UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

# Aplicación de la Norma Internacional ISO/IEC 27005:2018 para la Gestión de Riesgos de Seguridad de la Información en Dispositivos GPS, 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas


**AUTOR:**

Nina Yana, Ademir (orcid.org/0000-0002-4744-6953)

**ASESOR:**

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


**LÍNEA DE INVESTIGACIÓN:**

Auditoria de Sistemas y Seguridad de la Información

**LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:**

Desarrollo económico, empleo y emprendimiento

CALLAO - PERÚ

2022

## Dedicatoria

*A Dios y mi familia por ser lo más*
*maravilloso en este mundo.*

Ademir

**Agradecimiento**

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

A la empresa de transporte por la información brindada.

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

El autor

## 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 de la información en dispositivos GPS en el año 2022 mediante la aplicación de la norma internacional ISO/IEC 27005:2018. El tipo es investigación fue aplicada y de diseño preexperimental. Se determinó una muestra poblacional de 10 personas, a quienes se aplicó una Encuesta. El desarrollo de la solución tecnológica propuesta fue bajo la norma internacional ISO 27005:2018. Como resultado principal se puede decir que, para el primer indicador: "Identificación de los riesgos de seguridad de la información" hubo un incremento de 1.43 a 4.63 puntos (3.20 puntos = Δ 64.00%); para el segundo indicador: "Evaluación de riesgos de seguridad de la información" hubo otro incremento de 1.61 a 4.50 puntos (2.89 puntos = Δ 57.80%) y; para el tercer indicador, "Tratamiento de riesgos de seguridad de la información" hubo otro incremento de 1.50 a 4.58 puntos (2.88 puntos = Δ 61.80%). Como conclusión general se tuvo que, la aplicación de la norma internacional ISO 27005 mejora cuantiosamente la gestión de riesgos de seguridad de la información en dispositivos GPS en el año 2022.



***Palabras clave:*** *Norma internacional, ISO 27005:2018, riesgos de seguridad de la información, dispositivos GPS.*

## Abstract

This research had the overall objective of improving information security risk management in GPS devices in the year 2022 by applying the international standard ISO/IEC 27005:2018. The type of research was applied and pre-experimental design. A population sample of 10 people was determined, to whom a survey was applied. The development of the proposed technological solution was under the international standard ISO 27005:2018. As main result it can be said that, for the first indicator: "Identification of information security risks" there was an increase from 1.43 to 4.63 points (3.20 points =  64.00%); for the second indicator: "Evaluation of information security risks" there was another increase from 1.61 to 4.50 points (2.89 points =  57.80%) and; for the third indicator, "Treatment of information security risks" there was another increase from 1.50 to 4.58 points (2.88 points =  61.80%). As a general conclusion, the application of the international standard ISO 27005 greatly improves the management of information security risks in GPS devices in the year 2022.



***Keywords:*** *International standard, ISO 27005:2018, information security risks, GPS devices.*

# I. INTRODUCCIÓN

Fernández (2020) sostiene lo siguiente: ¿qué haríamos si no existiese el **Sistema de Posicionamiento Global (GPS)** en nuestro móvil o cualquier dispositivo? Seguramente la vida no se detendría. Pero existe la costumbre de su alta aplicación, a tal punto que diariamente, varios dependen de este valioso instrumento, considerando que esta aplicación se halla en todo tipo de dispositivo. Pero nos preguntamos nuevamente ¿se debe exponer nuestra intimidad de esta forma?

Novoa (2020) afirma que, el **sistema GPS** opera a través de una red de 24 satélites en órbita a una altitud de 20.000 km, cubriendo toda la superficie de la Tierra en órbitas sincrónicas. Si desea determinar su posición, el receptor ubica en forma automática al menos cuatro satélites de la red y recibe señales de ellos indicando sus respectivas identificaciones y las horas de cada uno. Esto facilita establecer la ubicación con una precisión de centímetros, sin embargo la precisión en metros es la más común. Inicialmente fue destinado a uso militar, pero estuvo disponible para civiles en la década de 1980. El GPS funciona las 24 horas del día, en cualquier clima del mundo. Puede ser gratis su uso.

PECB (2020) sostiene que, la **norma internacional ISO/IEC 27005** otorga pautas para establecer un direccionamiento sistematizado del manejo de riesgos de protección de datos, necesarios para identificar las demandas empresariales relacionadas con los requisitos para el prototipo de un programa de manejo de protección de datos efectivo. Este estándar internacional también es compatible con los conceptos de ISO/IEC 27001 y tiene como objetivo respaldar la implantación efectiva de la protección de datos basado en un enfoque de manejo de riesgos.

SSI (2017) nos dice que, la **normativa internacional ISO/IEC 27005** sustituye la normativa internacional ISO 13335-2. La normativa se publicó al inicio en junio de 2008, pero tuvo una mejor variante en 2011 y ahora es válido desde 2018. De acuerdo a esto, el riesgo se define a la advertencia que puede explotar las vulnerabilidades de los activos y producir estragos. Este riesgo se relaciona a la aplicación, posesión, ejecución, disposición y acogida de

tecnología de la información por parte de la compañía. En este sentido, el indicador de riesgo indica si la empresa está expuesta o es muy probable a la exposición a riesgos superiores a su riesgo aceptable.

Kando (2018) afirma que, los expertos en protección encontraron varias vulnerabilidades en los servicios de geolocalización lo que podría facilitar que un atacante aproveche los datos confidenciales en muchísimos instrumentos de seguimiento de localización vía web, aprovechando de varios dispositivos inteligentes que tengan GPS incluyendo rastreadores de infantes, autos, mascotas, etc. lo cual permite a los propietarios rastrear su paradero. Estos riesgos incluyen claves sencillas de obtener, archivos expuestos, puntos finales de API no tan seguros y problemas tampoco seguros referentes directamente a objetos - IDOR. La explotación de estas vulnerabilidades permite que un tercero sin autorización o un pirata informático obtenga información privada seleccionada de cada dispositivo de seguimiento, incluido toda coordenada de GPS, número de teléfono, diseño y datos de la clase de dispositivo, números de IMEI, y cada nombre personalizado y más.

En este contexto, algunas empresas de transporte han incorporado el **sistema GPS** como herramienta tecnológica dentro de su organización para gestionar y analizar la información geográfica, procesar y visualizar mapas y gráficos del espacio de trabajo y, proporcionar sistemas de seguridad para el seguimiento de transporte por satélite con el fin de prevenir y controlar el alto riesgo que existe en el traslado de combustibles y/o materiales peligrosos. De este modo, la seguridad de los sistemas integrados por GPS, como es el caso del sistema de satélites, proporciona mayor calidad, eficacia y precisión.

Últimamente, estas empresas continuamente han mejorado en temas de seguridad de la información; pero todavía tienen algunas carencias (**problemas específicos**) mayormente en el manejo de riesgos informáticos vinculados al uso de dispositivos GPS en su labor cotidiana como son: disponer de permisos de acceso a la ubicación, mantener activada permanentemente la geolocalización, añadir la información de geolocalización a las fotografías y vídeos que se realiza, entre otras. La información asociada al transporte de algunos materiales es confidencial, y debe ser protegida de forma incesante; por lo cual, existen diversas herramientas y estándares que

permiten identificar problemas asociados a los riesgos de los mismos; por lo que, gestionar de forma adecuada la información por parte de las compañías permite garantizar el cumplimiento del servicio y la seguridad integral de los operadores que participan en el traslado.

Se instituyó la **formulación del problema**: *General:* ¿En qué condición el despliegue de la norma internacional ISO/IEC 27005:2018 infiere en la gestión de riesgos de seguridad de la información en dispositivos GPS en el año 2022? *Específicos:* Dificultad concreta 1 - ¿En qué condición el despliegue de la norma internacional ISO/IEC 27005:2018 infiere en la identificación de riesgos de seguridad de la información en dispositivos GPS en el año 2022? Dificultad concreta 2 - ¿En qué condición el despliegue de la norma internacional ISO/IEC 27005:2018 influye en la evaluación de riesgos de seguridad de la información en dispositivos GPS en el año 2022? Dificultad concreta 3 - ¿En qué condición el despliegue de la norma internacional ISO/IEC 27005:2018 infiere en el tratamiento de riesgos de seguridad de la información en dispositivos GPS en el año 2022?

Se instituyó la **justificación de la investigación**: *Conveniencia*, optimizó la gestión de riesgos de seguridad de la información en dispositivos electrónicos que usan GPS; *Relevancia social*, incluyó una ventaja comunitaria al disponer de ciudadanos más confiados en el manejo de la información en labores frecuentes utilizando servicios de GPS; *Utilidad metodológica*, fue sustento de subsiguientes exploraciones sobre administración de riesgos de seguridad de la información; *Implicancias prácticas*, hizo conocer las vulnerabilidades presentes en dispositivos GPS; *Valor teórico*, hizo comprender las bases teóricas respecto a seguridad de la información de dispositivos GPS y la norma internacional ISO/IEC 27005:2018.

Se instituyó los **objetivos**: *General*: Mejorar la gestión de riesgos de seguridad de la información en dispositivos GPS en el año 2022 mediante el despliegue de la norma internacional ISO/IEC 27005:2018; *Específicos*: Fin concreto 1 - Mejorar la identificación de riesgos de seguridad de la información en dispositivos GPS; Fin concreto 2 - Mejorar la evaluación de riesgos de

seguridad de la información en dispositivos GPS; Fin concreto 3 - Mejorar el tratamiento de riesgos de seguridad de la información en dispositivos GPS.

Se instituyó las **hipótesis**: *General:* “El despliegue de la norma internacional ISO/IEC 27005:2018 mejora significativamente la gestión de riesgos de seguridad de la información en dispositivos GPS en el año 2022”. *Específicas:* “El despliegue de la norma internacional ISO/IEC 27005:2018 mejora la identificación de riesgos de seguridad de la información en dispositivos GPS en el año 2022”; “El despliegue de la norma internacional ISO/IEC 27005:2018 mejora la evaluación de riesgos de seguridad de la información en dispositivos GPS en el año 2022”; “El despliegue de la norma internacional ISO/IEC 27005:2018 mejora el tratamiento de riesgos de seguridad de la información en dispositivos GPS en el año 2022”; “El despliegue de la norma internacional ISO/IEC 27005:2018 mejora el monitoreo de riesgos de seguridad de la información en dispositivos GPS en el año 2022”.

## II. MARCO TEÓRICO

En este estudio se halló un grupo de **antecedentes** (ya sean artículos científicos y/o trabajos investigativos) permitiendo saber de estudios anteriores a la problemática definida en el primer capítulo como:

Patel & Zambrano (2020) en su estudio titulado “Auditoría de seguridad informática en base a la normativa ISO 27005:2013 para descubrir y aprovechar debilidades en una red de gestión emulada para una compañía prestadora de servicios” tuvo como finalidad establecer la vulnerabilidad de cada sistema de datos que posee la empresa a través del estándar ISO 27005:2013. El método aplicado fue de cascada a través de 5 etapas (Descubrir, Explorar, Evaluar, Intervenir y Reportar) que reconocían las vulnerabilidades. Se identificó que la compañía tenía sistemas Windows sin actualización y que podrían ser una ventaja para los crackers. En conclusión, se demostró que el ISO27005 sirve para disminuir las incidencias de protección en toda la red de administración.

Sánchez (2022) en su estudio titulado “Diseño de una propuesta sobre el uso de un SGSI para la compañía de transporte ecuatoriana bajo la normativa ISO 27005” tuvo como finalidad diseñar un proyecto sobre el sistema de manejo de protección de datos en base a la norma ISO 27005 y así manejar la información de una empresa de transportes. Se empleó un método analítico para clasificar y examinar el sistema de información mediante el método MAGERIT y el enfoque PHVA. Como resultado se obtuvo que la propuesta de un sistema de información bajo la norma 27005:2013 permite optimizar la seguridad de los datos informativos con el fin de dar seguridad y defender cada bien de la compañía. Concluyendo que la información en una empresa es un activo importante para su funcionamiento, por lo tanto, es fundamental implementar mecanismos de control para salvaguardar la información de amenazas.

Dávila y Dextre (2021) en su estudio realizó una gestión de toda vulnerabilidad para contribuir en alcanzar un buen nivel de protección de datos en el centro de salud AMC, la metodología fue cuantitativa descriptiva para analizar cualquier escenario y situaciones que facilitan vulnerabilidades del sistema de información. Concluyendo, que la implementación de un manejo

de vulnerabilidades en el centro de salud AMC contribuye al manejo de vulnerabilidades en el parque informático.

Risco (2021) en su estudio estableció cómo influye un sistema de manejo para la protección de datos basado en la normativa 27005:2013 en una compañía que se dedica a la construcción. El método empleado fue cuantitativo aplicado, con un modelo preexperimental. También, se empleó registros para determinar las mejoras. Como resultado se logró incrementar la seguridad de las dimensiones en un 80%. Concluyendo que el sistema de manejo con la normativa contribuye favorablemente en la protección de la organización.

Hernández (2020) en su investigación tuvo como objetivo principal el diseño de un proyecto de manejo en la protección de datos según la norma ISO 27005 para una organización para determinar que se controle internamente la seguridad. La metodología empleada fue mediante la recolección de información por encuestas o reuniones, seguidamente se estableció 3 fases para conocer el diagnostico, planificación y desarrollo. Como resultado, se halló que esta compañía, no contaba con un sistema de protección biométrica o de control que facilitara el control de acceso y salida de los usuarios. Concluyendo, que el uso de un proyecto de manejo de protección permitía mayor control del sistema administrativo, y una apropiada gestión de riesgos que afectan a la información.

A fin de comprender mejor la exploración propuesta, se necesitó el estudio de un grupo de **bases teóricas** como:

*Norma internacional ISO/IEC 27005*: Definida al grupo de normas que determinan una orientación sistemática para el manejo de riesgos de protección de datos necesarios para reconocer las demandas empresariales referentes a los requerimientos de protección de datos y crear un proyecto de manejo eficaz para ello. Dicha normativa internacional también es acorde con los conceptos de ISO/IEC 27001 y tiene como objetivo respaldar la implantación efectiva de protección de datos en base a un planteamiento de manejo de riesgos. Con la certificación ISO/IEC 27005, obtendrá las capacidades y el aprendizaje que se requiere al comenzar a implementar el modo de administrar los posibles daños en el cuidado de la data. Por tanto,

debe poder identificar, apreciar, examinar, valorar y abordar diversos riesgos de protección de los datos en que está expuesta su empresa (PECB, 2020).

*Gestión de riesgos de seguridad de la información*: Definido en actividades recurrentes enfocadas a analizar, planificar, implementar, gestionar y monitorear todas las contramedidas y políticas de seguridad implementadas contra los riesgos de protección de datos. El reajuste de la definición, sostenimiento y mejoramiento continuo de un proyecto de manejo de protección de datos puede demostrar que cada compañía utiliza una proyección sistemática a situar, examinar y administrar los peligros de protección de datos. En cuanto a identificar riesgos, un evento se convierte en riesgo sólo si existe cierto grado de incertidumbre. Los valores de los activos pueden cambiar durante la implementación del proyecto, pero ¿hasta qué punto es probable que cambie?, por tanto, en proyectos pequeños se debe evitar el riesgo. Necesitamos asegurarnos de que estamos viendo la realidad del riesgo, no las causas y consecuencias. Los ejemplos de riesgos de TI incluyen: Sistemas operativos que son vulnerables y no están actualizados. Diseño de aplicación deficiente e incompleto, incluidos errores y errores recurrentes, tecnología obsoleta, bajo rendimiento de la infraestructura de TI; Cuando se trata de la evaluación de riesgos, debe correlacionar los escenarios de riesgo de TI con sus implicaciones comerciales para comprender el impacto de los posibles eventos adversos. Las evaluaciones de riesgos se realizan discretamente en el periodo y brindan una descripción general temporal de los riesgos evaluados hasta que se realiza la siguiente evaluación. Las evaluaciones de riesgos a menudo se realizan en múltiples iteraciones, la primera iteración realiza una valoración de gran nivel para reconocer los riesgos mayores y las siguientes repeticiones realizan un estudio detallado de los riesgos grandes y aceptables. Múltiples elementos apoyan a escoger eventualidades que tengan un nivel de riesgo: Probabilidades; Consecuencia; Ocurrencias; Urgencias; Maleabilidad; Dependencias; Proximidad (SSI, 2017).

*Dispositivos GPS*: Se define como un dispositivo que funciona a través de satélites que transmiten señales de radio que contienen datos de cada ubicación. Además, te informa sobre el estado actual y la hora exacta. Esto

es gracias al reloj atómico a bordo. Todas las señales de radio transmitidas por satélites se trasladan por intermedio del espacio a la rapidez de la luz aproximadamente, o alrededor de 300 000 km/s. Un dispositivo GPS que se mueve hacia la Tierra recibe señales de radio de los satélites y comienza a "registrar" la hora exacta en que esas señales llegaron al dispositivo. Esta información es la base para calcular la distancia a los satélites dentro de la línea de visión. Al final, una vez que el dispositivo GPS ha determinado su distancia a por lo menos cuatro satélites, usa la geometría para determinar su posición en la tierra en tres dimensiones (Fernández, 2020).

Además, se tuvo un grupo de **enfoques conceptuales** donde se sustentaba el estudio como:

*Geolocalización*: Consiste en encontrar la ubicación geográfica de objetos como teléfonos móviles, automóviles, carreteras. Puede usar una variedad de métodos para hacer esto, como la codificación de su correo postal, la dirección IP de su computadora o el sistema de geolocalización de su teléfono celular. El Sistema de posicionamiento global se utiliza para determinar la ubicación geográfica aproximada de su teléfono inteligente. El sistema consiste en una red de satélites geoestacionarios que cubren todo el globo. Para obtener su posición, el dispositivo se conecta a por lo menos tres satélites y recibe identificadores y tiempos respectivos de estos satélites. Este mecanismo calcula el tiempo en que la señal del satélite demora en llegar, además debido a la demora o delay resultante se determina la localización mediante triangulación (OSI, 2016).

*Amenaza*: Situación en la que ocurre una incidencia dentro de una organización, que causa daños graves o pérdidas menores a los activos de información. Un proyecto de manejo de protección de datos sostenidas en la ISO 27001 ayuda a monitorear las intimidaciones que puedan causar incidencias (ISO 27001, 2020).

*Vulnerabilidad*, Son fragilidades del activo las que podrían ser aprovechadas por un peligro para concretar un ataque hacia el activo. Además, es una potencialidad o eventualidad en que se concrete la intimidación a ese activo (ISO 27001, 2020).

*Riesgo:* posibilidad en que un peligro se transforme en una catástrofe. La vulnerabilidad y amenaza cada una no es peligrosa por sí sola; sin embargo, si van juntas conciben un riesgo: el potencial de un desastre (ISO 27001, 2020).

*Parches de seguridad: S*on actualizaciones que se acumulan y están destinadas a corregir las vulnerabilidades de la computadora. Cada sistema operativo presenta fragilidades en la seguridad y la forma de darle solución es con actualizaciones de dicho sistema que contengan esos parches o correcciones (Fernández, 2020).

*Problemas de seguridad*: Hay muchos tipos de problemas de incompatibilidad causados por actualizaciones importantes que los sistemas operativos reciben dos veces anualmente, u otro problema de compatibilidad con otros, ya sea con el hardware o el software. Además podría ser una vulnerabilidad o un problema de seguridad. Todo sistema operativo tiene alguna vulnerabilidad y urge reparar ya que otro pueda explotarlas anteriormente (XATACA, 2020).

En tanto a los **métodos y normativas globales alternativas** para la implementación de la solución tecnológica ofrecida; actualmente, se cuenta con algunos métodos estándar y normas internacionales para la implantación de proyectos de protección de la información, tales como:

*Metodología MAGERIT v3*, se trata de un método de estudio y manejo de peligros a nivel público, de uso gratuito y que no requiere aprobación previa. Es de interés de las empresas dentro del Esquema Nacional de Seguridad (ENS), el cumplimiento de los principios del manejo de protección en base a riesgos y los requerimientos de estudio y manejo de riesgos, dadas sus dependencias de la tecnología de información para realizar tareas, prestar servicios y lograr objetivos comerciales. Concluyendo, MAGERIT implanta procesos de manejo de peligros en un ámbito a fin de que los organismos gubernamentales consideren y tomen decisiones sobre los peligros que se generan del despliegue de la tecnología informática (PAE, 2018).

*Norma internacional ISO 27005:2018*, norma acerca de tecnología de la información, técnica y manejo de la protección de datos, otorga orientación a

las organizaciones sobre cómo abordar estos requisitos al tiempo que otorga un marco para gestionar de manera eficaz los riesgos referentes con la protección de datos. Recientemente se actualizó una nueva versión, ISO/IEC 27005, que contiene requisitos para los programas de administración segura, para cumplir con ISO/IEC 27001 y satisfacer las demandas de las organizaciones más exigentes de la actualidad. La norma ISO/IEC 27005:2018 ha sido revisada para actualizarla y satisfacer las demandas de la sociedad actual. Proteger la información corporativa, ya sea la confidencialidad comercial o los datos de los clientes, nunca ha estado en el centro de atención (ISOTools, 2018).

*Norma internacional ISO/IEC 27002:2013*, compuesta de catorce (14) zonas de vigilancia, en la cual la mitad solamente manejan temas de protección informática como: Manejo de activos, focalizada en atender la información como recurso y en cómo deberían resolverse las medidas apropiadas para almacenarlos de los incidentes, quiebras en la protección y en el cambio no deseado; Control de ingreso, se controla a los que accedan a datos en una postura importante. Además no siempre el personal de una empresa necesita ingresar a toda la información para llevar a cabo su tarea diaria, solo que tendremos roles que necesitan un mayor ingreso y otros con un ingreso restringido. Para marcar las diferencias, deben determinar cada control en registros de cada usuario, manejo de las concesiones de ingreso, etc. es por ello que el monitoreo se incorpora en esta sección; Criptografía, si la información es confidencial o importante, puede ser de interés utilizar diversas métodos criptográficos para respaldar y asegurar su autenticidad, confidencialidad e integridad; Seguridad física y del entorno, la protección no es técnica solamente, también es física, así que el simple hecho de no tener pantallas e impresoras en áreas de fácil acceso por personal externo no solo maneja bien la seguridad, sino que eventualmente se convierte en un hábito que conduce a una gestión más eficiente; Seguridad de las operaciones, hay un fuerte elemento técnico en cada aspecto a disposición: seguridad contra malware, réplicas de protección, monitoreo sobre el software que utiliza, manejo de vulnerabilidades, etc.; Seguridad de las comunicaciones, basado en casi todas las interacciones de información y datos en diferentes niveles

se realizan mediante las redes sociales, lo que asegura la protección apropiadamente de la vía de emisión de estos importantes datos; obtención, despliegue y sostenimiento de cada sistema informatizado, la protección no es tema de una zona o proceso específico, ni es general, debe abarcar a toda la empresa y existir como un componente transverso importante en el periodo de vida de un proyecto de gestión (ISO Tools Excellence, 2016).

Basado en tres métodos/normas internacionales postulantes, se decidió por usar el **mecanismo de evaluación especializada** para la selección de la mejor conveniente ganando la normativa internacional ISO/IEC 27005:2018 - ver Anexo 3.

# III. METODOLOGÍA

## 3.1. Tipo y diseño de investigación

- Tipo de investigación

  *Aplicada* en el sentido que usa mecanismos probados y usados en soluciones informáticas empresariales.

- Diseño de investigación

  *Preexperimental* en el sentido que recurre a la experimentación sencilla con el uso de un único grupo de control.

## 3.2. Variables y operacionalización

- Variables

  - Independiente: Norma internacional ISO/IEC 27005:2018

    - Definición conceptual:

      "Conjunto de lineamientos para el establecimiento de un enfoque sistemático de administración de peligros de información segura" (PECB, 2020).

    - Definición operacional:

      La norma internacional ISO/IEC 27005:2018 se puede medir a través de la implementación y gestión eficaz de un proceso de gestión del riesgo de la seguridad de la información en una organización.

  - Dependiente: Gestión de riesgos de seguridad de la información

    - Definición conceptual:

      "Actividad recurrente enfocada al estudio, a la proyección, la realización, el monitoreo y el rastreo de las acciones desplegadas y la directiva de seguridad de peligros en información segura" (SSI, 2017).

- Definición operacional:

  La administración de peligros de información segura se puede medir por la identificación, evaluación, y tratamiento de los mismos.

- Operacionalización

La operatividad de las variables de visualizan en el tablero matricial en el segundo anexo del vigente informe.

## 3.3. Población, muestra y muestreo

- Población (N)

Está conformada por los usuarios (colaboradores) que trabajan en la compañía elegida y que son garantes de forma directa e indirecta de la administración de peligros.

**Tabla 1**. *Población*

| Cargo / Puesto | Cantidad |
|---|---|
| Gerente general | 1 |
| Jefe de área | 3 |
| Operario | 6 |
| Total | 10 |

Fuente: (Elaboración propia, 2022)

$$N = 10\ personas$$

- Muestra (n)

Siendo la población inferior a 30, se deduce que la muestra fue semejante a la población. Se tuvo entonces:

$$n = N = 10\ personas$$

- Muestreo

De clase no probabilística debido a que se manipula la deliberación de la muestra poblacional.

## 3.4. Técnicas e instrumentos de recolección de datos

- Técnicas:

  Se recurrió a los mecanismos técnicos de absorción de la data empresarial como:

  - Encuesta.
  - Análisis documental.

- Instrumentos:

  Se recurrió a los mecanismos instrumentales de absorción de la data empresarial como:

  - Cuestionario.
  - Ficha de datos.

## 3.5. Procedimientos

Las actividades que se realizaron para dar cumplimiento a la efectivización de los fines concretos planteados fueron:

- Fin concreto 1: Mejorar la identificación de riesgos de seguridad de la información en dispositivos GPS

  Se uso mecanismos técnicos de absorción de la opinión de los usuarios de la compañía seleccionada como fue el caso de la Encuesta recurriendo en todo instante a mecanismos instrumentales de registro de la opinión de los mismos como fue el caso del Cuestionario en referencia a la identificación de riesgos de seguridad de la información en dispositivos GPS (ver Anexo 4).

- Fin concreto 2: Mejorar la evaluación de riesgos de seguridad de la información en dispositivos GPS

  Se uso mecanismos técnicos de absorción de la opinión de los usuarios de la compañía seleccionada como fue el caso de la

Encuesta recurriendo en todo instante a mecanismos instrumentales de registro de la opinión de los mismos como fue el caso del Cuestionario en referencia a la evaluación de riesgos de seguridad de la información en dispositivos GPS (ver Anexo 4).

- Fin concreto 3: Mejorar el tratamiento de riesgos de seguridad de la información en dispositivos GPS

  Se uso mecanismos técnicos de absorción de la opinión de los usuarios de la compañía seleccionada como fue el caso de la Encuesta recurriendo en todo instante a mecanismos instrumentales de registro de la opinión de los mismos como fue el caso del Cuestionario en referencia al tratamiento de riesgos de seguridad de la información en dispositivos GPS (ver Anexo 4).

## 3.6. Método de análisis de datos

Se recurrió al mecanismo estadístico para desarrollar el componente descriptivo y el componente inferencial en el tratamiento y estudio de la data empresarial absorbida.

El mecanismo estadístico descriptivo buscó hacer una comparativa visual (a nivel gráfico y tabular) de los escenarios iniciales y finales con respecto al uso de la solución técnica ofrecida.

El mecanismo estadístico inferencial buscó hacer un cálculo de operación normalizada a fin de determinar el comportamiento de cada indicador (paramétrico y no paramétrico) con respecto a las variables inmersas en el estudio.

## 3.7. Aspectos éticos:

Hubo en todo momento respeto por la originalidad de la investigación (sistema Turnitin), los principios morales del reglamento de ética de la Universidad y el uso de normas bibliográficas como ISO-690.

# IV. RESULTADOS

- **Análisis descriptivo**
  - Primer indicador:

**Tabla 2.** *Análisis descriptivo del primer indicador*

**Estadísticos descriptivos**

| | N | Mínimo | Máximo | Media | Desv. Desviación |
|---|---|---|---|---|---|
| IRSI-Preprueba | 10 | 1,20 | 1,70 | 1,5030 | ,16841 |
| IRSI-Posprueba | 10 | 4,30 | 4,90 | 4,8026 | ,15274 |
| N válido (por lista) | 10 | | | | |

Fuente: (Elaboración propia, 2022)

Como se aprecia en la tabla precedente, la identificación de riesgos de seguridad de la información anterior al despliegue de la norma internacional ISO 27005:2018 poseía un promedio estadístico de 1.50 puntos y subsiguiente al despliegue de la norma internacional ISO 27005:2018 posee un promedio estadístico de 4.80 puntos, logrando un acrecentamiento de 3.30 puntos (Δ 66.00%).

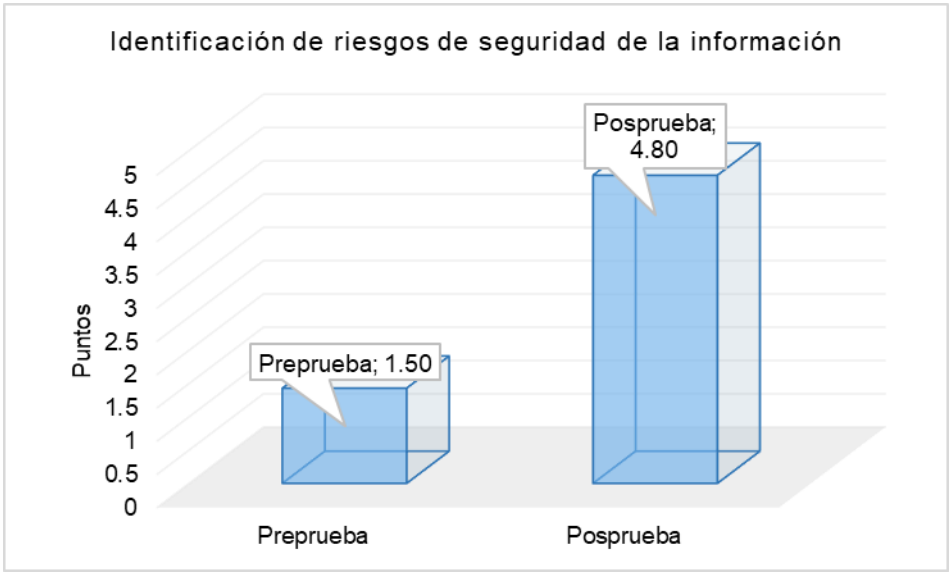



*Figura 1.* Medias de preprueba y posprueba del primer indicador.

- Segundo indicador:

**Tabla 3.** *Análisis descriptivo del segundo indicador*

Estadísticos descriptivos

| | N | Mínimo | Máximo | Media | Desv. Desviación |
|---|---|---|---|---|---|
| ERSI-Preprueba | 10 | 1,38 | 1,92 | 1,5832 | ,14725 |
| ERSI-Posprueba | 10 | 4,15 | 4,85 | 4,6471 | ,15687 |
| N válido (por lista) | 10 | | | | |

Fuente: (Elaboración propia, 2022)

Como se aprecia en la tabla precedente, la evaluación de riesgos de seguridad de la información anterior al despliegue de la norma internacional ISO 27005:2018 poseía un promedio estadístico de 1.58 puntos y subsiguiente al despliegue de la norma internacional ISO 27005:2018 posee un promedio estadístico de 4.65 puntos, logrando un acrecentamiento de 3.07 puntos (Δ 61.40%).

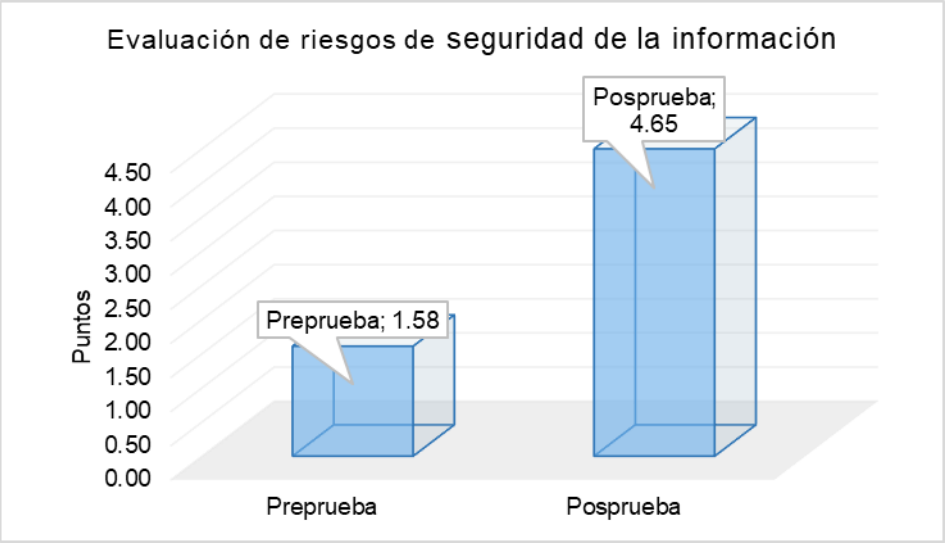



*Figura 2.* Medias de preprueba y posprueba del segundo indicador.

- Tercer indicador

**Tabla 4.** *Análisis descriptivo del tercer indicador.*

Estadísticos descriptivos

| | N | Mínimo | Máximo | Media | Desv. Desviación |
|---|---|---|---|---|---|
| TRSI-Preprueba | 10 | 1,45 | 1,90 | 1,7025 | ,16374 |
| TRSI-Posprueba | 10 | 4,25 | 4,80 | 4,7470 | ,17825 |
| N válido (por lista) | 10 | | | | |

Fuente: (Elaboración propia, 2022)

Como se aprecia en la tabla precedente, el tratamiento de riesgos de seguridad de la información anterior al despliegue de la norma internacional ISO 27005:2018 poseía un promedio estadístico de 1.70 puntos y subsiguiente al despliegue de la norma internacional ISO 27005:2018 posee un promedio estadístico de 4.75 puntos, logrando un acrecentamiento de 2.95 puntos (Δ 59.00%).

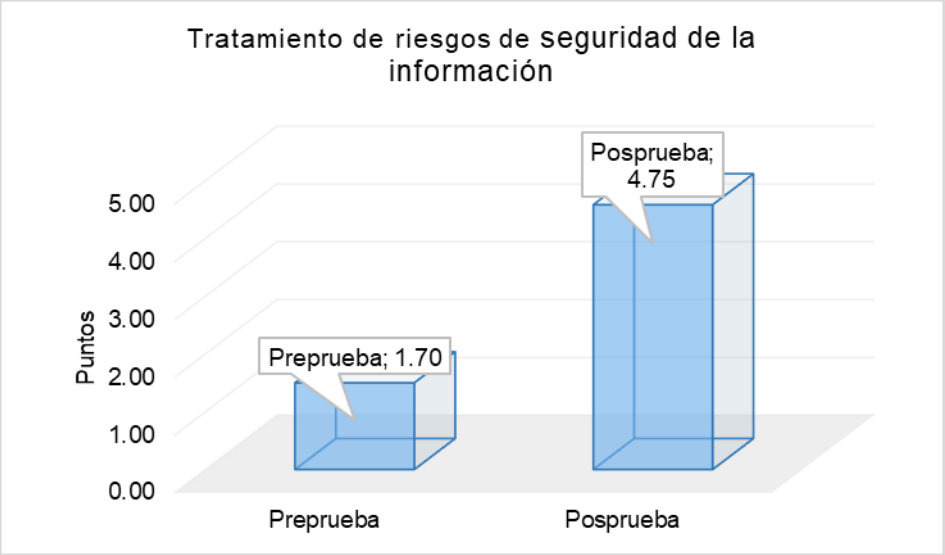



*Figura 3.* Medias de preprueba y posprueba del tercer indicador.

- **Análisis inferencial**

Los exámenes estadísticos usados para determinar la normalidad por indicador se basaron en el test de Shapiro-Wilk (muestra ≤ 50).

- Primer indicador:

$H_0$: “La identificación de los riesgos de seguridad de la información (sin el despliegue de la norma internacional ISO 27005:2018) si tiene reparto normal”.

$H_1$: “La identificación de los riesgos de seguridad de la información (sin el despliegue de la norma internacional ISO 27005:2018) no tiene reparto normal”.

$H_0$: “La identificación de los riesgos de seguridad de la información (con el despliegue de la norma internacional ISO 27005:2018) no tiene reparto normal”.

$H_1$: “La identificación de los riesgos de seguridad de la información (con el despliegue de la norma internacional ISO 27005:2018) si tiene reparto normal”.

Se tuvo como importe de significancia: α = 0.05

Importe de Sig. > 0.05, se acoge la teoría denegada ($H_0$).
Importe de Sig. <= 0.05, se acoge la teoría afirmada ($H_1$).

**Tabla 5.** *Prueba de normalidad del primer indicador*

| | Shapiro-Wilk | | |
|---|---|---|---|
| | Estadístico | gl | Sig. |
| IRSI-PrePrueba | ,795 | 10 | ,047 |
| IRSI-PosPrueba | ,826 | 10 | ,262 |

Fuente: (Elaboración Propia, 2022)

Con respecto a la tabla precedente**,** el importe de significancia en condición preprueba fue 0.047 (≤ 0.05); mientras que el mismo importe de significancia en condición posprueba fue 0.262 (> 0.05). Por lo que, al examinar ambos resultados, se estableció que, no había presencia de un reparto normal, lo que implicó el uso del examen no paramétrica de Wilcoxon.

- Segundo indicador:

  $H_0$: “La evaluación de los riesgos de seguridad de la información (sin el despliegue de la norma internacional ISO 27005:2018) si tiene reparto normal”.

  $H_1$: “La evaluación de los riesgos de seguridad de la información (sin el despliegue de la norma internacional ISO 27005:2018) no tiene reparto normal”.

  $H_0$: “La evaluación de los riesgos de seguridad de la información (con el despliegue de la norma internacional ISO 27005:2018) no tiene reparto normal”.

  $H_1$: “La evaluación de los riesgos de seguridad de la información (con el despliegue de la norma internacional ISO 27005:2018) si tiene reparto normal”.

  Se tuvo como importe de significancia: $\alpha = 0.05$

  Importe de Sig. > 0.05, se acoge la teoría denegada ($H_0$).

  Importe de Sig. <= 0.05, se acoge la teoría afirmada ($H_1$).

**Tabla 6.** *Prueba de normalidad del indicador 2*

| | Shapiro-Wilk | | |
|---|---|---|---|
| | Estadístico | gl | Sig. |
| ERSI-Preprueba | ,953 | 10 | ,042 |
| ERSI-Posprueba | ,845 | 10 | ,243 |

Fuente: (Elaboración Propia, 2022)

Con respecto a la tabla precedente**,** el importe de significancia en condición preprueba fue 0.042 (≤ 0.05); mientras que el mismo importe de significancia en condición posprueba fue 0.243 (> 0.05). Por lo que, al examinar ambos resultados, se estableció que, no había presencia de un reparto normal, lo que implicó el uso del examen no paramétrica de Wilcoxon.

- Tercer indicador:

$H_0$: “El tratamiento de los riesgos de seguridad de la información (sin el despliegue de la norma internacional ISO 27005:2018) si tiene reparto normal”.

$H_1$: “El tratamiento de los riesgos de seguridad de la información (sin el despliegue de la norma internacional ISO 27005:2018) no tiene reparto normal”.

$H_0$: “El tratamiento de los riesgos de seguridad de la información (con el despliegue de la norma internacional ISO 27005:2018) no tiene reparto normal”.

$H_1$: “El tratamiento de los riesgos de seguridad de la información (con el despliegue de la norma internacional ISO 27005:2018) si tiene reparto normal”.

Se tuvo como importe de significancia: α = 0.05

Importe de Sig. > 0.05, se acoge la teoría denegada ($H_0$).

Importe de Sig. <= 0.05, se acoge la teoría afirmada ($H_1$).

**Tabla 7.** *Prueba de normalidad del tercer indicador*

| | Shapiro-Wilk | | |
|---|---|---|---|
| | Estadístico | gl | Sig. |
| TRSI-PrePrueba | ,924 | 10 | ,048 |
| TRSI-PosPrueba | ,861 | 10 | ,215 |

Fuente: (Elaboración Propia, 2022)

Con respecto a la tabla precedente**,** el importe de significancia en condición preprueba fue 0.048 (≤ 0.05); mientras que el mismo importe de significancia en condición posprueba fue 0.215 (> 0.05). Por lo que, al examinar ambos resultados, se estableció que, no había presencia de un reparto normal, lo que implicó el uso del examen no paramétrica de Wilcoxon.

- **Contrastación de hipótesis**

Dado que, las muestras poblacionales no poseían un reparto normal, se optó por usar el examen no paramétrico de Wilcoxon.

- Teoría concreta 1:

"El despliegue de la norma internacional ISO 27005:2018 mejora la identificación de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

Teorías estadísticas:

$H_0$: "El despliegue de la norma internacional ISO 27005:2018 no mejora la identificación de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

$$H_0: IRSIa >= IRSIp$$

$H_1$: "El despliegue de la norma internacional ISO 27005:2018 si mejora la identificación de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

$$H_1: IRSIa < IRSIp$$

Se tuvo como importe de significancia: $\alpha = 0.05$

Importe de Sig. > 0.05, se acoge la teoría denegada ($H_0$).

Importe de Sig. <= 0.05, se acoge la teoría afirmada ($H_1$).

**Tabla 8.** *Prueba Wilcoxon para el primer indicador*

Estadísticos de prueba[a]

| | IRSI-Posprueba - IRSI-Posprueba |
|---|---|
| Z | -1,633[b] |
| Sig. asintótica(bilateral) | ,024 |

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: (Elaboración propia, 2022)

El importe de significancia fue 0.024 (≤ 0.05) desestimando la teoría denegada y acogiendo la teoría afirmada. Ello infirió: "El despliegue de la norma internacional ISO 27005:2018 si mejora de manera cuantiosa la identificación de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

- Teoría concreta 2:

"El despliegue de la norma internacional ISO 27005:2018 mejora la evaluación de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

Teorías estadísticas:

$H_0$: "El despliegue de la norma internacional ISO 27005:2018 no mejora la evaluación de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

$$H_0: ERSIa >= ERSIp$$

$H_1$: "El despliegue de la norma internacional ISO 27005:2018 si mejora la evaluación de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

$$H_1: ERSIa < ERSIp$$

Se tuvo como importe de significancia: $\alpha = 0.05$

Importe de Sig. > 0.05, se acoge la teoría denegada ($H_0$).

Importe de Sig. <= 0.05, se acoge la teoría afirmada ($H_1$).

**Tabla 9.** *Prueba Wilcoxon para el segundo indicador*

Estadísticos de prueba[a]

| | ERSI-Posprueba - ERSI-Posprueba |
|---|---|
| Z | -1,914[b] |
| Sig. asintótica(bilateral) | ,032 |

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: (Elaboración propia, 2022)

El importe de significancia resultante fue 0.032 (≤ 0.05) desestimando la teoría denegada y acogiendo la teoría afirmada. Ello infirió: "El despliegue de la norma internacional ISO 27005:2018 si mejora de manera cuantiosa la evaluación de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

- Teoría concreta 3:

"El despliegue de la norma internacional ISO 27005:2018 mejora la evaluación de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

Teorías estadísticas:

$H_0$: "El despliegue de la norma internacional ISO 27005:2018 no mejora el tratamiento de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

$$H_0: TRSIa >= TRSIp$$

$H_1$: "El despliegue de la norma internacional ISO 27005:2018 si mejora el tratamiento de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

$$H_1: TRSIa < TRSIp$$

Se tuvo como importe de significancia: $\alpha = 0.05$

Importe de Sig. > 0.05, se acoge la teoría denegada ($H_0$).
Importe de Sig. <= 0.05, se acoge la teoría afirmada ($H_1$).

**Tabla 10.** *Prueba Wilcoxon para el tercer indicador*

Estadísticos de prueba[a]

| | TRSI-Posprueba - TRSI-Posprueba |
|---|---|
| Z | -1,832[b] |
| Sig. asintótica(bilateral) | ,046 |

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: (Elaboración propia, 2022)

El importe de significancia resultante fue 0.046 (≤ 0.05) desestimando la teoría denegada y acogiendo la teoría afirmada. Ello infirió: "El despliegue de la norma internacional ISO 27005:2018 si mejora de manera cuantiosa el tratamiento de riesgos de seguridad de la información en dispositivos GPS en el año 2022".

## V. DISCUSIÓN

En lo concerniente al primer indicador: “Identificación de riesgos de seguridad de la información”, los importes estadísticos resultantes antepuesto y subsiguiente al despliegue de la solución fueron 1.50 y 4.80 puntos respectivamente, logrando un acrecentamiento de 3.30 puntos (∆ 66.00%). Estos logros fueron parecidos a los conseguidos por (Patel & Zambrano, 2020), quienes en su estudio establecieron la vulnerabilidad de cada sistema de datos que posee la empresa a través del estándar ISO 27005:2013. El método aplicado fue de cascada a través de 5 etapas (Descubrir, Explorar, Evaluar, Intervenir y Reportar) que reconocían las vulnerabilidades. Se identificó que la compañía tenía sistemas Windows sin actualización y que podrían ser una ventaja para los crackers. En conclusión, se demostró que el ISO27005 sirve para disminuir las incidencias de protección en toda la red de administración. En el mismo sentido, son parecidos a los conseguidos por (Sánchez, 2022), quien en su estudio obtuvo que la propuesta de un sistema de información bajo la norma 27005:2013 permite optimizar la seguridad de los datos informativos con el fin de dar seguridad y defender cada bien de la compañía. Concluyendo que la información en una empresa es un activo importante para su funcionamiento, por lo tanto, es fundamental implementar mecanismos de control para salvaguardar la información de amenazas. El sustento teórico de lo sucedido anteriormente, se basa en las bases teóricas de la norma internacional ISO 27005:2018 que promueve las capacidades y el aprendizaje que se requiere al comenzar a implementar el procedimiento de administración de peligros de protección de datos. Por tanto, debe poder identificar, apreciar, examinar, valorar y abordar diversos riesgos de protección de los datos en que está expuesta su empresa (PECB, 2020).

En lo concerniente al segundo indicador: “Evaluación de riesgos de seguridad de la información”, los importes estadísticos resultantes antepuesto y subsiguiente al despliegue de la solución fueron 1.58 y 4.65 puntos respectivamente, logrando un acrecentamiento de 3.07 puntos (∆ 61.40%). Estos logros fueron parecidos a los conseguidos por (Dávila & Dextre, 2021), quienes en su estudio realizaron una gestión de toda vulnerabilidad para contribuir en alcanzar un buen nivel de protección de datos en el centro de

salud AMC, la metodología fue cuantitativa descriptiva para analizar cualquier escenario y situaciones que facilitan vulnerabilidades del sistema de información. Concluyendo, que la implementación de un manejo de vulnerabilidades en el centro de salud AMC contribuye al manejo de vulnerabilidades en el parque informático. En el mismo sentido, son parecidos a los conseguidos por (Risco, 2021), quien en su estudio estableció cómo influye un sistema de manejo para la protección de datos basado en la normativa 27005:2013 en una compañía que se dedica a la construcción. El método empleado fue cuantitativo aplicado, con un modelo preexperimental. También, se empleó registros para determinar las mejoras. Como resultado se logró incrementar la seguridad de las dimensiones en un 80%. Concluyendo que el sistema de manejo con la normativa contribuye favorablemente en la protección de la organización. El sustento teórico de lo sucedido anteriormente, se basa en las bases teóricas de la norma internacional ISO 27005:2018 que promueve las capacidades y el aprendizaje que se requiere al comenzar a implementar el procedimiento de administración de peligros de protección de datos. Por tanto, debe poder identificar, apreciar, examinar, valorar y abordar diversos riesgos de protección de los datos en que está expuesta su empresa (PECB, 2020).

En lo concerniente al tercer indicador: “Tratamiento de riesgos de seguridad de la información”, los importes estadísticos resultantes antepuesto y subsiguiente al despliegue de la solución fueron 1.70 y 4.75 puntos respectivamente, logrando un acrecentamiento de 2.88 puntos ($\Delta$ 61.80%). Estos logros fueron parecidos a los conseguidos por (Hernández, 2020), quien en su estudio halló que esta compañía, no contaba con un sistema de protección biométrica o de control que facilitara el control de acceso y salida de los usuarios. Concluyendo, que el uso de un proyecto de manejo de protección permitía mayor control del sistema administrativo, y una apropiada gestión de riesgos que afectan a la información. El sustento teórico de lo sucedido anteriormente, se basa en las bases teóricas de la norma internacional ISO 27005:2018 que promueve las capacidades y el aprendizaje que se requiere al comenzar a implementar el procedimiento de administración de peligros de protección de datos (PECB, 2020).

## VI. CONCLUSIONES

1. Se obtuvo una mejora de la identificación de los riesgos de seguridad de la información en dispositivos GPS en el año 2022 logrando importes estadísticos resultantes antepuesto y subsiguiente al despliegue de la norma internacional ISO 27005:2018 de 1.50 y 4.80 puntos respectivamente, logrando un acrecentamiento de 3.30 puntos (Δ 66.00%).
2. Se obtuvo una mejora de la evaluación de los riesgos de seguridad de la información en dispositivos GPS en el año 2022 logrando importes estadísticos resultantes antepuesto y subsiguiente al despliegue de la norma internacional ISO 27005:2018 de 1.58 y 4.65 puntos respectivamente, logrando un acrecentamiento de 3.07 puntos (Δ 61.40%).
3. Se obtuvo una mejora del tratamiento de los riesgos de seguridad de la información en dispositivos GPS en el año 2022 logrando importes estadísticos resultantes antepuesto y subsiguiente al despliegue de la norma internacional ISO 27005:2018 de 1.50 y 4.80 puntos respectivamente, logrando un acrecentamiento de 3.30 puntos (Δ 66.00%).

## VII. RECOMENDACIONES

A los Directivos de la empresa de transporte:

Se pide la ejecución de la solución técnica ofrecida tal y como se ha planteado en la investigación desarrollada, toda vez que es importante que los requerimientos informáticos sugeridos sean cumplidos a cabalidad.

Al Jefe de informática:

Se pide optimizar la solución técnica ofrecida considerando alternativa de automatización para la administración de riesgos de información segura en dispositivos GPS.

Al Jefe de personal:

Se pide sensibilizar en buenas prácticas de seguridad a los trabajadores de la compañía elegida, puesto que son ellos quienes representan los actores principales afectados de la administración de peligros de información segura en dispositivos GPS.

Al personal operario:

Se pide respetar y ejecutar todas las recomendaciones que brinda la norma internacional ISO/IEC 27005:2018 a fin de lograr un beneficio efectivo en el uso de los dispositivos GPS.

**REFERENCIAS**


Dávila, A., & Dextre, J. (2021). *"Propuesta de una implementación de un programa de gestión de vulnerabilidades de seguridad informática para mitigar los siniestros de la información en el policlínico de salud AMC alineado a la NTP-ISO/IEC 27001:2014 en la ciudad de Lima - 2021".* Lima: UTP.

Fernández, L. (4 de Abril de 2020). Obtenido de https://www.redeszone.net/tutoriales/seguridad/amenazas-privacidad-gps/

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

Hernández, A. (2020). *"Diseño de un sistema de gestión de seguridad de la información de acuerdo a la norma ISO 27005 para el caso estudio de la compañía QWERTY S.A".* Bogotá: UNAD.

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 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/

Kando, E. (4 de Enero de 2018). *Sistemas de Localización GPS expuestos a Riesgos Cibernéticos*. Obtenido de https://wiseplant.com/cientos-de-sistemas-de-localizacion-gps-expuestos-a-riesgos-ciberneticos/

Novoa, G. (1 de Enero de 2020). *Qué es el GPS y para qué puede usarse en seguridad*. Obtenido de https://www.gestiondelriesgo.com/artic/discipl/4141.htm

OSI. (20 de Septiembre de 2016). *Geolocalización: Virtudes y riesgos*. Obtenido de https://www.osi.es/es/actualidad/blog/2016/09/20/geolocalizacion-virtudes-y-riesgos

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

Patel, N., & Zambrano, K. (2020). *"Auditoria de seguridad informática en base a la normativa ISO 27005:2013 para descubir y aprovechar debilidades en una red de gestión emulada para una Compañía prestadora de servicios".* Guayaquil: UG.

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/

Risco, G. (2021). *"Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín,2021".* Moyobamba: UCV.

Sánchez, P. (2022). *"Diseño de una propuesta sobre la aplicación de un SGSI para la empresa de transporte la Ecuatoriana bajo la norma ISO 27001".* Tacna: EPGN.

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/

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

## ANEXOS

### Anexo 1 - Matriz de consistencia

Título: Aplicación de la norma internacional ISO/IEC 27005:2018 para la Gestión de riesgos de seguridad de la información en dispositivos GPS, 2022.

Autor: Nina Yana, Ademir.

| Problema | Objetivo | Hipótesis | Variable |
|---|---|---|---|
| General:<br>¿De qué manera la aplicación de la norma internacional ISO/IEC 27005:2018 influye en la gestión de riesgos de seguridad de la información en dispositivos GPS en el año 2022? | General:<br>Mejorar la gestión de riesgos de seguridad de la información en dispositivos GPS en el año 2022 mediante la aplicación de la norma internacional ISO/IEC 27005:2018. | General:<br>“La aplicación de la norma internacional ISO/IEC 27005:2018 mejora significativamente la gestión de riesgos de seguridad de la información en dispositivos GPS en el año 2022”. | Independiente:<br>Norma internacional ISO/IEC 27005:2018 |
| Específicos:<br>1. ¿De qué manera la aplicación de la norma internacional ISO/IEC 27005:2018 influye en la identificación de riesgos de seguridad de la información en dispositivos GPS en el año 2022?<br>2. ¿De qué manera la aplicación de la norma internacional ISO/IEC 27005:2018 influye en la evaluación de riesgos de seguridad de la información en dispositivos GPS en el año 2022?<br>3. ¿De qué manera la aplicación de la norma internacional ISO/IEC 27005:2018 influye en el tratamiento de riesgos de seguridad de la información en dispositivos GPS en el año 2022? | Específicos:<br>1. Mejorar la identificación de riesgos de seguridad de la información en dispositivos GPS.<br>2. Mejorar la evaluación de riesgos de seguridad de la información en dispositivos GPS.<br>3. Mejorar el tratamiento de riesgos de seguridad de la información en dispositivos GPS. | Específicas:<br>1. “La aplicación de la norma internacional ISO/IEC 27005:2018 mejora la identificación de riesgos de seguridad de la información en dispositivos GPS en el año 2022”.<br>2. “La aplicación de la norma internacional ISO/IEC 27005:2018 mejora la evaluación de riesgos de seguridad de la información en dispositivos GPS en el año 2022”.<br>3. “La aplicación de la norma internacional ISO/IEC 27005:2018 mejora el tratamiento de riesgos de seguridad de la información en dispositivos GPS en el año 2022”. | Dependiente:<br>Gestión de riesgos de seguridad de la información |

<table>
<tr><td colspan="4">Metodología</td></tr>
<tr>
<td>Tipo de investigación:<br>Aplicada</td>
<td>Población (N):<br>$N = 10\ personas$</td>
<td>Técnicas de recolección de datos:<br>• Encuesta<br>• Análisis documental</td>
<td>Método de análisis de datos:<br>• Estadística descriptiva<br>• Estadística inferencial</td>
</tr>
<tr>
<td>Diseño de investigación:<br>Preexperimental</td>
<td>Muestra (n):<br>$n = 10\ personas$</td>
<td>Instrumentos de recolección de datos:<br>• Cuestionario<br>• Ficha de datos</td>
<td>Aspectos éticos:<br>Se respetará el derecho a la propiedad intelectual (Originalidad de la investigación - Reporte Turnitin).<br>Se tomará en cuenta el Código de ética de la Universidad César Vallejo (RCU Nº 0126-2017/UCV).<br>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:<br>Norma internacional ISO/IEC 27005:2018 | “Conjunto de directrices para el establecimiento de un enfoque sistemático de gestión de riesgos de seguridad de la información” (PECB, 2020). | La norma internacional ISO/IEC 27005:2018 se puede medir a través de la implementación y gestión eficaz de un proceso de gestión del riesgo de la seguridad de la información en una organización. | | | |
| Dependiente:<br>Gestión de riesgos de seguridad de la información | “Actividad recurrente enfocada al análisis, a la planificación, la ejecución, el control y el seguimiento de todas las medidas implantadas y la política de seguridad de riesgos en seguridad de la información” (PMG-SSI, 2017). | La gestión de riesgos de seguridad de la información se puede medir por la identificación, evaluación, tratamiento y monitoreo de los mismos. | Persona | Nivel de identificación del riesgo de seguridad de la información | Ordinal |
| | | | | Nivel de evaluación del riesgo de seguridad de la información | Ordinal |
| | | | | Nivel de tratamiento del riesgo de seguridad de la información | 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: 08/05/2022

Título del proyecto de investigación: "Aplicación de la norma internacional ISO/IEC 27005 para la Gestión de riesgos de seguridad de la información en dispositivos electrónicos con GPS, 2022".

Autor: Nina Yana, Ademir

**Evaluación de la metodología/norma internacional para la gestión de riesgos de seguridad de la información**

Mediante el método de juicio experto, Usted tiene la facultad de calificar las metodologías/normas internacionales involucrados, 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 el presente proyecto de investigación y, también si hubiese algunas sugerencias:

| Ítem | Criterios | Metodología / Norma internacional | | |
|---|---|---|---|---|
| | | ISO 27005:2018 | MAGERIT v3 | ISO 27002:2013 |
| 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/normas internacionales 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: 08/05/2022

Título del proyecto de investigación: "Aplicación de la norma internacional ISO/IEC 27005 para la Gestión de riesgos de seguridad de la información en dispositivos electrónicos con GPS, 2022".

Autor: Nina Yana, Ademir

**Evaluación de la metodología/norma internacional para la gestión de riesgos de seguridad de la información**

Mediante el método de juicio experto, Usted tiene la facultad de calificar las metodologías/normas internacionales involucrados, 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 el presente proyecto de investigación y, también si hubiese algunas sugerencias:

| Ítem | Criterios | Metodología / Norma internacional | | |
|---|---|---|---|---|
| | | ISO 27005:2018 | MAGERIT v3 | ISO 27002:2013 |
| 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/normas internacionales 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: 08/05/2022

Título del proyecto de investigación: "Aplicación de la norma internacional ISO/IEC 27005 para la Gestión de riesgos de seguridad de la información en dispositivos electrónicos con GPS, 2022".

Autor: Nina Yana, Ademir

**Evaluación de la metodología/norma internacional para la gestión de riesgos de seguridad de la información**

Mediante el método de juicio experto, Usted tiene la facultad de calificar las metodologías/normas internacionales involucrados, 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 el presente proyecto de investigación y, también si hubiese algunas sugerencias:

| Ítem | Criterios | Metodología / Norma internacional | | |
|---|---|---|---|---|
| | | ISO 27005:2018 | MAGERIT v3 | ISO 27002:2013 |
| 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/normas internacionales 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 empresa de transporte

A continuación, se presenta una lista de preguntas contenidas en doce (12) ítems que corresponden a su percepción sobre la gestión de riesgos operacionales en la empresa. 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 des seguridad de la información | Riesgo | 1. ¿Qué opina Usted sobre el cumplimiento normativo para la identificación de riesgos de seguridad de la información? | | | | | |
| | | 2. ¿Qué opina Usted sobre el manejo responsable de la información en la identificación de riesgos de seguridad de la información? | | | | | |
| | | 3. ¿Qué opina Usted sobre el procedimiento utilizado para la identificación de riesgos de seguridad de la información? | | | | | |
| | | 4. ¿Qué opina Usted sobre el cumplimiento normativo para la evaluación de riesgos de seguridad de la información? | | | | | |
| | | 5. ¿Qué opina Usted sobre el manejo responsable de la información en la evaluación de riesgos de seguridad de la información? | | | | | |
| | | 6. ¿Qué opina Usted sobre el procedimiento utilizado para la evaluación de riesgos de seguridad de la información? | | | | | |
| | | 7. ¿Qué opina Usted sobre el cumplimiento normativo para el tratamiento de riesgos de seguridad de la información? | | | | | |
| | | 8. ¿Qué opina Usted sobre el manejo responsable de la información en el tratamiento de riesgos de seguridad de la información? | | | | | |
| | | 9. ¿Qué opina Usted sobre el procedimiento utilizado para el tratamiento de riesgos de seguridad de la información? | | | | | |

Anexo 5. Validez de los instrumentos de recolección de datos

**Hoja de validación del instrumento**

**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. ¿Qué opina Usted sobre el cumplimiento normativo para la identificación de riesgos de seguridad de la información? | x | | x | | x | | |
| 2. ¿Qué opina Usted sobre el manejo responsable de la información en la identificación de riesgos de seguridad de la información? | x | | x | | x | | |
| 3. ¿Qué opina Usted sobre el procedimiento utilizado para la identificación de riesgos de seguridad de la información? | x | | x | | x | | |
| 4. ¿Qué opina Usted sobre el cumplimiento normativo para la evaluación de riesgos de seguridad de la información? | x | | x | | x | | |
| 5. ¿Qué opina Usted sobre el manejo responsable de la información en la evaluación de riesgos de seguridad de la información? | x | | x | | x | | |
| 6. ¿Qué opina Usted sobre el procedimiento utilizado para la evaluación de riesgos de seguridad de la información? | x | | x | | x | | |
| 7. ¿Qué opina Usted sobre el cumplimiento normativo para el tratamiento de riesgos de seguridad de la información? | | | | | | | |
| 8. ¿Qué opina Usted sobre el manejo responsable de la información en el tratamiento de riesgos de seguridad de la información? | x | | x | | x | | |
| 9. ¿Qué opina Usted sobre el procedimiento utilizado para el tratamiento de riesgos de seguridad de la información? | 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**<br>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 |
|  <br>**DNI:** 18161457 Trujillo, 15 de mayo del 2022 | |

**Hoja de validación del instrumento**

**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. ¿Qué opina Usted sobre el cumplimiento normativo para la identificación de riesgos de seguridad de la información? | x | | x | | x | | |
| 2. ¿Qué opina Usted sobre el manejo responsable de la información en la identificación de riesgos de seguridad de la información? | x | | x | | x | | |
| 3. ¿Qué opina Usted sobre el procedimiento utilizado para la identificación de riesgos de seguridad de la información? | x | | x | | x | | |
| 4. ¿Qué opina Usted sobre el cumplimiento normativo para la evaluación de riesgos de seguridad de la información? | x | | x | | x | | |
| 5. ¿Qué opina Usted sobre el manejo responsable de la información en la evaluación de riesgos de seguridad de la información? | x | | x | | x | | |
| 6. ¿Qué opina Usted sobre el procedimiento utilizado para la evaluación de riesgos de seguridad de la información? | x | | x | | x | | |
| 7. ¿Qué opina Usted sobre el cumplimiento normativo para el tratamiento de riesgos de seguridad de la información? | | | | | | | |
| 8. ¿Qué opina Usted sobre el manejo responsable de la información en el tratamiento de riesgos de seguridad de la información? | x | | x | | x | | |
| 9. ¿Qué opina Usted sobre el procedimiento utilizado para el tratamiento de riesgos de seguridad de la información? | 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**<br>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 de TIC |
|  <br>**DNI:** 18070765 | Trujillo, 15 de mayo del 2022 |

**Hoja de validación del instrumento**

**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. ¿Qué opina Usted sobre el cumplimiento normativo para la identificación de riesgos de seguridad de la información? | x | | x | | x | | |
| 2. ¿Qué opina Usted sobre el manejo responsable de la información en la identificación de riesgos de seguridad de la información? | x | | x | | x | | |
| 3. ¿Qué opina Usted sobre el procedimiento utilizado para la identificación de riesgos de seguridad de la información? | x | | x | | x | | |
| 4. ¿Qué opina Usted sobre el cumplimiento normativo para la evaluación de riesgos de seguridad de la información? | x | | x | | x | | |
| 5. ¿Qué opina Usted sobre el manejo responsable de la información en la evaluación de riesgos de seguridad de la información? | x | | x | | x | | |
| 6. ¿Qué opina Usted sobre el procedimiento utilizado para la evaluación de riesgos de seguridad de la información? | x | | x | | x | | |
| 7. ¿Qué opina Usted sobre el cumplimiento normativo para el tratamiento de riesgos de seguridad de la información? | | | | | | | |
| 8. ¿Qué opina Usted sobre el manejo responsable de la información en el tratamiento de riesgos de seguridad de la información? | x | | x | | x | | |
| 9. ¿Qué opina Usted sobre el procedimiento utilizado para el tratamiento de riesgos de seguridad de la información? | 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**<br>Aplicable [ X ] Aplicable después de corregir [ ] No aplicable [ ] | |
| **Apellidos y nombres del juez evaluador** | Ms. Córdova Otero, Juan Luis |
| **Especialidad del evaluador** | Sistemas de información y comunicación |
|  <br>**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 | 10 | 100,0 |
| | Excluido[a] | 0 | ,0 |
| | Total | 10 | 100,0 |

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

Estadísticas de fiabilidad

| Alfa de Cronbach | N de elementos |
|---|---|
| ,915 | 10 |

# Anexo 7. Desarrollo de la solución propuesta

## APLICACIÓN DE LA NORMA INTERNACIONAL ISO/IEC 27005:2018 PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN DISPOSITIVOS GPS

Según ELADE (2017) ISO 27005 presenta información de utilidad para la gestión de riesgos en la seguridad de la información.

ISO 27005 muestra un enfoque directamente centrado en Risk Management para Tecnologías de la Información. Este enfoque tiene que estar alineado con la gestión de riesgos empresarial general de la compañía. Esta norma parte del mismo modelo definido en ISO 31000.

Gracias a esta norma se pueden seguir unas pautas para gestionar riesgos en Tecnologías de la Información, tales como aquellos originados por aplicaciones en condiciones vulnerables, sistemas operativos sin actualizaciones o tecnologías obsoletas, por poner unos ejemplos. ISO 27005 reemplaza a la norma ISO 13335-2 Gestión de Seguridad de la Información y la tecnología de las comunicaciones.

De acuerdo a ISO 27005 se establece un contexto en el que se indica un enfoque y criterios de evaluación, impacto y aceptación. Se definen alcances y límites. Se organiza la Gestión de Riesgos de Seguridad de la Información.

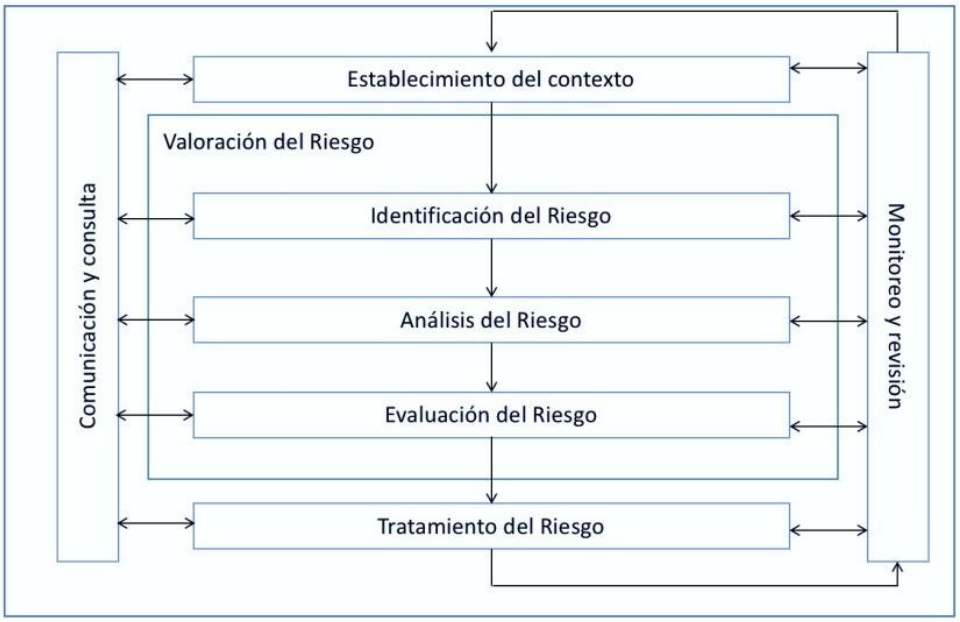
La norma ISO 27005 comprende la identificación, evaluación y tratamiento de los riesgos, pero también comprende la aceptación del riesgo, la comunicación y consulta, el monitoreo y revisión de los riesgos.

ISO 27005 se puede aplicar en todas las empresas, independientemente del tipo de organización que sea o de su tamaño. Esta norma facilita la gestión de los riesgos de Seguridad de la Información. Proporciona una orientación detallada para los encargados de implementar el Sistema de Gestión de la Seguridad de la Información (SGSI), profesionales del Risk Management y perfiles de seguridad.

Para el estudio realizado se tomó en cuenta una empresa de transporte que había incorporado el sistema GPS como herramienta tecnológica dentro de su organización para gestionar y analizar la información geográfica, procesar y visualizar mapas y gráficos del espacio de trabajo y, proporcionar sistemas de seguridad para el seguimiento de transporte por satélite con el fin de prevenir y controlar el alto riesgo que existe en el traslado de combustibles y/o materiales peligrosos. De este modo, la seguridad de los sistemas integrados por GPS, como es el caso del sistema de satélites, proporciona mayor calidad, eficacia y precisión.

Por temas de confidencialidad de la información recopilada, sólo se mostrarán los formatos utilizados para el desarrollo de la solución técnica propuesta.

**Proceso de gestión de riesgos bajo la Norma internacional ISO/IEC 27005:2018**




**Actividades de la gestión de riesgos bajo la Norma internacional ISO/IEC 27005:2018**

| IDENTIFICAR CONTEXTO | ANALIZAR RIESGOS | VALORAR RIESGOS | TRATAR RIESGOS |
|---|---|---|---|
| • Identificar activos<br>• Valorar activos<br>• Identificar amenazas<br>• Identificar vulnerabilidades<br>• Identificar agentes generadores | • Estimar impacto por materialización de amenazas<br>• Estimar probabilidad de ocurrencia<br>• Determinar riesgos<br>• Identificar controles existentes<br>• Evaluar controles existentes | • Estimar estado del riesgo<br>• Priorizar riesgos | • Toma de desiciones<br>• Plan de tratamiento de riesgos |

## Actividad 1a: Identificación de activos de información

**LISTA DE ACTIVOS**

| ID Activo | Nombre Activo | Descripción de Activo | Tipo de activo | Propietario de activo | Responsabilidad sobre |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## Actividad 1b: Valoración de activos de información

**LISTA DE ACTIVOS**

| Propietario de activo | Responsabilidad sobre el activo | Información que maneja el activo | Valoración cualitatitvo del activo | | | Valoración cuantitativo del activo | | | Valor promedio |
|---|---|---|---|---|---|---|---|---|---|
| | | | Disponibilidad | Integridad | Confidencialidad | Disponibilidad | Integridad | Confidencialidad | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Bajo
Medio
Alto

## Actividad 1c: Identificación de vulnerabilidades

**LISTA DE VULNERABILIDADES**

| ID Activo | Nombre Activo / Área de práctica organizacional | ID Vulnerabilidad | Descripción Vulnerabilidad |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

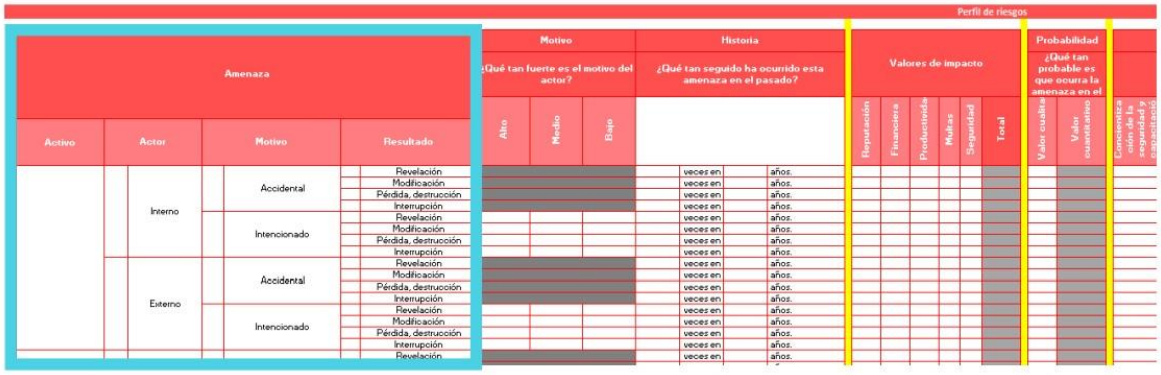
## Actividad 1d: Identificar agentes generadores

**Lista de Acciones**

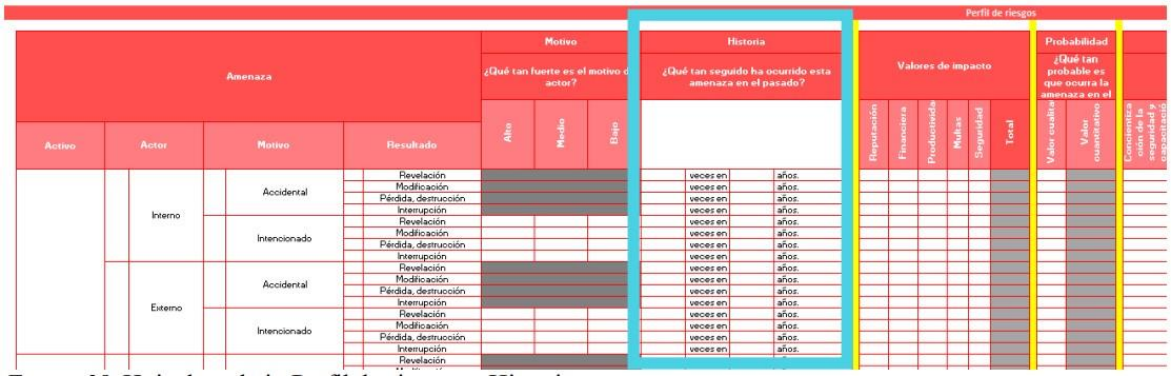
| Elemento de Acción<br>¿Qué medidas piensa tomar?<br>Asigne un número de identificación a cada elemento de acción. | ¿Para qué actividad es relevante este elemento de acción? | | ¿Qué información adicional desea documentar para cada acción?<br>¿Quién es responsable de completar el elemento de acción? |
|---|---|---|---|
| | | | Responsabilidad: |
| | | | ¿Cuando se debe completar el elemento de acción?<br>Fecha de Terminación: |
| | | | ¿Qué apoyo adicional se requiere para completar el elemento de acción?<br>Soporte adicional: |

## Actividad 2a: Hoja de perfil de riesgos


## Actividad 2b: Perfil de riesgos (Actor, Motivo y Resultado)



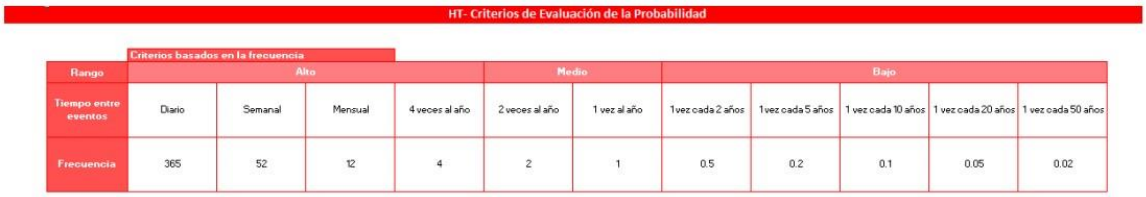
## Actividad 2c: Perfil de riesgo (Historia)



Perfil de riesgos

| Amenaza | | | | Motivo | | | Historia | Valores de impacto | | | | | | Probabilidad | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Activo | Actor | Motivo | Resultado | ¿Qué tan fuerte es el motivo d actor? | | | ¿Qué tan seguido ha ocurrido esta amenaza en el pasado? | | | | | | | ¿Qué tan probable es que ocurra la amenaza en el | | |
| | | | | Alto | Medio | Bajo | | Reputación | Financiera | Productividad | Multas | Seguridad | Total | Valor cualita | Valor cuantitativo | Consecuencia ción de la seguridad y cumplimiento |
| | Interno | Accidental | Revelación | | | | veces en años. | | | | | | | | | |
| | | | Modificación | | | | veces en años. | | | | | | | | | |
| | | | Pérdida, destrucción | | | | veces en años. | | | | | | | | | |
| | | | Interrupción | | | | veces en años. | | | | | | | | | |
| | | Intencionado | Revelación | | | | veces en años. | | | | | | | | | |
| | | | Modificación | | | | veces en años. | | | | | | | | | |
| | | | Pérdida, destrucción | | | | veces en años. | | | | | | | | | |
| | | | Interrupción | | | | veces en años. | | | | | | | | | |
| | Externo | Accidental | Revelación | | | | veces en años. | | | | | | | | | |
| | | | Modificación | | | | veces en años. | | | | | | | | | |
| | | | Pérdida, destrucción | | | | veces en años. | | | | | | | | | |
| | | | Interrupción | | | | veces en años. | | | | | | | | | |
| | | Intencionado | Revelación | | | | veces en años. | | | | | | | | | |
| | | | Modificación | | | | veces en años. | | | | | | | | | |
| | | | Pérdida, destrucción | | | | veces en años. | | | | | | | | | |
| | | | Interrupción | | | | veces en años. | | | | | | | | | |
| | | | Revelación | | | | veces en años. | | | | | | | | | |

## Actividad 2e: Criterios de evaluación de probabilidad de incidentes



HT- Criterios de Evaluación de la Probabilidad

Criterios basados en la frecuencia

| Rango | Alto | | | | Medio | | Bajo | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Tiempo entre eventos | Diario | Semanal | Mensual | 4 veces al año | 2 veces al año | 1 vez al año | 1 vez cada 2 años | 1 vez cada 5 años | 1 vez cada 10 años | 1 vez cada 20 años | 1 vez cada 50 años |
| Frecuencia | 365 | 52 | 12 | 4 | 2 | 1 | 0.5 | 0.2 | 0.1 | 0.05 | 0.02 |

## Actividad 3a: Valoración del incidente

| Lista de escenarios de incidentes | | | | | | |
|---|---|---|---|---|---|---|
| aza | Escenario | Consecuencia | Probabilidad de la amenaza | Valor cuantitativa de la amenaza | Valorización cualitativa de incidente | Valorización cuantitativa de incidente |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

## Actividad 3b: Probabilidad de la amenaza

| Lista de escenarios de incidentes | | | | | | |
|---|---|---|---|---|---|---|
| aza | Escenario | Consecuencia | Probabilidad de la amenaza | Valor cuantitativa de la amenaza | Valorización cualitativa de incidente | Valorización cuantitativa de incidente |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

## Actividad 4: Estrategia de protección

| | | | | |
|---|---|---|---|---|
|  |  |  |  |  |
| Concientización de la seguridad y capacitación | Estrategia de seguridad | Administración de la seguridad | Políticas de seguridad y regulaciones | Administración de Seguridad Colaborativa |
|  |  |  |  |  |
| Plan de Contingencia / Recuperación ante desastres | Control de acceso físico | Monitoreo y Auditoría de seguridad física | Administración de sistema y red | Monitoreo y Auditoría de la seguridad TI |
|  |  |  |  |  |

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 - CALLAO, asesor de Tesis titulada: "Aplicación de la norma internacional ISO/IEC 27005:2018 para la Gestión de riesgos de seguridad de la información en dispositivos GPS, 2022", cuyo autor es NINA YANA ADEMIR, constato que la investigación tiene un índice de similitud de 25.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 12 de Octubre del 2022

| **Apellidos y Nombres del Asesor:** | **Firma** |
|---|---|
| AGREDA GAMBOA EVERSON DAVID<br>**DNI:** 18161457<br>**ORCID:** 0000-0003-1252-9692 | Firmado electrónicamente por: AGREDA el 12-10-2022 07:56:23 |

Código documento Trilce: TRI - 0433931

INVESTIGA UCV