



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS.

Método de seguridad de la información basada en la ISO 27001 para
el seguimiento y control de vulnerabilidades en Pymes
TESIS PARA OBTENER EL TÍTULO PROFESIONAL
DE:
Ingeniero de Sistemas

AUTORES:

Huaman Espinoza Frederick Lui (orcid.org/ 0000-0002-2240-7384)

Ipanama Mendoza Ryder (orcid.org/ 0000-0002-7921-6220)

ASESOR:

Ing. Mg. Saboya Ríos, Nemías (orcid.org 0000-0002-7166-2197)

LÍNEA DE INVESTIGACIÓN:

AUDITORÍA DE SISTEMAS Y SISTEMAS DE INFORMACIÓN

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2022

Dedicatoria

Dedicamos con todo el amor y cariño nuestros hijos por estar a nuestro lado en este momento importante de nuestras vidas, quien es la motivación e inspiración para ser mejor persona y profesional.

A nuestros amigos y compañeros de estudio y trabajo que compartieron sus ideas y conocimientos sin esperar algo a cambio.

A mi papá que me protege, a mi mamá y familiares que complementan mi felicidad y que los quiero mucho.

Ryder Ipanama Mendoza

A mi amada madre por estar siempre conmigo, con su cariño y apoyo incondicional, a mis familiares que con su compañía complementan mi felicidad y que los quiero mucho.

Frederick Lui Huaman Espinoza

Agradecimiento

Agradecemos a nuestros formadores, personas de gran sabiduría quienes se han esforzado por ayudarnos a llegar al punto en el que nos encontramos.

Sencillo no ha sido el proceso, pero gracias a las ganas de transmitimos sus conocimientos y dedicación que los ha regido, hemos logrado importantes objetivos como culminar el desarrollo de nuestra tesis con éxito y obtener una afable titulación profesional.

Índice de contenidos

Dedicatoria.....	ii
Agradecimiento	iii
Índice de contenidos	iv
Índice de tablas	v
Índice de figuras	vi
Resumen.....	vii
Abstract.....	viii
I. INTRODUCCIÓN.....	1
II. MARCO TEÓRICO	4
III. METODOLOGÍA	10
3.1 Tipo y diseño de investigación	10
3.2 Variables y operacionalización	11
3.3 Población, muestra y muestreo.....	15
3.4 Técnicas e instrumentos de recolección de datos:.....	16
3.5 Procedimientos	18
3.6 Método de análisis de datos.....	21
3.7 Aspectos éticos	22
IV. RESULTADOS	23
V. DISCUSIÓN.....	41
VI. CONCLUSIONES	44
VII. RECOMENDACIONES.....	45
REFERENCIAS.....	46
ANEXOS.....	46

Índice de tablas

Tabla 1.	<i>Resumen de población</i>	16
Tabla 2.	<i>Análisis descriptivo de Valor de Tasación de activos de información</i> 23	
Tabla 3.	<i>Análisis descriptivo de Porcentaje de cumplimiento de controles de la norma</i>	24
Tabla 4.	<i>Análisis descriptivo de Porcentaje de incidentes en registro de comunicación de acceso remoto.</i>	26
Tabla 5.	<i>Porcentaje de registro de usuarios no autorizados</i>	27
Tabla 6.	Pruebas de normalidad.....	29
Tabla 7.	Prueba de rangos comparativos de wilcoxon para Valor de tasación de activos de información.....	31
Tabla 8.	Prueba estadística de Wilcoxon, Valor de tasación de activos.	31
Tabla 9.	Rangos comparativos de la prueba de wilcoxon para porcentaje de cumplimiento para controles de la norma.....	33
Tabla 10.	Estadísticos de prueba de Wilcoxon de porcentaje de cumplimiento de controles de la norma.....	34
Tabla 11.	Rangos comparativos de la prueba de wilcoxon porcentaje de incidentes en registro de comunicación de acceso remoto	36
Tabla 12.	Estadísticos de prueba de Wilcoxon de velocidad de descarga	36
Tabla 13.	Rangos comparativos de la prueba de wilcoxon porcentaje de registro de usuarios no autorizados	38
Tabla 14.	Resultados con la prueba de Wilcoxon para el porcentaje de usuarios no autorizados.....	39

Índice de figuras

Figura 1.	Fases de evaluación de riesgo norma ISO 27001.....	7
Figura 2.	Representación Visual de PDCA.....	8
Figura 3.	<i>Gráfico de líneas de indicador 1</i>	24
Figura 4.	<i>Gráfico de líneas de indicador 2</i>	25
Figura 5.	<i>Gráfico de líneas de indicador 3</i>	26
Figura 6.	<i>Gráfico de líneas de indicador 4</i>	28
Figura 7.	<i>Campana de gauss</i>	32
Figura 8.	<i>Campana de gauss</i>	34
Figura 9.	<i>Campana de gauss</i>	37
Figura 10.	<i>Campana de gauss</i>	39

Resumen

El objetivo de esta investigación fue el de conseguir la eficacia en la SGI cuando se implementa la metodología basada en la ISO 27001 ,para realizar el seguimiento y el control de las vulnerabilidades en las pymes. Se empleó como metodología el ciclo PDCA puesto a que nos permite realizar las etapas para el desarrollo del método. De igual forma se consideraron cuatro indicadores para su medición, Valor de tasación activos de información valorados, Porcentaje de estado de cumplimiento de los controles de la norma, Porcentaje de incidencia en el registro de comunicación de acceso remoto, Porcentaje de registro de usuarios no autorizados. El resultado de cada indicador fue evaluado en dos momentos, el primero fue realizando un diagnóstico inicial de los activos y el segundo después de 15 días obteniendo resultados favorablemente a todos los indicadores mencionados, resaltando que para el seguimiento y control de vulnerabilidad con un valor de 71.46% indicando que hay una mejora y con el registro de usuarios no autorizados con un 95% de confianza. Se concluye que a nivel general se comprobó la eficacia del método de SGI basado en la ISO 27001.

Palabras clave: Modelo de Gestión de riesgos; SGI; ISO 27001

Abstract

The objective of this research was to achieve effectiveness in information security when implementing the methodology based on ISO 27001 to monitor and control vulnerabilities in SMEs. The PDCA cycle was used as a methodology since it allows us to perform the stages for the development of the method. Similarly, four indicators were considered for measurement: appraisal value of valued information assets, percentage of compliance status of the standard controls, percentage of incidence in the remote access communication record, and percentage of unauthorized user record. The result of each indicator was evaluated in two moments, the first was performing an initial diagnosis of the assets and the second after 15 days obtaining favorably to all indicators, highlighting that for the monitoring and control of vulnerability with a value of 71.46% indicating that there is an improvement and with the registration of unauthorized users with 95% confidence. It is concluded that at a general level the effectiveness of the information security method based on ISO 27001 was proven.

Keywords: Risk Management Model; Information Security; ISO 27001

I. INTRODUCCIÓN

Durante estos últimos años a nivel mundial se han venido dando sucesos que pusieron en riesgo los activos de información, estos afectaron a las empresas tanto del privado como del sector público siendo este último de mayor vulnerabilidad en sus tres (03) ámbitos: la confidencialidad, la integridad y la disponibilidad, estos son muy importantes para mantener la ventaja en competitividad, los beneficios económicos y el respeto de las normas y las leyes.

(Laudon y Laudon, 2017), La SGI juega un papel muy importante en las empresas teniendo como característica principal la conservación de los datos mediante la disponibilidad, confidencialidad e integridad de los recursos tecnológicos ya que están sujetos a los riesgos de vulnerabilidad de ataques que puede producir pérdidas en su capacidad de operación de las empresas, para conseguir el propósito en la seguridad informática se debería de encargar en la de regular y establecer los lineamientos a seguir para la protección de los activos, dicho de otro modo, se va a encargar de la parte operativa y de su estructura metodológica.

(Figueroa-Suárez et al., 2017), Es por ello que las empresas y las microempresas no son sensatos de los peligros a los que están expuestos con su información, donde muchas empresas se rehúsan a realizar una implementación de una metodología de seguridad; las empresas prestan atención después de haberse producido alguna eventualidad y/o al instante de ser requerido por alguna entidad de supervisión; esto es debido a que no cuentan con las personas con conocimientos o los especialistas para realizar las gestiones para proteger sus datos de información, debido a como se viene mencionando por el crecimiento de las Tecnologías en la globalización, surgiendo nuevas amenazas y formas de cometer delitos cibernéticos.

(Baca, 2016) Los SGSI forman parte de los activos de una empresa y deben identificarse para analizar los riesgos a la que están expuestos y poder gestionar los procesos aplicando los debidos controles de la norma ISO 27001.

(Ministerio Producción, 2020), En el Perú Más de 1,7 millones de Pymes están oficialmente activas en el mercado, este segmento de actividad representa el 99,5% del total de empresas formales de la economía peruana, el 95,2% son pequeñas empresas, el 4,1% pequeñas y el 0,2% medianas. De los cuales el 85,2% no cuenta con un método de SGI 14.8% viene implementando a una seguridad de sus activos. Estos porcentajes se dan al no establecer y adoptar un control de medidas basados en un método de seguridad.

Entonces lo que se aplicó en este proyecto, es proponer el diseño del método de seguridad de información siguiendo el estándar basado en la ISO 27001 mediante el ciclo PDCA.

Por lo expuesto en la presente problemática en esta investigación, se planteó la siguiente pregunta

PG: ¿En qué medida el método de SGI basado en el ISO 27001 es eficaz en el seguimiento y control de vulnerabilidades en Pymes?

PE1: ¿En qué medida el método de SGI basado en la ISO 27001 es eficaz en el seguimiento de vulnerabilidad en pymes?

PE2: ¿En qué medida el método de SGI basado en la ISO 27001 es eficaz en el control de vulnerabilidad en pymes?

Justificación Metodológica. En la actual investigación se justifica, tal como indica, Pallas Mega (2009), que para asegurar la protección de las fuentes activas de información es muy importante en cualquier organización, y en este sentido se utiliza como modelo para establecer, implementar, monitorear y mejorar los sistemas ISO 27001, para toda la empresa basado en objetivos y condiciones de seguridad.

Justificación tecnológica: El método que se desarrolló basado en el ISO 27001 para el seguimiento y el control de vulnerabilidad en Pymes permitió mejorar la SI y la vulnerabilidad de datos, de forma que las empresas se vieron protegidas.

Justificación Práctica: El método SGI diseñado de acuerdo con la norma ISO 27001 permitió en modernizar la gestión de la información a través de la

interacción con los usuarios en los diferentes sectores de la empresa, potenciando la seguridad de la información procesados en las PYMES.

En la presente investigación tiene como objetivo establecer un método de trabajo para mejorar la gestión de procesos dentro de las empresas con el tratamiento de la información y la gestión de las tecnologías que utiliza la ISO 27001 para cumplir con los controles de SGI establecidos por la misma.

OG: Es determinar la eficacia del método de SGI basado en la ISO 27001 en el seguimiento y control de vulnerabilidad en pymes.

OE1: Es determinar la eficacia del método de SGI basado en la ISO 27001 para seguimiento de vulnerabilidades en pymes.

OE2: Es determinar la eficacia del método de SGI basado en la ISO 27001 para el control de vulnerabilidad en pymes.

Hipótesis general: El método de SGI basado en la ISO 27001 es eficaz en el seguimiento y control de vulnerabilidad en Pymes.

HE1: El método de SGI basado en la ISO 27001 es eficaz en el seguimiento de vulnerabilidades en Pymes.

HE2: El método de SGI basado en la ISO 27001 es eficaz en el control de vulnerabilidad en Pymes

II. MARCO TEÓRICO

Como apoyo de este estudio se recurrió a exploraciones antecesoras que se asemejan con el mismo objetivo de investigación, internacional como nacional, entre las que se encuentra.

Antecedentes Internacionales

(Tola y Lenin, 2015), en este estudio se aplicó la metodología del PDCA, MAGERIT y gestión del riesgo. Se concluyó estableciendo los objetivos y políticas del SGSI, que la empresa debe continuar la confidencialidad, disponibilidad e integridad de la información y para ello se requiere la participación de la alta gerencia siendo de vital importancia. Durante del ciclo en un SGSI, basado en la metodología de la ISO 27001, se encuentra la mejora continúa haciéndose indispensable que se cree procedimientos para la revisión del sistema y el monitoreo.

(Polanco, 2014). En esta investigación se identificó que el sistema contable de la empresa no cuenta con un manual de procedimiento. Por lo tanto, el objetivo del departamento de contabilidad era diseñar un manual que contribuya al mejoramiento de esta. Donde concluyeron y se establecieron indicadores de gestión para manejar el éxito de la organización en la caracterización de procesos como es la efectividad.

(Sánchez, 2013), en esta tesis, se planteó el objetivo en el desarrollo de un método en donde cubra las principales políticas de SGI, según la norma ISO 27001 y es un plan de acción para mejorar la SGI en una pequeña o mediana empresa de la ciudad de Quito, basado en la práctica de esta norma, para lograr la eficiencia, en las actividades de proteger y proteger información, especialmente contra un posible ataque.

(Sanchez y Calderon, 2012), en esta tesis, tuvo como finalidad esquematizar una guía una buena implementación y certificación en ISO 27001:2005, ya que los resultados de la investigación pueden indicar que existen amenazas y riesgos que podrían afectar las operaciones y el buen comportamiento del sistema informático

proponiendo procedimientos para el tratamiento aplicando los controles y políticas de la norma.

(Bermudes y Bailon, 2015). En este proyecto se tuvo como objetivo de mejorar los procesos y servicios dando como resultado que se mejoró los procesos y servicios, aumentando la competitividad de la empresa salvaguardando la integridad, disponibilidad y confidencialidad de los datos.

(Moyano y Suarez, 2017). En esta investigación se tuvo como resultado que la SGI se consigue ejecutando un grupo de controles, prácticas, procedimientos, políticas, funciones del sistema y estructuras organizativas. Se requiere controlar y ser implementados, establecidos, monitoreados para aseverar que se ejecutan los objetivos definidos de seguridad y de una empresa.

Antecedentes Nacionales.

(Quispe, 2020), En esta tesis se dio como resultado que se ha mejorado la eficiencia de los procesos actuales y reduciendo el riesgo mediante la implementación de la norma ISO 27001.

(Rodríguez, Cruzado y Mejía, 2020), En esta investigación se tuvo como objetivo de su investigación el dominio de la aplicación de la norma ISO 27001 en una empresa privada sobre la SGI realizaron el estudio de metodología cuantitativa teniendo como muestra 30 trabajadores en la cual se evidenció la influencia de la norma en las tres dimensiones de confidencialidad, integridad, disponibilidad.

(Alcantára Flores, 2015), en su tesis se tiene como resultado como logró la mejora de los procesos en el procedimiento de las anomalías de la SGI y el tratamiento de los riesgos disminuyendo el nivel de riesgo con respecto a los activos de la información.

(Quincho Ccesa, 2017), Diseño de SGSI bajo la NTP ISO 27001, teniendo como problemática de no conocer los alcances para implementar el diseño, como tratar

los peligros y la aplicación de las inspecciones, finalmente se concluye identificando los alcances para la aplicación del SGSI y los procesos a seguir para elaborar los controles.

(Niño, 2018), Modelo de un SGSI para fortalecer la disponibilidad, integridad y confidencialidad, el problema de la institución es que no contaba con un modelo de SGSI para la administrar el SGI, con este estudio se identificó los problemas, la cual permitió establecer un modelo de gestión para la administración del SGSI.

Como se evidencia, todos los proyectos presentados están dirigidos al método de la SGI en donde se basa en la importancia de la triada como es la disponibilidad, confidencialidad e integridad de la información, teniendo en cuenta el de contener el procedimiento del método para su tratamiento dentro de las empresas e instituciones. Esta triada básica en donde se consolida la estructura de la SGI se va a diferenciar según los ámbitos en que se realiza dicho método, es así que lo que es importante saber que la información incumpla.

(Alexander, 2015), un sistema de gestión de seguridad de información (SGSI) se puede puntualizar como una sucesión de procedimientos, métodos, recursos y responsabilidades que instaura la alta gerencia a fin de inspeccionar y administrar la confianza de los recursos de información y certificar que la efectividad de la institución predomina.

La norma (ISO 2700, 2015) es una progresión de patrones que ha sido elaborado por ISO (Organización Internacional de Estandarización) e IEC (Comisión Electrotécnica Internacional), quienes plantearon un marco de trabajo para el SGSI adaptable a distintas entidades, ya sea pública o privada, de macro o micro dimensión estructural.

Como describe (Andress, 2014), para preservar los sistemas de información de datos, las normas ISO 27000, ISO 27001 e ISO 27002 ofrecen fines de control, directrices, requerimientos y controles determinados, con los cuales la institución puede adquirir una apropiada seguridad de la información. Por lo tanto, que la ISO

27001 es aval para una institución considerando lo que estipula la norma, por lo que dicha infalibilidad se puede documentar como aplicada y gestionada conforme a una norma de organización internacional.

Para un SGSI según la ISO 27001, se debe de tener en cuenta el objetivo principal del sistema la evaluando el riesgo, permitiendo a la empresa tener como visión principal para explicar el radio de alcance de la norma, de este modo como las medidas y políticas a instaurar, incorporar la mejora continua del sistema de la metodología.



Figura 1. Fases de evaluación de riesgo norma ISO 27001.

Gestión de activos: La organización debe definir y aplicar un proceso para tratar los riesgos tal como son. En esta etapa, seleccionaremos las dimensiones de control adecuadas para cada riesgo, con el objetivo de:

Admitir el riesgo siempre explicable. Por ejemplo, el costo de colocar un generador puede ser excesivamente alto, por lo que la institución puede decidir por pagarlo.

Método PDCA.

(Meire, 2018), PDCA es una herramienta de calidad utilizada en el control de procesos con un enfoque en la resolución de problemas. La aplicación tiene cuatro fases:

P (Plan: Planificar): seleccionar un proceso, actividad o máquina a mejorar y desarrollar medidas claras y procesables, siempre con el objetivo de lograr los resultados deseados.

D (Do: Hacer): Ejecutar el plan preparado y monitorear su progreso.

C (Check: Check): Analizar los resultados obtenidos al implementar el plan y, si es necesario, reevaluar el plan.

A (Actuar): si tiene éxito, el nuevo proceso se documenta y se convierte a un nuevo estándar.

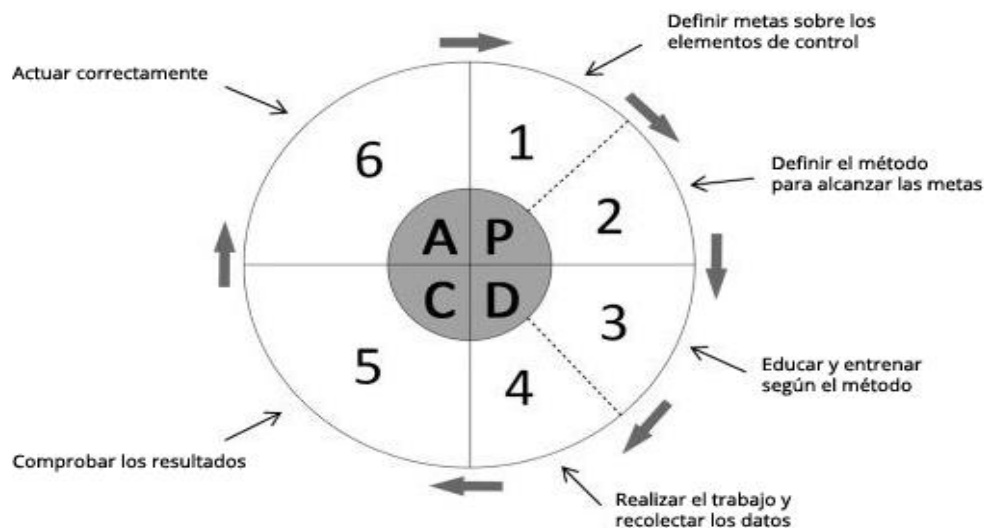


Figura 2. Representación Visual de PDCA.
Tomada de "Blog de Calidad", por Meire, 2018.

Identificación de activos: Se comprende por activo todo lo que tiene importancia para la entidad, esto incorporando los medios físicos (edificios o equipos), intelectuales o de información (Proyectos, aplicaciones, Ideas, etc.), reputación, marca, etc.

Identificar Riesgo: Reconocer para cada activo la posibilidad de que las vulnerabilidades o amenazas a ese activo puedan ocasionar daño parcial o total al activo, con respecto a su integridad, disponibilidad y la seguridad de esa propiedad.

Identificar los requisitos legales: Es todo reglamento que la entidad está reglamentado a cumplir con sus socios, clientes o proveedores.

Identificar las Vulnerabilidades: Son las fragilidades propias del activo que lo hacen dispuesto de sufrir irrupción o afección.

Identificar las Amenazas: Aquellos intrusos que puedan perpetuar y perjudicar el activo de la información, tales como incendios, desastres naturales o ataques de virus, espionaje etc.

Cálculo del riesgo: Esto se hace en base a la posibilidad de agudeza del riesgo y su impacto en la entidad ($\text{Riesgo} = \text{impacto} \times \text{probabilidad de amenaza}$). Con este proceso, identificamos la inseguridad que deben ser verificados de manera prioritaria.

Tratamiento de Riesgo: La entidad debe aclarar y acomodar un proceso para tratar los riesgos tal como son. En esta etapa, seleccionaremos las normas de control apropiado para cada riesgo, con el objetivo de: Responsabilización de inseguridad: siempre justificable. Por ejemplo, el costo de colocar un generador puede ser excesivamente alto, por lo que la institución puede decidir por pagarlo.

Controles y Secciones de la norma ISO 27001: La Norma ISO 27001 posee 114 controles la cuales están divididas en 14 secciones, para un adecuado uso del método en el seguimiento y control de vulnerabilidades en pymes se toma como base las siguientes secciones referidas a los controles.

III. METODOLOGÍA

Este capítulo describe el diseño y los métodos utilizados en la investigación. Se define la población analizada, se determina la muestra, se describe el proceso de construcción del instrumento utilizado para la medición del presente estudio, se analiza su confiabilidad y validez. Finalmente, se desarrollan las técnicas estadísticas usadas en el estudio de la dimensión explicativa.

3.1 Tipo y diseño de investigación

Tiendo como objetivo de esta investigación el de determinar la eficacia del método de SGI basado en la ISO 27001 en el seguimiento y control de vulnerabilidad en pymes, y tiene la intención el método de SGI basado en la ISO 27001 es eficaz en el seguimiento y control de vulnerabilidad en Pymes, y se tiene la intención de comprobar la hipótesis planteada en el capítulo anterior, para este efecto se ha diseñado una investigación de tipo cuantitativo, de corte longitudinal, descriptivo y aplicada.

(Hurtado y Toro, 2006), Es de tipo Cuantitativo dado a que se usaron técnicas estadísticas al realizar el cálculo de cada una de las variables, es de corte longitudinal dado a que se recopilan datos basados en los estudios a lo largo de un tiempo usando diferentes variables.

3.1.1 Tipo de Investigación

En esta investigación el tipo que se aplicó en esta aplicación es el **descriptivo y aplicada**, sabiendo que la finalidad es el de conocer la relación u obtener el nivel de asociación que existe entre las variables

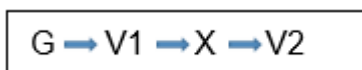
(Tamayo, 2012), nos menciona que la **investigación descriptiva**, se realiza una descripción, el análisis, la inspección y análisis de la información y el procesos o composición de los fenómenos; la consideración que se realiza sobre los resultados dominadores o sobre personas en individual o grupal, funciona en el presente; en este tipo de investigación se realiza sobre los contextos de hecho, caracterizándose principalmente por darnos una comentario correcto.

También (Tam Malaga, Vera y Oliveros, 2008), nos refiere que el propósito de la investigación es de tipo aplicada, lo cual es de instaurar nuevas tecnologías basándose en los conocimientos que se adquirieron, por lo consiguiente en este trabajo se consideró el tipo aplicada, dado a que se desea encontrar aplicar la norma ISO 27001 en la propuesta de un método de SGI basándose en los activos de información dentro de los procesos que se realizan en las instituciones.

3.1.2 Diseño de Investigación

Se usó un diseño no experimental debido a que solo describimos las características de cada una de las variables del estudio sin intervenir en el proceso del mismo.

(Hernández, 2014), nos menciona que este tipo de investigación no experimental se clasifica en transversales y longitudinales. Según lo descrito en esta investigación se estableció el diseño no experimental con corte longitudinal de tipo descriptivo simple.



G = Grupo

V1 = Grupo Pre-test

V2 = Grupo Post-test

X = Relación entre variables, coeficiente de correlación.

Variable 1: seguridad de información (V1)

Variable 2: Seguimiento y control de vulnerabilidades (V2)

3.2 Variables y operacionalización

3.2.1 Variable Independiente (V1): SGI

Tomando nuestra primera variable de SGI y nuestras dimensiones la cual lo definimos de la siguiente manera.

Definición Conceptual. (Godoy, 2014), hace mención que la SGI es el conjunto de medidas reactivas y preventivas que las empresas e instituciones deben aplicar: procedimientos, normas, políticas, planes de contingencia, evaluar el riesgo, y demás medidas con el propósito primordial de asegurar la integridad, disponibilidad y confidencialidad de la información de dicha entidad.

También (Godoy, 2014), menciona que la confidencialidad es la posesión que impide el desplazamiento de datos por usuarios o personas no autorizados, corroborando solo a aquellos usuarios que tengan el permiso para el acceso a la información; también (Sampieri 2014, pág 40), nos menciona que la confidencialidad, nos garantiza que únicamente deben acceder a la información, quienes estén acreditados. Al igual que (Burgos, Francisco y Escalona, 2017), en la página 237, reiteran que, para la confidencialidad, se debe de buscar notificar el ingreso no acreditado a los datos, ya sea en forma intencional o sin intenciones. Y la pérdida de esta seguridad puede ocurrir en distintas maneras, ejemplo con la revelación premeditada de divulgar la confidencialidad de la empresa u organización.

Definición Operacional El método de SGI basado en la ISO 27001, permitirá a las empresas medianas y pequeñas en adoptar e implementar las medidas preventivas sobre la SGI mediante los controles que establece la ISO 27001 y de esta forma mitigar los riesgos que se puedan originar.

Indicadores. Confidencialidad, integridad y disponibilidad.

3.2.2 Variable Dependiente (V2): Seguimiento y control de Vulnerabilidad.

En nuestra segunda variable Seguimiento y control de Vulnerabilidad, fundamentaremos sus respectivas dimensiones e indicadores la cual es de la siguiente manera:

Definición Conceptual: (Van de Velde, 2009) la sistematización, el registro y la observación de monitorear los resultados en los términos utilizados, metas que se indicaron y que se vinieron cumpliendo intermedicamente cumplidas, respecto a los tiempos y los presupuestos previstos con los métodos y maniobras que determinan de como se viene realizando el proyecto en su equipo y el amoldamiento que se debe de realizar.

De igual forma (Edwin Rolando, 2013) nos indica que al realizar un seguimiento nos conlleva una acción permanente en el tiempo del proceso de los proyectos, permitiendo una revisión pródigamente del trabajo en conjunto, tanto en la eficiencia de la aplicación de recursos humanos y materiales, como de su eficacia en la consumación de los objetivos propuestos. Es muy importante que el seguimiento realice como parte elemental con los responsables de la gestión, para que no sea solo una mera supervisión.

Definición Operacional: Para esta investigación procederemos a desarrollar con 2 Dimensiones, la de gestión de Activos y la de Seguridad de las comunicaciones, empleando dos indicadores en cada uno de las dimensiones ya mencionadas.

Dimensión 1: Gestión de activos, todo aquel que tenga un valor en la empresa que requiera una protección. Un activo de información es todo aquello que posee información, en estos contamos como los contratos, fichas, acuerdos, base de datos, ficheros, aplicaciones, software de información, equipos informáticos, entre otros.

Para ello se emplearon los siguientes indicadores para realizar la medición, en esta dimensión tenemos:

1. Valor de tasación de activos de información valorados.
2. Porcentaje de estado de cumplimiento de los controles de la norma.

En la 2 Dimensión respecto a la Seguridad de las comunicaciones, (García, 2020), COMSEC (del inglés Communications Security), Empresa de desarrollo de cifrado de las comunicaciones que se encomienda para la prevención de alguna institución no autorizada que interrumpe la comunicación pudiendo ingresar de forma descifrable los datos de información. En tanto esta instrucción incluye campos de investigación como la Criptología, la transmisión segura, la emisión segura, la seguridad de flujo del tráfico y la seguridad física de los equipos que ocupa de las comunicaciones.

Para ello se emplearon los siguientes indicadores para realizar la medición, en esta dimensión tenemos:

3. % de incidencias en registro de comunicación de acceso remoto.

$$\% \text{ de incidencias RCAR} = \text{NIR} / \text{TIR} \times 100$$

$$\% \text{ de incidencias IRCAR} = \frac{\text{NIR}}{\text{TIR}} \times 100$$

Donde:

%IRCAR = Porcentaje incidencias en registro de comunicación de acceso remoto

NIR = Número de incidencias resueltas.

TIR = Total de incidencias reportadas.

En la segunda variable que es el Control de Vulnerabilidad el procedimiento que permite identificar analizar y controlar las

vulnerabilidades sujetas al riesgo mediante una adecuada toma de decisiones en la empresa (Unir, 2022).

Dimensión: Control de acceso: Destinadas a controlar monitorizar los accesos, estableciendo controles de acuerdo a las políticas definidas de la organización, también limita los accesos a la información y a las instalaciones de procesamiento de la información.

4. % de Registro de usuarios no autorizados

Formula:

$$\% RUNA = CUNAV / TUNAR \times 100$$

$$\% RUNA = \frac{CUNAV}{TUNAR} \times 100$$

Donde:

%RUNA = Porcentaje de usuarios no autorizados.

CUNAV = Cantidad de usuarios no autorizados verificados.

TUNAR = Total de usuarios no autorizados registrados.

3.3 Población, muestra y muestreo

3.3.1 Población

El (INEI 2006, pag. 51), considera que “es un grupo de elementos o unidades con una característica definida, en tiempo y un lugar definido, donde los componentes pueden ser; granjas, personas, frutas, hogares, escuelas, hospitales, empresas, y cualquier otro”.

Asimismo, (Sampieri 2014, páp 174), nos menciona que la población “es el conglomerado de todos los elementos, personas o casos que coinciden con determinadas descripciones comunes”.

En la presente investigación, la población estuvo conformada por todos los activos de la información de la empresa en donde se viene realizando dicha investigación, según la clasificación que indica la ISO 27001.

3.3.2 Muestra

La muestra que se utilizó en la siguiente investigación son los activos y resultados obtenidos en los diferentes indicadores siendo como se consigna en la siguiente tabla.

Tabla 1. *Resumen de población*

Indicadores	Muestra	Periodo
Valor de tasación activos de información valorados.	12	3 días
Porcentaje de estado de cumplimiento de los controles de la norma	15	15 días
Porcentaje de incidencias en registro de comunicación de accesos remotos.	15	15 días
Porcentaje de registro de usuarios no autorizados.	15	15 días

Elaboración Propia

Muestreo

En esta investigación el muestreo no se ha realizado, debido a que cómo menciona (Carrasco, 2000), que cuando se considera el total de la población como se ha venido considerando en esta investigación respecto a los activos de información, tal como se muestran en la tabla 1.

3.4 Técnicas e instrumentos de recolección de datos:

(Angulo, 2011), nos dice que el procedimiento el método usado en esta investigación “es el proceso que el examinador va usar para distinguir un evento o suceso y lograr obtener indagación sobre este, de igual forma se respalda de las herramientas a fin de proteger los datos obtenidos obteniendo estos mediante una grabadora, una cámara fotográfica, una filmadora, un cuestionario, entre otros; estos elementos van a ser indispensables que nos acceden a los registros de lo observado durante esta investigación”

De igual forma el (INEI, 2006, pág 29), nos menciona que estas técnicas “es una forma de recoger información, que muy rutinariamente se realiza por medio de un cuestionario en donde este puede ser gestionado por el encuestado o por un encuestador”

Para esta investigación se usaron herramientas de recolección como son la Observación, el Análisis, el Síntesis, la lista de chequeo y la ficha de recolección de datos.

Observación: La observación es un procedimiento de información de la entidad en donde el investigador viene realizando la pesquisa, usando así los recursos del internet y el software de gestión.

Análisis: Para realizar el análisis de estado actual de los procedimientos de información, así como el soporte de los modelos de administración de sistemas informáticos y los activos que cuenta la empresa para implantar el método.

Síntesis: Las variables que se vinieron usando para este estudio que serán sintetizadas para plantear un método basado en la normativa internacional ISO 27001 y la norma técnica peruana NTP ISO/IEC 27001:2014.

Lista de Chequeo: Estas listas de constatación son instrumentos que nos permiten verificar, son usados mediante la observación de un grupo de ítems, la ejecución o la presentación de estos están basados en un determinado proceso u actividad. En la exploración se permitió decretar el número de controles que se van a usar para el cumplimiento con respecto a la ISO 27001.

Ficha de trabajo: Esta herramienta es uno de los métodos que nos ayuda a recolectar y almacenar la información de los activos. Cada una de estas fichas vana a tener una serie de datos de extensión variable pero todos sugerido a un mismo tema, lo cual se le confiere la unidad y el valor propio.

3.5 Procedimientos

Para empezar a realizar y en cumplimiento de la investigación que es aportar en un método de seguridad de información basándonos principalmente en la ISO 27001 para contribuir en el seguimiento y el control de las vulnerabilidades que pueden ocasionarse en una empresa pyme, debemos de conocer los siguiente:

La ISO 27001 cuenta con 10 clausulas principales que y 10 FASES que son:

a. Pilares

1. Alcance y Campo de Aplicación
2. Referencias Normativas ISO 27001
3. Términos y Definiciones
4. Contexto de la Organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora

b. Fases

Fase 1 auditoria inicial iso 27001 gap analysis

Fase 2 análisis del contexto de la organización y determinación del alcance

Fase 3 elaboración de la política. Objetivos del sgsi

Fase 4 planificación del sgsi

Fase 5 documentación del sgsi

Fase 6 implementando un sgsi

Fase 7 comunicación y sensibilización sgsi

Fase 8 auditoria interna según iso 27001

Fase 9 revisión por la dirección según iso 27001

Fase 10 el proceso de certificación iso 27001

De las cuales la familia ISO contribuye continuamente para el conocimiento general desde el alcance los campos de la aplicación, hasta los términos y definiciones de la ISO 27000.

1. El alcance y el campo de la aplicación: El alcance de este método es para las empresas PYMES de nuestra localidad que aún no cuentan con ningún aporte de resguardo o protección en sus activos como empresa.
2. Se tomaron como referencia las normas que cuenta la ISO 27001
3. Los términos y definiciones son para toda la familia 27000 las cuáles se usarán de acuerdo a la normativa.
4. En el contexto de esta organización podemos resumir que se debe de comprender a la empresa y las consultas que realiza la Gerencia. Entre ellos contamos al 4.1. Definir los requisitos de seguridad de la información, considerando los servicios críticos que pueden causar el impacto en la empresa como en sus clientes y todas las partes que son involucradas para el resultado de sus pérdidas y sus confidencialización e integridad. 4.2 comprensión de las necesidades y las expectativas de las partes interesadas. 4.3 Determinación del alcance del sistema de gestión de la seguridad de la información. Y el 4.4 Sistema de gestión de seguridad de la información.
5. El liderazgo se encontrará basada mediante el 5.1 que es el Liderazgo y el compromiso en los actores principales de la organización como son de la alta gerencia y responsables del método a desarrollar asegurando que se establecen. 5.2 La política de la seguridad de los datos y los objetivos que se plantaron en esta investigación de acuerdo al método que se viene implementando. 5.3 Mediante los Roles la responsabilidad y las autoridades de la empresa.
6. Respecto a la planificación que se aplico en esta empresa se iniciaron después la autorización recibida por la empresa en donde se desarrolló dicho método procediendo a evaluar los riesgos que es el núcleo de cualquier SGSI eficaz.6.1 Se cuenta con las acciones para tratar los riesgos y las oportunidades, mediante 6.1.1 asegurándose a que el método pueda conseguir los resultados esperados. 6.1.2 Valorando los riesgos mediante un establecimiento y manteniendo los criterios de los riesgos en la SGI. 6.1.3 Definiendo y aplicando el proceso de tratamiento de riesgos de la SGI, determinando todos los controles que sean necesarios para el método. 6.2

Cumpliendo los objetivos de la SGI siendo coherentes con la política siendo estos medibles, teniendo los en cuenta los requisitos de la SGI.

7. El Soporte es en donde se compone por diferentes compuestos o apartados en donde se encontraron 7.1. los Recursos de la organización debe determinar y proporcionar los recursos para el método propuesto. 7.2. Determinando la competencia necesaria realizando un trabajo que afecta el desempeño. 7.3 contribuyendo la eficacia del SGSI con los beneficios de una mejora. 7.4 Con una comunicación en donde la empresa determina las necesidades de una comunicación ya sea interna o externa. 7.5 Informando los documentos de 7.5.2 creación y actualización de los documentos para el soporte y revisión, para su aprobación con respecto a los activos. 7.5.3 teniendo el control de toda esta información estando disponible y adecuado al uso de la empresa. Teniendo los controles de cambios.
8. La empresa debe de planificar correctamente 8.1 manteniendo la información documentada para que el método pueda tener un mejor control de los procesos necesarios para el cumplimiento de los todos los requisitos del SGI mediante el 6.1 que menciona que la empresa debe de implementar planes para conseguir. 8.2 Valorando los riesgos que debe de tener en cuenta la empresa valorando los riesgos de la seguridad de la información. 8.3 Para luego Tratar los riesgos de la SGI mediante un plan que en el método compone.
9. EN este punto las empresas deben de realizar el seguimiento del método para una medición y análisis para luego su evaluación. 9.1 evaluando el desempeño de la información realizando una medición, incluyendo los procesos y los controles de la SGI. 9.2 Se debe de realizar una auditoria interna para la observación de conformidad de los requisitos de la entidad, para ello se debe de cumplir la planificación, estableciendo e implantando un programa de auditoria interna 9.3 La empresa revisa el estado de los activos y la vulnerabilidad mediante el cumplimiento externos e internas, teniendo una retroalimentación sobre el desempeño.
10. Una vez teniendo claro los puntos anteriores se puede obtener las No conformidades y las acciones correctivas, 10.1 implantando una acción para revisar las eficacias de las acciones correctivas y conservando la información

documentada como evidencia. 10.2 obteniendo constantemente la mejora continua.

Para ello para nuestras variables e indicadores se procedió a trabajar en cumplimiento de lo manifestando en cada uno de los clausulas la cual se usaron los instrumentos para la recolección de datos que se usaron mediante las guías de observación, de los indicadores 1 y 2, se procederá a identificar y valorar a los activos de información y clasificarlos a través de categorías. De igual manera, con el empleo de otras guías de observación de los indicadores 3 y 4, se determinará el nivel de amenaza, los tipos de vulnerabilidades y con ello se establecerá el impacto y el nivel de riesgo. También, mediante listas de control (Chequeo) del indicador 5 y 6, se determinará el número de controles aplicados según la normativa, las políticas implementadas y el estado de cumplimiento de los controles en el marco de la norma ISO 2700

De igual forma se procedió a usar las listas de control o de Chequeo nos ayudó a valorar los indicadores 5 y 6, determinado la cantidad de controles que se aplicaron según la manifestado en las cláusulas de la normativa y el procedimiento las normas del método y el estado de cumplimiento de los controles en el marco de la norma ISO 27001

Mediante las fichas de Trabajo se procedió a recolectar los datos para los indicadores 7 y 8 obteniendo los porcentajes de incidencias y el porcentaje de registros de usuarios no autorizados.

3.6 Método de análisis de datos

Para nuestra investigación se realizó el análisis estadístico descriptivo e inferencial. (Azucena, 2016), el objetivo de la estadística descriptiva es el de resumir la información en donde contiene los datos de una forma más sencilla y presentable, consiguiendo de esta manera los parámetros que diferencian las características de un conjunto de datos.

En esta investigación se procedió en analizar la mediana, media, la desviación estándar, valores mínimos y máximos de los indicadores. En los resultados se usó el grafico de líneas por cada uno de los indicadores que usamos cuantitativamente que fueron el valor de tasación de los activos de información valorados, el % de estado de cumplimiento de los controles de la norma, % de incidentes en registro de comunicación de acceso remoto. % de registro de usuarios no autorizados.

Se recolectaron toda la información mediante las herramientas de las técnicas e instrumentos, para luego mediante la estadística inferencial, obtener generalizaciones y realizar las predicciones mediante los datos obtenidos. (Flores y Flores, 2021), menciona que el test o prueba Shapiro-Wilk se emplea para contrastar una normalidad cuando el tamaño de muestra es menor a 50 observaciones, por lo tanto, las muestras obtenidas cumplen con lo mencionado en todos los indicadores. También se usó la estadística no paramétrica aplicando la prueba de tes de mann-whitney- test de wilcoxon, debido a que las variables no cumplen con la normalidad el ($\text{sig} < \alpha = 0.05$) siendo muestras independientes.

Para proceder en realizar el análisis de información de datos se requirió el uso de herramientas como programas o sistemas que son indispensables ser usados en las computadoras (Hernández, 2014), para nuestra investigación hemos usado el software SPSS en la versión 26 en donde nos aportó con el apoyo de los análisis.

3.7 Aspectos éticos

Este estudio se desarrolló con la seguridad de confidencialidad en la obtención de los datos en la empresa Telsercom SAC, sin la divulgación más solo usando los datos obtenidos para la presente investigación con fines académicos, además se validó la autenticidad y la veracidad de los datos que se recabaron. Esta investigación se desarrolló mediante la normativa y reglamentos de la Universidad Cesar Vallejo, usando los documentos que se nos proporcionaron dentro de su plataforma de biblioteca virtual, repositorios de otras universidades. Por último se validó la originalidad e integridad con el porcentaje mínimo de similitud obtenido del software Turnitin.

IV. RESULTADOS

4.1. Resultados Descriptivos: Gestión de Activos

4.1.1. Resultado del indicador 1:

Con este indicador valor de tasación de activos de información, Muestran los resultados descriptivos en la tabla 2, después de aplicar el método los resultados promedio muestran que 197.25% y 336.16%, respectivamente muestran un ligero aumento en comparación con antes. La variabilidad porcentual después de aplicar el método es baja en 59.43%, el mínimo y máximo de los valores para Pretest y Postest son 167% y 233%, el valor máximo para Pretest es 233%, y Postest fue 400%.

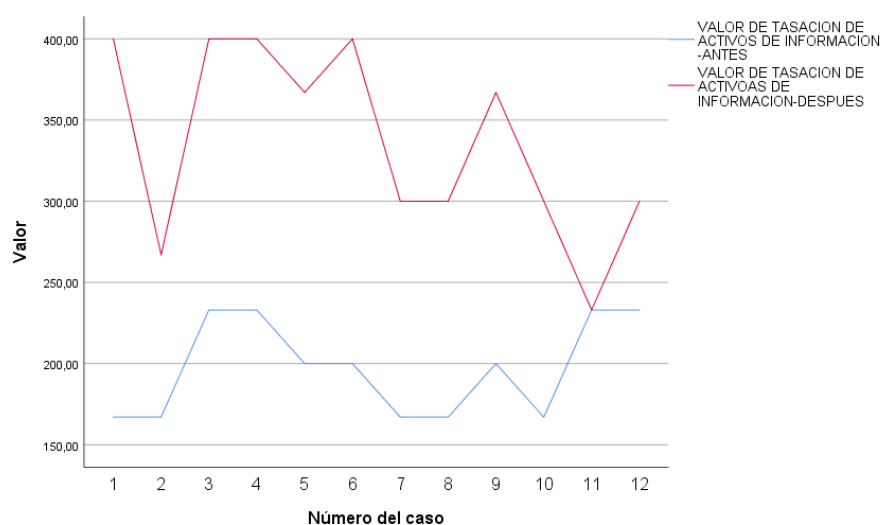
Tabla 2. *Análisis descriptivo de Valor de Tasación de activos de información*

ESTADÍSTICOS	ANTES	DESPUES
N	12	12
Media	197,2500	336,1667
Mediana	200,0000	333,5000
Moda	167,00	300,00 ^a
Desv. Desviación	29,71111	59,43650
Mínimo	167,00	233,00
Máximo	233,00	400,00

Elaboración Propia

Resultados de comparación del indicador valor de tasación de activos de información antes de implementar el método, muestra un valor de 197.25% y después de la implementación del método un valor de 336.16 indicando que hay una mejora significativa en dicho indicador.

Figura 3. Gráfico de líneas de indicador 1



Elaboración Propia

4.1.2. Resultados de indicador 2.

Con este indicador porcentaje de estado de cumplimiento de los controles de la norma, muestran los resultados descriptivos en la tabla 3, después de aplicar el método los resultados promedio muestran el antes y después 31.50 % y 88.07 % respectivamente muestra un leve aumento con respecto al antes. La variabilidad porcentual después de aplicar el método bajó 12.09%, y los valores mínimos del pre test y post test es 10% y 67%, el valor máximo de Postest fue 100% y Postest fue 67%

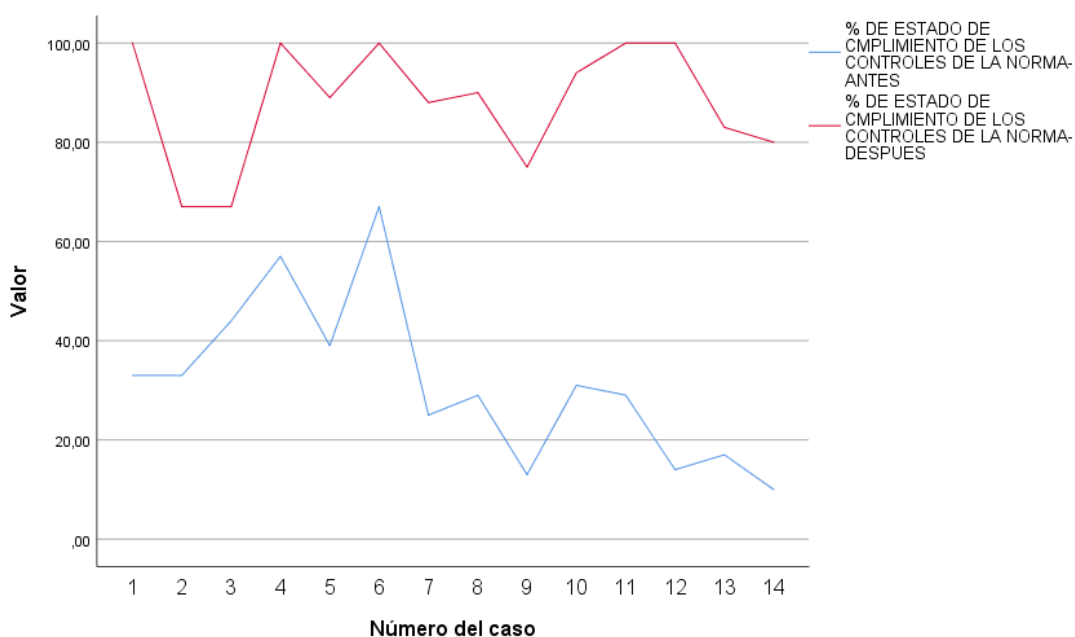
Tabla 3. Análisis descriptivo de Porcentaje de cumplimiento de controles de la norma

ESTADÍSTICOS	ANTES	DESPUES
N	14	14
Media	31,5000	88,0714
Mediana	30,0000	89,5000
Moda	29,00 ^a	100,00
Desv. Desviación	16,41646	12,09236
Mínimo	10,00	67,00
Máximo	67,00	100,00

Elaboración Propia

Al comparar los resultados del indicador porcentaje de estado de cumplimiento de los controles de la norma antes de implementar el método, muestra un valor de 31.50% y después de la implementación del método un valor de 88.07% indicando que hay una mejora significativa en dicho indicador.

Figura 4. Gráfico de líneas de indicador 2



Elaboración Propia

4.2. Resultados descriptivos de Seguridad de las Comunicaciones

4.2.1. Resultado de indicador 3.

Con respecto al indicador porcentaje de incidentes en registro de comunicación de acceso remoto, muestran los resultados descriptivos en la tabla 4. Después de aplicar el método los resultados promedio muestran 55.66% y 71.46% respectivamente, se denota en comparación con el antes un ligero aumento, la variabilidad porcentual después de la aplicación del método bajó en 8.11% y los valores mínimos y máximo del pre test y post test es 20% y 50% , el valor máximo del pre test fue de 75 % y el post test fue de 80%.

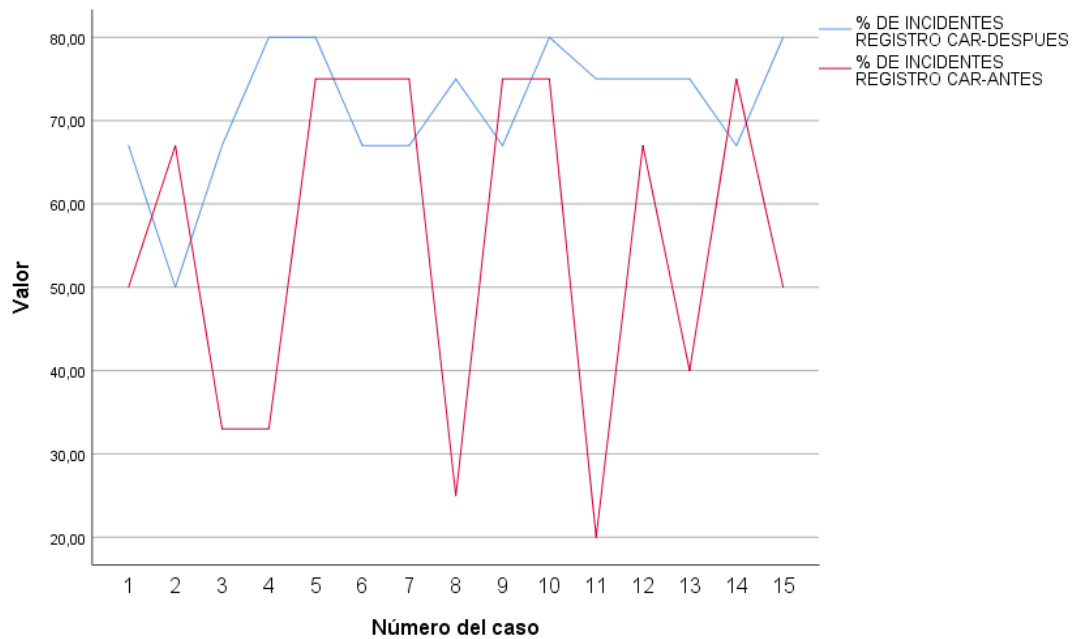
Tabla 4. Análisis descriptivo de Porcentaje de incidentes en registro de comunicación de acceso remoto.

ESTADISTICOS	ANTES	DESPUES
N	15	15
Media	55,6667	71,4667
Mediana	67,0000	75,0000
Moda	75,00	67,00
Desv. Desviación	20,78690	8,11407
Mínimo	20,00	50,00
Máximo	75,00	80,00

Elaboración Propia

La comparación de resultados del indicador porcentaje de incidencias en registro de comunicación de acceso remoto antes de implementar el método muestra un valor de 55.66% y después de la implementación del método un valor de 71.46 indicando que hay una mejora significativa en el indicador mencionado.

Figura 5. Gráfico de líneas de indicador 3



Elaboración Propia

4.3. Resultados descriptivos de Control de Acceso

4.3.1. Resultados de indicador 4.

Con este indicador porcentaje de registro de usuarios no autorizados, los resultados descriptivos que se visualiza en la Tabla 5, después de aplicar el método los resultados muestran 59,40% y 90,60%, respectivamente muestran un aumento leve en comparación con el antes. La variabilidad porcentual después de aplicar el método bajó 10,49 %, y los valores mínimo y máximo antes y después del ensayo son del 25 % y 67 %., el valor máximo del pre test fue de 83 % y el post test fue de 100 %.

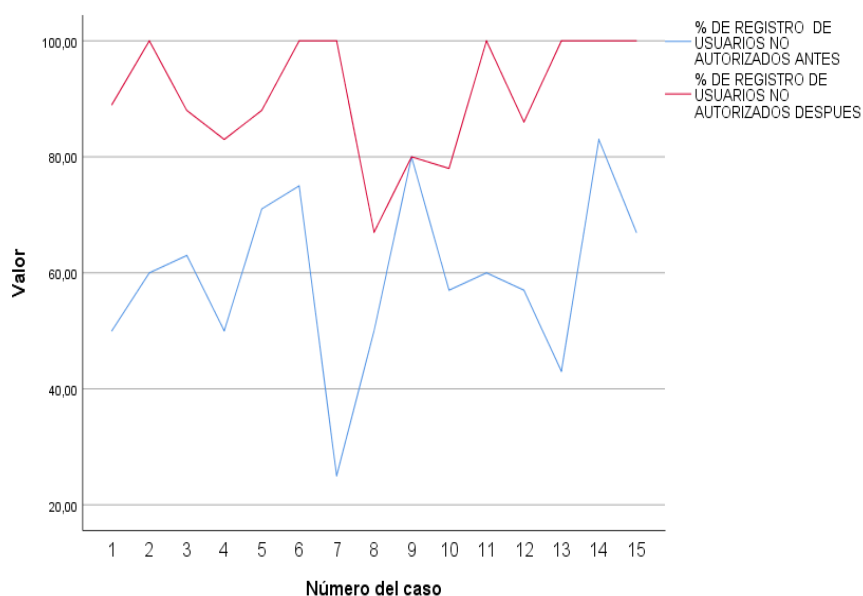
Tabla 5. *Porcentaje de registro de usuarios no autorizados*

ESTADISTICOS	ANTES	DESPUES
N	15	15
Media	59,4000	90,6000
Mediana	60,0000	89,0000
Moda	50,00	100,00
Desv. Desviación	15,02284	10,49354
Mínimo	25,00	67,00
Máximo	83,00	100,00

Elaboración Propia

La comparación de resultados del indicador porcentaje de registro de usuarios no autorizados antes de implementar el método muestra un valor de 59.40% y después de la implementación del método un valor de 90.60 indicando que hay una mejora significativa en el registro incidencias resueltas.

Figura 6. Gráfico de líneas de indicador 4



Elaboración Propia

4.3. Resultados del contraste de hipótesis de la investigación

4.3.1. Análisis de normalidad de los datos

Hipótesis de normalidad

H₀: Los datos analizados presentan una distribución normal

H_a: Los datos analizados no presentan una distribución normal

Análisis de normalidad Shapiro-Wilk

En esta investigación la prueba que se consideró fue Shapiro Wilk porque los casos de la muestra fueron menos de 30 casos para contraste normal. La Tabla 5 demuestra que el índice de valor de tasación de activos de la información, que el resultado de sig = 0.006, fue menor $\alpha = 0.05$, con este indicador se termina haciendo uso de estadísticas no paramétricas para el indicador. Para población de muestra relacionadas, Además, se reconoció. Esto requiere la aplicación de la prueba de Wilcoxon.

Para el indicador porcentaje de estado de cumplimiento de los controles de la norma donde la tabla 2 muestra el resultado del pre test del sig=0.346 y el resultado del post test del sig=0.038 lo cual nos dice que fue menor al $\alpha = 0.05$, lo que concluye el uso de estadísticas no paramétricas para este indicador y también permite que

el indicador se adapta a la población de muestras relacionadas, esto requiere la aplicación de la prueba de wilcoxon.

Para el indicador porcentaje de incidentes en registro de comunicación de acceso remoto el valor del Pretest del sig = 0.020 y el resultado del post test 0.04 es menor que el valor del $\alpha = 0.05$ lo que concluye el uso de la estadística no paramétrica, el indicador se adapta a la población de muestra relacionadas por la cual es necesario la aplicación de Wilcoxon.

Para el indicador porcentaje de registro de usuarios no autorizados el valor del Pretest del sig =0.794 y el resultado de Postest del sig=0.01 lo cual nos dice que fue menor que el $\alpha = 0.05$, lo que concluye el uso de la estadística no paramétrica, el indicador el indicador se adapta a la población de muestra relacionadas por la cual es necesario la aplicación de wilcoxon. Dichos indicadores serán comparados con una confianza del 95%.

Tabla 6. Pruebas de normalidad

Indicador	Pre-test			Pos-test		
	Shapiro-Wilk			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Valor de tasación de activos de información	0.781	12	0.006	0.864	12	0.055
Porcentaje de cumplimiento de los controles de la norma	0.934	14	0.346	0.867	14	0.038
Porcentaje de incidentes en registro de comunicación de acceso remoto.	0.831	15	0.020	0.824	15	0.041
Porcentaje de registro de usuarios no autorizados.	0.966	15	0.794	0.837	15	0.011

Elaboración Propia

CONTRASTE DE HIPÓTESIS:

4.4. Contraste de hipótesis de Gestión de Activos

4.4.1. Contraste de Indicador 1

Ho: $Me^1 = Me^2$: El método de SI no favorece en el valor de tasación de los activos de la información.

Ha: $Me^1 \neq Me^2$: El método de SGI favorece en el valor de tasación de activos de la información.

Nivel de confianza

Para el nivel de confianza que se viene considerando en este estudio fue de 0.95 con un nivel de significancia del $\alpha=0.05$

Regla de decisión

Rechazar la H_0 si $\text{sig} < \alpha$

Aceptar la H_0 si $\text{sig} > \alpha$

Estadística de prueba:

La prueba wilcoxon se consideró como estadística para el estudio para muestras relacionadas (autor), Ya que no cumplieron las variables analizadas con los supuestos de normalidad, la fórmula es la siguiente.

$$T = \text{Min}[T(+), T(-)]$$

Donde T se ajusta a una distribución NORMAL por lo que es necesario utilizar la siguiente formula:

$$Z = \frac{T - n(n + 1)/4}{\sqrt{n(n + 1)(2n + 1)/24}}$$

Resultados del estadístico de prueba utilizando SPSS 26.0

Al estudiar la variable valor de tasación en comparación con los resultados descriptivos en dos tiempos de la tabla 7 (Pre-test, Post-test), se demostró que el valor medio del intervalo negativo ($\bar{x}^- = 0.00$) fue menor que el valor positivo ($\bar{x}^+ = 6,00$). indicó que los resultados del Postest fueron superiores, indicando que el método ayudó al valor tasado de los activos de información, también como resultado de la suma de los rangos a favor del estudio.

Tabla 7. Prueba de rangos comparativos de wilcoxon para Valor de tasación de activos de información

Indicador		N	Rango promedio	Suma de rangos
VALOR DE TASACION DE ACTIVOS DE INFORMACION Pre - Post	Rangos negativos	0 ^a	0,00	0,00
	Rangos positivos	11 ^b	6,00	66,00
	Empates	1 ^c		
	Total	12		

Elaboración Propia

La tabla 8 los resultados de las comparaciones de la prueba de wilcoxon evidencian, donde el sig = 0.006 < α = 0.05, donde demuestra que los valores de tasación muestran diferencia favorable respecto al antes y después del estudio.

Tabla 8. Resultados con la prueba de Wilcoxon, Valor de tasación de activos.

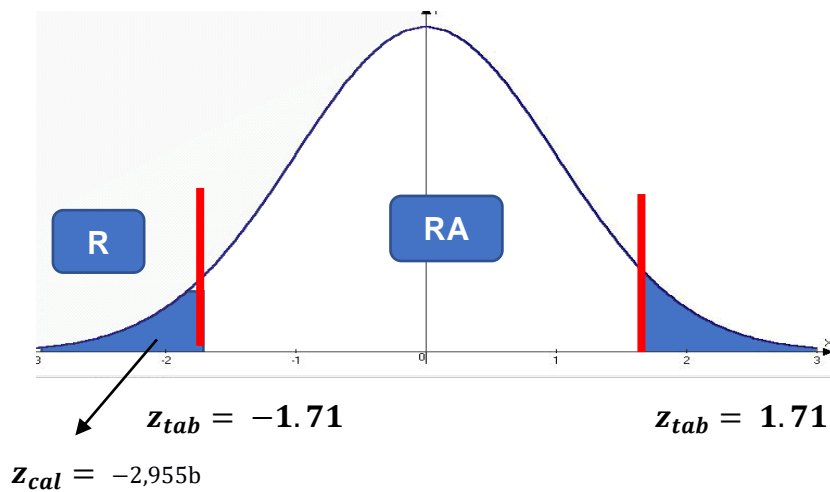
Prueba	PORCENTAJE
Z	-2,955 ^b
Sig. asintótica(bilateral)	0,003

Elaboración Propia

Distribución estadística de prueba:

Para probar la hipótesis, se determinó **una** prueba estándar aproximada distribuida en forma de Ztab ($1 - \alpha$, $n_1 + n_2 - 2$). Sustituyendo los valores, el resultado es z tab $1 - 0.05 = 0.95$. así mismo, el resultado de la decisión se comparó con el valor Zcal = 2.955b y se representa en la campana gauss que se muestra (ver figura 7).

Figura 7. Campana de gauss



Elaboración Propia

En la figura 7 nos evidencia el resultado de Z_{cal} ubicándose en la zona de rechazo, hecho que nos lleva a rechazar al H_0 a favor de la H_a , lo que lleva a la conclusión, mediante lo evidenciado en los resultados es favorable el método de seguridad que contribuyó el registro de usuarios no autorizados con un 95% de confianza

4.4.2. Contraste de hipótesis: Indicador 2

Formulación de hipótesis

H_0 : $Me^1 = Me^2$: El método de SGI no favorece en el porcentaje de cumplimiento de los controles de la norma.

H_a : $Me^1 \neq Me^2$: El método de SGI favorece en el porcentaje de cumplimiento de los controles de la norma.

Nivel de confianza

Para el nivel de confianza que se viene considerando en este estudio fue de 0.95 con un nivel de significancia del $\alpha=0.05$

Regla de decisión

Rechazar la H_0 si $sig < \alpha$

Aceptar la H_0 si $sig > \alpha$

Estadística de prueba:

La prueba wilcoxon se consideró como estadística para el estudio para muestras relacionadas (autor), Ya que no cumplieron las variables analizadas con los supuestos de normalidad, la fórmula es la siguiente.

$$T = \text{Min}[T(+), T(-)]$$

Donde T se ajusta a una distribución NORMAL por lo que es necesario utilizar la siguiente formula:

$$Z = \frac{T - n(n + 1)/4}{\sqrt{n(n + 1)(2n + 1)/24}}$$

Resultados del estadístico de prueba utilizando SPSS 26.0

El estudio de la variable porcentaje de cumplimiento de los controles de la norma, comparado con el resultado descriptivo tala 9 (Pre-test , Pos-test), el promedio del rango negativo demuestra ($\bar{x} = 0.00$) es menor al positivo ($\bar{x} = 6.00$). indica que el Postest de los resultados obtenidos fueron mayores, demostrando que el método ayudo el porcentaje de cumplimiento de la norma, también el resultado de la suma de rangos inclina a favor del estudio.

Tabla 9. Rangos comparativos de la prueba de wilcoxon para porcentaje de cumplimiento para controles de la norma.

Indicador		N	Rango promedio	Suma de rangos
PORCENTAJE DE CUMPLIMIENTO PARA CONTROLES DE LA NORMA Pre - Post	Rangos negativos	0 ^a	,00	,00
	Rangos positivos	14 ^b	7,50	105,00
	Empates	0 ^c		
	Total	14		

Elaboración Propia

La tabla 10 por otro lado muestra los resultados de las comparaciones de la prueba de wilcoxon, donde el sig = 0.346 < $\alpha = 0.05$, demostrando de esta manera

que el porcentaje de cumplimiento de los controles muestra diferencia favorable respecto al antes y el después del estudio.

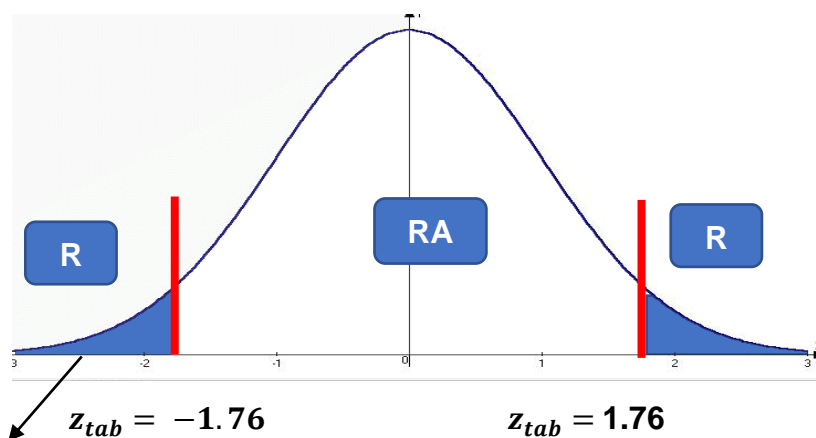
Tabla 10. Resultados con la prueba de Wilcoxon de porcentaje de cumplimiento de controles de la norma.

Prueba	PORCENTAJE DE CUMPLIMIENTO DE LOS CONTROLES DE LA NORMA
Z	-3,297 ^b
Sig. asintótica(bilateral)	,001

Distribución estadística de prueba:

Para el contraste de hipótesis se determinó la prueba de normalidad aproximada distribuida como $Z_{tab}(1-\alpha, n1 + n2 - 2)$. Reemplazando los valores se tuvo como resultados $z_{tab} 1 - 0.05 = 0.95$. por otro lado, el resultado de decisión comparó con el valor de $Z_{cal} = -2,329^b$ se representó en la campana de gauss

Figura 8. Campana de gauss



$Z_{cal} = -3,29^b$

Elaboración Propia

En la figura 8 nos evidencia el resultado de Z_{cal} ubicándose en la zona de rechazo, hecho que nos lleva a rechazar al H_0 a favor de la H_a , lo que lleva a la conclusión, mediante lo evidenciado en los resultados es favorable el método de seguridad que contribuyó el registro de usuarios no autorizados con un 95% de confianza

4.5. Contraste de hipótesis de Seguridad de las comunicaciones

4.5.1. Contraste de hipótesis: indicador 3.

Formulación de hipótesis

Ho: $Me^1 = Me^2$: El método de SI, no favorece en porcentaje de incidentes de en registro de comunicación de acceso remoto.

Ha: $Me^1 \neq Me^2$: El método de SI, favorece en porcentaje de incidentes de en registro de comunicación de acceso remoto.

Nivel de confianza

Para el nivel de confianza que se viene considerando en este estudio fue de 0.95 con un nivel de significancia del $\alpha=0.05$

Regla de decisión

Rechazar la Ho si $\text{sig} < \alpha$

Aceptar la Ho si $\text{sig} > \alpha$

Estadística de prueba:

La prueba wilcoxon se consideró como estadística para el estudio para muestras relacionadas(autor), Ya que no cumplieron las variables analizadas con los supuestos de normalidad, la fórmula es la siguiente.

$$T = \text{Min}[T(+), T(-)]$$

Donde T se ajusta a una distribución NORMAL por lo que es necesario utilizar la siguiente formula:

$$Z = \frac{T - n(n + 1)/4}{\sqrt{n(n + 1)(2n + 1)/24}}$$

Resultados del estadístico de prueba utilizando SPSS 26.0

El estudio de la variable Porcentaje de incidentes en registro de comunicación de acceso remoto comparado con el resultado descriptivo tabla 11 (Pre-test y Pos-test), el promedio del rango negativo demuestra ($\bar{x} = 9.15$) es mayor al positivo ($\bar{x} =$

5.70) indica que el Postest de los resultados fueron mayores, demostrando que el método ayudó en el porcentaje de incidentes en registro de comunicación de acceso remoto, también el resultado de la suma de rangos inclina a favor del estudio.

Tabla 11. Rangos comparativos de la prueba de wilcoxon porcentaje de incidentes en registro de comunicación de acceso remoto

Indicador		N	Rango promedio	Suma de rangos
PORCENTAJE DE INCIDENTES EN REGISTRO DE COMUNICACIÓN DE ACCESO REMOTO Pre - Post	Rangos negativos	10 ^a	9,15	91,50
	Rangos positivos	5 ^b	5,70	28,50
	Empates	0 ^c		
	Total	15		

Elaboración Propia

La tabla 12 muestra los resultados de las comparaciones de la prueba de wilcoxon evidencian, donde el sig = **0.009** < $\alpha = 0.05$, al no supera la prueba de normalidad demostrando de esta manera que el porcentaje de incidentes muestra diferencia favorable respecto al antes y el después.

Tabla 12. Resultados con la prueba de Wilcoxon de velocidad de descarga

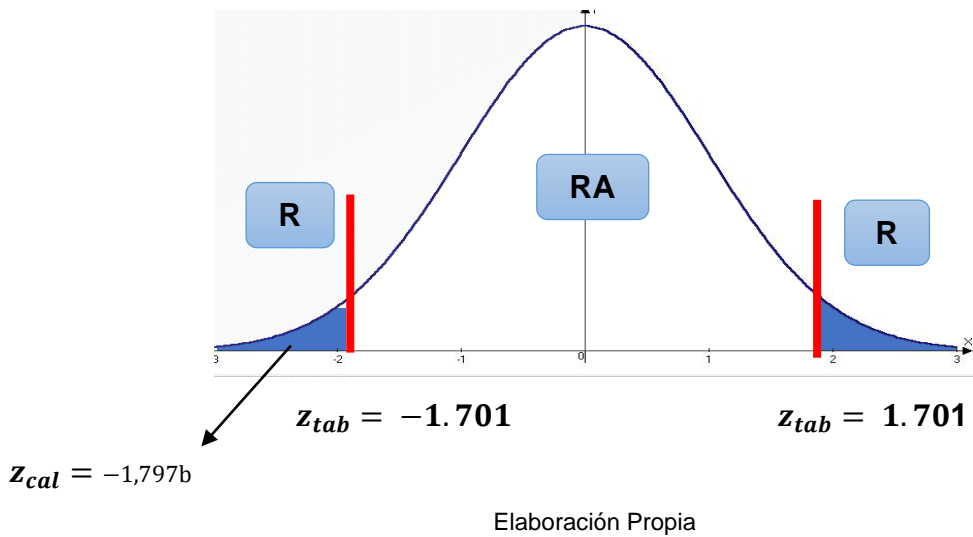
Prueba	PORCENTAJE DE INCIDENTES
Z	-1,797 ^b
Sig. asintótica(bilateral)	,072

Elaboración Propia

Distribución de la estadística de prueba:

Para decretar el contraste de hipótesis se usó la prueba de normalidad aproximada distribuida como $Z_{tab}(1-\alpha, n1 + n2 - 2)$. En este caso sustituyendo los valores se obtuvo como resultados $z_{tab}(1 - 0.05) = 1.95$. Los resultados de la decisión, se contrastó con el valor de $Z_{cal} = -1,797b$ y representando en la campana de gauss

Figura 9. Campana de gauss



En la figura 9 nos evidencia el resultado de Z_{cal} ubicándose en la zona de rechazo, hecho que nos lleva a rechazar al H_0 a favor de la H_a , lo que lleva a la conclusión, mediante lo evidenciado en los resultados es favorable el método de seguridad que contribuyó el registro de usuarios no autorizados con un 95% de confianza

4.6. Contraste de hipótesis de Control de Acceso

4.6.1. Contraste de hipótesis: indicador 4.

Formulación de hipótesis

H_0 : $Me^1 = Me^2$: El método de seguridad de la información no favorece en porcentaje de usuarios no autorizados.

H_a : $Me^1 \neq Me^2$: El método de seguridad de la información favorece en porcentaje de usuarios no autorizados.

Nivel de confianza

Para el nivel de confianza que se viene considerando en este estudio fue de 0.95 con un nivel de significancia del $\alpha=0.05$

Regla de decisión

Rechazar la Ho si sig < α

Aceptar la Ho si sig > α

Estadística de prueba:

La prueba wilcoxon se consideró como estadística para el estudio para muestras relacionadas (autor), ya que no cumplieron las variables analizadas con los supuestos de normalidad, la fórmula es la siguiente.

$$T = \text{Min}[T(+), T(-)]$$

Donde T se ajusta a una distribución NORMAL por lo que es necesario utilizar la siguiente fórmula:

$$Z = \frac{T - n(n + 1)/4}{\sqrt{n(n + 1)(2n + 1)/24}}$$

Resultados del estadístico de prueba utilizando SPSS 26.0

El estudio de la variable porcentaje de usuarios no autorizados comparado con los resultados descriptivos tabla 13 (Pre-test y Pos-test), el promedio del rango negativo ($\bar{x} = 7.50$) es mayor al positivo ($\bar{x} = .00$). indica que el pos-test de los resultados fue menor, demostrando que el método ayudó en el registro de usuarios no autorizados, también el resultado de la suma de rangos inclina a beneficio del estudio.

Tabla 13. Rangos comparativos de la prueba de wilcoxon porcentaje de registro de usuarios no autorizados

Indicador		N	Rango promedio	Suma de rangos
PORCENTAJE DE REGISTRO DE USUARIOS NO AUTORIZADOS Pre - Post	Rangos negativos	14 ^b	7.50	105,00
	Rangos positivos	0 ^b	.00	,00
	Empates	1 ^c		
	Total	15		

Elaboración Propia

La tabla 14 muestra los resultados de las comparaciones de la prueba de wilcoxon evidencian, donde el sig = **0.794** < $\alpha = 0.05$ y el post-test el sig < 0.011 al no supera la

prueba de normalidad demostrando de esta manera que el porcentaje de incidentes muestra diferencia favorable respecto al antes y el después

Tabla 14. Resultados con la prueba de Wilcoxon para el porcentaje de usuarios no autorizados

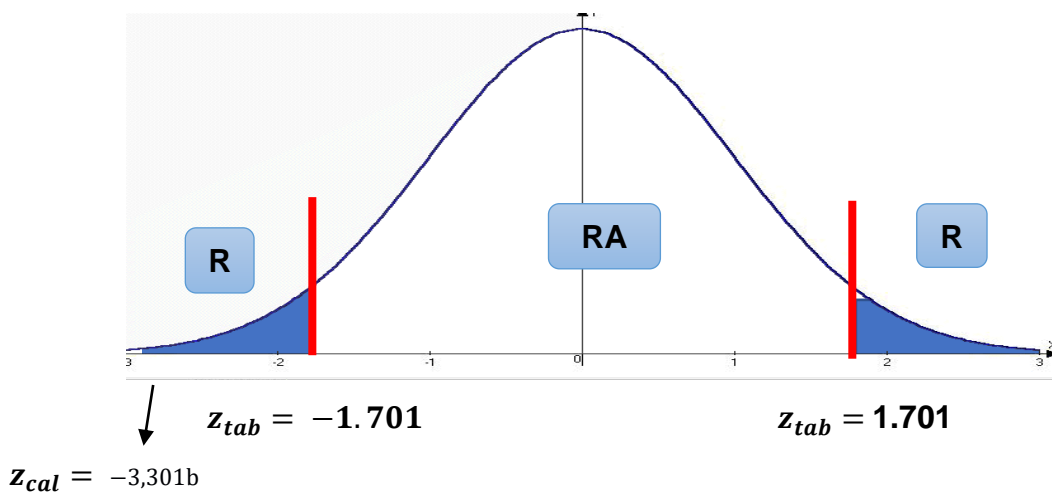
Prueba	PORCENTAJE DE REGISTRO DE USUARIOS NO AUTO
Z	-3,301 ^b
Sig. asintótica(bilateral)	,001

Elaboración Propia

Distribución de la estadística de prueba:

Para decretar el contraste de hipótesis se usó la prueba de normalidad aproximada distribuida como $Z_{tab}(1-\alpha, n1 + n2 - 2)$. En este caso sustituyendo los valores se obtuvo como resultados $z_{tab}(1 - 0.05) = 1.95$. Los resultados de la decisión, se contrastó con el valor de $Z_{cal} = -3301^b$ y representando en la campana de gauss.

Figura 10. Campana de gauss



La figura 10 nos evidencia el resultado de Z_{cal} ubicándose en la zona de rechazo, hecho que nos lleva a rechazar al H_0 a favor de la H_a , lo que lleva a la conclusión, mediante lo evidenciado en los resultados es favorable el método de seguridad que contribuyó el registro de usuarios no autorizados con un 95% de confianza.

V. DISCUSIÓN

El método de SGI apoyado en la ISO 27001 para el seguimiento y control de vulnerabilidad en pymes, considerando la metodología , se realizó la valoración y la clasificación de los activos de información con las dimensiones de disponibilidad, integridad, confidencialidad, gestión de activos, seguridad de las comunicaciones y control de acceso, además se determinó la vulnerabilidad de ocurrencia de las amenazas más relevantes como el mal funcionamiento de los equipos y las vulnerabilidades más frecuente. La presente investigación obtuvo resultados para el valor de tasación de activos de la información, en el pre-test el diagnóstico fue de 197.25 % y luego de la implementación del método seguridad, con un valor mayor pos test de 336.16%, en cuanto al porcentaje de incidentes en registro de comunicación de acceso remoto, el pre-test arrojó un valor de 55.66% y posteriormente a la implementación en la etapa de pos-test escaló a 71.46%, y para el porcentaje de usuarios no autorizados el valor Pretest alcanzó un valor de 59.40 % y después de la implementación en etapa Postest subió a 90.60%.En esta investigación nuestro objetivo es determinar la eficacia del método de SI basado en ISO 27001 para seguimiento y control de vulnerabilidad en pymes mediante los indicadores considerados de importancia que son los activos de la información por categoría, valor de tasación de los activos, numero de amenazas de activos de información, controles y porcentaje de controles aplicados.

(Rodriguez, Cruzado & Otros, 2020), en su estudio realizado, obtuvieron resultados favorables en su investigación en la que se propone la ISO 27001 como un instrumento que garantiza la SI para los clientes y proveedores. Por otro lado. En la confidencialidad de la información, se evidencia en la discreción de activos como componente principal en la toma de decisiones para la empresa, con respecto a la disponibilidad integridad, garantizó el fácil acceso y la credibilidad de los recursos ante la gran demanda de flujo de información en los procesos.

(Moyano y Suarez, 2017), en la tesis titulada “Plan de implementación de SGSI basado en ISO: 27001 para negocios de interfaces y soluciones”, siguiendo la metodología definen las tres dimensiones para la SGI que son confidencialidad, disponibilidad e integridad, al evaluar se concluye que la SGI se consigue

ejecutando un grupo de controles, que pueden ser políticas, estructuras organizativas, procedimientos, prácticas y funciones de software. Estos controles necesitan ser constituidos, insertados, vigilados para asegurar que se cumplan los objetivos específicos de seguridad y negocio de una organización. Además, (Quincho Ccesa, 2017), en su investigación diseño de un sistema de gestión basado en la NTP-ISO/IEC 27001:2014 realiza la valoración porcentual por secciones según la tabla, con los valores correspondientes de 0%, 25%, 50%, 75, 100% para evaluar el estado inicial de la institución a implementar, respecto a los requerimientos de la NTP ISO/IEC 27001:2014, se presentó los resultados mediante una cuadro en donde se consideró la valoración cuantitativa. Lo contrario de este estudio no detalla el objetivo a cumplir de los controles de valoración cualitativo y cuantitativo. Se obtuvo resultados en función de cada indicador en relación porcentual según norma.

Sobre el desarrollo de controles para monitorear y revisar la seguridad de los activos de información de la Ciudad de Marcavelica, con base en la NTPISO/IEC 27001:2014. Se realiza en base a un pre diagnóstico del nivel de riesgo de los activos de información, de la cual se determinó los controles por indicador a aplicar a la SI. (Alcantára Flores, 2015), en la tesis “Guía para implementar seguridad basada en la norma ISO/IEC 27001, soporte de seguridad en sistema informático de la comisaría Del Norte P.N.P. Concluye con la aplicación de políticas y controles con los indicadores de, nivel de seguridad, numero de procesos, nivel de riesgo, nivel de programas de capacitación, las técnicas usadas fueron ficha de observación, encuetas, entrevistas, reportes. Presentan nueve tablas de contenido como guía para la implementación de la seguridad basado en la ISO 27001, logrando incrementar el nivel de seguridad, y el plan de tratar los riesgos.

(Moreira, 2019) En su estudio mostró una mejora del 73% en la seguridad física cumpliendo con la norma ISO 27001 y un aumento del 50% en el control de acceso, permitiendo la aplicación de la norma. Para los controles de seguridad de la información, evaluar el riesgo y desarrollar precauciones para proteger los activos

estratégicos de la organización en la infraestructura técnica y servicios informáticos del municipio autónomo descentralizado de Chone Canton.

(Niño, 2018), Como resultado de aplicar el método MAGERIT y realizar un análisis de riesgo cuantitativo, se pudo conocer la amenaza a la que estaban expuestos los activos de información de ODEI Rambaiké, y quedó claro que el nivel de SGI de la institución era bajo.

VI. CONCLUSIONES

Al culminar esta investigación y haber obtenido los resultados del estudio, se llegó a la siguiente conclusión:

- Se determinó la eficacia del método de SGI basado en la ISO 27001 para el seguimiento de vulnerabilidad en pymes, se logró incrementar la SI luego de la implementar el método, también ayudó en la mejora de la comunicación entre las áreas de la empresa.
- También determinó la eficacia del método de SGI apoyado en la ISO en el control de vulnerabilidad en pymes, luego de aplicar los controles y políticas de seguridad en todas las áreas de la empresa.
- De acuerdo al previo análisis de riesgo realizado en la empresa se estableció las bases para establecer la mejora continua del método de SI, identificando los activos, las amenazas, las vulnerabilidades estimando los riesgos en la confidencialidad, disponibilidad, integridad. Estableciendo a si las bases mínimas a tener cuenta para la implementación del método de seguridad de la información, teniendo en cuenta que el método está sujeto a la mejora continua de los procesos y que nunca concluye.
- Los resultados obtenidos a nivel general se comprobó la eficacia del método de SI basado en la ISO 27001 contenido mediante la confidencialidad, integridad y disponibilidad de información siendo un aporte fundamental para la mejora de los niveles de seguridad de la información en las pymes en el área IT.
- Se han propuesto controles y políticas para el monitoreo y auditoría de seguridad de los activos de información. Incluye pasos e indicadores para implementar el SGSI en función del alcance del riesgo y el diagnóstico de impacto y cerrar brechas clave. Representativo de las vulnerabilidades encontradas en varios activos evaluados de la información.
- Mencionamos que solo en el procedimiento de las fases en este método solo llegamos a la FASE 4 por el tiempo de dicha investigación.

VII. RECOMENDACIONES

Se detalla las siguientes recomendaciones luego de haber obtenido los resultados y cumplir con los objetivos de esta investigación:

- Le sugiere que las futuras investigaciones de acuerdo con las nuevas normativas y actualizaciones de la norma ISO27001.
- El mismo que permite una mejor protección del valor de la información. Se recomienda adentrar la investigación en la ISO 27001, enfocadas a la gestión de la SI dentro de las pymes cubriendo un análisis más completo y obtener mejores resultados.
- Se recomienda que antes de implementar el método de seguridad de la SGI realizar un levantamiento de la infraestructura de la empresa, con el fin de identificar las vulnerabilidades, riesgos, identificado todo esto saber que controles aplicar para implementación del método.

REFERENCIAS

- ALCANTÁRA FLORES, J.C., 2015. Guía de implementación de la seguridad basado en la norma ISO/IEC27001, para apoyar la seguridad en los sistemas informáticos de la Comisaria del Norte P.N.P. en la ciudad de Chiclayo. *Universidad Católica Santo Toribio de Mogrovejo - USAT* [en línea], Disponible en: <http://tesis.usat.edu.pe/handle/usat/539>.
- ALEXANDER, J., 2015. Diseño De Un Sistema De Gestión De Seguridad De La Información Para Instituciones Militares. [en línea], pp. 192. Disponible en: <https://bibdigital.epn.edu.ec/handle/15000/10439?locale=en%0Ahttps://bibdigital.epn.edu.ec/bitstream/15000/10439/3/CD-6187.pdf>.
- ANDRESS, J., 2014. *Fundamentos de la seguridad de la información, segunda edición*. S.l.: s.n. ISBN 9780128007440.
- ANGULO, E., 2011. Política Fiscal y estrategica como factor de desarrollo de la mediana empresa comercial .S. [en línea], pp. 24. Disponible en: http://ridum.umanizales.edu.co:8080/jspui/bitstream/6789/377/4/Muñoz_Zapata_Adriana_Patricia_Artículo_2011.pdf.
- AZUCENA, S., 2016. Estadística descriptiva e inferencial. *El rincón de picanúmeros* [en línea]. Disponible en: <https://evidencia.com/archivos/3568>.
- BACA, V., 2016. Diseño de un sistema de gestión de seguridad de información para la unidad de gestión educativa local - Chiclayo. *Ingeniería: Ciencia, Tecnología e Innovación* [en línea], vol. 3, no. 1, pp. 42-56. Disponible en: <http://revistas.uss.edu.pe/index.php/ING/article/view/357/346>.
- BERMUDES y BAILON, 2015. Análisis En Seguridad Informática Y Seguridad De La Información Basado En La Norma Iso/lec 27001- Sistemas De Gestión De Seguridad De La Información Dirigido a Una Empresa De Servicios Financieros. , pp. 180.
- BURGOS, N., FRANCISCO, J. y ESCALONA, E., 2017. Prueba Piloto: Validación De Instrumentos Y Procedimientos Para Recopilar Data Antropométrica Con Fines Ergonómicos Purposes. *Ingeniería y Sociedad UC*, vol. 12, no. 1, pp. 31-47.

- EDWIN ROLANDO, 2013. Monitoreo seguimiento y Evaluacion. [en línea],
Disponible en: <http://edwingarcia1975.blogspot.com/2013/02/monitoreo-seguimiento-y-evaluacion.html#:~:text=Se entiende por seguimiento a,proyecto en su conjunto y.>
- FIGUEROA-SUÁREZ, J.A., RODRÍGUEZ-ANDRADE, R.F., BONE-OBANDO, C.C. y SALTOS-GÓMEZ, J.A., 2017. La seguridad informática y la seguridad de la información. *Polo del Conocimiento*, vol. 2, no. 12, pp. 145.
- FLORES, C. y FLORES, K., 2021. Pruebas Para Comprobar La Normalidad De Datos En Procesos Productivos: Anderson-Darling, Ryan-Joiner, Shapiro-Wilk Y Kolmogórov-Smirnov. *Periodicidad: Semestral*, vol. 23, no. 2, pp. 2021. ISSN 1560-0408.
- GARCIA, J., 2020. ComSec. *Comsec aplicacion que usan los ministros españoles para cifrar sus llamadas* [en línea]. Disponible en: [https://www.xataka.com/aplicaciones/comsec-app-que-usan-ministros-espanoles-su-movil-para-cifrar-llamadas-mensajes.](https://www.xataka.com/aplicaciones/comsec-app-que-usan-ministros-espanoles-su-movil-para-cifrar-llamadas-mensajes)
- GODOY, L., 2014. Seguridadd de la información. *Seguridad estaretegica*.
- HERNÁNDEZ, R., 2014. *Metodología de la investigación*. S.l.: s.n. ISBN 9788578110796.
- HURTADO, L.I. y TORO, G.J., 2006. *Paradigmas y metodos de investigacion*. S.l.: s.n. ISBN 9803284134.
- INEI, 2006. Sistema Estadistico nacional. *Paper Knowledge . Toward a Media History of Documents*,
- ISO 2700, 2015. Serie 2700. *Serie 2700* [en línea]. Disponible en: <https://www.iso27000.es/sgsi.html>.
- JINNSON MANUEL MOREIRA ÁLVAREZ, 2019. SEGURIDAD DE LA INFORMACIÓN DE INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS INFORMÁTICOS DEL GADM DEL CANTÓN CHONE BASADO EN LA NORMA ISO/IEC 27001. ,
- LAUDON, K.C. y LAUDON, J.P., 2017. *Sistemas de información gerencial*. S.l.:

s.n. ISBN 9786073209496.

MEIRE, 2018. Que es PDCA? *Qualiex* [en línea]. Disponible en:

<https://blogdelacalidad.com/que-es-pdca/>.

MINISTERIO, de la producción, 2020. Micro,pequeña y mediana empresas

(Mipyme). *Estudios Económicos* [en línea]. Disponible en:

<https://ogeiee.produce.gob.pe/index.php/en/shortcode/estadistica-oee/estadisticas-mipyme#:~:text=Más de 1%2C7 millones,pequeña y 0.2%25 mediana->.

MOYANO y SUAREZ, 2017. PLAN DE IMPLEMENTACION DEL SGSI BASADO EN LA ISO 27001:2013 PARA LA EMPRESA INTERFACE Y SOLUCIONES. , pp. 111.

NIÑO, N., 2018. Modelo De Un Sistema De Gestión De Seguridad De Información

– Sgsi, Para Fortalecer La Confidencialidad, Integridad, Disponibilidad Y Monitorear Los Activos De Información Para El Lambayeque., Instituto Nacional De Estadística E Informática - Inei Filial. [en línea], pp. 161.

Disponible en: <https://hdl.handle.net/20.500.12893/5935>.

POLANCO, A., 2014. DISEÑO DE UN MANUAL DE PROCEDIMIENTOS DEL SISTEMA CONTABLE EN LA EMPRESA FEVECOMEX S.A.S. BASADO EN LA NORMA TECNICA COLOMBIANA PARA LA SEGURIDAD DE LA INFORMACION NTC-ISO/IEC 27001/2006. *Paper Knowledge . Toward a Media History of Documents*, vol. 2006.

QUINCHO CCESA, M., 2017. Diseño De Un Sistema De Gestión De Seguridad

De La Información Bajo La Ntp Iso/iec 27001:2014 Para La Municipalidad Provincial De Huamanga. [en línea], pp. 2016. Disponible en:

http://209.45.73.22/bitstream/handle/UNSCH/1751/TESIS_SIS48_Cce.pdf?sequence=1&isAllowed=y.

QUISPE, E.S.A., 2020. Implementación de la norma ISO 27001 en el

departamento de tecnología de información de la empresa Esvicsac, Callao.

Repositorio Institucional - UCV [en línea], pp. 0-2. Disponible en:

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47276/Arias_QE

S-SD.pdf?sequence=1&isAllowed=y.

RODRIGUEZ, L., CRUZADO, C. y MEJÍA, C., 2020. Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*, vol. 8, no. 3. ISSN 23077999. DOI 10.20511/pyr2020.v8nspe3.786.

SÁNCHEZ, Á.P., 2013. *Diseño de un sistema de gestión de la seguridad de la información para comercio electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito* [en línea]. S.l.: s.n. ISBN 7777777777. Disponible en: <http://repositorio.puce.edu.ec:80/xmlui/handle/22000/6293>.

SANCHEZ, D. y CALDERON, D., 2012. "DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA COMWARE S.A. EN LA CIUDAD DE QUITO, APLICANDO LA NORMA ISO/IEC 27001". ,

TAM MALAGA, J., VERA, G. y OLIVEROS, R.R., 2008. *Tipos, métodos y estrategias de investigación*. 2008. S.l.: s.n.

TAMAYO, M., 2012. *El Proceso de investigación Científica*. S.l.: s.n.

TOLA, D. y LENIN, F., 2015. LA INFORMACIÓN PARA UNA EMPRESA DE CONSULTORÍA Y Resumen. , no. 1.

UNIR, 2022. Certificación ISO 27001 y para que sirve? [en línea]. Disponible en: <https://www.unir.net/ingenieria/revista/iso-27001/#:~:text=La ISO 27001 es una,y aplicaciones que la tratan>.

VAN DE VELDE, H., 2009. *Sistemas de Evaluación, Monitoreo, Seguimiento y Evaluación de Proyectos Sociales* [en línea]. S.l.: s.n. ISBN 9789992408315. Disponible en: <http://abacoenred.com/wp-content/uploads/2016/01/Sistemas-de-Evaluación-Monitoreo-Seguimiento-Evaluación-III-edición.pdf.pdf>.

ANEXOS

Anexo 1: Carta de autorización para la realización y difusión de resultados.



"Año del Fortalecimiento de la Soberanía Nacional"

LOS OLIVOS, 16 de febrero de 2021

Señor(a)
JOEL WILFREDO FRANCO ABREGU
GERENTE DE OPERACIONES
TELSERCOM SAC
AV COLOMBIA 439 INTERIOR 103 PUEBLO LIBRE

Asunto: Autorizar para la ejecución del Proyecto de Investigación de INGENIERÍA DE SISTEMAS

De mi mayor consideración:

Es muy grato dirigirme a usted, para saludarlo muy cordialmente en nombre de la Universidad Cesar Vallejo Filial LOS OLIVOS y en el mio propio, desearte la continuidad y éxitos en la gestión que viene desempeñando.

A su vez, la presente tiene como objetivo solicitar su autorización, a fin de que el Bach. FREDERICK LUI HUAMAN ESPINOZA del Programa de Titulación para universidades no licenciadas, Taller de Elaboración de Tesis de la Escuela Académica Profesional de INGENIERÍA DE SISTEMAS, pueda ejecutar su investigación titulada: **"MÉTODO DE SEGURIDAD DE INFORMACIÓN BASADA EN LA ISO 27001 PARA EL SEGUIMIENTO Y CONTROL DE VULNERABILIDADES EN PYMES"**, en la institución que pertenece a su digna Dirección; agradeceré se le brinden las facilidades correspondientes.

Sin otro particular, me despido de Usted, no sin antes expresar los sentimientos de mi especial consideración personal.

Atentamente,



Ing. M. Sc. Janina Cotrina Linares,
Coordinadora Nacional del taller
de titulación de Ingeniería de
Sistemas
UCV - Tarapoto

Ing. Joel Franco Abregú
GERENCIA DE OPERACIONES
TELSERCOM S.A.C.

cc: Archivo PTUN.

"Año del Fortalecimiento de la Soberanía Nacional"

LOS OLIVOS, 16 de febrero de 2021

Señor(a)
JOEL WILFREDO FRANCO ABREGU
GERENTE DE OPERACIONES
TELSERCOM S.A.C
AV COLOMBIA 439 INTERIOR 103 PUEBLO LIBRE

Asunto: Autorizar para la ejecución del Proyecto de Investigación de INGENIERÍA DE SISTEMAS

De mi mayor consideración:

Es muy grato dirigirme a usted, para saludarlo muy cordialmente en nombre de la Universidad Cesar Vallejo Filial LOS OLIVOS y en el mio propio, desearte la continuidad y éxitos en la gestión que viene desempeñando.

A su vez, la presente tiene como objetivo solicitar su autorización, a fin de que el Bach. RYDER IPANAMA MENDOZA del Programa de Titulación para universidades no licenciadas, Taller de Elaboración de Tesis de la Escuela Académica Profesional de INGENIERÍA DE SISTEMAS, pueda ejecutar su investigación titulada: **"MÉTODO DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA ISO 27001 PARA EL SEGUIMIENTO Y CONTROL DE VULNERABILIDADES EN PYMES"**, en la institución que pertenece a su digna Dirección; agradeceré se le brinden las facilidades correspondientes.

Sin otro particular, me despido de Usted, no sin antes expresar los sentimientos de mi especial consideración personal.

Atentamente,



Ing. M. Sc. Janina Cotrina Linares. **Ing. Joel Franco Abregu**
Coordinadora Nacional del taller de titulación de Ingeniería de Sistemas
UCV - Tarapoto
GERENCIA DE OPERACIONES
TELSERCOM S.A.C.



Lima, 13 de mayo del 2022

Señora:

Ing. M. Sc Janina Cotrina Linares
Coordinadora Nacional del taller de titulación de Ingeniería de Sistemas
Universidad Cesar Vallejo-Tarapoto

Estimada señora:

Por medio de la presente, reciba usted mi saludo cordial en nombre de la empresa Telsercóm.

Habiendo recibido su solicitud para que el Bachiller FREDERICK LUI HUAMAN ESPINOZA, del programa de Titulación de su Universidad, ejecute en nuestra Empresa su investigación titulada "METODO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 27001 PARA EL SEGUIMIENTO Y CONTROL DE VULNERABILIDAD EN PYMES" el área de gerencia de nuestra empresa AUTORIZA la ejecución de dicha investigación. Asimismo, nos comprometemos a brindarle todas las facilidades para que culmine con éxito el estudio a realizar.

Agradeciendo el beneficio que la empresa pueda obtener de dicho estudio, me despido de usted.

Atentamente:

Ing. Joel Franco Abregú
GERENCIA DE OPERACIONES
TELSECOM S.A.C.



Lima, 13 de mayo del 2022

Señora:

Ing. M. Sc Janina Cotrina Linares
Coordinadora Nacional del taller de titulación de Ingeniería de Sistemas
Universidad Cesar Vallejo-Tarapoto

Estimada señora:

Por medio de la presente, reciba usted mi saludo cordial en nombre de la empresa Telsercóm.

Habiendo recibido su solicitud para que el Bachiller RYDER IPANAMA MENDOZA, del programa de Titulación de su Universidad, ejecute en nuestra Empresa su investigación titulada "METODO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 27001 PARA EL SEGUIMIENTO Y CONTROL DE VULNERABILIDAD EN PYMES" el área de gerencia de nuestra empresa AUTORIZA la ejecución de dicha investigación. Asimismo, nos comprometemos a brindarle todas las facilidades para que culmine con éxito el estudio a realizar.

Agradeciendo el beneficio que la empresa pueda obtener de dicho estudio, me despido de usted.

Atentamente:



Ing. Joel Franco Abregú
GERENCIA DE OPERACIONES
TELSECOM S.A.C.

Anexo 2: Carta de Conformidad de Proyecto



"AÑO DEL FORTALECIMIENTO DE LA SOBERANIA NACIONAL"

Lima, 01 de junio del 2022

Señora:
Ing. M. Sc Janina Cotrina Linares
Coordinadora Nacional del taller de titulación de Ingeniería de Sistemas
Universidad Cesar Vallejo-Tarapoto

ASUNTO: CONFORMIDAD DEL PROYECTO

Es grato dirigirme a usted para saludarle cordialmente en nombre de la empresa Telsercom y hacer de su conocimiento que el señor **Frederick Lui Huamán Espinoza** con DNI N°43447195 y el señor **Ryder Ipanama Mendoza** con DNI N°10124220 estudiantes de la experiencia curricular de Desarrollo del Proyecto de Investigación, de la carrera de **INGENIERIA DE SISTEMAS** de vuestra casa de estudios, desarrolló el proyecto **"METODO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 27001 PARA EL SEGUIMIENTO Y CONTROL DE VULNERABILIDADES EN PYMES"**, el cual fue implementado para las pruebas respectivas de su funcionamiento.

En tal sentido, hago de su conocimiento que el Señor **Frederick Lui Huamán Espinoza** y el señor **Ryder Ipanama Mendoza**, ha realizado la entrega del proyecto. Por lo que estamos ofreciendo la **CONFORMIDAD Y ACEPTACIÓN DEL PROYECTO** desarrollado de acuerdo al compromiso definido.

Atentamente:
DNI: 09660337



Ing. Joel Franco Abregú
GERENCIA DE OPERACIONES
TELSERCOM S.A.C.

Anexo 3: Operacionalización de variables

OPERACIONALIZACIÓN DE VARIABLE

TITULO: “Método de Seguridad de la información basado en la ISO 27001 para el seguimiento y control de vulnerabilidad en pymes”

Tipo	Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Escala de Medición	Instrumentos
Variable Dependiente	VD1 Seguimiento de Vulnerabilidad	Viene a ser la observación, registro y sistematización de los resultados del monitoreo en términos de las metas intermedias cumplidas, los tiempos y presupuestos previstos y la estrategia de avance. (Quintero, 1995)	El método de seguridad de la información basado en la ISO 27001, permitirá a las empresas adoptar e implementar las medidas preventivas sobre la seguridad de la información mediante los controles que establece la ISO 27001 para mitigar los riesgos.	1. Gestión de activos	* Valor de tasación activos de información valorados.	Razón	Guía de Observación
	VD2 Control de Vulnerabilidad	Procedimiento que permite identificar analizar y controlar las vulnerabilidades sujetas al riesgo mediante una adecuada toma de decisiones en la empresa (ISO 27001).		2. Seguridad de las comunicaciones.	*. Porcentaje de estado de cumplimiento de los controles de la norma	Razón	Lista de Chequeo
3. Control de acceso			*. Porcentaje de incidentes en registro de comunicación de acceso remoto	Razón	Ficha de Registro del Indicador		
					*. Porcentaje de registro de usuarios no autorizados.	Razón	Ficha de Registro del Indicador

Anexo 4: MATRIZ DE CONSISTENCIA

TITULO: “Método de Seguridad de la información basado en la ISO 27001 para el seguimiento y control de vulnerabilidad en pymes”

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES E INDICADORES	METODOS Y TECNICAS DE INVESTIGACION
<p>PROBLEMA GENERAL</p> <p>El método de seguridad de la información basado en la ISO 27001 es eficaz en el seguimiento y control de vulnerabilidad en Pymes.</p> <p>PROBLEMA ESPECIFICO</p> <p>PE1: ¿En qué medida el método de seguridad de la información basado en la ISO 27001 es eficaz en el seguimiento de vulnerabilidad en Pymes??</p> <p>PE2: ¿En que medida el método de seguridad de la información basado en la ISO 27001 es eficaz en el control de vulnerabilidad en Pymes?</p>	<p>OBJETIVO GENERAL</p> <p>Determinar la eficacia del método de seguridad de la información basado en la ISO 27001 en el seguimiento y control de vulnerabilidad en pymes</p> <p>OBJETIVOS ESPECÍFICOS</p> <p>OE1: Determinar la eficacia del método de seguridad de la información basado en la ISO 27001 en el seguimiento de vulnerabilidad en pymes.</p> <p>OE2: Determinar la eficacia del método de seguridad de la información basado en la ISO 27001 en el control de vulnerabilidad en pymes.</p>	<p>HIPÓTESIS GENERAL</p> <p>El método de seguridad de la información basado en la ISO 27001 es eficaz en el seguimiento y control de vulnerabilidad en Pymes.</p> <p>HIPÓTESIS ESPECÍFICOS</p> <p>HE1: El método de seguridad de la información basado en la ISO 27001 es eficaz en el seguimiento de vulnerabilidad en Pymes.</p> <p>HE2: El método de seguridad de la información basado en la ISO 27001 es eficaz en el control de vulnerabilidad en Pymes.</p>	<p>VARIABLE INDEPENDIENTE</p> <p>Seguridad de la información</p> <p>D1. Confidencialidad</p> <p>D2. Integridad</p> <p>D3. Disponibilidad</p> <p>VARIABLE DEPENDIENTE</p> <p>VD1: Seguimiento de vulnerabilidad</p> <p>1 Gestión de activos</p> <p>*. Valor de tasación activos de información valorados.</p> <p>*. % de estado de cumplimiento de los controles de la norma</p> <p>2. Seguridad de las comunicaciones.</p> <p>* % de incidencias en registro de comunicación de accesos remotos.</p> <p>VD2: Control de Vulnerabilidad</p> <p>3. Control de acceso.</p> <p>* % de registro de usuarios no autorizados.</p>	<p>Métodos:</p> <p>Tipo: Descriptivo y aplicada</p> <p>Enfoque: Cuantitativo</p> <p>Diseño: Experimental</p> <p>$G \rightarrow O1 \rightarrow X \rightarrow O2$</p> <p>G= grupo</p> <p>O1= Grupo experimental de pre test</p> <p>O2 = Post Test</p> <p>X = Relación entre variable, coeficiente de relación.</p> <p>Técnicas de recolección</p> <p>- Fichaje.</p> <p>- Encuesta.</p>

Anexo 5. instrumento de validación



INSTRUMENTO DE VALIDEZ DE CONTENIDO DE LA PROPUESTA DE INGENIERÍA

TESIS: Método de seguridad de la información basado en la ISO 27001 para el seguimiento y control de vulnerabilidad en pymes.	Fecha 08/04/2022
--	----------------------------

ESCALA DE EVALUACIÓN

MUY MALO (1) MALO (2) REGULAR (3) BUENO (4) EXCELENTE (5)

Mediante la evaluación de expertos usted tiene la facultad de calificar el instrumento para validar la propuesta tecnológica utilizando la tabla de validación del instrumento. Esta tabla presenta escalas del 1 al 5 con su respectivo indicador de evaluación, se exhorta calificar de acuerdo a lo que Ud. considera como experto. Y proceda a realizar la sumatorias de los valores para establecer su validación.

I. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACIÓN				
		1	2	3	4	5
1. Claridad	Es formulado con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Organización	Esta organizado considerando las dimensiones e indicadores					X
4. Suficiencia	Las preguntas por dimensión consideran que son suficientes					X
5. Intencionalidad	Adecuado para valorar los aspectos del desarrollo de la aplicación presentada en la investigación.					X
6. Consistencia	Se encuentra basado en aspectos teóricos y científicos.					X
7. Coherencia	Las preguntas están relacionadas al indicador.					X
8. Metodología	Responde al propósito de evaluación del producto tecnológico para investigación.					X
9. Pertenencia	El instrumento es adecuado al tipo de usuario al cual será aplicado.					X
TOTAL		42				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

- [34 -45] El instrumento puede ser aplicado, tal como está elaborado
- [22 -33] El instrumento debe ser mejorado antes de ser aplicado
- [9 -21] El instrumento debe replanteado en su totalidad

III. FIRMA DEL EXPERTO

Master EDUARDO RONCAL AVALOS

DNI: 09901133

INSTRUMENTO DE VALIDEZ DE CONTENIDO DE LA PROPUESTA DE INGENIERÍA

TESIS: Método de seguridad de la información basado en la ISO 27001 para el seguimiento y control de vulnerabilidad en pymes.	Fecha 08/04/2022
--	----------------------------

ESCALA DE EVALUACIÓN
MUY MALO (1) MALO (2) REGULAR (3) BUENO (4) EXCELENTE (5)

Mediante la evaluación de expertos usted tiene la facultad de calificar el instrumento para validar la propuesta tecnológica utilizando la tabla de validación del instrumento. Esta tabla presenta escalas del 1 al 5 con su respectivo indicador de evaluación, se exhorta calificar de acuerdo a lo que Ud. considera como experto. Y proceda a realizar la sumatorias de los valores para establecer su validación.


I. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		1	2	3	4	5
1. Claridad	Es formulado con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Organización	Esta organizado considerando las dimensiones e indicadores					X
4. Suficiencia	Las preguntas por dimensión consideran que son suficientes					X
5. Intencionalidad	Adecuado para valorar los aspectos del desarrollo de la aplicación presentada en la investigación.					X
6. Consistencia	Se encuentra basado en aspectos teóricos y científicos.					X
7. Coherencia	Las preguntas están relacionadas al indicador.					X
8. Metodología	Responde al propósito de evaluación del producto tecnológico para investigación.					X
9. Pertenencia	El instrumento es adecuado al tipo de usuario al cual será aplicado.					X
TOTAL		40				
Sugerencias						

II. OPCIÓN DE APLICABILIDAD

- [34 -45] El instrumento puede ser aplicado, tal como está elaborado
- [22 -33] El instrumento debe ser mejorado antes de ser aplicado
- [9 -21] El instrumento debe replanteado en su totalidad

III. FIRMA DEL EXPERTO


 Master HUGO RONALD BUSTAMANTE
 MONDRAGÓN
 DNI: 40295718

**INSTRUMENTO DE VALIDEZ DE CONTENIDO DE LA PROPUESTA DE INGENIERÍA****TESIS:** Método de seguridad de la información basado en la ISO 27001 para el seguimiento y control de vulnerabilidad en pymes.**Fecha**
08/04/2022**ESCALA DE EVALUACIÓN**
MUY MALO (1) MALO (2) REGULAR (3) BUENO (4) EXCELENTE (5)

Mediante la evaluación de expertos usted tiene la facultad de calificar el instrumento para validar la propuesta tecnológica utilizando la tabla de validación del instrumento. Esta tabla presenta escalas del 1 al 5 con su respectivo indicador de evaluación, se exhorta calificar de acuerdo a lo que Ud. considera como experto. Y proceda a realizar la sumatorias de los valores para establecer su validación.

I. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		1	2	3	4	5
1. Claridad	Es formulado con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Organización	Esta organizado considerando las dimensiones e indicadores					X
4. Suficiencia	Las preguntas por dimensión consideran que son suficientes					X
5. Intencionalidad	Adecuado para valorar los aspectos del desarrollo de la aplicación presentada en la investigación.					X
6. Consistencia	Se encuentra basado en aspectos teóricos y científicos.					X
7. Coherencia	Las preguntas están relacionadas al indicador.					x
8. Metodología	Responde al propósito de evaluación del producto tecnológico para investigación.					X
9. Pertenencia	El instrumento es adecuado al tipo de usuario al cual será aplicado.					X
TOTAL		43				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

- (x) [34 -45] El instrumento puede ser aplicado, tal como está elaborado
- () [22 -33] El instrumento debe ser mejorado antes de ser aplicado
- () [9 -21] El instrumento debe replanteado en su totalidad

III. FIRMA DEL EXPERTO
MAESTRO NEMIAS SABOYA RIOS

DNI: 42001721

Anexo 6. Instrumentos usados para recolección de datos

Anexo de instrumento Pretest y Postest

GUÍA DE OBSERVACIÓN DE ACTIVOS

Instrucciones: En los días de observación se cuantificará el número de activos de información con la que se cuenta en la PYME.

CATEGORÍA DE ACTIVOS			
TIPO	CÓDIGO	CATEGORÍA	DESCRIPCIÓN
Activos de Información	AI01	Información en formato digital	Bases de datos y documentos que se conservan en formato electrónico
	AI02	Información escrita	Documentos que se conservan en forma impresa en papel
	AI03	Información hablada	Conversaciones telefónicas, presenciales o mediante medios virtuales
Activos de software	AS01	Software base o sistema operativo	Software considerado básico o sistema operativo
	AS02	Software licenciado, herramientas y utilitarios	Microsoft Office, antivirus, entre otros
	AS03	Software de desarrollo propio	Sistemas integrados, aplicativos entre otros
	AS04	Software de Administración de Base de Datos	SQL, MySQL, Oracle entre otros
	AS05	Otro tipo de software	Software desarrollado por terceros entre otros
Activos de Hardware	AH1	Equipo de procesamiento de datos	Servidores, computadoras, laptops, entre otros
	AH2	Equipo de comunicaciones	Routers, switches, access point, antenas, modems entre otros
	AH3	Medios de almacenamiento	Discos duros, respaldo, Dvds, memorias USB entre otros

	AH4	Mobiliario y equipamiento	Estantes, armarios, mesas, archivadores entre otros
	AH5	Otros equipos	Impresoras, fotocopadoras, scanners, cámaras entre otros
Activo de Servicios	ASV1	Procesamiento y comunicaciones	Servicio de procesamiento de la información, impresiones, fotocopias, telefonía, celular entre otros
	ASV2	Servicios generales	Aire acondicionado, electricidad entre otros
	ASV3	Otros servicios	Servicio de intermediarios, entre otros

CANTIDAD DE ACTIVOS IDENTIFICADOS					
ID ACTIVO	NOMBRE DEL ACTIVO	CÓDIGO DE LA CATEGORÍA	UBICACIÓN EN EL ÁREA	PROPIETARIO	ROL
AI01	Copias de respaldo	Información en formato digital	Data Center	La Empresa	Respaldo de Contingencia
AI02	Información escrita	Archivo físico - Datos de configuración de los sistemas de información	Almacén	La Empresa	Archivos de facturas y otros
AS01	Windows	Software base o sistema operativo	Data center	La empresa	Software base de sistema operativo
AS02	Microsoft office	Software licenciado, herramientas y utilitarios	Distribuido en las áreas en puestos de trabajo	La empresa	Microsoft Office
AS03	SQL, MySQL, Oracle entre otros	Software de Administración de Base de Datos	Data Center	La Empresa	Administra la base de datos de la empresa
AS04	Linux Software Apache	Software desarrollado por terceros entre otros	Data Center	La Empresa	Administra base de datos

AS05	Medios de Almacenamiento	Discos duros, respaldo, Dvds, memorias USB entre otros	Data center y en pc de usuarios final	La empresa	Procesamiento de datos
AH01	Servidores, computadoras, laptops, entre otros	Hardware Servidor Físico	Data Center	La empresa La empresa	Proceso de datos
AH02	Routers, switchs, access point, antenas, modems y otros	Equipo de comunicaciones	Data Center	La empresa	Control de tráfico de datos
AH03	Control de Acceso	Equipo de control de asistencia	RR.HH	La empresa	Control de trabajadores
AH04	Impresoras, fotocopiadoras, scanners, cámaras entre otros	Otros equipos	RR.HH y Áreas específicas	LA empresa	Proceso de datos y control .
A Servicio 01	Aire Acondicionado	Servicios generarles	Data Center, Gerencia general	La empresa	Disipación de equipos de TI y G.General

Anexo de instrumento Pretest y Postest

GUÍA DE OBSERVACIÓN DE TASACIÓN

En esta guía de observación se determina el nivel de los activos de información en la PYME

Instrucciones: En los días de observación se determinará el nivel de tasación de los activos de información. En la columna de confidencialidad, integridad y disponibilidad, se asigna un puntaje de acuerdo al criterio de valoración de acuerdo a lo que correspondería de acuerdo a la siguiente tabla:

VALOR	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
1	Se puede difundir, es de dominio público	Se puede tolerar que no esté disponible al menos una semana	Los errores o Modificaciones no autorizadas no generan impacto en la organización
2	Restringido para uso interno, si se filtra no ocasiona riesgo	Se puede tolerar que no esté disponible al menos un día	Los errores o modificaciones no autorizadas generan impacto leve en la organización
3	Protegido es necesario controles para su acceso, si se filtra ocasiona riesgo moderado a la organización	Se puede tolerar que no esté disponible al menos una hora	Los errores o modificaciones no autorizadas generan impacto moderado en la organización
4	información muy sensible, si se filtra se ocasiona un daño grave a la organización	No se tolera que el activo no se encuentre disponible	Los errores o modificaciones no autorizadas generan impacto crítico en la organización

La columna de tasación será el promedio aritmético de la valoración de las columnas de confidencialidad (C), integridad (I) y disponibilidad (D)

$$\text{Tasación} = (D+C+I) / 3$$

VALOR DE TASACIÓN DE LOS ACTIVOS DE INFORMACIÓN				
ID ACTIVO	DIMENSIÓN (Tasación = D+C+I)/3)			TASACIÓN ANTES
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	
AI01	2	2	1	1.67
AI02	2	1	2	1.67
AS01	3	2	2	2.33
AS02	3	2	2	2.33
AS03	2	3	1	2.00
ASO4	3	2	1	2.00
AH01	2	2	1	1.67
AH02	2	2	1	1.67
AH03	2	2	2	2.00
AH04	2	2	1	1.67
AH05	2	3	2	2.33
AH06	2	3	2	2.33
			TOTAL	38.33

Anexo de instrumento Pretest y Postest

GUÍA DE OBSERVACIÓN DE AMENAZAS

En esta guía de observación identificaremos las amenazas sobre los activos de información en la empresa PYME.

Indicador: Número de amenazas sobre activos de información.

Instrucciones: En los días de observación se cuantificará el número de activos de información en la PYME. En la columna de probabilidades de ocurrencia, se asigna un puntaje de acuerdo al criterio de valoración de la tabla siguiente.

VALOR		
NIVEL	PUNTAJE	CRITERIO
Baja	1	Muy rara vez
Mediana	2	Hasta dos veces al año
Alta	3	Hasta una vez al mes
Muy alta	4	Más de una vez al mes
Extrema	5	Varias veces a la semana o al día

AMENAZA SOBRE ACTIVOS DE INFORMACIÓN			
ID ACTIVO	AMENAZA	FUENTE DE LA AMENAZA	VALOR
01	Acceso a la red o al sistema de información por personas no autorizadas.	Externa	2
02	Incumplimiento de relaciones contractuales	Interna	4
03	Comprometer información confidencial.	Interna	5
04	Ocultar la identidad de un usuario.	Interna	3
05	Daño causado por un tercero.	Externa	3
06	Destrucción de registros.	Externa	4

07	Desastre generado por causas humanas.	Interna	1
08	Desastre natural, incendio, inundación, rayo.	Externa	2
09	Revelación de información.	Interna	1
10	Divulgación de contraseñas.	Interna	4
12	Errores en mantenimiento.	Externa	7
13	Fallo de los enlaces de comunicación.	Externa	5
14	Falsificación de registros.	Externa	3
15	Fuga de información.	Interna	3
16	Interrupción de procesos de negocio.	Externa	3
17	Mal funcionamiento del equipo.	Interna	3
18	Código malicioso.	Externa	4
19	Errores de software.	Externa	2
20	Hurtos o vandalismo.	Externa	1
21	Cambio involuntario de datos en un sistema de información.	Externa	2
22	Cambios no autorizados de registros.	Externa	3
23	Instalación no autorizada de software.	Interna	3
24	Acceso físico no autorizado.	Externa	3
25	Uso no autorizado de material con copyright.	Externa	3
26	Uso no autorizado de software.	Externa	3
27	Error de usuario.	Externa	2

Anexo de instrumento Pretest y Postest

GUÍA DE OBSERVACIÓN DE VULNERABILIDAD

Determinar las vulnerabilidades sobre activos de información para la empresa PYME.

Instrucciones: En los días de observación se cuantificará el número de activos de información en la PYME. En la columna de probabilidades de ocurrencia, se asigna un puntaje de acuerdo al criterio de valoración de la tabla siguiente.

VALOR		
NIVEL	PUNTAJE	CRITERIO
Baja	1	Muy rara vez
Mediana	2	Hasta dos veces al año
Alta	3	Hasta una vez al mes
Muy alta	4	Más de una vez al mes
Extrema	5	Varias veces a la semana o al día

VULNERABILIDADES SOBRE ACTIVOS DE INFORMACIÓN		
ID ACTIVO	VULNERABILIDADES	VALOR
02	Contraseñas predeterminadas no modificadas.	3
03	Eliminación de medios de almacenamiento sin eliminar datos.	1
04	Sensibilidad del equipo a los cambios de voltaje.	2
05	Inadecuada seguridad del cableado.	2
06	Inadecuada gestión de capacidad del sistema.	2
07	Gestión inadecuada del cambio.	1
08	Clasificación inadecuada de la información.	3
09	Control inadecuado del acceso físico.	1
10	Mantenimiento inadecuado.	2
11	Inadecuada gestión de red.	3
12	Respaldo inapropiado o irregular	3
13	Inadecuada gestión y protección de contraseñas.	3
14	Protección física no apropiada	4
15	Reemplazo inadecuado de equipos viejos.	3
16	Falta de formación y conciencia sobre seguridad.	3

17	Inadecuada segregación de funciones.	1
18	Insuficiente supervisión de los empleados y vendedores.	3
19	Pruebas de software insuficientes.	2
20	Falta de política de acceso o política de acceso remoto.	2
21	Ausencia de política de escritorio limpio y pantalla clara	3
22	Falta de control sobre los datos de entrada y salida.	4
23	Falta de documentación interna.	2
24	Carencia o mala implementación de la auditoría interna.	2
25	Falta de políticas para el uso de la criptografía.	3
26	Desprotección en equipos móviles.	1
27	Falta de redundancia, copia única	2
28	Ausencia de sistemas de identificación y autenticación.	1
29	Copia no controlada de datos.	3
30	Descarga no controlada de Internet.	3
31	Uso incontrolado de sistemas de información.	3
32	Software no documentado.	1

Anexo de instrumento Pretest y Postest

LISTA DE CHEQUEO DE CONTROLES APLICADOS

Se Determina los Controles aplicados según la normativa para la empresa PYME.

Indicador: Porcentaje de estado de cumplimiento de los controles de la norma

Instrucciones: Mediante la lista de los controles según la normativa, se marcará aquellos que se aplican a la empresa PYME.

CONTROLES APLICADOS SEGÚN LA NORMATIVA			
Sección 27001	Controles	Si/pre	Si/post
A.5	Políticas de seguridad de la información		
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información	x	x
A.5.1.1	Políticas para la seguridad de la información	x	x
A.5.1.2	Revisión de las políticas para la seguridad de la información		x
A.6	Organización de la seguridad de la información		
A.6.1	Organización interna		
A.6.1.1	Roles y responsabilidades para la seguridad de la información		x
A.6.1.2	Separación de deberes	x	
A.6.1.3	Contacto con las autoridades		x
A.6.1.4	Contactos con grupos de interés especial		x
A.6.1.5	Seguridad de la información en la gestión de proyectos	x	x
A.6.2	Dispositivos móviles y teletrabajo		x
A.6.2.1	Política para dispositivos móviles		x
A.6.2.2	Teletrabajo	x	x
A.7	Seguridad de los recursos humanos		
A.7.1	Antes de asumir el empleo		x
A.7.1.1	Selección	x	x
A.7.1.2	Términos y condiciones del empleo	x	x
A.7.2	Durante la ejecución del empleo		

A.7.2.1	Responsabilidades de la dirección	x	x
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información		x
A.7.2.3	Proceso disciplinario	x	x
A.7.3	Terminación y cambio de empleo		
A.7.3.1	Terminación o cambio de responsabilidades de empleo		
A.8	Gestión de activos		
A.8.1	Responsabilidad por los activos		
A.8.1.1	Inventario de activos	x	x
A.8.1.2	Propiedad de los activos	x	x
A.8.1.3	Uso aceptable de los activos	x	x
A.8.1.4	Devolución de activos	x	x
A.8.2	Clasificación de la información		x
A.8.2.1	Clasificación de la información		x
A.8.2.2	Etiquetado de la información		x
A.8.2.3	Manejo de activos	x	x
A.8.3	Manejo de medios	x	x
A.8.3.1	Gestión de medios removibles	x	x
A.8.3.2	Disposición de los medios	x	x
A.8.3.3	Transferencia de medios físicos		x
A.9	Control de acceso		
A.9.1	Requisitos del negocio para control de acceso		
A.9.1.1	Política de control de acceso	x	x
A.9.1.2	Acceso a redes y a servicios en red	x	x
A.9.2	Gestión de acceso de usuarios		
A.9.2.1	Registro y cancelación del registro de usuarios	x	x
A.9.2.2	Suministro de acceso de usuarios	x	x
A.9.2.3	Gestión de derechos de acceso privilegiado		x
A.9.2.4	Gestión de información de autenticación secreta de usuarios		x
A.9.2.5	Revisión de los derechos de acceso de los usuarios		x
A.9.2.6	Retiro o ajuste de los derechos de acceso		x
A.9.3	Responsabilidades de los usuarios		
A.9.3.1	Uso de información de autenticación secreta	x	x
A.9.4	Control de acceso a sistemas y aplicaciones		
A.9.4.1	Restricción de acceso a la información		x
A.9.4.2	Procedimiento de ingreso seguro	x	

A.9.4.3	Sistema de gestión de contraseñas	x	x
A.9.4.4	Uso de programas utilitarios privilegiados		x
A.9.4.5	Control de acceso a códigos fuente de programas		x
A.10	Criptografía		
A.10.1	Controles criptográficos		x
A.10.1.1	Política sobre el uso de controles criptográficos		x
A.10.1.2	Gestión de llaves		x
A.11	Seguridad física y del entorno		
A.11.1	Áreas seguras		x
A.11.1.1	Perímetro de seguridad física	x	x
A.11.1.2	Controles de acceso físico	x	x
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	x	x
A.11.1.4	Protección contra amenazas externas y ambientales	x	x
A.11.1.5	Trabajo en áreas seguras		x
A.11.1.6	Áreas de despacho y carga		x
A.11.2	Equipos		
A.11.2.1	Ubicación y protección de los equipos	x	x
A.11.2.2	Servicios de suministro	x	x
A.11.2.3	Seguridad del cableado		x
A.11.2.4	Mantenimiento de equipos	x	x
A.11.2.5	Retiro de activos	x	x
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		
A.11.2.7	Disposición segura o reutilización de equipos		
A.11.2.8	Equipos de usuarios desatendidos		x
A.11.2.9	Política de escritorio limpio y pantalla limpia		x
A.12	Seguridad de las operaciones		
A.12.1	Procedimientos operacionales y responsabilidades		x
A.12.1.1	Procedimientos de operación documentados		x
A.12.1.2	Gestión de cambios	x	x
A.12.1.3	Gestión de capacidad	x	
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		x
A.12.2	Protección contra códigos maliciosos		x
A.12.2.1	Controles contra códigos maliciosos		x
A.12.3	Copias de respaldo		x
A.12.3.1	Respaldo de la información	x	x
A.12.4	Registro y seguimiento		x

A.12.4.1	Registro de eventos		X
A.12.4.2	Protección de la información de registro	X	X
A.12.4.3	Registros del administrador y del operador	X	X
A.12.4.4	Sincronización de relojes		X
A.12.5	Control de software operacional		X
A.12.5.1	Instalación de software en sistemas operativos		X
A.12.6	Gestión de la vulnerabilidad técnica		X
A.12.6.1	Gestión de las vulnerabilidades técnicas		X
A.12.6.2	Restricciones sobre la instalación de software		X
A.12.7	Consideraciones sobre auditorias de sistemas de información		
A.12.7.1	Controles de auditoria de sistemas de información	X	X
A.13	Seguridad de las comunicaciones		
A.13.1	Gestión de la seguridad de las redes		
A.13.1.1	Controles de redes		
A.13.1.2	Seguridad de los servicios de red		X
A.13.1.3	Separación en las redes		X
A.13.2	Transferencia de información		X
A.13.2.1	Políticas y procedimientos de transferencia de información		X
A.13.2.2	Acuerdos sobre transferencia de información		
A.13.2.3	Mensajería electrónica	X	X
A.13.2.4	Acuerdos de confidencialidad o de no divulgación		X
A.14	Adquisición, desarrollo y mantenimiento de sistemas		
A.14.1	Requisitos de seguridad de los sistemas de información		X
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información		X
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas		X
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	X	X
A.14.2	Seguridad en los procesos de desarrollo y soporte		X
A.14.2.1	Política de desarrollo seguro	X	X
A.14.2.2	Procedimientos de control de cambios en sistemas	X	X
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		X

A.14.2.4	Restricciones en los cambios a los paquetes de software		x
A.14.2.5	Principios de construcción de los sistemas seguros		x
A.14.2.6	Ambiente de desarrollo seguro		x
A.14.2.7	Desarrollo contratado externamente		x
A.14.2.8	Pruebas de seguridad de sistemas	x	x
A.14.2.9	Prueba de aceptación de sistemas	x	x
A.14.3	Datos de prueba		
A.14.3.1	Protección de datos de prueba	x	x
A.15	Relaciones con los proveedores		
A.15.1	Seguridad de la información en las relaciones con los proveedores		x
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores		x
A.15.1.2	Tratamiento de seguridad dentro de los acuerdos con proveedores		x
A.15.1.3	Cadena de suministro de tecnología de información y comunicación		x
A.15.2	Gestión de la prestación de servicios de proveedores		x
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	x	x
A.15.2.2	Gestión de cambios en los servicios de los proveedores	x	x
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información		x
A.16.1.1	Responsabilidades y procedimientos	x	x
A.16.1.2	Reporte de eventos de seguridad de la información		x
A.16.1.3	Reporte de debilidades de seguridad de la información		x
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		x
A.16.1.5	Respuesta a incidentes de seguridad de la información		x
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información		x

A.16.1.7	Recolección de evidencia		x
A.17	Aspectos de seguridad de la información de la gestión de continuidad del negocio		
A.17.1	Continuidad de seguridad de la información		x
A.17.1.1	Planificación de la continuidad de la seguridad de la información		x
A.17.1.2	Implementación de la continuidad de la seguridad de la información		x
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información		x
A.17.2	Redundancias		x
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	x	
A.18	Cumplimiento		
A.18.1	Cumplimiento de requisitos legales y contractuales		x
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales		x
A.18.1.2	Derechos de propiedad intelectual		x
A.18.1.3	Protección de registros		x
A.18.1.4	Privacidad y protección de información de datos personales		
A.18.1.5	Reglamentación de controles criptográficos		x
A.18.2	Revisiones de seguridad de la información		
A.18.2.1	Revisión independiente de seguridad de la información		x
A.18.2.2	Cumplimiento con las políticas y normas de seguridad		x
A.18.2.3	Revisión del cumplimiento técnico		x

Tabla Resumen por Secciones Pre-tes

PORCENTAJE DE ESTADO DE CUMPLIMIENTO DE LOS CONTROLES DE LA NORMA				
Sección	Control	Ítems Total	Ítems que se cumplen	Porcentaje de cumplimiento
A.5	Políticas de seguridad de la información	2	1	50%

A.6	Organización de la seguridad de la información	10	3	33.3 %
A.7	Seguridad de los recursos humanos	10	4	25%
A.8	Gestión de activos	14	8	12.5 %
A.9	Control de acceso	19	7	14.28 %
A.10	Criptografía	4	2	50%
A.11	Seguridad física y del entorno	18	4	25%
A.12	Seguridad de las operaciones	22	6	16.66%
A.13	Seguridad de las comunicaciones	8	1	12.5 %
A.14	Adquisición, desarrollo y mantenimiento de sistemas	18	5	20 %
A.15	Relaciones con los proveedores	8	2	25%
A.16	Gestión de incidentes de seguridad de la información	9	1	11.11%
A.17	Aspectos de seguridad de la información de la gestión de continuidad del negocio	7	1	14,28
A.18	Cumplimiento	11	0	0 %

Anexo de instrumento Pretest y Postest

Ficha de Registro del Indicador: % de incidencias en registro de comunicación de acceso remoto

Instrucción: La ficha se llenará con los datos obtenidos de registro de incidencias reportados por los usuarios.

FICHA DE REGISTRO DE INCIDENCIAS					
Autor	Frederick Huamán, Ryder Ipanama		Tipo de prueba	Pre Test	Abril
				Post Test	Mayo
Empresa	Pyme				
Variable	Control de Vulnerabilidad (Variable Dependiente)				
Dimensión	Seguridad de las comunicaciones				
Periodo	1 días.				
Indicador	Descripción	Técnica	Unidad medida	Fórmula	
% de incidencias en registro de comunicación de acceso remoto.	Consiste en determinar el porcentaje de incidentes registrados en los accesos remotos.	Fichaje	Porcentaje	$\% IRCAR = \frac{NIR}{TIR} \times 100$	
				%IRCAR = Porcentaje de incidencia en registro de comunicación de acceso remoto.	
				NIR = Número de incidencias resueltas.	
				TIR = Total de incidencias reportadas.	
N°	Fecha	Numero IR	Total de Incidentes R.	Porcentaje De incidentes	
1	14/04/2022	2	3	0.67	
2	15/04/2022	2	4	0.50	

3	16/04/2022	1	3	0.33
4	18/04/2022	1	2	0.50
5	19/04/2022	3	4	0.75
6	20/04/2022	3	4	0.75
7	21/04/2022	3	3	1.00
8	22/04/2022	1	2	0.50
9	23/04/2022	3	3	1.00
10	25/04/2022	3	4	0.75
11	26/04/2022	1	5	0.20
12	27/04/2022	2	3	0.67
13	28/04/2022	2	3	0.67
14	29/04/2022	4	5	0.80
15	30/04/2022	3	4	0.75

Anexo de instrumento Pretest y Postest

Ficha de Registro del Indicador: % de registro de usuarios no autorizados.

Instrucción: La ficha se llenará con los datos obtenidos de registro de incidencias reportados por los usuarios.

FICHA DE REGISTRO					
Autor	Frederick Huamán, Ryder Ipanama		Tipo de prueba	Pre Test	Abril
				Post Test	Mayo
Empresa	Pyme				
Variable	Control de Vulnerabilidad (Variable Dependiente)				
Dimensión	Control de acceso				
Periodo	15 días				
Indicador	Descripción	Técnica	Unidad de medida	Fórmulas	
% de registro de usuarios no autorizados.	Es la cantidad de usuarios que intenta realizar registro sin contar con autorización.	Fichaje	Porcentaje	$\% PUNA = \frac{CUNAV}{TUNAR} \times 100$ <p>PUNA = Porcentaje de usuarios no autorizados.</p> <p>CUNAV = Cantidad de usuarios no autorizados verificados.</p> <p>TUNAR = Total de usuarios no autorizados registrados.</p>	
N°	Día	CUNAV	CTUNAR	% PUNA	
1	14/04/2022	2	3	0.67	
2	15/04/2022	1	4	0.80	
3	16/04/2022	4	5	1.00	
4	18/04/2022	1	1	1.00	
5	19/04/2022	3	3	0.50	
6	20/04/2022	1	2	1.00	
7	21/04/2022	1	1	0.50	

8	22/04/2022	2	4	0.50
9	23/04/2022	2	3	0.67
10	25/04/2022	1	2	0.50
11	26/04/2022	2	3	0.67
12	27/04/2022	3	3	1.00
13	28/04/2022	2	3	0.67
14	29/04/2022	1	3	0.33
15	30/04/2022	2	4	0.50

Anexo 7: MÉTODO DE SEGURIDAD DE INFORMACIÓN BASADA EN LA ISO 27001 PARA EL SEGUIMIENTO Y CONTROL DE VULNERABILIDADES EN PYMES

PYME	METODOLOGÍA	CÓDIGO: SGSI- METO-01 V1	
	TÍTULO: MÉTODO DE SEGURIDAD DE INFORMACIÓN BASADA EN LA ISO 27001 PARA EL SEGUIMIENTO Y CONTROL DE VULNERABILIDADES EN PYMES		
	Aprobado por:		Fecha Aprobación:
	Reemplaza a:	N° de Paginas	Fecha Publicación:

METODO
DE SEGURIDAD DE INFORMACIÓN BASADA EN LA ISO 27001 PARA EL
SEGUIMIENTO Y CONTROL DE VULNERABILIDADES EN PYMES
PYME
SGSI- METO-01

1. OBJETIVO

EL objetivo es establecer una metodología de seguridad de información basada en la ISO 27001 para el seguimiento y control de vulnerabilidades en pymes.

2. ALCANCE

Se aplica para el seguimiento y el control de vulnerabilidades de los activos en los procesos que forman parte del alcance del SGSI de las Pymes.

3. DEFINICIONES

Identificación de activos: Se entiende por activo todo lo que tiene valor para la organización, incluyendo medios físicos (edificios o equipos), intelectuales o de información (Ideas, aplicaciones, proyectos, etc.), marca, reputación, etc.

Identificar las Vulnerabilidades: Son las debilidades propias del activo que lo hacen susceptible de sufrir ataques o daños.

Identificar las Amenazas: Aquellos intrusos que puedan suceder y dañar el activo de la información, tales como desastres naturales, incendios o ataques de virus, espionaje etc.

Identificar los requisitos legales: Es toda normativa que la organización está obligada a cumplir con sus clientes, socios o proveedores.

Identificar Riesgo: Identificar para cada activo corporativo la probabilidad de que las amenazas o vulnerabilidades a ese activo puedan causar daño total o parcial al activo de información, en cuanto a la disponibilidad, seguridad e integridad de esa propiedad.

Cálculo del riesgo: Esto se hace en base a la probabilidad de ocurrencia del riesgo y su impacto en la organización ($\text{Riesgo} = \text{impacto} \times \text{probabilidad de amenaza}$). Con este proceso, identificamos los riesgos que deben ser controlados de manera prioritaria.

Tratamiento de Riesgo: La organización debe definir y aplicar un proceso para tratar los riesgos tal como son. En esta etapa, seleccionaremos las medidas de control adecuadas para cada riesgo, con el objetivo de: Asunción de riesgo:

siempre justificable. Por ejemplo, el costo de instalar un generador puede ser demasiado alto, por lo que la organización puede optar por pagarlo.

Controles y Secciones de la norma ISO 27001: La Norma ISO 27001 posee 114 controles la cuales están divididas en 14 secciones, para un adecuado uso del método en el seguimiento y control de vulnerabilidades en pymes se toma como base las siguientes secciones referidas a los controles.

4. NORMATIVAS

Norma ISO 27001

Norma ISO/IEC 27001:2013

5. RESPONSABILIDADES

5.1. Los Propietarios de los Activos de Información:

- ✓ Dar cumplimiento a este procedimiento.
- ✓ Promover la participación activa del personal en la identificación, análisis y evaluación de riesgos de seguridad de la información.
- ✓ Revisar y dar la conformidad a la matriz de riesgos.

5.2. El Comité de Gestión de Seguridad de Información

- ✓ Aprobar el resultado de la evaluación de riesgos.

5.3. El Oficial de Seguridad de la Información

- ✓ Verificar el cumplimiento del presente documento.
- ✓ Liderar los talleres a desarrollarse para la identificación, análisis y evaluación de riesgos de seguridad de la información.
- ✓ Compilar información remitida por los propietarios relacionada a la identificación, análisis y evaluación de riesgos de seguridad de la información.

- ✓ Presentar a los propietarios de procesos el resultado del análisis de riesgos.
- ✓ Presentar al Comité de Gestión de Seguridad de Información el resultado del análisis de riesgos para su aprobación

6. DESARROLLO

En el proceso de Análisis para el seguimiento y control de vulnerabilidades en pymes está sujeto a los métodos de valorización cuantitativos y esta orientado a los activos de información que soportan los procesos. Para ello se muestra el Mapa de Procesos de la Empresa.



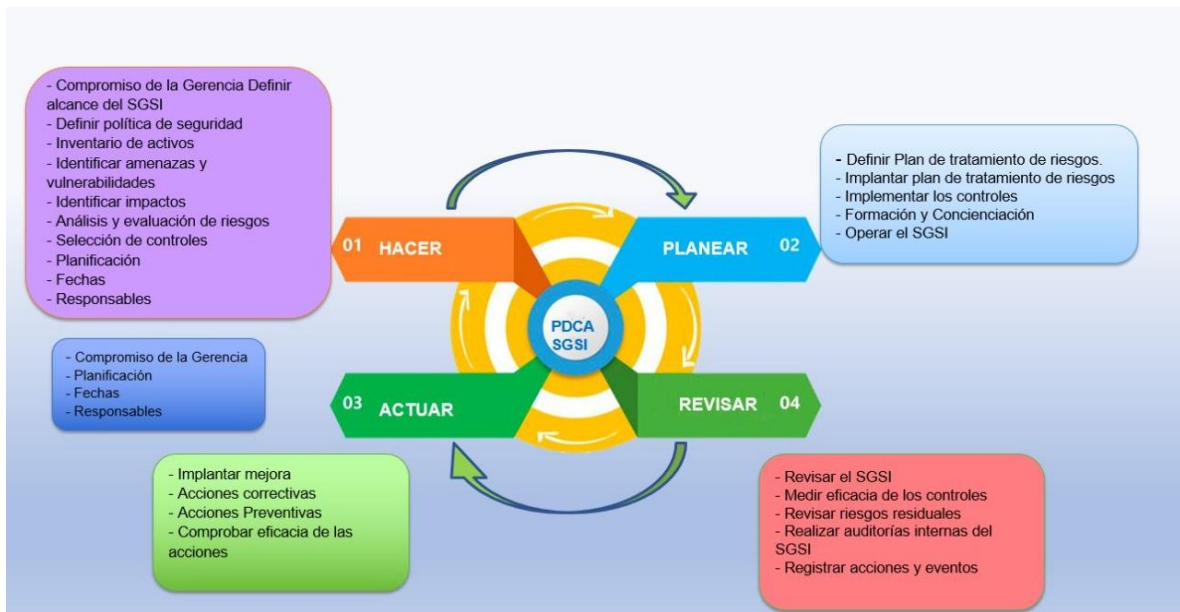
Usaremos el método PDCA que es una herramienta de la Calidad que se utiliza para el control de procesos, que tiene como foco la solución de problemas. Su aplicación consiste en cuatro fases que se adaptan de una forma muy sencilla a los sistemas de gestión siendo usados por las normas ISO. Conocido como ciclo de Deming o circulo de PDCA, por sus siglas en ingles que son PLAN, DO, CHEK y ACT.

En cada uno se desarrollará diferentes actividades correspondientes a cada fase que se detallan a continuación:

Figura 1:

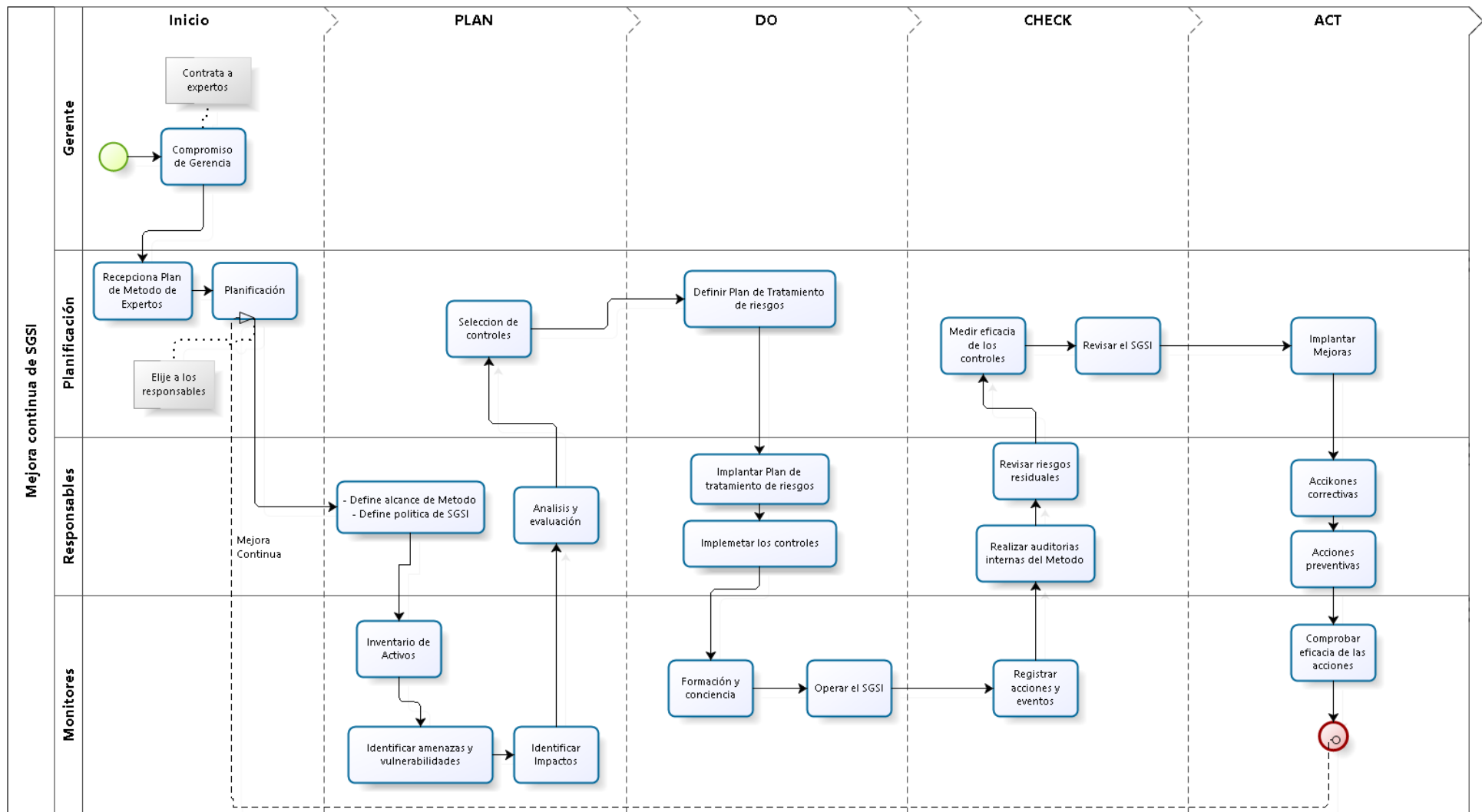


Figura 2



Para una mejor seguimiento y estructuración, procederemos a realizar un diagrama de flujo del Método de PDCA mediante los involucrados en cada fase y actividades ya antes mencionadas.

Para el inicio de constatación nos apoyaremos del procedimiento de Inventario de Activos de Información, para luego utilizar en el formato correspondiente.



Etapas del Método PDCA:

- Planificar(PLAN)

En primer lugar, se debe hacer un análisis y un estudio del proceso decidiendo así que mejoras se deben hacer y como lo llevarlo a cabo. (M.Aleman, 2004)

Esta etapa se divide en 5 pasos sucesivos que son:

- ✓ Definir el objetivo.
- ✓ Recopilar los datos.
- ✓ Elaborar el diagnóstico.
- ✓ Elaborar pronósticos.
- ✓ Planificar los cambios.

- Hacer (DO)

Es aquí donde se deben realizar el cambio tomando en cuenta la decisión que se haya tomado y la planificación que se ha efectuado. Siempre se recomienda hacerlo en pequeñas escalas para que de este modo podamos verificar los resultados y hacer algunos cambios en los modelos si es necesario, para trasladarlos a situaciones reales de trabajo mostrando mayor seguridad en el resultado final. (M. Aleman, 2004).

- Chequear (CHECK)

Una vez efectuado el acto, debemos verificar. Esto involucra el análisis y la medición de los efectos producidos por el cambio realizado al proceso, sin dejar pasar la comparación de las metas prospectadas con los resultados obtenidos chequeando si se ha logrado el objetivo del previsto. (M. Aleman, 2004) Se indica realizar los siguientes procesos:

- ✓ Se realizará la Ejecución de procedimientos de seguimiento y revisión de controles.
- ✓ Se debe realizar revisiones regulares de cumplimiento.
- ✓ Se debe medir la eficacia de los controles y verificación de satisfacción.
- ✓ Se debe realizar evaluación de riesgos según calendarios
- ✓ Se debe realizar auditorías internas.
- ✓ Se debe actualizar los planes de seguridad y registrar.

- Actuar (ACTION)

Para terminar el periodo debemos analizar los resultados, viendo que se puede mejorar, implementar, realizar acciones, etc., lo cual permitirá la mejora continua (M.Alemany, 2004) Se debe seguir los siguientes procesos:

- ✓ Implementar las mejoras identificadas para el plan de seguridad de información.
- ✓ Implementar las acciones correctivas y preventivas pertinentes.
- ✓ Comunicar acciones y mejoras a todas las partes involucradas.
- ✓ Asegurarse que las mejoras logren los objetivos previstos.

6.1. Identificación de Activos

La identificación y valorización de activos de información, se realizará según lo indicado. Clasificación de Activos de Información Mediante la Guía de Observación de Inventario de Activos.

6.2. Tasación de Activos de información valorados

La tasación y valorización de activos de información, se realizará según lo indicado. Dicha Tasación de Activos de Información es Mediante la Guía de Observación de Tasación.

6.3 Amenazas detectadas sobre los activos

Las Amenazas detectadas de activos de información, se realizará según lo indicado. Dicho registro se realiza mediante es Mediante la Guía de Observación de Tasación.

6.4. Determinar las vulnerabilidades sobre activos de información

La vulnerabilidad de los activos de información, se realizará según lo indicado. Dicha Tasación de Activos de Información es Mediante la Guía de Observación de Tasación.

6.5. Porcentaje de estado de cumplimiento de los controles de la norma

El Porcentaje de cumplimiento de controles de la norma de, se realizará según lo indicado. Dicho registro se realiza mediante es Mediante la Lista de Chequeo de Controles Aplicados.

Para la implementación del Sistema Integrado de Gestión basado en basado en la seguridad de la información ISO/IEC 27001:2014 y la continuidad del negocio ISO/IEC 22301 en la empresa, será segmentado de la siguiente manera para definir los procesos que se relacionan en nuestra propuesta:



6.6. Porcentaje de incidencias en registro de comunicación de acceso remoto

El Porcentaje de incidencias en registro de comunicación de acceso remoto, se realizará según lo indicado. Dicho registro se realiza mediante es Mediante la Ficha de Registro de Incidencias.

6.7. Porcentaje de registro de usuarios no autorizados

El Porcentaje de registro de usuarios no autorizados, se realizará según lo indicado. Dicho registro se realiza mediante es Mediante la Ficha de Registro de Incidencias.

Anexo 8: Declaración de autenticidad de los autores



UNIVERSIDAD CÉSAR VALLEJO

DECLARATORIA DE AUTENTICIDAD DE LOS AUTORES

Nosotros Huaman Espinoza Frederick Lui y Ipanama Mendoza Ryder alumnos de la Facultad de Ingeniería y Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo sede Lima Norte, declaramos juramento que todos los datos e información que acompañan al Trabajo Tesis titulado “Método de seguridad de la información basada en la ISO 27001 para el seguimiento y control de vulnerabilidades en Pymes” son:

1. De nuestra autoría.
2. El presente Trabajo de Tesis no ha sido plagiado ni total, ni parcialmente.
3. El Trabajo de Tesis no ha sido publicado ni presentado anteriormente.
4. Los resultados presentados en el presente Trabajo de Tesis son reales, no han sido falseados, ni duplicados, ni copiados.

Lima, 11 junio 2022

Nombre de participante:

.....
Huaman Espinoza Frederick Lui

DNI: 43447195

.....
Ipanama Mendoza Ryder

DNI: 10124220