UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Aplicación de la norma ISO 27001 para la gestión de la seguridad de la información en la empresa Plataforma Buscador Académico BUSAC. S.A. en Ecuador

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Cerezo Zambrano, Jamil Javier (orcid.org/0000-0002-9675-3239)

ASESOR:

Dr. Pacheco Torres, Juan Francisco (orcid.org/0000-0002-8674-3782)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

TRUJILLO – PERÚ

2022

DEDICATORIA

A mis padres, mis ángeles que me ven progresar desde el cielo,

A mis hermanos, porque han sido un ejemplo como estudiantes y profesionales.

A mi esposa por estar a mi lado en los momentos más difíciles de mi vida

A mis tías, Margarita y Lorena, por todo su apoyo y cariño de madre que me dieron cuando más lo necesité.

AGRADECIMIENTO

A Dios, por nunca abandonarme, por la inteligencia y las oportunidades para seguir progresando.

A mis padres, por la educación impartida, base fundamental de todas las decisiones en mi vida, piedra angular en mi formación como ser humano.

A mis hermanos, por ser ejemplo de profesionales y el apoyo para alcanzar mis metas.

A mi esposa, por ser parte fundamental en mi vida, apoyarme cuando más lo necesité y por el apoyo para alcanzar mis metas, las palabras no me alcanzarán para agradecerte todo lo que has hecho y sigues haciendo por mí.

A mis tías Margarita y Lorena, por la compañía, la solidaridad, el afecto, los consejos y todo aquello que me permitió superar momentos terribles en el pasado y que me permitieron seguir avanzando y forjarme como profesional.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo de investigación tuvo como objetivo el de mejorar la seguridad de la información en la empresa Guru-IT, esto mediante la implementación de la norma ISO 27001, utilizando este marco metodológico se desarrollaron políticas de seguridad que permitieron garantizar la disponibilidad, integridad y confidencialidad de la información. Se realizaron mediciones de vulnerabilidades que fueron recolectadas mediante el instrumento guía de observación para su posterior análisis estadístico, producto de este análisis se pudo obtener una mejora en la tasa de vulnerabilidades detectadas en el post test que se redujo en un 13,55 % en base a los datos del pre test, de igual manera se obtuvo una reducción en los tiempos de implementación de prácticas de seguridad y de detección de componentes vulnerables, 5,65 % y 11,97 % respectivamente, entre los datos del pre test y post test. En conclusión, la implementación de la norma permitió mejorar la seguridad de la información, aportando así competitividad y dando un mayor valor comercial a la empresa.

Palabras clave: ISO 27001, SGSI, Seguridad de la Información, Disponibilidad, Confidencialidad, Integridad.

ABSTRACT

The objective of this research work was to improve information security in the Guru-IT company, this through the implementation of the ISO 27001 standard, using this methodological framework, security policies were developed that allowed guaranteeing the availability, equipment and confidentiality of information. It was possible to detect vulnerabilities that were collected through the observation guide instrument for subsequent statistical analysis, as a result of this analysis it was possible to obtain an improvement in the rate of vulnerabilities detected in the post test, which was reduced by 13.55% based on In the pre-test data, in the same way, a reduction in the implementation times of security practices and detection of vulnerable components was obtained, 5.65% and 11.97% respectively, between the pre-test and post-test data. In conclusion, the implementation of the standard made it possible to improve information security, thus contributing to competitiveness and giving a greater commercial value to the company.

Keywords: ISO 27001, ISMS, Information Security, Availability, Confidentiality, Integrity.

I. INTRODUCCIÓN

Actualmente, la seguridad no es un tema que se limita al aspecto físico en las empresas, sino que juega un papel muy importante también en la información, ya que esta se considera un activo (Lopez et al., 2022), tanto como por su apoyo a la gerencia, así como también al momento de tomar decisiones, incluso esta se utiliza como producto o servicio intercambiable principalmente como objeto de negocio. Por esto y más la seguridad de la información(Andrzejewski, 2020), (en adelante SI por sus siglas) no debe abordarse solo desde un enfoque defensivo y reactivo, sino que se debe requerir que esta sea incorporada como elemento estratégico(Altamirano-de-la-Borda, 2021).

Al cumplir estándares, regulaciones e incorporar mecanismos de la SI, las compañías envían un importante mensaje a sus consumidores, al mismo tiempo que generan la confianza necesaria para su competitividad en el mercado. Es por esto que la SI no se limita a un mercado tecnológico e informático, si no que ha sido adaptada y requerida en todo el mundo en empresas de cualquier sector económico y de cualquier tamaño(García, 2007).

Plataforma Buscador Académico Busac. S.A. (de ahora en adelante conocida como Guru-IT por su nombre comercial) forma parte del grupo de empresas Gurusoft, es una empresa dedicada al soporte especializado de infraestructura IT, su principal benefactor Gurusoft empresa dedicada a la venta de soluciones orientadas a la facturación electrónica, está presente en nueve países de Latinoamérica, lo que hace extensa la cantidad de información que maneja en todas sus áreas, gestionar la seguridad de toda esa información se vuelve una tarea titánica y a medida que pasa el tiempo y la empresa crece, su dificultad aumenta.

La contratación de personal especializado, la compra de mejores equipos, no garantizan que se robustezca la seguridad de la información, ya que, si se tiene al personal y los equipos, pero no un marco de trabajo o sistema de gestión, que provean lineamientos de acción y protección, no se podrá identificar y tratar el riesgo asociado a la información y procesos de la empresa.

Es por ello que se planteó la ejecución de un Sistema de Gestión de Seguridad de la Información (en adelante SGSI) con una normativa ISO 27001 que provee un marco metodológico para identificar aquellos activos de información que impactan significativamente en la empresa, como piloto se plantea desarrollar esta investigación con el principal benefactor de Guru-IT que es Gurusoft, para ello se considera llevar a cabo un análisis y evaluación de los riesgos y por último optar por las opciones de tratamiento del riesgo a implementar con el objetivo de reducir las posibilidades de daño a la empresa por parte de las amenazas.

Para este trabajo investigativo se formula la siguiente problemática general: ¿De qué manera se puede mejorar la SI en la empresa Guru-IT, Ecuador en el año 2022?

Las variables que intervienen en la propuesta del trabajo de investigación son, como variable dependiente está Gestión de SI, como variable independiente la implementación de la norma ISO 27001, y como variable interviniente se define a la empresa Guru-IT

Los problemas específicos de la investigación son los siguientes: ¿De qué manera influirá aplicar la norma ISO 27001 en el tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura IT de la organización? ¿De qué manera influirá aplicar la norma ISO 27001 en la cantidad de componentes vulnerables de la infraestructura IT de la organización? ¿De qué manera influirá aplicar la norma ISO 27001 en la cantidad de vulnerabilidades detectadas en los componentes de la infraestructura IT de la organización? ¿De qué manera influirá la aplicación de la norma ISO 27001 en el tiempo de detección de vulnerabilidades en los componentes de la infraestructura IT de la organización?

Basándonos en lo anteriormente descrito, podemos sustentar los siguientes motivos como justificación del trabajo investigativo: de forma operativa se justifica ya que al reducir los equipos vulnerables y controlar sus vulnerabilidades o el tiempo de respuesta a las mismas, se reduce el tiempo en que los equipos se encuentren detenidos, o que estos no funcionen en condiciones óptimas.

Tecnológicamente hablando, la justificación viene dada ya que al implementar un SGSI con base en la norma ISO 27001 se automatiza el proceso de gestionar la

seguridad de los componentes de infraestructura, aprovechando así al máximo los recursos tecnológicos (Gesconsultor, AGGIL).

En cuanto a la justificación económica, se espera mantener operativos los componentes de infraestructura, y evitar pérdidas económicas por fallos en la seguridad de los mismos que afecten a los procesos operativos de la empresa(Boban & Cosic, 2008).

En el ámbito social, un SGSI con base en la norma ISO 27001 permitirá mantener a salvo y resguardada la información sensible de la empresa, de igual manera la información de los clientes, garantizando así la privacidad de los datos(Lin et al., 2018).

Como objetivo general se plantea: Mejorar la gestión de la SI en la empresa Guru-IT mediante la implementación de la norma ISO 27001. Como objetivos específicos de la investigación se plantean: Reducir el tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura IT de la organización. Reducir la cantidad de componentes vulnerables de la infraestructura IT de la organización. Reducir la cantidad de vulnerabilidades detectadas en los componentes de la infraestructura IT de la organización. Reducir el tiempo de detección de vulnerabilidades en los componentes de la infraestructura IT de la organización.

Según lo mencionado, se plantea la hipótesis siguiente: La implementación de la norma ISO 27001 permitirá mejorar la SI en Guru-IT en Ecuador 2022. Las hipótesis específicas se definen de la siguiente manera:

- La implementación de la norma ISO 27001 permitirá reducir el tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura IT de la organización.
- La implementación de la norma ISO 27001 permitirá reducir la cantidad de componentes vulnerables en la infraestructura IT de la organización.
- La implementación de la norma ISO 27001 permitirá reducir la cantidad de vulnerabilidades detectadas en los componentes de la infraestructura IT de la organización.

- La aplicación de la norma ISO 27001 permitirá reducir el tiempo promedio de detección de vulnerabilidades en los componentes de infraestructura IT de la organización.

II. MARCO TEÓRICO

Para la sustentación de la propuesta de este trabajo de investigación se hace referencia a trabajos de igual índole a nivel Nacional e Internacional. En cuanto a las revisiones internacionales se describe a Alexander & Jimenez (2021) con su trabajo realizado en España, en el cual se propone implementar un SGSI, el mismo se dividió en varias etapas partiendo con un análisis FODA que contextualiza y comprende la situación en la que se encuentra la empresa en cuanto al ámbito de la SI, para luego realizar un análisis diferencial con motivo de evaluación de la norma ISO/IEC 27001 en la empresa, dando como resultado los documentos propuestos para cumplir con la normativa de la implementación del SGSI.

El autor Rivera & Guerrero et al., (2019) en su trabajo establece que el esquema mostrado define e identifica los “debes” de la Norma, así como la “información documentada”, su propósito principal es que a través de una breve lectura se pueda tener un panorama claro y completo de los requisitos a cumplir.

En su trabajo de investigación Baca (2016) adopta COBIT 5 como marco de trabajo, el cual luego de analizar los resultados y utilizando diferentes instrumentos metodológicos se pudo identificar, analizar y diagnosticar varios factores que condicionan la SI en la UGEL – Chiclayo.

(Rojas & Romero, 2018) en su trabajo enfocado en una empresa de telecomunicaciones, basándose en un estudio realizado por IBM el cual determina que dichas empresas no poseen un control destinado a la protección de la información, desarrollaron un manual de políticas de seguridad, en el cual establecieron controles que les permitieron mitigar riesgos y vulnerabilidades, así como también el desarrollo de una herramienta con la capacidad de dar aviso y monitorear sobre el estado de los controles establecidos al personal pertinente.

En Colombia, los investigadores (Orjuela & Cárdenas, s. f. 2017) hicieron una propuesta para establecer un SGSI que permitió estandarizar los procesos llevados a cabo, así como su seguridad, todo esto en el área de TI, su desarrollo se resumió en cinco fases, planeación, contexto organizacional, gestión de riesgos, selección de salvaguardas y evaluación y/o auditoría de cumplimiento,

todo esto utilizando las fases de la metodología PHVA (Planificar, Hacer, Verificar, Actuar) y siempre alineándose a los objetivos y políticas de la empresa.

En la República de Moldova (RM) los autores (Technical University of Moldova & Alexei, 2021) realizaron un trabajo de investigación para el cumplimiento de estándares internacionales de SI, la comparativa fue realizada entre los Controles Obligatorios de Seguridad Cibernética (MCSR por sus siglas en inglés) y la norma ISO 27001, teniendo alineada la MCSR con la norma internacional garantizan la seguridad de los datos y recursos de la organización, generando también ventaja competitiva e interés en socios extranjeros.

En el ámbito nacional, Briones & Balón (2016) proponen una normalización de procesos, con controles que direccionan de una manera equitativa los procesos de la empresa para su posterior evaluación, esto permite una reestructuración organizacional con la que vendrán de la mano mejoras en el tratamiento de la SI. Su metodología se define de la siguiente manera, primero inicia con el diseño del CICLO PDCA de la empresa, donde se establecen cada una de las fases que contempla la norma, y luego de un análisis del estado inicial de la empresa se elaboran las políticas de seguridad.

(Valenzuela et al., s. f. 2018) en su trabajo desarrolló una guía para la implementación de un SGSI en el Ministerio de Salud Pública (MSP), el trabajo se alineó a la norma técnica ecuatoriana NTE ISO/IEC 27000, se implementaron políticas y controles que garantizan la confidencialidad, disponibilidad e integridad de la información, con esta propuesta permitieron configurar un proceso ágil para el servicio de agendamiento de citas del Contact Center del MSP

En el trabajo de (Secaira et al., 2020) enfocado en las instituciones de educación superior, identificó los procesos claves de una universidad (UTEQ, objeto de estudio) con el fin de identificar y clasificar los activos de información, así como también los controles que permitieron definir los alcances de su SGSI en base a la norma ISO 27001, todo esto con el objetivo de asegurar los activos ante posibles riesgos y demás vulnerabilidades; todo esto acompañado de un plan de concienciación y capacitación en aras de garantizar la confidencialidad, integridad y disponibilidad de la información.

(Coello Yagual & Pico Versoza, 2018) en su trabajo realizó un análisis acerca de las ventajas y desventajas de la SI, específicamente al momento de la toma de decisiones en aquellas empresas que usan Cloud Computing (CC) y Big Data BD), el estudio comprendió la norma ISO 27001 como elemento fundamental en la implementación de un SGSI, este último utilizado como herramienta para proteger los datos de tipo estructurado y no estructurado que conciernen al CC y BD.

Para la fundamentación conceptual la norma ISO/IEC 27001 publicada en el 2013, proporciona los requisitos para definir, aplicar, mantener y optimizar un SGSI. Con la aplicación de la norma, las organizaciones gestionan la seguridad de sus activos, permite evaluar los riesgos y aplicar los controles requeridos para la mitigación, reducción al mínimo o eliminación de los riesgos(ISO, 2013).

La norma se estructura de la siguiente manera para cumplir con los requisitos o disposiciones establecidas(Alexander & Jimenez, 2021):

Objeto y campo de aplicación, guía sobre la aplicación y uso de la norma(Alexander & Jimenez, 2021). Normativas referenciadas, anexo de documentos normativos para aplicar la norma y la metodología PDCA(Alexander & Jimenez, 2021).

Términos y definiciones, se establecen los términos y conceptos referentes a la SI y a la aplicación de la norma(Alexander & Jimenez, 2021). Contexto organizacional, contextualización de la organización y este como punto de referencia en la implementación del SGSI(Alexander & Jimenez, 2021).
Liderazgo, compromisos asumidos por el área directiva de la organizaciónpara la implementación del SGSI(Alexander & Jimenez, 2021). Planificación, plan que define los activos de importancia a proteger y las medidas a tomar para mitigar, reducir y prevenir los riesgos(Alexander & Jimenez, 2021).
Soporte, apoyar con los recursos para la implementación de lo planificado(Alexander & Jimenez, 2021).
Operación, seguimiento, inspección y cumplimiento de lo planificado para el tratamiento de riesgos(Alexander & Jimenez, 2021). Evaluación del desempeño, auditar y revisar para evaluación del desempeño de las operaciones ejecutadas (Alexander & Jimenez, 2021). Mejora continua, actualización constante del

sistema de gestión para identificar oportunidades de mejora(Alexander & Jimenez, 2021).

La norma ISO 27001 requiere un conjunto de documentos que se precisan para el cumplimiento normativo de la correcta implementación de un SGSI y a su vez la certificación del sistema(Alexander & Jimenez, 2021).

A continuación, se listan los documentos antes mencionados necesarios para el cumplimiento normativo:

- Política de seguridad. Procedimiento de Auditorías Internas. Gestión de indicadores. Procedimiento Revisión por Dirección. Gestión de Roles y Responsabilidades. Metodología de Análisis de Riesgos. Declaración de Aplicabilidad.

Según (Kenyon, 2019) las políticas basadas en la norma ISO 27001 desarrollarse en dos grandes niveles (superior e inferior), las políticas superiores serían aquellas que resumen la información de las políticas inferiores, estas no ahondan en detalles y deben indexar las políticas inferiores según el caso, también deben ser socializadas a todo el personal, la capacitación y concientización debe realizarse de manera transversal, en cambio las inferiores contienen todos los detalles y paso a paso de las políticas a cumplirse, la diferencia en estas radica en que deben socializar al personal apropiado según sea necesario.

Los autores (Haftom Gebreziagbher, 2018), (Mantra et al., 2020), (Eskaluspita, 2020) y (Pérez & Sáenz, 2017) coinciden en la importancia de la aplicación de un SGSI basado en la norma ISO 27001 para salvaguardar la información sensible de los diferentes estudiantes, docentes y personal administrativo que reposa en sus bases de datos, así como también información contable que se considere de suma importancia para las instituciones y su funcionamiento.

La gestión de SI según Niño Morante (2018) se define como un grupo de registros y procedimientos que solicitan la unificación de la tecnología, los ordenamientos y el comportamiento del usuario humano de tal manera que se lleven a cabo los objetivos de la SI, permitiendo que esta se encuentre disponible, íntegra y sea confidencial(Calder et al., 2010).

Un SGSI, basado en la norma UNEISO/IEC 27001, se considera parte del sistema de gestión general, enfocado en base al riesgo empresarial, que se instituye para establecer, implementar, operar, supervisar, examinar, conservar y mejorar la SI. Debido a esto, se puede decir que el objetivo principal de una organización al implementar este tipo de sistemas, es la identificación de los riesgos, la gestión de los mismos mediante las inspecciones correspondientes con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información, esto no significa un porcentaje de seguridad del 100%, sin embargo, permiten reducir el riesgo y el impacto de una forma estructurada y organizada(Rodriguez & Muñoz, s. f. 2018).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

Por el método de obtención de los datos, este trabajo se considera una investigación experimental que según se estipula es aquella en la que el investigador controla y manipula las variables independientes y examina las variables dependientes para determinar las variaciones relacionadas (Agudelo, s. f., 2008).

En base al enfoque adoptado, se define como una investigación cuantitativa, la cual es un proceso de tipo indagatorio con el objetivo de establecer algún conocimiento, así lo definen (Yucra Quispe & Bernedo Villalta, 2020), considerando además que este conocimiento deseado obtener pueda ser verificado, ordenado y sistematizado.

Y según su finalidad, se establece una investigación aplicada, que según definición de Nieto, s. f. (2018) esta nos permite solucionar problemas presentados en los procesos de producción.

Diseño de investigación

El diseño adoptado fue investigativo de tipo pre experimental, los mismos estudian las variables para analizar sus conductas resultantes en la investigación (Agudelo, s. f., 2008).

$$G = O1 \longrightarrow X \longrightarrow O2$$

Pre-test – Tratamiento – Post-test

Dónde:

G: Grupo experimental

X: Tratamiento

O1-O2: Mediciones pre-test/post-test del SGSI con base en la Norma ISO 27001:2013

3.2. Variables y operacionalización

Conceptualizando la variable independiente la norma ISO 27001 se define que esta forma parte de un conjunto de estándares internacionales sobre la SI (familia ISO 27000), estas contienen una colección de buenas prácticas que se utilizan para establecer, implementar, conservar y optimizar el SGSI, esta norma es certificable, lo cual quiere decir que si una compañía requiere que se le realice una auditoría a una entidad certificadora y el resultado es que está dentro de la normativa, obtiene la certificación(Ladino A. et al., 2011).

La definición operacional de la norma ISO 27001 consiste en seguir las buenas prácticas y lineamientos establecidos en la misma para reducir los incidentes ligados a la SI, debido a que la norma es certificable luego de realizada una auditoría, las empresas se ven obligadas a contar con un SGSI que debe estar implementado con al menos tres meses de anticipación a la auditoría, la misma que consta de tres fases, pre-auditoría (obtiene información sobre la situación de la organización) y la primera y segunda fase que consisten en examinar la documentación y denotar cualquier falencia de la norma(G. P. Rodríguez, 2017).

Conceptualizando la variable dependiente Gestión de la SI, se entiende por esta a la combinación de métodos y sistemas que avalan la CIA de la información, teniendo como objetivo la protección de la misma, y de los sistemas de la información que permiten su acceso, así como su uso, propagación, interrupción o pérdida sin autorización(Solá, s. f.).

La definición operacional de la SI consiste en tres grandes áreas, gestión de riesgos (reconoce y de prioridad los riesgos ligados al desarrollo de un servicio, producto u organización), proceso de ingeniería de seguridad (establece e efectúa soluciones a los inconvenientes que surgen debido a los riesgos) y proceso de aseguramiento (nivel de confianza que conforman los requisitos de seguridad)(Solá, s. f.).

Los indicadores presentados para la variable dependiente son los siguientes:

1. Tasa de vulnerabilidades detectadas en los componentes de la infraestructura TI.

2. Tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI de la organización.
3. Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI.
4. Tasa de componentes vulnerables de la infraestructura TI.

La tabla a continuación contiene los indicadores con sus respectivos instrumentos de medición.

Tabla 1 Indicadores e instrumentos de medición

Indicador	Instrumento	Cantidad	Fórmula
Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI	Guía de observación	50	Tiempo promedio para implementación de prácticas de seguridad = (Tiempo total para implementación de prácticas de seguridad / Número de prácticas implementadas)
Tasa de componentes vulnerables de la infraestructura TI	Guía de observación	50	Tasa componentes vulnerables = (Número de componentes-Cantidad total de componentes vulnerables)/Cantidad total de componentes vulnerables
Tasa de vulnerabilidades en los componentes	Guía de observación	50	Tasa de vulnerabilidades en los componentes = (Cantidad total de vulnerabilidades en los componentes - Número de componentes vulnerables) / Cantidad total de vulnerabilidades en los componentes
Tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI de la organización	Guía de observación	50	Tiempo promedio para implementación de prácticas de seguridad = (Tiempo total para identificar vulnerabilidades en los componentes / Tiempo total para identificar vulnerabilidades en los componentes)

Fuente: Elaboración propia

3.3. Población, muestra y muestreo

Población

Se utiliza el método inductivo que consiste en estudiar de lo particular a lo general(Ojeda, s. f. 2020), en la población y muestra, deseando que la parte objeto de estudio se distinga del entorno o población, asegurando así las conclusiones de la investigación, la población tomada en cuenta para este estudio son los componentes de la infraestructura IT resultando así en 50 equipos aproximadamente.

Muestra

Se determina la muestra mediante una fórmula de tipo aleatorio simple, se toma en cuenta un nivel de confianza del 95% con margen de error del 5%. Resultando en una muestra de: 45 componentes.

$$\text{Tamaño de la muestra} = Z2 * (p) * (1-p) / c2$$

Dónde:

Z = Nivel de confianza (95%)

p = .5

c = Marguen de error (.04 = ± 4)

Debido a que la población (50) y el tamaño de la muestra (45) no difiere significativamente se tomará la población total como parte de la muestra

Muestreo

No se aplica muestreo debido a que se toma la población total como la muestra de la investigación

3.4. Técnicas e instrumentos de recolección de datos

Técnica de recolección de datos

La técnica utilizada es la observación, esta no permitirá cumplir lo definido en los indicadores.

Instrumentos

Se utilizarán guías de observación para recopilar información y definir una base de datos. Estas nos permitirán alcanzar los objetivos planteados.

Validez y confiabilidad

La viabilidad de los instrumentos será verificada por tres expertos en investigación y seguridad de la información.

3.5. Procedimientos

Se recolectarán datos en base a la técnica de observación ya definida. Además, se utilizarán herramientas de detección de vulnerabilidades. Para realizar el procedimiento correspondiente se examinará el estado y vulnerabilidades de los componentes.

3.6. Método de análisis de datos

Para el análisis de los datos se contrastará la información de vulnerabilidad obtenida de los componentes, con las buenas prácticas y lineamientos establecidos en la norma. Se utilizará el software SPSS(Pallant, 2020) para la digitación de la información obtenida mediante el cuestionario predefinido para captura de información, además se realizará una prueba de normalidad(Ghasemi & Zahediasl, 2012) para analizar cuánto difiere la distribución de los datos observados respecto a lo esperado. Con respecto a la comprobación de hipótesis se aplicará el método estadístico en base al resultado, si es paramétrico una opción es la prueba T Students(Mishra et al., 2019) en dónde se evaluarán medias del grupo de estudio para comprobar si la hipótesis es nula o válida, caso contrario (si no es paramétrico) se utilizará la prueba de Wilcoxon(Moses, 2014) para los mismos fines.

3.7. Aspectos éticos

La información utilizada en este proyecto de investigación fue debidamente solicitada a la empresa objeto de estudio, misma que autorizó el uso de la misma para los fines pertinentes (su uso está regulado por un acuerdo de confidencialidad). Para el desarrollo del formato del trabajo de investigación se siguieron las pautas brindadas por la Universidad César Vallejo para los trabajos de posgrado.

IV. RESULTADOS

Estadística descriptiva

Medidas estadísticas del indicador Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI

Tabla 2 Medidas estadísticas del indicador Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI

Estadísticos descriptivos

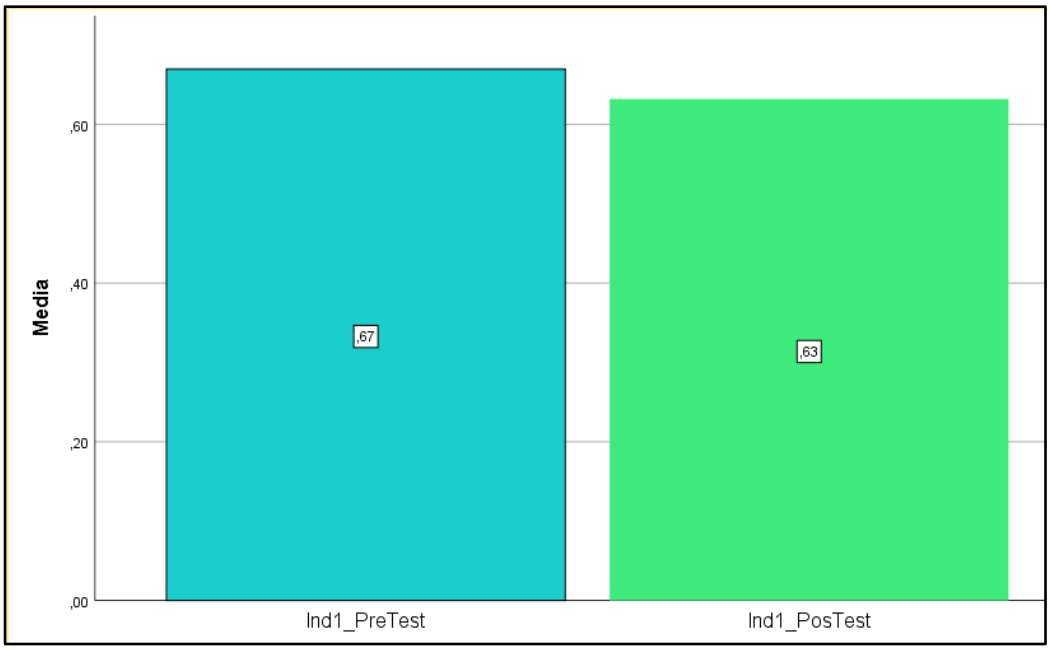
	N	Mínimo	Máximo	Media	Desv. Desviación
Ind1_PreTest	50	,43	,88	,6696	,11117
Ind1_PosTest	50	,39	,83	,6318	,11135
N válido (por lista)	50				

Fuente: Elaboración propia

En la tabla 1 se visualizan las medidas de dispersión y centralización del indicador Tiempo promedio (en horas) de implementación de prácticas de seguridad en los componentes de infraestructura TI, evidenciando una media PostTest (0,6318) por debajo del PreTest (0,6696), indicando así una reducción del tiempo promedio de implementación de prácticas de seguridad con una diferencia de 0,0378 que corresponde a un 5,65 %.

En cuanto a los rangos, se evidenció una reducción en los tiempos del PreTest (0,43 a 0,88) al PostTest (0,39 a 0,83), bajando de 0,45 a 0,44. Con respecto a su desviación estándar en el PreTest es 0,11117 (16,60% respecto a la media) y en el PostTest 0,11135 (17,62% respecto a la media).

Figura 1 Medias del indicador Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI



Fuente: Elaboración propia

La figura 1 que corresponde a las medias del indicador Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI, presenta una reducción del 5,64% del postTest en relación al pretest.

Medidas estadísticas del indicador Tasa de componentes vulnerables de la infraestructura TI

Tabla 3 Medidas estadísticas del indicador Tasa componentes vulnerables de la infraestructura TI

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
Ind2_PreTest	50	,39	,82	,5902	,11435
Ind2_PosTest	50	,37	,70	,5102	,08780
N válido (por lista)	50				

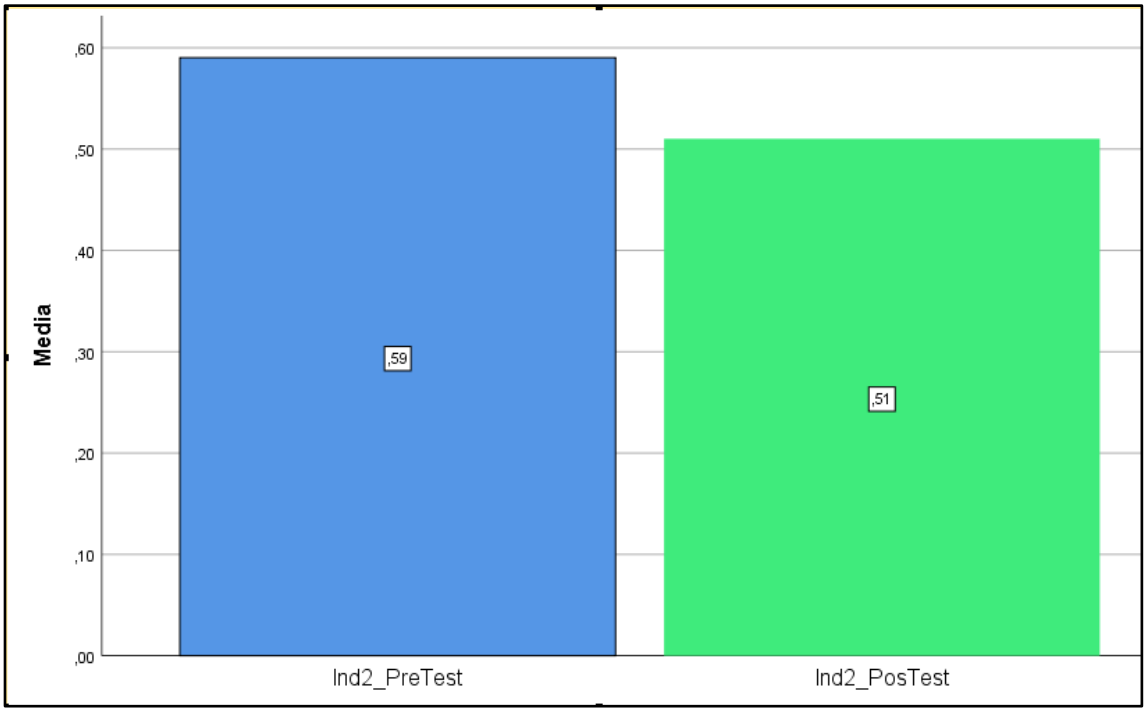
Fuente: Elaboración propia

En la tabla 2 se visualizan las medidas de dispersión y centralización del indicador Tasa componentes vulnerables de la infraestructura TI, evidenciando una media

PostTest (0,5102) por debajo del PreTest (0,5902), indicando así una reducción de la tasa de los componentes vulnerables con una diferencia de 0,08 que corresponde a un 13,55 %.

En cuanto a los rangos, se evidenció una reducción en los tiempos del PreTest (0,39 a 0,82) al PostTest (0,37 a 0,70), bajando de 0,43 a 0,33. Con respecto a su desviación estándar en el PreTest es 0,11435 (19,37% respecto a la media) y en el PostTest 0,08780 (17,20% respecto a la media).

Figura 2 Medias del indicador Tasa de componentes vulnerables de la infraestructura TI



Fuente: Elaboración propia

La figura 2 que corresponde a las medias del indicador Tasa de componentes vulnerables de la infraestructura TI, presenta una reducción del 13,55% del postTest en relación al pretest.

Medidas estadísticas del indicador Tasa de vulnerabilidades en los componentes de la infraestructura TI

Tabla 4 Medidas estadísticas del indicador Cantidad promedia de vulnerabilidades detectadas en los componentes de la infraestructura TI

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación

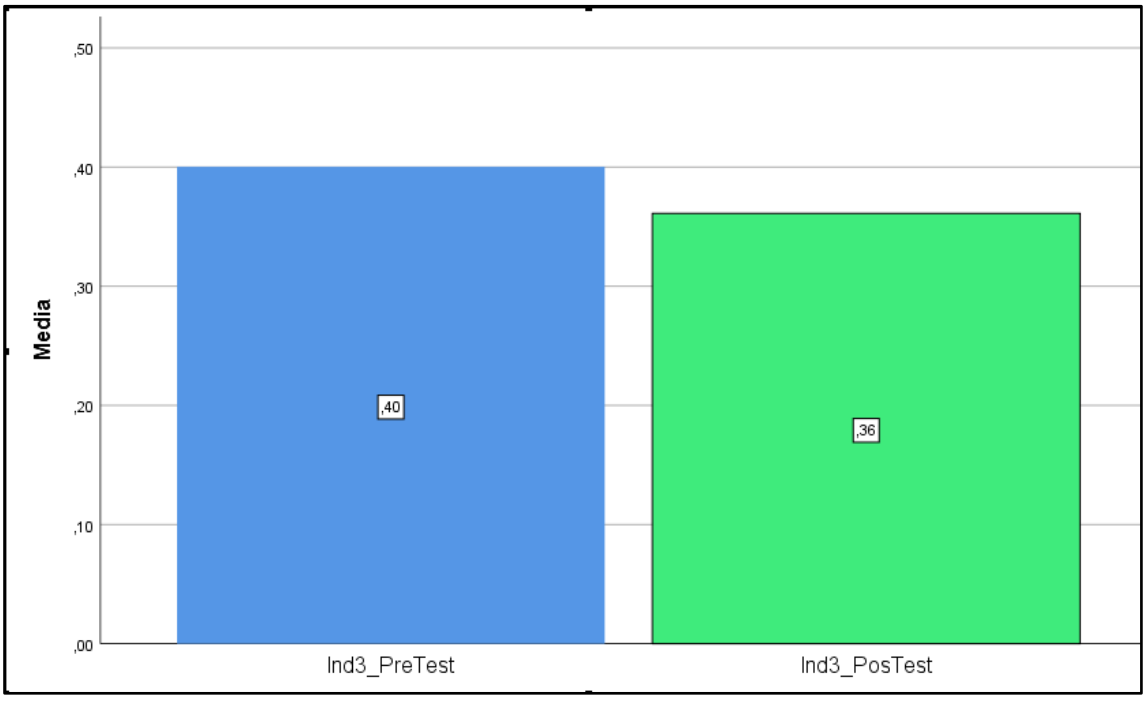
Ind3_PreTest	50	,00	,80	,4002	,23287
Ind3_PosTest	50	,00	,68	,3612	,18824
N válido (por lista)	50				

Fuente: Elaboración propia

En la tabla 3 se visualizan las medidas de dispersión y centralización del indicador Tasa componentes vulnerables de la infraestructura TI, evidenciando una media PostTest (0,3612) por debajo del PreTest (0,4002), indicando así una reducción en la cantidad promedia de vulnerabilidades detectadas en los componentes con una diferencia de 0,039 que corresponde a un 9,75 %.

En cuanto a los rangos, se evidenció una reducción en los tiempos del PreTest (0,00 a 0,80) al PostTest (0,00 a 0,68), bajando de 0,80 a 0,68. Con respecto a su desviación estándar en el PreTest es 0,23287 (58,18% respecto a la media) y en el PostTest 0,18824 (52,11% respecto a la media).

Figura 3 Medias del indicador Tasa de vulnerabilidades en los componentes de la infraestructura TI



Fuente: Elaboración propia

La figura 3 que corresponde a las medias del indicador Tasa de componentes vulnerables de la infraestructura TI, presenta una reducción del 9,75% del postTest en relación al pretest.

Medidas estadísticas del indicador Tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI de la organización

Tabla 5 Medidas estadísticas del indicador Tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI

Estadísticos descriptivos

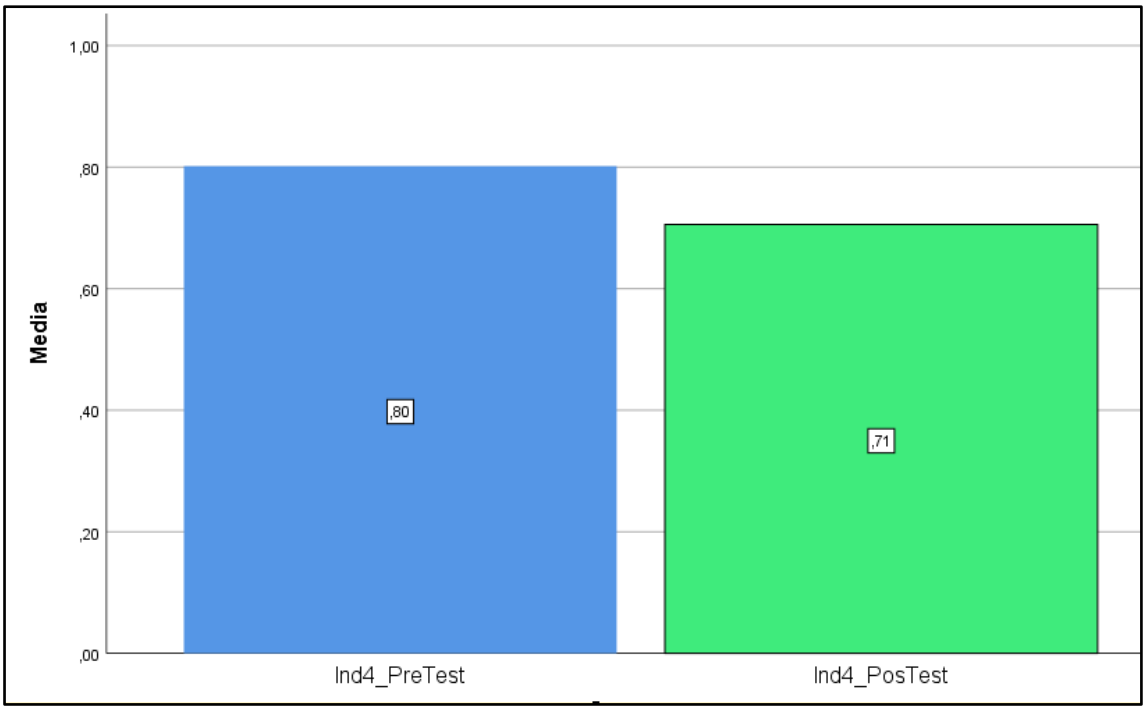
	N	Mínimo	Máximo	Media	Desv. Desviación
Ind4_PreTest	50	,24	3,00	,8016	,65056
Ind4_PosTest	50	,24	2,55	,7056	,54105
N válido (por lista)	50				

Fuente: Elaboración propia

En la tabla 4 se visualizan las medidas de dispersión y centralización del indicador tiempo promedio (en horas) de detección de vulnerabilidades en los componentes de la infraestructura TI, evidenciando una media PostTest (0,7056) por debajo del PreTest (0,8016), indicando así una reducción en el tiempo promedio de detección de vulnerabilidades en los componentes con una diferencia de 0,096 que corresponde a un 11,97 %.

En cuanto a los rangos, se evidenció una reducción en los tiempos del PreTest (0,24 a 3,00) al PostTest (0,24 a 2,55), bajando de 2,76 a 2,31. Con respecto a su desviación estándar en el PreTest es 0,65056 (81,15% respecto a la media) y en el PostTest 0,54105 (76,67% respecto a la media).

Figura 4 Medias del indicador Tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI de la organización



Fuente: Elaboración propia

La figura 4 que corresponde a las medias del indicador tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI, presenta una reducción del 11,25% del postTest en relación al pretest.

Estadística inferencial

Tabla 6 Prueba de normalidad de los indicadores pretest y postest

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Ind1_PreTest	,141	50	,014
Ind1_PosTest	,134	50	,026
Ind2_PreTest	,116	50	,093
Ind2_PosTest	,171	50	,001
Ind3_PreTest	,078	50	,200*
Ind3_PosTest	,097	50	,200*
Ind4_PreTest	,252	50	,000
Ind4_PosTest	,255	50	,000

Fuente: Elaboración propia

Se utilizó la prueba de Normalidad Shapiro Wilk(Razali & Wah, s. f. 2011) debido a que el tamaño de la muestra es 50. En la tabla 5 se muestran los resultados del nivel de significancia que es Sig = 0,14 en el pretest y 0,026 postTest del primer indicador. Para el segundo indicador su nivel de Sig = 0,093 para el pretest y 0,001 en el postTest, en cambio para el tercer indicador su nivel de Sig = 0,200 en el pretest y 0,200 para el postTest, y los valores de significancia del indicador 4 dio como resultado Sig = 0,000 para el pretest y postTest.

Para los indicadores 1, 2 y 4 se evidencia que no existe normalidad debido a que su nivel de significancia es menor a 0,050, en cambio para el tercer indicador se evidencia que existe normalidad porque los valores de significancia son mayores a 0.050.

Prueba de hipótesis

Hipótesis de investigación 1:

- **H1:** La aplicación de la norma ISO 27001 permitirá disminuir el tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI.
- **Indicador:** Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI

Hipótesis estadísticas

Definición de variables:

  - **TPIPSa:** Tiempo promedio de implementación de prácticas de seguridad antes de la implementación.
  - **TPIPSd:** Tiempo promedio de implementación de prácticas de seguridad después de la implementación.
- **Hipótesis nula Ho:** La aplicación de la norma ISO 27001 ayudará a aumentar el tiempo promedio de implementación de prácticas de seguridad.

Ho: TPIPSd – TPIPSa >= 0

- **Hipótesis alternativa Ha:** La aplicación de la norma ISO 27001 ayudará a disminuir el tiempo promedio de implementación de prácticas de seguridad

Ha: TPIPSd – TPIPSa < 0

Prueba Wilcoxon Indicador Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI.

Tabla 7 Prueba Wilcoxon aplicado al indicador Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI

Rangos

		N	Rango promedio	Suma de rangos
Ind1_PosTest - Ind1_PreTest	Rangos negativos	50[a]	25,50	1275,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	50		

a. Ind1_PosTest < Ind1_PreTest

b. Ind1_PosTest > Ind1_PreTest

c. Ind1_PosTest = Ind1_PreTest

Fuente: Elaboración propia

En la tabla 6 se visualizan los rangos, se evidencia que la población entera se encuentra negativa (reducción de tiempo), esto significa que se redujo el tiempo de implementación de prácticas de seguridad en los componentes de infraestructura TI

Tabla 8 Estadísticos de prueba del indicador tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI

Estadísticos de prueba[a]

	Ind1_PosTest - Ind1_PreTest
Z	-6,288[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: Elaboración propia

La tabla 7 nos muestra un valor de significancia de 0,000 que es menor a 0,050, entonces, se rechaza la hipótesis nula y se acepta la hipótesis de la investigación la cual indica que la aplicación de la norma ISO 27001 ayudará a disminuir significativamente el tiempo de implementación de prácticas de seguridad en los componentes de infraestructura TI.

Hipótesis de investigación 2:

- **H1:** La aplicación de la norma ISO 27001 permitirá disminuir la tasa de componentes vulnerables en la infraestructura TI.
- **Indicador:** Tasa de componentes vulnerables de la infraestructura TI

Hipótesis estadísticas

Definición de variables:

- **TCVa:** Tasa de componentes vulnerables antes de la implementación.
- **TCVd:** Tasa de componentes vulnerables después de la implementación.

- **Hipótesis Nula Ho:** La aplicación de la norma ISO 27001 permitirá aumentar la tasa de componentes vulnerables de la infraestructura TI.

Ho: TCVd – TCVa >= 0

- **Hipótesis Alternativa Ha:** La aplicación de la norma ISO 27001 permitirá disminuir la tasa de componentes vulnerables de la infraestructura TI.

Ha: TCVd – TCVa < 0

Prueba Wilcoxon Tasa de componentes vulnerables de la infraestructura TI.

Tabla 9 Prueba Wilcoxon aplicado al indicador tasa de componentes vulnerables de la infraestructura TI

Rangos

		N	Rango promedio	Suma de rangos
Ind2_PosTest - Ind2_PreTest	Rangos negativos	50[a]	25,50	1275,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	50		

a. Ind2_PosTest < Ind2_PreTest

b. Ind2_PosTest > Ind2_PreTest

c. Ind2_PosTest = Ind2_PreTest

Fuente: Elaboración propia

En la tabla 8 se visualizan los rangos, se evidencia que la población entera se encuentra negativa (reducción de tasa), lo cual quiere decir que se redujo la tasa de componentes vulnerables de la infraestructura TI.

Tabla 10 Estadísticos de prueba del indicador tasa de componentes vulnerables de la infraestructura TI

Estadísticos de prueba[a]	
	Ind2_PosTest - Ind2_PreTest
Z	-6,185[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: Elaboración propia

La tabla 9 nos muestra un valor de significancia de 0,000 que es menor a 0,050, entonces, se rechaza la hipótesis nula y se acepta la hipótesis de la investigación que indica que la aplicación de la norma ISO 27001 ayudará a disminuir significativamente el tiempo de implementación de prácticas de seguridad en los componentes de infraestructura TI.

Hipótesis de investigación 3:

- **H1:** La aplicación de la norma ISO 27001 permitirá disminuir la tasa de vulnerabilidades en los componentes de la infraestructura TI.
- **Indicador:** Tasa vulnerabilidades en los componentes de la infraestructura TI

Hipótesis estadísticas

Definición de variables:

  - **TVCa:** Tasa de vulnerabilidades en los componentes antes de la implementación.
  - **TVCd:** Tasa de vulnerabilidades en los componentes después de la implementación.
- **Hipótesis Nula Ho:** La aplicación de la norma ISO 27001 permitirá aumentar la tasa de vulnerabilidades en los componentes infraestructura TI.

Ho: TVCd – TVCa >= 0

- **Hipótesis Alternativa Ha:** La aplicación de la norma ISO 27001 permitirá disminuir la tasa de vulnerabilidades en los componentes infraestructura TI.

Ha: TVCd – TVCa < 0

Prueba T Students Indicador de Tasa de vulnerabilidades en los componentes de la infraestructura TI.

Tabla 11 Prueba T. Diferencia de las medias del indicador tasa de vulnerabilidades en los componentes de la infraestructura TI

Prueba de muestras emparejadas

		Diferencias emparejadas							
			Desv.	Desv. Error	95% de intervalo de confianza de la diferencia				Sig.
		Media	Desviación	promedio	Inferior	Superior	t	gl	(bilateral)
Par 1	Ind3_PreTest - Ind3_PosTest	,03900	,05891	,00833	,02226	,05574	4,681	49	,000

Fuente: Elaboración propia

En la tabla 10 se muestra los resultados con la prueba T, que podemos observar que existe diferencia significativa estadística (p-valor < 0.05), se rechaza la hipótesis nula y se acepta que existe diferencia en las medias de pretest y post con respecto a la tasa de vulnerabilidades en los componentes de la infraestructura TI.

Hipótesis de investigación 4:

- **H1:** La aplicación de la norma ISO 27001 permitirá disminuir el tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI.
- **Indicador:** Tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI

Hipótesis estadísticas

Definición de variables:

  - **TPDVa:** Tiempo promedio de detección de vulnerabilidades antes de la implementación.
  - **TPDVd:** Tiempo promedio de detección de vulnerabilidades después de la implementación.
- **Hipótesis Nula Ho:** La aplicación de la norma ISO 27001 ayudará a aumentar el tiempo promedio de detección de vulnerabilidades en los componentes de infraestructura TI.

Ho: TPDVd – TPDVa >= 0

- **Hipótesis Alternativa Ha:** La aplicación de la norma ISO 27001 ayudará a disminuir el tiempo promedio de detección de vulnerabilidades en los componentes de infraestructura TI.

Ha: TPDVd – TPDVa < 0

Prueba Wilcoxon Indicador Tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI de la organización.

Tabla 12Prueba Wilcoxon aplicada al indicador tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI de la organización

Rangos

		N	Rango promedio	Suma de rangos
Ind4_PosTest - Ind4_PreTest	Rangos negativos	49[a]	25,00	1225,00
	Rangos positivos	1[b]	50,00	50,00
	Empates	0[c]		
	Total	50		

a. Ind4_PosTest < Ind4_PreTest

b. Ind4_PosTest > Ind4_PreTest

c. Ind4_PosTest = Ind4_PreTest

Fuente: Elaboración propia

En la tabla 11 se visualizan los rangos, se evidencia que la mayoría de la población se encuentra negativa (reducción de tiempo) y solo existe 1 par en el rango positivo (aumento de tiempo), lo cual quiere decir que se redujo el tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI de la organización.

Tabla 13 Estadísticos de prueba del indicador tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI

Estadísticos de prueba[a]

	Ind4_PosTest - Ind4_PreTest
Z	-5,687[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: Elaboración propia

La tabla 12 nos muestra un valor de significancia de 0,000 que es menor a 0,050, entonces, se rechaza la hipótesis nula y se acepta la hipótesis de la investigación que indica que la aplicación de la norma ISO 27001 ayudará a disminuir significativamente el tiempo de detección de vulnerabilidades en los componentes de infraestructura TI.

V. DISCUSIÓN

Considerando los resultados del trabajo de investigación se evidencia una mejora en los indicadores correspondientes a la variable dependiente, habiendo aplicado el experimento y recolectados los datos del post test.

Para conocer la normalidad de los datos se utilizó la prueba Kolmogorov-Smirnov(R. H. C. Lopes, 2011), dando como resultado que no se presenta normalidad de datos en los indicadores 1,2, y 4 de esta investigación, caso contrario para el tercer indicador.

Por ello, se usó la prueba Wilcoxon para comparar las medias de los indicadores 1,2 y 4, dando como efecto que el valor de significancia sea 0,026, 0,001 y 0,000 respectivamente, para el tercer indicador se aplicó la prueba T-Students en la comparación de su media arrojó un valor de significancia de 0,200. Debido a esto, se rechazaron las hipótesis nulas H_0 y por consiguiente se aceptaron las hipótesis alternativas H_1 en los cuatro indicadores.

Rodriguez (2020) en su trabajo tuvo como objetivo estudiar la influencia de la gestión de la norma ISO 27001 en la SI de una empresa privada en Lima (Perú). Aplicando una metodología cuantitativa y realizando un estudio pre-experimental (considerando una muestra de 30 trabajadores de la empresa) la conclusión demuestra que existe una influencia de la gestión de ISO en la SI y las dimensiones de confidencialidad, integridad y disponibilidad.

Con la implementación de la norma ISO 27001 se habla de que las empresas se encuentran a la mitad del camino de la aplicación del Reglamento General de Protección de Datos (RGPD, que es un marco a nivel europeo), así lo establece Lopes (2019) en su trabajo, debido a que si bien poseen similitudes, por ejemplo el RGPD solo ocasionalmente sugiere prácticas específicas, la norma establece con claridad lo que las organizaciones necesitan hacer para estar seguros.

Esto suma a las ventajas de la implementación de la norma, debido a que se cumple o se tiene una guía (hoja de ruta) para el cumplimiento de demás estándares internacionales.

Stoica & Candoi-Savu (2020) en su trabajo tuvieron como objetivo crear un enfoque matemático que pueda cuantificar la necesidad de implementar la norma ISO 27001 en una empresa, y definir cuáles son los beneficios reales de hacerlo, con el respaldo del enfoque matemático la implementación de la norma se hace necesaria, permitiendo así disminuir la tasa de componentes vulnerables (indicador 2).

De igual manera las vulnerabilidades en estos últimos (indicador 3), establecen también que las operaciones mientras se evalúan los procesos sean revisadas con sumo cuidado y dependiendo de la complejidad de los mismos se debe ampliar o reducir, esto contribuye a los tiempos de detección de vulnerabilidades en los componentes (indicador 4), posteriormente habiendo identificado la combinación adecuada de factores o controles, se disminuye el tiempo de implementación de prácticas de seguridad (indicador 1).

Martin & Victorino (2018) en su trabajo realizaron un análisis y un diagnóstico del sistema de SI utilizando un modelo planteado, esto arroja un conjunto de fortalezas y debilidades, esto sirvió como punto de referencia para la certificación en la norma ISO 27001, posterior a ello realizaron una auditoría para revisar de forma detallada la política de seguridad adoptada, para garantizar que esta cumple con los estándares de la norma.

Fathurohman & Witjaksono (2020) emplean un enfoque más específico en su trabajo para el análisis y diseño de un SGSI basado en la norma, se centran en los controles de anexo: gestión de activos, control de acceso, criptografía, salvaguardias físicas y ambientales, seguridad de operación, seguridad de comunicación, adquisición, desarrollo y mantenimiento de sistemas, cada una de estas proveen pautas para el control específico de las áreas seleccionadas de la entidad donde se va a implementar, con esto elaboraron políticas de seguridad que permitieron mejorar el rendimiento de los sistemas, agilizar el soporte y el logro de estrategias comerciales de la institución.

En base a los indicadores tasa de componentes vulnerables y tasa de vulnerabilidades por componentes, el autor (Abazi, 2020) presentó un enfoque, modelo y solución para la evaluación de los riesgos asociados a la SI en el sector

bancario, compañías de seguro y compañías IT, mediante este enfoque exploró las brechas que poseen las grandes organizaciones en su intento de implementar seguridad, para controlar esto propone los siguientes controles:

- Evaluaciones periódicas de los riesgos asociados a los datos.
- Actualizar software de seguridad.
- Mantener una política de encriptación interna.
- Cifrar datos y mantenerlos resguardados en caso de ataque.
- Preparar y capacitar al personal en materia de seguridad de los datos.
- Asegurar que los partners posean estándares de protección de datos.
- Implementar outsourcing para auditoría y evaluaciones de seguridad.

Estos controles coinciden en parte con los establecidos en las políticas desarrolladas en esta investigación.

Akinyemi (et al., 2020) en su trabajo utilizó una combinación de métodos cualitativos para realizar un análisis FODA(Ballesteros et al., 2015) del SGSI, los hallazgos del FODA posteriormente se validaron mediante un instrumento de encuesta, para finalmente analizar y validar los resultados mediante métodos estadísticos, este tipo de enfoques permite conocer de manera cualitativa la percepción del SGSI implementado, es importante mantener y mejorar las fortalezas encontradas, así como también cumplir o alcanzar las oportunidades, en cuanto a las debilidades y amenazas es imperante mitigarlas o abordarlas mediante la norma investigada en este trabajo, teniendo en cuenta que a pesar de que la institución posee un SGSI si no se realizó un correcto análisis inicial, o si no se definió el alcance correctamente se puede llegar a implementar un SGSI débil o ineficiente, que posteriormente incurrirá en brechas de seguridad.

(Ayu & Syamsuar, 2020) en su trabajo realizaron un estudio basado en la norma ISO 27001 para medir y evaluar los riesgos asociados a la SI, similar a mi propuesta, estos autores también utilizaron el método de observación para la recolección de los datos (ellos añadieron entrevistas).

Básicamente la investigación se dividió en tres etapas: identificación de activos, identificación de amenazas y vulnerabilidades de seguridad, evaluación del riesgo

de CIA (confidencialidad, integridad, disponibilidad), encontraron que se debe mejorar principalmente en aspectos como la divulgación y propagación de información, así como también la propagación e implementación de malware, todo esto con el fin de mejorar la seguridad de los activos de la universidad del desarrollo humano.

En el trabajo de investigación de (Singgrit & Pamuji, 2020) se realizó un análisis para conocer o determinar el nivel de seguridad de un SGSI implementado en el gobierno de Karawang, utilizando el cuestionario PDCA dirigido principalmente a dos tipos de encuestados (usuarios y líderes), los resultados indicaron que los usuarios confían en un 52 % en el nivel de seguridad de la información, mientras que los líderes confían solo en un 48 %.

Esto se encuentra por debajo de lo requerido por la norma ISO (64 %), por lo que proponen un marco SGSI basado en la norma ISO 27001 que permita gestionar el aspecto secreto, la integridad y la SI.

(Yupanqui et al., 2017) propuso un diseño de política de seguridad TI en base a la metodología Magerit, que consiste básicamente en identificar activos, clasificarlos, identificar parámetros, clasificar amenazas, evaluación de impacto cualitativa, identificación de controles y diseño de propuestas de políticas, esta se elaboró con un propósito de aplicabilidad y lineamientos básicos, que especifican reglas sobre cómo utilizar adecuadamente un activo para protegerlo de amenazas potenciales a las que se encuentra expuesto.

Este aspecto es coincidente con el presente trabajo de investigación, ya que, si bien los indicadores se usan para medir la propuesta de la norma, las políticas que se desarrollaron y el cumplimiento de las mismas es lo que permitirá alcanzas los objetivos propuestos.

En la investigación que tiene por objetivo medir la brecha entra la situación actual de una petrolera y la protección de la SI según las disposiciones de la norma, realizada por (Mohammed & Jasim, 2022) se adoptó el enfoque de estudio del caso y se utilizó una lista de verificación, con los métodos de análisis estadísticos (media aritmética, porcentaje de solicitud de documentación) se evidenció un desfase en la realidad situacional de la empresa y la documentación real, la cual

se encontraba en un 36 %, por ello los autores realizan un plan de documentación, para alcanzar la meta que establece la norma (64 %) y para posteriormente poder realizar la implementación de la norma mediante un SGSI.

J. A. R. Rodríguez (2019) en su trabajo implementó un SGSI basado en la norma ISO 27001 para un operador de información PILA, que básicamente se encarga de movimientos financieros de la empresa, se elaboró un análisis la organización en base al cumplimiento normativo, donde se puede evidenciar las desviaciones que más tarde servirán para el análisis de adecuación de los diferentes controles. Con el análisis situacional de la empresa, el autor elaboró un plan director para la implementación del SGSI el cuál mejoró notablemente el nivel existente en cuanto a seguridad. Teniendo un análisis real de la empresa, se puede trabajar también en un plan de mejora continua, o uno de continuidad de negocio.

En similitud al presente trabajo de investigación se elaboraron documentos o procedimientos establecidos en la norma: Política de seguridad, Procedimiento de auditorías internas, Gestión de indicadores, Procedimiento de revisión de la dirección, Gestión de roles y responsabilidades, Metodología de análisis de riesgos, Declaración de aplicabilidad (J. A. R. Rodríguez, 2019).

El trabajo de investigación de (Kobayashi et al., 2019) propone en su estudio un método de descripción de casos de aseguramiento basado en el SGSI ISO 27001, para definir políticas de SI a través de la creación conjunta de valores entre una empresa matriz y su subsidiaria, esta política varía entre sus empresas, por ello deben acordar fusionar las políticas, aquello resultará en:

1. Aclarar el rango de acuerdo y desacuerdo entre las políticas de seguridad de la información de dos empresas.
2. Evidenciar como dos empresas concluyen mutuamente un acuerdo final para toda la gama, mediante el uso del caso de garantía creado.

Para evaluar los marcos y estándares de gobierno empresarial (EGIT) para TI, como COBIT 5 e ISO 27001, cada marco y estándar define su propio alcance, definiciones y terminología, por lo que al adoptarlos se requiere mucho esfuerzo. El uso de estos marcos y estándares por sí solo limita su aplicabilidad a dominios

específicos de tecnología de la información (TI), lo que impide que las organizaciones se den cuenta de los beneficios de EGIT. Además, debido a que estos marcos y estándares se superponen, es intuitivo que diferentes departamentos desperdicien recursos manejando ambos enfoques por separado cuando una organización está tratando de ser eficiente y efectiva(Almeida et al., 2018).

Por ello (Almeida et al., 2018) propone facilitar la evaluación simultánea de COBIT 5 e ISO 27001. Esto se logró mediante una representación de metamodelo de arquitectura empresarial (EA) de ISO 27001 y un mapeo a COBIT 5 utilizando el lenguaje de modelado ArchiMate EA. El metamodelo ISO 27001 también se amplió con la especificación técnica ISO/IEC (TS) 33052 e ISO/IEC TS 33072. Debido a que estos estándares proponen un modelo de referencia de procesos y un modelo de evaluación de procesos para la gestión de la seguridad de la información. A través del proceso mapeado a ISO/IEC TS 33052, se realizó un estudio de campo sobre la gestión de solicitudes de servicio e incidentes para el proceso COBIT 5 y la gestión correspondiente para ISO 27001.

El autor (Fajar et al., 2018) implementó el estándar ISO 27001:2013., esto a su vez afecta la continuidad del negocio. Al aplicar la norma, las organizaciones necesitan saber qué tan bien se están aplicando sus procesos y qué pasos se pueden tomar para mejorar su desempeño. Por ello primero se realizó un análisis factorial para identificar los factores que afectan la SI, luego se realizaron observaciones y entrevistas para recopilar datos sobre los PT.

Luego se desarrollaron recomendaciones y acciones correctivas utilizando el método de análisis de brechas. Los factores que tuvieron mayor impacto en la SI del cliente fueron los elementos de control de acceso y operaciones de seguridad. Como resultado de la revisión del control de acceso IS027001:2013, se encontró que 11 de los 33 ítems de verificación correspondían a NC (no conformidad), 9 ítems a la categoría mayor y los 2 ítems restantes a la categoría menor. Por otro lado, para los aspectos de seguridad operacional de los 12 elementos operativos, 5 cayeron en la categoría NC (no conforme) y todos cayeron en la categoría menor(Fajar et al., 2018).

VI. CONCLUSIONES

Con la implementación de la norma ISO 27001 se pueden definir las siguientes conclusiones para cada uno de los indicadores:

1. El tiempo promedio de implementación de prácticas de seguridad en los componentes de la infraestructura TI se redujo en un 5,65 % con respecto al pretest, esto permitirá tener un equipo seguro en menor tiempo.
2. La tasa de componentes vulnerables de la infraestructura TI se redujo en un 13,55 % con respecto al pretest, esto permitirá tener una infraestructura menos vulnerable y reducir los ataques.
3. La tasa de vulnerabilidades en los componentes de la infraestructura TI se redujo en un 9,75 % con respecto al pretest, esto ayuda a mantener seguros los equipos y mitigar los riesgos de ataques.
4. El tiempo promedio de detección de vulnerabilidades de los componentes de infraestructura TI se redujo en un 11,97 % con respecto al pretest, permitiendo así un accionar más rápido frente a un ataque.
5. La aplicación de la Norma ISO 27001:2013 en la empresa Guru-IT tuvo resultados satisfactorios, aportando así mayor seguridad a su infraestructura, permitiendo mantener seguros sus activos y ayudando a mitigar los posibles ataques que se susciten en un futuro.

VII. RECOMENDACIONES

1. Se recomienda al gerente de sistemas de la empresa Guru-IT aplicar las políticas de SI definidas en base a la norma ISO 27001 para detectar las amenazas, corregir o mitigar las vulnerabilidades detectadas.
2. También se recomienda a los gerentes, jefes o personas con cargos de similar índole de las empresas (especialmente a las del ámbito informático) a implementar un SGSI basado en la norma ISO 27001 para garantizar la seguridad de sus procesos, y también la confidencialidad, disponibilidad e integridad de sus datos.
3. A la comunidad universitaria y científica se invita al desarrollo de investigaciones orientadas a la seguridad de la información, con la utilización de la norma ISO 27001 como guía y marco metodológico de los procesos de seguridad de la información.

REFERENCIAS

Abazi, B. (2020). *A novel approach for information security risk assessment maturity framework based on ISO 27001* [PhD, Corvinus University of Budapest]. https://doi.org/10.14267/phd.2020016

Agudelo, G. (s. f.). *DISEÑOS DE INVESTIGACIÓN EXPERIMENTAL Y NO-EXPERIMENTAL*. 46.

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

Alexander, W., & Jimenez, O. (2021). *Elaboración del plan director de implementación del SGSI basado en la ISO/IEC27001 para una empresa de Servicios y Soluciones Informáticas*.

Almeida, R., Lourinho, R., Silva, M. M. da, & Pereira, R. (2018). A Model for Assessing COBIT 5 and ISO 27001 Simultaneously. *2018 IEEE 20th Conference on Business Informatics (CBI)*, *01*, 60-69.

Altamirano-de-la-Borda, K. J. (2021). *La seguridad de la información en la administración pública*. 77-95. https://doi.org/10.26439/ciis2020.5480

Andrzejewski, K. (2020). Security information management systems. *Management Sciences*, *24*(4), 1-9. https://doi.org/10.15611/ms.2019.4.01

Ayu, R., & Syamsuar, D. (2020). *RISK ANALYSIS OF INSAN UNIVERSITY SYSTEM USING ISO 27001.pdf*.

Baca, V. (2016). Diseño de un sistema de gestión de seguridad de información para la unidad de gestión gducativa local—Chiclayo. *Ingeniería: Ciencia, Tecnología e Innovación*, *3*(1), 16.

Ballesteros, H., Verde, J. D. C., Costabel, M., Sangiovanni, R., Dutra, I. de C., Rundie, D., Cavaleri, F., & Bazán, L. (2015). *Análisis FODA: Fortalezas, Oportunidades, Debilidades y Amenazas.*

Boban, M., & Cosic, Z. (2008). *Methodology of Risk Analysis as the most Important Aspect of Information Security in Digital Economy*.

BRIONES, K. P. F., & BALÓN, O. A. C. (2016). *ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL Facultad de Ingeniería en Electricidad y Computación MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA*. 2.

Calder, A., (Firm), P., (Firm), S. B. O., & Books24x7, I. (2010). *Selling information security to the board: A primer*.

Coello Yagual, R. R., & Pico Versoza, L. M. (2018). Análisis de las ventajas y desventajas del sistema de gestión dela seguridad de la información y su influencia en la competitividad de las empresas que utilizan Cloud Computing y Big Data en el Ecuador. *INNOVA Research Journal*, 181-195. https://doi.org/10.33890/innova.v3.n4.2018.562

Eskaluspita, A. Y. (2020). ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University. *IOP Conference Series: Materials Science and Engineering*, *879*(1), 012074. https://doi.org/10.1088/1757-899X/879/1/012074

Fajar, A. N., Christian, H., & Girsang, A. S. (2018). Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet. *Journal of Physics*, 10.

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

Computer Science and Electrical Engineering, *1*(1), 1-11. https://doi.org/10.25008/bcsee.v1i1.2

García, J. (2007). Seguridad en redes corporativas. *Interfaces*, 17-34.

Ghasemi, A., & Zahediasl, S. (2012). Normality Tests for Statistical Analysis: A Guide for Non-Statisticians. *International Journal of Endocrinology and Metabolism*, *10*(2), 486-489. https://doi.org/10.5812/ijem.3505

Haftom Gebreziagbher. (2018, diciembre 31). *Information System Security Framework and Vulnerability Assessment for Ethiopian Higher Educational Institution using ISO/IEC 27001*. 12-18.

ISO. (2013). *ISO/IEC 27001:2013*. https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-2:v1:en

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

Kobayashi, N., Nakamoto, A., Kawase, M., Ioki, M., & Shirasaka, S. (2019). A Proposal of Information Security Policy Agreement Method for Merger and Acquisition Using Assurance Case and ISO 27001. *2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*, 727-733.

Ladino A., M. I., Villa S., P. A., & Lopez E., A. M. (2011). *Fundamentos ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS.pdf*. *XVII*(47), 334-339.

Lin, I.-L., Lin, C.-M., & Sun, C. (2018). A Study on the Integration of ISO 27001 & 27011 and the New Personal Information Protection Act in the Telecom Enterprises in Taiwan. *2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications*, 393-398.

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. *Journal of Information Systems Engineering & Management*, *4*(2). https://doi.org/10.29333/jisem/5888

Lopes, R. H. C. (2011). Kolmogorov-Smirnov Test. *International Encyclopedia of Statistical Science*.

Lopez, C., Sandoval, D., & Herrera, E. (2022). *Importancia de la información Financiera como soporte en la planeación estratégica de las PYMES*. https://repository.usta.edu.co/bitstream/handle/11634/44422/2022SandovalDiego.pdf?sequence=1&isAllowed=y

Mantra, I., Abd. Rahman, A., & Saragih, H. (2020). Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education. *International Journal of Engineering & Technology*, *9*(2), 429. https://doi.org/10.14419/ijet.v9i2.30581

Martin, W. G. M., & Victorino, L. P. S. (2018). *MODELO GUÍA PARA LA CERTIFICACIÓN EN ISO 27001 DE LAS ENTIDADES, QUE HAN IMPLEMENTADO LAS NORMAS ESTABLECIDAS POR LA ESTRATEGIA DE GOBIERNO EN LÍNEA.* 225.

Mishra, P., Singh, U., Pandey, C., Mishra, P., & Pandey, G. (2019). Application of student's t-test, analysis of variance, and covariance. *Annals of Cardiac Anaesthesia*, *22*(4), 407. https://doi.org/10.4103/aca.ACA_94_19

Mohammed, T. J., & Jasim, N. A. (2022). Designing a model to protect documented information according to the integration of some international standards (ISO 27001: 2013) (ISO 10013: 2021): A case study. *International Journal of Health Sciences*, 10684-10697. https://doi.org/10.53730/ijhs.v6nS3.8376

Moses, L. E. (2014). *Wilcoxon-Mann-Whitney Test: Definition and Example*.

Nieto, N. T. E. (s. f.). *TIPOS DE INVESTIGACIÓN*. 4.

Niño Morante, N. R. (2018). *MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN SGSI.pdf*. https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/5935/BC-TES-TMP-788%20NI%c3%91O%20MORANTE.pdf?sequence=1&isAllowed=y

Ojeda, P. C. (s. f.). *Universo, población y muestra*. 15.

Orjuela, L. A. M., & Cárdenas, Y. E. S. (s. f.). *PLAN DE IMPLEMENTACIÓN DEL SGSI BASADO EN LA NORMA ISO 27001:2013 PARA LA EMPRESA INTERFACES Y SOLUCIONES*. 94.

Pallant, J. F. (2020). *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using IBM SPSS*.

Pérez, O. F., & Sáenz, N. E. M. (2017). *Propuesta de Políticas de Seguridad de la Información para la institución Educativa de Educación Básica y Media del departamento de Boyacá, basadas en la norma ISO 27001:2013.*

Razali, N. M., & Wah, Y. B. (s. f.). *Power comparisons of Shapiro-Wilk, Kolmogorov-Smirnov, Lilliefors and Anderson-Darling tests*. 13.

Rivera-Guerrero, C. B., Felipe-Redondo, A. M., & Nuñez-Cárdenas, F. J. (2019). Esquema de ISO 27001 Sistema de Gestión de la Seguridad de la Información. *Ciencia Huasteca Boletín Científico de la Escuela Superior de Huejutla*, *7*(13), 28-29. https://doi.org/10.29057/esh.v7i13.3537

Rodriguez Baca, L. S., Cruzado Puente de la Vega, C. F., Mejía Corredor, C., Universidad EAN, Alarcón Diaz, M. A., & Universidad César Vallejo. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información

de una empresa privada peruana. *Propósitos y Representaciones*, *8*(3). https://doi.org/10.20511/pyr2020.v8nSPE3.786

Rodríguez, G. P. (2017). *PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN UNA ENTIDAD DEL SECTOR PÚBLICO BASADO EN LA NTC ISO 27001:2013*. 70.

Rodríguez, J. A. R. (2019). *Plan de Implementación de la norma ISO/IEC ISO 27001:2013 para un Operador de Información PILA*. 69.

Rodriguez, P. A. G., & Muñoz, J. C. P. (s. f.). *GUÍA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA ENTIDADES DE CONTACT CENTER*. 82.

Rojas, D. S. B., & Romero, E. L. A. (2018). *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) APLICADA AL ÁREA DE OPERACIONES DE UNA EMPRESA DE TELECOMUNICACIONES.* 89.

Secaira, J. I. M., Ocampo, R. D., Mera, E. Z., & Kovalenko, E. D. (2020). *El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). (Original)*.

Singgrit, P., & Pamuji, G. C. (2020). *The Use of ISO 27001 Framework for Government's Online E-Monitoring System Implementation*. 8.

Solá, Á. P. S. (s. f.). *DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS Y COMPUTACIÓN*. 164.

Stoica, L. A., & Candoi-Savu, R. A. (2020). Math approach of implementing ISO 27001. *Proceedings of the International Conference on Business Excellence*, *14*(1), 521-530. https://doi.org/10.2478/picbe-2020-0049

Technical University of Moldova, & Alexei, A. (2021). ENSURING INFORMATION SECURITY IN PUBLIC ORGANIZATIONS IN THE REPUBLIC OF

MOLDOVA THROUGH THE ISO 27001 STANDARD. *Journal of Social Sciences*, *IV(1)*. https://doi.org/10.52326/jss.utm.2021.4(1).11

Valenzuela, T., Maribel, K., Egas, R., & Bernabe, M. (s. f.). *TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN GERENCIA DE SISTEMAS*. 65.

Yucra Quispe, T., & Bernedo Villalta, L. Z. (2020). Epistemología e Investigación Cuantitativa. *IGOBERNANZA*, *3*(12), 107-120. https://doi.org/10.47865/igob.vol3.2020.88

Yupanqui, J. R. A., Oré, S. B., & Unidad de Posgrado de la Facultad de Sistemas e Informática, Universidad Nacional Mayor de San Marcos (UNMSM), Av. Germán Amézaga s/n, Lima, Perú. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *25*, 112-134. https://doi.org/10.17013/risti.25.112-134

ANEXOS

Anexos: Instrumentos de recolección de datos

1. Guía de observación N°1: Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI.

Guía de observación de medición del indicador de Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI				
Investigador:		Jamil Javier Cerezo Zambrano		
Proceso observado:		Implementación de prácticas de seguridad		
Pre-Test				
N° de Obs.	Fecha	Tiempo total para implementación de prácticas de seguridad	Número de prácticas implementadas	Tiempo promedio para implementación de prácticas de seguridad = (Tiempo total para implementación de prácticas de seguridad / Tiempo total para implementación de prácticas de seguridad)
1				
2				
3				
4				
5				
6				
N				

2. Guía de observación N°2: Cantidad promedia de componentes vulnerables de la infraestructura TI.

Guía de observación de medición del indicador de Cantidad promedia de componentes vulnerables de la infraestructura TI				
Investigador:		Jamil Javier Cerezo Zambrano		
Proceso observado:		Detección de componentes vulnerables		
Pre-Test				
N° de Obs.	Fecha	Cantidad total de componentes vulnerables	Número de componentes	Cantidad promedia de componentes vulnerables = (Cantidad total de componentes vulnerables - Número de componentes) / (Cantidad total de componentes vulnerables)
1				
2				
3				
4				
5				
6				
N				

3. Guía de observación N°3: Cantidad promedia de vulnerabilidades detectadas en los componentes de la infraestructura TI.

Guía de observación de medición del indicador de Cantidad promedia de vulnerabilidades detectadas en los componentes de la infraestructura TI				
Investigador:		Jamil Javier Cerezo Zambrano		
Proceso observado:		Detección de vulnerabilidades por componentes		
Pre-Test				
N° de Obs.	Fecha	Cantidad total de vulnerabilidades en los componentes	Número de componentes vulnerables	Cantidad promedia de componentes vulnerables = (Cantidad total de vulnerabilidades en los componentes - Número de componentes vulnerables) / (Cantidad total de vulnerabilidades en los componentes)
1				
2				
3				
4				
5				
6				
N				

4. Guía de observación N°4: Tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI de la organización

Guía de observación de medición del indicador de Tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI de la organización				
Investigador:		Jamil Javier Cerezo Zambrano		
Proceso observado:		Detección de vulnerabilidades por componentes		
Pre-Test				
N° de Obs.	Fecha	Tiempo total para identificar vulnerabilidades en los componentes	Número de vulnerabilidades encontradas	Tiempo promedio para implementación de prácticas de seguridad = (Tiempo total para identificar vulnerabilidades en los componentes - Número de vulnerabilidades encontradas) / (Tiempo total para identificar vulnerabilidades en los componentes)
1				
2				
3				
4				
5				
6				
N				

TABLA DE OPERACIONALIZACIÓN DE VARIABLES

Tabla 14 TABLA DE OPERACIONALIZACIÓN DE VARIABLES

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ESCALA DE MEDICIÓN
INDEPENDIENTE: Norma ISO 27001	ISO 27001 se define que esta forma parte de un conjunto de estándares internacionales sobre la SI (familia ISO 27000), estas contienen una colección de buenas prácticas que se utilizan para establecer, implementar, mantener y mejorar el SGSI, esta norma es certificable, significa que si una empresa solicita una auditoría a una entidad certificadora acreditada y la supera, obtiene la certificación.	La definición operacional de la norma ISO 27001 consiste en seguir las buenas prácticas y lineamientos establecidos en la misma para reducir los incidentes ligados a la SI, debido a que la norma es certificable posterior a una auditoría, las organizaciones se ven obligadas a contar con un SGSI que debe estar implementado con al menos tres meses de anticipación a la auditoría, la misma que conta de tres fases, pre-auditoría (obtiene información sobre la situación de la organización) y la primera y segunda fase que consisten en examinar la documentación y denotar cualquier falencia de la norma.	- Estándar - Certificación - Planificación - Mejora		De razón.

DEPENDIENTE: Gestión de la seguridad de la información	se entiende por esta a la combinación de sistemas y procedimientos que garantizan la confidencialidad, integridad y disponibilidad de la información, teniendo como fin la protección de la misma, y de los sistemas de la información de acceso, así como su uso, divulgación, interrupción o destrucción no autorizada	La definición operacional de la SI consiste en tres grandes áreas, gestión de riesgos (identifica y prioriza los peligros ligados al desarrollo de un producto, sistema u organización), proceso de ingeniería de seguridad (establece e implementa soluciones a los problemas suscitados debido a las amenazas) y proceso de aseguramiento (nivel de confianza que conforman los requisitos de seguridad)	- Disponibilidad - Integridad - Confidencialidad	1.Tasa de vulnerabilidades detectadas en los componentes de la infraestructura TI. 2.Tiempo promedio de detección de vulnerabilidades en los componentes de la infraestructura TI de la organización. 3.Tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura TI. 4.Tasa de componentes vulnerables de la infraestructura TI.	De razón.

Fuente: Elaboración propia

MATRIZ DE CONSISTENCIA

Tabla 15 MATRIZ DE CONSISTENCIA

MATRIZ DE CONSISTENCIA **TÍTULO DE LA TESIS:** Aplicación de la norma ISO 27001 para la gestión de la seguridad de la información en la empresa Plataforma Buscador Académico BUSAC. S.A. en Ecuador					
FORMULACIÓN DEL PROBLEMA	**OBJETIVOS**	**HIPÓTESIS**	**VARIABLES Y DIMENSIONES**	**METODOLOGÍA**	**JUSTIFICACIÓN**
GENERAL: ¿De qué manera se puede mejorar la SI en la empresa Guru-IT, Ecuador en el año 2022?	**GENERAL:** Mejorar la gestión de la SI en la empresa Guru-IT mediante la implementación de la norma ISO 27001	**GENERAL:** La implementación de la norma ISO 27001 permitirá mejorar la SI en Guru-IT en Ecuador 2022	**INDEPENDIENTE:** Norma ISO 27001 **Dimensiones:** - Estándar - Certificación - Planificación - Mejora	**Tipo y Diseño de Investigación:** **Tipo de investigación:** Experimental **Diseño de Investigación:** Preexperimental **Población:** La población total de componentes en la infraestructura IT de la organización son de 50 **Muestra:** Se determina la muestra mediante una fórmula de tipo	**Operativa:** De forma operativa se justifica ya que al reducir los equipos vulnerables y controlar sus vulnerabilidades o el tiempo de respuesta a las mismas, se reduce el tiempo en que los equipos se encuentren detenidos, o que estos no funcionen en condiciones óptimas **Tecnológica:** La justificación viene dada ya que al implementar un SGSI con base en la norma ISO 27001 se

				aleatorio simple, se toma en cuenta un nivel de confianza del 95% y un margen de error del 5%. El resultado es una muestra de: 45 componentes. **Muestreo:** No se aplica muestreo debido a que se toma la población total como la muestra de la investigación	automatiza el proceso de gestionar la seguridad de los componentes de infraestructura, aprovechando así al máximo los recursos tecnológicos **Económica:** En cuanto a la justificación económica, se espera mantener operativos los componentes de infraestructura, y evitar pérdidas económicas por fallos en la seguridad de los mismos que afecten a los procesos operativos de la empresa. **Social:** En el ámbito social, un SGSI con base en la norma ISO 27001 permitirá mantener a salvo y resguardada la información sensible de la
ESPECÍFICOS: – ¿De qué manera influirá aplicar la norma ISO 27001 en el tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura IT de la organización? – ¿De qué manera influirá aplicar la norma ISO 27001 en la cantidad de	**ESPECÍFICOS:** – Reducir el tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura IT de la organización. – Reducir la cantidad de componentes vulnerables de la infraestructura IT de la organización. – Reducir la cantidad de vulnerabilidades	**ESPECÍFICAS:** – La implementación de la norma ISO 27001 permitirá reducir el tiempo promedio de implementación de prácticas de seguridad en los componentes de infraestructura IT de la organización.	**DEPENDIENTE:** Gestión de la seguridad de la información **Dimensiones:** - Disponibilidad - Integridad - Confidencialidad	**Técnicas e Instrumentos de recolección de Datos:** Guías de observación	

componentes vulnerables de la infraestructura IT de la organización? – ¿De qué manera influirá aplicar la norma ISO 27001 en la cantidad de vulnerabilidades detectadas en los componentes de la infraestructura IT de la organización? – ¿De qué manera influirá la aplicación de la norma ISO 27001 en el tiempo de detección de vulnerabilidades en los componentes de la infraestructura IT de la organización?	detectadas en los componentes de la infraestructura IT de la organización. – Reducir el tiempo de detección de vulnerabilidades en los componentes de la infraestructura IT de la organización.	– La implementación de la norma ISO 27001 permitirá reducir la cantidad de componentes vulnerables en la infraestructura IT de la organización. - La implementación de la norma ISO 27001 permitirá reducir la cantidad de vulnerabilidades detectadas en los componentes de la infraestructura IT de la organización. – La aplicación de la norma ISO 27001 permitirá reducir el tiempo promedio de detección de vulnerabilidades en los componentes de infraestructura IT de la organización.			empresa, de igual manera la información de los clientes, garantizando así la privacidad de los datos.

Fuente: Elaboración propia

Carta de solicitud de aceptación de elaboración de tesis

"AÑO DEL FORTALECIMIENTO DE LA SOBERANÍA NACIONAL"

Trujillo, 02 de junio de 2022

CARTA N.° 093-2022-UCV-VA-EPG-F01/J
Sr. José Luis Zambrano Pinto
Representante Legal
PLATAFORMA BUSCADOR ACADÉMICO BUSAC. S.A.
Presente. -

ASUNTO: AUTORIZACIÓN PARA EL DESARROLLO DE TESIS

Es grato dirigirme a usted para saludarle cordialmente y así mismo presentar al estudiante **JAMIL JAVIER CEREZO ZAMBRANO,** del programa de **MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN,** de la Escuela de Posgrado de la Universidad César Vallejo.

El estudiante en mención solicita autorización para aplicar los instrumentos necesarios para el desarrollo de su tesis denominada: **"APLICACIÓN DE LA NORMA ISO 27001 PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA PLATAFORMA BUSCADOR ACADÉMICO BUSAC. S.A. EN ECUADOR, 2022",** en la institución que Ud. Dirige.

El objetivo principal de este trabajo de investigación es gestionar la seguridad de la información en la empresa "Plataforma Buscador Académico BUSAC. S.A." mediante la implementación de la norma ISO 27001.

Agradeciendo la atención que brinde a la presente, aprovecho la oportunidad para expresarle mi consideración y respeto.

Atentamente. –

Mg. Ricardo Benites Allaga
Jefe de la Escuela de Posgrado-Trujillo
Universidad César Vallejo

ADJUNTO:
- Instrumentos de recolección de datos.

Carta de aceptación de elaboración de tesis

GuruIT

03/06/2022

Ing. Jamil Cerezo Zambrano

Presente

En atención de su solicitud de autorización para el desarrollo de su Tesis denominada **"APLICACIÓN DE LA NORMA ISO 27001 PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA PLATAFORMA BUSCADOR ACADÉMICO BUSAC. S.A. EN ECUADOR, 2022",** y de la aplicación de instrumentos para recolectar datos. Como representante legal de la empresa PLATAFORMA BUSCADOR ACADÉMICO BUSAC. S.A., se aprueba su requerimiento por el tiempo que estime necesario.

Atentamente.

JOSE ZAMBRANO

Jose Luis Zambrano Pinto
Representante Legal de
PLATAFORMA BUSCADOR ACADÉMICO BUSAC. S.A.

TRANSFORMACIÓN Digital

Carta de aceptación de resultados de tesis

GuruIT

21/07/2022

Ing. Jamil Cerezo Zambrano

Presente

Mediante el presente documento se comunica que se aceptan los resultados que surgieron del desarrollo de su tesis de maestría denominada **"APLICACIÓN DE LA NORMA ISO 27001 PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA PLATAFORMA BUSCADOR ACADÉMICO BUSAC. S.A. EN ECUADOR, 2022"**, la ejecución de la misma fue de mucho valor para la empresa.

Atentamente.

JOSE ZAMBRANO

Jose Luis Zambrano Pinto
Representante Legal de
PLATAFORMA BUSCADOR ACADÉMICO BUSAC. S.A.

TRANSFORMACIÓN Digital

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO – EXPERTO 1

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO

VARIABLE: MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA IMPLEMENTACIÓN DE LA NORMA ISO 27001 EN LA EMPRESA Plataforma Buscador Académico BUSAC. S.A., 2022

N°	INDICADORES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	INDICADOR 1: TIEMPO PROMEDIO DE IMPLEMENTACIÓN DE PRÁCTICAS DE SEGURIDAD EN LOS COMPONENTES DE INFRAESTRUCTURA TI Fórmula: Tiempo total para implementación de prácticas de seguridad / Número de prácticas implementadas	X		X		X		
2	INDICADOR 2: TASA COMPONENTES VULNERABLES Fórmula: (Número de componentes-Cantidad total de componentes vulnerables)/Cantidad total de componentes vulnerables	X		X		X		
3	INDICADOR 3: TASA DE VULNERABILIDADES EN LOS COMPONENTES Fórmula: (Cantidad total de vulnerabilidades en los componentes - Número de componentes vulnerables) / Cantidad total de vulnerabilidades en los componentes	X		X		X		
4	INDICADOR 4: TIEMPO PROMEDIO PARA IMPLEMENTACIÓN DE PRÁCTICAS DE SEGURIDAD Fórmula: Tiempo total para identificar vulnerabilidades en los componentes / Tiempo total para identificar vulnerabilidades en los componentes	X		X		X		

Observaciones (precisar si hay suficiencia): SUFICIENTE

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

Apellidos y nombres del juez evaluador: Msc. Ortega Acosta Juan Carlos C.C: 1204758757

21/07/2022

Especialista: Metodólogo [X] Temático [ ]

Grado: Maestro [ ] Doctor [X]

[1]**Claridad:** Se entiende con dificultad algún enunciado del ítem, es conciso, exacto y directo.
[2]**Pertinencia:** Si el ítem pertenece a la dimensión.
[3]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo.

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

firmado electrónicamente por:
JUAN CARLOS
ENRIQUE ORTEGA
ACOSTA

Firma del experto Informante

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO – EXPERTO 2

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO

VARIABLE: MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA IMPLEMENTACIÓN DE LA NORMA ISO 27001 EN LA EMPRESA PLATAFORMA BUSCADOR ACADÉMICO BUSAC. S.A., 2022

N°	INDICADORES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	INDICADOR 1: TIEMPO PROMEDIO DE IMPLEMENTACIÓN DE PRÁCTICAS DE SEGURIDAD EN LOS COMPONENTES DE INFRAESTRUCTURA TI Fórmula: Tiempo total para implementación de prácticas de seguridad / Número de prácticas implementadas	X		X		X		
2	INDICADOR 2: TASA COMPONENTES VULNERABLES Fórmula: (Número de componentes-Cantidad total de componentes vulnerables)/Cantidad total de componentes vulnerables	X		X		X		
3	INDICADOR 3: TASA DE VULNERABILIDADES EN LOS COMPONENTES Fórmula: (Cantidad total de vulnerabilidades en los componentes - Número de componentes vulnerables) / Cantidad total de vulnerabilidades en los componentes	X		X		X		
4	INDICADOR 4: TIEMPO PROMEDIO PARA IMPLEMENTACIÓN DE PRÁCTICAS DE SEGURIDAD Fórmula: Tiempo total para identificar vulnerabilidades en los componentes / Tiempo total para identificar vulnerabilidades en los componentes	X		X		X		

Observaciones (precisar si hay suficiencia): SUFICIENTE

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

Apellidos y nombres del juez evaluador: Msc. Zhuma Mera Emilio Rodrigo C.C: 1715393193

14/07/2022

Especialista: Metodólogo [ ] Temático [X]

Grado: Maestro [X] Doctor [ ]

[1]**Claridad:** Se entiende con dificultad algún enunciado del ítem, es conciso, exacto y directo.
[2]**Pertinencia:** Si el ítem pertenece a la dimensión.
[3]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo.

EMILIO RODRIGO ZHUMA MERA

Firmado digitalmente por EMILIO RODRIGO ZHUMA MERA
Fecha: 2022.07.15 21:56:18 -05'00'

Firma del experto Informante

CERTIFICADO DE VALIDEZ DE CONTENIDO DE INSTRUMENTO – EXPERTO 3

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO

VARIABLE: MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA IMPLEMENTACIÓN DE LA NORMA ISO 27001 EN LA EMPRESA Plataforma Buscador Académico BUSAC. S.A., 2022

N°	INDICADORES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	INDICADOR 1: TIEMPO PROMEDIO DE IMPLEMENTACIÓN DE PRÁCTICAS DE SEGURIDAD EN LOS COMPONENTES DE INFRAESTRUCTURA TI Fórmula: Tiempo total para implementación de prácticas de seguridad / Número de prácticas implementadas	X		X		X		
2	INDICADOR 2: TASA COMPONENTES VULNERABLES Fórmula: (Número de componentes-Cantidad total de componentes vulnerables)/Cantidad total de componentes vulnerables	X		X		X		
3	INDICADOR 3: TASA DE VULNERABILIDADES EN LOS COMPONENTES Fórmula: (Cantidad total de vulnerabilidades en los componentes - Número de componentes vulnerables) / Cantidad total de vulnerabilidades en los componentes	X		X		X		
4	INDICADOR 4: TIEMPO PROMEDIO PARA IMPLEMENTACIÓN DE PRÁCTICAS DE SEGURIDAD Fórmula: Tiempo total para identificar vulnerabilidades en los componentes / Tiempo total para identificar vulnerabilidades en los componentes	X		X		X		

Observaciones (precisar si hay suficiencia): SUFICIENTE

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

Apellidos y nombres del juez evaluador: PhD. OVIEDO BAYAS BYRON WLADIMIR **C.C:** 0914200373

11/07/2022

Especialista: Metodólogo [X] Temático [ ]

Grado: Maestro [ ] Doctor [X]

[1]**Claridad:** Se entiende con dificultad algún enunciado del ítem, es conciso, exacto y directo.
[2]**Pertinencia:** Si el ítem pertenece a la dimensión.
[3]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo.

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

BYRON
WLADIMIR
OVIEDO BAYAS

Firma del experto Informante

Desarrollo de políticas de seguridad basadas en la norma ISO 27001

Política de seguridad de la información

SISTEMAS	POLÍTICA	CÓDIGO: 2.1.1. GA SIS POL
GuruIT TRANSFORMACIÓN Digital	POLITICA DE SEGURIDAD DE INFORMACIÓN	SUSTITUYE A: Ninguna
		VIGENCIA: 22/12/2023
		ACTUALIZACIÓN:
		Página 1 de 2

1. **OBJETIVO**

   Definir los riesgos y controles del área de sistemas a fin de prevenir potenciales pérdidas por errores o usos mal intencionados de equipos o información.

2. **ALCANCE**

   Esta política aplica para todos los colaboradores que tengan asignado o hagan uso de un equipo de computación, programas de computación o licencia. Aplica para cualquier equipo de computación que sea propiedad de Guru-IT o programa que sea contratado por el Guru-IT.

3. **DEFINICIONES**

   - **Equipos de computación:** equipos de computación que son adquiridos por la empresa, aplica para: computadores estacionarios o portátiles, tablets, servidores, celulares, impresoras, scanners, proyectores, equipos de comunicación de datos y UPS.
   - **Programas contratados:** involucra a los programas de computación o licencias, de utilitarios, lenguajes, sistemas operativos, aplicaciones, etc. Incluyendo correo electrónico, mensajería, navegación de internet, acceso a sistemas en línea, etc.
   - **Riesgos de acceso:** Personas no autorizadas pueden tener acceso no autorizado a programas o equipos de computación pudiendo leer, modificar, agregar o eliminar información.

4. **DOCUMENTOS REFERENCIALES**

   - N/A

5. **POLÍTICAS**

   - Política que se debe regir para la contratación de servicios profesionales, para el desarrollo o mantenimiento de programas además para la instalación o mantenimiento de equipos.
   - El acceso a un equipo o programa de computación debe ser autorizado por el nivel gerencial.
   - El acceso será controlado mediante claves de acceso individuales, confidenciales y cambiadas periódicamente.
   - Los usuarios estarán imposibilitados de modificar las propiedades y configuraciones de los equipos y programas que utilizan. No podrán instalar software o programas, en caso de requerir alguno de estos el usuario deberá solicitar al Departamento de Sistemas su instalación.

ELABORÓ	REVISÓ	AUTORIZÓ	AUTORIZÓ
Coordinador de Sistemas	Jefe de Sistemas	Gerente de Sistemas	Gerente General

Política de autorización de acceso aplicaciones de negocio

1. **OBJETIVO:**

   Brindar soporte en la creación o actualización de acceso a las aplicaciones de la empresa Guru-IT

2. **ALCANCE**

   Aplica para el personal de Guru-IT

3. **RESPONSABLES**

   - Gerentes de área
   - Jefe Sistemas
   - Coordinador Desarrollo de Software
   - Coordinador SAP
   - Especialistas de Sistemas
   - Consultor SAP
   - Jefes y Coordinadores

4. **DEFINICIONES**

   N/A

POLÍTICAS GENERALES

a. Nombres de Usuario.

   - Debe estar compuesto de la inicial del primer nombre y el apellido. Ejemplo: IAPELLIDO
   - Debe ser único en toda la organización.
   - Debe vincular visiblemente a una persona.
   - En el caso de nombres repetidos se incluirá la inicial del segundo nombre o apellido. Ejemplo: JPLopez
   - Solo se pueden crear cuentas genéricas para el manejo de procesos automáticos.

b. Clave de Accesos

   - Las claves son únicas e intransferibles.

Política plan de contingencias

SISTEMAS	PROCEDIMIENTO	CODIGO: 2.2.5 GA SIS PRO
GuruIT TRANSFORMACIÓN Digital	PLAN DE CONTINGENCIAS	SUSTITUYE A: Ninguno
		VIGENCIA: 19/05/2022
		ACTUALIZACIÓN: 19/05/2022
		Página 1 de 3

1. **OBJETIVO**

   Mantener la continuidad del negocio manteniendo la operatividad de los servidores y sus recursos para apoyar los procesos de Guru-IT

2. **ALCANCE**

   Este procedimiento aplica para todos los servidores de la empresa Guru-IT

3. **RESPONSABLES**

   - Gerente de Sistemas
   - Jefe de Sistemas
   - Coordinador de Sistemas
   - Coordinador de Desarrollos & Software
   - Especialistas de Sistemas
   - Asistente de Sistemas

4. **DEFINICIONES**

   - Equipos de Computación: computadores estacionarios o portátiles, servidores, impresoras, scanner, proyectores, equipos de comunicación de datos, UPS, etc.
   - Programas de Computación: programas utilitarios, licencias, lenguajes de programación, sistemas operativos, aplicaciones, etc.
   - Servicios Profesionales: servicios para el desarrollo o mantenimiento de programas o para la instalación o mantenimiento de equipos.
   - **ANÁLISIS DE RIESGO**

Riesgo	Tipo de probabilidad
Incendio	Alta
Inundación	Media en centro de cómputo
Terremoto	Media
Ataque externo	Baja
Erupción volcánica	Baja
Tormenta eléctrica	Media

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, PACHECO TORRES JUAN FRANCISCO, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - TRUJILLO, asesor de Tesis Completa titulada: "Aplicación de la norma ISO 27001 para la gestión de la seguridad de la información en la empresa Plataforma Buscador Académico BUSAC. S.A. en Ecuador", cuyo autor es CEREZO ZAMBRANO JAMIL JAVIER, constato que la investigación cumple con el índice de similitud establecido, y verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

TRUJILLO, 13 de Agosto del 2022

Apellidos y Nombres del Asesor:	**Firma**
PACHECO TORRES JUAN FRANCISCO **DNI:** 18167212 **ORCID** 0000-0002-8674-3782	Firmado digitalmente por: JPACHECO el 13-08-2022 09:47:22

Código documento Trilce: TRI - 0413091

INVESTIGA UCV