa (2017), en su investigación comenta que la evaluación de riesgos informáticos viene a ser el procedimiento por donde se proceden a identificar cuáles son las vulnerabilidades de la seguridad de información.

Políticas de seguridad informática: se desenvuelven con la finalidad de resguardar los activos informáticos de una organización a partir de la conservación de la integridad, disponibilidad y confidencialidad de la información (Mifsud, 2012). Igualmente, las políticas de seguridad informática no se basan en solo identificar las amenazas a la que se expone una organización, sino también analizar el origen de estas, ya que pueden ser tanto externas como internas (Sánchez, 2007). No obstante, la documentación donde se establecen las políticas de seguridad informática debe ser dinámica, puesto que se ajustará y mejorará constantemente según a las condiciones donde fueron desarrolladas (Ladino, et al., 2011).

Normas de seguridad informática: son estándares confiables, los cuales son supervisados por el equipo TI de una organización; estas normas son

conformadas por un conjunto de documentos legales y técnicos donde se establecen los lineamientos respectivos para su cumplimiento (Borbón, 2011).

Activos de información: son los recursos relacionados para la preparación, archivamiento, gestión o transmisión de la información, a partir de ello se pueden distinguir dos tipos de activos de información: activos primarios, donde se incluye los procesos comerciales de la organización; y lo activos de apoyo donde se incluye el hardware (dispositivos periféricos), software (sistemas operativos y aplicaciones) y personas (usuarios y clientes) (Bermúdez, 2015).

Amenaza informática: es toda ejecución de acciones o elementos que logran atentar contra la seguridad de la información, estas en su mayoría se deben a la vulnerabilidad en servicios o sistemas informáticos (Chamorro, 2015).

Vulnerabilidad informática: Es el resultado de la materialización o probabilidad de desarrollo de las amenazas de información (Silva et al., 2019).

De acuerdo con las descripciones mencionadas anteriormente, se continuará con los **enfoques teóricos específicos,** en los cuales se señalarán las definiciones puntuales del desarrollo de la investigación:

Sistema de gestión de seguridad de la información: también conocido abreviadamente como SGSI, es considerado como un proceso de mejora continua principalmente de los controles de seguridad de la información, y está sujeta a soportar cambios en los procesos que la organización defina. Asimismo, dentro de su alcance es mantener protegida la información a partir de su confidencialidad, integridad y disponibilidad (López y Zamora 2015). La implementación de un SGSI permitirá entender los riesgos al cual está expuesta la información y los sistemas que la controlan; con ello también se tendrá la documentación correspondiente la cual será legible para todo el personal que pertenece a la organización (Figueroa, et al., 2017). Dentro de los beneficios de la implementación de un SGSI se tiene que: la organización enseñará las medidas requeridas y tomadas para la protección de información, además apoyará en la toma de decisiones a partir de datos

estadísticos, aumentando así la credibilidad de mejora para la alta dirección, finalmente con la implementación se tiene opciones en la integración con diversas certificaciones a futuro como la ISO 9001, 14001 y OHSAS 18001 (Castillo, 2022).

ISO: sus siglas significan “Organización Internacional de Normalización”, dentro de sus principales objetivos es ayudar a las organizaciones en su eficacia y eficiencia de sus procesos internos y externos (Charlet, 2017).

Norma ISO 27001: internacionalmente es la norma más usada para la implementación de un SGSI, actualmente la versión más usada a nivel latinoamericano es la ISO 27001:2013, ya que se puede prevenir riesgos y mejorar los procesos de información de la organización (Russell, 2022).

Vásquez (2020), conceptualiza que la ISO 27001, se basa en describir cómo se gestiona la seguridad de información en una organización.

La estructuración de la norma ISO 27001:2013 está basada en las 11 cláusulas del ciclo de Deming (Figura 1).

Figura 1

Estructura Norma ISO/IEC 27001:2013

Nota: Córdoba (2021)

Para Córdova (2021), las cláusulas mencionadas, tienen la siguiente definición: introducción que fundamenta la consistencia de la norma internacional y que una vez establecido podrá implementarse, mantener y mejorar constantemente un SGSI; el alcance es un estándar aplicable a cualquier organización; las normas para consulta permiten la verificación del estándar general 27001:2013; los términos y definiciones también se verifican en base al estándar general y el contexto de la organización permite enfocarse en los lineamientos y perspectivas de la organización. Además, el área de planificación involucra: el liderazgo sujeto a la alta directiva de la organización para definir el SGSI como proceso estratégico; la planificación regula el desarrollo de la SGSI, gestiona riesgos y se basa en el cumplimiento e identificación de problemas y el soporte hace referencia a medios importantes con el fin de lograr un éxito de la SGSI en la organización. Asimismo, en la operación (hacer) deberá implementarse la SGSI basándose en el funcionamiento de la entidad; la evaluación de desempeño (comprobar) indica un análisis comparativo entre metas y objetivos del SGSI y la mejora (actuar) que describe los mejores métodos de mejora continua en base a la norma. Finalmente, es importante indicar que la implementación de la norma ISO 27001:2013 tiene pasos que se deben cumplir para alcanzar un adecuado SGSI en la organización, lo cual permite que la empresa lleve un mejor control de seguridad de la información, evitando errores.

Según Russell (2022) la norma ISO 27001:2013, indica las siguientes ventajas competitivas: resolver los diferentes riesgos de la seguridad de información, ejecutar las acciones preventivas necesarias, garantizar una gestión eficiente en la seguridad de la información y permitir las integraciones de otros modelos de sistemas de gestión más simplificadas.

Para Lema y Donoso (2021), la versión 2013 se divide en 14 dominios, 35 objetivos de control y 114 controles: la política de seguridad de la información permite a la organización a disponer reglamentos pertinentes; la organización de la seguridad de la información indica la coordinación de la implementación y operacionalización en la seguridad de la información; la seguridad de los recursos humanos busca que los trabajadores y clientes deben entender su nivel

de responsabilidad para el puesto elegido; la gestión de activos debe conocer los activos de información, para su correcta administración y adecuada protección. Además, Mamani (2020), menciona que el control de acceso permite resguardar el acceso de información para que el personal visualice la información que solo requiera; la criptografía asegura el uso efectivo de la confidencialidad y autenticidad de información; la seguridad física y ambiental permite la prevención física sin autorización y al no permiso del procesamiento de la información.

La seguridad en las operaciones asegura el uso correcto y el buen funcionamiento de los equipos de procesamiento de la información; la seguridad de las comunicaciones respalda la protección de información y los equipos que la soportan en la red de la organización, la adquisición, desarrollo y mantenimiento de sistemas permite garantizar la seguridad informática considerado el ciclo de vida de sistemas de información; las relaciones con los proveedores permite proteger los activos valiosos de la organización a los que los proveedores pueden acceder o en los que pueden influir.

Por último, la gestión de incidentes de seguridad de la información plantea resguardar un carácter lógico y eficiente para el ciclo de incidentes, sucesos y vulnerabilidades; todo aspecto con respecto a la seguridad de información en relación a todas las actividades que se relación para alcanzar el proceso de gestión y continuidad de un negocio se plasmará en la seguridad de información de los sistemas o medios de gestión para garantizar la mejora continua de la organización y la conformidad en donde se evita la omisión de los términos legales y reglamentos pactados respecto a la seguridad de la información. Finalmente, es importante indicar que, al implementarse estas normas en la organización, esta deberá contar con una estructura y reglamento propio, por lo que estos pasos son pertinentes en base a la seguridad de información del cliente y de la empresa.

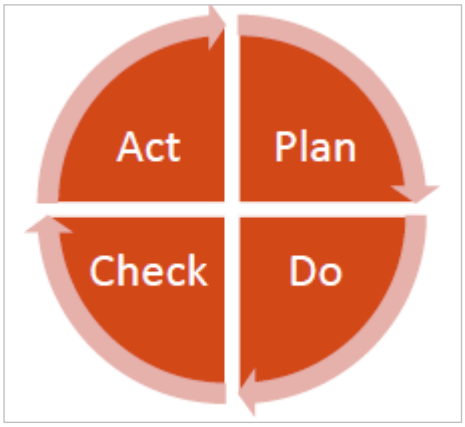
Ciclo de deming: también conocido como PDCA o PHVA, es una metodología conformada por cuatro fases: las cuales son: P- Planificar, H-Hace, V – Verificar y A – Actuar (Córdova, 2021).

Espinoza (2013), menciona que el ciclo de Deming considera las cuatro etapas que vienen a ser planear, hacer, verificar y actuar, comenta que de acuerdo con una investigación se puede hacer uso de 2 etapas o más.

Rodríguez (2021), en su investigación realizada, refuerza este concepto al mencionar que cuando se implementa un SGSI bajo la ISO 27001 es necesario usar una metodología que tenga una evolución constante y continua.

Figura 2

Fases de la metodología ciclo de deming



Nota: PDCA (2020)

Dentro de las definiciones de las fases del ciclo de Deming, la norma ISO ya planteó la fase de planificación para su implementación por tal razón, las etapas se conceptualizan de la siguiente manera:

Planificar: incluye toda la creación de objetivos y procesos necesarios para lograr los óptimos resultados requeridos por la organización; también incluye el análisis interno y externo del contexto de la organización para su futura mejora. Asimismo, van a permitir a la organización tener un control autónomo con el fin de realizar un análisis minucioso y poder obtener resultados positivos para el bienestar de la empresa (Córdova, 2021).

Hacer: la ISO 27001:2013 indica que la organización debe implementar los procesos importantes y controlarlos a partir del cumplimiento de los objetivos centrales de la seguridad a través del tratamiento de riesgos de la seguridad de la información. Además, implica que en base al conocimiento de riesgos de seguridad se implementen métodos y normas para prevención de ciberataques y perdida parcial o total de información clasificada (García, 2018).

Verificar: En el capítulo 9 de la ISO 27001:2013, señala que la evaluación periódica del desarrollo de la seguridad de la información es importante para garantizar la eficacia del SGSI. Asimismo, es importante destacar que llevar a cabo la implementación de la norma ISO 27001:2013 va a permitir tener una mayor influencia en el control de seguridad (Córdova, 2021).

Actuar: Se pretende prevenir circunstancias no deseadas, para así mejorar la ejecución del SGSI a través de acciones innovadores y correctivas. Así pues, es importante indicar que el control de la seguridad de la información busca resguardar toda la información propia de la organización (García, 2018).

Finalmente, para la argumentación correspondiente a las dimensiones de la variable, se definirán las dimensiones correspondientes:

Para la variable independiente; implementación de Norma ISO 27001:2013, según el manual de apoyo ISO 27001:2013, referenciado señala que es una norma basada en la seguridad y la información que se requiera asegurar la confidencialidad. Asimismo, el plasmar esta norma permite disponibilidad de la información en la organización y de los sistemas, lo cual será de gran importancia en la entidad (Córdova, 2021).

Planificación: comprende los contextos de la organización, donde se define los alcances del SGSI; liderazgo, donde se establece roles y responsabilidades para la seguridad de la información; planificación, donde se realiza el plan de tratamientos de riesgos; apoyo, donde se verifica la disponibilidad de la documentación y concientización de las nuevas medidas adoptadas. Además, la

planificación en la organización va a permitir tener un orden en la secuencia a seguir y así evitar riesgos (Cardona y Restrepo, 2020).

Ejecución: señala el funcionamiento para la implementación de evaluación y tratamiento de riesgos. Asimismo, se vera la ejecución luego de plasmar la norma ISO 27001:2013, en base a los puntos establecidos el control de la seguridad de información estará mejor implementada (Fermín, 2015).

Verificación: indica los requerimientos para evaluar y analizar los objetivos de la organización. Además, se indica que deberán ser constantemente evaluados y verificados los ítems necesarios para cumplir con el control de la seguridad de información (Cardona y Restrepo, 2020).

Mejora continua: define los requerimientos para las correcciones necesarias para un avance innovador. Es decir, se deberán subsanar los errores cometidos y llegar a mejorarlos para el correcto funcionamiento de la organización (Córdova, 2021).

Por otro lado, en la variable dependiente; control de seguridad de la información, según Mejía (2020), se define como las medidas o procedimientos dedicados a resguardar toda la información con la finalidad de asegurar la continuidad de una organización; no obstante, señala 4 soportes primordiales para la información. Ante lo mencionado serán consideradas las presentes características como dimensiones para la presente investigación.

Disponibilidad: Es la respuesta de los recursos actos para mostrar la información, a quien este autorizado y tenga la facultad de administrarlo. Sin embargo, se indica que todo el personal encargado debe estar capacitado y así poder prevenir errores para la entidad (Mejía, 2020).

Adaptabilidad: Refiere a las condiciones como la capacidad y espacio que debe someterse la información para incorporarse a nuevas alternativas. Además,

se deberá tener el espacio adecuado para almacenar la información y así poder tener un resguardo en caso este se vea afectado (Mejía, 2020).

Accesibilidad: Se basa en el tiempo de respuesta al que está sometida la información, este debe ser inmediato y sostenible a pesar de que exista mayor volumen de información. Sin embargo, ante un evento de riesgo es imperativo que el tiempo de acción o recuperación sea el menor posible con el fin de evitar malestar en el usuario y en la empresa (Mejía, 2020).

Resguardo: Congrega desde la frecuencia, capacidad, privilegios y entorno en que se debe realizar una copia de la información. Así mismo, tener un resguardo de la información total de la empresa sería un soporte vital, porque evitará perder parcial o totalmente información clasificada (Mejía, 2020).

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

La investigación es de tipo aplicada, mientras que la básica es empleado para el desarrollo de nuevos conocimientos, mientras que la investigación aplicada, también llamada investigación tecnológica, permite mejorar o perfeccionar el funcionamiento de lo ya existente, como son los sistemas, reglas, procesos o reglas; asimismo permite calificar la solución de la problemática basándose en ver si es eficaz o ineficaz, eficiente o deficiente y no en respuestas simples como sí, no o probable (Hernández et al., 2018).

Para el enfoque de investigación la actual investigación es de naturaleza cuantitativa porque las variables deben ser observable y medibles, asimismo el proceso va, de lo general a lo especifico, permitiendo dividir las variables en partes según las dimensiones medidas (Arias, 2021).

El diseño de investigación fue preexperimental ya que las variables son manipulables y se verificara la causalidad una de otra, además se usó el tipo transversal ya que se realizó la manipulación de variables en un mismo momento (Hernández et al., 2018); por último, se precisa que la investigación fue correlacional ya que implican la manipulación de la variable independiente y los efectos que puedan que este generar sobre la variable dependiente, por tal se usara el siguiente esquema de investigación:

GRe = O1 X O 2

Donde van a indicar los diferentes ítems para el esquema de la investigación: el GRe (grupo experimental) se indica para el control de seguridad informática; el O1 (prueba Pretest) son los valores de los indicadores medidos (antes de la implementación); el X (condición) es la implementación de la ISO 27001:2013 y el O2 (post-test) son los valores de los indicadores medidos después de la implementación (Hernández et al, 2018).

3.2 Variables y operacionalización

Variable independiente: norma ISO 27001:2013.

Definición conceptual: se centra como guía de buenas prácticas para el desarrollo y ejecución de procedimientos que regularan la seguridad de la información contra diferentes amenazas; además, con su implementación se podrá garantizar la estabilidad, competitividad y oportunidad en el mercado empresarial (Silva et al, 2019)

Definición operacional: es la ejecución de los términos relacionados a la seguridad informática con relación a la empresa, ya que a partir de ello se diseñará un plan de trabajo aplicado a la consultoría privada.

Indicadores: según Silva et al., (2019) la estructura de norma ISO 27001:2013, cuenta con 10 clausulas, de las cuales desde la cláusula 5 a 10 cuentan con dimensiones relacionadas.

Tabla 1

Variable independiente

Dimensión	Indicadores
Planificación	Liderazgo
	Planificación
	Soporte
Ejecución	Operación
Verificación	Evaluación del desempeño
Mejoramiento	Mejora - continuidad

Escala de medición: debido a que la variable independiente es de tipo cuantitativa, se aplicara la escala Likert, donde cada indicador expresa solo una cualidad según su existencia: no existe, inicio, en desarrollo y completada.

Variable dependiente: control de seguridad de información.

Definición conceptual: tiene como propósito la protección de todos los activos que involucren la información de la empresa, esto comprende desde los sistemas, aplicaciones, infraestructura, datos y equipos; para garantizar y minimizar costos ante posibles daños por alguna amenaza se requiere establecer políticas y planes de seguridad TI (Silva et al., 2019).

Definición operacional: es la protección de la información, a partir de las buenas prácticas establecidas por algunas metodologías o normas ya establecidas en el campo de seguridad TI.

Indicadores: según Mejía (2020); se basa en las dimensiones de disponibilidad, adaptabilidad, accesibilidad y resguardo, actualmente estas cuentan con características las cuales permiten su medición.

Tabla 2

Variable dependiente

Dimensión	Indicadores
Disponibilidad	Tiempos de acceso
	Tipos de acceso
	Políticas de acceso
Adaptabilidad	Crecimiento de información
	Adaptación de nuevas tecnologías
	Espacio disponible
Accesibilidad	Capacidad de almacenamiento físico
	Acceso a consultas
	Tiempo de respuesta
Resguardo	Respaldo de seguridad
	Almacenamiento del respaldo de seguridad
	Acceso al respaldo de seguridad
	Seguridad física

Escala de medición: debido a que la variable dependiente es de tipo cuantitativa, se aplicará la escala de Likert, donde cada indicador expresa solo una cualidad según su experiencia en uso: nunca, casi nunca, a veces, casi siempre y siempre.

3.3 Población, muestra y muestreo

Población: para Arias (2021), se considera como el conjunto finito o infinito de actores bajo características semejantes, la población se encuentra constituida por un total de 78 trabajadores que laboran en la consultoría privada ver tabla 1, además que tengan estos criterios de selección:

Criterios de selección

Criterios de inclusión: Todos los profesionales (técnicos y titulados) que acepten participar en el estudio.

Criterios de exclusión: Todos los no profesionales (técnicos y titulados) que no han sido participes en el estudio.

Muestra: según Arias (2021) señala que, si una población (N) es pequeña o reducida, se permite considerar en su totalidad para la muestra; por tal, En vista que la población es de 78 trabajadores, se considera el total de este para la muestra.

De acuerdo con Mucha et al (2021), la muestra es una parte del universo de datos, para calcular estos datos se sigue procedimientos a través de fórmulas estadísticas.

Muestreo: para Arias (2021), se considera como una técnica, la cual permite estudiar a la muestra, para su distribución esta puede ser probabilístico y no probabilístico; El presente estudio es probabilístico aleatorio simple.

3.4 Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos: Para el planteamiento del presente estudio no se requiere considerar técnicas expertas o más recientes, para ello se considerará

la más apropiada para la variable dependiente Arias (2021). Es importante indicar que se utilizara la observación como parte de la técnica de estudio, por lo que las variables deben estar conceptualizadas y evaluadas antes de iniciar la recolección de datos.

Instrumento: La encuesta como técnica permite la recopilación de datos entrevistando a los encuestados para proporcionar la información necesaria para una investigación. Arias (2021). Es decir, es una técnica comúnmente utilizada en las ciencias sociales, y con el tiempo se ha expandido a la investigación científica. Por lo que, es importante mencionar que es un instrumento que logra adquirir resultados con datos observables que el investigador tiene pensado, y se obtiene a través de los indicadores establecidos por cada dimensión de la variable de estudio.

Se deben cumplir los siguientes criterios para seleccionar las encuestas como un método entre los métodos cuantitativos, según Hernández, et al., (2018) la encuesta deberá incluir: las dimensiones de la variable y pregunta de investigación; el instrumento debe tener criterios de confiabilidad y validez para ser usado. Además, debe siempre plantearse preguntas abiertas y deben ser segmentadas a partir de conceptos sólidos. Por último, los resultados de la encuesta siempre terminan con tabla de frecuencias; además, debe usar estadísticas descriptivas e inferenciales para revelar resultados.

Una encuesta es una pregunta que un investigador hace por escrito u oralmente a una parte de la población, conocida como muestra de población, para obtener información sobre lo que está estudiando (Caballero, 2021).

Instrumentos para la recolección de datos: ante la definición de encuesta, el cuestionario es el instrumento para la recolección de datos.

Cuestionario: Este tipo de instrumento tiene un conjunto de interrogantes que se enumeran en formatos con múltiples alternativas para sus respuestas

posibles para la persona que es encuestada, así mismo se debe tener presente que no existe respuesta correcta o incorrecta, toda respuesta realizada produce diferentes resultados (Arias, 2021).

Los resultados de un cuestionario conducen siempre a la verificación de las hipótesis planteadas previamente por el investigador y una de sus principales características es que ésta se encuentre estandarizada y todas las preguntas sean dirigidas a un único objetivo.

El tipo de cuestionario a usar será el **politómico,** debido a que utiliza la escala de Likert, y se tiene de tres a más opciones.

Validez y confiabilidad de los instrumentos

Para, Arias (2021). la validación de un instrumento se refiere cuando este puede medir el valor de la variable, a partir de la validación se puede determinar si el instrumento es confiable o no.

Para el presente contexto de la investigación, se hizo la validación del instrumento por cada variable, a partir de los juicios de 03 profesionales.

La presente tabla 3 se visualiza la concordancia de los expertos consideraron que para su aprobación de las dimensiones deben oscilar entre “Desarrollo” y “Completado” ya que se estaría implementando la ISO 27001:2013.

Tabla 3

Validez del instrumento para las dimensiones de la variable dependiente

Experto	Controles para el instrumento de medición				Condición
	No existe	Inicio	Desarrollo	Completado	
Dr. Marlon Frank Acuña Benites	-	-	x	x	Aplicable
Mg. Giancarlo Sánchez Atuncar	-	-	x	x	Aplicable
Mg. Juan Orlando Pérez Alvarado	-	-	x	x	Aplicable

Fuente: Consultora SYSLCI

En la tabla 3 se visualiza la evaluación de expertos que se realizó para el presente estudio, se puede observar que los tres expertos han considerado la condición como aplicable en lo que respecta la medición de instrumentos, así como también se muestra la concordancia que han tenido los expertos ya que han considerado que para la aprobación de las dimensiones estos deben oscilar entre " casi siempre" y " siempre", debido a que de esta manera existirá un control adecuado en lo que respecta a la seguridad de información.

Tabla 4

Validez del instrumento para los dimensiones de la variable independiente

Experto	Controles para el instrumento de medición					Condición
	Nunca	Casi Nunca	A Veces	Casi Siempre	Siempre	
Dr. Marlon Frank Acuña Benites	-	-	-	x	x	Aplicable
Mg. Giancarlo Sánchez Atuncar	-	-	-	x	x	Aplicable
Mg. Juan Orlando Pérez Alvarado	-	-	-	x	x	Aplicable

Fuente: Consultora SYSLCI

Según, Arias (2021) en referencia a la confiabilidad del instrumento, es el nivel en que el mismo objeto medido genera el mismo resultado.

Para Villavicencio et al (2019) la confiabilidad viene a ser la capacidad por el cual se repite una medida bajo las mismas condiciones.

En la actual investigación, se considera confiable el instrumento empleado ya que los 03 expertos se asemejan a un mismo resultado, asimismo se afianzará dicha confiabilidad a partir de la evaluación del coeficiente en el alfa de Cronbach, en el software de estadística SPSS 25.

Tabla 5

Escala de confiablidad

Escalabilidad	Nivel de confiabilidad
< a 0.9	Muy aceptable
Entre 0.8 a 0.89	Aceptable
Entre 0.7 a 0.79	Baja
> a 0.69	Inaceptable

Fuente: Arias (2021)

3.5 Procedimientos

La presente investigación realizó los siguientes procedimientos:

Se inicia realizando el procedimiento para recolectar los datos por parte de los especialistas de la empresa, entre ellos auditores, gerentes y personal administrativo de la consultora privada SYSLCI, además se explicaron los objetivos alcanzados por el trabajo de investigación. las dimensiones e indicadores utilizados para cada una de las variables identificadas y cómo se alinean con el tema central de los controles de seguridad de la información.

Después de obtener el consentimiento de los consultores, se planificaron las actividades a realizar, se definieron cuáles serán las herramientas de recopilación de datos y se definió el software para procesar los datos recopilados.

Luego se procedió a formular los objetivos de la investigación, se procede a buscar y revisar las referencias bibliográficas que sustentaran la respuesta de la investigación.

Posteriormente de la aprobación de los expertos, se realizó una encuesta virtual entre los profesionales, utilizando herramientas de medición de variables,

siendo todos los datos recopilados ingresado en el software estadístico SPSS Statistics 23.0 para luego ser tratados estadísticamente.

Finalmente, se procedió a evaluar los datos que han sido obtenidos y en razón a ello se procedió con la elaboración de los cuadros para ser explicados evaluando las hipótesis establecidas en el trabajo de investigación.

3.6 Método de análisis de datos

Los instrumentos utilizados para el trabajo de investigación fueron aprobados por los expertos para confirmar la confiabilidad, además de determinar si el instrumento es confiable y confiable se determinó el Alfa de Cronbach (Tuapanta, 2017).

El valor mínimo aceptable para el coeficiente alfa de Cronbach es 0,7; por debajo de este valor la consistencia interna de la escala utilizada es mínima (Tuapanta, 2017).

El presente estudio de investigación utiliza un enfoque cuantitativo, el uso de herramientas de recolección de datos y la determinación de la validez de las hipótesis específicas de cada indicador.

Se utiliza el uso de estadística descriptiva para determinar niveles, además del uso de estadística inferencial para comparar hipótesis dadas por estimaciones de parámetros (Wang et al., 2019).

3.7 Aspectos éticos

Este estudio es de mi autoría, ya que el proceso de realizar la recolección, el procesamiento e interpretación los datos fue realizada bajo criterio e interpretación, las fuentes bibliográficas utilizadas en el estudio se citan de acuerdo con los estándares de la American Psychological Association (APA) 7ma Edición. Además, la presente tesis de investigación es evaluado dentro del programa “Turnitin” para la elaboración de un informe original con base en la Resolución de Investigación de la Vicerrectoría N° 008-2017-VI/UCV. Asimismo, se han seguido las instrucciones

solicitadas por la Universidad Cesar Vallejo según Acuerdo Rectoral N° 0089-2019/UCV.

Por último, se utilizaron cuestionarios para recopilar datos como parte de un cuestionario para profesionales de la consultoría bajo la aprobación de la gerencia general de SYSLCI.

3.8. Metodología de desarrollo para la implementación de la ISO 27001

Se utilizó la metodología Deming, se pone de conocimiento que la ISO 27001 no refiere ni sugiere que tipo de metodología se debe de usar, sin embargo, este tipo de metodología se adapta a las normas para realizar un sistema de gestión de seguridad de información. Este tipo de metodología permitió enfocar las fases de planificar, hacer, verificar y actuar en el presente estudio, con la finalidad de alcanzar la mejora continua de los procedimientos que la empresa ya cuenta, se ha establecido una lista de políticas de seguridad que la empresa adopte para cumplir los requisitos de una ISO 27001 (ver anexo 4).

IV. RESULTADOS

4.1 Estadística descriptiva.

Se realizó el cálculo de los estadísticos descriptivos e inferencial para las 4 dimensiones con respecto al control en la seguridad de información. Las dimensiones analizadas son los siguientes: la disponibilidad de la información, la adaptabilidad de información, accesibilidad de la información, resguardo de la información. A continuación, se procede a describir la estadística descriptiva e inferencial.

Tabla 6

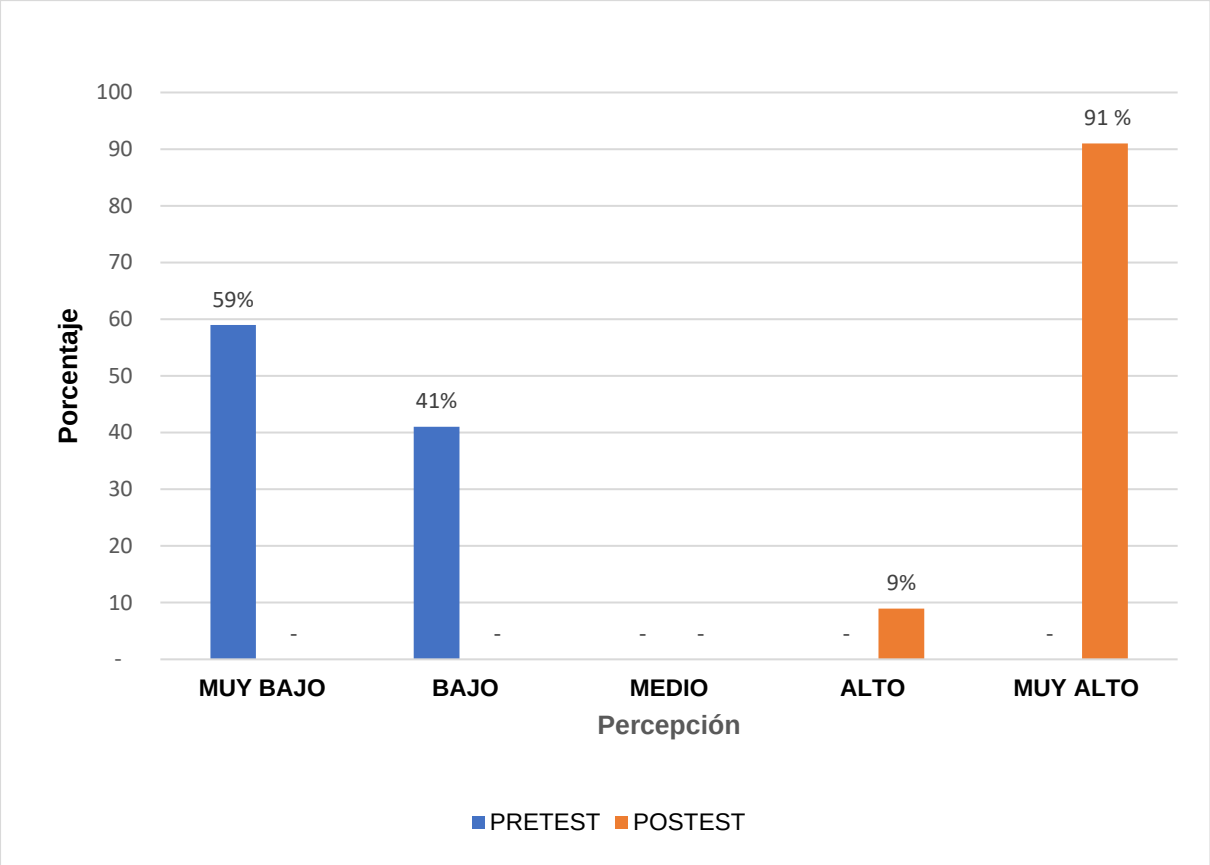
Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desviación estándar
Disponibilidad Pre	78	,00	25,00	13,0385	6,40504
Disponibilidad Post	78	75,00	100,00	87,3718	6,50496
Adaptabilidad Pre	78	,00	25,00	12,5641	5,90749
Adaptabilidad Post	78	75,00	100,00	87,6923	6,38038
Accesibilidad Pre	78	,00	25,00	12,9487	6,04936
Accesibilidad Post	78	75,00	100,00	87,8462	7,15882
Resguardo Pre	78	,00	20,00	,3205	2,30467
Resguardo Post	78	75,00	95,00	87,3718	5,07888
N válido (por lista)	78				

Se visualiza en la tabla 6 el valor de las medias de las cuatro dimensiones analizadas, se puede evidenciar que en las cuatro dimensiones se mejoró el control de seguridad de información, por lo tanto, existe una mejora entre pre-test y post-test.

Figura 3

Disponibilidad de la información (Dimensión 1)



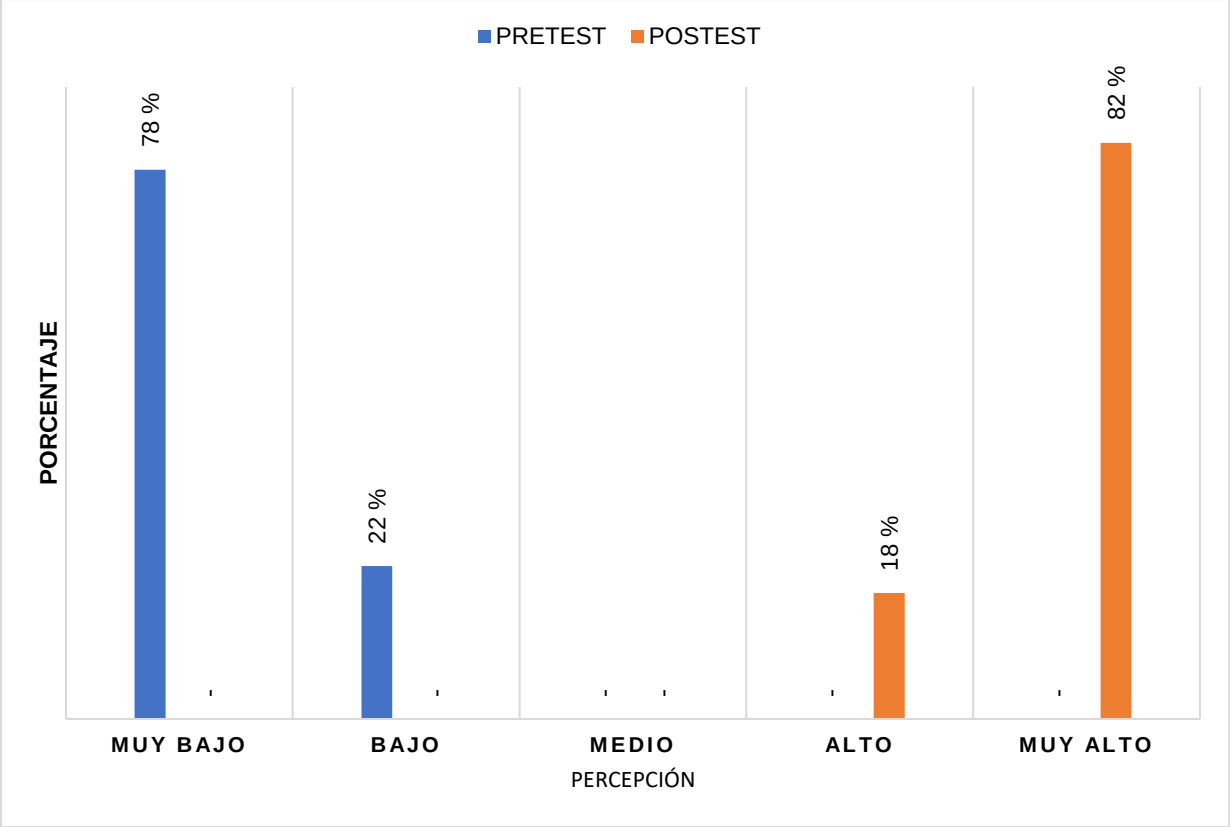
En la figura 3; se puede comprobar que antes de la implementación de la

Fuente: elaboración propia

ISO 27001:2013, un 59 % obtuvo una percepción “Muy bajo” y un 41% obtuvo la percepción de “Bajo” referente a la disponibilidad de información para control de seguridad de información; por otro lado, después de la implementación de la ISO 27001:2013, se obtuvo un 91% de percepción de mejora considera “Muy Alto” en el control de seguridad de información y un 9 % consideró “Alto”. Por consiguiente, se afirma que al aplicar la ISO 2701:2013 la disponibilidad de información con la que cuenta la empresa ha sido más que la esperada, ahora los usuarios con privilegios en el sistema de gestión podrán conocer de forma segura la información existente en la empresa.

Figura 4

Adaptabilidad de la información (Dimensión 2)



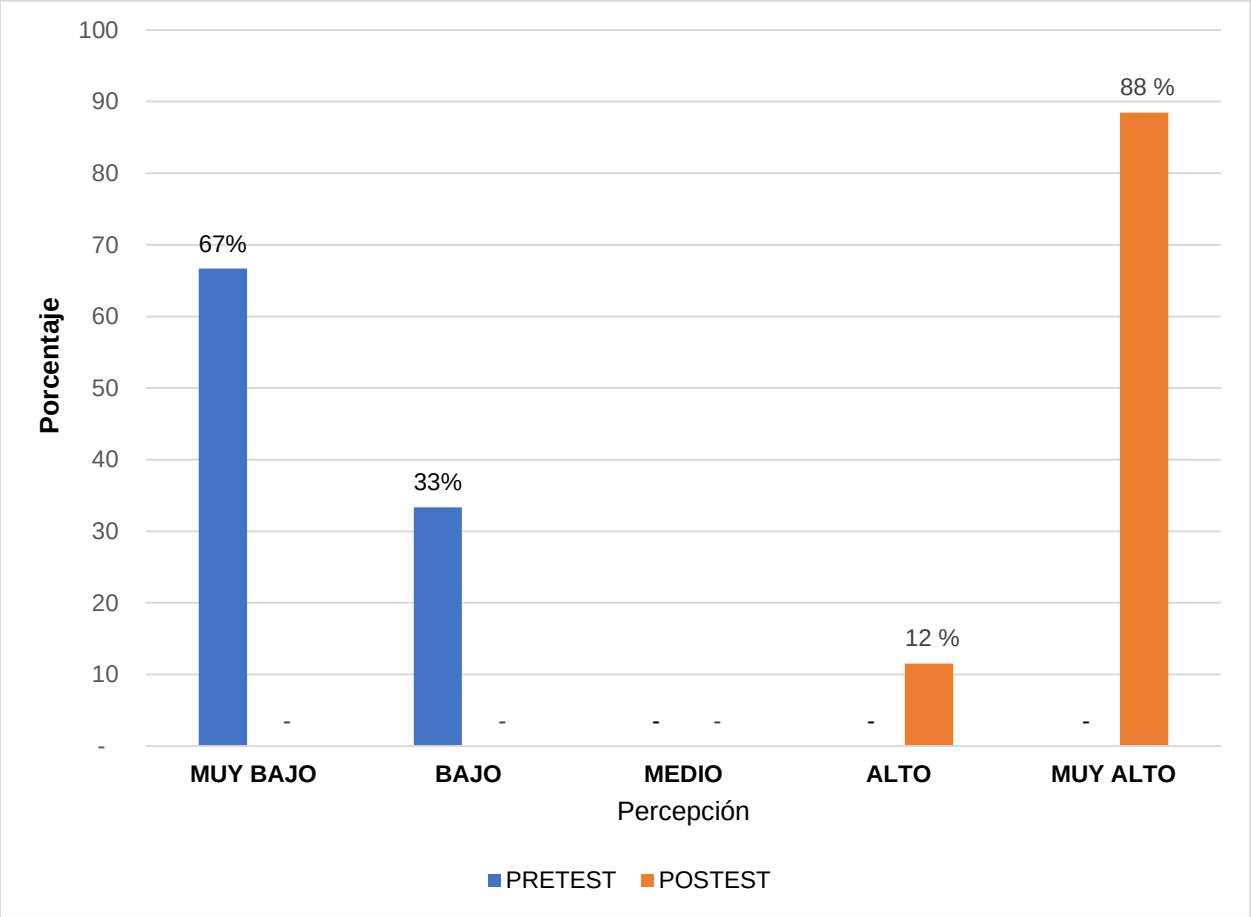
Fuente: elaboración propia

En la figura 4; se puede comprobar que antes de la implementación de la ISO 27001:2013, un 78 % obtuvo una percepción “Muy bajo” y 22% la percepción de “Bajo” referente a la adaptabilidad de la información para el control de seguridad de información; por otro lado, después de la implementación de la ISO 27001:2013, se obtuvo un 82% de percepción mejora “Muy Alto” en el control de seguridad de información y un 18% consideró “Alto”.

De acuerdo al análisis realizado se afirma que gracias a la implementación de la ISO 27001:2013, la empresa al tener una adaptabilidad de información consistente está se encuentra preparada para cualquier tipo de cambio que ocurra en el tiempo, por consiguiente, responderá al cambio de forma flexible.

Figura 5

Accesibilidad de la información (Dimensión 3)



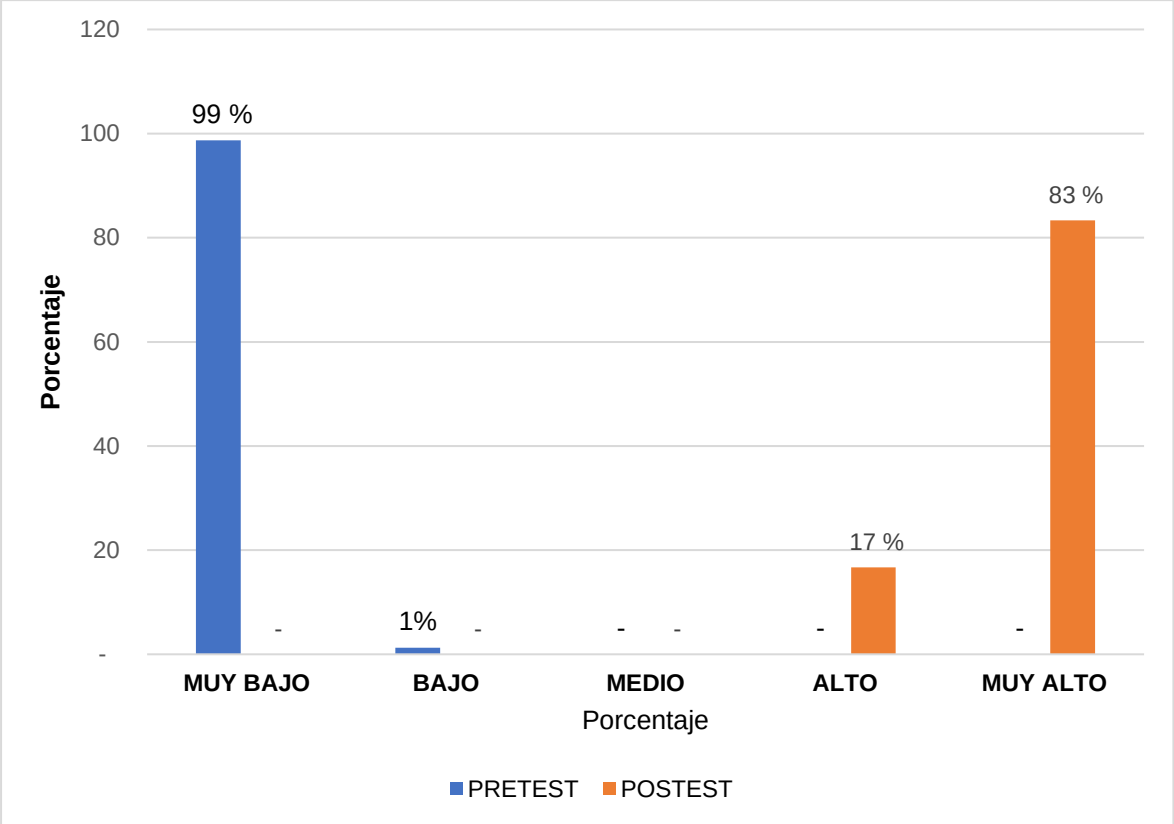
Fuente: elaboración propia

En la figura 5; se puede comprobar que antes de la implementación de la ISO 27001:2013, un 67 % obtuvo una percepción “Muy bajo” y 33 % la percepción de “Bajo” referente a la accesibilidad de la información para control de seguridad de información; por otro lado, después de la implementación de la ISO 27001:2013, se obtuvo un 88 % de percepción mejora “Muy Alto” en el control de seguridad de información y un 12 % consideró “Alto”.

De los datos analizados se concluye que debido a la implementación de la ISO 27001:2013 la empresa mejoró considerablemente la accesibilidad de su información, esto debido gracias que se realizaron controles de seguridad tales como encriptación de datos, contraseñas seguras y usuarios con privilegios para obtener información de la empresa.

Figura 6

Resguardo de la información (Dimensión 4)



Fuente: elaboración propia

En la figura 6; se puede comprobar que antes de la implementación de la ISO 27001:2013, un 99 % obtuvo una percepción “Muy bajo” y 1 % la percepción de “Bajo” referente al resguardo de la información para el control de seguridad de información; por otro lado, después de la implementación de la ISO 27001:2013, se obtuvo un 83 % de percepción mejora “Muy Alto” en el control de seguridad de información y un 17 % consideró “Alto”.

Se concluye de acuerdo con lo datos analizados que gracias a la implementación de la ISO 27001:2013, la empresa mejoró el resguardo de la información, esto debido a que ahora la empresa realiza copias de seguridad de la información periódicamente, las copias de respaldo se están guardando en discos duros con copia a espacios en la nube.

4.2 Prueba de normalidad:

La variable dependiente control de seguridad de información en la presente investigación cuenta con 4 dimensiones específicas, por tal se obtendrá los resultados correspondientes de cada una de ellas, también es preciso señalar que se entiende por:

Ho: Hipótesis nula

Ha: Hipótesis alternativa, entonces para:

Hipótesis general: La norma ISO 27001:2013 mejorará el control de seguridad de información en la consultoría privada.

Prueba de normalidad

Ho = El control de seguridad de información tiene distribución normal

Ha = El control de seguridad de información no tiene distribución normal

Para el cálculo de la prueba de normalidad de la hipótesis general, se usaron los datos recopilados del control de seguridad de información, pre-test y post-test implementación de la ISO 27001.

Tabla 7

Pruebas de normalidad hipótesis general

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Control de seguridad de la información Pre	,153	78	,000	,973	78	,097
Control de seguridad de la información Post	,089	78	,200*	,978	78	,207

En la tabla 7, se puede evidenciar que se usaron 78 grados de libertad (gl), por tal; este al ser mayor a 30 se empleó la prueba de Kolmogorov-Smirnov. Asimismo, al tener un nivel de significancia (Sig.) inferior a 0.05 y otro mayor a 0.05, se procede a rechazar la Ho; es decir, el control de seguridad de información no

sigue una distribución normal y se requiere un análisis no paramétrico bajo la prueba estadística de rangos wilcoxon.

Hipótesis específica 1: La norma ISO 27001:2013 gestiona correctamente la disponibilidad de la información para el control de seguridad de información.

Prueba de normalidad

Ho = La disponibilidad de información tiene distribución normal

Ha = La disponibilidad de información no tiene distribución normal

Para el cálculo de la prueba de normalidad de la hipótesis 1, se usaron los datos recopilados de la dimensión “disponibilidad” de información pre y post implementación de la ISO 27001.

Tabla 8

Pruebas de normalidad Hipótesis específica 1

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Disponibilidad Pre	,234	78	,000	,866	78	,000
Disponibilidad Post	,218	78	,000	,899	78	,000

gl= Grados de Libertad

Sig. = P = Significancia

En la tabla 8, se puede evidenciar se usaron 78 grados de libertad (gl), por tal; este al ser mayor a 30 se empleó la prueba de Kolmogorov-Smirnov. Asimismo, los niveles de la significancia (Sig.) son menores a 0.05, por lo que se procede a rechazar la Ho; es decir la “Disponibilidad” de la información no sigue una distribución normal y se requiere un análisis no paramétrico bajo la prueba estadística de rangos de wilcoxon.

Hipótesis específica 2: La norma ISO 27001:2013 gestiona correctamente la adaptación de la información para el control de seguridad de información

Prueba de normalidad

Ho = La adaptabilidad de información tiene distribución normal

Ha = La adaptabilidad de información no tiene distribución normal

Para el cálculo de la prueba de normalidad de la hipótesis 2, se usaron los datos recopilados de la dimensión “adaptabilidad” de información pre-test y post-tes implementación de la ISO 27001.

Tabla 9

Pruebas de normalidad Hipótesis específica 2

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Adaptabilidad Pre	,186	78	,000	,929	78	,000
Adaptabilidad Post	,163	78	,000	,932	78	,000

En la tabla 9, se puede evidenciar se usaron 78 grados de libertad (gl), por tal; este al ser mayor a 30 se empleó la prueba de Kolmogorov-Smirnov. Asimismo, los niveles de la significancia (Sig.) son menores a 0.05, por lo que se procede a rechazar la Ho; es decir la “Adaptabilidad” de la información no sigue una distribución normal y se requiere un análisis no paramétrico bajo la prueba estadística de rangos de wilcoxon.

Hipótesis específica 3: La norma ISO 27001:2013 gestiona correctamente la accesibilidad de la información para el control de seguridad de información

Prueba de normalidad

Ho = La accesibilidad de información tiene distribución normal

Ha = La accesibilidad de información no tiene distribución normal

Para el cálculo de la prueba de normalidad de la hipótesis 3, se usaron los datos recopilados de la dimensión “accesibilidad” de información pre-test y post-test implementación de la ISO 27001.

Tabla 10

Pruebas de normalidad Hipótesis específica 3

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Accesibilidad Pre	,221	78	,000	,894	78	,000
Accesibilidad Post	,201	78	,000	,905	78	,000

En la tabla 10, se puede evidenciar se usaron 78 grados de libertad (gl), por tal; este al ser mayor a 30 se empleó la prueba de Kolmogorov-Smirnov. Asimismo, los niveles de la significancia (Sig.) son inferiores a 0.05, por lo que se procede a rechazar la Ho; es decir la “Accesibilidad” de la información no sigue una distribución normal y se requiere un análisis no paramétrico bajo la prueba estadística de prueba de rangos de wilcoxon.

Hipótesis específica 4: La norma ISO 27001:2013 gestiona correctamente el resguardo de la información para el control de seguridad de información

Prueba de normalidad

Ho = El resguardo de información tiene distribución normal

Ha = El resguardo de información no tiene distribución normal

Para el cálculo de la prueba de normalidad de la hipótesis 4, se usaron los datos recopilados de la dimensión “Resguardo” de información pre-test y post-test implementación de la ISO 27001.

Tabla 11

Pruebas de normalidad Hipótesis específica 4

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Resguardo Pre	,517	78	,000	,124	78	,000
Resguardo Post	,218	78	,000	,894	78	,000

En la tabla 11, se puede evidenciar se usaron 78 grados de libertad (gl), por tal; este al ser mayor a 30 se empleó la prueba de Kolmogorov-Smirnov. Asimismo, los niveles de la significancia (Sig.) son menores a 0.05, por lo que se procede a rechazar la Ho; es decir el “Resguardo” de la información no sigue una distribución normal y se requiere un análisis no paramétrico bajo la prueba estadística de rangos de wilcoxon.

4.3 Prueba de Confiabilidad

Para obtener la confiabilidad fue necesario realizar 10 cuestionarios de prueba piloto con profesionales elegidos aleatoriamente, asimismo para el cálculo del valor del coeficiente de confiabilidad se usó el ALFA DE CROMBACH, debido a que se usa una escala politómica (Mas de 2 opciones a elegir) en las respuestas del instrumento – cuestionarios.

Regla de decisión:

Si: α > = 0.7000, Se aprueba la confiabilidad del instrumento.

Tabla 12

Estadística de fiabilidad

Alfa de Cronbach	N de elementos
,938	10

A raíz de los resultados encontrados en la tabla 12, se determina que se aprueba la confiabilidad del instrumento en lo que respecta a la variable dependiente “Control de seguridad de información”, ya que es mayor a 0.700; a su vez se detalla que, al tener nivel de confiabilidad de 0.938, se considera como “Muy Confiable” según la tabla 4.

4.4 Prueba de contraste

Hipótesis General

Ho = La norma ISO 27001:2013 no mejorará el control de seguridad de información en la consultoría privada.

Ha = La norma ISO 27001:2013 mejorará el control de seguridad de información en la consultoría privada.

Regla de decisión:

Si p < = 0.05, Se rechaza la hipótesis nula (Ho)

Tabla 13

Estadísticos de contraste – Hipótesis general

	Control de seguridad de la información Post Control de seguridad de la información Pre
Z	-7,684[b]
Sig. asintótica(bilateral)	,000

En la tabla 13, correspondiente a la prueba de rangos de Wilcoxon, se determina que la significancia en el control de seguridad de información es menor al 0.05, por lo que se procede a rechazar la hipótesis nula, concluyendo que la norma ISO 27001:2013 mejorara el control de seguridad de información en la consultoría privada.

Hipótesis específica 1:

Análisis inferencial

Ho = La norma ISO 27001:2013 no gestiona correctamente la disponibilidad de la información para el control de seguridad de información.

Ha = La norma ISO 27001:2013 gestiona correctamente la disponibilidad de la información para el control de seguridad de información.

Regla de decisión:

Si p < = 0.05, Se rechaza la hipótesis nula (Ho)

Tabla 14

Estadísticos de contraste – Hipótesis específica 1

	Disponibilidad Post Disponibilidad Pre
Z	-7,696[b]
Sig. asintótica(bilateral)	,000

En la tabla 14, correspondiente a la prueba de rangos de Wilcoxon, se determina que la significancia en la “disponibilidad” de la información es inferior al 0.05, por lo que se procede a rechazar la hipótesis nula, concluyendo que la norma ISO 27001:2013 gestiona correctamente la disponibilidad de la información para el control de seguridad de información.

Hipótesis específica 2:

Análisis inferencial

Ho = La norma ISO 27001:2013 no gestiona correctamente la adaptabilidad de la información para el control de seguridad de información.

Ha = La norma ISO 27001:2013 gestiona correctamente la adaptabilidad de la información para el control de seguridad de información.

Regla de decisión:

Si p < = 0.05, Se rechaza la hipótesis nula (Ho)

Tabla 15

Estadísticos de contraste – Hipótesis específica 2

	Adaptabilidad Post - Adaptabilidad Pre
Z	-7,718[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

.

De la tabla 15, correspondiente a la prueba de rangos de Wilcoxon, se determina que la significancia en la “adaptabilidad” de la información es inferior al

0.05, por lo que se procede a rechazar la hipótesis nula, concluyendo que la norma ISO 27001:2013 gestiona correctamente la adaptabilidad de la información para el control de seguridad de información.

Hipótesis específica 3:

Análisis inferencial

Ho = La norma ISO 27001:2013 no gestiona correctamente la accesibilidad de la información para el control de seguridad de información.

Ha = La norma ISO 27001:2013 gestiona correctamente la accesibilidad de la información para el control de seguridad de información.

Regla de decisión:

Si p < = 0.05, Se rechaza la hipótesis nula (Ho)

Tabla 16

Estadísticos de contraste – Hipótesis específica 3

	Accesibilidad Post - Accesibilidad Pre
Z	-7,694[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

En la tabla 16, correspondiente a la prueba de rangos de Wilcoxon, se visualiza que la significancia en la “accesibilidad” de la información es menor al 0.05, por lo que se rechaza la hipótesis nula, concluyendo que la norma ISO 27001:2013 gestiona correctamente la accesibilidad de la información para el control de seguridad de información.

Hipótesis específica 4:

Análisis inferencial

Ho = La norma ISO 27001:2013 no gestiona correctamente el resguardo de la información para el control de seguridad de información.

Ha = La norma ISO 27001:2013 gestiona correctamente el resguardo de la información para el control de seguridad de información.

Regla de decisión:

Si p < = 0.05, Se rechaza la hipótesis nula (Ho)

Tabla 17

Estadísticos de contraste – Hipótesis específica 4

	Resguardo Post - Resguardo Pre
Z	-7,744[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

En la tabla 16, correspondiente a la prueba de rangos de Wilcoxon, se determina que la significancia en el “Resguardo” de la información es menor al 0.05, por lo que se procede a rechazar la hipótesis nula, concluyendo que la norma ISO 27001:2013 gestiona correctamente el resguardo de la información para el control de seguridad de información.

V. DISCUSIÓN

A raíz de los resultados mostrados en la presente investigación, se logró alcanzar una mejora significativa en las cuatro dimensiones desarrollados con respecto a la variable dependiente control de la seguridad de información luego de realizar la implementación de la norma ISO27001 en una consultoría privada, Lima 2023. En cuanto a la hipótesis general, se indica que la norma ISO 27001:2013 mejora el control de seguridad de información en el consultorio privado; debido a que estas variables presentan un nivel de significancia de p=0,000 (p<0,05); se rechaza la hipótesis nula y se acepta la hipótesis alterna; por consiguiente, se afirma que la norma ISO 27001:2013 mejora el control de seguridad de información en la consultoría privada. Así como también la investigación señala que la implementación de la norma ISO27001 conlleva un mejor control, seguridad y confidencialidad respecto a la información de cada organización.

Para la dimensión 1: disponibilidad de la información

Según los datos obtenidos después de la implementación de la norma ISO 27001 se logró un aumento de la percepción sobre la correcta gestión del control de la seguridad de información. El análisis descriptivo del primer indicador se realizó mediante encuestas a 78 profesionales, en los cuales se observó un aumento de 91% luego de la aplicación de la norma ISO 27001.

Al realizar la comparación de los valores se observó que antes de la implementación de la ISO 27001:2013, un 59 % obtuvo una percepción “Muy bajo” y 41% la percepción de “Bajo” referente a la disponibilidad de información para control de seguridad de información; por otro lado, después de la implementación de la ISO 27001:2013, se obtuvo un 91% de percepción de mejora “Muy Alto” en el control de seguridad de información y un 9 % consideró “Alto”.

Para el análisis inferencial se usó la prueba de Kolmogorov - Smimov la cual arrojó que los datos analizados siguen una distribución no paramétrica. Para el contraste de hipótesis se usó la prueba de rangos de Wilcoxon, en la tabla 7 se observa que el valor de Z es -7,684, y se tiene un valor de significancia 0,000, lo que confirma el rechazo a la hipótesis nula y se acepta la hipótesis alterna, llegando

a la conclusión que con la norma ISO 27001:2013 gestiona correctamente la disponibilidad de la información para el control de seguridad de información.

Los resultados hallados guardan relación con la investigación desarrollada por Mejía (2020), donde se evidenció un avance favorable de 60% al aplicarse la norma ISO 27001 para la disponibilidad de la información, ya que en su pretest obtuvo una percepción de 11 % y en su post-test un 71%, asimismo al usar Kolmogorov- Smirnov bajo la prueba de Wilcoxon para la prueba de hipótesis se comprobó la aceptación de la hipótesis alternativa, lo cual indicó que la implementación de la normativa ISO 27001:2013 permite disminuir riesgos en la disponibilidad de la información, ya que existió una media de 0,236 en el pre-test y 0,347 en el post- test; por lo cual, es preciso señalar que obtuvo un diseño experimental donde en la prueba no paramétrica el nivel de significancia al ser menor a 0.05, se aceptó la hipótesis alternativa.

Por otro lado, en la investigación realizada por Quintana (2019), donde su objetivo fue implementar la norma ISO 27001 para la disponibilidad de la información, por lo que al realizar la validación de las pruebas hipótesis, se determinó la aceptación de la hipótesis alternativa, obteniendo una media mayor a 0,05, en su pretest obtuvo un p=0,61 y en su post- test un p=0,52; concluyéndose que la disponibilidad de la información mejora luego de la implementación de la ISO 27001, es preciso señalar que obtuvo un diseño experimental donde la prueba no paramétrica indica que el nivel de significancia al ser menor a 0.05, se acepta la hipótesis alternativa.

Por consiguiente se puede indicar que la implementación de la norma ISO 27001 permitió un desarrollo a favor de la disponibilidad de la información, a partir de una programación en los horarios de acceso de los usuarios a la información, disposición inmediata de toda la información según el crecimiento de la base de datos, establecimiento de perfiles de acceso a los usuarios con la información necesaria y autorizada, cumplimiento de permisos y políticas de acceso a los repositorios de información y base de datos. Por lo que, se logró afianzar dicha dimensión.

Para la dimensión 2 adaptabilidad de la información

A raíz de los resultados obtenidos después de la implementación de la norma ISO 27001:2013 se logró un aumento de la percepción sobre la correcta adaptabilidad de la información para el control de seguridad de información. El análisis descriptivo de la segunda dimensión realizó mediante encuestas a 78 profesionales, en los cuales se observó un aumento de 82% luego de la aplicación de la Norma ISO 27001:2013.

Al realizar la comparación de los valores se observó que antes de la implementación de la ISO 27001:2013, un 78 % obtuvo una percepción “Muy bajo” y 22% la percepción “Bajo” referente a la adaptabilidad para control de seguridad de información; por otro lado, después de la implementación de la ISO 27001:2013, se obtuvo un 82% de percepción mejora “Muy Alto” en el control de seguridad de información y un 18 % consideró “Alto”.

En lo que respecta al análisis inferencial se usó la prueba de Kolmogorov-Smimov, los niveles de la significancia (Sig.) son menores a 0.05, por consiguiente, los datos analizados siguieron un análisis no paramétrico bajo la prueba estadística de rangos de WILCOXON. En al análisis descriptivo se determinó que el valor de su media fue 0.186 en el pre-test y 0,163 en el post-test; así como el valor de significancia entre ambas de 0.00 ($p<0.05$). Por lo que con estos resultados se pudo observar que se acepta la hipótesis alternativa y se rechaza la hipótesis nula, comprobándose que la norma ISO 27001:2013 gestiona correctamente la adaptabilidad de la información para el control de seguridad de información.

Estos resultados guardan relación con los obtenidos por Atencio (2019), donde se mencionó que, al aplicarse la norma ISO 27001:2013 hubo un avance favorable del 69% para la adaptabilidad de la información, en su pre-test obtuvo una percepción de 8% y en su post-test un 77%, asimismo al usar Kolmogorov-Smirnov bajo la prueba de Wilcoxon, aceptó la hipótesis alternativa, la cual señaló que la implementación de la normativa ISO 27001:2013 permite disminuir riesgos en la adaptabilidad de la información, ya que existió una media de 0,125 en el pre-test y 0,156 en el post-test; es preciso señalar que obtuvo un diseño experimental

de prueba no paramétrica y que el nivel de significancia al ser menor a 0.05, se aceptó la hipótesis alternativa, por lo que señala la importancia de plasmarlo y la adaptabilidad de la información.

Por otro lado, en la investigación realizada por Córdova (2021), donde su objetivo fue plasmar la la norma ISO 27001:2013 para la adaptabilidad de la información, al mismo tiempo, también reconocer los diversos riesgos que conlleva el riesgo tanto económico y administrativo a la cual se vería expuesto la entidad universitaria. Asimismo, a partir del conocimiento del personal del Departamento de Sistemas e Informática (DSI) se observa que el 63% indica tener un conocimiento ineficiente respecto al conocimiento de la Norma ISO27001, por lo que señala la importancia de plasmarlo y gestionarlo como una herramienta de proceso adaptabilidad en la organización.

Hay que mencionar, además que los investigadores indicados al aprobarse las hipótesis alternativas, se puede identificar que la implementación de la norma ISO 27001:2013 permitió un desarrollo a favor de la adaptabilidad de la información y nuevas tecnologías, con el fin forjar nuevas alternativas para la simplificación de espacio lógico y físico; con ello afianzar dicha dimensión.

Para la dimensión 3 accesibilidad de la información

El análisis descriptivo de la tercera dimensión se realizó mediante encuestas a 78 profesionales, en los cuales se observó un aumento de 88% con respecto a la accesibilidad de la información luego de la aplicación de la Norma ISO 27001:2013.

Al realizar la comparación de los valores se observó que antes de la implementación de la ISO 27001:2013, un 67 % obtuvo una percepción “Muy bajo” y 33% la percepción de “Bajo” referente a la accesibilidad para control de seguridad de información; por otro lado, después de la implementación de la ISO 27001:2013, se obtuvo un 88% de percepción mejora “Muy Alto” en el control de seguridad de información y un 12% consideró “Alto”.

En lo que respecta al análisis inferencial se usó la prueba de Kolmogorov-Smimov, el análisis arroja que la distribución de los datos obtenidos es no

paramétrica, para el contraste de hipótesis se usó la prueba de Wilcoxon, descriptivamente se encontró que el valor de la media fue 0.221 en el pre-test y 0,201 en el post-test; así como el valor de significancia entre ambas de 0.00 ($p<0.05$). Con estos resultados se observó que se acepta la hipótesis alternativa, comprobándose que la norma ISO 27001:2013 gestiona correctamente la accesibilidad de la información para el control de seguridad de información.

Estos datos guardan relación con la investigación realizada por Guardia (2022), donde se evidenció que existió un avance favorable en 72% al aplicarse la norma ISO 27001 para la accesibilidad de la información, ya que en su pre-test obtuvo una percepción de 8 % y en su post-test un 80%; asimismo, al usar Kolmogorov- Smirnov bajo la prueba de rangos de Wilcoxon se comprobó la aceptación de la hipótesis alternativa, la cual señalo que la implementación de la normativa ISO 27001:2013 permite disminuir riesgos en la accesibilidad de la información, ya que existió una media de 0,324 en el pre-test y 0,298 en el post-test; por lo que, es preciso señalar que obtuvo un diseño experimental donde en la prueba no paramétrica el nivel de significancia al ser menor a 0.05, se aceptó la hipótesis alternativa.

Por otro lado, en la investigación realizada por Nacipucha (2019). mencionó que, se obtuvo una aprobación de 78 % como post-test al implementar la norma ISO 27001:2013 para la accesibilidad de la información, en comparación al 15% como pretest; por lo que al realizar la validación de las pruebas hipótesis, se determinó la aceptación de la hipótesis alternativa, en donde se obtuvo una media mayor a 0,05; en su pre-test con un $p=0,74$ y en su post-test un $p=0,91$. Asimismo, la accesibilidad de la información mejora luego de la implementación de la ISO 27001:2013.

Con relación a lo plateando y obtenido por los investigadores mencionados al aprobarse las hipótesis alternativas, se puede identificar que la implementación de la norma ISO 2700 permite un desarrollo a favor de la accesibilidad de la información, a partir de tiempos de respuesta óptimos de la información, controles

de divulgación de información, y dinamismo para la accesibilidad de información, bajo ello se afianzó dicha dimensión.

Para la dimensión 4 resguardo de información

El análisis descriptivo de la dimensión resguardo se realizó mediante encuestas a 78 profesionales, en los cuales se observó un aumento de 83% en lo que respecta al resguardo de información luego de la aplicación de la norma ISO 27001:2013.

Al realizar la comparación de los valores se observó que antes de la implementación de la ISO 27001:2013, un 99 % tuvo una percepción “Muy bajo” y 1% la percepción de “Bajo” referente a la accesibilidad para control de seguridad de información; por otro lado, después de la implementación de la ISO 27001:2013, se obtuvo un 83% de percepción de mejora “Muy Alto” en el control de seguridad de información y un 17% consideró “Alto”.

Para el análisis inferencial se usó la prueba de Kolmogorov-Smirnov bajo la prueba de rangos de Wilcoxon, esto debido a que los datos analizados siguieron una distribución no paramétrica, se logró determinar que el valor de la media fue 0.517 en el pre-test y 0,218 en el post- test; así como el valor de significancia entre ambas de 0.00 ($p<0.05$). Con estos resultados se afirma que se acepta la hipótesis alternativa, comprobándose que la norma ISO 27001:2013 gestiona correctamente el resguardo de la información para la control de seguridad de información.

Estos datos guardan relación con la investigación realizada por Chicaiza (2022), se encontró un avance favorable en 80% al aplicarse la norma ISO 27001:2013 para el resguardo de la información, ya que en su pretest obtuvo una percepción de 5 % y en su post- test un 85%, asimismo al usar Kolmogorov-Smirnov bajo la prueba de Wilcoxon se comprobó la aceptación de la hipótesis alternativa, la cual señaló que la implementación de la normativa ISO 27001:2013 permite disminuir riesgos en el resguardo de la información, por lo que presento una media de 0,567 en el pre-test y 0,442 en el post-test; que obtuvo un diseño experimental donde en la prueba no paramétrica el nivel de significancia al ser

menor a 0.05, se aceptó la hipótesis alternativa. Asimismo, el resguardo de la información mejora luego de la implementación de la ISO 27001.

Del mismo modo, Lozano (2020), indicó que se obtuvo una aprobación de 76% como post-test al implementar la norma ISO 27001:2013 para el resguardo de la información, en comparación al 7% como pretest; por lo que al realizar la validación de las pruebas hipótesis, se determinó la aceptación de la hipótesis alternativa, en la cual se tuvo una media mayor a 0,05; en su pretest obtuvo un p=0,221 y en su post- test un p=0,855; por lo tanto el resguardo de la información mejora luego de la implementación de la ISO 27001:2013; es preciso señalar que tuvo un diseño experimental donde en la prueba no paramétrica el nivel de significancia al ser menor a 0.05, se aceptó la hipótesis alternativa.

Por último, de lo descrito y obtenido por los investigadores mencionados al aprobarse las hipótesis alternativas, se puede identificar que la implementación de la norma ISO 27001:2013 permite un desarrollo a favor del resguardo de la información, a partir de un ordenamiento de las copias de seguridad, optimización de recursos para el almacenamiento de información, establecimiento de controles de auditoria para la seguridad de física y lógica de la información y creación de privilegios para acceder a la información histórica o en backup; con ello se consolida dicha dimensión.

Finalmente, todos los investigadores coinciden que los fundamentos por la ISO 27001:2013 son la guía viable y recomendada para optimizar las prácticas en la gestión de información, ya que abarca selectivamente la implementación y administración de los controles necesarios para el contexto de seguridad de la información de cualquier compañía o empresa.

VI. CONCLUSIONES

Primera: Se determinó que la implementación de la Norma ISO 27001:2013 influyó de forma positiva en el control de la seguridad de información en la consultoría privada. Asimismo, dentro del análisis inferencial se aceptaron las hipótesis planteadas en el trabajo de investigación para los cuatro objetivos específicos, en base a las pruebas realizadas de rangos de Wilcoxon. Gracias a la implementación de la ISO la empresa ha mejorado considerablemente su seguridad de información, la adaptabilidad, accesibilidad, resguardo y disponibilidad hoy se encuentran protegidas a través de un sistema de gestión acorde a las exigencias del mercado.

Segunda: De acuerdo con el primer objetivo específico, se determinó a través de los resultados descriptivos que la disponibilidad de la información mejoró el control de seguridad de la información, toda vez que al realizar la prueba de hipótesis hubo una mejora en un 87.69 % para el control de seguridad, Se observa que la “disponibilidad” de información ha mejorado después de la implementación de la ISO 27001, al tener un desenvolvimiento del 13,0385 % al 87,3718 % en su media. Lo que se establece que la implementación de la norma ISO 270001 contribuye a la eficacia en el control de la seguridad. En el análisis inferencial se utilizó la prueba de Wilcoxon, se observó que el valor de sig. fue 0,000, es decir menor de 0.05, ante estos resultados obtenidos se pudo concluir que se rechaza la hipótesis nula H0 y se acepta la hipótesis alternativa H1, por tanto, la norma ISO 27001:2013 gestiona correctamente la disponibilidad de la información para el control de seguridad de información. La empresa ha obtenido una mejora considerable en cuanto a la disponibilidad de información, al contar con la ISO 27001 la pyme aseguró la fiabilidad de los datos de la empresa, así como también el acceso autorizado de los usuarios a la data.

Tercera: De acuerdo con el segundo objetivo específico, se determinó a través de los resultados descriptivos que la adaptabilidad de la información mejoró el control de seguridad de la información, toda vez que al realizar la prueba de hipótesis hubo una mejora en un 82 % para el control de seguridad, lo que se establece que la implementación de la norma ISO 27001 contribuye a la eficacia en

el control de la seguridad. En el análisis inferencial se utilizó la prueba de Wilcoxon, se observó que el valor de sig. Fue 0,000, es decir menor de 0.05, ante estos resultados obtenidos se pudo concluir que se rechaza la hipótesis nula H0 y se acepta la hipótesis alternativa H1, por tanto, la norma ISO 27001:2013 gestiona correctamente la adaptabilidad de la información para el control de seguridad de información. La empresa ha obtenido una capacidad alta para prevenir futuros cambios laboralmente, así como también al contexto económico que puede surgir en el país, gracias a la aplicación de la ISO 27001 la rapidez de la gerencia en la toma de decisiones ante una emergencia ha vuelto sostenible y rentable sus servicios.

Cuarta: De acuerdo con el tercer objetivo específico, se determinó a través de los resultados descriptivos que la accesibilidad de la información mejoró el control de seguridad de la información, toda vez que al realizar la prueba de hipótesis hubo una mejora en un 88% para el control de seguridad, lo que se establece que la implementación de la norma ISO 27001:2013 contribuye a la eficacia en el control de la seguridad. En el análisis inferencial se utilizó la prueba de Wilcoxon, se observó que el valor de sig. fue 0,000, es decir menor de 0.05, ante estos resultados obtenidos se pudo concluir que se rechaza la hipótesis nula H0 y se acepta la hipótesis alternativa H1, por tanto, la norma ISO 27001:2013 gestiona correctamente la accesibilidad de la información para el control de seguridad de información. Debido a la implementación de la ISO 27001:2013 la empresa mejoró considerablemente la accesibilidad de su información, se realizaron controles de seguridad tales como encriptación de datos, contraseñas seguras y usuarios con privilegios para obtener información de la empresa.

Quinta: De acuerdo con el cuarto objetivo específico, se determinó a través de los resultados descriptivos que el resguardo de la información influyó de forma positiva en el control de seguridad de la información, toda vez que al realizar la prueba de hipótesis hubo una mejora en un 83 % para el control de la seguridad, lo que establece que la implementación de la norma ISO 27001:2013 contribuye a la eficacia en el control de la seguridad. En el análisis inferencial se utilizó la prueba de Wilcoxon, se observó que el valor de sig. fue 0,000, es decir menor de 0.05, ante

estos resultados obtenidos se pudo concluir que se rechaza la hipótesis nula H0 y se acepta la hipótesis alternativa H1, por tanto, la norma ISO 27001:2013 gestiona correctamente el resguardo de la información para el control de seguridad de información. Es decir, la empresa mejoró el resguardo de la información, esto debido a que ahora la empresa realiza copias de seguridad de la información periódicamente, las copias de respaldo se están guardando en discos duros con copia a espacios en la nube.

VII. RECOMENDACIONES

Primero: De acuerdo con el objetivo general, se recomienda al jefe del área de sistemas de la empresa SYS LCI S.A.C realizar auditorías internas luego de la implementación de la norma ISO27001:2013 para la consultoría privada, esto con la finalidad de obtener una mejora continua en su sistema de gestión, plasmar la norma 27001:2013 permitirá mayor seguridad, y efectividad respecto al control de seguridad de la información.

Segundo: En relación con el objetivo 2, se recomienda al jefe del área de sistemas de la empresa SYS LCI S.A.C realizar auditorías de seguimiento con la finalidad de medir la evolución de la norma ISO 27001:2013, al tener conocimiento del estado en tiempo real del sistema de gestión, se podrá salvaguardar la información de los clientes pertenecientes a esta empresa, por consiguiente, se podrá mitigar los ciberataques y riesgos que puedan presentarse.

Tercero: En relación con el objetivo 3, se recomienda al jefe del área de sistemas de la empresa SYS LCI S.A.C implemente manuales de procedimientos en lo que respecta a la adaptabilidad de la información, con la finalidad de que la empresa se vuelva dinámica y adaptable en lo que respecta a la seguridad de información.

Cuarto: En relación con el objetivo 4, se recomienda al jefe del área de sistemas de la empresa SYS LCI S.A.C realice planes de acción para complementar posibles controles faltantes en referente a la accesibilidad de la información, debido a que esto será un beneficio del usuario y de la empresa, de tal modo que al contar con información en tiempo real se podrá mejorar los procesos de toma de decisiones.

Quinto: En relación con el objetivo 5, se recomienda al jefe del área de sistemas de la empresa SYS LCI S.A.C defina a través de un análisis de riesgo el plan de acción para realizar el resguardo de la información, de tal manera que se irá reduciendo la perdida de archivos importantes para la empresa, mejorando la eficacia de los procesos de información para el cliente.

REFERENCIAS

Agé, M. (2013). *Seguridad informática - Ethical Hacking: Conocer el ataque para una mejor defensa.* (2ª ed.). ACISSI.

Aguilera, P. (2010). *Seguridad informática. Informática y comunicaciones*. Editorial Editex, S. A. Madrid, España.

Aladra (2015) file:///C:/Users/Lenovo/Downloads/ecob,+36988-39275-1-CE.pdf

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

Atencio, E. (2019). *Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú.* [Tesis doctorado, Universidad Nacional Daniel Alcides Carrión]. http://repositorio.undac.edu.pe/handle/undac/1474

Bermúdez, K. (2015). *Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001- sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros*. [Tesis doctorado Universidad politécnica salesiana]. https://dspace.ups.edu.ec/handle/123456789/10372

Borbón, J. (2011). *Buenas prácticas, estándares y normas*. Revista Seguridad. https://acortar.link/0M0jtm

Caballero R. (2021). Metodología de la investigación científica. UDEGRAF

Castillo, R. (2022). *Desarrollo de una aplicación web y móvil para la gestión de riesgos de seguridad de la información aplicado a una empresa de consultoría de sistemas.* [Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos]. https://hdl.handle.net/20.500.12672/18129

Cardona, J y Restrepo, R. (2020). *Evaluación de la implementación de la norma ISO 27001 en empresas del sector privado, bajo un enfoque cultural.* Tecnológico de Antioquia, Institución Universitaria. https://dspace.tdea.edu.co/handle/tdea/921

Charlet, L. (2019). *ISO CASCO – standards for conformity assessment.* ITU. https://www.itu.int/dms_pub/itu-d/oth/07/20/D07200000010001PDFE.pdf

Chamorro, C. (2015). *Propuesta para un adecuado manejo de la seguridad de la información en base a la norma ISO 27002 para la Dirección de Gestión Tecnológica del Ministerio del Deporte.* [Tesis doctorado, Escuela Politécnica Nacional]. http://bibdigital.epn.edu.ec/handle/15000/12650

Chicaiza, D. (2019). *Modelo de gestión de la seguridad de la información para pequeñas empresas.* [Tesis de maestría, Universidad Técnica de Ambato]. http://repositorio.uta.edu.ec/jspui/handle/123456789/29348

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.

Espinoza, H. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.* [Tesis de Ingeniería, Pontificia Universidad Católica del Perú]. http://hdl.handle.net/20.500.12404/4957

Fermín (2015). file:///C:/Users/Lenovo/Downloads/19565.pdf

Fernández, V. (2006). *Desarrollo de sistemas de información: una metodología basada en el modelado.* Ediciones UPC

Figueroa, J., Rodríguez, R., Bone, C., & Saltos, J. (2017). La seguridad informática y la seguridad de la información. *Revista CientíficoAcadémica Multidisciplinaria Polo del Conocimiento, 2*(14), 145-155. doi:10.23857/pc.v2i12.420

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*

Gaviria, S. (2019). *Importancia de la implementación del SGSI 27001 en la seguridad informática de ACESCO*. [Tesis de administración, UMNG]. https://repository.unimilitar.edu.co/handle/10654/3215

Guardia, R. (2020). *Diseño de un modelo de seguridad de la información para minimizar los riesgos informáticos en la gestión académica del instituto de educación superior tecnológico público "ELEAZAR GUZMAN BARRON" - HUARAZ" – 2018.* [Tesis de maestría, Universidad Nacional Santiago Antúnez de Mayolo]. http://repositorio.unasam.edu.pe/handle/UNASAM/4212

Guachi, T. (2012). *Norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la cooperativa de ahorro y crédito san francisco ltda.* [Tesis de Ingeniería, Universidad Técnica de Ambato]. http://repositorio.uta.edu.ec/handle/123456789/2361

Guerrero, S. (2022). Informe inventario de activos de información ETITC. *Escuela Tecnológica Instituto Técnico Central, 1(13),16 - 74. https://etitc.edu.co/archives/infoinvactinfoabr22.pdf*

Guzmán, C. (2019). *Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso*. [Tesis de Ingeniería. Institución Universitaria Politécnico Grancolombiano]. http://hdl.handle.net/10823/654

Hernández, R., Fernández, C y Baptista, L. (2018). *Metodología de la investigación.* (6 ed.). McGraw-Hill / Interamericana Editores

Heredero, P. (2006). *"Dirección y gestión de los sistemas de información en la empresa".* (2º. Ed.). ESIC EDIT.

Ladino, M., Villa, P., López, A., (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia Et Technica,* 47, 334-339. https://www.redalyc.org/articulo.oa?id=84921327061

Lema, R. y Donoso, D. (2018). *Implementación de un sistema de gestión de seguridad de información basado en la Norma ISO 27001:2013 para el control físico y digital de documentos aplicado a la empresa LOCKERS S.A.* [Tesis de Maestría, Universidad de las Fuerzas Armadas. http://repositorio.espe.edu.ec/handle/21000/14397

López, E. y Zamora, H. (2015). *Evaluación de la Red Inalámbrica en el Hospital Escuela Cesar Amador Molina, basado en la norma IEEE 802.11 y controles de seguridad del estándar ISO 27002-2013 Matagalpa, I semestre 2015.* [Tesis de maestría, Universidad Nacional Autónoma de Nicaragua]

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

Mamani, W. (2020). *Análisis de riesgo de la información según la norma iso 27001:2013: previo a una implementación.* [Tesis de Bachiller, Universidad Peruana Unión]. http://hdl.handle.net/20.500.12840/3734

Mifsud, E. (2012). *MONOGRÁFICO: Introducción a la seguridad informática - Políticas de seguridad*. Gobierno de España. https://acortar.link/vXlFL2

Morales, J.G. (2022). *Influencia del COVID 19 en el incremento de los Ciberataques a Nivel Mundial*. [Tesis de maestría, Universidad piloto de Colombi]. http://repository.unipiloto.edu.co/handle/20.500.12277/11574

Mucha, L., & Lora, M. (2021). Técnica de muestreo para investigación cuantitativa: aplicación informática. Perú, Perú. Obtenido de http://www.scielo.org.bo/pdf/rpc/v09n08/v09n08a12.pdf

Nacipucha, J. (2019). A*nálisis y diseño para un modelo de gestión de seguridad de la información basados en normas ISO/IEC 27001:2013 para la empresa Artehogar en la ciudad de Guayaquil.* [Tesis doctorado, Universidad de Guayaquil]. http://repositorio.ug.edu.ec/handle/redug/44410

Plúa, G. (2017). *Diseño de un plan estratégico de seguridad informática aplicada a la red de telecomunicación de datos del gobierno autónomo descentralizado del cantón Jipijapa*. [Tesis de maestría, Universidad Técnica de Ambato]. http://repositorio.unesum.edu.ec/handle/53000/980

Rossi, G. (2021). *La seguridad y defensa en la era de la cuarta revolución industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas hibridas.* [Tesis de maestría, Academia Diplomática del Perú Javier Pérez de Cuéllar]. http://repositorio.adp.edu.pe/handle/ADP/170

Russell, J. (2022). *ISO 27001:2013 Guía de implantación para la seguridad de la información. NQA organismo de certificación global.* https://acortar.link/xoHfq8

Rodríguez, C. (2021). *Propuesta de implementación de un sistema de gestión de seguridad de la información aplicando la Norma ISO 27001:2013 para una institución del Estado en la Provincia Constitucional de Callao - 2021*. [Tesis de Ingieneria, Universidad Tecnologica del Perú]. https://hdl.handle.net/20.500.12867/5101

Sánchez, R. (2007). *Análisis de riesgos en seguridad informática caso UNMSM. de la Especialidad de sistemas e informática – 2007.* [Tesis de Ingeniería, Universidad Nacional Mayor de San Marcos]. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/14862/Sanchez_sr.pdf?sequence=1&isAllowed=y

Seguridad América (2022, marzo 17). *Perú: aumenta los riesgos de ciberataques a través de suplantación de identidad*. https://acortar.link/CLGkoE

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

Solarte, F., Enriquez, E y Del Carmen, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL, 28*(5). http://200.10.147.88/index.php/tecnologica/article/view/456/321

Solano, G. (2020). Propuesta mediante la normativa ISO 27001 para la gestión de la seguridad de la información en la empresa Udersol en Costa Rica [Tesis de pregrado, Universidad Latina de Costa Rica]. https://repositorio.ulatina.ac.cr/handle/20.500.12411/293?locale=es

Téllez, J. (1988). *Contratos, riesgos y seguros informáticos*. Universidad Autónoma de México. (UNAM). http://ru.juridicas.unam.mx:80/xmlui/handle/123456789/9871

Tuapanta J. (2017). Alfa de Cronbach para validar un cuestionario de uso de tic en docentes universitarios*. MKT Descubre*. *32*(12), 37 -48. https://core.ac.uk/download/pdf/234578641.pdf

Vivanco, H y Quintana, A. (2019). *Diseño de un modelo de gestión de seguridad de la información para la Universidad Iberoamericana del Ecuador.* [Tesis doctorado, Universidad Tecnológica Israel. https://repositorio.uisrael.edu.ec/handle/47000/2019

Vela, O., Requejo, M., Cubillas, C., Pérez M y Alfaro, P. (2019). Análisis de la clasificación de normas técnicas para la gestión de infraestructuras y servicios de tecnologías de la información. *DINA, 94* (5), 484. https://doi.org/10.6036/9303

Villavicencio, E., Torracchi, E., Pariona, M., & Alvear, M. (2019). ¿cómo plantear las variables de una investigación?: operacionalización de las variables. Revista OACTIVA UC Cuenca, 4, 9-14. Obtenido de https://oactiva.ucacue.edu.ec/index.php/oactiva/article/view/289/500

Vásquez, J.F. (2018). *Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI*. [Tesis de Ingeniería, Universidad Nacional Mayor de San Marcos].https://hdl.handle.net/20.500.12672/8436

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

Wang, B., Wang, R., & Wang, Y. (2019). Compatible matrices of Spearman's rank correlation. *Paper. Statistics and Probability Letters, 151*(1), 67–72. https://doi.org/10.1016/j.spl.2019.03.015

ANEXOS

Anexo 1: Operacionalización de variables

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	TÉCNICA	INSTRUMENTO	ESCALA DE MEDICIÓN
Implementación de Norma ISO 27001:2013	Se centra como guía de buenas prácticas para el desarrollo y ejecución de procedimientos que regularan la seguridad de la información contra diferentes amenazas. Academy (2018)	Es la ejecución de los términos relacionados a la seguridad informática con relación a la empresa	Planificación	• Análisis de brecha inicial • Compromiso de alta dirección • Comprender el contexto de la organización • Comprender necesidades y expectativas • Determinar el alcance del SGSI • Determinar políticas de SI • Determinar objetivos de SI • Crear procedimiento de gestión de riesgos • Crear procedimiento de gestión de incidencia	Encuesta	Cuestionario	Escala Likert 0 Muy Bajo 1 Bajo 2 Medio Bajo 3 Medio 4 Medio Alto 5

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	TÉCNICA	INSTRUMENTO	ESCALA DE MEDICIÓN
				• Crear procedimiento de auditoría interna • Gestionar los riesgos • Crear plan de tratamiento de riesgos • Determinar la declaración de aplicabilidad • Crear plan de capacitación y concientización.			Alto
			Ejecución	• Implementar plan de tratamiento de riesgos • Implementar plan de capacitación y concientización			
			Verificación	• Preparar la auditoría interna • Ejecutar auditoria • Revisar con la alta dirección los resultados obtenidos			

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	TÉCNICA	INSTRUMENTO	ESCALA DE MEDICIÓN
			Mejora Continua	• Crear plan de acciones correctivas • Implementar plan de acciones correctivas • Análisis de brecha final			
Control de seguridad de la información	Tiene como propósito la protección de todos los activos que involucren la información de la empresa, esto comprende desde los sistemas, aplicaciones, infraestructura, datos y equipos	Es la protección de la información, a partir de las buenas prácticas establecidas por algunas metodologías o normas	Disponibilidad	• Tiempos de acceso • Tipos de acceso • Políticas de acceso	Encuesta	Cuestionario	Escala Likert 0 Nunca 1 Casi Nunca 2 A veces 3 Casi siempre 4 Siempre
			Adaptabilidad	• Crecimiento de información • Adaptación de nuevas tecnologías • Espacio disponible • Capacidad de almacenamiento físico			
			Accesibilidad	• Acceso a consultas • Tiempo de respuesta			
			Resguardo	• Respaldo de seguridad			

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	TÉCNICA	INSTRUMENTO	ESCALA DE MEDICIÓN
	(Sánchez, Villafranca, Fernández y Piattini, 2018)			• Almacenamiento del respaldo de seguridad • Acceso al respaldo de seguridad • Seguridad física			

Anexo 2: validación de instrumentos

CARTA DE PRESENTACIÓN

Señor: Dr. Marlon Frank Acuña Benites

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Nos es muy grato comunicarnos con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que siendo estudiante del programa **de maestría en Ingeniería de Sistemas con mención en tecnologías de la información** de la Universidad, en la sede Lima, promoción XXIII, aula B1, requerimos validar los instrumentos con los cuales recogeremos la información necesaria para poder desarrollar nuestra investigación.

El título de investigación es: **Norma ISO 27001 para el control de seguridad de la información en una consultoría privada, Lima 2023** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, hemos considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las variables y dimensiones.
- Matriz de operacionalización de las variables.
- Certificado de validez de contenido de los instrumentos.

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

Firma
Apellidos y nombre:
Aleman Balladares Fernando Yasmani
D.N.I: 41867726

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS

VARIABLE : Control de seguridad de la información

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Disponibilidad	Si	No	Si	No	Si	No	
1	¿La empresa cuenta con horarios establecidos para acceder al repositorio de información?							
2	¿Existen tipos de acceso para los usuarios?							
3	¿Existente políticas de acceso al repositorio de la información?							
4	¿Los usuarios cuentan con los mismos permisos para acceder a la información?							
	DIMENSION 2 : Adaptabilidad	Si	No	Si	No	Si	No	
5	¿El repositorio de información pueden ser adaptables a nuevas tecnologías?							
6	¿Es importante mejorar la adaptabilidad del repositorio de información?							
7	¿Existen unidades de almacenamiento de respaldo?							
8	¿Considera optimo el espacio asignado a la PC/Laptop asignado?							
9	¿Es necesario mejorar la capacidad física de la PC/Laptop asignado?							
	DIMENSION 3 : Accesibilidad	Si	No	Si	No	Si	No	
10	¿Cualquier usuario puede acceder a toda la información del repositorio?							
11	¿Existen controles de acceso para ingresar a la PC/Laptop de los usuarios?							
12	¿Se debería mejorar los permisos a las carpetas de almacenamiento de información?							
13	¿El tiempo de respuesta del repositorio de información es óptimo?							
	DIMENSION 4 : Resguardo	Si	No	Si	No	Si	No	
14	¿Se realizan copias de resguardo del repositorio de información?							
15	¿Se considera primordial realizar copias de resguardo periódicamente?							
16	¿Se cuenta con una ubicación asignada para el almacenamiento de información de los usuarios en la PC/Laptop asignada?							
17	¿Se cuenta con protocolos para acceder a las copias de resguardo de información?							
18	¿Se cuenta con seguridad física al repositorio de información?							

Observaciones (precisar si hay suficiencia): .....

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

Apellidos y nombres del juez validador. Dr/ Mg: **MARLON FRANK ACUÑA BENITES** **DNI: 42097456**

Especialidad del validador: :.....

[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

24 de octubre del 2022

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE MIDE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS.
VARIABLE : Norma iso 27001

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Planificación	Si	No	Si	No	Si	No	
1	5.1. ¿La dirección aprueba el cumplimiento de los objetivos de seguridad de la información para la implementación de la ISO 27001?							
2	5.1. ¿El equipo de proyecto asegura la integración de los requisitos para implementar la ISO 27001 en los procesos de la empresa?							
3	5.2. ¿Existe apoyo a los trabajadores para su contribución efectiva de la ISO 27001?							
4	5.3. ¿Se ha establecido una política de seguridad de la información?							
5	5.3. ¿Se han definido roles y responsabilidades para la seguridad de información?							
6	6.1.1. ¿La empresa realiza análisis de riesgos de la seguridad de información?							
7	6.1.2. ¿La empresa define y aplica el proceso de valoración de riesgos de la seguridad de información?							
8	6.1.3. ¿La empresa tiene un plan de tratamiento de riesgos de la seguridad de la información?							
9	6.2. ¿La empresa tiene documentado los objetivos de la seguridad de información?							
10	6.2. ¿La empresa cuenta con un plan de mejora basado en el cumplimiento de objetivos?							
11	7.1. ¿La empresa proporciona los recursos necesarios para la gestión de la seguridad informática?							
12	7.2. ¿Existen evaluaciones de desempeño acerca de la seguridad de información?							
13	7.3 ¿Existen políticas de seguridad de información?							
14	7.4. ¿Se tienen definidos canales de atención para la seguridad de información?							
15	7.5.1. ¿Se cuenta con documentación de la seguridad de información para asegurar la efectividad?							
16	7.5.3. ¿Se controla que la información requerida para la gestión de la seguridad esté disponible y protegida?							
	DIMENSION 2 : Ejecución	Si	No	Si	No	Si	No	
17	8.1. ¿Existe una planificación, ejecución y control de procesos para la gestión de seguridad de información?							

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
18	8.2. ¿Se llevan a cabo evaluaciones de riesgo planificados?							
19	8.3. ¿La empresa cuenta con un plan de tratamiento de riesgos?							
	DIMENSION 3 : Verificacion	Si	No	Si	No	Si	No	
20	9.1. ¿La empresa realiza el seguimiento, análisis y evaluación de la gestión de seguridad de información?							
21	9.2. ¿La empresa realiza auditorías internas?							
22	9.3. ¿La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia?							
23	9.4. ¿La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información?							
	DIMENSION 4 : Mejoramiento	Si	No	Si	No	Si	No	
24	10.1. ¿La empresa controla y corrige las normas de cumplimiento de la seguridad de información?							
25	10.2. ¿La empresa mejora continuamente la adecuación y efectividad de la gestión de la seguridad de información?							

Observaciones (precisar si hay suficiencia):_____

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

Apellidos y nombres del juez validador. Dr/ Mg: **MARLON FRANK ACUÑA BENITES** **DNI: 42097456**

Especialidad del validador:.....

24 de octubre del 2022

[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 Informante.

CARTA DE PRESENTACIÓN

Señor : Giancarlo Sánchez Atuncar

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Nos es muy grato comunicarnos con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, siendo estudiante del programa **de maestría en Ingeniería de Sistemas con mención en tecnologías de la información** de la Universidad, en la sede Lima, promoción XXIII, aula B1, requerimos validar los instrumentos con los cuales recogeremos la información necesaria para poder desarrollar nuestra investigación.

El título de investigación es: **Norma ISO 27001 para el control de seguridadde la información en una consultoría privada, Lima 2023** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, hemos considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las variables y dimensiones.
- Matriz de operacionalización de las variables.
- Certificado de validez de contenido de los instrumentos.

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

Firma
Apellidos y nombre:
Aleman Balladares Fernando Yasmani
D.N.I: 41867726

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS

VARIABLE : Control de seguridad de la información

Nº	DIMENSIONES / Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Disponibilidad	Si	No	Si	No	Si	No	
1	¿La empresa cuenta con horarios establecidos para acceder al repositorio de información?	x		x		x		
2	¿Existen tipos de acceso para los usuarios?	x		x		x		
3	¿Existente políticas de acceso al repositorio de la información?	x		x		x		
4	¿Los usuarios cuentan con los mismos permisos para acceder a la información?							
	DIMENSION 2 : Adaptabilidad	Si	No	Si	No	Si	No	
5	¿El repositorio de información pueden ser adaptables a nuevas tecnologías?	x		x		x		
6	¿Es importante mejorar la adaptabilidad del repositorio de información?	x		x		x		
7	¿Existen unidades de almacenamiento de respaldo?	x		x		x		
8	¿Considera optimo el espacio asignado a la PC/Laptop asignado?	x		x		x		
9	¿Es necesario mejorar la capacidad física de la PC/Laptop asignado?							
	DIMENSION 3 : Accesibilidad	Si	No	Si	No	Si	No	
10	¿Cualquier usuario puede acceder a toda la información del repositorio?	x		x		x		
11	¿Existen controles de acceso para ingresar a la PC/Laptop de los usuarios?	x		x		x		
12	¿Se debería mejorar los permisos a las carpetas de almacenamiento de información?	x		x		x		
13	¿El tiempo de respuesta del repositorio de información es optimo?	x		x		x		
	DIMENSION 4 : Resguardo	Si	No	Si	No	Si	No	
14	¿Se realizan copias de resguardo del repositorio de información?	x		x		x		

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
15	¿Se considera primordial realizar copias de resguardo periódicamente?	x		x		x		
16	¿Se cuenta con una ubicación asignada para el almacenamiento de información de los usuarios en la PC/Laptop asignada?	x		x		x		
17	¿Se cuenta con protocolos para acceder a las copias de resguardo de información?	x		x		x		
18	¿Se cuenta con seguridad física al repositorio de información?	x		x		x		

Observaciones (precisar si hay suficiencia): si hay suficiencia en el instrumento.

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

Apellidos y nombres del juez validador. Mg. Giancarlo Sánchez Atuncar **DNI: 41488834**

Especialidad del validador: Ingeniero de Sistemas

[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

25 de octubre del 2022

Firma del Experto Informante.

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE MIDE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS.

VARIABLE : Implementacion de norma iso 27001

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Planificación	Si	No	Si	No	Si	No	
1	5.1. ¿La dirección aprueba el cumplimiento de los objetivos de seguridad de la información para la implementación de la ISO 27001?	x		x		x		
2	5.1. ¿El equipo de proyecto asegura la integración de los requisitos para implementar la ISO 27001 en los procesos de la empresa?	x		x		x		
3	5.2. ¿Existe apoyo a los trabajadores para su contribución efectiva de la ISO 27001?	x		x		x		
4	5.3. ¿Se ha establecido una política de seguridad de la información?	x		x		x		
5	5.3. ¿Se han definido roles y responsabilidades para la seguridad de información?	x		x		x		
6	6.1.1. ¿La empresa realiza análisis de riesgos de la seguridad de información?	x		x		x		
7	6.1.2. ¿La empresa define y aplica el proceso de valoración de riesgos de la seguridad de información?	x		x		x		
8	6.1.3. ¿La empresa tiene un plan de tratamiento de riesgos de la seguridad de la información?	x		x		x		
9	6.2. ¿La empresa tiene documentado los objetivos de la seguridad de información?	x		x		x		
10	6.2. ¿La empresa cuenta con un plan de mejora basado en el cumplimiento de objetivos?	x		x		x		
11	7.1. ¿La empresa proporciona los recursos necesarios para la gestión de la seguridad informática?	x		x		x		
12	7.2. ¿Existen evaluaciones de desempeño acerca de la seguridad de información?	x		x		x		
13	7.3 ¿Existen políticas de seguridad de información?	x		x		x		
14	7.4. ¿Se tienen definidos canales de atención para la seguridad de información?	x		x		x		
15	7.5.1. ¿Se cuenta con documentación de la seguridad de información para asegurar la efectividad?	x		x		x		
16	7.5.3. ¿Se controla que la información requerida para la gestión de la seguridad esté disponible y protegida?	x		x		x		
	DIMENSION 2 : Ejecución	Si	No	Si	No	Si	No	
17	8.1. ¿Existe una planificación, ejecución y control de procesos para la gestión de seguridad de información?	x		x		x		

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
18	8.2. ¿Se llevan a cabo evaluaciones de riesgo planificados?							
19	8.3. ¿La empresa cuenta con un plan de tratamiento de riesgos?							
	DIMENSION 3 : Verificación	Si	No	Si	No	Si	No	
20	9.1. ¿La empresa realiza el seguimiento, análisis y evaluación de la gestión de seguridad de información?	x		x		x		
21	9.2. ¿La empresa realiza auditorías internas?							
22	9.3. ¿La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia?							
23	9.4. ¿La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información?							
	DIMENSION 4 : Mejoramiento	Si	No	Si	No	Si	No	
24	10.1. ¿La empresa controla y corrige las normas de cumplimiento de la seguridad de información?	x		x		x		
25	10.2. ¿La empresa mejora continuamente la adecuación y efectividad de la gestión de la seguridad de información?							

Observaciones (precisar si hay suficiencia): si hay suficiencia en el instrumento.

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

Apellidos y nombres del juez validador **Mg. Giancarlo Sánchez Atuncar** **DNI: 41488834**

Especialidad del validador: Ingeniero de Sistemas

25 de octubre del 2022

Firma del Experto Informante.

[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

CARTA DE PRESENTACIÓN

Señor Juan Orlando Perez Alvaro

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Nos es muy grato comunicarnos con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que siendo estudiante del programa **de maestría en Ingeniería de Sistemas con mención en tecnologías de la información** de la Universidad, en la sede Lima, promoción XXIII, aula B1, requerimos validar los instrumentos con los cuales recogeremos la información necesaria para poder desarrollar nuestra investigación.

El título de investigación es: **Norma ISO 27001 para el control de seguridad de la información en una consultoría privada, Lima 2023** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, hemos considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las variables y dimensiones.
- Matriz de operacionalización de las variables.
- Certificado de validez de contenido de los instrumentos.

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

Firma
Apellidos y nombre:
Aleman Balladares Fernando Yasmani
D.N.I: 41867726

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS

VARIABLE : Control de seguridad de la información

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Disponibilidad	Si	No	Si	No	Si	No	
1	¿La empresa cuenta con horarios establecidos para acceder al repositorio de información?	X		X		X		
2	¿Existen tipos de acceso para los usuarios?	X		X		X		
3	¿Existente políticas de acceso al repositorio de la información?	X		X		X		
4	¿Los usuarios cuentan con los mismos permisos para acceder a la información?	X		X		X		
	DIMENSION 2 : Adaptabilidad	Si	No	Si	No	Si	No	
5	¿El repositorio de información pueden ser adaptables a nuevas tecnoloqías?	X		X		X		
6	¿Es importante mejorar la adaptabilidad del repositorio de información?	X		X		X		
7	¿Existen unidades de almacenamiento de respaldo?	X		X		X		
8	¿Considera optimo el espacio asignado a la PC/Laptop asignado?	X		X		X		
9	¿Es necesario mejorar la capacidad física de la PC/Laptop asignado?	X		X		X		
	DIMENSION 3 : Accesibilidad	Si	No	Si	No	Si	No	
10	¿Cualquier usuario puede acceder a toda la información del repositorio?	X		X		X		
11	¿Existen controles de acceso para ingresar a la PC/Laptop de los usuarios?	X		X		X		
12	¿Se debería mejorar los permisos a las carpetas de almacenamiento de información?	X		X		X		
13	¿El tiempo de respuesta del repositorio de información es óptimo?	X		X		X		
	DIMENSION 4 : Resguardo	Si	No	Si	No	Si	No	
14	¿Se realizan copias de resguardo del repositorio de información?	X		X		X		

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
15	¿Se considera primordial realizar copias de resguardo periódicamente?	X		X		X		
16	¿Se cuenta con una ubicación asignada para el almacenamiento de información de los usuarios en la PC/Laptop asignada?	X		X		X		
17	¿Se cuenta con protocolos para acceder a las copias de resguardo de información?	X		X		X		
18	¿Se cuenta con seguridad física al repositorio de información?	X		X		X		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA EN EL INSTRUMENTO

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

Apellidos y nombres del juez validador: Mg. Juan Orlando Perez Alvaro DNI: 40545360

Especialidad del validador: Ingeniero de Sistemas

24 de octubre del 2022

[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 DIGITAL

Firmado digitalmente por: PEREZ ALVARO Juan Orlando FAU 20131370998 soft
Motivo: Soy el autor del documento
Fecha: 25/10/2022 09:50:56-0500

Firma del Experto Informante.

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE MIDE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS.

VARIABLE : Norma iso 27001

Nº	DIMENSIONES / Items	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Planificación	Si	No	Si	No	Si	No	
1	5.1. ¿La dirección aprueba el cumplimiento de los objetivos de seguridad de la información para la implementación de la ISO 27001?	X		X		X		
2	5.1. ¿El equipo de proyecto asegura la integración de los requisitos para implementar la ISO 27001 en los procesos de la empresa?	X		X		X		
3	5.2. ¿Existe apoyo a los trabajadores para su contribución efectiva de la ISO 27001?	X		X		X		
4	5.3. ¿Se ha establecido una política de seguridad de la información?	X		X		X		
5	5.3. ¿Se han definido roles y responsabilidades para la seguridad de información?	X		X		X		
6	6.1.1. ¿La empresa realiza análisis de riesgos de la seguridad de información?	X		X		X		
7	6.1.2. ¿La empresa define y aplica el proceso de valoración de riesgos de la seguridad de información?	X		X		X		
8	6.1.3. ¿La empresa tiene un plan de tratamiento de riesgos de la seguridad de la información?	X		X		X		
9	6.2. ¿La empresa tiene documentado los objetivos de la seguridad de información?	X		X		X		
10	6.2. ¿La empresa cuenta con un plan de mejora basado en el cumplimiento de objetivos?	X		X		X		
11	7.1. ¿La empresa proporciona los recursos necesarios para la gestión de la seguridad informática?	X		X		X		
12	7.2. ¿Existen evaluaciones de desempeño acerca de la seguridad de información?	X		X		X		
13	7.3 ¿Existen políticas de seguridad de información?	X		X		X		
14	7.4. ¿Se tienen definidos canales de atención para la seguridad de información?	X		X		X		
15	7.5.1. ¿Se cuenta con documentación de la seguridad de información para asegurar la efectividad?	X		X		X		
16	7.5.3. ¿Se controla que la información requerida para la gestión de la seguridad esté disponible y protegida?	X		X		X		
	DIMENSION 2: Ejecución	Si	No	Si	No	Si	No	
17	8.1. ¿Existe una planificación, ejecución y control de procesos para la gestión de seguridad de información?	X		X		X		

Nº	DIMENSIONES / Items	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
18	8.2. ¿Se llevan a cabo evaluaciones de riesgo planificados?	X		X		X		
19	8.3. ¿La empresa cuenta con un plan de tratamiento de riesgos?	X		X		X		
	DIMENSION 3 : Verificación	Si	No	Si	No	Si	No	
20	9.1. ¿La empresa realiza el seguimiento, análisis y evaluación de la gestión de seguridad de información?	X		X		X		
21	9.2. ¿La empresa realiza auditorías internas?	X		X		X		
22	9.3. ¿La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia?	X		X		X		
23	9.4. ¿La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información?	X		X		X		
	DIMENSION 4 : Mejoramiento	Si	No	Si	No	Si	No	
24	10.1. ¿La empresa controla y corrige las normas de cumplimiento de la seguridad de información?	X		X		X		
25	10.2. ¿La empresa mejora continuamente la adecuación y efectividad de la gestión de la seguridad de información?	X		X		X		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA EN EL INSTRUMENTO

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

Apellidos y nombres del juez validador : Mg. Juan Orlando Perez Alvaro DNI: 40545360

Especialidad del validador: Ingeniero de Sistemas

24 de octubre del 2022

[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 DIGITAL

Firmado digitalmente por: PEREZ ALVARO Juan Orlando FAU 20131370998 soft
Motivo: Soy el autor del documento
Fecha: 25/10/2022 09:50:27-0500

Firma del Experto Informante.

Anexo 3: Carta de presentación

UNIVERSIDAD CÉSAR VALLEJO

"Año del Fortalecimiento de la Soberanía Nacional"

Lima, 16 de noviembre de 2022
Carta P. 1245-2022-UCV-VA-EPG-F01/J

Ing. De sistemas
Carlos Alfredo Vílchez Benites
Jefe de TI
Soluciones y Servicios LCI

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a ALEMAN BALLADARES, FERNANDO YASMANI; identificado con DNI N° 41867726 y con código de matrícula N° 6000018263; 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:

Norma ISO 27001 para el Control de la Seguridad de Información en una Consultoría Privada, 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 ALEMAN BALLADARES, FERNANDO YASMANI 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,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Dra. Estrella A. Esquiagola Aranda
Jefa
Escuela de Posgrado UCV
Filial Lima Campus Los Olivos

SOLUCIONES Y SERVICIOS LCI SAC
VILCHEZ BENITES CARLOS
JEFE DE SISTEMAS
CIP: 166804

Somos la universidad de los que quieren salir adelante.

ucv.edu.pe

Anexo 4: Galería de fotos

SYSLEINCO	**POLITICAS** **SEGURIDAD DE LA INFORMACION**	FECHA: 27/10/2022 PAG: 2 de 30 VER: 1.5
SUMARIO	Este documento presenta los controles de Seguridad y Privacidad de la Información para la consultoría contable LCI SOLUCIONES Y SERVICIOS; acorde a los requerimientos de la normativa ISO 27001, bajo estrategias de Gobierno Digital y requerimientos de la organización.	
IDIOMA	ESPAÑOL	
CODIGO	LCI-PSI-22	
CATEGORIA	DOCUMENTO TECNICO	
VERIFICADO	GERENCIA GENERAL	ROJAS ZAPATA DEYSI
REALIZADO	JEFE DE SISTEMAS	VILCHEZ BENITES CARLOS
APROBADO	DIRECTIVA INSTITUCIONAL	
Información Adicional:	El presente documento fue verificado mediante auditoria externa, por lo que ante cualquier etapa de mejora o adaptación deberá considerarse una revisión en las fases de planificación, implementación, evaluación y nuevas mejoras.	

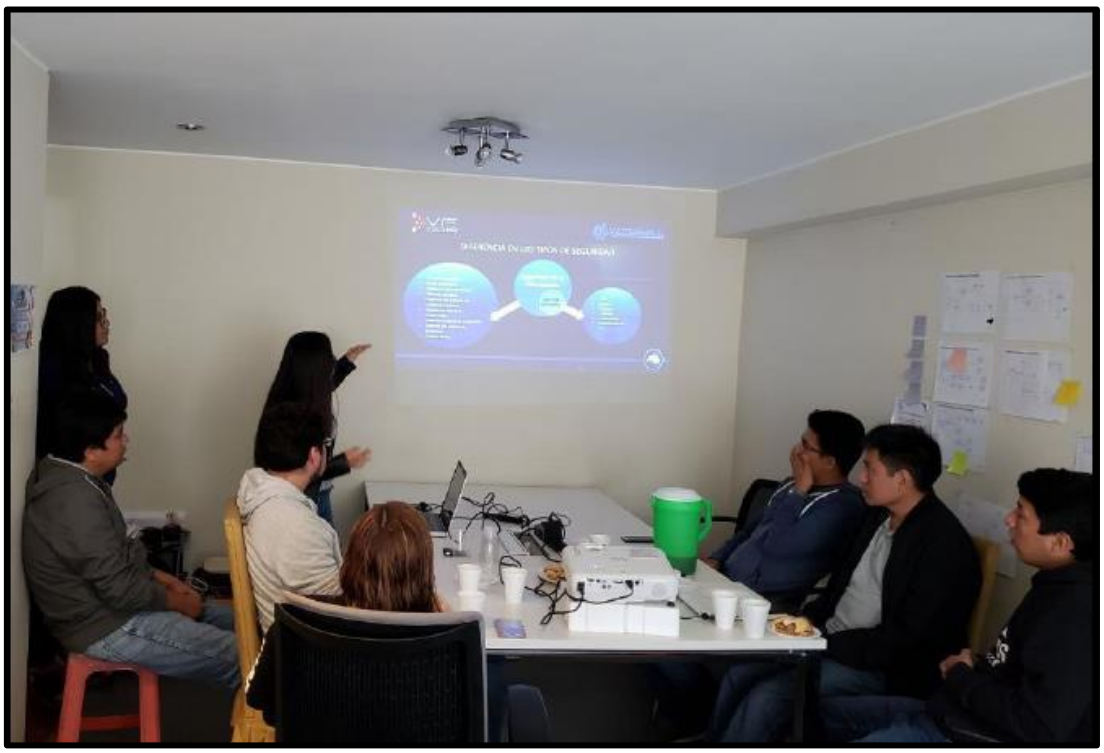
Delgadillo Pardo Ángel
Alta Dirección

Aedo Barrios Franklin
Alta Dirección

Rojas Zapata Deysi
Gerente General

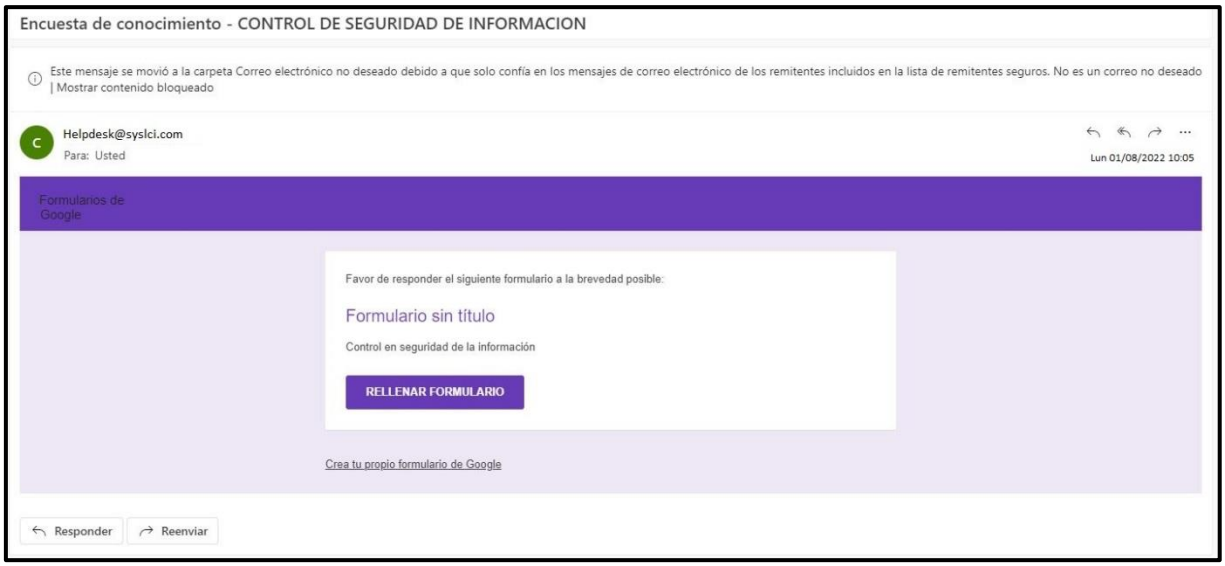
Vilchez Benites Carlos
Jefe de sistemas

Presentación de políticas para seguridad de la información
en la empresa SYS LCI

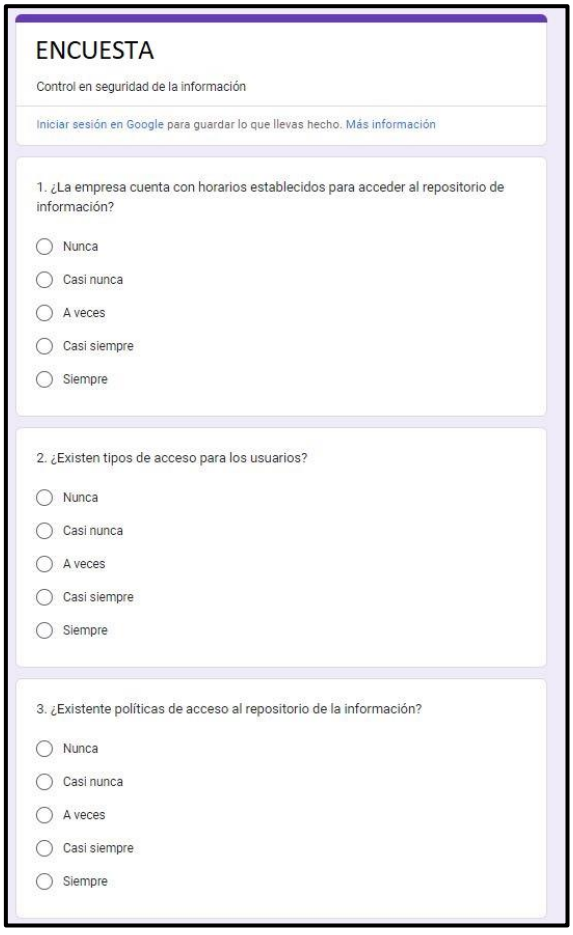


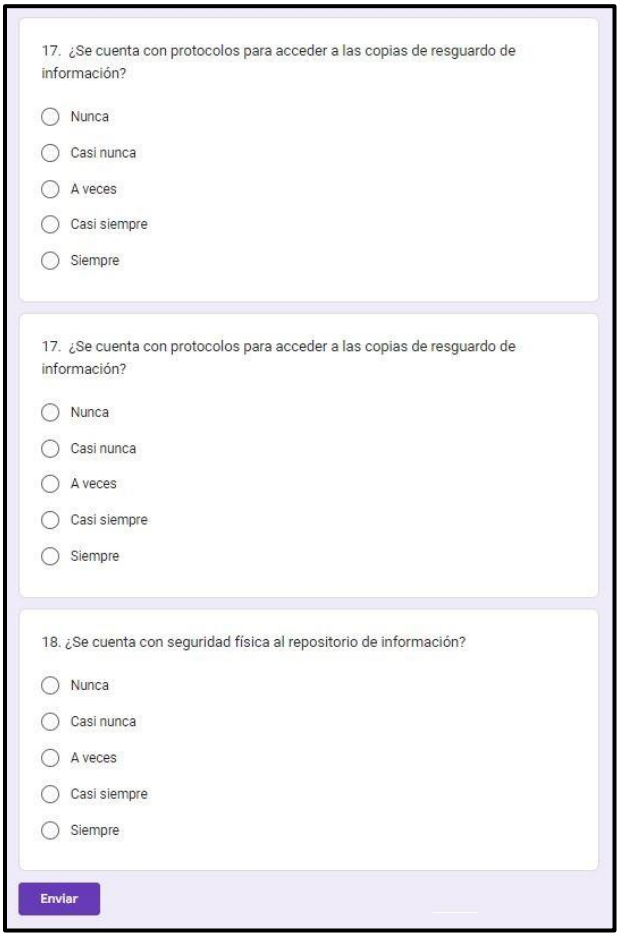
Charla de capacitación a usuarios

Evaluación sobre políticas de seguridad de la información



Notificación por mail para encuesta Pre- test – Post-test





Metodología de Desarrollo para la implementación de la ISO 27001

I. Introducción

De acuerdo con Charlet, 2017, ISO sus siglas significan “Organización Internacional de Normalización”, dentro de sus principales objetivos es ayudar a las organizaciones en su eficacia y eficiencia de sus procesos internos y externos. Así como también Russel (2022) menciona que **La norma ISO 27001:** internacionalmente es la norma más usada para la implementación de un SGSI (Sistema de gestión de seguridad de información), actualmente la versión más usada a nivel latinoamericano es la ISO 27001:2013, ya que se puede prevenir riesgos y mejorar los procesos de información de la organización.

Según Russell (2022) la norma ISO 27001:2013, indica las siguientes ventajas competitivas: resolver los diferentes riesgos de la seguridad de información, ejecutar las acciones preventivas necesarias, garantizar una gestión eficiente en la seguridad de la información y permitir las integraciones de otros modelos de sistemas de gestión más simplificadas.

La empresa privada, lugar donde se desarrolla la investigación, realiza servicios de consultoría Contable. actualmente existe un total de 293 clientes, de los cuales son atendidos y distribuidos entre 78 profesionales (trabajadores), durante su instancia en la consultora ha detectado diversos déficits, de los cuales en conjunto con la gerencia general han priorizado y coincidido que la organización:

No cuenta con políticas en seguridad de la información, lo que impide en mejorar la disponibilidad de la misma en base a una correcta accesibilidad, la mayoría de trabajadores cometen desorden de la información almacenándolas en diferentes ubicaciones, también no existe una correcta distribución de acceso a la información de la empresa.

Existe un déficit en el crecimiento de la información la cual está siendo almacenada de manera improvisada en discos reutilizados y en su mayoría la información se encuentra dividida en diversas unidades por que la capacidad no es suficiente.

Existe retraso para acceder a la información histórica se debe a que la información se encuentra almacenada en unidades externas de almacenamiento, esto dificulta el acceso a la información con urgencia.

El resguardo de información está expuesta a amenazas externas y climáticas, ya que los dispositivos o unidades están almacenados inapropiadamente en cajas o reubicadas en diferentes unidades.

Los siguientes puntos detallados deben de ser resueltos para que la empresa obtenga la seguridad de su información, por consiguiente, se hace de la necesidad de implementar la ISO 27001.

Políticas de gestión en la seguridad de información:

Seguridad de la información: se conceptualiza a partir del conjunto de procedimientos, medidas, técnicas y herramientas que deben asegurar y reaccionar ante cualquier atentado en contra de la información. (Agé, 2013). La seguridad de información según la ISO 27001, cuenta con tres aspectos primordiales enfocados a proteger: integridad, disponibilidad y confidencialidad de la información, de igual modo hace mención que toda organización debe clasificar la información en 3 tipos: critica, valiosa y sensible.

La política del Sistema de gestión de seguridad e información centrará todos los objetivos organizaciones, establecerá un marco referencial para fijar todos los objetivos, a continuación, se describe los criterios con respecto a estimar los riesgos en cuanto al SGSI: se definirá todos los procedimientos para clasificar los riesgos,

se determina toda amenaza, se analiza y evalúa las amenazas, y se determina los objetivos para evaluar la seguridad de información.

1.1. Metodología seleccionada

1.1.1. Ciclo de mejora continua o Deming

Dentro de las definiciones de las fases del ciclo de deming, la norma ISO ya planteo la fase de planificación para su implementación por tal las etapas se conceptualizan de la siguiente manera:

Planificar: incluye toda la creación de objetivos y procesos necesarios para lograr los óptimos resultados requeridos por la organización; también incluye el análisis interno y externo del contexto de la organización para su futura mejora. Asimismo, van a permitir a la organización tener un control autónomo con el fin de realizar un análisis minucioso y poder obtener resultados positivos para el bienestar de la empresa. (Córdova, 2021).

La metodología se enfoca en la aplicación de la ISO 27001:2013, para la cual se procede a realizar las siguientes actividades:

- Se analiza el contexto inicial
- La gerencia se compromete para iniciar la planificación
- Se analiza y comprende el contexto donde se realizará la aplicación.
- Se analiza y comprende que necesidades y expectativas necesitan la organización.
- Se determina cual es el alcance del Sistema de gestión de seguridad de información.
- Se crea los procedimientos para mitigar la gestión de riesgos.
- Se crea los procedimientos para mitigar la gestión de incidencias.
- Se crea el plan para tratar los posibles riesgos.

Hacer: la ISO 27001:2013 indica que la organización debe implementar los procesos importantes y controlarlos a partir del cumplimiento de los objetivos centrales de la seguridad a través del tratamiento de riesgos de la seguridad de la información. Además, implica que en base al conocimiento de riesgos de seguridad se implementen métodos y normas para prevención de ciberataques y perdida parcial o total de información clasificada. (García, 2018).

Las actividades que se realizan son las siguientes:

- Se implementa el plan de tratamiento para mitigar riesgos.
- Se implementa el plan de acción para capacitar y concientizar.

Verificar: En el capítulo 9 de la ISO 27001:2013, señala que la evaluación periódica del desarrollo de la seguridad de la información es importante para garantizar la eficacia del SGSI. Asimismo, es importante señalar que la implementación de la norma ISO 27001:2013 va a permitir tener una mayor influencia en el control de seguridad. (Córdova, 2021).

Las actividades que se realizan son las siguientes:

- La organización se prepara para la auditoría interna.
- Se procede a ejecutar la auditoría interna.
- La gerencia realiza la revisión de los resultados que se han obtenido.

Actuar: Se pretende prevenir circunstancias no deseadas, para así mejorar la ejecución del SGSI a través de acciones innovadores y correctivas. Así pues, es importante indicar que el control de la seguridad de la información busca resguardar toda la información propia de la organización. (García, 2018).

Las actividades que se realizan son las siguientes:

- Se crea el plan de acción para eventos que necesiten correcciones y mejoras.
- Se implementa el plan de acciones correctivas.
- Se analiza cual es la brecha que se ha alcanzado.

1.2. Desarrollo del Proyecto

1.2.1. Fase 1: Planificar

En esta fase se buscó identificar y establecer el Sistema de gestión de seguridad e información, para ellos se procedió a analizar cuál es la brecha que existe para cumplir los requisitos para implementar la ISO 27001:2013.

A continuación, se describe los niveles de cumplimiento para la implementación de la ISO:

No existe evidencia en la pyme que se cumpla los requisitos para la implementación de la ISO. (Porcentaje alcanzado 0%)

Inicio, La pyme ha reconocido que existe problemas y necesitan ser resueltos, de acuerdo al levantamiento de información hay indicios que cumplan este requisito, pero no existe evidencia alguna. (Porcentaje alcanzado al 30%).

Desarrollo, existe un avance considerable en cuanto al cumplimiento de requisitos para la implementación, aun así, no se encuentra al 100%.

Completo, se completa al 100% y se encuentra evidencia.

1.2.1.1. Análisis de la brecha digital

Se realizó el análisis de la brecha de controles de seguridad de información, para todo análisis realizado, se encontró que si es necesario el control de seguridad. Los dominios analizados de acuerdo a la ISO fueron los siguientes:

- Aspectos de seguridad de información
- Gestor de incidentes
- Relación de proveedores
- Adquisición y mantenimiento de sistemas
- Seguridad en las comunicaciones internas y externas
- Seguridad física y ambiental.
- Políticas de seguridad de la información

Para dar cumplimiento a todos resultados analizados se realizó **un acta de reunión** en el cual la empresa da inicio al proceso de implementación de la ISO.

Compromiso de la Gerencia

En este paso del SGSI, la administración y la gerencia explicar cuál es la situación actual de la empresa y se comprometen a cumplir con los recursos, alcances y tiempo para la implementación de la SGSI.

Políticas de seguridad de información

Para determinar cuál es la política de seguridad de la información se ha tenido en cuenta en qué nivel se encuentra la pyme para cumplir los requisitos para la implementación de la ISO 27001, se incluyen los compromisos de la gerencia, el alcance, todos estos aprobados por el gerente general.

Políticas de gestión de contraseñas

Toda contraseña creada en la pyme deberá cumplir los requisitos que el encargado del área de sistemas conjuntamente con el comité de la ISO ha definido, las cuales son:

- Toda contraseña debe al menos contar con 9 caracteres que incluyan el uso de mayúsculas, números y caracteres.
- No se deberá usar la misma contraseña para otro tipo de acceso en el sistema.
- Se deberá realizar el cambio de contraseña dos veces al año.
- No se deberá utilizar contraseñas antiguas.

Política de gestión de accesos

Para determinar cuáles son las políticas de gestión de accesos se delimita cuáles son los accesos que se tiene para los ordenadores, sistemas de información y las redes. Toda medida de control de accesos está orientadas a controlar y monitorizar todo medio digital que tenga acceso a la información de la organización.

- Se limita el acceso a la información y a toda instalación que se tenga acceso a los servicios de red.
- Revisión de credenciales de acceso a los usuarios.

- Gestión de cancelación de credenciales.

Políticas de gestión de incidentes de seguridad

Para determinar la política de gestión de incidentes se realiza los siguientes objetivos:

- Se definen los roles y responsabilidades dentro de la pyme.
- Se gestiona los eventos que conlleven a la seguridad de información con el fin de determinar la clasificación de los incidentes.
- Se aplican las correcciones que se establecen en la política de seguridad de información con la finalidad de mitigar el impacto negativo que pueda suscitarse en la pyme.
- Se definió mecanismos para monitorear el coste de los incidentes.

Política de gestión en la concientización y capacitación

Se determina como el personal se concientiza en las actividades de difusión de las políticas de seguridad de información, para ello se realiza las siguientes actividades:

- Charlas periódicas con respecto a la seguridad de información.
- Campañas de concientización.
- Manuales de procedimiento para mejorar el desempeño de la accesibilidad de información.

1.2.2. Fase 2: Hacer

Implementación del plan de tratamiento de riesgos

Para la implementación del plan de tratamiento de riesgos se aplican las siguientes medidas de control de seguridad:

- Aviso de actualización de datos vía email.
- Organigrama de puestos para identificar responsabilidades
- Memorándum para llamadas de atención.

- Elaboración de ficha de puestos con la finalidad de buscar quienes son las personas con conocimientos en seguridad de información.
- Acuerdos de confidencialidad de la seguridad de información, se procede a señar el uso correcto de toda la información expuesta con el uso de correos electrónicos, clausula para evitar fugas de información.
- Formato de entrega de equipos donde se indica el nombre del personal y especificaciones de equipos asignados.
- Acceso a carpetas para acceso a usuarios, se estructura las carpetas de cada área de la empresa y se específica a las personas que tienen privilegios al uso de cada uno de las carpetas.
- Etiquetado de información y clasificación en la valorización de los activos de la información, así como también en el inventario de activos.

Implementación del plan de capacitación y concientización

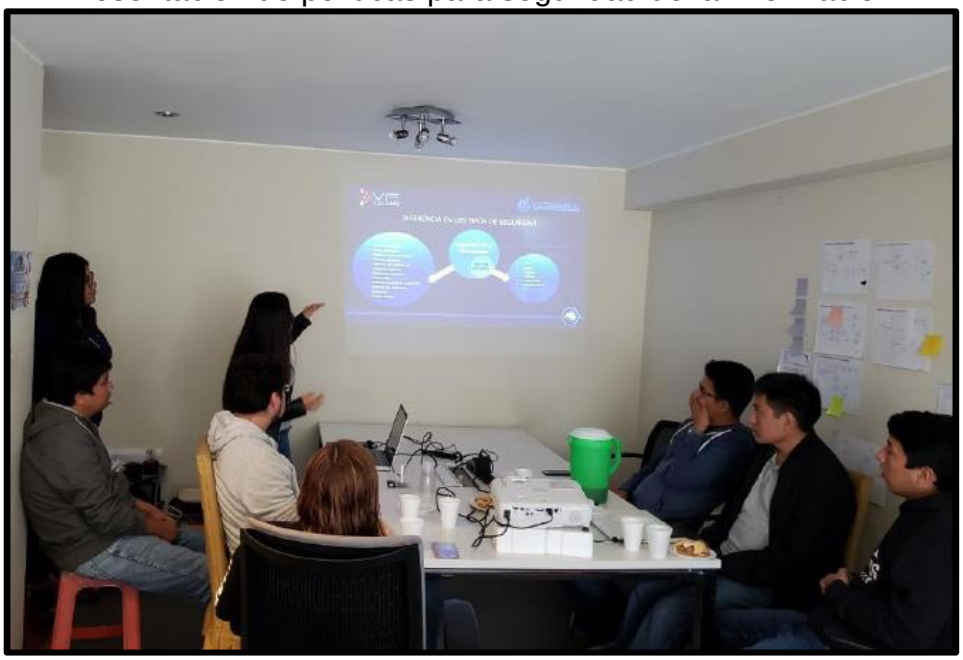
Se realiza charlas de seguridad de información para concientizar al personal sobre el uso de la seguridad de información, se brinda capacitaciones de seguridad a las siguientes áreas:

- Área logística y recursos humanos.
- Área comercial y área de calidad
- Oficina de operaciones.
- Área de mantenimiento.

Campañas de seguridad de información

La campaña de seguridad de información se realizó antes de las charlas y capacitaciones, se utilizaron correos electrónicos para que el personal tenga referencia de los planes de capacitación que tendrá la empresa.

Presentación de políticas para seguridad de la información:



En la empresa SYS LCI

Charla de capacitación a usuarios

1.3. Fase 3: Verificar

Se procede a realizar el monitoreo del funcionamiento del sistema de gestión de seguridad de información, se han controlado las medidas de seguridad y se realizan las auditorías internas para conocer el nivel de riesgo.

Se ejecutó el procedimiento de los seguimientos y revisión de los controles. En esta fase se comprueba si las políticas de seguridad han seguido los procedimientos implementados. Toda evaluación de riesgos se llevó de forma continua y periódica.

Formato 01 del registro de uso del cifrado de seguridad

REGISTRO DE USO DEL CIFRADO

Versión: V.01

Fecha: 18 DE DICIEMBRE DEL 2022

Código: UC2022-01

N°	Unidades de almacenamiento / archivos / carpeta / mensajes	Necesita cifrado		Tipo de cifrado utilizado	Herramienta Utilizada
		SI	NO		
1	DISCO DURO PC ESCRITORIO 1	X		CLAVE PRIVADA	DASHLANE
2	DISCO DURO PC ESCRITORIO 2	X		CLAVE PRIVADA	DASHLANE
3	DISCO DURO PC ESCRITORIO 3	X		CLAVE PRIVADA	DASHLANE
4	DISCO DURO PC ESCRITORIO 4	X		CLAVE PRIVADA	DASHLANE
5	DISCO DURO DE SERVIDOR DE CORREOS	X		CLAVE PRIVADA	DASHLANE
6	DISCO DURO DE SERVIDOR DE ARCHIVOS	X		CLAVE PRIVADA	DASHLANE
7	CARPETA / DDGENERAL/ UNIDAD C / PC ESCRITORIO DE DIRECCION	X		CLAVE PRIVADA	DASHLANE
8	CARPETA / DDSECRETARIA/ UNIDAD C / PC ESCRITORIO DE SECRETARIA	X		CLAVE PRIVADA	DASHLANE
9	CARPETA / DDLOGISTICA/ UNIDAD C / PC ESCRITORIO DE LOGISTICA	X		CLAVE PRIVADA	DASHLANE
10	CARPETA / DDVENTAS/ UNIDAD C / PC ESCRITORIO DE VENTAS	X		CLAVE PRIVADA	DASHLANE

Formato 1. Registro del Uso del Cifrado

Formato 2. Proceso para realizar el proceso de backup

Proceso para realizar el respaldo de información	
Versión:V.01 Fecha: 17 DE DICIEMBRE DEL 2022 Código: PR. BCKUP-01	
Responsable Nombres y apellidos: JORGE CARDENAS MOGROVEJO Cargo: ADMINISTRADOR DE SISTEMAS Correo:JCARDENAS220@GMAIL.COM	
Tipo de información a respaldar	
Fuente de datos: (Carpetas, documentos en office, bases de datos, archivos del sistema entre otros.	SE PROCEDE A REALIZAR LA COPIA DE SEGURIDAD DE LAS CARPETAS ASIGNADAS A LAS AREAS DE VENTAS, LOGISTICA, DIRECCION Y SECRETARIA
Respaldo alojado en toda unidad compartida.	SE RESPALDA LA INFORMACIÓN EN EL SERVIDOR DE ARCHIVOS CON UNA COPIA DE SEGURIDAD EN LA NUBE
Listar archivos a respaldar.	- ARCHIVO DE VENTAS DEL MES DE OCTUBRE - ARCHIVO DE VENTAS DEL MES DE NOVIEMBRE - ARCHIVO DE COMPRAS DEL AREA DE LOGISTICA
Información del Servidor a respaldar	- SERVIDOR DE ARCHIVOS HP UBICACIÓN, SALA DE SERVIDORES
Detalle del respaldo.	- ARCHIVOS GENERADOS DEL MES DE OCTUBRE Y NOVIEMBRE

Formato 2. Proceso para realizar el proceso de backup

Formato 03: Acceso a los recursos compartidos en Red

Acceso de los recursos compartidos en red Versión:V.01 Fecha:18 DE OCTUBRE DEL 2022 Código: ARR-2022-01		
DATOS DEL RESPONSABLE		
Departamento: LOGISTICA Nombres y apellidos: MARTIN CACERES Teléfono y extensión: 51-5475263 - 0021 Correo: LOGISTICA2012.T@GMAIL.COM		
DATOS DEL SOLICITANTE Departamento: VENTAS Nombres y apellidos: MIRIAM CARDENAS Teléfono y extensión: 51-5475263 -0020 Correo: VENTAS2021.V@GMAIL.COM		
DATOS DEL RECURSOS Nombre del servidor: HP-SERVER2018-ST001 Nombre de los recursos: ARCHIVOS DE COMPRAS Ruta a la cual se solicita acceder: : C://PCESCRITORIO/LOGISTICA*COMPRAS2022		
N°	Nombres y Apellidos MARTIN CACERES	Permisos Asignados ACCESO A CARPETA DE COMRAS

Formato 3 Acceso a los recursos compartidos en red

Formato 4 Asignación de roles y responsabilidades de personal

Asignación de roles y responsabilidades del personal Versión: V.01 Fecha: 18 DE OCTUBRE DEL 2022 Código: ARP-2022-01			
Nombre	**Rol**	**Responsabilidad**	**Actividad**
MARTIN CACERES	Administrador	Encargado del área de logística	Acceso a carpeta de logística
MIRIAM CARDENAS	Administrador	Encargado del área de ventas	Acceso a carpeta de ventas
FERNANDO ESPINOZA	Técnico Soporte	Encargado del área de helpdesk	Soporte técnico
ROGER CACERES	Técnico Soporte	Encargado del área de helpdesk	Soporte técnico
TANIA MENDEZ	Administrador	Encargado del área de secretaria	Acceso a carpeta de secretaria
EDUARDO COSSER	Administrador	Encargado del área de producción	Acceso a carpeta de producción

Formato 4 Acceso de roles y responsabilidades

Formato 5 Informe de utilización de antivirus en los equipos

<table>
<tr><td colspan="3">Informe de utilización de antivirus en los equipos</td></tr>
<tr><td rowspan="2">Versión: v.01
Fecha: 20 de octubre del 2022
Código: CS-011254-01</td><td colspan="2">Versión: v.01</td></tr>
<tr><td>Fecha:
20 de octubre del 2022</td><td>Código:
CS-011254-01</td></tr>
<tr><td colspan="3">Nombre del equipo: LAPTOP INTEL CORE I3 INSIDE – ESCRITORIO 01-VENTAS</td></tr>
<tr><td colspan="3">Dirección del equipo: AREA DE VENTAS 01</td></tr>
<tr><td colspan="3">Sistema operativo: WINDOWS 8.1</td></tr>
<tr><td colspan="3">Usuario del equipo: MIRIAM CARDENAS</td></tr>
<tr><td colspan="3">Departamento: VENTAS</td></tr>
<tr><td colspan="3">Tipo de antivirus adquirido: AVAST ANTIVIRUZ</td></tr>
<tr><td colspan="3">Tipo de licenciamiento: ANUAL</td></tr>
<tr><td colspan="3">¿Protección en tiempo real? SI</td></tr>
<tr><td colspan="3">¿Actualización automática? ACTIVADO</td></tr>
<tr><td colspan="3">OBSERVACIONES: SE VENCE EL 30 DE DICIEMBRE DEL 2022</td></tr>
</table>

Formato 6: Plan de pruebas del sistema de información

<table>
<tr><td colspan="3">Plan de pruebas del sistema de información</td></tr>
<tr><td rowspan="2"></td><td colspan="2">Versión: V.01</td></tr>
<tr><td>Fecha: 21 DE OCTUBRE DEL 2022</td><td>Código: PSI-01254-FT</td></tr>
<tr><td colspan="3">Descripción: Se procede a revisar vulnerabilidades del sistema operativo.</td></tr>
<tr><td colspan="3">Pre requisitos: activación de Windows 8 y security defender, firewall</td></tr>
<tr><td colspan="3">Procedimientos a seguir: revisión de licenciamiento, licencia de antivirus, puertos abiertos y acceso de red.</td></tr>
<tr><td colspan="3">Resultado esperado: licencia de antivirus actualizado, y firewall en estado optimo</td></tr>
<tr><td colspan="3">Resultado Obtenido: licencias ya adquiridas para la renovación anual.</td></tr>
</table>

1.4. Fase 4: Actuar

Luego de haber implementado el plan de seguridad de información de acuerdo a las buenas prácticas que nos dice la ISO 27001 se realizó los siguientes puntos:

Alcance del plan de seguridad informática

SYSLEINCO	**POLITICAS** **SEGURIDAD DE LA INFORMACION**	FECHA: 27/10/2022 PAG: 2 de 30 VER: 1.5
SUMARIO	Este documento presenta los controles de Seguridad y Privacidad de la Información para la consultoría contable LCI SOLUCIONES Y SERVICIOS; acorde a los requerimientos de la normativa ISO 27001, bajo estrategias de Gobierno Digital y requerimientos de la organización.	
IDIOMA	ESPAÑOL	
CODIGO	LCI-PSI-22	
CATEGORIA	DOCUMENTO TECNICO	
VERIFICADO	GERENCIA GENERAL	ROJAS ZAPATA DEYSI
REALIZADO	JEFE DE SISTEMAS	VILCHEZ BENITES CARLOS
APROBADO	DIRECTIVA INSTITUCIONAL	
Información Adicional:	El presente documento fue verificado mediante auditoria externa, por lo que ante cualquier etapa de mejora o adaptación deberá considerarse una revisión en las fases de planificación, implementación, evaluación y nuevas mejoras.	

Delgadillo Pardo Ángel
Alta Dirección

Aedo Barrios Franklin
Alta Dirección

Rojas Zapata Deysi
Gerente General

Vilchez Benites Carlos
Jefe de sistemas

En el departamento de tecnologías de información y comunicación se incluyen todos los ordenadores y servidores y laptops que se conectan a la red, el área de TICS es la que se encarga de la distribución y mantenimiento.

Las funciones de los servidores son el almacenamiento de archivos y la distribución de toda la información que tiene la empresa, los servidores encontrados son: 1 Servidor de archivos y un servidor de base de datos. La base de datos de la empresa se encuentra almacenada en el servidor de archivos, se encontraron los siguientes sistemas almacenados:

- CONCAR (sistema contable que maneja la empresa)
- SIFFA (sistema de control de activos)
- SOFT (Sistema que controla el inventario de la empresa)
- SGDI (Sistema que recibe los incidentes de la empresa)
- OFFICE para la elaboración de documentos

Caracterización del sistema informático

- El cableado de red se encuentra a base de cables UTP de categoría 6, su velocidad de transmisión es de 100 Mbps.
- La conexión de red está desde un punto troncal, a base de switch administrables, este tipo de switch trabaja conjuntamente con el router para brindar los servicios de internet.
- El personal que maneja los equipos de seguridad tiene sólidos conocimientos para resolver cualquier tipo de incidente.

Resultados del análisis de riesgos

Los activos que han sido protegidos son los siguientes:

- Red de trabajo optimizada
- Servicios de correo electrónico activos
- Base de datos centralizada correctamente
- Servidor de archivos direccionando correctamente.

Las amenazas que fueron identificadas y que cobran importancia son las siguientes:

- Presencia de los virus informáticos en las computadoras
- Pishing
- Fuga de información
- Escaso monitoreo de la red
- Fallas de hardware.

Política de contraseñas

- El personal del área de TIC´s requerirá el nombre del usuario y contraseña cuando se requiera dar uso del sistema de información.
- Las contraseñas han sido cambiadas cada 30 días.
- Cuando el usuario detecto que su información fue vulnerada, el departamento de TIC´s notificó de inmediato la fuga de información.
- Se proceden a aplicar los formatos de seguridad.
- Cuando un usuario se desvincula de la empresa, inmediatamente el departamento de información procede a suspender sus credenciales, pero no los elimina para resguardar la información.
- Si existe incumplimiento de la política de contraseñas el departamento de seguridad comunicará al área administrativa para que considere las acciones administrativas que está corresponda.

Política de uso de correo electrónico

- Las cuentas de correo electrónico son usadas solamente con fines laborables
- Toda información que se transmite por vía correo siempre es confidencial
- Si un usuario identificó que un correo es de un remitente no seguir, este deberá de evitar recepcionarlo.

- Si se encuentra un correo con acción de spam deberá ser eliminado.
- En los correos electrónicos que se han creado existe en la bandeja de entrada una carpeta con el nombre de Resguardo.

Política de la información clasificada

- Toda información es clasificada según la prioridad que está requiera.
- Se ha procedido a implementar etiquetas para clasificar la información.
- Se elaboró documentos que registren la información de todo activo que tiene la empresa.
- Se elaboró documentos el cual establece la clasificación de reservado, confidencial.
- La pyme se hará responsable si los usuarios no siguen la política de confidencialidad.
- Los acuerdos que han firmado los usuarios entraran en vigencia cuando se hayan vulnerado la clasificación de la información.
- La organización se reserva el derecho de la evaluación periódica.

Política de navegación

- El acceso que tienen los usuarios al servicio de internet siempre está sujeta a las políticas que brinda el departamento de tecnología de información y comunicación.
- Los usuarios no tienen acceso a redes sociales, a través de proxys se limita el acceso.
- Se monitora de forma periódica el acceso a internet.
- Se ha procedido a implementar etiquetas para clasificar la información.
- Se ha procedido a monitorear los ordenadores conectados a la red, para conocer si no está actualizado los parches de seguridad.

Política de resguardo de información

- El jefe del área de TIC´s selecciona cuales son los componentes que son más eficaces para guardar la información.
- Se procedió a realizar las copias de seguridad de información.
- Se procedió a cifrar toda información que sea de carácter confidencial.
- Se procedió a elaborar formatos para llevar el registro de resguardo de información.
- Se procedió a determinar la ubicación de los archivos de seguridad.
- Se procedió a realizar copias de seguridad a la nube.

Anexo 6: Matriz de consistencia

Problema	Objetivos	Hipótesis	**Variable Independiente:** Implementación de Norma ISO 27001:2013				
			Dimensiones	**Indicadores**	**Ítems**	**Escala de medición**	**Niveles rangos**
Problema general ¿Cómo influye la implementación de la norma ISO 27001:2013 para el control de seguridad de información en la consultoría privada? **Problema Específico** ¿Cómo influye la implementación de la norma ISO 27001:2013 en la disponibilidad de la información para el control de seguridad de información?	**Objetivo General** Determinar en qué medida influye la implementación de la norma ISO 27001:2013 en el control de seguridad de información en una consultoría privada **Objetivo Específico** Determinar en qué medida influye la disponibilidad de la información para el control de seguridad de información.	**Hipótesis General** La norma ISO 27001:2013 mejorará el control de seguridad de información en la consultoría privada. **Hipótesis Específico** La norma ISO 27001:2013 gestiona correctamente la disponibilidad de la información para el control de seguridad de información.	Planificación	• Análisis de brecha inicial • Compromiso de alta dirección • Comprender el contexto de la organización • Comprender necesidades y expectativas • Determinar el alcance del SGSI • Determinar políticas de SI • Determinar objetivos de SI • Crear procedimiento de gestión de riesgos • Crear procedimiento de gestión de incidencia • Crear procedimiento de auditoría interna • Gestionar los riesgos • Crear plan de tratamiento de riesgos • Determinar la declaración de aplicabilidad • Crear plan de capacitación y concientización.	1-16	Escala Likert 0 Muy Bajo 1 Bajo 2 Medio Bajo 3 Medio 4 Medio Alto 5 Alto	0 – 22 % No existe 23 – 50 % Inicio 51 – 75 % En proceso 76 – 100 % Completo
			Ejecución	• Implementar plan de tratamiento de riesgos • Implementar plan de capacitación y concientización	17-19		
			Verificación	• Preparar la auditoría interna • Ejecutar auditoria • Revisar con la alta dirección los resultados obtenidos	20-23		
			Mejora Continua	• Crear plan de acciones correctivas • Implementar plan de acciones correctivas • Análisis de brecha final	24-25		

			Variable Dependiente: Control de seguridad de información				
			Dimensiones	**Indicadores**	**Ítems**	**Escala de medición**	**Niveles y rangos**
Problema Específico	**Objetivo Específico**	**Hipótesis Específico**				Escala Likert	
¿Cómo influye la implementación de la norma ISO 27001:2013 en la disponibilidad de la información para el control de la seguridad de información?	Determinar en qué medida influye la disponibilidad de la información para el control de la seguridad de información.	La norma ISO 27001:2013 gestiona correctamente la disponibilidad de la información para el control de la seguridad de información.	Disponibilidad	• Tiempos de acceso • Tipos de acceso • Políticas de acceso	1-4	0 Nunca	Muy Bajo 0 – 15 %
¿Cómo influye la implementación de la norma ISO 27001:2013 en la Adaptabilidad de la información para el control de la seguridad de información?	Determinar en qué medida influye la Adaptabilidad de la información para el control de la seguridad de información.	La norma ISO 27001:2013 gestiona correctamente la Adaptabilidad de la información para el control de la seguridad de información.	Adaptabilidad	• Crecimiento de información • Adaptación de nuevas tecnologías • Espacio disponible • Capacidad de almacenamiento físico	5-9	1 Casi Nunca 2 A veces	Bajo 16 - 30 % Medio 31 – 60 % alto 61 – 80 %
¿Cómo influye la implementación de la norma ISO 27001:2013 en la Accesibilidad de la información para el control de la seguridad de información?	Determinar en qué medida influye la Accesibilidad de la información para el control de la seguridad de información.	La norma ISO 27001:2013 gestiona correctamente la Accesibilidad de la información para el control de la seguridad de información.	Accesibilidad	• Acceso a consultas • Tiempo de respuesta	10-13	3 Casi siempre	Muy Alto - 100 %

¿Cómo influye la implementación de la norma ISO 27001:2013 en el resguardo de la información para el control de la seguridad de información?	Determinar en qué medida influye en el resguardo de la información para el control de la seguridad de información.	La norma ISO 27001:2013 gestiona correctamente el resguardo de la información para el control de seguridad de información	Resguardo	• Respaldo de seguridad • Almacenamiento del respaldo de seguridad • Acceso al respaldo de seguridad • Seguridad física	14-18	4 Siempre	

Anexo 7: Foto de Base de datos

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD
1	PRETEST		Preguntas	4 Disponibilidad (%)						5 Adaptabilidad (%)							4 Accesibilidad (%)						5 Resguardo (%)							
2	Control de seguridad de información	78	Trabajador	1	2	3	4	1(	10	1	2	3	4	5	2(	10	1	2	3	4	1	10	1	2	3	4	2	1	TOTAL (S
3			1	1	0	0	1	2	13	0	1	0	1	1	3	15	0	0	0	0	0	0	1	0	1	1	1	4	20	12
4	0		2	1	1	0	1	3	19	0	0	0	1	0	1	5	0	0	0	1	1	6	1	1	1	0	1	4	4	9
5	Nunca		3	0	0	1	0	1	6	1	1	1	1	1	5	25	0	1	0	0	1	6	1	0	1	1	0	3	1	10
6	1		4	0	0	0	0	0	0	1	1	1	0	0	3	15	1	0	1	1	3	19	1	0	1	0	0	2	0	8
7	Casi nunca		5	0	0	0	1	1	6	0	1	0	1	1	3	15	0	1	0	0	1	6	1	0	0	0	1	2	0	7
8	2		6	0	0	0	1	1	6	1	0	0	0	0	1	5	1	1	1	1	4	25	1	1	1	1	1	5	0	9
9	A veces		7	1	0	1	1	3	19	0	0	0	1	1	2	10	0	1	1	0	2	13	0	0	1	1	0	2	0	10
10	3		8	0	1	0	1	2	13	0	0	0	1	0	1	5	0	1	1	1	3	19	0	1	0	1	1	3	0	9
11	Casi siempre		9	1	0	1	1	3	19	1	0	1	0	1	3	15	0	0	1	0	1	6	1	0	1	0	1	3	0	10
12	4		10	1	1	1	0	3	19	1	1	1	0	1	4	20	1	1	0	0	2	13	0	1	0	1	0	2	0	13
13	Siempre		11	0	1	1	0	2	13	0	0	1	1	0	2	10	0	1	1	1	3	19	1	1	1	1	0	4	0	10
14			12	0	1	1	1	3	19	1	0	1	0	1	3	15	1	0	0	0	1	6	1	0	0	0	1	2	0	10
15			13	0	0	1	1	2	13	0	0	1	0	0	1	5	1	0	0	1	2	13	1	1	1	0	0	3	0	8
16			14	0	1	0	0	1	6	1	1	0	0	1	3	15	1	0	0	0	1	6	1	0	0	0	0	1	0	7
17			15	1	0	0	1	2	13	1	0	1	0	1	3	15	0	1	0	0	1	6	0	1	1	1	1	4	0	8
18	0 - 15		16	0	0	0	0	0	0	0	1	1	1	1	4	20	1	0	1	1	3	19	0	0	1	0	0	1	0	10
19	muy bajo		17	0	1	1	0	2	13	0	0	0	1	0	1	5	0	0	1	1	2	13	0	1	1	0	1	3	0	8
20	16 al 30		18	1	1	1	0	3	19	1	0	1	0	0	2	10	0	0	1	1	2	13	0	0	0	0	1	1	0	10
21	Bajo		19	1	0	0	1	2	13	0	0	1	0	1	2	10	1	1	1	0	3	19	0	1	0	0	1	2	0	10
22	31 al 60		20	1	1	0	1	3	19	0	1	0	0	1	2	10	1	0	0	0	1	6	0	1	1	1	0	3	0	9
23	Medio		21	0	0	0	1	1	6	1	0	0	1	0	2	10	0	1	1	1	3	19	1	1	1	0	0	3	0	9
24	61 al 80		22	1	0	0	1	2	13	0	1	1	0	0	2	10	0	1	0	1	2	13	1	1	1	1	0	4	0	9
25	Alto		23	1	0	1	1	3	19	0	1	1	1	1	4	20	1	0	1	0	2	13	1	0	0	1	1	3	0	13
26	81 al 100		24	1	0	1	0	2	13	1	1	0	0	1	3	15	1	0	0	0	1	6	0	1	0	0	1	2	0	8
27	Muy Alto		25	1	0	0	0	1	6	0	0	1	0	0	1	5	0	0	1	1	2	13	0	1	1	0	0	2	0	6
28			26	0	0	1	0	1	6	0	0	0	0	1	1	5	1	1	1	1	4	25	1	1	0	0	1	3	0	9
29			27	1	0	0	1	2	13	1	1	0	1	1	4	20	1	1	0	1	3	19	0	0	0	1	1	2	0	13
30			28	0	1	1	0	2	13	0	0	0	0	1	1	5	1	0	1	1	3	19	1	0	1	0	0	2	0	9
31			29	1	1	1	0	3	19	1	1	1	0	0	3	15	1	0	0	0	1	6	1	0	1	0	0	2	0	10
32			30	0	0	1	0	1	6	1	0	1	1	1	4	20	0	1	1	0	2	13	0	1	0	0	1	2	0	10
33			31	1	1	1	0	3	19	0	0	0	1	0	1	5	1	0	0	1	2	13	0	1	1	1	1	4	0	9
34			32	0	0	1	0	1	6	0	0	1	1	1	3	15	0	0	1	0	1	6	1	0	1	1	1	4	0	7
35			33	1	1	0	0	2	13	0	1	1	1	0	3	15	0	1	0	1	2	13	0	1	1	0	0	2	0	10
36			34	0	0	1	1	2	13	0	0	0	0	0	0	0	0	1	1	0	2	13	0	0	1	1	0	2	0	6
37			35	1	1	0	1	3	19	0	0	1	1	1	3	15	1	1	1	1	4	25	1	0	0	1	1	3	0	15
38			36	0	0	1	0	1	6	1	0	0	0	1	2	10	0	1	1	1	3	19	1	0	1	0	1	3	0	9
39			37	0	1	0	0	1	6	0	1	1	1	1	4	20	1	0	0	1	2	13	0	1	1	0	1	3	0	10
40			38	1	1	0	1	3	19	1	1	0	1	1	4	20	1	1	0	1	3	19	1	0	1	1	0	3	0	14
41			39	1	0	0	0	1	6	0	0	0	0	1	1	5	1	0	0	0	1	6	0	1	0	0	1	2	0	4
42			40	1	0	1	1	3	19	1	1	1	0	1	4	20	1	0	0	1	2	13	1	1	0	1	1	4	0	13
43			41	1	0	1	1	3	19	0	1	1	1	0	3	15	1	0	0	1	2	13	1	0	1	0	1	3	0	12
44			42	0	0	1	0	1	6	0	0	0	0	1	1	5	1	1	0	1	3	19	0	0	0	1	1	2	0	8
45			43	1	0	0	0	1	6	1	0	0	1	1	3	15	1	1	0	0	2	13	1	1	0	0	0	2	0	8
46			44	0	1	0	1	2	13	1	1	1	0	0	3	15	0	1	0	1	2	13	1	0	0	1	0	2	0	10
47			45	1	1	0	1	3	19	1	0	1	1	0	3	15	0	1	1	0	2	13	1	0	0	0	0	1	0	12
48			46	1	1	1	1	4	25	1	0	1	0	0	2	10	0	1	0	1	2	13	0	1	0	1	1	3	0	12
49			47	1	1	0	1	3	19	1	0	1	1	1	4	20	0	1	1	1	3	19	1	0	1	1	1	4	0	14
50			48	1	1	1	0	3	19	0	0	1	0	0	1	5	1	1	0	1	3	19	0	0	0	1	1	2	0	11

51		49	1	1	0	1	3	19	0	0	0	0	1	1	5	1	0	1	0	2	13	0	0	0	0	0	0	0	9
52		50	0	1	0	0	1	6	0	1	1	0	0	2	10	1	1	1	0	3	19	0	1	1	1	1	4	0	9
53		51	0	1	0	0	1	6	0	0	0	1	1	2	10	0	1	1	0	2	13	0	1	1	0	1	3	0	7
54		52	1	0	1	1	3	19	0	1	1	1	1	4	20	0	1	0	1	2	13	1	1	0	0	0	2	0	13
55		53	0	1	1	1	3	19	0	1	0	1	0	2	10	1	1	0	1	3	19	1	0	1	0	0	2	0	12
56		54	1	1	1	1	4	25	1	1	1	1	0	4	20	1	0	1	1	3	19	1	0	1	1	0	3	0	16
57		55	1	0	1	1	3	19	1	1	0	1	0	3	15	0	0	0	0	0	0	0	1	1	1	1	4	0	8
58		56	0	1	0	1	2	13	0	1	0	1	0	2	10	1	1	1	0	3	19	0	0	0	0	1	1	0	10
59		57	0	1	1	1	3	19	0	1	0	1	1	3	15	1	1	0	1	3	19	0	1	0	0	1	2	0	13
60		58	0	0	1	1	2	13	1	1	0	0	0	2	10	0	1	0	0	1	6	1	1	1	1	0	4	0	7
61		59	1	0	0	0	1	6	1	1	0	0	1	3	15	1	1	1	0	3	19	1	0	0	1	0	2	0	10
62		60	1	0	0	0	1	6	0	0	0	0	0	0	0	1	0	0	0	1	6	1	0	1	0	0	2	0	3
63		61	1	1	0	1	3	19	0	1	1	1	0	3	15	1	0	1	0	2	13	0	0	0	1	0	1	0	12
64		62	1	0	0	0	1	6	0	0	1	0	1	2	10	1	0	1	0	2	13	1	1	1	1	1	5	0	7
65		63	0	1	0	0	1	6	1	1	1	0	1	4	20	1	0	1	1	3	19	1	0	1	0	0	2	0	11
66		64	1	1	0	0	2	13	1	1	1	0	0	3	15	1	0	0	0	1	6	1	0	1	1	1	4	0	8
67		65	0	1	1	1	3	19	0	0	0	1	1	2	10	1	0	0	1	2	13	0	0	0	0	0	0	0	10
68		66	0	1	1	1	3	19	0	0	1	0	0	1	5	0	1	0	0	1	6	0	0	1	0	1	2	0	8
69		67	0	0	0	1	1	6	0	1	1	0	0	2	10	0	0	0	1	1	6	0	0	1	0	0	1	0	6
70		68	1	0	1	0	2	13	0	1	0	1	0	2	10	0	0	0	0	0	0	0	0	0	0	1	1	0	6
71		69	1	1	1	0	3	19	0	0	0	0	0	0	0	1	1	1	0	3	19	0	0	0	0	0	0	0	9
72		70	0	0	1	0	1	6	1	1	0	0	0	2	10	1	1	0	0	2	13	1	1	0	1	1	4	0	7
73		71	0	1	1	0	2	13	1	0	1	1	1	4	20	1	1	0	0	2	13	1	0	0	0	1	2	0	11
74		72	0	0	1	0	1	6	1	0	1	1	1	4	20	0	0	0	1	1	6	0	0	0	1	0	1	0	8
75		73	0	0	0	0	0	0	1	1	1	1	0	4	20	1	1	0	0	2	13	1	1	1	1	1	5	0	8
76		74	0	1	0	0	1	6	1	0	0	0	1	2	10	0	0	0	0	0	0	0	1	0	0	1	2	0	4
77		75	0	1	1	1	3	19	0	0	1	1	1	3	15	1	0	1	1	3	19	1	0	1	0	1	3	0	13
78		76	1	1	1	0	3	19	1	1	0	1	0	3	15	0	1	0	1	2	13	1	1	1	1	0	4	0	12
79		77	1	1	1	1	4	25	1	1	1	1	1	5	25	1	0	1	0	2	13	1	1	0	0	1	3	0	16
80		78	1	1	0	1	3	19	1	1	1	0	0	3	15	1	1	0	1	3	19	1	0	1	0	1	3	0	13

84	POSTEST		Preguntas	4 Disponibilidad (%)						5 Adaptabilidad (%)							4 Accesibilidad (%)						5 Resguardo (%)							
85	Control de seguridad de información	78	Trabajador	1	2	3	4	16	100	1	2	3	4	5	20	100	1	2	3	4	16	100	1	2	3	4	5	20	100	
86	0: Nunca		1	4	4	3	3	14	88	3	4	4	4	4	19	95	4	4	4	4	16	100	3	4	3	3	3	16	80	91
87	1: Casi Nunca		2	4	3	3	3	13	81	3	3	4	4	3	17	85	3	3	3	3	12	75	3	4	3	3	4	17	85	82
88	2: A veces		3	3	4	3	4	14	88	3	4	4	4	4	19	95	3	4	4	4	15	94	3	3	3	4	3	16	80	89
89	3: Casi siempre		4	4	3	3	4	14	88	3	4	4	4	3	18	90	4	3	4	3	14	88	4	4	3	3	3	17	85	88
90	4: Siempre		5	4	4	4	3	15	94	4	4	3	3	4	18	90	3	4	3	4	14	88	4	4	3	4	4	19	95	92
91			6	3	3	4	4	14	88	3	3	4	4	4	18	90	3	4	4	4	15	94	3	3	4	3	4	17	85	89
92			7	4	3	4	4	15	94	3	3	3	4	4	17	85	4	4	3	4	15	94	4	4	4	3	4	19	95	92
93			8	4	3	4	4	15	94	3	4	3	4	3	17	85	3	3	3	3	12	75	3	3	3	4	3	16	80	83
94			9	3	4	4	3	14	88	3	4	4	3	3	17	85	4	3	4	4	15	94	4	3	4	4	4	19	95	90
95			10	3	3	3	4	13	81	3	4	4	3	4	18	90	4	4	3	4	15	94	4	4	4	3	4	19	95	90
96			11	3	3	4	3	13	81	4	4	4	4	3	19	95	4	3	3	4	14	88	3	4	3	4	3	17	85	87
97			12	3	3	4	3	13	81	4	4	3	3	4	18	90	4	3	4	3	14	88	3	3	4	3	4	17	85	86
98			13	4	4	3	4	15	94	4	3	3	4	3	17	85	4	4	3	3	14	88	3	3	4	3	4	17	85	88
99			14	4	3	4	3	14	88	3	4	3	4	4	18	90	3	4	3	3	13	81	4	3	4	3	4	18	90	87
100			15	4	3	3	3	13	81	3	3	3	4	3	16	80	4	4	3	4	15	94	4	3	3	4	4	18	90	86
101			16	4	4	3	4	15	94	3	4	4	3	3	17	85	3	4	4	3	14	88	4	3	3	3	3	16	80	87
102			17	4	4	3	4	15	94	3	3	4	4	3	17	85	4	4	4	3	15	94	4	3	4	4	3	18	90	91
103			18	3	4	4	4	15	94	4	4	4	3	3	18	90	4	4	3	3	14	88	3	3	3	3	3	15	75	87
104			19	4	4	4	3	15	94	4	3	3	3	4	17	85	4	4	3	3	14	88	3	4	4	4	3	18	90	89
105			20	3	4	4	3	14	88	3	3	3	4	3	16	80	4	3	4	4	15	94	4	3	4	4	4	19	95	89
106			21	3	3	3	3	12	75	3	3	4	3	4	17	85	3	4	4	3	14	88	3	3	3	4	4	17	85	83

107		22	3	3	3	4	13	81	4	4	4	3	4	19	95	4	4	3	4	15	94	3	3	3	4	4	17	85	89
108		23	3	3	4	4	14	88	4	4	4	3	4	19	95	4	3	4	3	14	88	4	3	4	4	4	19	95	91
109		24	4	3	3	4	14	88	3	3	3	4	4	17	85	4	4	3	4	15	94	4	3	3	4	3	17	85	88
110		25	3	4	4	3	14	88	3	4	3	4	3	17	85	4	4	4	3	15	94	4	4	4	3	4	19	95	90
111		26	3	3	3	4	13	81	4	3	4	4	4	19	95	4	4	4	4	16	100	3	4	3	3	3	16	80	89
112		27	3	4	3	3	13	81	3	4	3	3	3	16	80	3	4	3	3	13	81	3	3	3	4	4	17	85	82
113		28	4	4	3	4	15	94	3	3	3	4	3	16	80	3	3	3	3	12	75	3	4	4	4	4	19	95	86
114		29	4	3	4	3	14	88	3	4	3	4	4	18	90	4	4	3	3	14	88	3	4	4	4	3	18	90	89
115		30	3	4	4	3	14	88	4	4	4	3	3	18	90	4	4	3	3	14	88	3	4	4	3	3	17	85	88
116		31	3	3	4	4	14	88	3	3	4	4	3	17	85	3	3	3	4	13	81	3	3	4	4	4	18	90	86
117		32	3	3	3	3	12	75	4	4	3	4	4	19	95	3	3	3	3	12	75	3	4	3	3	4	17	85	83
118		33	4	3	4	4	15	94	4	4	3	3	3	17	85	3	4	4	4	15	94	4	3	3	4	4	18	90	91
119		34	3	3	3	4	13	81	4	4	3	3	3	17	85	3	3	4	3	13	81	4	3	3	4	3	17	85	83
120		35	4	3	4	4	15	94	3	3	3	4	4	17	85	4	3	3	3	13	81	4	3	3	4	3	17	85	86
121		36	3	3	4	4	14	88	4	4	4	3	4	19	95	3	4	4	4	15	94	3	4	4	3	3	17	85	90
122		37	4	3	3	4	14	88	4	4	3	4	4	19	95	4	4	3	4	15	94	3	3	4	3	4	17	85	90
123		38	4	4	4	3	15	94	4	4	4	4	3	19	95	4	4	4	4	16	100	3	3	4	3	4	17	85	93
124		39	3	3	3	3	12	75	4	3	3	3	3	16	80	3	4	4	4	15	94	3	4	4	3	4	18	90	85
125		40	3	3	4	4	14	88	3	4	4	4	4	19	95	4	4	3	4	15	94	4	3	3	4	3	17	85	90
126		41	4	4	3	3	14	88	3	3	4	4	4	18	90	3	3	3	3	12	75	4	4	3	4	4	19	95	87
127		42	3	4	3	4	14	88	4	3	4	4	3	18	90	4	4	4	3	15	94	4	3	4	4	4	19	95	92
128		43	3	4	3	3	13	81	3	4	4	4	4	19	95	4	4	4	4	16	100	3	3	3	4	4	17	85	90
129		44	4	3	3	4	14	88	3	3	3	3	3	15	75	4	3	3	4	14	88	4	4	3	3	4	18	90	85
130		45	3	3	4	3	13	81	3	3	3	3	4	16	80	3	4	4	4	15	94	3	4	3	4	3	17	85	85
131		46	4	3	4	4	15	94	4	3	3	3	4	17	85	4	3	4	4	15	94	4	4	3	3	4	18	90	91
132		47	3	3	3	3	12	75	3	4	3	3	3	16	80	4	4	4	3	15	94	4	3	4	4	3	18	90	85
133		48	3	3	4	4	14	88	4	4	3	3	4	18	90	3	3	4	3	13	81	4	4	4	4	3	19	95	88
134		49	3	4	4	4	15	94	4	4	4	4	4	20	100	4	4	4	4	16	100	3	3	4	4	4	18	90	96
135		50	3	3	3	4	13	81	4	3	3	4	3	17	85	3	3	3	3	12	75	4	3	4	3	4	18	90	83
136		51	4	4	3	4	15	94	4	4	4	4	3	19	95	3	3	3	3	12	75	3	3	3	4	3	16	80	86
137		52	3	3	3	4	13	81	3	4	3	4	4	18	90	3	3	4	3	13	81	4	4	4	3	4	19	95	87
138		53	4	3	3	3	13	81	3	3	3	4	4	17	85	4	4	4	3	15	94	4	4	4	3	3	18	90	88
139		54	4	3	3	4	14	88	3	4	4	4	3	18	90	4	4	3	3	14	88	3	3	4	3	3	16	80	86
140		55	4	4	3	3	14	88	3	3	3	4	4	17	85	3	4	3	3	13	81	3	4	4	4	4	19	95	87
141		56	4	4	4	4	16	100	3	4	3	3	4	17	85	3	3	3	4	13	81	3	4	4	3	3	17	85	88
142		57	4	3	3	4	14	88	4	4	3	4	3	18	90	3	3	4	4	14	88	3	4	4	4	3	18	90	89
143		58	3	4	4	3	14	88	4	4	4	4	4	20	100	4	3	3	4	14	88	4	3	4	4	4	19	95	93
144		59	4	4	4	4	16	100	3	3	3	3	3	15	75	3	3	3	4	13	81	4	4	4	3	4	19	95	88
145		60	4	3	3	3	13	81	3	4	4	3	4	18	90	4	4	4	4	16	100	4	3	3	3	3	16	80	88
146		61	3	3	4	3	13	81	4	3	4	4	3	18	90	4	3	3	4	14	88	4	3	3	4	3	17	85	86
147		62	3	4	4	4	15	94	3	4	4	3	4	18	90	4	3	3	4	14	88	4	3	3	4	4	18	90	90
148		63	3	4	4	4	15	94	3	3	4	4	4	18	90	3	3	3	3	12	75	3	3	4	3	4	17	85	86
149		64	4	4	3	3	14	88	3	3	4	3	4	17	85	3	3	3	4	13	81	3	3	4	4	4	18	90	86
150		65	4	4	3	4	15	94	3	4	4	3	3	17	85	3	3	3	4	13	81	3	3	4	4	4	18	90	88
151		66	4	3	4	3	14	88	3	3	3	3	3	15	75	4	4	3	4	15	94	3	4	3	3	4	17	85	85
152		67	3	4	4	4	15	94	4	3	4	3	3	17	85	4	3	4	3	14	88	4	3	4	3	4	18	90	89
153		68	3	4	3	3	13	81	3	3	3	3	3	15	75	4	3	3	4	14	88	4	4	3	3	3	17	85	82
154		69	3	3	4	3	13	81	4	4	4	4	4	20	100	4	3	3	4	14	88	3	4	3	4	3	17	85	88

Anexo 8: Aspectos administrativos

Recursos y presupuesto

Recursos humanos:

Para la presente investigación se usaron los siguientes recursos expuestos en la tabla 21.

Tabla 21

Materiales de recursos humanos

Cantidad	Perfiles de recurso	Costo por Horas Extras	Cantidad de horas	Costo De horas	Total
1	Jefe de proyectos TI	-	5 meses	s/ 3500	s/17 500
1	Asistente TI	s/ 13	70	s/ 910	s/ 910
5	Jefes de área	s/ 35	36	s/ 1260	s/ 6300
71	Profesionales - Consultores	s/ 16	2	s/ 32	s/ 2272

Fuente: Elaboración propia

Equipos y bienes duraderos:

Para la presente investigación se usaron los siguientes equipos basados en Hardware

Tabla 22

Costo en equipos de hardware

Cantidad	Equipo	Característica	Total
1	Laptop Dell	Procesador: Intel Core i7 10ma Gen Memoria RAM: 12 GB Disco solido: 480 GG	s/ 3200

Fuente: Elaboración propia

Para la presente investigación se usaron los siguientes bienes basados en Softwares

Tabla 23

Costo en bienes de software

Software	Característica	Total
Offices 365	Word y Excel	s/ 110
Project Managert	Gestor de proyectos	s/ 330
Foxit Reader	Visor PDF	s/ 0

Fuente: Elaboración propia

Asesorías especializadas y servicios:

Se contaron con las siguientes asesorías para el cumplimiento de algunas actividades de la etapa inicial del proyecto.

Tabla 24

Costos por actividades

Actividad	Descripción	Cantidad	Total
Auditor externo	Asesoramiento para revisión	1 persona	s/ 1200
Capacitación	Seguridad de la información	6 personas	s/ 580

Fuente: Elaboración propia

Gastos operativos:

Se consideran gastos recurrentes o que incluyeron para la parte operativa del proyecto.

Tabla 25

Costos indirectos

Detalle	Costos Unitarios	Cantidad	Total
Luz	s/ 380	5 meses	s/ 1900
Internet	s/ 250	5 meses	s/ 1250
Hojas	s/ 18	2 paquetes	s/ 36
Tintas de impresora	s/ 50	4	s/ 200

Fuente: Elaboración propia

Financiamiento

Para cumplir el objetivo de la implementación de la ISO 27001 y todas las medidas de seguridad de la información en la consultora, la gerencia general ha decidido ser la responsable de la inversión correspondiente, asimismo se ha consolidado la información de diferentes aseguradoras para el cumplimiento de lo requerido:

Seguro contra desastres naturales y no naturales:

Se propone la protección de las oficinas ante terremotos, inundaciones, incendios, vandalismo y cortocircuito. Por tal, bajo la cotización de la empresa aseguradora PACIFICO, se determinó el siguiente costo.

Tabla 26

Costos de seguro contra desastres naturales y no naturales

Descripción	**Costos Unitarios**
Seguro para REMYPE	s/ 200

Fuente: Seguro PACIFICO

Póliza de equipos:

Ante daños físicos o perdidas, se validó la cotización de un seguro de todo riesgo de equipos electrónicos con la aseguradora MAPFRE:

Tabla 27

Costos de póliza de equipos

Descripción	**Costos Unitarios**
Seguro de riesgos para equipos electrónicos	s/ 250

Fuente: Seguro MAPFRE

Soporte técnico para el mantenimiento correctivo y preventivo:

Se está programando una inversión para los mantenimientos, diagnósticos y reparaciones que requieran los equipos tecnológicos de la empresa.

Tabla 28

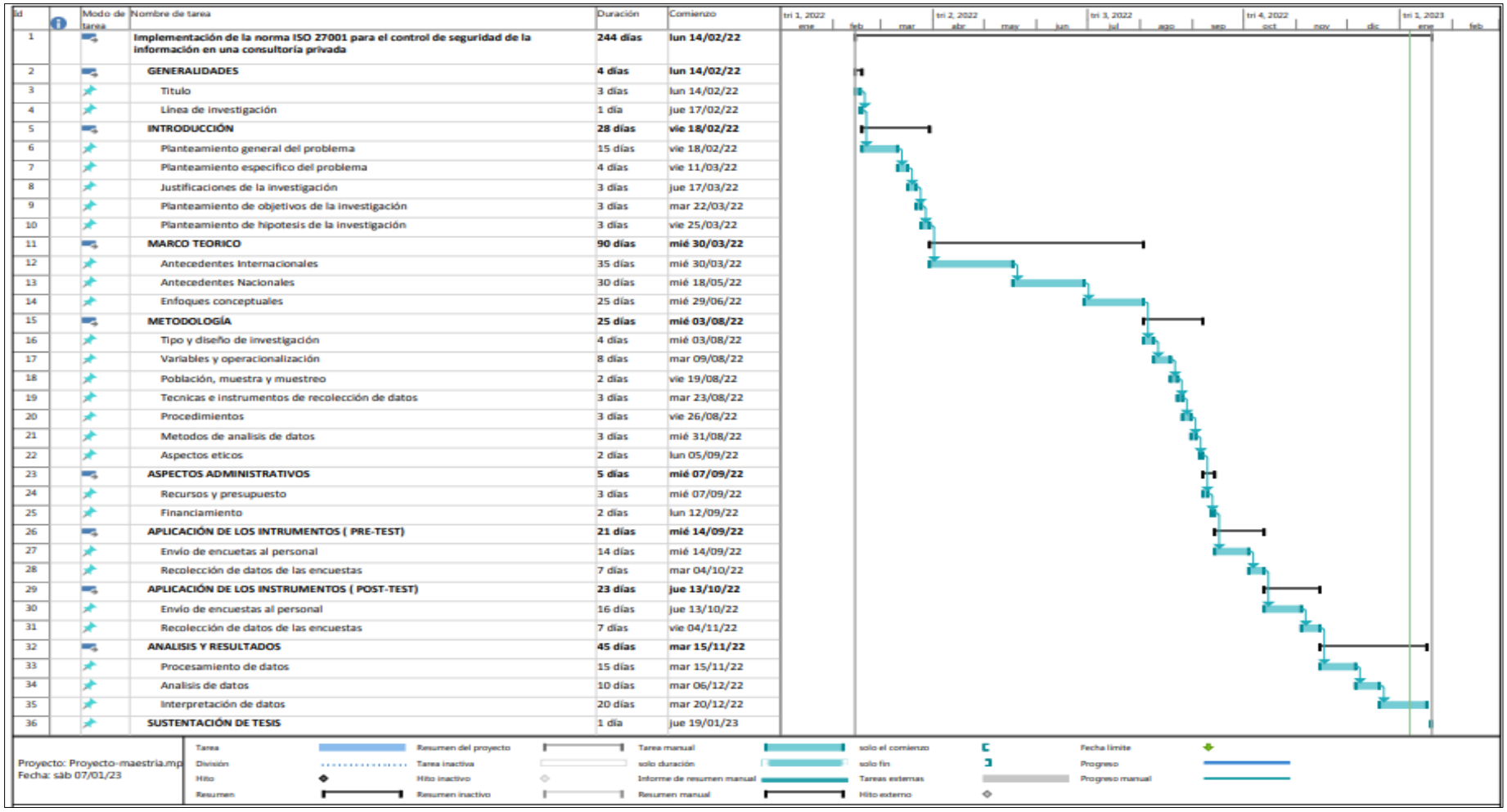
Costos de soportes técnicos

Descripción	**Costos Unitarios**
Mantenimiento bimestral de los equipos	s/ 370
Reparación trimestral de los equipos	s/ 345

Fuente: Seguro MAPFRE

Figura 7

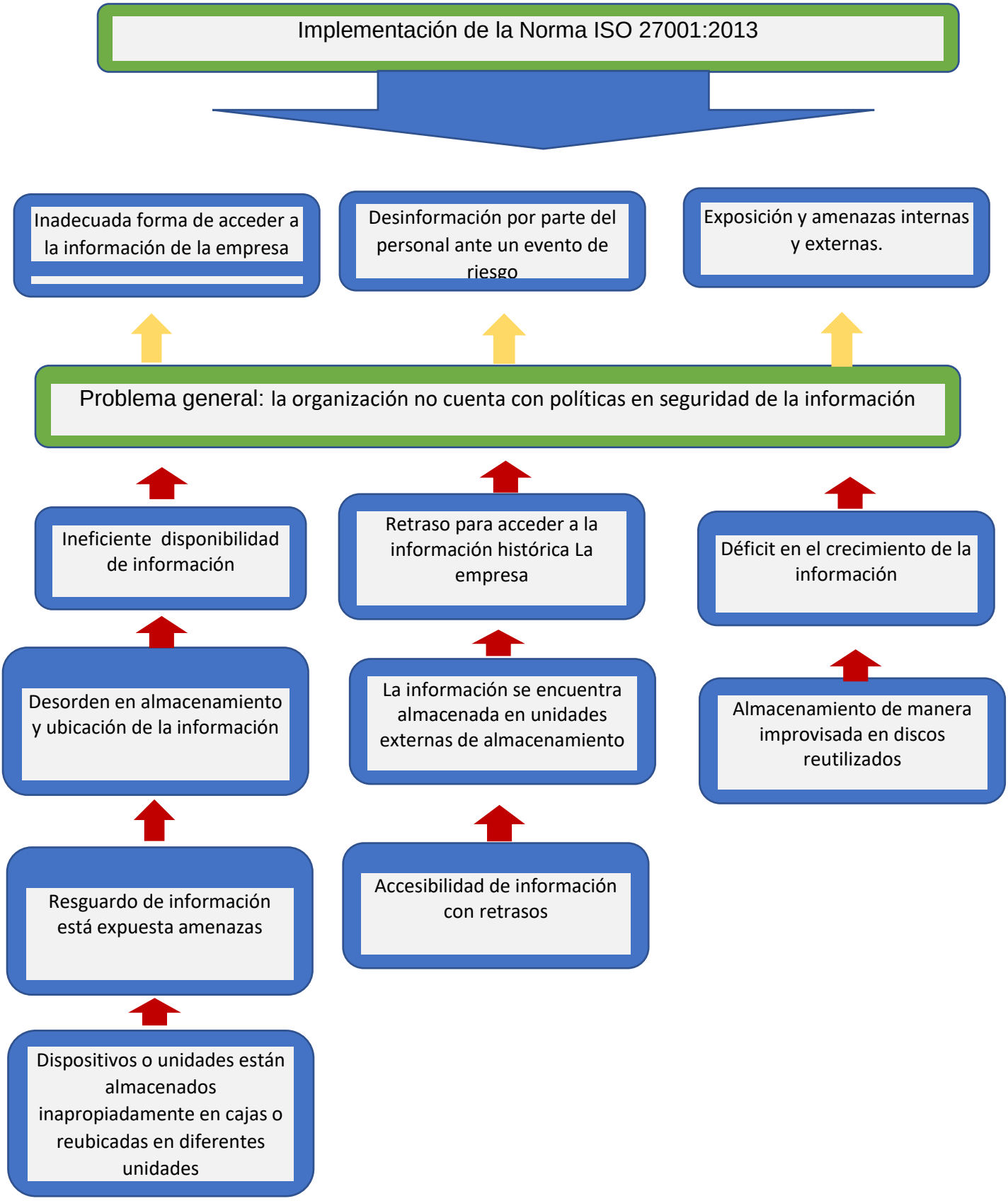
Cronograma de ejecución



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo
1		**Implementación de la norma ISO 27001 para el control de seguridad de la información en una consultoría privada**	**244 días**	**lun 14/02/22**
2		**GENERALIDADES**	**4 días**	**lun 14/02/22**
3		Titulo	3 días	lun 14/02/22
4		Línea de investigación	1 día	jue 17/02/22
5		**INTRODUCCIÓN**	**28 días**	**vie 18/02/22**
6		Planteamiento general del problema	15 días	vie 18/02/22
7		Planteamiento especifico del problema	4 días	vie 11/03/22
8		Justificaciones de la investigación	3 días	jue 17/03/22
9		Planteamiento de objetivos de la investigación	3 días	mar 22/03/22
10		Planteamiento de hipotesis de la investigación	3 días	vie 25/03/22
11		**MARCO TEORICO**	**90 días**	**mié 30/03/22**
12		Antecedentes Internacionales	35 días	mié 30/03/22
13		Antecedentes Nacionales	30 días	mié 18/05/22
14		Enfoques conceptuales	25 días	mié 29/06/22
15		**METODOLOGÍA**	**25 días**	**mié 03/08/22**
16		Tipo y diseño de investigación	4 días	mié 03/08/22
17		Variables y operacionalización	8 días	mar 09/08/22
18		Población, muestra y muestreo	2 días	vie 19/08/22
19		Tecnicas e instrumentos de recolección de datos	3 días	mar 23/08/22
20		Procedimientos	3 días	vie 26/08/22
21		Metodos de analisis de datos	3 días	mié 31/08/22
22		Aspectos eticos	2 días	lun 05/09/22
23		**ASPECTOS ADMINISTRATIVOS**	**5 días**	**mié 07/09/22**
24		Recursos y presupuesto	3 días	mié 07/09/22
25		Financiamiento	2 días	lun 12/09/22
26		**APLICACIÓN DE LOS INTRUMENTOS (PRE-TEST)**	**21 días**	**mié 14/09/22**
27		Envío de encuetas al personal	14 días	mié 14/09/22
28		Recolección de datos de las encuestas	7 días	mar 04/10/22
29		**APLICACIÓN DE LOS INSTRUMENTOS (POST-TEST)**	**23 días**	**jue 13/10/22**
30		Envío de encuestas al personal	16 días	jue 13/10/22
31		Recolección de datos de las encuestas	7 días	vie 04/11/22
32		**ANALISIS Y RESULTADOS**	**45 días**	**mar 15/11/22**
33		Procesamiento de datos	15 días	mar 15/11/22
34		Analisis de datos	10 días	mar 06/12/22
35		Interpretación de datos	20 días	mar 20/12/22
36		**SUSTENTACIÓN DE TESIS**	1 día	jue 19/01/23

Fuente: Elaboración Propia

Anexo 9: Árbol de problemas



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: "Norma ISO 27001 para el Control de la Seguridad de Información en una Consultoría Privada, Lima 2023", cuyo autor es ALEMAN BALLADARES FERNANDO YASMANI, constato que la investigación tiene un índice de similitud de 20.00%, 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, 06 de Enero del 2023

Apellidos y Nombres del Asesor:	**Firma**
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID:** 0000-0001-5207-9353	Firmado electrónicamente por: MACUNABE el 06-01-2023 14:58:58

Código documento Trilce: TRI - 0511347

INVESTIGA UCV