UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Enfoque de la Norma ISO/IEC 27005 para la Gestión de riesgos de seguridad operacional en la Clínica SERVIMEDIC, Bagua Grande 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniera de Sistemas

AUTORA:

Alvarado Sanchez, Maria Elena (orcid.org/0000-0002-8053-3143)

ASESOR:

Dr. Agreda Gamboa, Everson David (orcid.org/0000-0003-1252-9692)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Auditoria y Seguridad de la Información

TRUJILLO - PERÚ

2023

Dedicatoria

A Dios por su infinito amor celestial en todo este tiempo.

A mi Familia por ser fuente de superación constante en mi vida.

María Elena

Agradecimiento

A la Universidad César Vallejo por su apoyo permanente en este reto profesional.

A la clínica SERVIMEDIC por la información brindada.

A mi Asesor de tesis por su valiosa orientación en la presente investigación.

La autora

Índice de contenidos

Pág.

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

Esta investigación tuvo como objetivo general mejorar la gestión de riesgos de seguridad operacional en la clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022 mediante el enfoque de la norma ISO/IEC 27005. El tipo es investigación fue aplicada y de diseño preexperimental. Se determinó una muestra poblacional de 8 personas, a quienes se aplicó una Encuesta. El desarrollo de la solución tecnológica propuesta fue bajo la norma ISO/IEC 27005 en su versión 2018. Como resultado principal se pudo decir que, para el primer indicador: "Identificación de los riesgos de seguridad operacional" hubo un incremento de 1.54 a 4.65 puntos (3.11 puntos = Δ 66.88%); para el segundo indicador: "Evaluación de riesgos de seguridad operacional" hubo otro incremento de 1.68 a 4.76 puntos (3.08 puntos = Δ 64.71%); para el tercer indicador: "Tratamiento de riesgos de seguridad operacional" hubo otro incremento de 1.70 a 4.75 puntos (3.05 puntos = Δ 64.21%). Como conclusión general se tuvo que, la aplicación de la norma ISO 27005 mejoró cuantiosamente la gestión de riesgos de seguridad operacional en la clínica de salud en estudio.

Palabras clave: Norma ISO/IEC 27005, Gestión de riesgos, Seguridad operacional, Clínica de salud.

Abstract

The general objective of this research was to improve operational safety risk management at the SERVIMEDIC clinic in the city of Bagua Grande in the year 2022 using the ISO/IEC 27005 approach. The type of research was applied and of pre-experimental design. A population sample of 8 people was determined, to whom a survey was applied. The development of the proposed technological solution was under the ISO/IEC 27005 standard in its 2018 version. As main result it could be said that, for the first indicator: "Identification of operational security risks" there was an increase from 1.54 to 4.65 points (3.11 points = Δ 66.88%); for the second indicator: "Evaluation of operational security risks" there was another increase from 1.68 to 4.76 points (3.08 points = Δ 64.71%); for the third indicator: "Treatment of operational security risks" there was another increase from 1.70 to 4.75 points (3.05 points = Δ 64.21%). The overall conclusion was that the application of ISO 27005 greatly improved the management of operational safety risks in the health clinic under study.

Keywords: ISO/IEC 27005 standard, Risk management, Operational safety, Health clinic.

I. INTRODUCCIÓN

Castellanos (2017) manifiesta que, el fin primordial de la **gestión de riesgos** es comprender y aprovechar las conformidades para obtener beneficios y reducir los detrimentos conociendo y atacando las amenazas. La gestión de riesgos requiere la creación de una arquitectura y organización adecuada, así como el desarrollo de una sapiencia organizativa enfocada a la anticipación, así como la implementación de un mecanismo natural y sistematizado para conseguir la gestión de peligros. La gobernanza de peligros en sí misma es un procedimiento que se inicia con la creación de un contexto operativo y luego la tipificación, el examen, la valoración y el tratamiento de los riesgos. Al mismo tiempo, se supervisa y monitorea todo el procedimiento y se comunican los logros, aminorando mermas y acrecentando los beneficios.

Sphera (2022) sostiene que, hay riesgos asociados con las compañías fuertes y menos fuertes en el mundo. Algunos peligros son latentemente dañinos para los trabajadores, además que, terceros pueden amenazar las acciones, las tareas, los programas, la manufactura y más. **La administración del riesgo operacional** es una manera de lograr una visión general del rastro de peligro de una compañía en todo el eslabón de aprovisionamiento, y cualquiera en la compañía tienen un rol que representar para asegurar que la sapiencia de seguridad de la organización sea lo mejor posible.

EALDE (2018) manifiesta que, el despliegue del framework de **administración de peligros de seguridad operacional** implica un análisis integral del proceso. La cultura de riesgos permite tomar conciencia de la importancia del framework para la gobernanza de peligros en la organización. La responsabilidad recae en los empleados y la junta. El directorio debe asegurar que esta responsabilidad se extienda a toda la organización con una comunicación y transparencia que promueva la difusión para que las partes interesadas puedan analizar su exposición a los riesgos operacionales.

UDEMY (2020) afirma que, **ISO 27005** está destinado a todas las organizaciones que desean mejorar su programa de administración de peligros de seguridad. Para esto, es necesario utilizar un enfoque sistemático

para la gobernanza de peligros de seguridad, identificando las necesidades de la organización en concordancia con los requisitos de seguridad. Dicho enfoque debe adaptarse al entorno de la organización y ser particularmente coherente con la **gestión del riesgo operativo** o del negocio. La gobernanza de peligros de seguridad debía ser un componente completo de cada una de las operaciones del programa de gobernanza de seguridad informática y debía aplicarse tanto al despliegue del programa como a su marcha continua.

EBS (2017) aduce que, la ISO 27005 presenta una orientación que se centra directamente en la **gestión de riesgos de TI**. Este enfoque debe estar coordinado con la gestión del riesgo operacional de la empresa. Por lo tanto, las pautas se pueden utilizar para mitigar los riesgos de tecnología informatizada, como los causados por programas sensibles, programas operativos obsoletos o tecnologías antiguas. La administración de peligros de seguridad generalmente implica identificar, evaluar y abordar los riesgos.

En este escenario, se presenta a la **Clínica SERVIMEDIC**, la cual ofrece un servicio de salud privado de buena calidad con más de 5 años de amplia experiencia en su rubro, con excelente personal médico, conveniente infraestructura y know-how, siempre dedicada a los pacientes con familiaridad y seguridad que lo caracteriza (SERVIMEDIC, 2018).

Con el paso del tiempo, si bien es cierto, esta entidad de salud ha ido creciendo; aun así, exhibe ciertas debilidades (**problemas específicos**) más aún enfocado en la administración de peligros de seguridad operativa como: posible limitaciones, errores o incompatibilidades en el factor humano, en las operaciones internas, en las tecnologías informativas y en la infraestructura de la dependencia sanitaria.

Se incluyó la **formulación del problema**: *General:* ¿Bajo qué estado el uso del estándar ISO/IEC 27005 colige en la administración de peligros de aseguramiento operativo en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022? *Específicos:* Deficiencia precisa 1 - ¿Bajo qué estado el despliegue del estándar ISO/IEC 27005 colige en la tipificación de peligros de aseguramiento operativo en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el 2022? Deficiencia precisa 2 - ¿Bajo qué estado el despliegue del estándar ISO/IEC 27005 colige en la valoración de peligros de

aseguramiento operativo en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el 2022? Deficiencia precisa 3 - ¿Bajo qué estado el despliegue del estándar ISO/IEC 27005 colige en la terapia de peligros de aseguramiento operativo en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en 2022?

Se incluyó la **justificación de la investigación**: *Conveniencia*, fomentó la gobernanza de peligros de seguridad operativa en la dependencia de salud; *Relevancia social*, incluyó un beneficio general para los empleados y directivos de la entidad sanitaria disponiendo de información segura; *Utilidad metodológica*, fue el soporte para próximas indagaciones respecto a la gobernanza de peligros de seguridad operativa; *Implicancias prácticas*, permitió reconocer las flaquezas actuales en una clínica de salud; *Valor teórico*, coadyuvó a indagar adecuadamente las bases teóricas respecto a peligros de seguridad operacional y el estándar ISO/IEC 27005.

Se incluyó los **objetivos**: *General*: Coadyuvar la administración de peligros de aseguramiento operativo en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022 por intermedio del despliegue del estándar ISO 27005; *Específicos*: Finalidad puntual 1 - Coadyuvar la identificación de peligros de seguridad operativa; Finalidad puntual 2 - Coadyuvar la evaluación de peligros de seguridad operativa; Finalidad puntual 3 - Coadyuvar el tratamiento de peligros de seguridad operativa.

Se incluyó las **hipótesis**: *General:* “El despliegue del estándar ISO/IEC 27005 coadyuva cuantiosamente la administración de peligros de aseguramiento operativo en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022”. *Específicas:* Conjetura puntual 1 - “El despliegue del estándar ISO/IEC 27005 coadyuva la tipificación de peligros de aseguramiento operativo en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en 2022”; Conjetura puntual 2 - “La aplicación del estándar ISO/IEC 27005 coadyuva la valoración de peligros de aseguramiento operativo en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en 2022”; Conjetura puntual 3 - “La aplicación del estándar ISO/IEC 27005 coadyuva el tratamiento de peligros de aseguramiento operativo en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el 2022”.

II. MARCO TEÓRICO

Se incluyó una congregación de **antecedentes** que contribuyeron a examinar indagaciones anteriores y afines de la realidad problemática descrita como:

Navarro (2019) en su estudio presentó la implementación de la administración de peligros tecnológicos basado en el estándar ISO/IEC 27005 en el departamento de tecnologías informatizadas de la Dirección de TI de la DGI para reducir el impacto de los riesgos físicos, lógicos y organizacionales a través de una estructura metodológica híbrida entre Ciclo de calidad y la normatividad ISO/IEC 27005, que identifica los bienes más sensibles en la práctica en base a los fines de la compañía, luego se evalúan para el despliegue de la administración de peligros y, por último, se presentan los logros obtenidos, así como los desenlaces sobre la administración de riesgos a través de un mecanismo alineado.

Patiño (2018) en su estudio desarrolló la guía metodológica de práctica estándar NTE INEN ISO/IEC 27005 para la administración de peligros de TIC en comunidades del rubro estatal para mejorar la gobernanza de la información segura. Fue necesario conocer la normatividad ISO/IEC 27005 para establecer el grado de administración del peligro tecnológico en las dependencias estatales, desarrollando un análisis cualitativo-cuantitativo con diseño discrecional y se discurrió una muestra no probable. La tecnología de encuestas se aplicó con un cuestionario a los directivos de know-how de instituciones estatales. Aún a costa de la inserción de normatividad mundial, el proceso sigue siendo complejo porque las normativas fueron creadas para compañías prósperas en una trama diferente. En contestación, se propuso una guía minuciosa en la que se despliega cada fase con sus unidades de actuación y su implementación en el rubro estatal para validar cada fase predefinida.

García y otros (2019) en su estudio implementó un mecanismo de administración de peligros de información segura para PYMES que integra el método OCTAVE-S y el estándar ISO/IEC 27005, que incluye un estudio de métodos y estándares de gobernanzas de peligros, bosquejo de seguridad informatizada del mecanismo de gobernanza de peligros, validación del

modelo. La unificación permitió la caracterización pertinente y efectiva de los peligros desde la orientación cualitativa brindando la oportunidad de utilizar los valores reconocidos para los bienes desde la orientación cuantitativa. También, le permitió tipificar, examinar y luego tratar los peligros más importantes según fuera los requisitos de la compañía. Se anhela que, este piloto ayudase a gestionar los peligros de la información segura para las Pymes a fin de aminorar la inferencia de los peligros a los que están inmersos.

Puyén y otros (2018) en su estudio creyó necesario gestionar su seguridad identificando y analizando bienes de data, identificando bienes complicados, identificando debilidades e intimidaciones a esos bienes complejos y proponiendo mecanismos para ayudar a mitigar esos riesgos. El empleo correcto de los mecanismos de administración de peligros en la información segura promoviendo la sapiencia de la data segura en toda la compañía o entidad, crea confianza entre los consumidores y demuestra su fuerza y capacidades a los competidores.

Montoya (2020) en su estudio buscó aminorar los grados de peligros ante una plasmación de intimidaciones que podían impactar a los bienes de data considerables y, por ende, a los procedimientos de una compañía. Sin embargo, no todo mecanismo de seguridad ofrece una posibilidad del 100%, pues siempre habrá puntos débiles como puertas abiertas para ser usadas de forma maliciosa al no tener claro la importancia de esas extenuaciones. Se detalló visiblemente los tres elementos fundamentales para administrar los peligros, comprendiendo bien el procedimiento de examinación de peligros que conducía a una tipificación, estudio y estimación de riesgos.

Se incluyó la examinación de un bloque de **bases teóricas** como:

Norma ISO/IEC 27005, la última versión de ISO/IEC 27005 fue 2018. Brinda orientación a las organizaciones sobre cómo consumar con los requerimientos de administración de la información segura y know-how informatizado, al tiempo que brinda un marco para administrar de manera segura los peligros vinculados con la información segura para consumar con los requerimientos puntuales de la ISO/IEC 27001. Es un acomodo del cuadro estándar ISO 3100 para la información segura. Busca cumplir con los requerimientos del estándar ISO 27001 para responder el 'por qué' y el 'qué'

de la gobernanza de peligros de la información asegurada. Esto se refiere al hecho de que se pueden utilizar varios enfoques o metodologías de administración de peligros para consumar con los requerimientos de la ISO/IEC 27001. El adjunto de ISO/IEC 27005 es adaptable, pero no el magnífico, entonces se pueden usar otros cómo consumar con los requerimientos de administración de peligros según las insuficiencias y bienes de cada compañía (Adinelsa, 2021).

Seguridad operacional, puede definirse como la probabilidad de incidir en detrimentos por fracasos humanos, técnicas, circunstancial, de arquitectura o extrínsecas que puedan situar en peligro el normal progreso de las tareas empresariales y evitar la consecución de los fines corporativos (Pirani, 2020).

Gestión de riesgos de seguridad operacional, es una tarea frecuente relacionada con la revisión, planificación, ejecución, supervisión y monitoreo de las contramedidas implementadas y políticas de aseguramiento aplicadas. Representa establecer, mantener y mejorar continuamente las actualizaciones del SGSI demuestra que una organización utiliza un enfoque sistemático para caracterizar, examinar y gobernar los peligros de seguridad (SSI, 2018).

Adicionalmente, se incluyó un bloque de **enfoques conceptuales** como:

Amenaza, escenario que muestra la ocurrencia de un incidente en el interior de una compañía, que genera pérdidas cuantiosas o mayores a los bienes de data. Un programa de administración de la información segura basado en la ISO 27001 permite controlar los desafíos que fomentarían el origen de sucesos (ISO-27002, 2018).

Vulnerabilidad, características y circunstancias de las comunidades, sistemas o activos que los hacen vulnerables a los efectos nocivos de las amenazas (ISO-27002, 2018).

Riesgo, representa la mezcla de la posibilidad de que ocurra un suceso y sus implicaciones desaprobatorias. Los elementos constituyentes son peligros y debilidades (ISO-27002, 2018).

Respecto a **estándares mundiales postulantes** para el despliegue de la oferta técnica encomendada; al día de hoy, se dispone de ciertos métodos aceptados y estándares internacionales para la implementación de proyectos de seguridad informática, como es el caso de: ISO 31000, ISO 27005 e ISO 27002. Se dispuso usar el *modelo de evaluación especialista* para la elección de aquella que fuera la más conveniente en la solución ofertada siendo la triunfadora el estándar *ISO/IEC 27005* en su *versión 2018* - ver Anexo 3.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

- **Tipo de investigación**

  Aplicada pues estuvo sostenida por el éxito previo de medios y mecanismos usados en pro de la solución de situaciones problemáticas análogas o semejantes.

- **Diseño de investigación**

  Preexperimental pues se centró en la maniobra del grupo de control, de tal forma que no se recurrió completamente a la aleatoriedad para la selección de los elementos participativos.

3.2. Variables y operacionalización

- **Variables**

  - **Variable independiente:** Norma ISO/IEC 27005

    - **Definición Conceptual:**

      "Brinda orientación a las organizaciones sobre cómo consumar con los requerimientos de administración de la información segura y know-how informatizado, al tiempo que brinda un marco para administrar de manera segura los peligros vinculados con la información segura para consumar con los requerimientos puntuales de la ISO/IEC 27001" (Adinelsa, 2021).

    - **Definición operacional:**

      El estándar ISO/IEC 27005 se ha medido por intermedio del despliegue y administración efectiva de un procedimiento de administración del peligro de la data asegurada dentro de una compañía.

- **Variable dependiente:** Gestión de riesgos de seguridad operacional

  - **Definición Conceptual:**

    "Tarea frecuente relacionada con la revisión, planificación, ejecución, supervisión y monitoreo de las contramedidas implementadas y políticas de aseguramiento aplicadas" (SSI, 2018).

  - **Definición operacional:**

    La gobernanza de albures de seguridad operativa se ha medido por la tipificación, examinación y terapia de éstos.

- **Operacionalización**

Los pormenores de la operativización de las variables de investigación se exhiben en la tabla matricial situado en el bloque de anexos del actual documento - ver Anexo 2.

3.3. Población, muestra y muestreo

- **Población**

Estuvo conformado por los empleados que laboran en la clínica y, que estuvieron comprometidos de un modo u otro con la gobernanza de los peligros.

Tabla 1. *Población*

Cargo / Puesto	Cantidad
Director	1
Coordinador	3
Supervisor	1
Operario	3
Total	8

Fuente: (Elaboración propia, 2022).

$$N = 8\, personas$$

- **Muestra**

  En vista que la población fue mínima o semejante a 30; por ello, la muestra reflejó ser semejante. Se calculó:

$$n = N = 8\ personas$$

- **Muestreo**

  De corte *no probabilístico* pues en cada momento se maniobró los elementos muestrales para la ejecución de exámenes estadísticos.

3.4. Técnicas e instrumentos de recolección de datos

- **Técnicas**

  Se incluyó los primordiales medios de recopilación de la data segura de la clínica de salud como:

  - Encuesta.
  - Análisis documental.

- **Instrumentos**

  Se incluyó los principales artefactos de recopilación de la data segura de la clínica de salud como:

  - Cuestionario.
  - Ficha documental.

3.5. Procedimientos

Se procedió a describir los pasos seguidos en el procedimiento de cumplimiento de cada finalidad puntual como sigue:

- Primer paso: Se procedió a extraer las principales opiniones respecto al despliegue del estándar ISO/IEC 27005 presente en cada fase: tipificación, evaluación y tratamiento de los peligros. Para ello, se dispuso del despliegue de una Encuesta a los principales representantes de la entidad sanitaria elegida desplegando como instrumental al Cuestionario (ver Anexo 4).
- Segundo paso: Se procedió a procesar la data extraída respecto a la seguridad operativa que se maneja en la entidad sanitaria empleando algunos métodos o mecanismos estadísticos apropiados según correspondiera.
- Tercer paso: Se procedió a exhibir los resultados conseguidos luego del procesamiento de la data absorbida mostrando el cumplimiento de cada finalidad puntual planteada en la investigación.

3.6. Método de análisis de datos

Se recurrió al medio descriptivo e inferencial orientando al procedimiento y la examinación estadística de la data absorbida.

El medio estadístico descriptivo se empleó para visualizar gráficamente los logros conseguidos en los escenarios previo y ulterior al despliegue de la solución propuesta (estándar ISO/IEC 27005).

El medio estadístico inferencial se empleó para visualizar la normalización de los indicadores procesados en la consecución de cada finalidad puntual, toda vez que se complementó con un mecanismo estadístico distributivo pertinente (parametrizado o no parametrizado).

3.7. Aspectos éticos:

El vigente informe consideró el irrestricto respeto por la autoría de las publicaciones examinadas para desarrollar la investigación, así como la creación original del informe (por parte de la autora), tal como lo establece fehacientemente el reglamento de principios éticos de la

Universidad. Además, se desplegó el programa de estándar bibliográfico ISO-690 en la escritura del documento y el uso del programa antiplagio Turnitin como herramienta de verificación del índice de similitud.

IV. RESULTADOS

- **Análisis descriptivo**
  - Primer indicador:

Tabla 2. *Examen descriptivo del primer indicador*

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
IRSO-Preprueba	4	1,10	1,84	1,5398	,17624
IRSO-Posprueba	4	4,20	4,96	4,6517	,14831
N válido (por lista)	4				

Fuente: (Elaboración propia, 2022).

Al visualizar el tabloide previo, la tipificación de peligros de la información segura antepuesto al despliegue del estándar ISO 27005 ostentaba una media estadística de 1.54 puntos y subsiguiente al despliegue del estándar ISO 27005 ostenta una media estadística de 4.65 puntos, consiguiendo una progresión de 3.11 puntos (Δ 66.88%).

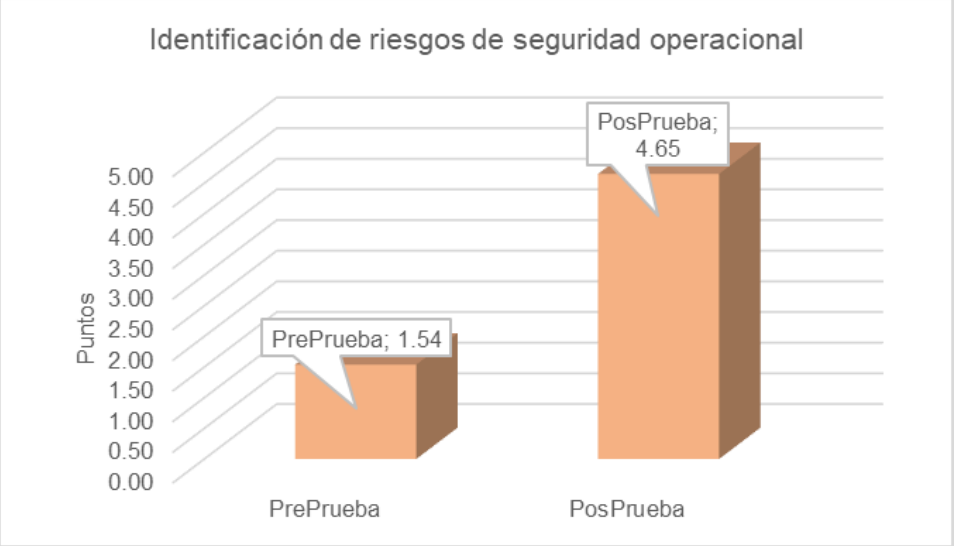

Figura 1. Promedios de preprueba y posprueba del primer indicador.

Fuente: (Elaboración propia, 2022).

- Segundo indicador:

Tabla 3. *Examen descriptivo del segundo indicador*

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
ERSO-Preprueba	4	1,24	1,86	1,6771	,15792
ERSO-Posprueba	4	4,22	4,97	4,7645	,16309
N válido (por lista)	4				

Fuente: (Elaboración propia, 2022).

Al visualizar el tabloide previo, la tipificación de peligros de la información segura antepuesto al despliegue del estándar ISO 27005 ostentaba una media estadística de 1.68 puntos y subsiguiente al despliegue del estándar ISO 27005 ostenta una media estadística de 4.76 puntos, consiguiendo una progresión de 3.08 puntos (Δ 64.71%).

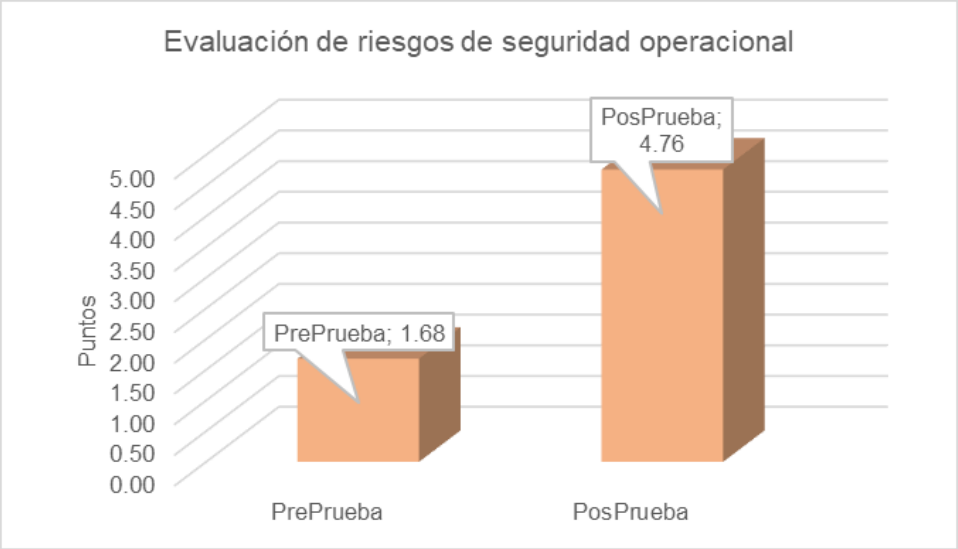

Figura 2. Promedios de preprueba y posprueba del segundo indicador.

Fuente: (Elaboración propia, 2022).

- Tercer indicador

Tabla 4. *Examen descriptivo del tercer indicador.*

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
TRSO-Preprueba	4	1,18	1,88	1,7039	,13681
TRSO-Posprueba	4	4,35	5,00	4,7490	,14167
N válido (por lista)	4				

Fuente: (Elaboración propia, 2022).

Al visualizar el tabloide previo, la tipificación de peligros de la información segura antepuesto al despliegue del estándar ISO 27005 ostentaba una media estadística de 1.70 puntos y subsiguiente al despliegue del estándar ISO 27005 ostenta una media estadística de 4.75 puntos, consiguiendo una progresión de 3.05 puntos (Δ 64.21%).

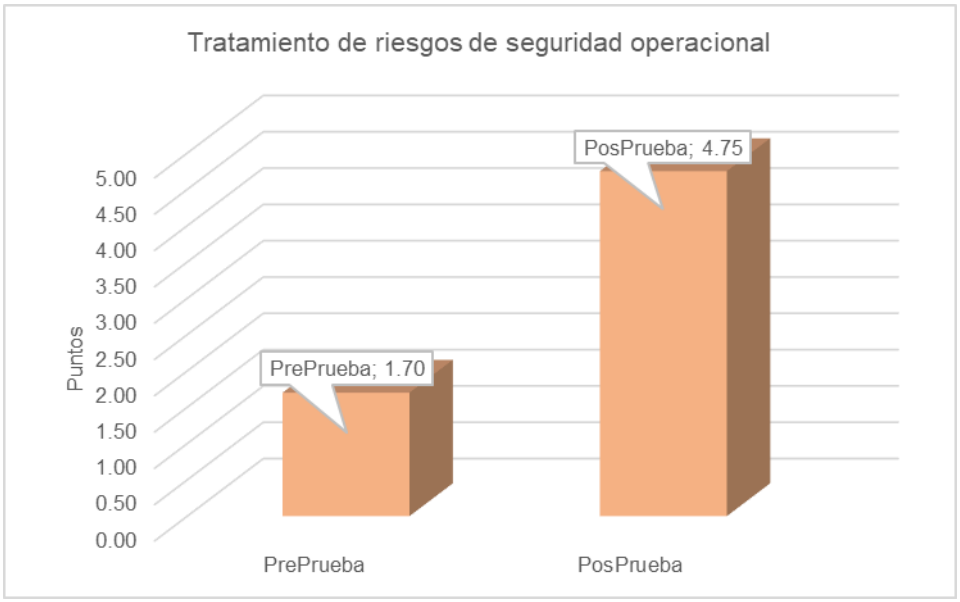

Figura 3. Promedios de preprueba y posprueba del tercer indicador.

Fuente: (Elaboración propia, 2022).

- **Análisis inferencial**

La revisión estadística empleada para calcular la normalización por indicador se basó en el examen Shapiro-Wilk (muestra ≤ 50).

- Primer indicador:

H_0: “La tipificación de los peligros de la data asegurada (sin el uso del estándar ISO 27005) si tiene partición normalizada”.

H_1: “La tipificación de los peligros de la data asegurada (sin el uso del estándar ISO 27005) no tiene partición normalizada”.

H_0: “La tipificación de los peligros de la data asegurada (con el uso del estándar ISO 27005) no tiene partición normalizada”.

H_1: “La tipificación de los peligros de la data asegurada (con el uso del estándar ISO 27005) si tiene partición normalizada”.

Se mantuvo como valía de éxito: $\alpha = 0.05$

Valía de éxito. > 0.05, se ampara la conjetura nula (H_0).

Valía de éxito. <= 0.05, se ampara la conjetura alterna (H_1).

Tabla 5. *Examen de normalidad del primer indicador*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
IRSO-PrePrueba	,813	4	,043
IRSO-PosPrueba	,854	4	,148

Fuente: (Elaboración Propia, 2022).

En referencia al tabloide previo, la valía de éxito en escenario preprueba fue 0.043 (≤ 0.05); mientras que la misma valía de éxito en escenario posprueba fue 0.148 (> 0.05). En tal sentido, al revisar ambos logros, se definió que, que para el primer indicador no había existencia de una partición normalizada, lo que derivó en el empleo del test no parametrizado de Wilcoxon.

- Segundo indicador:

H_0: “La valoración de los peligros de la información asegurada (sin el uso del estándar ISO 27005) si tiene partición normalizada”.

H_1: “La valoración de los peligros de la información asegurada (sin el uso del estándar ISO 27005) no tiene partición normalizada”.

H_0: “La valoración de los peligros de la información asegurada (con el uso del estándar ISO 27005) no tiene partición normalizada”.

H_1: “La valoración de los peligros de la información asegurada (con el uso del estándar ISO 27005) si tiene partición normalizada”.

Se mantuvo como valía de éxito: α = 0.05

Valía de éxito. > 0.05, se ampara la conjetura nula (H_0).

Valía de éxito. <= 0.05, se ampara la conjetura alterna (H_1).

Tabla 6. *Examen de normalidad del indicador 2*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
ERSO-Preprueba	,905	4	,045
ERSO-Posprueba	,917	4	,167

Fuente: (Elaboración Propia, 2022).

En referencia al tabloide previo, la valía de éxito en escenario preprueba fue 0.045 (≤ 0.05); mientras que la misma valía de éxito en escenario posprueba fue 0.167 (> 0.05). En tal sentido, al revisar ambos logros, se definió que, para el segundo indicador no había existencia de una partición normalizada, lo que derivó en el empleo del test no parametrizado de Wilcoxon.

- Tercer indicador:

  H_0: “La terapia de los peligros de la información asegurada (sin el uso del estándar ISO 27005) si tiene partición normalizada”.

  H_1: “La terapia de los peligros de la información segura (sin el uso del estándar ISO 27005) no tiene partición normalizada”.

  H_0: “La terapia de los peligros de la información asegurada (con el uso del estándar ISO 27005) no tiene partición normalizada”.

  H_1: “La terapia de los peligros de la información asegurada (con el uso del estándar ISO 27005) si tiene partición normalizada”.

  Se mantuvo como valía de éxito: α = 0.05

Valía de éxito. > 0.05, se ampara la conjetura nula (H_0).

Valía de éxito. <= 0.05, se ampara la conjetura alterna (H_1).

Tabla 7. *Examen de normalidad del tercer indicador*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
TRSO-PrePrueba	,834	4	,047
TRSO-PosPrueba	,867	4	,190

Fuente: (Elaboración Propia, 2022).

En referencia al tabloide previo, la valía de éxito en escenario preprueba fue 0.047 (≤ 0.05); mientras que la misma valía de éxito en escenario posprueba fue 0.190 (> 0.05). En tal sentido, al revisar ambos logros, se definió que, para el tercer indicador no había existencia de una partición normalizada, lo que derivó en el empleo del test no parametrizado de Wilcoxon.

- **Contrastación de hipótesis**

Como las muestras poblacionales anteriores no exhibían una partición normalizada, se usó el test no parametrizado de Wilcoxon.

- Conjetura puntual 1:

"El uso del estándar ISO 27005 coadyuva la tipificación de peligros de seguridad operativa en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

Conjeturas estadísticas:

H_0: "El uso del estándar ISO 27005 no coadyuva la tipificación de peligros de seguridad operativa en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

$$H_0: IRSOa >= IRSOp$$

H_1: "El uso del estándar ISO 27005 si coadyuva la tipificación de peligros de seguridad operativa en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

$$H_1: IRSOa < IRSOp$$

Se mantuvo como valía de éxito: $\alpha = 0.05$

Valía de éxito > 0.05, se ampara la conjetura nula (H_0).

Valía de éxito <= 0.05, se ampara la conjetura alterna (H_1).

Tabla 8. *Examen de Wilcoxon para el primer indicador*

Estadísticos de prueba[a]

	IRSO-Posprueba - IRSO-Posprueba
Z	-1,487[b]
Sig. asintótica(bilateral)	,036

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: (Elaboración propia, 2022).

La valía de éxito fue 0.036 (≤ 0.05) desechando la conjetura nula y amparando la conjetura alterna. Esto dedujo: "El uso del estándar ISO 27005 si coadyuva de forma valiosa la tipificación de peligros de seguridad operativa en la clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

- Conjetura puntual 2:

"El uso del estándar ISO 27005 coadyuva la valoración de peligros de seguridad operativa en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

Conjeturas estadísticas:

H_0: "El uso del estándar ISO 27005 no coadyuva la valoración de peligros de seguridad operativa en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

H_0: ERSOa >= ERSOp

H_1: "El uso del estándar ISO 27005 no coadyuva la valoración de peligros de seguridad operativa en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

H_1: ERSOa < ERSOp

Se mantuvo como valía de éxito: α = 0.05

Valía de éxito > 0.05, se ampara la conjetura nula (H_0).

Valía de éxito <= 0.05, se ampara la conjetura alterna (H_1).

Tabla 9. *Examen de Wilcoxon para el segundo indicador*

Estadísticos de prueba[a]

	ERSO-Posprueba - ERSO-Posprueba
Z	-1,824[b]
Sig. asintótica(bilateral)	,027

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: (Elaboración propia, 2022).

La valía de éxito fue 0.027 (≤ 0.05) desechando la conjetura nula y amparando la conjetura alterna. Esto dedujo: "El uso del estándar ISO 27005 si coadyuva de forma valiosa la valoración de peligros de seguridad operativa en la clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

- Conjetura puntual 3:

"El uso del estándar ISO 27005 coadyuva la terapia de peligros de seguridad operativa en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

Conjeturas estadísticas:

H_0: "El uso del estándar ISO 27005 no coadyuva la terapia de peligros de seguridad operativa en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

$$H_0: TRSOa >= TRSOp$$

H_1: "El uso del estándar ISO 27005 no coadyuva la terapia de peligros de seguridad operativa en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

$$H_1: TRSOa < TRSOp$$

Se mantuvo como valía de éxito: $\alpha = 0.05$

Valía de éxito > 0.05, se ampara la conjetura nula (H_0).
Valía de éxito <= 0.05, se ampara la conjetura alterna (H_1).

Tabla 10. *Examen de Wilcoxon para el tercer indicador*

Estadísticos de prueba[a]

	TRSO-Posprueba - TRSO-Posprueba
Z	-1,904[b]
Sig. asintótica(bilateral)	,049

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: (Elaboración propia, 2022).

La valía de éxito fue 0.049 (≤ 0.05) desechando la conjetura nula y amparando la conjetura alterna. Esto dedujo: "El uso del estándar ISO 27005 si coadyuva de forma valiosa la terapia de peligros de seguridad operativa en la clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022".

V. DISCUSIÓN

Referente al primer indicador: “Identificación de peligros de seguridad operativa”, las valías estadísticas logradas anterior y posterior al uso de la propuesta técnica fueron 1.54 y 4.65 puntos correspondientemente, consiguiendo una progresión de 3.11 puntos (∆ 66.88%). Estos logros fueron semejantes a los obtenidos por (Navarro, 2019), quien para reducir el impacto de los riesgos físicos, lógicos y organizacionales a través de una estructura metodológica híbrida entre Ciclo de calidad y la normatividad ISO/IEC 27005, que identifica los bienes más sensibles en la práctica en base a los fines de la compañía, luego se evalúan para el despliegue de la administración de peligros. También, son semejantes a los conseguidos por (Patiño, 2018), quien aplicó con un cuestionario a los directivos de know-how de instituciones estatales. Aún a costa de la inserción de normatividad mundial, el proceso sigue siendo complejo porque las normativas fueron creadas para compañías prósperas en una trama diferente. En contestación, se propuso una guía minuciosa en la que se despliega cada fase con sus unidades de actuación y su implementación en el rubro estatal para validar cada fase predefinida. El soporte de lo acontecido previamente, se sostiene en las bases teóricas del estándar ISO 27005 que, brinda orientación a las organizaciones sobre cómo consumar con los requerimientos de administración de la información segura y know-how informatizado, al tiempo que brinda un marco para administrar de manera segura los peligros vinculados con la información segura para consumar con los requerimientos puntuales de la ISO/IEC 27001 (Adinelsa, 2021).

Referente al segundo indicador: “Valoración de peligros de seguridad operativa”, las valías estadísticas logradas anterior y posterior al uso de la propuesta técnica fueron 1.68 y 4.76 puntos correspondientemente, consiguiendo una progresión de 3.08 puntos (∆ 64.71%). Estos logros fueron semejantes a los obtenidos por (García, y otros, 2019) quienes, incluyeron un estudio de métodos y estándares de gobernanzas de peligros, bosquejo de seguridad informatizada del mecanismo de gobernanza de peligros, validación del modelo. La unificación permitió la caracterización pertinente y efectiva de los peligros desde la orientación cualitativa brindando la oportunidad de utilizar

los valores reconocidos para los bienes desde la orientación cuantitativa. También, le permitió tipificar, examinar y luego tratar los peligros más importantes según fuera los requisitos de la compañía. También, son semejantes a los conseguidos por (Puyén, y otros, 2018) quienes, creyeron necesario gestionar su seguridad identificando y analizando bienes de data, identificando bienes complicados, identificando debilidades e intimidaciones a esos bienes complejos y proponiendo mecanismos para ayudar a mitigar esos riesgos. El soporte de lo acontecido previamente, se sostiene en las bases teóricas del estándar ISO 27005 que, Es un acomodo del cuadro estándar ISO 3100 para la información segura. Busca cumplir con los requerimientos del estándar ISO 27001 para responder el 'por qué' y el 'qué' de la gobernanza de peligros de la información asegurada. Esto se refiere al hecho de que se pueden utilizar varios enfoques o metodologías de administración de peligros para consumar con los requerimientos de la ISO/IEC 27001 (Adinelsa, 2021).

Referente al tercer indicador: “Terapia de peligros de seguridad operativa”, las valías estadísticas logradas anterior y posterior al uso de la propuesta técnica fueron 1.70 y 4.75 puntos correspondientemente, consiguiendo una progresión de 3.05 puntos (Δ 64.21%). Estos logros fueron semejantes a los obtenidos por (Montoya, 2020) quien, buscó aminorar los grados de peligros ante una plasmación de intimidaciones que podían impactar a los bienes de data considerables y, por ende, a los procedimientos de una compañía. Sin embargo, no todo mecanismo de seguridad ofrece una posibilidad del 100%, pues siempre habrá puntos débiles como puertas abiertas para ser usadas de forma maliciosa al no tener claro la importancia de esas extenuaciones. También, son semejantes a los conseguidos por (Patiño, 2018) quien, desarrolló la guía metodológica de práctica estándar NTE INEN ISO/IEC 27005 para la administración de peligros de TIC en comunidades del rubro estatal para mejorar la gobernanza de la información segura. Fue necesario conocer la normatividad ISO/IEC 27005 para establecer el grado de administración del peligro tecnológico en las dependencias estatales, desarrollando un análisis cualitativo-cuantitativo con diseño discrecional y se discurrió una muestra no probable. El soporte de lo acontecido previamente, se sostiene en las bases teóricas del estándar ISO

27005 que, 27005 es adaptable, pero no el magnífico, entonces se pueden usar otros cómo consumar con los requerimientos de administración de peligros según las insuficiencias y bienes de cada compañía (Adinelsa, 2021).

VI. CONCLUSIONES

1. Se consiguió una progresión de la tipificación de los peligros de seguridad operativa en la clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022 consiguiendo valías estadísticas finales antepuesto y subsiguiente al despliegue del estándar ISO 27005 de 1.54 y 4.65 puntos correspondientemente, generando una amplificación de 3.11 puntos (Δ 66.88%).
2. Se consiguió una progresión de la valoración de los peligros de seguridad operativa en la clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022 consiguiendo valías estadísticas finales antepuesto y subsiguiente al despliegue del estándar ISO 27005 de 1.68 y 4.76 puntos correspondientemente, generando una amplificación de 3.08 puntos (Δ 64.71%).
3. Se consiguió una progresión de la terapia de los peligros de seguridad operativa en la clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022 consiguiendo valías estadísticas finales antepuesto y subsiguiente al despliegue del estándar ISO 27005 de 1.70 y 4.75 puntos correspondientemente, generando una amplificación de 3.05 puntos (Δ 64.21%).

VII. RECOMENDACIONES

Al Director general:

Se aconseja la puesta en práctica de la norma ISO 27005 propuesta como solución en la investigación soportado en un conjunto de requerimientos técnicos funcionales y no funcionales según corresponda.

A los Jefes de área:

Se aconseja perfeccionar el periodo de vida de la administración de peligros de seguridad operativa incorporando el mejoramiento continuo progresivo.

A los Supervisores:

Se aconseja elaborar un plan de monitoreo recurrente para garantizar el cumplimiento de las recomendaciones plasmadas en la normatividad de la ISO 27005.

A los Operarios:

Se aconseja incorporar en su labor cotidiana todas las buenas prácticas de administración de peligros de seguridad operativa que demanda la normativa global ISO/IEC 27005.

REFERENCIAS

Adinelsa. 2021. Incidentes y Riesgos de Seguridad de la Información. [En línea] 1 de Marzo de 2021. [Citado el: 15 de Marzo de 2022.] http://www.adinelsa.com.pe/files/adinelsaweb/Comunicaciones_Imagen_Institucional/ADINELSA-CHARLA-Incidentes-Riesgos-SI.pdf.

Castellanos, José. 2017. Gestión del Riesgo Operacional. [En línea] 1 de Diciembre de 2017. [Citado el: 15 de Marzo de 2022.] http://www.riesgooperacional.com/docs/31%20Riesgo%20oper%20paper.pdf

EALDE. 2018. El Marco de Gestión de Riesgos Operacionales. [En línea] 9 de Enero de 2018. [Citado el: 15 de Marzo de 2022.] https://www.ealde.es/marco-gestion-de-riesgos-operacionales/.

EBS. 2017. ISO 27005 para la Gestión de Riesgos de Tecnologías de la Información. [En línea] 7 de Septiembre de 2017. [Citado el: 15 de Marzo de 2022.] https://www.ealde.es/iso-27005-gestion-de-riesgos/.

García, Johari y Huamani, Sarita. 2019. *"Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú".* Lima : UPC, 2019.

ISO 27001. (7 de Enero de 2020). *Análisis de riesgos en ISO 27001*. Obtenido de https://www.escuelaeuropeaexcelencia.com/2020/01/analisis-de-riesgos-en-iso-27001-evaluar-consecuencias-y-probabilidades/#:~:text=La%20evaluaci%C3%B3n%20cuantitativa%20en%20un,usualmente%20expresados%20en%20cifras%20monetarias.

ISO-27002. 2018. Análisis de riesgos en ISO 27002. [En línea] 7 de Enero de 2018. https://www.escuelaeuropeaexcelencia.com/2020/01/analisis-de-riesgos-en-iso-27001-evaluar-consecuencias-y-probabilidades/#:~:text=La%20evaluaci%C3%B3n%20cuantitativa%20en%20un,usualmente%20expresados%20en%20cifras%20monetarias..

ISO Tools Excellence. (01 de 01 de 2016). *Norma ISO 27002*. Recuperado el 15 de 03 de 2018, de https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/

ISOTools. (28 de Julio de 2018). *ISO/IEC 27005:2018, la norma que reducirá el riesgo de brechas en la seguridad informática*. Obtenido de https://www.isotools.org/2018/08/15/iso-iec-270052018-reducira-el-riesgo-de-brechas-en-la-seguridad/

ISOTools. 2018. ISO/IEC 27005:2018, la norma que reducirá el riesgo de brechas en la seguridad informática. [En línea] 28 de Julio de 2018.

Montoya, Martín. 2020. *"Evaluación de riesgo de seguridad de información según ISO 27005, OGITT – Instituto Nacional de Salud".* Lima : UCV, 2020.

Navarro, Judith. 2019. *“Aplicación de Gestión de Riesgos Tecnológicos basada en la norma ISO/IEC 27005 en el área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI”.* Managua : UNI-DEPG, 2019.

PAE. (1 de Enero de 2018). *MAGERIT v3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Patiño, Susana. 2018. *"Propuesta Metodologógica de Gestión de Riesgos de Tecnología de Información y Comunicación para Entidades Públicas con ISO/IEC 27005".* Sangolquí : ESPE, 2018.

PECB. (1 de Enero de 2020). *Capacitaciones en Riesgos de Seguridad de la Información ISO/IEC 27005*. Obtenido de https://pecb.com/es/education-and-certification-for-individuals/iso-iec-27005

PMG-SSI. (5 de Enero de 2017). *ISO 27005: ¿Cómo identificar los riesgos?* Obtenido de https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/

Pirani. 2020. Manual para un sistema de gestión de riesgo operacional. [En línea] 1 de Enero de 2020. [Citado el: 20 de Marzo de 2022.] https://www.piranirisk.com/es/academia/especiales/manual-para-el-sistema-de-gestion-del-riesgo-operacional.

Puyén, Vicente y Rivas, Betty. 2018. *"Modelo de gestión de riesgos basados en la Norma ISO/IEC 27005 y Metodología MAGERIT para mejorar la Gestión de seguridad de la información en el Hospital Regional de Lambayeque".* Lambayeque : UNPRG, 2018.

SERVIMEDIC. 2018. Página Oficial de Facebook. [En línea] 1 de Enero de 2018. [Citado el: 15 de Marzo de 2022.] https://www.facebook.com/PuntoAparteTV/videos/%EF%B8%8F%EF%B8%

8Fservimedic-amazonas-m%C3%A9dicos-especialistas-a-tu-serviciocuenta-con-laboratorio-/2020921054738879/.

Sphera. 2022. ¿Qué es la gestión de riesgos operacionales? [En línea] 14 de Enero de 2022. https://sphera.com/glosario-es/que-es-la-gestion-de-riesgos-operacionales/?lang=es.

SSI. 2018. ISO 27005: ¿Cómo identificar los riesgos? [En línea] 5 de Enero de 2018. https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/.

UDEMY. 2020. [En línea] 1 de Junio de 2020. [Citado el: 15 de Marzo de 2022.] https://www.udemy.com/course/iso-27005-gestion-de-riesgos-de-seguridad-de-informacion/?utm_source=adwords&utm_medium=udemyads&utm_campaign=DSA-WebIndex_la.ES_cc.LATAM&utm_term=_._ag_120316893258_._ad_504879908808_._kw__._de_c_._dm__._pl__._ti_dsa-38210881.

UM. 2020. Empresas de Base Tecnológica. [En línea] 1 de Enero de 2020. [Citado el: 20 de Mayo de 2022.] https://www.um.es/web/otri/contenido/empresas-de-base-tecnologica.

XATACA. (4 de Septiembre de 2020). *Parches de seguridad de Windows*. Obtenido de https://www.xataka.com/basics/parches-seguridad-windows-instalarlos#:~:text=Los%20parches%20de%20seguridad%20de%20Windows%20son%20actualizaciones%20acumulativas%20enfocadas,traiga%20estos

ANEXOS

Anexo 1 - Matriz de consistencia

Título: Enfoque de la Norma ISO/IEC 27005 para la Gestión de riesgos de seguridad operacional en la Clínica SERVIMEDIC, Bagua Grande 2022.

Autora: Alvarado Sánchez, María Elena

Problema	Objetivo	Hipótesis	Variable
General: ¿De qué manera el enfoque de la norma ISO/IEC 27005 influye en la gestión de riesgos de seguridad operacional en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022?	General: Mejorar la gestión de riesgos de seguridad operacional en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022 mediante el enfoque de la norma internacional ISO/IEC 27005:2018.	General: “El enfoque de la norma ISO/IEC 27005 mejora significativamente la gestión de riesgos operacionales en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022”.	Independiente: Norma ISO/IEC 27005
Específicos: 1. ¿De qué manera el enfoque de la norma ISO/IEC 27005 influye en la identificación de riesgos de seguridad operacionales en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022? 2. ¿De qué manera el enfoque de la norma ISO/IEC 27005 influye en la evaluación de riesgos de seguridad operacionales en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022? 3. ¿De qué manera el enfoque de la norma ISO/IEC 27005 influye en el tratamiento de riesgos de seguridad operacionales en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022?	Específicos: 1. Mejorar la identificación de riesgos de seguridad operacional. 2. Mejorar la evaluación de riesgos de seguridad operacional. 3. Mejorar el tratamiento de riesgos de seguridad operacional.	Específicas: 1. “El enfoque de la norma ISO/IEC 27005 mejora la identificación de riesgos de seguridad operacionales en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022”. 2. “El enfoque de la norma ISO/IEC 27005:2018 mejora la evaluación de riesgos de seguridad operacionales en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022”. 3. “El enfoque de la norma ISO/IEC 27005 mejora el tratamiento de riesgos de seguridad operacionales en la Clínica SERVIMEDIC de la ciudad de Bagua Grande en el año 2022”.	Dependiente: Gestión de riesgos de seguridad operacional

<table>
<tr><td colspan="4">Metodología</td></tr>
<tr>
<td>Tipo de investigación:
Aplicada</td>
<td>Población (N):
$N = 8\ personas$</td>
<td>Técnicas de recolección de datos:
• Encuesta
• Análisis documental</td>
<td>Método de análisis de datos:
• Estadística descriptiva
• Estadística inferencial</td>
</tr>
<tr>
<td>Diseño de investigación:
Preexperimental</td>
<td>Muestra (n):
$n = 8\ personas$</td>
<td>Instrumentos de recolección de datos:
• Cuestionario
• Ficha de datos</td>
<td>Aspectos éticos:
Se respetará el derecho a la propiedad intelectual (Originalidad de la investigación - Reporte Turnitin).
Se tomará en cuenta el Código de ética de la Universidad César Vallejo (RCU Nº 0126-2017/UCV).
Se usará para la redacción de las referencias bibliográficas el sistema de Normas ISO-690.</td>
</tr>
</table>

Anexo 2 - Matriz de operacionalización de variables

Variable	Definición Conceptual	Definición Operacional	Dimensión (Sub variable)	Indicador	Escala de medición
Independiente: Norma ISO/IEC 27005	“Brinda orientación a las organizaciones sobre cómo consumar con los requerimientos de administración de la información segura y know-how informatizado, al tiempo que brinda un marco para administrar de manera segura los peligros vinculados con la información segura para consumar con los requerimientos puntuales de la ISO/IEC 27001” (Adinelsa, 2021).	El estándar ISO/IEC 27005 se ha medido por intermedio del despliegue y administración efectiva de un procedimiento de administración del peligro de la data asegurada dentro de una compañía.			
Dependiente: Gestión de riesgos de seguridad operacional	“Tarea frecuente relacionada con la revisión, planificación, ejecución, supervisión y monitoreo de las contramedidas implementadas y políticas de aseguramiento aplicadas” (SSI, 2018).	La gobernanza de albures de seguridad operativa se ha medido por la tipificación, examinación y terapia de éstos.	Riesgo	Identificación del riesgo de seguridad operacional	Ordinal
				Evaluación del riesgo de seguridad operacional	Ordinal
				Tratamiento del riesgo seguridad operacional	Ordinal

Anexo 3 - Método de juicio experto

Apellidos y nombres del experto: Agreda Gamboa, Everson David

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

Fecha: 27/05/2022

Título del proyecto de investigación: "Enfoque de la Norma ISO/IEC 27005 para la Gestión de riesgos de seguridad operacional en la Clínica SERVIMEDIC, Bagua Grande 2022".

Autora: Alvarado Sánchez, María Elena.

Evaluación de la norma internacional para la gestión de riesgos de seguridad operacional

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

Ítem	Criterios	Norma internacional		
		ISO 27005	ISO 31000	ISO 27002
1	Tiempo de implementación	3	3	2
2	Información	3	2	2
3	Requerimientos	3	3	2
4	Complejidad	3	3	2
5	Conocimiento	3	2	2
Total		15	13	10

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

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las metodologías/marcos de trabajo propuestas

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

Apellidos y nombres del experto: Mendoza Rivera, Ricardo Darío

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

Fecha: 27/05/2022

Título del proyecto de investigación: "Enfoque de la Norma ISO/IEC 27005 para la Gestión de riesgos de seguridad operacional en la Clínica SERVIMEDIC, Bagua Grande 2022".

Autora: Alvarado Sánchez, María Elena.

Evaluación de la norma internacional para la gestión de riesgos de seguridad operacional

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

Ítem	Criterios	Norma internacional		
		ISO 27005	ISO 27005	ISO 27005
1	Tiempo de implementación	2	2	2
2	Información	3	2	2
3	Requerimientos	3	3	2
4	Complejidad	2	2	1
5	Conocimiento	3	2	2
Total		13	11	9

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

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las metodologías/marcos de trabajo propuestas

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

Apellidos y nombres del experto: Córdova Otero, Juan Luis

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

Fecha: 27/05/2022

Título del proyecto de investigación: "Enfoque de la Norma ISO/IEC 27005 para la Gestión de riesgos de seguridad operacional en la Clínica SERVIMEDIC, Bagua Grande 2022".

Autora: Alvarado Sánchez, María Elena.

Evaluación de la norma internacional para la gestión de riesgos de seguridad operacional

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

Ítem	Criterios	Norma internacional		
		ISO 27005	ISO 27005	ISO 27005
1	Tiempo de implementación	3	3	2
2	Información	3	2	2
3	Requerimientos	3	3	2
4	Complejidad	3	2	2
5	Conocimiento	3	3	2
Total		15	13	10

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

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las metodologías/marcos de trabajo propuestas

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

Anexo 4. Instrumentos de recolección de datos

Cuestionario aplicado a los Usuarios de la clínica SERVIMEDIC

A continuación, se presenta una lista de preguntas contenidas en nueve (9) ítems que corresponden a su percepción sobre la gestión de riesgos de seguridad operacional en la clínica. Por favor, indique su apreciación objetiva marcando con una “X” sobre cualquier de los números 1, 2, 3, 4 ó 5, dónde:

1	2	3	4	5
Deficiente	Malo	Regular	Bueno	Excelente

Variable	Dimensión	Ítems	Opción de respuesta				
			1	2	3	4	5
Gestión de riesgos de seguridad operacional	Riesgo	1. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para la caracterización de riesgos de seguridad operacional?					
		2. ¿Cuál su percepción respecto al manejo responsable de la información para la caracterización de riesgos de seguridad operacional?					
		3. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para la caracterización de riesgos de seguridad operacional?					
		4. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para la valoración de riesgos de seguridad operacional?					
		5. ¿Cuál su percepción respecto al manejo responsable de la información para la valoración de riesgos operacionales?					
		6. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para la valoración de riesgos seguridad operacional?					
		7. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para el manejo de riesgos seguridad operacional?					
		8. ¿Cuál su percepción respecto al manejo responsable de la información para el manejo de riesgos seguridad operacional?					
		9. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para el manejo de riesgos seguridad operacional?					

Hoja de validación del instrumento (1)

I. Datos generales:

Cuestionario

II. II. Instrucciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión: Riesgo							
1. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para la caracterización de riesgos de seguridad operacional?	x		x		x		
2. ¿Cuál su percepción respecto al manejo responsable de la información para la caracterización de riesgos de seguridad operacional?	x		x		x		
3. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para la caracterización de riesgos de seguridad operacional?	x		x		x		
4. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para la valoración de riesgos de seguridad operacional?	x		x		x		
5. ¿Cuál su percepción respecto al manejo responsable de la información para la valoración de riesgos operacionales?	x		x		x		
6. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para la valoración de riesgos seguridad operacional?	x		x		x		
7. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para el manejo de riesgos seguridad operacional?	x		x		x		
8. ¿Cuál su percepción respecto al manejo responsable de la información para el manejo de riesgos seguridad operacional?	x		x		x		
9. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para el manejo de riesgos seguridad operacional?	x		x		x		

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

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

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

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

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Dr. Agreda Gamboa, Everson David
Especialidad del evaluador	Redes y Comunicaciones
 **DNI:** 18161457	Trujillo, 27 de mayo del 2022

Hoja de validación del instrumento (2)

I. Datos generales:

Cuestionario

II. II. Instrucciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión: Riesgo							
1. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para la caracterización de riesgos de seguridad operacional?	x		x		x		
2. ¿Cuál su percepción respecto al manejo responsable de la información para la caracterización de riesgos de seguridad operacional?	x		x		x		
3. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para la caracterización de riesgos de seguridad operacional?	x		x		x		
4. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para la valoración de riesgos de seguridad operacional?	x		x		x		
5. ¿Cuál su percepción respecto al manejo responsable de la información para la valoración de riesgos operacionales?	x		x		x		
6. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para la valoración de riesgos seguridad operacional?	x		x		x		
7. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para el manejo de riesgos seguridad operacional?	x		x		x		
8. ¿Cuál su percepción respecto al manejo responsable de la información para el manejo de riesgos seguridad operacional?	x		x		x		
9. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para el manejo de riesgos seguridad operacional?	x		x		x		

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

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

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

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

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Dr. Mendoza Rivera, Ricardo Darío
Especialidad del evaluador	Gestión de Proyectos
 **DNI:** 18070765	Trujillo, 27 de mayo del 2022

Hoja de validación del instrumento (3)

I. Datos generales:

Cuestionario

II. II. Instrucciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión: Riesgo							
1. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para la caracterización de riesgos de seguridad operacional?	x		x		x		
2. ¿Cuál su percepción respecto al manejo responsable de la información para la caracterización de riesgos de seguridad operacional?	x		x		x		
3. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para la caracterización de riesgos de seguridad operacional?	x		x		x		
4. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para la valoración de riesgos de seguridad operacional?	x		x		x		
5. ¿Cuál su percepción respecto al manejo responsable de la información para la valoración de riesgos operacionales?	x		x		x		
6. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para la valoración de riesgos seguridad operacional?	x		x		x		
7. ¿Cuál su percepción respecto al cumplimiento de normatividad estándar para el manejo de riesgos seguridad operacional?	x		x		x		
8. ¿Cuál su percepción respecto al manejo responsable de la información para el manejo de riesgos seguridad operacional?	x		x		x		
9. ¿Cuál su percepción respecto a las responsabilidades y procedimientos para el manejo de riesgos seguridad operacional?	x		x		x		

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

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

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

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

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Ms. Córdova Otero, Juan Luis
Especialidad del evaluador	Sistemas de comunicación
 **DNI:** 18122765	Trujillo, 27 de mayo del 2022

Anexo 6 - Confiabilidad de los instrumentos de recolección de datos

Resumen de procesamiento de casos

		N	%
Casos	Válido	9	100,0
	Excluido[a]	0	,0
	Total	9	100,0

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

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,861	9

Anexo 7 - Solución propuesta

ENFOQUE DE LA NORMA ISO/IEC 27005 PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL EN LA CLÍNICA SERVIMEDIC, BAGUA GRANDE

Proceso de ges

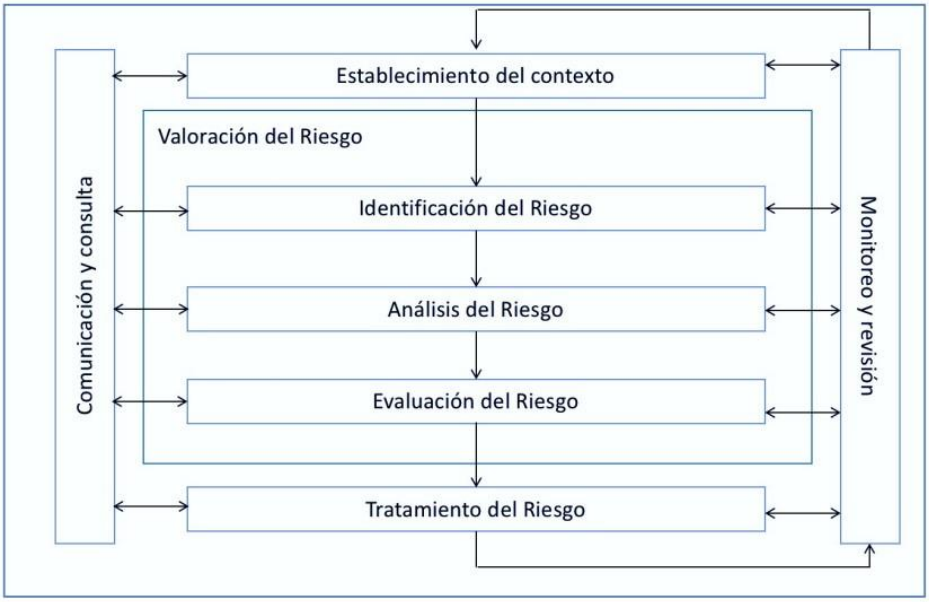

Figura. Proceso de gestión de riesgos. Tomado de (SISTESEG, 2018).

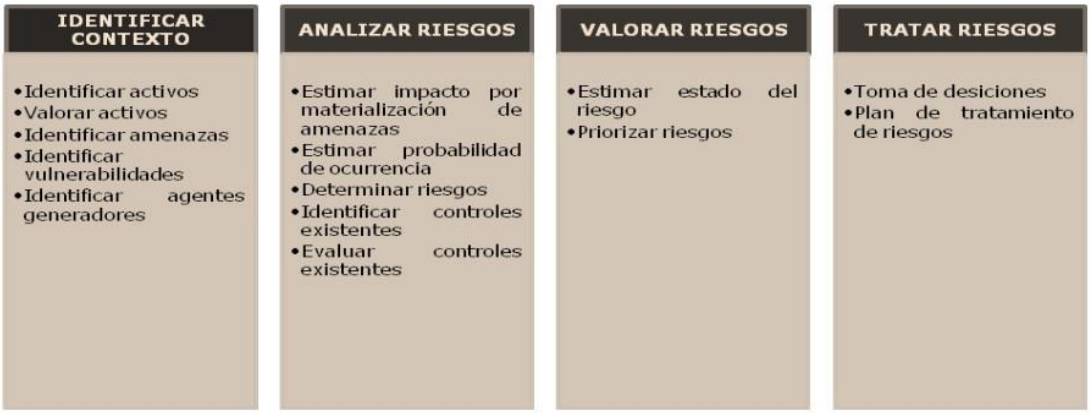

Figura. Etapas de la gestión de riesgos. Tomado de (SISTESEG, 2018).

A continuación, se presentará únicamente un bosquejo gráfico de la aplicación de la norma internacional ISO 27005:2018 para la gestión de riesgos de seguridad operacional en la clínica SERVIMEDIC, esto debido a la cláusula de confidencialidad de los datos de la entidad de salud.

Etapa 1: Identificación de activos de información y físicos de la Clínica SERVIMEDIC

Activos de información y físicos		
Activos físicos	Infraestructura física	Oficinas
	Hardware	Servidores, dispositivos de comunicaciones, computadoras de escritorio.
	Tecnología Software	Aplicaciones
Activos de información	Electrónica	Información importante para el negocio.
	Documentos	Información importante para el negocio
personal	Dueños de información	Nivel directivo dueño de la información que asigna permisos para leer utilizar y modificar la información.
		Personal que utiliza la información para su trabajo.
Servicios		Correo electrónico

Etapa 2: Valoración de activos de información de la Clínica SERVIMEDIC

	Valoración de los activos			
	MINIMO (1)	MEDIO (3)	GRAVE (5)	CATASTRÓFICO (7)
Las pérdidas económicas por indisponibilidad del activo son:				
Los servicios prestados se ven afectados por la indisponibilidad del activo de la siguiente forma:	Interrupción leve o nula en suministro de servicios.	Obliga al cliente a cambiar de proveedor de forma transitoria.	Pérdida de algunos clientes de forma definitiva.	Pérdida de clientes clave.
La indisponibilidad del activo afecta la operación así:	Retrasos en funciones no vitales	Retrasos leves en funciones vitales.	Retrasos graves en funciones vitales	Interrupción inmediata de funciones vitales
La indisponibilidad del activo afecta la imagen en el sentido que:	No afectar la confianza en los productos o servicios.	Pérdida de confianza en un servicio específico o en una parte de la organización.	Pérdida de confianza de parte de los clientes.	Pérdida de confianza del mercado y daños a la imagen de marca.
La indisponibilidad del activo afecta el cumplimiento de obligaciones en el sentido que:	Produce una falta leve en el cumplimiento de algún contrato.	Produce una falta en el cumplimiento de algún contrato que obliga a renegociar.	Produce una falta grave en el cumplimiento de algún contrato.	Deja a la organización al margen de la ley

Etapa 2: Estimación del impacto de afectación de activos de la Clínica SERVIMEDIC

El impacto es la medida de daño causado por un incidente en el supuesto de que ocurra, afectando así, el valor de los activos, está perdida de valor la denominamos degradación del activo.

La medición del impacto la realizaremos utilizando la siguiente matriz:

VALORACION DEL ACTIVO	AFECTACION DEL ACTIVO				
	5%	25%	50%	75%	100%
MA: muy alto	A	A	A	A	MA
A: alto	M	M	A	A	A
M: medio	B	M	M	A	A
B: bajo	MB	MB	M	M	M
MB: muy bajo	MB	MB	MB	B	M

Etapa 3: Tratamiento de riesgos operacionales de la Clínica SERVIMEDIC

ZONA	IMPACTO	FRECUENCIA	MEDIDA
Zona de riesgo importante	**MA:** muy alto	Poco frecuente	Prevenir riesgo: Implementar controles frente a impacto.
	MA: muy alto	Normal	Prevenir riesgo: Implementar controles frente a impacto.
	A: alto	Frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	M: medio	Frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	M: medio	Muy frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
Zona de riesgo moderado	**A:** alto	Poco frecuente	Compartir riesgos. Prevenir riesgo: Implementar ó mejorar controles frente a impacto.
	A: alto	Normal	Compartir riesgos. Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	M: medio	Normal	Compartir riesgos. Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	B: bajo	Frecuente	Realizar análisis costo beneficio para decidir si el riesgo se asume, se previene o se comparte.
	B: bajo	Muy frecuente	Realizar análisis costo beneficio para decidir si el riesgo se asume, se previene o se comparte.
Zona tolerable del riesgo	**M:** medio	Poco frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto.
	B: bajo	Normal	Realizar análisis costo beneficio parta decidir si el riesgo se asume, se previene o se comparte.
	MB: muy bajo	Frecuente	Realizar análisis costo beneficio parta decidir si el riesgo se asume, se previene o se comparte.
	MB: muy bajo	Muy frecuente	Realizar análisis costo beneficio parta decidir si el riesgo se asume, se previene o se comparte.

Una vez seleccionado los controles que serán implementados para mitigación de riesgos es necesario elaborar un plan de acción que garantice un efectivo despliegue de los mismos.

La elaboración del plan de tratamiento de riesgos será responsabilidad del Oficial de Seguridad y la respectiva aprobación de los mismos del Comité de Seguridad.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, AGREDA GAMBOA EVERSON DAVID, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - TRUJILLO, asesor de Tesis titulada: "Enfoque de la Norma ISO/IEC 27005 para la Gestión de riesgos de seguridad operacional en la Clínica SERVIMEDIC, Bagua Grande 2022", cuyo autor es ALVARADO SANCHEZ MARIA ELENA, constato que la investigación tiene un índice de similitud de 22.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

TRUJILLO, 22 de Agosto del 2022

Apellidos y Nombres del Asesor:	**Firma**
AGREDA GAMBOA EVERSON DAVID **DNI:** 18161457 **ORCID:** 0000-0003-1252-9692	Firmado electrónicamente por: AGREDA el 22-08-2022 23:44:54

Código documento Trilce: TRI - 0423356

INVESTIGA UCV