



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

**Aplicación de la Norma internacional ISO 27005 para la Gestión
de riesgos operacionales en la empresa CANVIA, Lima 2022**

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de sistemas

AUTOR:

Abad García, Igor Alexey (orcid.org/0000-0001-6036-0129)

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:

Desarrollo económico, empleo y emprendimiento

TRUJILLO - PERÚ

2022

Dedicatoria

A Dios porque hizo de mi un buen hombre, buen esposo y buen padre.

A mi esposa e hijos quienes han sido el motor y motivo en todo este tiempo para seguir avanzando y progresando profesionalmente.

A mis Padres quienes fueron mi fortaleza y un respaldo emocional muy importante en mi vida.

Igor Alexey

Agradecimiento

A la Universidad César Vallejo por su apoyo.

A la empresa CANVIA por la información brindada.

A mi asesor de tesis por sus correctas orientaciones y apoyo permanente.

El autor

Índice de contenidos

	Pág.
Carátula	i
Dedicatoria	ii
Agradecimiento	iii
Índice de contenidos	iv
Índice de tablas	v
Índice de figuras	vi
Resumen.....	vii
Abstract.....	viii
I. INTRODUCCIÓN	1
II. MARCO TEÓRICO	5
III. METODOLOGÍA	12
3.1. Tipo y diseño de investigación	12
3.2. Variables y operacionalización.....	12
3.3. Población, muestra y muestreo:.....	13
3.4. Técnicas e instrumentos de recolección de datos:.....	14
3.5. Procedimientos	14
3.6. Método de análisis de datos.....	15
3.7. Aspectos éticos:	15
IV. RESULTADOS.....	17
V. DISCUSIÓN	31
VI. CONCLUSIONES	34
VII. RECOMENDACIONES	35
REFERENCIAS.....	36
ANEXOS	38

Índice de tablas

	Pág.
Tabla 1. Población.....	13
Tabla 2. Análisis descriptivo de indicador 1	17
Tabla 3. Análisis descriptivo del indicador 2.....	18
Tabla 4. Análisis descriptivo del indicador 3.....	19
Tabla 5. Prueba de normalidad del indicador 1	21
Tabla 6. Prueba de normalidad del indicador 2	23
Tabla 7. Prueba de normalidad del indicador 3.....	25
Tabla 8. Prueba Wilcoxon para el indicador 1	28
Tabla 9. Prueba Wilcoxon para el indicador 2.....	29
Tabla 10. Prueba T-Student para el indicador 3.....	30

Índice de figuras

	Pág.
Figura 1. Medias de preprueba y posprueba del indicador 1	17
Figura 2. Medias de preprueba y posprueba indicador 2	18
Figura 3. Medias de preprueba y posprueba del indicador 3	19
Figura 4. Histograma del indicador 1 (Preprueba).....	21
<i>Figura 5.</i> Histograma del indicador 1 (Posprueba).....	22
Figura 6. Histograma del indicador 2 (Preprueba).....	23
<i>Figura 7.</i> Histograma del indicador 2 (Posprueba).....	24
Figura 8. Histograma del indicador 3 (Preprueba).....	25
<i>Figura 9.</i> Histograma del indicador 3 (Posprueba).....	26

Resumen

Esta investigación tuvo como objetivo mejorar la gestión de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022 mediante la aplicación de la norma internacional ISO 27005; el tipo es investigación fue aplicada y de diseño preexperimental. Se utilizó una muestra poblacional de 8 directivos de la empresa responsables directo de la gestión de riesgos. Como resultados se tuvo que, para el primer indicador “Identificación de los riesgos operacionales” hubo un incremento de 1.43 a 4.63 puntos (3.20 puntos = Δ 64.00%), para el segundo indicador “Evaluación de riesgos operacionales” hubo otro incremento de 1.61 a 4.50 puntos (2.89 puntos = Δ 57.80%) y para el tercer indicador, “Tratamiento de riesgos operacionales” hubo otro incremento de 1.50 a 4.58 puntos (2.88 puntos = Δ 61.80%), lo cual permitió un resultado favorable al aplicar la norma internacional ISO 27005. Como conclusión general se tuvo que, la aplicación de la norma internacional ISO 27005 logra mejorar significativamente la gestión de riesgos operacionales en la empresa en estudio.

Palabras clave: norma internacional, ISO 27005, riesgos operacionales, empresa tecnológica.

Abstract

This research aimed to improve operational risk management in the CANVIA company in the city of Lima in the year 2022 through the application of the international standard ISO 27005; the type of research was applied and pre-experimental design. A population sample of 8 company managers directly responsible for risk management was used. As results we had that, for the first indicator "Identification of operational risks" there was an increase from 1.43 to 4.63 points (3.20 points = 64.00%), for the second indicator "Evaluation of operational risks" there was another increase from 1.61 to 4.50 points (2.89 points = 57.80%) and for the third indicator, "Treatment of operational risks" there was another increase from 1.50 to 4.58 points (2.88 points = 61.80%), which allowed a favorable result when applying the international standard ISO 27005. As a general conclusion, the application of the international standard ISO 27005 significantly improved operational risk management in the company under study.

Keywords: international standard, ISO 27005, operational risks, technology company.

I. INTRODUCCIÓN

Martínez (2016) sostiene que, la creación de nuevas tecnologías y nuevos procedimientos ha representado grandes avances en la optimización de los procesos operativos; al mismo tiempo, se evidencian desviaciones significativas, generalmente por diversas razones, que pueden generar pérdidas financieras para una entidad, pudiendo ser muy significativas e incluso conduciendo a su liquidación. En este sentido, es responsabilidad de la entidad el establecimiento de una conveniente administración de riesgos, la programación de mecanismos de control interno, así como la capacitación e interiorización de los funcionarios, pues la política de la empresa ayudaría a reducir la adquisición de riesgos innecesarios utilizando herramientas disponibles para implementar el ciclo de vida del riesgo; es decir. Etapas como la identificación, la evaluación, la mitigación y la gestión propiamente.

Arévalo (2022) afirma que, en el pasado, la administración de los riesgos se vinculaba principalmente a aspectos financieros, pero con a través del paso del tiempo hubo un cambio y se entendió que, el control a modo de prevención es fundamental en los procesos de la empresa, pues ayuda a anticiparse a situaciones que pueden surgir en el futuro y, si ese fuera el caso, ya habría un plan para ayudar a mitigar las pérdidas potenciales.

Cáceres (2018) indica que, la administración de los riesgos va más allá de su exploración y su evaluación, pues también debe realizarse a través de una exploración cuanti-cuali vinculada con las metas de la organización a modo anticipado. En tal sentido, la administración de los riesgos abarca toda la entidad, pues lo conformaría: su cultura, su transparencia a nivel interno y externo y, más aún, su capacidad de irradiar esta cultura en todos los involucrados de la organización sobre la base de una adecuada relación costo-beneficio, relacionado con los objetivos estratégicos propios de la organización”.

PMG-SSI (2017) manifiesta que, la **norma internacional ISO 27005** reemplaza al estándar internacional ISO 13335-2. De esta forma, la norma se publicó por primera vez en junio de 2008, aunque fue revisada en 2011 y actualmente tiene vigencia a partir de 2018. En tal sentido, el riesgo ha sido definido como una posible amenaza que detecta y se aprovecha de la

vulnerabilidad de un posible activo causando daño. El riesgo puede estar vinculado con el empleo, autoría, actividad, traslado e implementación de tecnologías computacionales en la empresa. De este modo, los indicadores asociados al riesgo indican si una empresa estaría expuesta a un riesgo que supere lo permitido.

PECB (2020) sustenta que, la norma internacional ISO 27005 provee recomendaciones de como generar un entorno sistémico orientado a la administración de los riesgos a nivel de gestión segura de la información permitiendo la identificación de los requerimientos de la organización en estudio crean un sistema seguro al respecto. También se dice, que este estándar mundial es afín al estándar mundial ISO 27001, pues contribuye con la gestión de la información segura bajo una perspectiva de riesgos.

BBVA (2015) sostiene que, los riesgos a nivel operativo son propios de las operaciones, sistemas, productos y actividades siendo su origen variado (operaciones, fraude a nivel interno y externo, tecnología, talento humano, malas prácticas, catástrofes y provisos); por lo tanto, la administración de los riesgos a nivel operativo debería integrarse fuertemente al diseño organizacional efectivo de la entidad.

En este contexto, se tiene a la empresa CANVIA, una organización líder en las actividades innovadores y de transformación digital de las múltiples empresas con giros de negocio variado en el Perú a lo largo de más de tres décadas. Canvia ha construido un solo equipo de más de 2500 expertos y consultores especializados que le permite ser partner de clase mundial de sus más de 300 clientes compañías líderes en tecnología de los sectores financieros Industria Comercio y sector público. Desde el año 2018, CANVIA forma parte del portafolio de Adventure Internacional considerado como fondos de capital privado significativos y activos desde sus 84 ha invertido sobre los 56,000 millones de dólares americanos en más de 375 proyectos de inversión de capital privado en 42 países (CANVIA, 2018).

En estos últimos años, la empresa en estudio ha crecido en sus operaciones de negocio, pero junto con ello también los riesgos latentes en sus operaciones; presentando algunas deficiencias notables (**problemas específicos**) con respecto a la gestión de riesgos operacionales como son:

Posibilidad de sufrir pérdidas por escasez, falla o insuficiencia de los recursos humanos; Posibilidad de experimentar pérdidas por defectos de proceso, mal funcionamiento o deficiencias; Posibilidad de daños por defectos técnicos, mal funcionamiento u omisiones; Posibilidad de experimentar daños debido a defectos, fallas o deficiencias de la infraestructura.

Se tuvo la **formulación del problema**: *General*: ¿De qué modo la aplicación de la norma internacional ISO 27005 impacta en la gestión de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022? *Específicos*: Problema específico 1 - ¿De qué modo la aplicación de la norma internacional ISO 27005 impacta en la identificación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022? Problema específico 2 - ¿De qué modo la aplicación de la norma internacional ISO 27005 impacta en la evaluación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022? Problema específico 3 - ¿De qué modo la aplicación de la norma internacional ISO 27005 impacta en el tratamiento de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022?

Se presentó la **justificación de la investigación**: *Por conveniencia*, permitió optimizar la administración de los riesgos operacionales en la empresa en estudio; *Relevancia social*, incluyó tranquilidad y facilidad de realizar operaciones con un contexto de seguridad frente a los riesgos; *Utilidad metodológica*, fue la base para próximas investigaciones sobre gestión de riesgos operacionales; *Implicancias prácticas*, permitió conocer las vulnerabilidades presentes en las operaciones de negocio; *Valor teórico*, ayudó a comprender mejor las bases teóricas de los riesgos operacionales y de la norma internacional ISO 27005.

Se formuló los siguientes **objetivos**: *General*: Mejorar la gestión de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022 mediante de la aplicación de la norma internacional ISO 27005; *Específicos*: Objetivo específico 1 - Mejorar la identificación de riesgos operacionales en la empresa; Objetivo específico 2 - Mejorar la evaluación de riesgos operacionales en la empresa; Objetivo específico 3 - Mejorar el tratamiento de riesgos de operacionales en la empresa.

Al final, la investigación formuló la **hipótesis**: *General*: “La aplicación de la norma internacional ISO 27005 mejora de forma significativa la gestión de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”. *Específicas*: Hipótesis específica 1 - “La aplicación de la norma internacional ISO 27005 mejora la identificación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”; Hipótesis específica 2 - “La aplicación de la norma internacional ISO 27005 mejora la evaluación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”; Hipótesis específica 3 - “La aplicación de la norma internacional ISO 27005 mejora el tratamiento de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

II. MARCO TEÓRICO

En este capítulo, se presenta inicialmente los **antecedentes** de la investigación realizada que ayudaron a conocer los estudios ya realizados con respecto a las variables de estudio. Se tiene:

Fajardo (2021) en su investigación buscó brindar los requisitos para adaptar una apropiada examinación de riesgos sobre los activos de tecnología críticos en una empresa, teniendo como meta incrementar la información segura en estos activos combinando las mejores prácticas y recomendaciones a nivel legislativo y normativo que fundamentan los procesos de gestión en seguridad.

Jacho (2020) en su investigación buscó determinar las vulnerabilidades de los procedimientos informáticos que poseía la compañía mediante el estándar mundial ISO 27005:2013. La metodología aplicada fue en cascada mediante el desarrollo de cinco (5) fases: Descubrimiento, Exploración, Evaluación, Intrusión y Reporte, las cuales se encargaban de reconocer las vulnerabilidades presentes. Como resultado, se identificó que la empresa poseía sistemas operativos Windows desactualizados pudiendo ser utilizados como una oportunidad abierta para los atacantes informáticos. Las conclusiones demostraron que el estándar ISO 27005 ayudó a minimizar los incidentes de seguridad en la red administrativa.

Nañez (2020) en su investigación buscó desarrollar un modelo de administración de riesgos basados en TI sobre la base del estándar mundial ISO 27005, así como el uso del método MAGERIT a fin de optimizar la gestión segura de la información en una Universidad de la ciudad de Chachapoyas - Perú. La propuesta representó un incremento valioso en la satisfacción de los usuarios con respecto a la administración de los servicios tecnológicos de la Universidad garantizando que los riesgos relacionados a TI sean conocidos, asumidos, administrados y reducidos de forma documental, sistémica, organizada, repetitiva, efectiva y configurable generando todos los cambios necesarios respecto a los riesgos, el medio ambiente y las tecnologías adoptadas por la entidad de educación superior.

Ordeñana (2019) en su investigación buscó presentar la implementación de la administración de los riesgos informáticos sobre la base del estándar ISO 27005 en las bases de datos y sistemas operativos de un departamento informático teniendo como meta la mitigación de los problemas en niveles lógico, físico y organizativo empleando el método combinado del ciclo de Deming y el estándar mundial ISO 27005; logrando para ello, la identificación de los activos más relevantes en el campo base de la organización y sus objetivos, evaluando posteriormente la ejecución de la administración de los riesgos, y finalmente observando los resultados generados así como las conclusiones en materia de administración de riesgos con el uso de un método adaptado.

Patiño (2018) en su investigación buscó conocer el estándar mundial ISO 27005 determinando el nivel de mitigación de los riesgos informáticos en entidades públicas que se sometieron a un estudio cualitativo-cuantitativo con alcance descriptivo y una muestra no probabilística. Se puso en práctica un cuestionario a dieciocho (18) gerentes de tecnología de entidades públicas ubicadas en la ciudad de Esmeraldas. Como regla, a pesar de la inclusión de regulaciones internacionales, todavía es difícil obtener esto, porque los estándares fueron creados para empresas desarrolladas en un contexto diferente. En respuesta, se propuso una guía detallada, desarrollando cada paso con su conjunto de actividades e implementándola en la comunidad del sector público para validar cada paso predefinido.

Quispe y Pacheco (2018) en su investigación buscaron diseñar un piloto de examinación de los riesgos de seguridad basado en el estándar mundial ISO 27005 logrando determinar la factibilidad de obtener un servicio en la nube, puesto que cada organización debería conocer los riesgos en materia de seguridad que se mantiene vigente sobre todo con respecto a mecanismos de seguridad especificados y, los riesgos que podrían adquirirse mediante el uso de un servicio nuevo basado en la nube, toda vez que, se debía tomar una decisión sobre esta elección.

Puyén y Rivas (2018) en su investigación buscaron proponer la mejora de la administración informática a nivel seguro en un Hospital mediante el

desarrollo de un modelo de administración de riesgos empleando el estándar mundial ISO 27005 y la aplicación del método MAGERIT.

Chunga (2017) en su investigación buscó examinar los posibles riesgos de los activos informáticos relacionados con el empleo del cuerpo docente según las pautas de la norma ISO 27005, puesto que la alta dirección no conocía a detalle los problemas que enfrentaba la organización. La motivación de este estudio fue conocer el estándar mundial ISO 27005 para una correcta administración de los riesgos, la cual podía ser utilizada para evaluar activos de información en base a los siguientes pasos; determinación del alcance, identificación de los activos informáticos, obteniendo una clasificación por tipo para evaluarse frente a las tres características clave de un Sistema de Gestión de la Seguridad de la Información (SGSI) como fue la privacidad, probidad y disposición de la información; a continuación, se identificaron los principales riesgos y problemas más delicados a fin de determinar la probabilidad y el impacto en la organización, lo que dio como consecuencia un determinado posicionamiento del riesgo. Finalmente, se propusieron medidas de control para intentar disminuir los riesgos ya identificados. Se emplearon herramientas debidamente validadas como fichas de observación, cuestionarios y guías de entrevista. El resultado de la examinación de los riesgos, arrojó que el 34% de fuentes de información identificadas con relación al empleo del personal docente fueron sumamente críticas.

Palomares (2016) en su investigación buscó conocer la consecuencia de desarrollar la ejecución de un sistema seguro de la información para los problemas futuros presentes en la red de información de la entidad basado en el empleo del estándar mundial ISO 27005. El estudio hecho fue aplicado, siendo el diseño de investigación preexperimental. La población se constituyó por treinta (30) puestos de trabajo y la muestra fue no probabilística, intencional. La observación fue la técnica empleada como instrumento diario de observación. Este instrumento fue validado con el resultado de una evaluación de ajuste revisada por pares, y la confiabilidad se obtuvo con la prueba estadística T-Student. Como resultado de este estudio se avaló que, la creación del sistema de información segura ha afectado significativamente los riesgos de la red informática de la empresa; habiendo disminuido el

número de amenazas detectadas en 8% y la gravedad de los impactos en un 4%.

También, se presenta un conjunto de **bases teóricas** orientadas a la mejor comprensión del tema de investigación como sigue:

Norma internacional ISO 27005, se define como: “Conjunto de directrices para establecer un marco sistemático orientado a la administración de riesgos en materia de seguridad informática necesarios para la identificación de los requisitos seguros de información que exige la entidad con el fin de proponer un sistema de administración de información segura y eficaz”. Además, este estándar mundial es consistente con las definiciones tratadas sobre el estándar mundial ISO/IEC 27001 y, está diseñado para permitir el desarrollo de manera efectiva la información segura sobre la base de un enfoque de riesgos. En cuanto al estándar mundial ISO 27005, permitió la adquisición de destrezas y experiencias cognitivas fundamentales para la implementación del proceso de administración de los riesgos de seguridad informática. En tal sentido, se debía identificar, evaluar, examinar y abordar los múltiples riesgos de seguridad informática presentes en diversas organizaciones (PECB, 2020).

Gestión de riesgos operacionales, se define como todo aquello que puede resultar de fallas humanas, operaciones internas inadecuadas o deficientes, errores del sistema y sucesos del entorno. La definición de riesgo operacional incluye las siguientes categorías de riesgo: proceso, falla externa e interna, tecnológica, talento humano, operaciones comerciales, accidentes, distribuidores (BBVA, 2015). Las principales fuentes de riesgo operativo son: Operaciones internas; Sucesos del entorno; Talento humano; Tecnologías informáticas y de comunicación - TIC. En cuanto a los procesos internos, pueden ocurrir pérdidas financieras debido a procesos críticos mal diseñados o procedimientos inexistentes, lo que puede conducir a un mal desarrollo y/o interrupciones del servicio; Los sucesos del entorno son probables pérdidas monetarias vinculadas con aquellos casos que están fuera del monitoreo de la entidad y podrían modificar el desarrollo de las operaciones de negocio; El talento humano es una pérdida financiera relacionada con el error humano, la negligencia, el fraude, el sabotaje, el robo, el espionaje en la industria o el lavado de activos, también la pérdida por problemas de índole laboral o un

entorno de trabajo deficiente; La tecnología informática y de comunicación - TIC, es la pérdida financiera potencial causada por el incorrecto uso de los sistemas informáticos que se emplean en la empresa, así como la violación de los tres (3) principios de seguridad informática: acceso seguro, preciso e ininterrumpido (CESCE, 2021).

Empresa de base tecnológica, representa la entidad sostenida por su actividad en el uso de nuevas tecnologías para la producción o mejora de productos, procesos o servicios. En el lenguaje popular y periodístico también se les conoce como empresas tecnológicas o simplemente empresas tecnológicas. La importancia de estas empresas para impulsar la estructura tecnológica y el desarrollo económico, crear puestos de trabajo de alta cualificación y crear un alto valor añadido para el entorno industrial, hizo que las universidades y otras instituciones nacionales de investigación les prestaran aún más atención como una transferencia real de motores de información. En muchos casos, estas empresas surgieron de las entidades de educación superior de I+D llamados incubadoras tecnológicas. Se trata de organizaciones caracterizadas por una fuerte base técnica y por una gran carga de innovación técnica. Son un medio relevante para la transferencia de logros científicos, que benefician a la sociedad con la probabilidad de obtener productos novedosos, orientados a favorecer la integración de la juventud a la vida profesional y laboral (UM, 2020).

También, se recurrió a los **enfoques conceptuales** para complementar lo revisado en los puntos anteriores como sigue:

Amenaza, representan escenarios en la empresa que generan perjuicio material o inmaterial a los activos informáticos. En tal sentido, los sistemas de gestión de seguridad ayudarían a mitigar las amenazas que conducen a situaciones peligrosas (ISO 27001, 2020).

Vulnerabilidad, es una debilidad del activo que puede explotarse amenazando con un ataque contra el bien o servicio informático. Asimismo, existe la posibilidad de que la incidencia perjudicial a dicho bien se materialice (ISO 27001, 2020).

Riesgo, representa la probabilidad de que algún desastre se haga realidad en una calamidad. Las vulnerabilidades o calamidades por sí solas no constituyen una amenaza. Sin embargo, al unirse, forman un riesgo o posibilidad de generar un desastre (ISO 27001, 2020).

Problema de seguridad, procede de diferentes tipos: por compatibilidad causados por actualizaciones importantes del sistema operativo u otros inconvenientes de compatibilidad, o por hardware o software procedentes de terceros. Asimismo, pueden representar huecos de seguridad que están presentes en diversos sistemas operativos, para lo cual será muy importante establecer parches de seguridad antes de que alguien los active (XATACA, 2020).

Respecto a las **metodologías, marcos de trabajo o normas internacionales** que fueron evaluadas como candidatas, se tuvo:

Metodología MAGERIT v3, es una metodología para la examinación y administración de los riesgos gestionada actualmente como un método público que se puede usar libremente y no requiere permiso previo. Las entidades del ámbito del Sistema Nacional de Seguridad (ENS) están principalmente interesadas en cumplir con la normativa soportado en la administración de los riesgos y la exigencia de examinación y tratamiento de los mismos, con el apoyo de las TIC para realizar tareas, brindar servicios y lograr las metas organizacionales. Esta metodología corresponde al punto ("Implementación de la administración de riesgos") del denominado "Proceso de administración de riesgos" incorporado en el "Marco administrativo de los riesgos"; es decir, incluye la toma de decisiones que deben asumir los órganos de gestión con el uso de las tecnologías informáticas (PAE, 2018).

Norma internacional ISO 27005, la nueva ISO 27001:2018 provee directrices inmediatas para administrar adecuadamente los riesgos vinculados a la seguridad informática y de los bienes informáticos de una organización. Adicionalmente, se contempla los requerimientos de gestión segura de la información tomando como base el estándar mundial ISO/IEC 27001-27002; de esta forma, se pretende disponer de una certificación para el cumplimiento de las exigencias que las entidades privadas y públicas tienen actualmente

sobre todo en materia de seguridad. El estándar mundial ISO 27005 ha sido nuevamente revisado y se ha actualizado a su versión más reciente en el año 2018 tomando como referencia las necesidades actuales de la población económicamente activa (ISOTools, 2018).

Norma internacional ISO 27002, se compone de catorce (14) áreas de control en seguridad informática como: La administración de activos se basa en el uso correcto de las medidas convenientes para protegerse contra incidentes, violaciones y cambios no deseados; Control de acceso Se controla quién puede acceder a los datos en el aspecto respectivo. Al final del día, no todos en una organización necesitan acceso a toda la información para realizar sus operaciones diarias, pero tenemos responsabilidades que requieren más acceso y en cambio existen otros casos donde el acceso debe ser más limitado. En cuanto a los controles de seguridad como: alta de usuarios, asignación de derechos, entre otros debe estar habilitado para lograr el cambio. si alguno de los controles contenidos en esta sección; Cifrado: Para datos sensibles o críticos, resulta importante aplicar técnicas de encriptación orientadas a la protección permanente de los datos y la aplicación de los controles seguros en materia de calidad de la información (principios de confidencialidad, integridad y disponibilidad). Asimismo, resulta también muy importante que la gestión segura no sólo sea a nivel lógico sino a la vez a nivel físico, pues el acceso a las instalaciones, ambientes diversos debería realizarse en las mejores condiciones de identificación de los usuarios, toda vez que debe evitarse posibles hurtos informáticos externos sobre todo a nivel de hardware; Seguridad operativa, se incluye un fuerte elemento informático en los diversos aspectos existentes, como es el caso de protección segura contra malware, respaldos, gestión del software utilizado, administración de las vulnerabilidades, etc.; Seguridad de las comunicaciones, se asume que la gran mayoría de las interconexiones llevan datos e información entre origen y destino empleando un medio de transmisión protegiendo adecuadamente los canales de transmisión de estos datos claves (ISO Tools Excellence, 2016).

En lo que respecta al **método de juicio experto** para elegir la metodología más adecuada se tuvo a la *Norma internacional ISO 27005* - ver Anexo 3.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

- **Tipo de investigación**
Aplicada.
- **Diseño de investigación**
Preexperimental.

3.2. Variables y operacionalización

- **Variables**
 - **Variable independiente:** Norma internacional ISO 27005
 - **Definición Conceptual:**

“Directrices para crear un entorno de sistemas para la administración de riesgos de seguridad informática y de información” (PECB, 2020).
 - **Definición operacional:**

La norma internacional ISO 27005 se puede medir a través de la ejecución y gestión eficaz de un método de administración de riesgos de seguridad de informática y de información en las organizaciones.
 - **Variable dependiente:** Gestión de riesgos operacionales
 - **Definición Conceptual:**

“Uno que puede resultar en detrimentos por causa de fallas humanos, sucesos internos inadecuados o deficientes, errores del sistema y sucesos del entorno” (BBVA, 2015).

- **Definición operacional:**

La gestión de riesgos operacionales se puede medir por la caracterización, valoración y tratamiento de los mismos.

▪ **Operacionalización**

La operacionalización de variables se encuentra detallada en la matriz que corresponde al Anexo 2.

3.3. Población, muestra y muestreo:

▪ **Población (N)**

Está representada por los usuarios (colaboradores) que laboran en la empresa elegida y que son responsables directa e indirectamente de la gestión de riesgos operacionales.

Tabla 1. Población

Cargo / Puesto	Cantidad
CEO	1
Jefe de unidad	2
Ejecutivo	5
Total	8

Fuente: (Elaboración propia, 2022)

Se presenta, entonces:

$$N = 8 \text{ personas}$$

▪ **Muestra (n)**

La muestra poblacional sería igual a la población, puesto que ésta es menor o igual que 30.

Se presenta, entonces:

$$n = N = 8 \text{ personas}$$

- **Muestreo**

Pertenece a la categoría no probabilístico dado se ha manipulado la participación de los elementos de la población muestral.

3.4. Técnicas e instrumentos de recolección de datos:

- **Técnicas:**

- Encuesta, técnica para recopilar datos baso en las opiniones de un grupo de personas.
- Análisis documental, técnica para recopilar información del negocio.

- **Instrumentos:**

- Cuestionario (Observación).
- Ficha de datos (Análisis documental).

3.5. Procedimientos

Durante la ejecución de la investigación, se tuvo que realizar cuatro (4) objetivos específicos (Oe) como sigue:

- Oe₁: Mejorar la identificación de riesgos operacionales en la empresa

Se optó por recopilar la opinión de los usuarios de la entidad elegida sobre el procedimiento de identificación de riesgos operacionales mediante el uso de la técnica de la Encuesta, empleando el instrumento Cuestionario (ver Anexo 4).

- Oe₂: Mejorar la evaluación de riesgos de seguridad de los riesgos operacionales de la empresa.

Se optó por recopilar la opinión de los usuarios de la entidad elegida sobre el procedimiento de evaluación de riesgos

operacionales mediante el uso de la técnica de la Encuesta, empleando el instrumento Cuestionario (ver Anexo 4).

- Oe3: Mejorar el tratamiento de riesgos operacionales de la empresa.

Se optó por recopilar la opinión de los usuarios de la entidad elegida sobre el procedimiento de tratamiento de riesgos operacionales mediante el uso de la técnica de la Encuesta, empleando el instrumento Cuestionario (ver Anexo 4).

3.6. Método de análisis de datos

Las operaciones de proceso y analítica de datos se realizaron empleando el uso de métodos estadísticos a nivel descripción y/a nivel inferencial.

En el primer caso (análisis descriptivo) se pudo contrastar gráficamente y tabularmente una situación anterior versus una situación posterior.

En el segundo caso, se pudo determinar tabular y gráficamente la normalidad de los indicadores que corresponden a la variable dependiente.

El método deductivo se empleó para procesar los resultados del estudio, porque es un estudio cuantitativo (ir de lo general a lo específico).

3.7. Aspectos éticos:

Este estudio consideró la creación de un acta de declaración de autoría (por parte del autor o autores) y la declaración de originalidad de la investigación (por el lado del asesor).

También, se revisó y consideró la Resolución del Consejo Universitario RCU N° 0126-2017/UCV respecto al uso del Código de Ética Universitario.

De igual forma, se consideró el empleo de la herramienta web del sistema Turnitin para generar el reporte del índice de similitud del informe de investigación desarrollado considerando un % menor a 30'%.

Finalmente, se empleó el sistema estándar de referencias bibliográficas ISO-690 para el registro y uso de diversas citas empleadas en el desarrollo de la investigación presente.

Cabe además recalcar, que fue importante tener presente en todo momento los principios éticos para el desarrollo de la investigación, pues esto permite que los conocimientos generados procedan de una investigación transparente y correcta según las directrices que exige la Universidad.

IV. RESULTADOS

- **Análisis descriptivo**
 - Análisis descriptivo para el indicador 1

Tabla 2. Análisis descriptivo de indicador 1

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
IRO-Preprueba	3	1,25	1,53	1,4267	,15373
IRO-Posprueba	3	4,50	4,75	4,6267	,12503
N válido (por lista)	3				

Fuente: (Elaboración propia, 2022)

Como se muestra en la tabla anterior, la identificación de riesgos operacionales que se tenía antes de la aplicación de la norma internacional ISO 27005 presentaba una media estadística de 1.43 puntos y después de la aplicación de la norma internacional ISO 27005 presenta una media estadística de 4.63 puntos, generando un incremento de 3.20 puntos en la medición del indicador (Δ 64.00%).

Lo anterior, queda evidenciado en la siguiente figura:

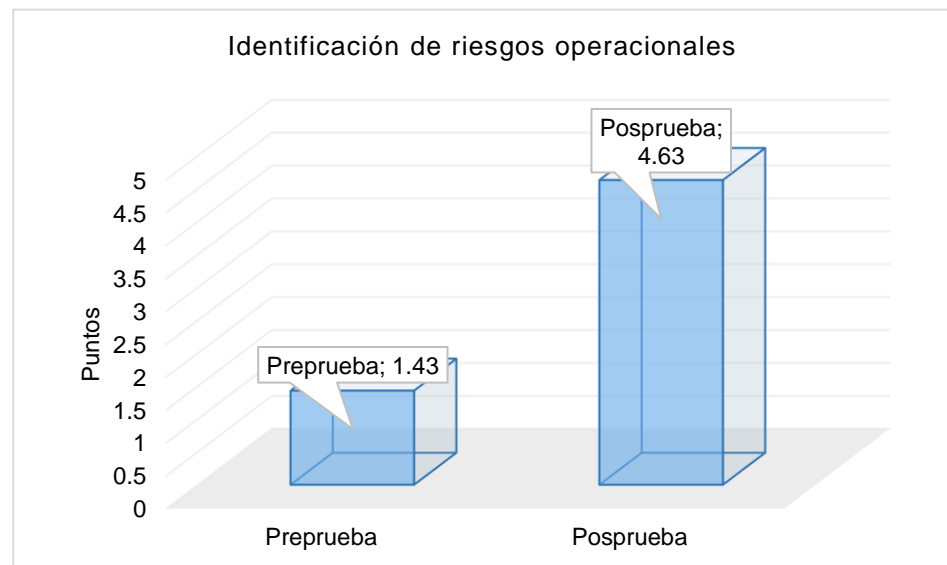


Figura 1. Medias de preprueba y posprueba del indicador 1

- Análisis descriptivo para el indicador 2

Tabla 3. Análisis descriptivo del indicador 2

	Estadísticos descriptivos				Desv. Desviación
	N	Mínimo	Máximo	Media	
ERO-Preprueba	3	1,45	1,87	1,6080	,22806
ERO-Posprueba	3	4,25	4,75	4,5000	,25000
N válido (por lista)	3				

Fuente: (Elaboración propia, 2022)

Como se muestra en la tabla anterior, la identificación de riesgos operacionales que se tenía antes de la aplicación de la norma internacional ISO 27005 presentaba una media estadística de 1.61 puntos y después de la aplicación de la norma internacional ISO 27005 presenta una media estadística de 4.50 puntos, generando un incremento de 2.89 puntos en la medición del indicador (Δ 57.80%).

Lo anterior, queda evidenciado en la siguiente figura:

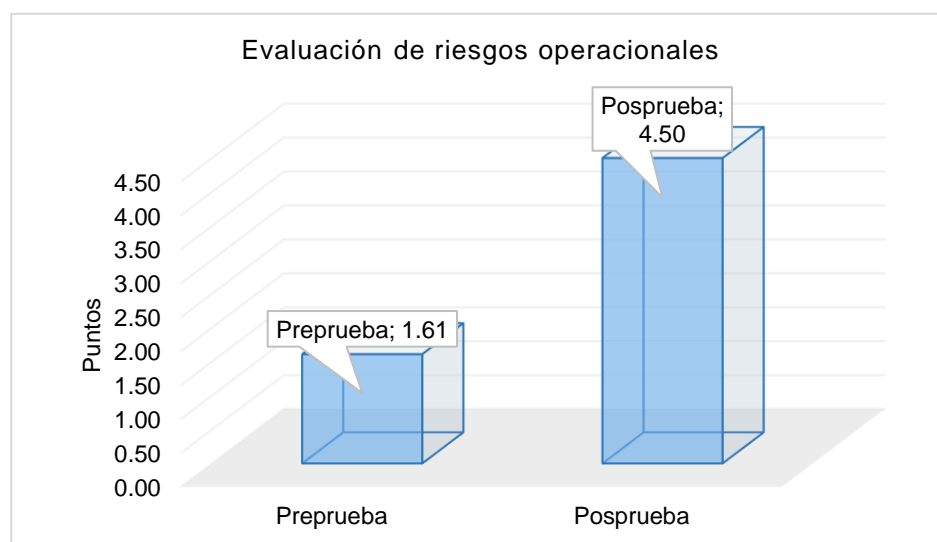


Figura 2. Medias de preprueba y posprueba indicador 2

- Análisis descriptivo para el indicador 3

Tabla 4. Análisis descriptivo del indicador 3

	Estadísticos descriptivos				Desv. Desviación
	N	Mínimo	Máximo	Media	
TRO-Preprueba	3	1,38	1,63	1,5033	,12503
TRO-Posprueba	3	4,50	4,63	4,5867	,07506
N válido (por lista)	3				

Fuente: (Elaboración propia, 2022)

Como se muestra en la tabla anterior, la identificación de riesgos operacionales que se tenía antes de la aplicación de la norma internacional ISO 27005 presentaba una media estadística de 1.50 puntos y después de la aplicación de la norma internacional ISO 27005 presenta una media estadística de 4.58 puntos, generando un incremento de 2.88 puntos en la medición del indicador (Δ 61.80%).

Lo anterior, queda evidenciado en la siguiente figura:

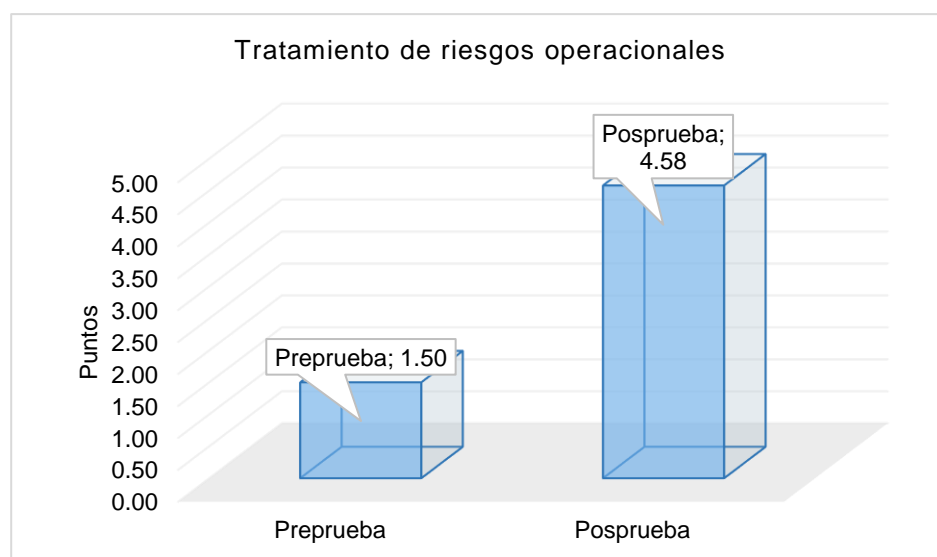


Figura 3. Medias de preprueba y posprueba del indicador 3

- **Análisis inferencial**

Se determinó las pruebas estadísticas para determinar la normalidad en cada indicador aplicando la prueba Shapiro-Wilk, esto debido a que cada muestra poblacional fue menor o igual que 50.

- Prueba de normalidad para el indicador 1

En este apartado, se redacta las hipótesis para determinar la normalidad del indicador 1 con el grado de significancia equivalente a 0.05.

H₀: “La identificación de los riesgos operacionales (sin la aplicación de la norma internacional ISO 27005) si tiene distribución normalizada”.

H₁: “La identificación de los riesgos operacionales (sin la aplicación de la norma internacional ISO 27005) no tiene distribución normalizada”.

H₀: “La identificación de los riesgos operacionales (con la aplicación de la norma internacional ISO 27005) no tiene distribución normalizada”.

H₁: “La identificación de los riesgos operacionales (con la aplicación de la norma internacional ISO 27005) si tiene distribución normalizada”.

Se contó con el grado de significancia: $\alpha = 0.05$

Con el grado de Sig. > 0.05, se admite la hipótesis negativa (H₀)

Con el grado de Sig. <= 0.05, se admite la hipótesis positiva (H₁)

Tabla 5. Prueba de normalidad del indicador 1

	Shapiro-Wilk		
	Estadístico	gl	Sig.
IRO-PrePrueba	,829	3	,187
IRO-PosPrueba	,999	3	,956

Fuente: (Elaboración Propia, 2022)

Basado en lo mostrado en la anterior tabla, el grado de significancia para el indicador en Preprueba fue de 0.187 (> 0.05); lo que implicó, admitir la primera hipótesis negativa; es decir que, si se tiene una distribución normalizada.

Basado en lo mostrado en la anterior tabla, el grado de significancia para el indicador en Posprueba fue de 0.956 (> 0.05); lo que implicó, admitir la segunda hipótesis negativa; es decir, no se tiene una distribución normalizada.

Al evaluar ambas hipótesis, se determinó que, no existía distribución normalizada, lo que significó el empleo de la prueba no paramétrica de Wilcoxon.

Asimismo, se muestra los histogramas respectivos:

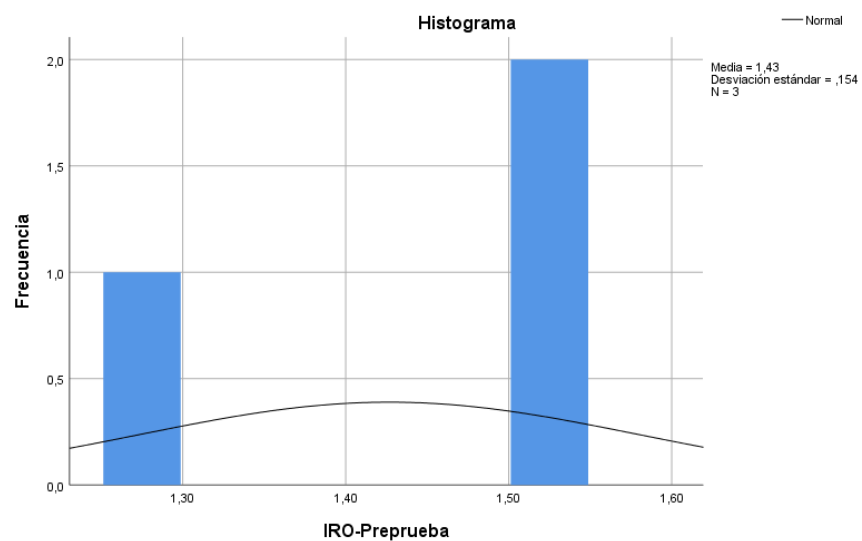


Figura 4. Histograma del indicador 1 (Preprueba)

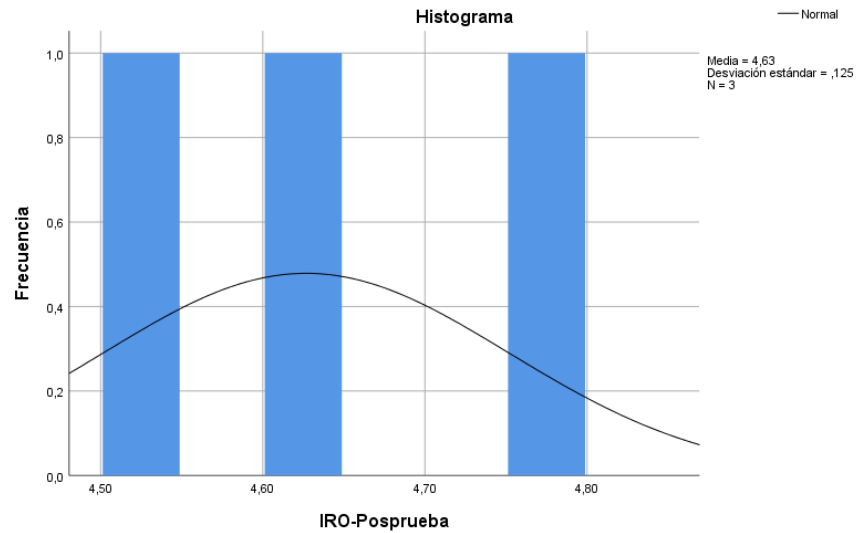


Figura 5. Histograma del indicador 1 (Posprueba)

- Prueba de normalidad para el indicador 2

En este apartado, se redacta las hipótesis para determinar la normalidad del indicador 1 con el grado de significancia equivalente a 0.05.

H₀: “La evaluación de los riesgos operacionales (sin la aplicación de la norma internacional ISO 27005) si tiene distribución normalizada”.

H₁: “La evaluación de los riesgos operacionales (sin la aplicación de la norma internacional ISO 27005) no tiene distribución normalizada”.

H₀: “La evaluación de los riesgos operacionales (con la aplicación de la norma internacional ISO 27005) no tiene distribución normalizada”.

H₁: “La evaluación de los riesgos operacionales (con la aplicación de la norma internacional ISO 27005) si tiene distribución normalizada”.

Se contó con el grado de significancia: $\alpha = 0.05$

Con el grado de Sig. > 0.05, se admite la hipótesis negativa (H₀)

Con el grado de Sig. <= 0.05, se admite la hipótesis positiva (H₁)

Tabla 6. Prueba de normalidad del indicador 2

	Shapiro-Wilk		
	Estadístico	gl	Sig.
ERO-Preprueba	,832	3	,193
ERO-Posprueba	1,000	3	1,000

Fuente: (Elaboración Propia, 2022)

Basado en lo mostrado en la anterior tabla, el grado de significancia para el indicador en Preprueba fue de 0.193 (> 0.05); lo que implicó, admitir la primera hipótesis negativa; es decir que, si se tiene una distribución normalizada.

Basado en lo mostrado en la anterior tabla, el grado de significancia para el indicador en Posprueba fue de 1.000 (> 0.05); lo que implicó, admitir la segunda hipótesis negativa; es decir, no se tenía una distribución normalizada.

Al evaluar ambas hipótesis, se determinó que, no existía distribución normalizada, lo que significó el empleo de la prueba no paramétrica de Wilcoxon.

Asimismo, se muestra los histogramas respectivos:

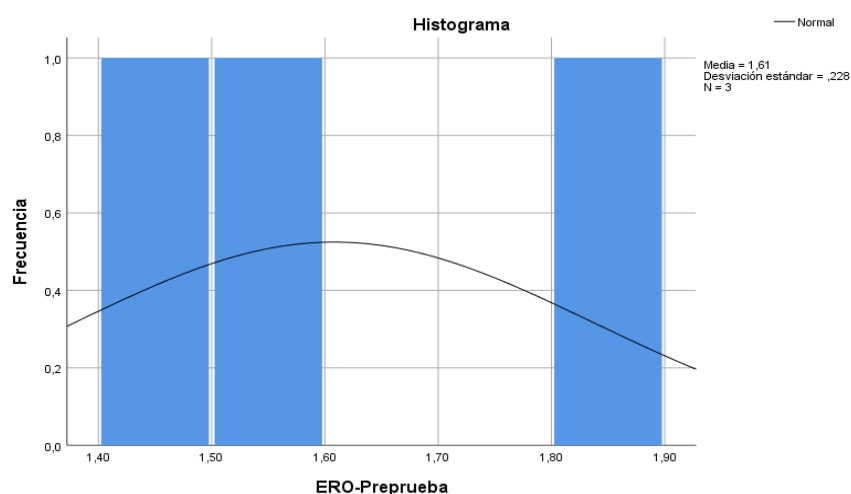


Figura 6. Histograma del indicador 2 (Preprueba)

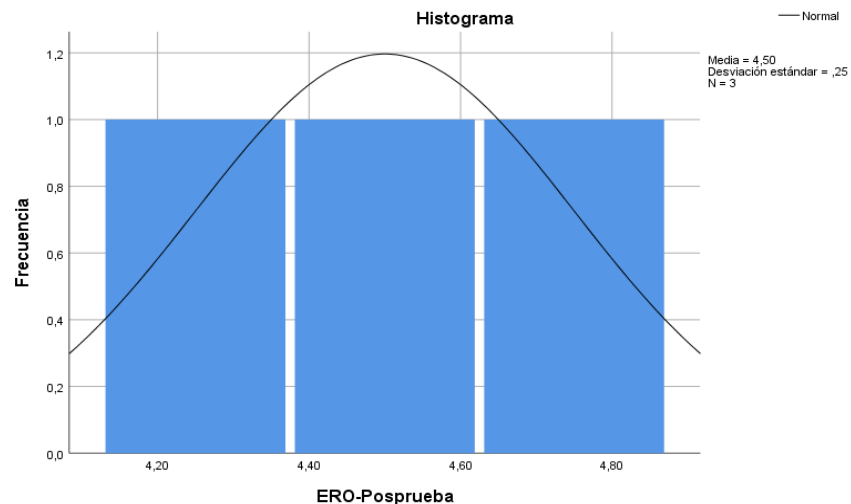


Figura 7. Histograma del indicador 2 (Posprueba)

- Prueba de normalidad para el indicador 3

En este apartado, se redacta las hipótesis para determinar la normalidad del indicador 1 con el valor de significancia equivalente a 0.05.

H₀: “La evaluación de los riesgos operacionales (sin la aplicación de la norma internacional ISO 27005) si tiene distribución normalizada”.

H₁: “La evaluación de los riesgos operacionales (sin la aplicación de la norma internacional ISO 27005) no tiene distribución normalizada”.

H₀: “La evaluación de los riesgos operacionales (con la aplicación de la norma internacional ISO 27005) no tiene distribución normalizada”.

H₁: “La evaluación de los riesgos operacionales (con la aplicación de la norma internacional ISO 27005) si tiene distribución normalizada”.

Se contó con el grado de significancia: $\alpha = 0.05$

Con el grado de Sig. > 0.05, se admite la hipótesis negativa (H₀)

Con el grado de Sig. <= 0.05, se admite la hipótesis positiva (H₁)

Tabla 7. Prueba de normalidad del indicador 3

	Shapiro-Wilk		
	Estadístico	gl	Sig.
TRO-PrePrueba	,999	3	,956
TRO-PosPrueba	,750	3	,000

Fuente: (Elaboración Propia, 2022)

Basado en lo mostrado en la anterior tabla, el grado de significancia para el indicador en Preprueba fue de 0.956 (> 0.05); lo que implicó, admitir la primera hipótesis negativa; es decir que, si se tiene una distribución normalizada.

Basado en lo mostrado en la anterior tabla, el grado de significancia para el indicador en Posprueba fue de 0.000 (< 0.05); lo que implicó, admitir la segunda hipótesis positiva; es decir, si se tenía una distribución normalizada.

Al evaluar ambas hipótesis, se determinó que, si existía distribución normalizada, lo que significó el empleo de la prueba paramétrica de T-Student.

Asimismo, se muestra los histogramas respectivos:

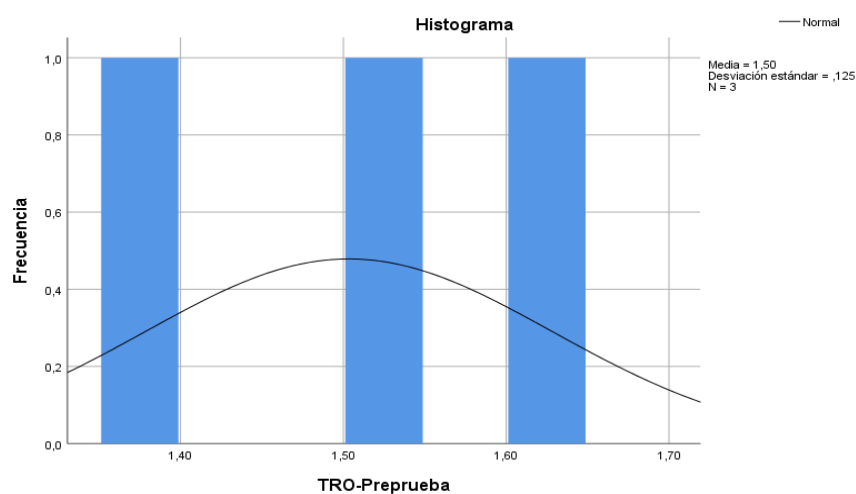


Figura 8. Histograma del indicador 3 (Preprueba)

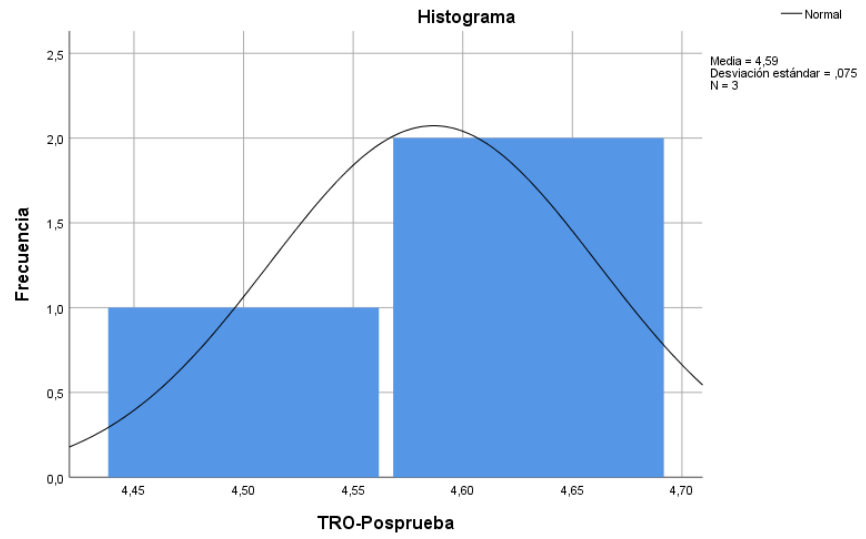


Figura 9. Histograma del indicador 3 (Posprueba)

- **Contrastación de hipótesis**

Con respecto a este apartado, se tiene que:

Las muestras poblacionales que no seguían una distribución normalizada emplearon la prueba no paramétrica de Wilcoxon.

Las muestras poblacionales que si seguían una distribución normalizada emplearon la prueba paramétrica de T-Student.

- Hipótesis específica 1:

“La aplicación de la norma internacional ISO 27005 mejora la identificación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

Hipótesis estadísticas:

H₀: “La aplicación de la norma internacional ISO 27005 no mejora la identificación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

$$H_0: IROa \geq IROp$$

H₁: “La aplicación de la norma internacional ISO 27005 si mejora la identificación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

$$H_1: IROa < IROp$$

Se contó con el grado de significancia: $\alpha = 0.05$.

Con el grado de Sig. > 0.05, se admite la hipótesis negativa (H₀)

Con el grado de Sig. <= 0.05, se admite la hipótesis positiva (H₁)

Tabla 8. Prueba Wilcoxon para el indicador 1

Estadísticos de prueba ^a	
IRO-Posprueba - IRO-Posprueba	
Z	-1,633 ^b
Sig. asintótica(bilateral)	,012

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: (Elaboración propia, 2022)

El grado de significancia generado fue 0.012 (< 0.05) rechazando la hipótesis negativa y aceptando la hipótesis positiva. Se concluyó que: “La aplicación de la norma internacional ISO 27005 si mejora de forma significativa la identificación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

- Hipótesis específica N° 2

“La aplicación de la norma internacional ISO 27005 mejora la evaluación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

Hipótesis estadísticas:

H₀: “La aplicación de la norma internacional ISO 27005 no mejora la evaluación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

$$H_0: EROa \geq EROp$$

H₁: “La aplicación de la norma internacional ISO 27005 si mejora la evaluación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

$$H_1: EROa < EROp$$

Se contó con el grado de significancia: $\alpha = 0.05$.

Con el grado de Sig. > 0.05, se admite la hipótesis negativa (H_0)

Con el grado de Sig. \leq 0.05, se admite la hipótesis positiva (H_1)

Tabla 9. Prueba Wilcoxon para el indicador 2

Estadísticos de prueba ^a	
ERO-Posprueba - ERO-Posprueba	
Z	-1,604 ^b
Sig. asintótica(bilateral)	,019

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: (Elaboración propia, 2022)

El valor de significancia generado fue 0.019 ($<$ 0.05) rechazando la hipótesis negativa y aceptando la hipótesis positiva. Se concluyó que: “La aplicación de la norma internacional ISO 27005 si mejora de forma significativa la evaluación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

- Hipótesis específica N° 3

“La aplicación de la norma internacional ISO 27005 mejora el tratamiento de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

Hipótesis estadísticas:

H_0 : “La aplicación de la norma internacional ISO 27005 no mejora el tratamiento de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

H_0 : $TRO_a \geq TRO_p$

H₁: “La aplicación de la norma internacional ISO 27005 si mejora el tratamiento de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

$$H_1: TRO_a < TRO_p$$

Se contó con el valor de significancia: $\alpha = 0.05$.

Con el grado de Sig. > 0.05, se admite la hipótesis negativa (H₀)

Con el grado de Sig. <= 0.05, se admite la hipótesis positiva (H₁)

Tabla 10. Prueba T-Student para el indicador 3

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
TRO_Preprueba TRO_Posprueba	-3,08333	,14434	,08333	-3,44189	-2,72478	-37,000	2	,001

Fuente: (Elaboración propia, 2022)

El valor de T calculado es -37.000 y es mayor a -1.5924, rechazando la hipótesis negativa y aceptando la hipótesis positiva. Se concluyó que: “La aplicación de la norma internacional ISO 27005 si mejora de forma significativa el tratamiento de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.

V. DISCUSIÓN

Con respecto al indicador 1 “Identificación de riesgos operacionales”, los valores estadísticos generados antes y después de la aplicación de la norma internacional ISO 27005 fueron 1.43 y 4.63 puntos respectivamente, generando un incremento de 3.20 puntos (Δ 64.00%). Estos resultados fueron equiparables a los obtenidos por (Fajardo, 2021), quien buscó brindar los requisitos para adaptar una apropiada examinación de riesgos sobre los activos de tecnología críticos en una empresa, teniendo como meta incrementar la información segura en estos activos combinando las mejores prácticas y recomendaciones a nivel legislativo y normativo que fundamentan los procesos de gestión en seguridad. Del mismo modo, son equiparables con (Jacho, 2020), quien buscó determinar las vulnerabilidades de los procedimientos informáticos que poseía la compañía mediante el estándar mundial ISO 27005:2013. La metodología aplicada fue en cascada mediante el desarrollo de cinco (5) fases: Descubrimiento, Exploración, Evaluación, Intrusión y Reporte, las cuales se encargaban de reconocer las vulnerabilidades presentes. Como resultado, se identificó que la empresa poseía sistemas operativos Windows desactualizados pudiendo ser utilizados como una oportunidad abierta para los atacantes informáticos. Las conclusiones demostraron que el estándar ISO 27005 ayudó a minimizar los incidentes de seguridad en la red administrativa. Lo anterior, se sustenta en la teoría de la gestión de riesgos basado en la norma internacional ISO 27005 como marco sistemático orientado a la administración de riesgos en materia de seguridad informática necesarios para la identificación de los requisitos seguros de información que exige la entidad con el fin de proponer un sistema de administración de información segura y eficaz (PECB, 2020).

Con respecto al indicador 2 “Evaluación de riesgos operacionales”, los valores estadísticos generados antes y después de la aplicación de la norma internacional ISO 27005 fueron 1.61 y 4.50 puntos respectivamente, generando un incremento de 2.89 puntos (Δ 57.80%). Estos resultados son equiparables a los obtenidos por (Nañez, 2020), quien buscó desarrollar un modelo de administración de riesgos basados en TI sobre la base del estándar mundial ISO 27005, así como el uso del método MAGERIT a fin de optimizar

la gestión segura de la información en una Universidad de la ciudad de Chachapoyas - Perú. La propuesta representó un incremento valioso en la satisfacción de los usuarios con respecto a la administración de los servicios tecnológicos de la Universidad garantizando que los riesgos relacionados a TI sean conocidos, asumidos, administrados y reducidos de forma documental, sistémica, organizada, repetitiva, efectiva y configurable generando todos los cambios necesarios respecto a los riesgos, el medio ambiente y las tecnologías adoptadas por la entidad de educación superior. Del mismo modo, fueron equiparables por (Ordeñana, 2019), quien presento la implementación de la administración de los riesgos informáticos sobre la base del estándar ISO 27005 en las bases de datos y sistemas operativos de un departamento informático teniendo como meta la mitigación de los problemas en niveles lógico, físico y organizativo empleando el método combinado del ciclo de Deming y el estándar mundial ISO 27005; logrando para ello, la identificación de los activos más relevantes en el campo base de la organización y sus objetivos, evaluando posteriormente la ejecución de la administración de los riesgos, y finalmente observando los resultados generados así como las conclusiones en materia de administración de riesgos con el uso de un método adaptado. Lo anterior, se sustenta en la teoría de la gestión de riesgos basado en la norma internacional ISO 27005, consistente con las definiciones tratadas sobre el estándar mundial ISO/IEC 27001 y, está diseñado para permitir el desarrollo de manera efectiva la información segura sobre la base de un enfoque de riesgos (CESCE, 2021).

Con respecto al indicador 3 "Tratamiento de riesgos operacionales", los valores estadísticos generados antes y después de la aplicación de la norma internacional ISO 27005 fueron 1.50 y 4.58 puntos respectivamente, generando un incremento de 2.88 puntos (Δ 61.80%). Estos resultados fueron equiparables a los obtenidos por (Patiño, 2018), quien buscó conocer el estándar mundial ISO 27005 determinando el nivel de mitigación de los riesgos informáticos en entidades públicas que se sometieron a un estudio cualitativo-cuantitativo con alcance descriptivo y una muestra no probabilística. Se puso en práctica un cuestionario a dieciocho (18) gerentes de tecnología de entidades públicas ubicadas en la ciudad de Esmeraldas.

Como regla, a pesar de la inclusión de regulaciones internacionales, todavía es difícil obtener esto, porque los estándares fueron creados para empresas desarrolladas en un contexto diferente. En respuesta, se propuso una guía detallada, desarrollando cada paso con su conjunto de actividades e implementándola en la comunidad del sector público para validar cada paso predefinido. Del mismo modo, fueron equiparables por (Puyén, y otros, 2018), quienes buscaron proponer la mejora de la administración informática a nivel seguro en un Hospital mediante el desarrollo de un modelo de administración de riesgos empleando el estándar mundial ISO 27005 y la aplicación del método MAGERIT. Lo anterior, se sustenta en la teoría de la gestión de riesgos basado en la norma internacional ISO 27005 para la adquisición de destrezas y experiencias cognitivas fundamentales para la implementación del proceso de administración de los riesgos de seguridad informática. En tal sentido, se debía identificar, evaluar, examinar y abordar los múltiples riesgos de seguridad informática presentes en diversas organizaciones (PECB, 2020).

VI. CONCLUSIONES

1. Se consiguió mejorar la identificación de los riesgos operacionales generando un incremento de 3.20 puntos (Δ 64.00%). Se inició con una Preprueba media de 1.43 puntos y se terminó con una Posprueba media de 4.63 puntos luego de la aplicación de la norma internacional ISO 27005 en la empresa CANVIA de la ciudad de Lima en el año 2022.
2. Se consiguió mejorar la evaluación de los riesgos operacionales generando un incremento de 2.89 puntos (Δ 57.80%). Se inició con una Preprueba media de 1.61 puntos y se terminó con una Posprueba media de 4.50 puntos luego de la aplicación de la norma internacional ISO 27005 en la empresa CANVIA de la ciudad de Lima en el año 2022.
3. Se consiguió mejorar la identificación de los riesgos operacionales generando un incremento de 2.88 puntos (Δ 61.80%). Se inició con una Preprueba media de 1.50 puntos y se terminó con una Posprueba media de 4.58 puntos luego de la aplicación de la norma internacional ISO 27005 en la empresa CANVIA de la ciudad de Lima en el año 2022.

VII. RECOMENDACIONES

Al CEO:

Se recomienda la implementación de la solución propuesta en este trabajo en base a la plataforma tecnológica que brinda el soporte necesario para la gestión del riesgo operacional en la empresa CANVIA.

Al Smart Operations Manager:

Se recomienda completar el ciclo de mejora continuando con el desarrollo de propuestas para la automatización de la gestión del riesgo operacional en CANVIA.

Al CHRO:

Se recomienda planificar capacitaciones técnicas a los empleados de la empresa CANVIA para que comprendan y manejen la gestión del riesgo operacional.

A los colaboradores:

Se recomienda incluir en la jornada de trabajo las buenas prácticas de gestión del riesgo operacional según el estándar internacional ISO 27005.

REFERENCIAS

- Arévalo, María. 2022.** Importancia de la gestión de riesgos dentro de las empresas. [En línea] 13 de Octubre de 2022. [Citado el: 20 de Mayo de 2022.] <https://www.piranirisk.com/es/blog/conozca-la-importancia-de-la-gestion-de-riesgos-dentro-de-las-empresas>.
- BBVA. 2015.** Riesgo Operacional. [En línea] 1 de Enero de 2015. [Citado el: 20 de Mayo de 2022.] <https://shareholdersandinvestors.bbva.com/microsites/pilarIII2015/es/3/apr.html>.
- Cáceres, Isabel. 2018.** Gestión Eficaz de Riesgos. [En línea] 11 de Mayo de 2018. [Citado el: 20 de Mayo de 2022.] <https://www.mcasares.es/>.
- CANVIA. 2018.** Portal Corporativo. [En línea] 1 de Enero de 2018. <https://www.canvia.com/>.
- CESCE. 2021.** ¿Qué es el riesgo operacional? [En línea] 20 de Enero de 2021. [Citado el: 20 de Mayo de 2022.] <https://www.cesce.es/es/w/asesores-de-pymes/que-es-el-riesgo-operacional>.
- Chunga, Katia. 2017.** *"Análisis de Riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basado en las directrices de la ISO/IEC 27005"*. Piura : UCV, 2017.
- Fajardo, Roland. 2021.** *"Evaluación de Riesgos de Seguridad de la Información para la Empresa MAKOTO S.A. basada en la Norma ISO 27005:2018"*. Bogotá : UCATOLICA, 2021.
- ISO 27001. 2020.** Análisis de riesgos en ISO 27001. [En línea] 7 de Enero de 2020. <https://www.escuelaeuropeaexcelencia.com/2020/01/analisis-de-riesgos-en-iso-27001-evaluar-consecuencias-y-probabilidades/#:~:text=La%20evaluaci%C3%B3n%20cuantitativa%20en%20un,u sualmente%20expresados%20en%20cifras%20monetarias..>
- ISO Tools Excellence. 2016.** Norma ISO 27002. [En línea] 01 de 01 de 2016. [Citado el: 15 de 03 de 2018.] <https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/>.
- 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.

<https://www.isotools.org/2018/08/15/iso-iec-270052018-reducira-el-riesgo-de-brechas-en-la-seguridad/>.

Jacho, Víctor. 2020. *"Auditoría de seguridad informática basada en el estándar ISO 27001:2013 para detectar y explotar vulnerabilidades en una red administrativa simulada para una empresa proveedora de servicios"*. Guayaquil : UG, 2020.

Martínez, Nayiber. 2016. *"La Importancia de la Identificación de los Riesgos Operativos en una Entidad Financiera en Colombia"*. Bogotá : UNIMILITAR, 2016.

Nañez, Óscar. 2020. *"Modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas Perú"*. Chachapoyas : UNPRG, 2020.

Nusa, I. y Faisal, F. 2015. Web-Based Information Systems: Developing a Design Theory. [En línea] 12 de Mayo de 2015. [Citado el: 16 de Mayo de 2022.] <https://iopscience.iop.org/article/10.1088/1757-899X/879/1/012015/pdf>.

Ordeñana, 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 : CORE, 2019.

PAE. 2018. MAGERIT v3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea] 1 de Enero de 2018. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

Palomares, Miriam. 2016. *"Sistema de seguridad informática para los riesgos en la red de datos de la Empresa Grupo Palomares SAC"*. Lima : UCV, 2016.

Patiño, Susana. 2018. *"Propuesta Metodológica de Gestión de Riesgos de Tecnología de Información y Comunicación (TIC) para Entidades Públicas conforme Normativa NTE INEN ISO/IEC 27005"*. Sangolquí : ESPE, 2018.

PECB. 2020. Capacitaciones en Riesgos de Seguridad de la Información ISO/IEC 27005. [En línea] 1 de Enero de 2020. <https://pecb.com/es/education-and-certification-for-individuals/iso-iec-27005>.

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

Puyén, Vicente y Rivas, Betty. 2018. *"Modelo de Gestión de Riesgos basado en la ISO/IEC 27005 y la Metodología MAGERIT para mejorar la Gestión de Seguridad de la Información en el Hospital Regional Lambayeque"*. Lambayeque : UNPRG, 2018.

Quispe, Esai y Pacheco, Diego. 2018. *"Modelo de evaluación de riesgos de seguridad de la información basado en la ISO/IEC 27005 para analizar la viabilidad de adoptar un servicio en la nube"*. Lima : UPC, 2018.

Temitope, A., Ahmad, R. y Olanrewaju, A. 2018. Examining the information dissemination process on social media during the Malaysia 2014 floods using Social Network Analysis (SNA). [En línea] 1 de Enero de 2018. [Citado el: 30 de Abril de 2022.]

https://www.researchgate.net/publication/322939084_Examining_the_information_dissemination_process_on_social_media_during_the_Malaysia_2014_floods_using_Social_Network_Analysis_SNA.

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. 2020. Parches de seguridad de Windows. [En línea] 4 de Septiembre de 2020. <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 27005 para la Gestión de riesgos operacionales en la empresa CANVIA, Lima 2022

Autor: Abad García, Igor Alexey

Problema	Objetivo	Hipótesis	Variable
<p>General:</p> <p>¿De qué modo la aplicación de la norma internacional ISO 27005 impacta en la gestión de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022?</p>	<p>General:</p> <p>Mejorar la gestión de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022 mediante la aplicación de la norma internacional ISO 27005.</p>	<p>General:</p> <p>“La aplicación de la norma internacional ISO 27005 mejora significativamente la gestión de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”.</p>	<p>Independiente:</p> <p>Norma internacional ISO 27005</p>
<p>Específicos:</p> <ol style="list-style-type: none"> 1. ¿De qué modo la aplicación de la norma internacional ISO 27005 influye en la identificación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima el año 2022? 2. ¿De qué modo la aplicación de la norma internacional ISO 27005 impacta en la evaluación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima el año 2022? 3. ¿De qué modo la aplicación de la norma internacional ISO 27005 impacta en el tratamiento de riesgos operacionales en la empresa CANVIA de la ciudad de Lima el año 2022? 	<p>Específicos:</p> <ol style="list-style-type: none"> 1. Mejorar la identificación de riesgos operacionales en la empresa. 2. Mejorar la evaluación de riesgos operacionales en la empresa. 3. Mejorar el tratamiento de riesgos operacionales en la empresa. 	<p>Específicas:</p> <ol style="list-style-type: none"> 1. “La aplicación de la norma internacional ISO 27005 mejora la identificación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”. 2. “La aplicación de la norma internacional ISO 27005 mejora la evaluación de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”. 3. “La aplicación de la norma internacional ISO 27005 mejora el tratamiento de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”. 4. “La aplicación de la norma internacional ISO 27005 mejora el monitoreo de riesgos operacionales en la empresa CANVIA de la ciudad de Lima en el año 2022”. 	<p>Dependiente:</p> <p>Gestión de riesgos operacionales</p>

Metodología			
<p>Tipo de investigación: Aplicada</p>	<p>Población (N): <i>N = 8 personas</i></p>	<p>Técnicas de recolección de datos:</p> <ul style="list-style-type: none"> • Encuesta • Análisis documental 	<p>Método de análisis de datos:</p> <ul style="list-style-type: none"> • Estadística descriptiva • Estadística inferencial • Deductivo (enfoque cuantitativo)
<p>Diseño de investigación: Preexperimental</p>	<p>Muestra (n): <i>n = 8 personas</i></p>	<p>Instrumentos de recolección de datos:</p> <ul style="list-style-type: none"> • Cuestionario • Ficha de datos 	<p>Aspectos éticos:</p> <p>Se respetará el derecho a la propiedad intelectual (Originalidad de la investigación - Reporte Turnitin).</p> <p>Se tomará en cuenta el Código de ética de la Universidad César Vallejo (RCU N° 0126-2017/UCV).</p> <p>Se usará para la redacción de las referencias bibliográficas el sistema de Normas ISO-690.</p>

Anexo 2 - Matriz de operacionalización de variables

Variable	Definición Conceptual	Definición Operacional	Dimensión (Sub variable)	Indicador	Escala de medición
Independiente: Norma internacional ISO 27005	“Directrices para crear un entorno de sistemas para la administración de riesgos de seguridad informática y de información” (PECB, 2020).	La norma internacional ISO 27005 se puede medir a través de la ejecución y gestión eficaz de un método de administración de riesgos de seguridad de informática y de información en las organizaciones.			
Dependiente: Gestión de riesgos operacionales	Uno que puede resultar en detrimentos por causa de fallas humanos, sucesos internos inadecuados o deficientes, errores del sistema y sucesos del entorno” (BBVA, 2015).	La gestión de riesgos operacionales se puede medir por la caracterización, valoración y tratamiento de los mismos.	Riesgo	Identificación del riesgo operacional	Ordinal
				Evaluación del riesgo operacional	Ordinal
				Tratamiento del riesgo operacional	Ordinal

Anexo 3 - Juicio experto para la elección de la metodología de trabajo

Apellidos y nombres del experto: Agreda Gamboa, Everson David

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

Fecha: 15/05/2022

Título de la investigación: "Aplicación de la norma internacional ISO 27005 para la Gestión de riesgos operacionales en la empresa CANMIA, Lima 2022".

Autor: Abad García, Igor Alexey

Evaluación de la norma internacional/metodología de gestión de riesgos (1)

Mediante el método de juicio experto, Usted tiene la facultad de calificar las metodologías/marcos de trabajo 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	Norma internacional / Metodología		
		ISO 27005	ISO 27002	MAGERIT
1	Complejidad	3	2	2
2	Tiempo de desarrollo	3	2	2
3	Información	3	3	2
4	Requerimientos	3	2	2
5	Claridad	3	3	1
6	Coherencia	3	3	2
Total		18	15	11

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

Sugerencias: Ninguna.



Firma del experto

Apellidos y nombres del experto: Mendoza Rivera, Ricardo Darío

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

Fecha: 15/05/2022

Título de la investigación: "Aplicación de la norma internacional ISO 27005 para la Gestión de riesgos operacionales en la empresa CANMIA, Lima 2022".

Autor: Abad García, Igor Alexey

Evaluación de la norma internacional/metodología de gestión de riesgos (2)

Mediante el método de juicio experto, Usted tiene la facultad de calificar las metodologías/marcos de trabajo 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	Norma internacional / Metodología		
		ISO 27005	ISO 27005	ISO 27005
1	Complejidad	2	2	2
2	Tiempo de desarrollo	3	2	2
3	Información	3	2	2
4	Requerimientos	3	2	2
5	Claridad	2	2	2
6	Coherencia	3	3	2
Total		18	13	12

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

Sugerencias: Ninguna.



Firma del experto

Apellidos y nombres del experto: Córdova Otero, Juan Luis

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

Fecha: 15/05/2022

Título de la investigación: "Aplicación de la norma internacional ISO 27005 para la Gestión de riesgos operacionales en la empresa CANVIA, Lima 2022".

Autor: Abad García, Igor Alexey

Evaluación de la norma internacional/metodología de gestión de riesgos (3)

Mediante el método de juicio experto, Usted tiene la facultad de calificar las metodologías/marcos de trabajo 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	Norma internacional / Metodología		
		ISO 27005	ISO 27005	ISO 27005
1	Complejidad	3	2	1
2	Tiempo de desarrollo	2	2	2
3	Información	3	3	2
4	Requerimientos	3	2	2
5	Claridad	3	2	1
6	Coherencia	3	2	2
Total		17	13	10

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

Sugerencias: Ninguna.



Firma del experto

Anexo 4. Instrumentos de recolección de datos

Cuestionario aplicado a los Usuarios de la empresa CANVIA

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 operacionales	Riesgo	1. ¿Qué opina Usted sobre el cumplimiento de normatividad estándar para la identificación de riesgos operacionales?					
		2. ¿Qué opina Usted sobre el manejo responsable de la información para la identificación de riesgos operacionales?					
		3. ¿Qué opina Usted sobre las responsabilidades y procedimientos para la identificación de riesgos operacionales?					
		4. ¿Qué opina Usted sobre el cumplimiento de normatividad estándar para la evaluación de riesgos operacionales?					
		5. ¿Qué opina Usted sobre el manejo responsable de la información para la evaluación de riesgos operacionales?					
		6. ¿Qué opina Usted sobre las responsabilidades y procedimientos para la evaluación de riesgos operacionales?					
		7. ¿Qué opina Usted sobre el cumplimiento de normatividad estándar para el tratamiento de riesgos operacionales?					
		8. ¿Qué opina Usted sobre el manejo responsable de la información para el tratamiento de riesgos operacionales?					
		9. ¿Qué opina Usted sobre las responsabilidades y procedimientos para el tratamiento de riesgos operacionales?					

Anexo 5. Validez de los instrumentos de recolección de datos

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

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 de normatividad estándar para la identificación de riesgos operacionales?	x		x		x		
2. ¿Qué opina Usted sobre el manejo responsable de la información para la identificación de riesgos operacionales?	x		x		x		
3. ¿Qué opina Usted sobre las responsabilidades y procedimientos para la identificación de riesgos operacionales?	x		x		x		
4. ¿Qué opina Usted sobre el cumplimiento de normatividad estándar para la evaluación de riesgos operacionales?	x		x		x		
5. ¿Qué opina Usted sobre el manejo responsable de la información para la evaluación de riesgos operacionales?	x		x		x		
6. ¿Qué opina Usted sobre las responsabilidades y procedimientos para la evaluación de riesgos operacionales?	x		x		x		
7. ¿Qué opina Usted sobre el cumplimiento de normatividad estándar para el tratamiento de riesgos operacionales?	x		x		x		
8. ¿Qué opina Usted sobre el manejo responsable de la información para el tratamiento de riesgos operacionales?	x		x		x		
9. ¿Qué opina Usted sobre las responsabilidades y procedimientos para el tratamiento de riesgos operacionales?	x		x		x		

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

2Pertinencia: 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	Tecnologías de la información
	
DNI: 18161457	Trujillo, 25 de junio del 2022

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

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 de normatividad estándar para la identificación de riesgos operacionales?	x		x		x		
2. ¿Qué opina Usted sobre el manejo responsable de la información para la identificación de riesgos operacionales?	x		x		x		
3. ¿Qué opina Usted sobre las responsabilidades y procedimientos para la identificación de riesgos operacionales?	x		x		x		
4. ¿Qué opina Usted sobre el cumplimiento de normatividad estándar para la evaluación de riesgos operacionales?	x		x		x		
5. ¿Qué opina Usted sobre el manejo responsable de la información para la evaluación de riesgos operacionales?	x		x		x		
6. ¿Qué opina Usted sobre las responsabilidades y procedimientos para la evaluación de riesgos operacionales?	x		x		x		
7. ¿Qué opina Usted sobre el cumplimiento de normatividad estándar para el tratamiento de riesgos operacionales?	x		x		x		
8. ¿Qué opina Usted sobre el manejo responsable de la información para el tratamiento de riesgos operacionales?	x		x		x		
9. ¿Qué opina Usted sobre las responsabilidades y procedimientos para el tratamiento de riesgos operacionales?	x		x		x		

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

²Pertinencia: Si el ítem pertenece a la dimensión.

³Relevancia: 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, 18 de junio del 2022

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

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 de normatividad estándar para la identificación de riesgos operacionales?	x		x		x		
2. ¿Qué opina Usted sobre el manejo responsable de la información para la identificación de riesgos operacionales?	x		x		x		
3. ¿Qué opina Usted sobre las responsabilidades y procedimientos para la identificación de riesgos operacionales?	x		x		x		
4. ¿Qué opina Usted sobre el cumplimiento de normatividad estándar para la evaluación de riesgos operacionales?	x		x		x		
5. ¿Qué opina Usted sobre el manejo responsable de la información para la evaluación de riesgos operacionales?	x		x		x		
6. ¿Qué opina Usted sobre las responsabilidades y procedimientos para la evaluación de riesgos operacionales?	x		x		x		
7. ¿Qué opina Usted sobre el cumplimiento de normatividad estándar para el tratamiento de riesgos operacionales?	x		x		x		
8. ¿Qué opina Usted sobre el manejo responsable de la información para el tratamiento de riesgos operacionales?	x		x		x		
9. ¿Qué opina Usted sobre las responsabilidades y procedimientos para el tratamiento de riesgos operacionales?	x		x		x		

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

2Pertinencia: 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 información
	
DNI: 18122765	Trujillo, 18 de junio del 2022

Anexo 6 - Confiabilidad de los instrumentos de recolección de datos

Resumen de procesamiento de casos

		N	%
Casos	Válido	8	100,0
	Excluido ^a	0	,0
	Total	8	100,0

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

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,825	9

Anexo 7. Desarrollo de la solución propuesta

Aplicación de la Norma internacional ISO 27005 para la empresa CANVIA

La norma ISO 27005 es el estándar internacional que se ocupa de la gestión de los riesgos relativos a la seguridad de información. La norma suministra las directrices para la gestión de riesgos, apoyándose fundamentalmente en los requisitos definidos en la ISO 27001.

Se trata de una norma aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización y sustituye a las la normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000 de Gestión de la Información y Comunicaciones Tecnología de Seguridad.

El aumento en el uso de tecnologías de la información puede posibilitar brechas o fisuras en aspectos de seguridad con respecto a su utilización, por ello se hace necesaria una gestión de la información desde una perspectiva tecnológica a tres niveles: aseguramiento y control sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde la perspectiva tecnológica (ISOTools, 2018).

- Proceso de gestión de riesgos bajo la norma internacional ISO 27005

Para la protección adecuada de los sistemas de información y activos de la organización, así como la implementación de sus controles de seguridad, se requiere ejecutar un conjunto de acciones que desarrollen un proceso de gestión de riesgos basado en los activos y los factores tanto internos como externos como se muestra en la figura adjunta (SISTESEG, 2018).

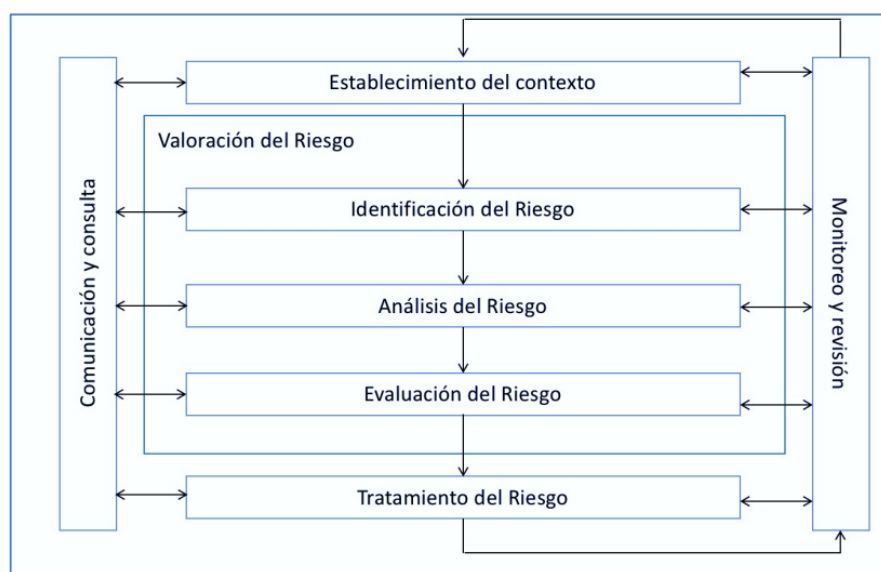


Figura. Proceso de gestión de riesgos.

A continuación, se muestra en la figura adjunta las actividades de cada una de las etapas del proceso de gestión de riesgos, con el fin de identificar con claridad la situación de cada uno de sus activos: valor, vulnerabilidades, y cómo están protegidos frente a amenazas.

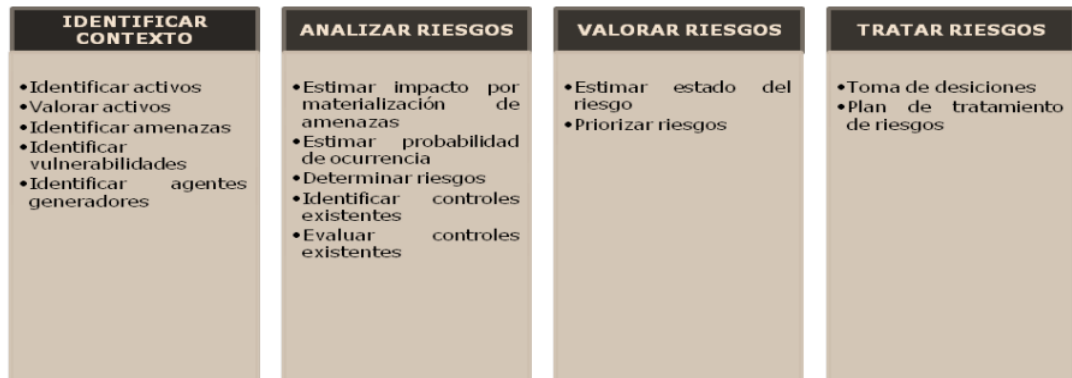


Figura. Etapas de la gestión de riesgos.

- Etapa 1: Identificación del contexto

Tiene como propósito conocer los eventos potenciales, estén o no bajo el control de la organización y que ponen en riesgos sus activos de información.

Entre sus actividades principales, se tiene:

- ✓ Identificación de activos de información

Tabla. Tipos de activos

Activos de información y físicos		
Activos físicos	Infraestructura física	Oficinas
	Hardware	Servidores de la empresa. Dispositivos de conectividad. Computadoras personales de la empresa.
	Software	Aplicaciones y sistemas de información.
Activos de información	Electrónica	Informes del negocio
	Documentos	
Personal	Dueños de información	Directivos de la empresa
	Usuarios de información	Operativos de la empresa
Servicios		Correo electrónico

✓ Valoración de activos

Una vez identificados los activos se realizará la valoración de cada uno de ellos en términos de valor para el negocio según:

❖ Disponibilidad:

Los activos de una determinada organización tendrán mayor valor en la medida que si no están disponibles se impactará gravemente el negocio. Igualmente, un activo que al no estar disponible no afecte de ningún modo el negocio, tendrá un menor valor.

Tabla. Valoración de la disponibilidad de activos

	Valoración de los activos			
	Mínimo (1)	Medio (3)	Grave (5)	Catastrófico (7)
Servicios		x		
Operaciones		x		
Imagen	x			
Cumplimiento	x			

❖ Confidencialidad:

Los activos de información reciben una valoración alta cuando su nivel de confidencialidad es mayor, teniendo en cuenta que la divulgación no autorizada de la misma puede afectar en alguna medida los intereses, imagen y operación de la compañía.

Tabla. Valoración de la confidencialidad de activos

	Infraestructura física	Clasificación
	Activos físicos	Hardware
Software		Uso interno
Activos de información		Electrónica
Personal	Documentos	Confidencial
	Dueños de información	Reservado
Servicios	Usuarios de información	Reservado
		Público

❖ **Integridad:**

Los activos son valorados con mayor valor cuando su alteración puede generar daños graves a la organización.

Tabla. Valoración de la integridad de activos

Activos físicos	Infraestructura física	Afectación
	Hardware	Muy alto
	Software	Alto
Activos de información	Electrónica	Medio
	Documentos	Medio
Personal	Dueños de información	Bajo
	Usuarios de información	Bajo
Servicios		Muy alto

✓ **Identificación de amenazas**

Las amenazas son resultados de actos deliberados que pueden afectar nuestros activos o los activos de información, sin embargo, existen eventos naturales o accidentales que deben ser considerados por su capacidad de generar incidentes de seguridad.

Tabla. Listado de amenazas

Causa	Evento o Amenaza
Eventos naturales	Terremotos, Sismos
Eventos externos	Ausencia de proveedores, conflictos en transporte
Condiciones internas	Ruptura de la cadena de suministro
Actos deliberados	Fallas de hardware, software, red
Actos accidentales	Sabotaje, incendios
Humano	Epidemia (COVID-19)

✓ **Identificación de vulnerabilidades**

Debe identificarse cada una de las amenazas que podrían materializarse; es decir, que vulnerabilidades permiten que las amenazas se conviertan en situaciones de riesgo reales.

Algunos tipos de vulnerabilidades serían:

- ❖ Ausencia de políticas.
- ❖ Empleado descontento.
- ❖ Errores de configuración.
- ❖ Falta de actualizaciones.
- ❖ Uso de servicios inseguros.

- Etapa 2: Análisis de los riesgos

Tiene como propósito establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos, a fin de determinar la capacidad de la organización para su aceptación o manejo.

Entre sus actividades principales, se tiene:

- ✓ Estimación del impacto sobre los activos

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.

Tabla. *Estimación del impacto sobre los activos*

	Infraestructura física	Valoración	Afectación
Activos físicos	Hardware	Muy alto	75%
	Software	Alto	50%
Activos de información	Electrónica	Medio	25%
	Documentos	Medio	25%
Personal	Dueños de información	Bajo	5%
	Usuarios de información	Bajo	5%
Servicios		Muy alto	75%

- ✓ Estimación de la probabilidad de ocurrencia

La probabilidad de ocurrencia se calcula con base en la siguiente tabla:

Tabla. Valoración cualitativa de la frecuencia

	Infraestructura física	Ocurrencia	Frecuencia
Activos físicos	Hardware	10	Frecuente
	Software	10	Frecuente
Activos de información	Electrónica	10	Frecuente
	Documentos	10	Frecuente
Personal	Dueños de información	1	Normal
	Usuarios de información	1	Normal
Servicios		100	Muy frecuente

✓ **Determinación de riesgos**

Conociendo el impacto de las amenazas sobre los activos es posible determinar el nivel de riesgo, teniendo en cuenta la frecuencia de ocurrencia de los incidentes.

Tabla. Determinación de riesgos

	Infraestructura física	Impacto
Activos físicos	Hardware	Muy alto
	Software	Alto
Activos de información	Electrónica	Medio
	Documentos	Medio
Personal	Dueños de información	Bajo
	Usuarios de información	Bajo
Servicios		100

✓ **Identificación de controles existentes**

Los controles existentes son las medidas con que se cuentan para reducir la exposición a los riesgos: procedimientos, mecanismos, controles tecnológicos, etc.

Para identificar los controles existentes puede utilizarse como referencia el estándar ISO/IEC 27001.

✓ Evaluación de controles existentes

Una vez identificados los controles existentes es necesario evaluar su efectividad frente a los riesgos que se pretenden mitigar.

Tabla. Valoración de controles existentes

Evaluación del control	Valores
Control formalmente establecido	Regular
Control perfectamente desplegado, configurado y mantenido	Regular
Procedimientos claros de uso del control y en caso de incidencias	Bueno
Usuarios formados y concienciados sobre la aplicación del control	Deficiente
Control funcional desde el punto de vista teórico y operacional	Regular

• Etapa 3: Valoración de los riesgos

Tiene como propósito determinar el nivel o grado de exposición de la organización a los impactos del riesgo, estimando las prioridades para su tratamiento.

Entre sus actividades principales, se tiene:

✓ Estimación del estado del riesgo

El riesgo se establece considerando los controles existentes, orientados a prevenir que el incidente se presente.

❖ Controles orientados a prevenir el incidente:

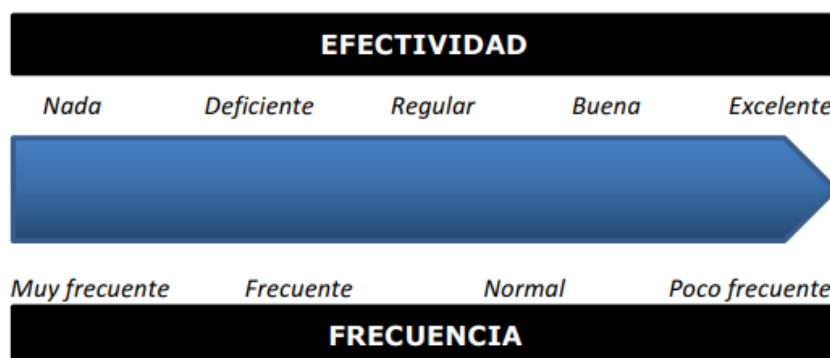


Figura. Efectividad de control y frecuencia

- ❖ Controles que limitan la degradación de activos:



Figura. Efectividad de control y degradación

- ✓ Priorización de riesgos

El riesgo nos muestra el grado de exposición frente a las amenazas evaluadas, es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables, y establecer la prioridad de las acciones requeridas para su tratamiento.

Las acciones que se deben ejecutar se harán con base en la siguiente tabla:

Tabla. Priorización de riesgos

Causa	Evento o Amenaza	Prioridad
Humano	Epidemia (COVID-19)	Muy alto
Eventos externos	Ausencia de proveedores, conflictos en transporte	Alto
Condiciones internas	Ruptura de la cadena de suministro	Medio
Actos deliberados	Fallas de hardware, software, red	Medio
Eventos naturales	Terremotos, Sismos	Bajo
Actos accidentales	Sabotaje, incendios	Bajo

- Etapa 4: Tratamiento de los riesgos

Tiene como propósito estructurar los criterios para la toma de decisiones respecto al tratamiento de los riesgos, en esta etapa se establece las guías de acción

necesarias para coordinar y administrar los eventos que pueden comprometer la confidencialidad, integridad y disponibilidad de los activos.

Entre sus actividades principales, se tiene:

✓ Toma de decisiones

Si el riesgo se ubica en la zona de riesgo Aceptable, permite a la organización aceptarlo; es decir, el riesgo se encuentra en un nivel que puede asumirse sin necesidad de tomar otras medidas de control.

Si el riesgo se ubica en la zona de riesgo Inaceptable, es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible.

Si el riesgo se sitúa en cualquiera de las otras zonas (riesgo tolerable, moderado o importante) se deben tomar medidas para llevar los riesgos a la zona Aceptable, con la implementación de los respectivos controles.

Las medidas dependen del punto en la cual se ubica el riesgo:

Tabla. *Estimación de riesgo sobre los activos*

	Infraestructura física	Medida
Activos físicos	Hardware	Prevenir riesgo
	Software	Revenir riesgo
Activos de información	Electrónica	Compartir riesgo
	Documentos	Compartir riesgo
Personal	Dueños de información	Realizar análisis C/B
	Usuarios de información	Realizar análisis C/B
Servicios		Prevenir

✓ Plan de tratamiento de riesgos

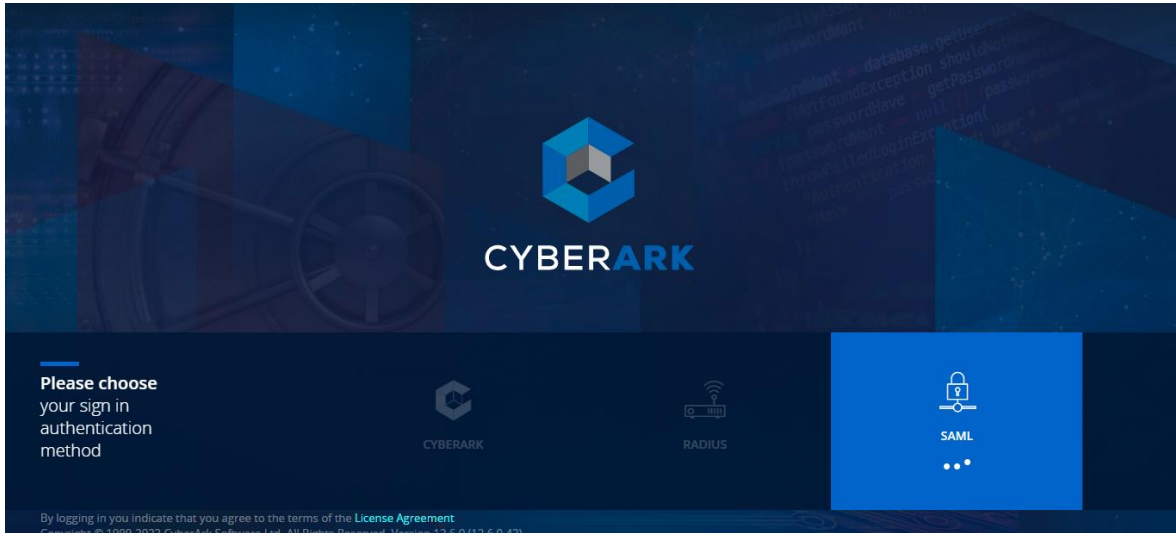
Una vez seleccionado los controles que serán implementados para mitigación de riesgos es necesario elaborar un plan de acción que garantice un efectivo despliegue de los mismos.

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

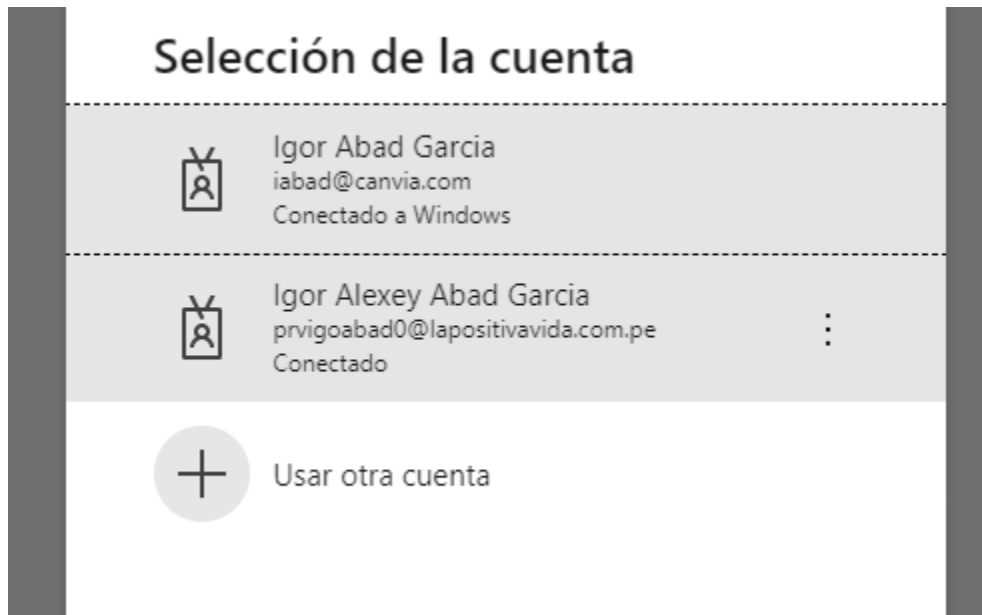
Sistema de monitoreo y control de acceso tipo PAM

Plataforma de control: CyberArk.

Se encarga de controlar los accesos a recursos (Servidores, equipos de usuarios, recursos compartidos).



Plataforma de inicio, utilizando la autenticación tipo SAML



Autenticación con doble factor

Vista de cuentas Último inicio de sesión: 25/10/2022 | prvigoabado

Filter Conexión ad hoc

Vistas Reciente Guardado

Mis cuentas	Estado
Todas las cuentas (predeterminado)	Deshabilitadas por el CPM
Utilizadas recientemente	Con errores
Favoritas	Agregadas recientemente
Sesión cerrada	Deshabilitada por el usuario

2 resultados para: All accounts Mas detalles y acciones en la interfaz clásica

Status	Nombre de usuario	Dirección	ID de plataforma	Safe ↑	Ac	
⚠	T1prvigoabado			Safe_Windows_Igor...	-	Conectar ...
	T1prvigoabado			Safe_Windows_Igor...	-	Conectar ...

Perfil de usuario con las cuentas autenticadas, estas cuentas son monitoreadas y se guarda toda acción generada en cualquier dispositivo, sea móvil, laptop, server, recurso compartido.

2 resultados para: All accounts

Status	Nombre de usuario
⚠	T1prvigoabado
	T1prvigoabado

T1prvigoabado El lapositiva vida Mas detalles y acciones en la interfaz clásica

Plataforma: Dominio_LaPositivaVida Safe: Safe_Windows_Igor_Ab Mostrar Copiar Conectar

Descripción general Detalles Versiones

Estado de conformidad Conforme

2

Días atrás

Cambiado por N/A
Oct 26, 2022 5:29 PM

Reconciliar Cambiar

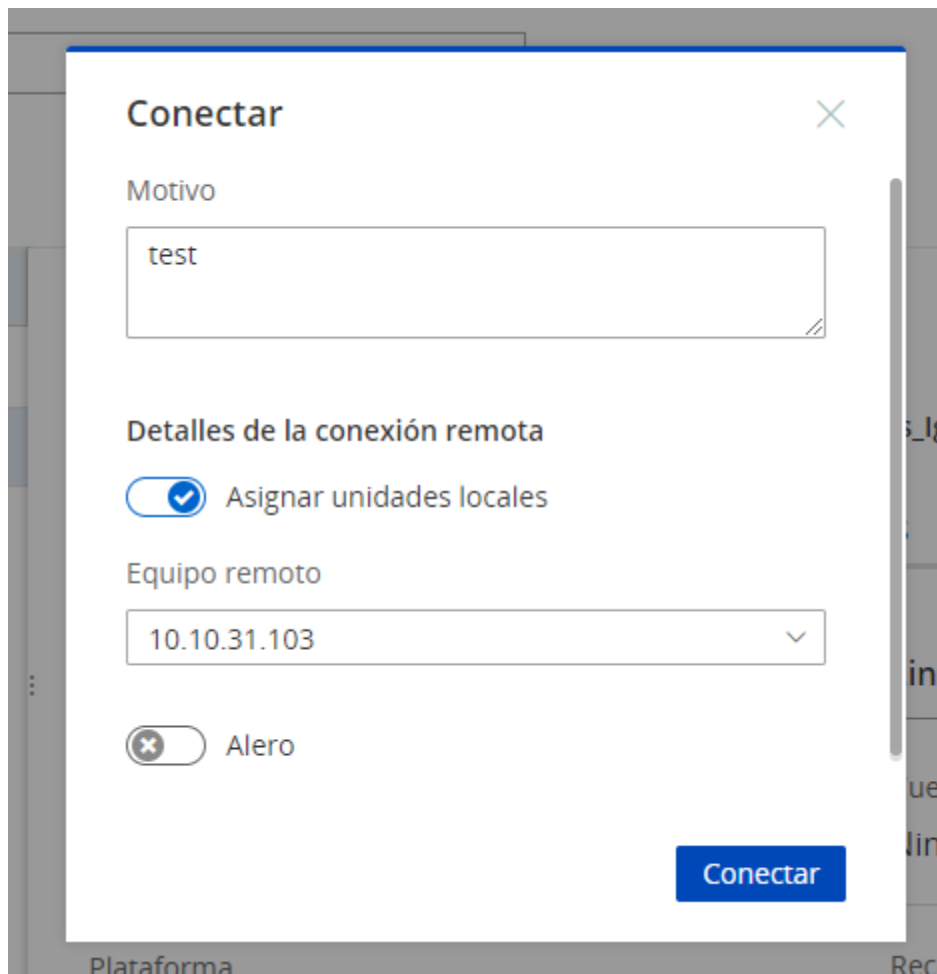
Dependencias

0 TOTAL

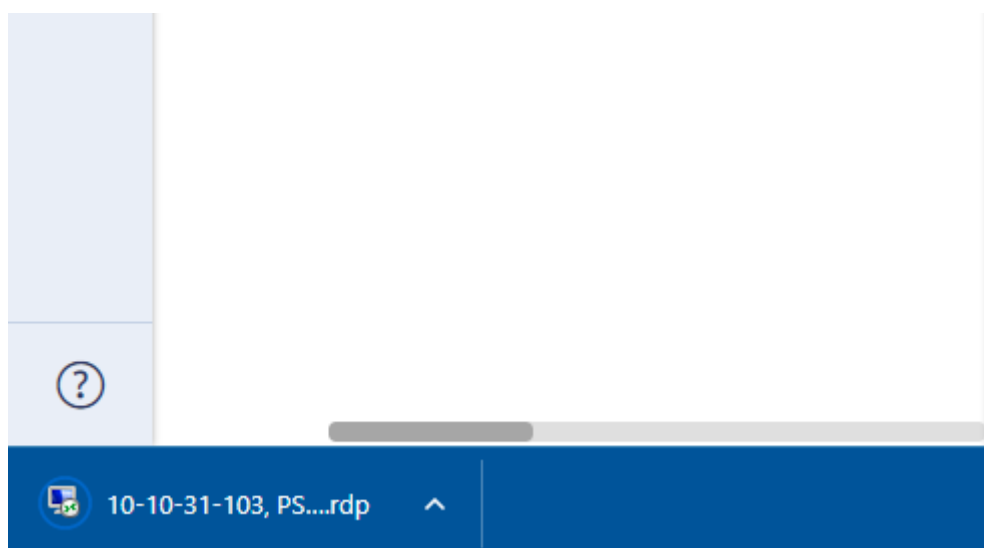
Último acceso

por N/A
Ayer

Detalle de los movimientos de acceso de la cuenta, estado de conformidad en relación a la sincronización con los servidores azure de la empresa y con el AD de la empresa, esto brinda una total auditoria sobre las acciones de la cuenta.



Acción de conectar remotamente vía remote desktop a un equipo, el sistema genera una conexión con doble factor de autenticación para evitar riesgos.



Finalmente se obtiene un acceso configurado y personalizado vía remote desktop anexo a la cuenta de usuario.

Último inicio de sesión: 25/10/2022

 [prvigoabad0](#) 

Información de inicio de sesión

Hora del último inicio de sesión: 25/10/2022 02:05 p. m.

IP de origen del último inicio de sesión: 10.142.44.57

Intentos de inicio de sesión fallidos: 0

Hora del último error de inicio de sesión: -

IP de origen del último error de inicio de sesión: -

Acerca de

Español [\(Cambiar\)](#)

 Cerrar sesión

fe_Windows_18

Versiones

Dependencias

Aquí podemos ver los detalles de la cuenta sobre el perfil.



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 - LIMA NORTE, asesor de Tesis titulada: "Aplicación de la Norma internacional ISO 27005 para la Gestión de riesgos operacionales en la empresa Canvia, Lima 2022", cuyo autor es ABAD GARCIA IGOR ALEXEY, constato que la investigación tiene un índice de similitud de %, 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, 24 de Setiembre del 2022

Apellidos y Nombres del Asesor:	Firma
AGREDA GAMBOA EVERSON DAVID : 18161457 ORCID: 0000-0003-1252-9692	Firmado electrónicamente por: AGREDA el 24-09- 2022 20:40:35

Código documento Trilce: INV - 0913027