UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Marco referencial basado en la ISO 27005 para gestión de riesgos de seguridad de información para empresas consultoras de TI

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

AUTOR:

Capcha Da Costa, Gian Carlos (orcid.org/0000-0003-0007-1071)

ASESOR:

Dr. Mendoza Apaza, Fernando (ORCID: 0000-0001-7981-8291)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo Económico, Empleo y Emprendimiento

Lima - Perú

2022

Dedicatoria

Esta tesis está dedicado a mi familia quienes son parte importante de mi vida, me apoyaron desde el primer momento para realizar este trabajo

Agradecimiento

Al Mg. Javier Seclen quien me guio y me brindo sus conocimientos en la realización de esta tesis. A mis padres por confiar, por las enseñanzas y los valores inculcados. Por último, a mis amigos de la vida y familiar por el apoyo incondicional.

Índice de contenidos

Índice de Tablas

Índice de Figuras

Resumen

El objetivo del presente trabajo fue determinar la eficacia del Marco de referencia basado en la ISO 27005 para la gestión de riesgos de seguridad de la información en consultoras de TI, como metodología se utilizó la ISO 27005 la medición se realizó por medio de tres indicadores: porcentaje de riesgos mitigados, porcentaje de incidentes resueltas de seguridad de información, Nivel de satisfacción respecto a la gestión de riesgos de seguridad de información. Los resultados indicaron que el marco referencial basado en la ISO 27005 fue eficaz en la gestión de riesgos de seguridad de la información en consultoras de TI, se concluyó que en el indicador porcentaje de riesgos mitigados incrementó en un 19,52%, para el indicador porcentaje de incidentes resueltas de seguridad de información incremento en un 13,98% por último el indicador nivel de satisfacción respecto a la gestión de riesgos de seguridad de información el 80,0% de los encuestados indicó sentirse totalmente de acuerdo. En conclusión, esta normativa ISO 27005 fue beneficiosa para los indicadores puesto que demostraron que un incremento en el porcentaje de incidentes resueltas y los riesgos mitigados también ayudando a que los trabajadores se sientan más seguros con los controles respectivos frente a los peligros informáticos que los perjudican.

Palabras clave: ISO 27005, Gestión de riesgos de seguridad de información, Consultoras de TI

Abstract

The objective of the present work was to determine the effectiveness of the Reference Framework based on ISO 27005 for the management of information security risks in IT consultants, as a methodology the ISO 27005 was used, the measurement was carried out by means of three indicators: percentage of risks mitigated, percentage of resolved information security incidents, level of satisfaction regarding information security risk management. The results indicated that the referential framework based on ISO 27005 was effective in the management of information security risks in IT consultants, it was concluded that in the indicator percentage of mitigated risks it increased by 19.52%, for the indicator percentage of resolved information security incidents increased by 13.98% lastly, the level of satisfaction indicator regarding information security risk management, 80.0% of those surveyed indicated that they felt totally in agreement. In conclusion, this ISO 27005 standard was beneficial for the indicators since it demonstrated that an increase in the percentage of incidents resolved and the risks mitigated also helping workers feel more secure with the respective controls against the computer hazards that harm them.

Keywords: ISO 27005, Information security risk management, IT Consultants.

I.INTRODUCCIÓN

En la actualidad el índice de ataques informáticos aumentó drásticamente, los especialistas afirman que se está volviendo un peligro para todos, según Jurgens y Bissell (2022, p.14) En los primeros 6 meses del 2021 los ataques cibernéticos aumentaron en un 150%, alertando que existen 100 nuevos ransomwares que circulan a nivel mundial afectando y perjudicando a las personas y empresas.

Con la llegada de la era digital potenciado por la pandemia incrementó los ataques cibernéticos drásticamente, con lo cual han aparecido nuevos virus cibernéticos en todas partes del mundo ocasionando robo de información y pérdidas económicas millonarias que ponen en peligro a estas empresas

Por otro lado, la seguridad informática se orienta en proteger la información con el propósito de evitar que una persona no autorizada pueda manipular los datos, de este modo Paltán (2018, p.18) La seguridad de la información está compuesta por medidas de protección en las cuales se ve la prevención, detección y corrección permitiendo proteger y tener seguro los activos de TI.

De acuerdo a lo antes mencionado, la información es valiosa y para esto se utilizan ciertas medidas de protección para salvaguardar y proteger estos activos ante una posible amenaza de un tercero que quiera robar o afectar a una empresa.

De esta manera, sin importar si una empresa solo se enfoca en TI está también corre peligro sobre los riesgos y ataques informáticos que se pueden presentar, según Tafur (2022, p.2) Los riesgos que se pueden presentar en una consultora de TI es la falta de controles inadecuados, la falta de seguridad en los accesos, bases de datos vulnerables todo esto ocasionado con la falta de un mapeo de riesgos.

Es por ello, que las empresas de consultoría de TI a pesar que saben sobre los sistemas, estas no están seguros de los posibles ataques que se puedan presentar hoy en día por falta de controles de seguridad y no contar con un mapeo de riesgos que se presentan.

Según Guerrero, Medina y Nogueria (2020, p.1) La gestión de riesgos contribuye a escoger la mejor solución apoyándose en los enfoques de los procesos, mejorando el uso de los recursos y la disminución de costos. De este modo, la gestión de riesgos apoya a las empresas a agilizar y fortalecer la toma de decisiones y usar los recursos adecuadamente

para los riesgos que se presenten logrando mitigar el daño y no pase a mayores perjudicando a la empresa.

Por otro lado, según Caballero y Horacio (2018, p.4) Un riesgo es una posibilidad que ocurra una pérdida, las cuales se pueden presentar en un software como códigos maliciosos, virus, etc. Dicho de este modo, la gestión de riesgos son métodos y herramientas que se utilizan para identificar, analizar los problemas que se presente en el software de esta manera plantear estrategias para gestionarlos.

Según Vásquez y Alva (2018, p.110) La continuidad del negocio busca que la empresa sepa sobre los riesgos que lo amenacen. De este modo, se enfoca en asegurar la continuidad del negocio considerando puntos como la cadena de suministros y plantear alternativas para la continuidad para optar la mejor decisión y promover la proactividad en todas las áreas.

En resumidas cuentas, la protección de la información en consultoras de TI es importante estas empresas son atacadas por hackers puesto que pueden infiltrarse a la organización y robar la información de cuentas, contraseñas de los usuarios, también siendo afectadas por phishing o malware poniendo en peligro los activos de la empresa, de esta manera según Arce, Zuña, Romero y Soledispa. (2019, p. 489) Durante su estudio encontró ataques como phishing o malware se presentan todos los días en las pymes en todas partes del mundo, entendiendo que la ciberseguridad es un tema nuevo la cual se debe investigar más a fondo.

Los atentados con la información de las organizaciones se ven todos los días a las pequeñas empresas esto es porque al ser una empresa que apenas está creciendo no cuentan con la tecnología suficiente para lograr combatirlos, de igual forma la ciberseguridad es un nuevo tema que se presenta en la era digital que actualmente se afronta. Sin embargo, hasta el momento existen pocas empresas que deseen implementar esta normativa como el ISO 27005 que ayudarían con la gestión de riesgos de seguridad de la información en las empresas.

Según la problemática del estudio se elaboró las siguientes preguntas:

PG: ¿En qué medida el Marco de referencia basado en la ISO 27005 favorece en la gestión de riesgos de seguridad de la información en consultoras de TI?

- **PE1:** ¿En qué medida el Marco de referencia basado en la ISO 27005 favorece en los controles de seguridad para la gestión de riesgos de seguridad de la información en consultoras de TI?
- **PE2:** ¿En qué medida el Marco de referencia basado en la ISO 27005 favorece en el tratamiento de incidentes en la gestión de riesgos de seguridad de la información en consultoras de TI?
- **PE3:** ¿En qué medida el Marco de referencia basado en la ISO 27005 favorece con el nivel de satisfacción en la gestión de riesgos de seguridad de la información en consultoras de TI?

Justificación metodológica:

La presente investigación busca usar el marco de referencia basado en la normativa ISO 27005 para contrarrestar los ataques cibernéticos que se dan hoy en día, de este modo según al Fikri et al. (2019, p.9) La utilización de esta herramienta se utiliza para simplificar el proceso de administración de peligros.

En resumen, la normativa ISO 27005 apoya a la gestión de riesgos, mejorando la seguridad de la información en la empresa y contribuye con la calidad y efectividad de los servicios críticos, ayudando en el análisis y valoración de inseguridades de este modo se puede identificar los riesgos que se presenta en la empresa y poder enfrentarlos y disminuir la probabilidad de impacto negativo.

Justificación Práctica:

Dentro de este orden de ideas según Salnyk et al. (2020, p.30) La normativa ISO 27005 analiza y evalúa los riesgos informáticos. En el que se puedan detallar las amenazas del riesgo y catalogarlas según una escala de amenazas y tener un mapeo de los riesgos que se pueden presentar.

En este sentido esta norma brinda indicaciones para el estudio de gestión de riesgos identificando el contexto del problema también brinda documentos de sistema de gestión con la cual posibilita la obtención de datos como la identificación, análisis y valoración de riesgos registrándose en matrices para posteriormente poner su peso respectivo de su valoración estas también valorizadas por los criterios de información de los activos: disponibilidad, integridad y confidencialidad y darles un tratamiento oportuno.

Justificación Teórica:

La finalidad de realizar una gestión de riesgos es identificar las potenciales inseguridades de información sean identificados, evaluados, tratados de forma oportuna, según Huaura (2019, p.15) Observando la variación en la arquitectura de la empresa y escenarios desafiantes tanteados por analistas, cumplir con la anticipación de los riesgos emergentes que dañan la confidencialidad de las operaciones se hace desafiante y por lo que es necesario estar alerta a las alteraciones que se plantean en las empresas.

Las empresas manejan información valiosa tanto de los trabajadores y clientes la implementación de controles para el riesgo identificados, genera indicadores de gestión que son proporcionados a la gerencia para dar el seguimiento oportuno y para luego tomar la mejor decisión en próximas inversiones.

De esta forma se planteó los siguientes objetivos de investigación que ayudarán con el estudio planteado:

Objetivos General:

- OG: Determinar la eficacia del Marco de referencia basado en la ISO 27005 para la gestión de riesgos de seguridad de la información en consultoras de TI.

Objetivos específicos:

- OE1: Determinar la eficacia del Marco de referencia basado en la ISO 27005 para los controles de seguridad para la gestión de riesgos de seguridad de la información en consultoras de TI.
- OE2: Determinar la eficacia del Marco de referencia basado en la ISO 27005 en el tratamiento de incidentes en la gestión de riesgos de seguridad de la información en consultoras de TI.
- OE3: Determinar la eficacia del Marco de referencia basado en la ISO 27005 para el nivel de satisfacción en la gestión de riesgos de seguridad de la información en consultoras de TI.

Luego de determinar los objetivos se plantea las siguientes hipótesis:

Hipótesis general:

- HG: El Marco de referencia basado en la ISO 27005 es eficaz en la gestión de riesgos de seguridad de la información en consultoras de TI.

Hipótesis específicas:

- HE1: El Marco de referencia basado en la ISO 27005 es eficaz para los controles de seguridad en la gestión de riesgos de seguridad de la información en consultoras de TI.
- HE2: El Marco de referencia basado en la ISO 27005 es eficaz en el tratamiento de incidentes en la gestión de riesgos de seguridad de la información en consultoras de TI.
- HE3: El Marco de referencia basado en la ISO 27005 es eficaz en el nivel satisfacción en la gestión de riesgos de seguridad de la información en consultoras de TI.

II. MARCO TEÓRICO

Para la elaboración de la investigación se presentarán estudios previos que se aplicaron a nivel internacional y nacional usados como base del estudio.

Antecedentes Internacionales

Quijije y Rodríguez (2020) En su investigación titulada "*Auditoría informática a la empresa MSA Consulting Group basado en la norma ISO 27005*." Tiene el propósito de implementar una evaluación teniendo como referencia la normativa ISO 27005,la metodología usada fue una investigación bibliográfica y una investigación de campo se usó un muestreo fue no probabilístico usando la observación y entrevista como instrumentos fue una encuesta para la recolección de datos, el resultado obtenido fue poder gestionar los riesgos informáticos donde se pudo identificar que el 69% de los activos estaban en riesgo representando un nivel medio y un 11% de nivel alto. En conclusión, luego del uso de la norma 27005 se pudo identificar las magnitudes de riesgo de seguridad de datos que se presentó en la empresa con esto aumentó el porcentaje de riesgos mitigados en la empresa en un 80%.

Castillo y Molina (2020) En su estudio titulado "*Análisis de riesgos al proceso de fiscalización de proyectos de ingeniería para una empresa que brinda servicios de ingeniería bajo la norma ISO/IEC 27005*" tuvo como propósito elaborar una observación de las inseguridades en la inspección de proyectos, la metodología utilizada fue la normativa ISO 27005 para la valoración del riesgo el resultado obtenido fue el uso de una matriz de riesgo para identificar las amenazas y vulnerabilidad encontradas determinar el grado de impacto y probabilidad teniendo como conclusión que el inventario de activos está en un nivel crítico para la continuación del proceso fiscalización presentando amenazas y vulnerabilidades en vista de exposición particular, de igual forma se buscó que estos controles estén dentro de estos procesos para dar respuesta a los peligros informáticos.

Hamit et al. (2020) En su artículo "*Adopting an ISO/IEC 27005:2011-based Risk Treatment Plan to Prevent Patients from Data Theft"* tiene como objetivo establecer el contexto de los criterios básicos y el alcance y los límites y las reglas sobre cómo realizar la valoración y aplicación de control. El tipo de estudio es explicativo, teniendo como resultado de tratamiento de peligros centrado en los riesgos y exámenes para que el sistema reduzca estos riesgos y proteja los datos del paciente. Esto eventualmente mejorará la seguridad de la información aumentando en un 65% respecto a los riesgos mitigados de la empresa, al mismo tiempo, aumentará la conciencia entre los miembros del equipo sobre los riesgos y los medios para manejarlos.

Fahrurozi et al. (2020) en su investigación titulada "*The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence*)" el cual tuvo como propósito ofrecer un procedimiento de diseño de gestión de seguridad según la ISO 27005, la metodología utilizada fue el Desing Research Methodology, como resultado obtenido fue la identificación de 45 activos la cual dio como resultado 121 vulnerabilidades de gran impacto constituidas 6 altas, 88 medias y 27 en conclusión esta normativa ayuda con de identificación, evaluación y posterior tratamiento a los riesgos esto apoyado con la ISO 27002 la cual brinda los controles de seguridad de información logrando aumentar el porcentaje sobre los riesgos mitigados en 75%.

Antecedentes Nacionales

Cabezas (2020) en su tesis titulada "*Implementación de un framework de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en lima*". tuvo finalidad la realizar y adaptar de un framework para ciberseguridad, las normativas utilizadas fueron la ISO 27005, 27032 Y 27000 de igual forma se utilizó el ciclo PHVA para el mejoramiento de la empresa el resultado obtenido fue la aplicación de controles informáticos y la concientización de los empleados a la protección de datos de la empresa.

Cruz (2019) En su investigación titulada "*Modelo de gestión de riesgos de TI enfocado en estándares adaptados para contribuir en la protección del activo de ti en el sector de distribuidoras de la región Lambayeque*" tuvo como objetivo poner en práctica un prototipo de gestión de riesgos tecnológicos, el tipo de investigación fue cuantitativa de tipo descriptiva, el diseño utilizado fue un método correlacional, para la población se consideró cuatro distribuidoras, el instrumento usado fue un cuestionario y la observación, los resultados obtenidos fue la identificación de 85 riesgos para posteriormente tomar la mejor decisión para la disminución del impacto de operaciones, de igual forma se alcanzó 5 proyectos que permitan dar tratamiento a 23 peligros de las cuales 7 de muy alto y 16 riesgos de prioridad moderada, de esta forma se logró la mejor toma de decisión y disminuir los peligros encontrados esto ayudó a la empresa en un crecimiento de 68% de incidentes resueltas.

García, Huamani y Alvarado (2018) en su artículo titulado "*Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas*" tuvo la finalidad de integrar la metodología OCTAVE-S con la norma ISO 27005 para elaborar un prototipo de gestión de riesgos, la técnica utilizada fue un enfoque cuantitativo con la cual se pueda cuantificar el riesgo sobrante según la eficacia de los controles presentados, logrando presentar un modelo adecuado a la empresa, Como resultado fue que se demostró un sencillo manejo y pudiendo establecer las políticas de seguridad adecuados para la disminución de peligros logrando un aumento del 76% de incidentes resueltos respecto a la seguridad de la información.

Carmona (2021) En su tesis titulada *"Implementación de una Metodología de Gestión de Riesgos alineada a la ISO 27005 y Magerit para el proceso "OSE" de una empresa de facturación electrónica en la ciudad de Lima - 2021."* Tuvo como finalidad de poner en práctica una metodología de gestión de riesgos basada en la ISO 27005 y Magerit, se utilizó un enfoque cuantitativo, el instrumento usado fue un cuestionario de satisfacción, para la población se consideró a los trabajadores de la empresa, el resultado obtenido fue que esta normativa ayudó a la clasificación de los activos logrando reconocer los activos más importantes encontrando los riesgos probables de su nivel de criticidad que los afectan, para posteriormente usar los controles necesarios para los peligros, con esto el nivel de satisfacción de los trabajadores aumentó en 80% indicando que esta normativa favoreció a la seguridad informática.

Base Teórica

Gestión de riesgos de seguridad de la información

Según Pinto (2017, p.52) Se entiende por gestión de riesgos de seguridad de la información a todas las disposiciones de precaución de las empresas que ayuden a resguardar y preservar los. De la misma manera según Huaura (2019, p.33) Los incidentes exponen a los activos de la organización generando la obligación de poner en práctica controles de seguridad a partir de un análisis de riesgo para la disminución de peligros.

Dimensión: Controles de seguridad

Los mecanismos de control sirven para el resguardo de datos sobre la modificación, divulgación y destrucción no autorizada de archivos importantes (Chavarría et al.,2021, p. 31).

Indicador: % de riesgos mitigados

La mitigación de riesgos es un proceso donde se ejecuta acciones la cual ayuda a reducir o eliminar el impacto de los incidentes (Liu et al.,2022, p. 2)

Fórmula:

$$\%\ \text{de riesgos mitigados} = \frac{\text{Total de riesgos identificados}}{\text{Total de riesgos solucionados}}\ \text{x}\ 100$$

Dimensión: Tratamiento de incidentes

Es un método útil para contener el suceso de seguridad con el propósito de disminuir que se propague la incidencia causando perjuicios (Ríos, 2020, p. 39).

Indicador: % de incidentes resueltas de seguridad de información

Consiste en identificar el porcentaje de incidentes que ya se dio un tratamiento de este modo se puede determinar la buena gestión del riesgo (Thangavelu, Krishnaswamy y Sharma, 2021, p. 15).

Fórmula:

$$\%\ \text{de incidentes resueltas de seguridad de información} = \frac{\text{N° de incidencias presentadas}}{\text{N° de Incidentes resueltos}}\ \text{x}\ 100$$

La satisfacción laboral es la sumatoria de actitudes que una persona puede adoptar ante los diferentes estados de emoción positivos o negativos resultantes de la experiencia de trabajo (Faya et al.,2018, p. 46).

Indicador: Nivel de satisfacción respecto a la gestión de riesgos de seguridad de información

Es la percepción que tienen los trabajadores o usuarios sobre la protección de su información ante los posibles riesgos informáticos (Van der Kleij et al.,2022, p. 2).

Marco referencial basados en la Normativa ISO 27005

Según Fajardo (2021, p. 8) afirma que esta normativa proporciona requisitos para adaptar una evaluación de riesgos sobre los activos tecnológicos críticos en la empresa. De igual manera según Quijije y Rodríguez (2020, p. 21) está normativa está elaborada para ayudar a poner en práctica la seguridad de los datos. Ver figura 1.

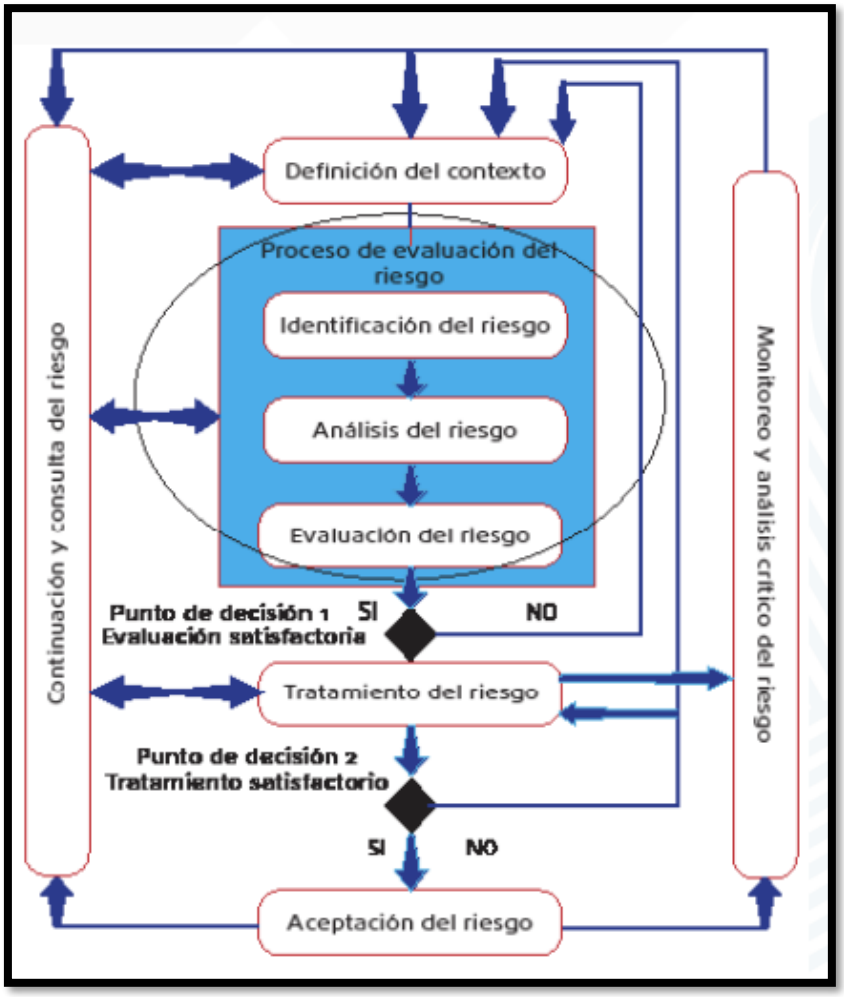


Figura 1. Posición de la Fase de análisis del riesgo en el proceso de gestión de riesgo

Evaluación del riesgo:

Identificación del Riesgo: En este punto comprende y establece los posibles sucesos con potencial causa de pérdida y efectuar levantamiento de cómo esto puede suceder (Kowask et al.,2018, p. 60).

Análisis de Riesgo: Es el paso para identificar las inseguridades, este reconocimiento se lleva a cabo de forma que se pueda identificar y conocer los potenciales eventos que tienen posible causa de pérdida (Kowask et al.,2018, p. 60).

Evaluación del riesgo: Se dará una valoración del riesgo de esta forma se utilizará para medir los riesgos de seguridad (Kowask et al.,2018, p. 105).

De esta se forma se considerando:

- La importancia de la importancia del proceso

- La precisión de los activos
- El historial de acontecimientos de eventos de seguridad
- El valor del activo para el proceso
- La posibilidad de sucesos y otros, de acuerdo a la organización y el alcance.

Es necesario que la empresa piense también en:

Las características de seguridad de la información (CID): Confidencialidad, Integridad, Disponibilidad

La necesidad de los procesos de negocios por un activo o grupo de activos.

La suma de riesgos pequeños y medianos que puede resultar en un riesgo total significativo

Tratamiento del riesgo

La secuencia del tratamiento del riesgo se observa en la figura 2 en la cual se tendrá un análisis como:

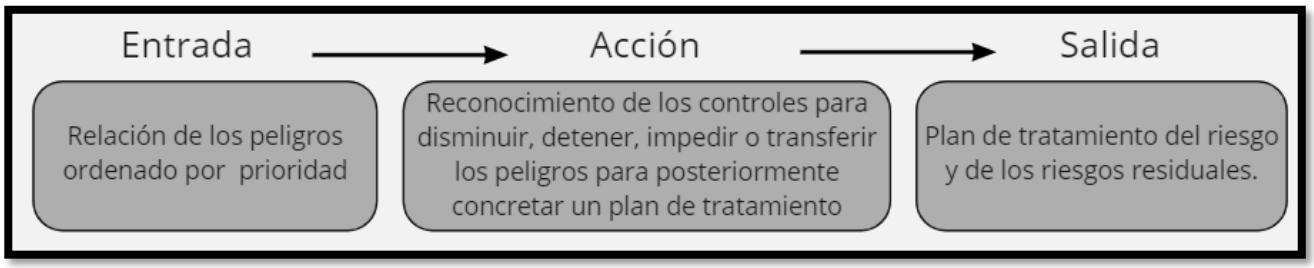


Figura 2. Tratamiento del riesgo

El tratamiento del riesgo se tiene cuatro estrategias:

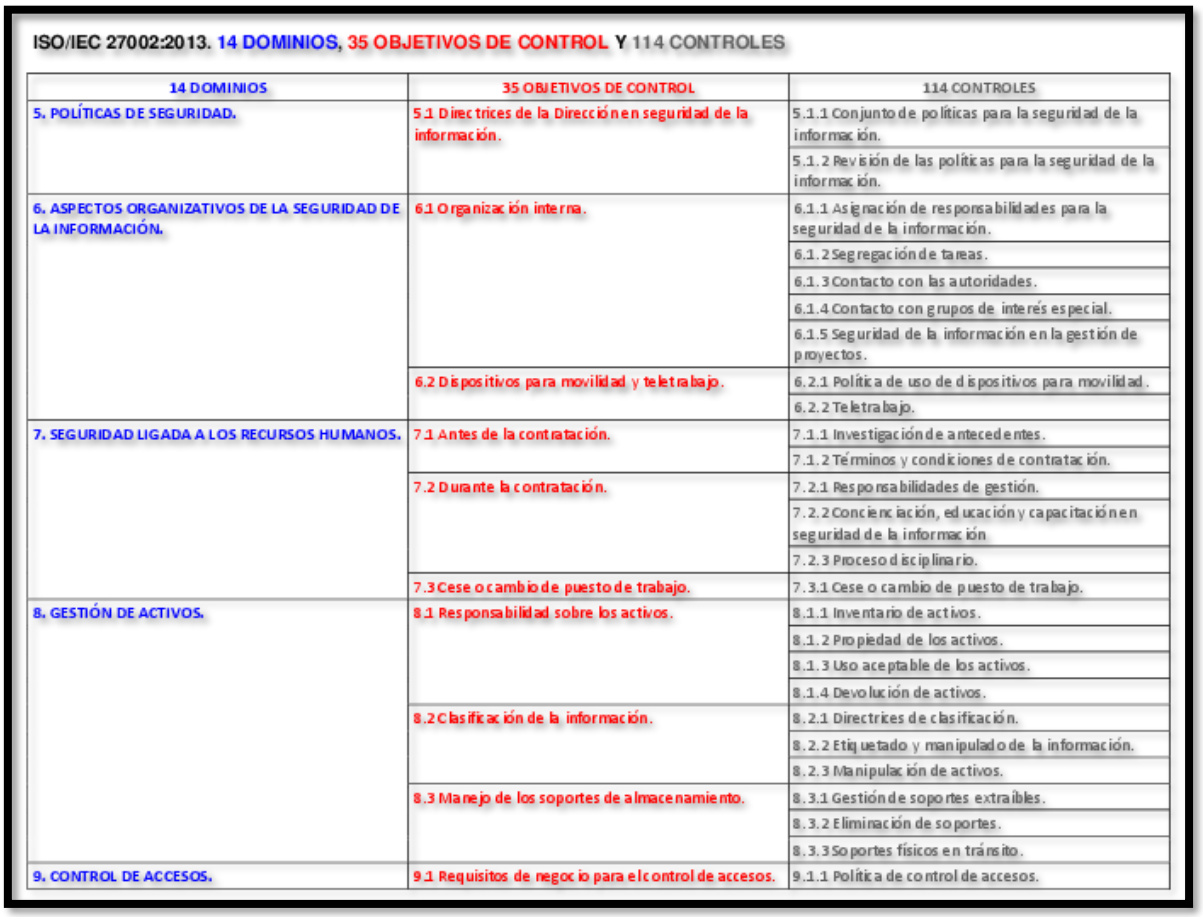
- Aceptar el riesgo
- Reducir el riesgo
- Transferir el riesgo
- Evadir el riesgo

De esta forma se plantea un tratamiento para la disminución de peligros siguiendo la normativa ISO 27002:2013 la cual brinda directrices para la elaboración de controles de seguridad

Según Burgdorf y Jendria (2022, p. 302) afirma que esta normativa brinda sugerencias de buenas prácticas de protección de datos a los involucrados. La Organización Internacional

de Normalización actualizo es normativa brindando 14 dominios, 35 objetivos y 114 controles:

Controles organizacionales, Controles de Personas, Controles físicos y Controles tecnológicos. Ver figura 3.



ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

14 DOMINIOS	35 OBJETIVOS DE CONTROL	114 CONTROLES
5. POLÍTICAS DE SEGURIDAD.	5.1 Directrices de la Dirección en seguridad de la información.	5.1.1 Conjunto de políticas para la seguridad de la información.
		5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	6.1 Organización interna.	6.1.1 Asignación de responsabilidades para la seguridad de la información.
		6.1.2 Segregación de tareas.
		6.1.3 Contacto con las autoridades.
		6.1.4 Contacto con grupos de interés especial.
		6.1.5 Seguridad de la información en la gestión de proyectos.
	6.2 Dispositivos para movilidad y teletrabajo.	6.2.1 Política de uso de dispositivos para movilidad.
		6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	7.1 Antes de la contratación.	7.1.1 Investigación de antecedentes.
		7.1.2 Términos y condiciones de contratación.
	7.2 Durante la contratación.	7.2.1 Responsabilidades de gestión.
		7.2.2 Concienciación, educación y capacitación en seguridad de la información
		7.2.3 Proceso disciplinario.
	7.3 Cese o cambio de puesto de trabajo.	7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.	8.1 Responsabilidad sobre los activos.	8.1.1 Inventario de activos.
		8.1.2 Propiedad de los activos.
		8.1.3 Uso aceptable de los activos.
		8.1.4 Devolución de activos.
	8.2 Clasificación de la información.	8.2.1 Directrices de clasificación.
		8.2.2 Etiquetado y manipulado de la información.
		8.2.3 Manipulación de activos.
	8.3 Manejo de los soportes de almacenamiento.	8.3.1 Gestión de soportes extraíbles.
		8.3.2 Eliminación de soportes.
		8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.	9.1 Requisitos de negocio para el control de accesos.	9.1.1 Política de control de accesos.

Figura 3.Cambios en la nueva ISO 27002:2013

Para ver más específico los controles mencionados estos se observan en el anexo 21.

A continuación, se muestra un cuadro comparativo entre las normas de gestión de riesgos de la seguridad la información

Tabla 1. Cuadro comparativo de normas

ISO 27005	ISO 27002	ISO 27001	ISO 3100
Esta normativa proporciona requisitos para adaptar una evaluación de riesgos sobre los activos tecnológicos críticos en la empresa Fajardo (2021, p.8). De igual manera está elaborado para ayudar a poner en uso el resguardo de datos según una perspectiva de gestión de riesgos Quijije y Rodríguez (2020, p.21), también esta normativa es compatible con la ISO 31000. De igual forma apoya las ideas generales de la ISO 27001 y está elaborada para apoyar el uso de satisfacción de la seguridad de la información. (Reyes 2019, p.7)	Es una directriz que brinda buenas prácticas respecto a seguridad de la información dando controles recomendables frente a los riesgos identificados.(International Organization for Standardization 2017, p.9)	Decreta las exigencias para la ejecución, mantenimiento y conservación de un SGSI. Se orienta en la evaluación y tratamientos de los riesgos de forma transparente dentro del contexto establecido, garantizando que los datos que tiene la empresa estén protegidos.(Reyes 2019, p.5)	Principios y directrices genéricas para la gestión de riesgos en cualquier tipo de empresa. La ISO 3100 no brinda metodologías, ya que tiene un tratamiento del peligro general, afrontando todo tipo de riesgo y no se enfoca en uno solo específicamente. (Reyes 2019, p.8)

Fuente: Elaboración Propia.

Marco Conceptual

Gestión de riesgo

Según Soler et al. (2018, p. 45) la gestión de riesgo es una perspectiva estructurada para el manejo de inquietudes relativas a la amenaza a través de actividades que intervienen en la identificación. De igual manera Barrio (2019, p. 48) afirma que la gestión de riesgos ayuda a adelantarse al peligro y resguardar los objetivos.

Sistema de Gestión de Seguridad de la Información

Según Fajardo (2021, p. 10) afirma que es un estándar en la cual se tiene una perspectiva sistemática para disponer, implementar, actuar, monitorear, verificar, conservar y aumentar la protección de datos empresariales.

Confidencialidad

Según Magaña (2020, p.5) nos dice que la confidencialidad garantiza que el resguardo de datos sea confidencial y solo sea usada por el personal permitido de esta forma asegurar que la información no caiga en manos de terceros que lo puedan dañar. La manera de asegurar un buen control en para la confidencialidad es utilizar nombre de usuarios y contraseñas, encriptación y lista de controles de accesos.

Integridad

Según Magaña (2020, p. 6) nos indica que la integridad establece que los datos estén en un formato que sea seguro y que responda satisfactoriamente a sus propósitos originales evitando que sea alterado por un tercero. De esta manera la información solo puede ser manipulada solo por personas autorizadas y que permanezca en su estado original cuando está en uso.

Disponibilidad

En el estudio de Magaña (2020, p. 6) afirma que la disponibilidad garantiza que los datos y recursos estén disponibles para las personas que los necesiten, usando procedimientos de mantenimiento de hardware, parches de software y optimización de red.

Vulnerabilidad

Es un aspecto del sistema en la cual puede ser perjudicado por un ataque informático, siendo una debilidad o puntos de accesos al sistema (Schiavonne,2022, p.26)

Diferencia Vulnerabilidad y Debilidad

Una debilidad es un descuido que puede provocar una vulnerabilidad, mientras que una vulnerabilidad es un inconveniente con el sistema ocasionada por un hacker para robar datos importantes (Schiavonne,2022, p.26).

Amenaza

Es un suceso que puede perjudicar y arruinar los activos del sistema (Schiavonne,2022, p.27).

Riesgo

Un riesgo es una posibilidad que un peligro explote la debilidad de un activo ocasionando perjuicios a la empresa (Schiavonne, 2022, p.28).

Impacto

El impacto señala el daño que provoca una vulnerabilidad cuando una amenaza afecta a un activo, estimando el valor del activo y el daño provocado (Schiavonne, 2022, p.28).

Mitigar

Se entiende que mitigar es moderar, aplacar disminuir o suavizar el grado del impacto provocado por un riesgo que perjudique a la empresa (Schiavonne, 2022, p.28).

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

Tipo de investigación

Para el presente estudio se definió como tipo cuantitativa. Según Ortega (2018, p. 3)Su desarrollo de análisis se enfoca en la medición y observación para responder a las incógnitas de exploración planteadas este enfoque utiliza los análisis estadísticos. De igual forma Hernández y Mendoza (2018, p.6) Este enfoque es adecuado para la estimación de magnitud del fenómeno y sostener la hipótesis planteada. Por otro lado, se utilizará un diseño de tipo aplicada, Según Carrasco (2019, p.43) la investigación aplicada se distingue por tener una finalidad inmediata y práctica bien definida, por eso se fomenta el estudio que afecta al comportamiento, a la innovación y a la actualización de un campo específico de la realidad.

Diseño de investigación

Para definir el diseño de investigación se consideró de tipo experimental. Según Guevara, Verdesoto y Castro (2020, p. 7) Este tipo de diseño se usa para observar la relación de causas y efecto de una situación. De esta forma también se consideró un diseño Pre-Experimental**,** Según Hernández y Mendoza (2018, p.6) afirma que sirve para aproximarse al fenómeno que se analiza de esta forma se trabaja con un grupo de estudio donde se hacen las pruebas en dos tiempos. Por otro lado Ramos (2021, p.4) Considera que la variable dependiente debe ser calculada por un instrumento de recolección de datos en dos oportunidades en el pre y post test.

El estudio se trabaja en el diseño experimental del tipo pre experimental ver figura 2.

***Figura 2**. Diseño de Investigación preexperimental*

GE (Grupo Experimental) Empresas Consultoras de TI

O1(Antes-PreTest) Utilización de herramientas según los indicadores previos a la ISO 27005

X (Intervención - Experimental) Marco referencial basados en la ISO 27005

O2 (Después - PostTest) Utilización de herramientas según los indicadores luego de la ISO 27005

3.2 Variables y operacionalización

En este presente estudio tiene como variables Gestión de riesgos de seguridad de la información las cuales tienen como dimensiones controles de seguridad, tratamiento de incidentes, nivel de satisfacción; en el anexo 1 se refleja la matriz de operalización de variables. A continuación, se observa el detalle:

A. Definición conceptual:

   Según Pinto (2017, p.52) Se entiende por gestión de riesgos de seguridad de la información a todas las disposiciones de precaución de las empresas que ayuden a salvaguardar y preservar los datos. Según Huaura (2019, p.33) Los incidentes exponen a los activos de la organización generando la obligación de poner en práctica controles de seguridad a partir de un análisis de riesgo para la disminución de peligros.

B. Definición operacional

   Según Narró (2021, p. 41)Es el grupo de acciones que ayudan a identificar, analizar y cuantificar un riesgo por medio del uso de acciones de evaluación orientación y supervisión. Estas medidas permiten reducir o mitigar el impacto del peligro.

C. Dimensiones

   Controles de seguridad (Chavarría et al.,2021, p. 31)

   Tratamiento de incidentes (Ríos, 2020, p. 39).

   Nivel de satisfacción (Faya et al.,2018, p. 46).

D. Indicadores

   % de riesgos mitigados (Liu et al.,2022, p. 2)

% de incidentes resueltas de seguridad de información (Thangavelu, Krishnaswamy y Sharma, 2021, p. 15).

Nivel de satisfacción respecto a la gestión de riesgos de seguridad de información (Van der Kleij et al.,2022, p. 2).

3.3 Población, muestra y muestreo

Población

Según Arias (2021, p. 113) La población es una porción finita o infinita las cuales tienen características similares o comunes entre ellos, la población es el total de partes de la investigación, la cual está delimitada por el investigador las cuales pueden estar establecido por N personas.

En esta investigación la población está constituida por los usuarios que se involucran con la empresa CFR Business & Solutions E.I.R.L. los cuales son 15 personas estas servirán como objeto de estudio para responder las encuestas en 2 periodos, mientras que la otra población será los registros de riesgos e Incidencias en un periodo de 20 días.

Para la elaboración del presente estudio se tendrá como población trabajadores de la empresa CFR Business & Solutions E.I.R.L, verificar el resumen de la población en la tabla 2.

Tabla 2. *Resumen de la población para la investigación*

Indicador	Población	Tiempo
% de riesgos mitigados	Registro de riesgos e Incidencias	20 días
% de incidentes resueltas de seguridad de información		
Nivel de satisfacción respecto a la gestión de riesgos de seguridad de información	15 personas	2 periodos

Fuente: Elaboración Propia

Criterios de Inclusión: Todos los registros de riesgos e Incidencias en la empresa.

Criterios de Exclusión: Todos los registros que no sean riesgos e incidentes en la empresa.

Muestra

Según Hernández y Mendoza (2018, p. 196) La muestra es un subconjunto reducido la cual representa a la población, los datos recaudados serán obtenidos de la muestra y la población perfilándose desde la situación problemática de la investigación. Así mismo Salazar y Castillo (2018, p. 13) Define que es un grupo de partes de la población donde se puede trabajar con el total de la población si esta es menor a 50 personas.

El tamaño de muestra será toda la población, siendo representada por los usuarios que se involucran con la empresa CFR Business & Solutions E.I.R.L., en un total de 15 personas, además de la totalidad de los registros de riesgos e Incidencias en la empresa en un periodo de 20 días.

Muestreo

El muestreo del presente proyecto será un muestreo no probabilístico, es un procedimiento de muestreo donde el investigador escoge una muestra basada en un juicio subjetivo siendo beneficioso para estudios exploratorios con una encuesta piloto. Así mismo se determina que será un muestreo intencional, se elige la muestra basada por su propio juicio basándose en su criterio propio de esta forma solo toma a individuos que cree necesarios para la investigación (Salgado 2019, p.30).

3.4 Técnicas e instrumentos de recolección de datos

Son elementos que utiliza el indagador para juntar información importante por medio de diversos instrumentos de recolección (Cisneros et al.,2022, p. 1172).

En este proyecto se utilizarán dos tipos de técnicas de acuerdo a los indicadores planteados mediante su respectivo instrumentó de recolección.

Técnicas de recolección de datos:

Fichaje: Es un método usado para llevar un registro de datos para la ejecución del estudio con el uso de fichas de registro según el indicador (Arias, 2020, p. 14).

La herramienta de recopilación de datos usado fue la ficha de registro, el cual tiene la finalidad de evaluar las diferentes características, funcionalidades o comportamiento de los elementos a estudiar (Arias, 2020, p. 55).

Las fichas de registro se observar en (Anexo 3, Anexo 5); se pondrá el nombre de la organización, variable, dimensión, el periodo será 20 días, la fecha donde se inició y final de la prueba, de igual forma se mostrará el indicador, descripción, el método aplicado, la fórmula que se usará para luego colocar los datos según el indicador.

A continuación, se mostrará los indicadores donde se emplearon las fichas de registro ver tabla 3.

Tabla 3. *Indicadores en las que se usarán las fichas de registro*

Variable	Indicador	Técnica	Herramienta
Gestión de riesgos de seguridad de la información	% de riesgos mitigados	Fichaje	Ficha de registro
	% de incidentes resueltas de seguridad de información		

Fuente: Elaboración Propia

Encuesta: Permite explorar la opinión general, teniendo como resultado descubrir la percepción de las personas, obteniendo que el investigador logre medir el nivel de satisfacción del encuestado (Torres, Karim y Salazar,2019, p. 4).

En el presente estudio se utilizará un cuestionario como mecanismo de recolección para reconocer el nivel de satisfacción de los trabajadores el contenido de estas fichas tendrá 10 preguntas, se responderá con una (X) (Ver Anexo 7) para este instrumento se aplicará la escala de Lickert donde los encuestados serán todos los trabajadores de CFR Business & Solutions E.I.R.L.

El instrumento será elaborado en la plataforma Google Forms y para el desarrollo de este instrumentó se enviará el link del cuestionario por WhatsApp de la empresa CFR Business & Solutions E.I.R.L. a todos los empleados, los datos recolectados sólo se usarán para la elaboración de esta investigación.

A continuación, se especificará el indicador que se usará el procedimiento de la encuesta y como herramienta del cuestionario ver tabla 4.

Tabla 4.*Indicador para el cuestionario de satisfacción.*

Variable	Indicador	Técnica	Herramienta
Gestión de riesgos de seguridad de la información	Nivel de satisfacción respecto a la gestión de riesgos de seguridad de información	Encuesta	Cuestionario de satisfacción

Fuente: Elaboración Propia

Validez de los instrumentos por expertos

Según Bernal et al. (2020, p. 2)Se encuentran diversas formas de validar un contenido entre los más usados el juicio de expertos caracterizado por contar con personas expertas en la materia usada para verificar la fiabilidad de una investigación. De igual forma Ibarra et al. (2018, p. 3) afirma que la validación se realiza por medio de una herramienta realizada por los expertos permitiendo medir el contenido. Por otro lado Juárez y Tobón (2018, p.5) La calidad de una herramienta de investigación se relaciona con la autenticación del contenido con la extracción de evidencias válidas.

Para la validación de expertos se elaboró diversas herramientas de uso, ver tabla 5.

Tabla 5.*Detalle de los instrumentos diseñados para el uso del validador*

Variable	Instrumento de uso del validador	Herramientas a validar
Dependiente	Instrumento de validación del experto por indicador	% de riesgos mitigados
		% de incidentes resueltas de seguridad de información
		Nivel de satisfacción respecto a la gestión de riesgos de seguridad de información

Fuente: Elaboración propia.

Para la validación de los instrumentos de recolección de datos fue necesario el juicio de expertos, ver Tabla 6.

Tabla 6. *Validez de los instrumentos de investigación por expertos*

N°	Expertos	Grado Académico	Puntaje a cada ficha de registro		
			% de riesgos mitigados	% de incidentes resueltas de seguridad de información	Encuesta de satisfacción
1	Mendoza Apaza, Fernando	Magister	90%	90%	Aplicable
2	Alarcón Cajas, Yohan Roy	Magister	95%	95%	Aplicable
Promedio Total			92.5%	92.5%	-

Fuente: Elaboración propia.

La validación de estos documentos se puede visualizar en el anexo 12, anexo 13, anexo 14, anexo 15, anexo 16, anexo 17, anexo 18, anexo 19.

Confiabilidad de los instrumentos por expertos

Es una herramienta para calcular donde se determina el nivel de exactitud de la medida (Jacobo, Pacheco y Bertheau,2020, p. 218). De igual forma según Santos (2017, p.1) La confiabilidad permite determinar el nivel en que los ítems de un test están asociados

3.5 Procedimientos

Para la elaboración del presente estudio en CFR Business & Solutions E.I.R.L. Se tramito una carta de presentación a gerente general (Anexo 9) y este emitió una carta de aceptación que se observa en el Anexo 11, para realizar el proyecto en la mencionada empresa esta se realizará de manera presencial. Para esto se coordinará reuniones con el gerente general para determinar las fechas de trabajo, la recolección de datos será todos los registros de incidencias en la empresa, el cuestionario de satisfacción será aplicada a 15 trabajadores, por otro lado, será necesario contar con el documento de consentimiento se observa en el Anexo 10, Para luego alistar los instrumentos para ser aplicado y verificar los datos reunidos.

Asimismo, se realizará la elección de la información obtenida, estableciendo el orden de los datos extraídos, el cual permitirá la elaboración de una matriz para realizar el análisis

estadístico correspondiente de la investigación para finalmente elaborar la tabulación con los datos recogidos, ver Figura 5.

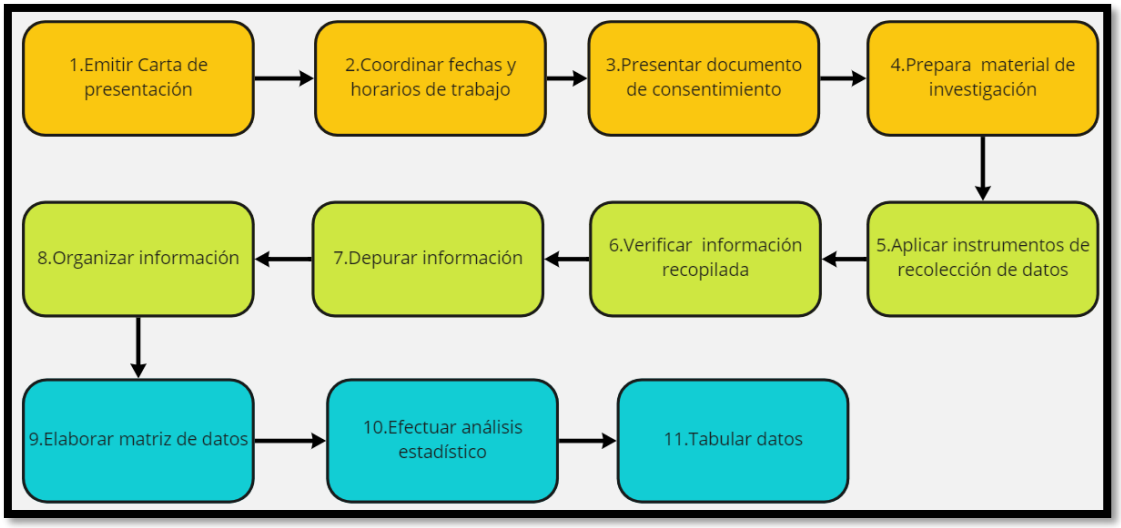


Figura 4. Fases del procedimiento de investigación

3.6 Método de análisis de datos

Para el proyecto se utilizó distintos datos numéricos los cuales son extraídos durante la recopilación de información para lograr validar las hipótesis desarrolladas logrando la medición de los intervalos numéricos.

Se usó un software estadístico SPSS la cual ayudó a realizar la captura y análisis de la información según los resultados de los indicadores logrando crear tablas y gráficos con la data.

De esta forma buscó determinar la eficacia del Marco de referencial basado en la ISO 27005 en la seguridad de la información para empresas consultoras de TI para esto se desarrolló un pre – test para identificar el estado actual de los indicadores para posteriormente realizar un post – test logrando identificar la nueva información recolectada.

Por otro lado se utilizó un análisis estadístico comparativo entre los dos grupos, usando pruebas paramétricas o pruebas no paramétricas de acuerdo al comportamiento de los datos, pudiendo ser T de Student para muestras relacionadas y en caso que los supuestos se lleguen a cumplir, se usará la prueba no paramétrica de Wilcoxon o prueba de u de Mann

Whitney en caso que no cumplan el supuesto, estos análisis funcionaran como evidencia de la hipótesis de la investigación siendo evaluado en un 95% de confianza y un 5% de error (Puma y Estrada,2020, p. 48).

3.7. Aspectos éticos

Para la recolección de información fue hecha en bases de datos nacionales e internacionales. Para esto se utilizó Google académico, ProQuest, ScienceDirect, SCOPUS, Libros y repositorios de universidades privadas y públicas.

La elaboración del estudio se basó en los reglamentos establecidos por la Universidad César Vallejo en su resolución del vicerrectorado de investigación N° 110-2022-VI-UCV.

Según El Peruano (2017, p. 5) la Ley N° 29733 protección de datos personales el cual tiene la finalidad de asegurar la información como la privacidad y anonimidad, en cuanto al uso de información personal íntima privada y familiar.

Por otro lado, según UCV (2017, p. 5) La ISO 690 es un estilo de redacción la cual ofrece directrices precisas para la elaboración de referencias bibliográficas de investigaciones.

La información fue extraída y analizada por criterios de juicio y transferencia, asegurando la confidencialidad de los trabajadores de la empresa, previamente para la elaboración de la investigación fue realizado un consentimiento informado, el cual se observa en el Anexo 10, de esta forma la organización emitió una carta de aceptación para la ejecución del estudio de investigación, ver el Anexo 11.

Esta investigación es original, puesto que no hay otro trabajo que comparta el mismo contenido en la empresa donde será aplicada la investigación.

IV. RESULTADOS

Resultados de porcentaje de riesgos mitigados

De acuerdo al indicador porcentaje de riesgos mitigados en la tabla 7 se refleja los resultados de la media luego de la implementación de la Normativa ISO 27005, la media aumentó en un 19.51%,La desviación que se obtuvo durante el pretest fue de un 11,82198 y luego de la implementación el resultado que arrojó en el post test fue de 10,83595 de igual forma los valores mínimos y máximos durante el pretest fueron de 50 y 88,89 respectivamente y durante el postest el mínimo fue de un 66,67 y el máximo en un 100%.

Tabla 7. *Análisis descriptivo del porcentaje de riesgos mitigados*

Estadísticos		Antes	Después
N	Válido	20	20
Media		67,3965	86,9100
Mediana		66,6700	83,3300
Moda		60,00	100,00
Desv. Desviación		11,82198	10,83595
Mínimo		50,00	66,67
Máximo		88,89	100,00

Fuente: Elaboración Propia.

Los resultados estadísticos del indicador porcentaje de riesgos mitigados antes de la ejecución fue de 67,40% y luego incrementó a un 86,91%. Ver figura 6.

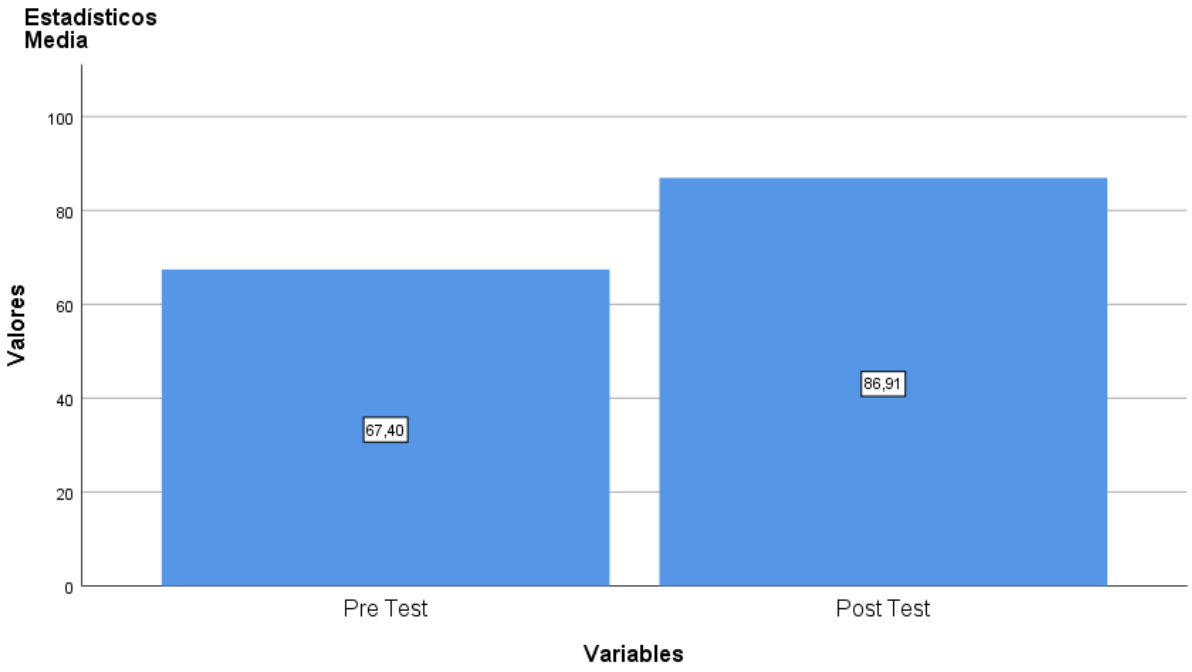


Figura 5. Porcentaje de la medida de porcentaje de riesgos mitigados

Resultados de porcentaje de incidentes resueltas de seguridad de información

De acuerdo al indicador porcentaje de riesgos mitigados, los resultados de la media luego de la implementación de la Normativa ISO 27005 aumentó en un 13,97%; de igual manera la desviación de riesgos mitigados es de 11,81% y luego de la implementación fue un 18,25%, los valores mínimos y máximos en el pretest fueron de 60 y 100 y durante el postest la estimación mínima fue de 50% y el máximo de 100%. (ver tabla 8).

Tabla 8. *Análisis descriptivo dé porcentaje de incidentes resueltas de seguridad de información*

Estadísticos		Antes	Después
N	Válido	20	20
Media		76,0240	90,0005
Mediana		75,0000	100,0000
Moda		75,00	100,00
Desv. Desviación		11,81131	18,25675
Mínimo		60,00	50,00
Máximo		100,00	100,00

Fuente: Elaboración Propia

El efecto comparativo de la media del indicador porcentaje de riesgos mitigados previo de la ejecución fue de 76,02% y luego incrementó a un 90%. Ver figura 7.

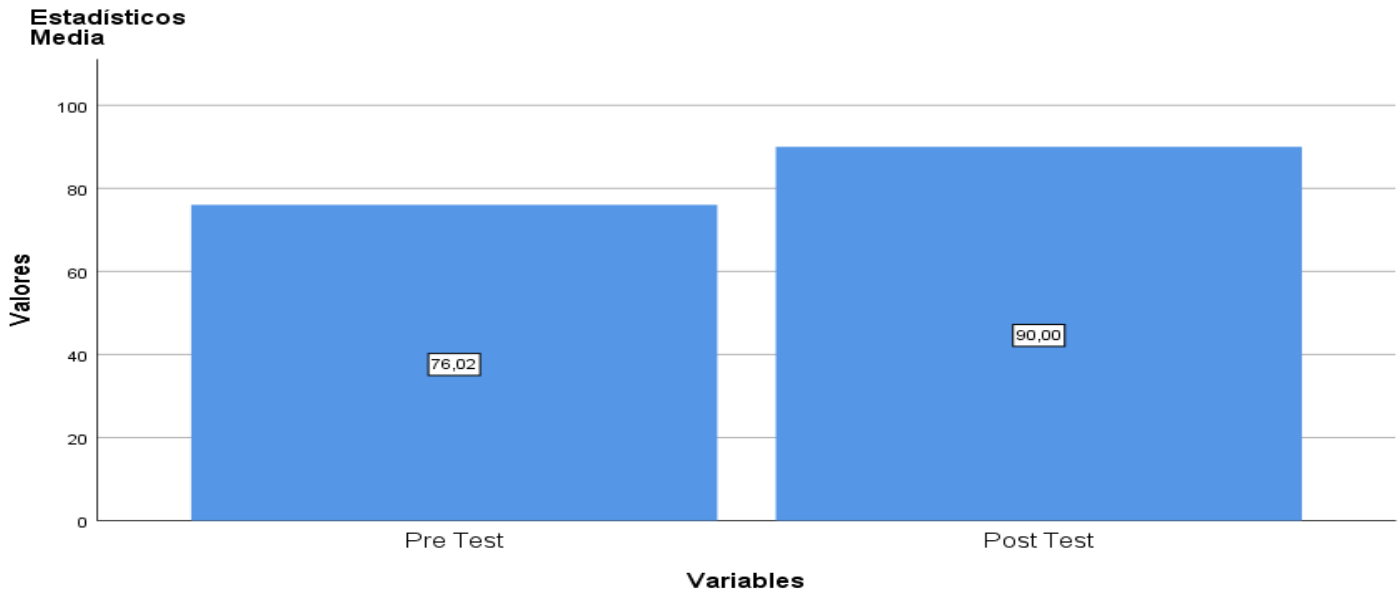


Figura 6. Porcentaje de la medida de porcentaje de incidentes resueltas de seguridad de información.

Resultados descriptivos de la satisfacción de los trabajadores

El resultado obtenido, respecto al indicador nivel de satisfacción respecto a la gestión de riesgos de seguridad de información. En el pre test los resultados obtenidos se identificaron que el 53,3% indicaron que se encuentran totalmente desacuerdo, el 33,3% está en desacuerdo y un 13,3 % en neutral. Luego de la implementación se obtuvo los efectos del post test donde se aprecia que el 20% indica que está de acuerdo y el 80% indica que está totalmente de acuerdo respecto a la seguridad de la información. (ver tabla 9).

Tabla 9. *Análisis descriptivo de satisfacción de los trabajadores*

Niveles	ANTES		DESPUÉS	
Totalmente desacuerdo	8	53,3%	0	0,0%
Desacuerdo	5	33,3%	0	0,0%
Neutral	2	13,3%	0	0,0%
De acuerdo	0	0,0%	3	20,0%
Totalmente de acuerdo	0	0,0%	12	80,0%
Total	15	100,0%	15	100,0%

Fuente: Elaboración Propia

Prueba de normalidad

El resultado para el indicador porcentaje de riesgos mitigados de la dimensión controles de seguridad antes y después de la aplicación de la normativa ISO 27005 se observa en la siguiente tabla (ver tabla 10,11)

Tabla 10. *Resumen de procesamiento de % de riesgos mitigados*

Resumen de procesamiento de casos						
	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
RIESGOS_PRE	20	100,0%	0	0,0%	20	100,0%
RIESGOS_POST	20	100,0%	0	0,0%	20	100,0%

Fuente: Elaboración Propia

Tabla 11. *Prueba de normalidad de % de riesgos mitigados*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
RIESGOS_PRE	,946	20	,308
RIESGOS_POST	,864	20	,009

Fuente: Elaboración Propia

Estos resultados indican el nivel de significancia respecto al % de riesgos mitigados obteniendo en el pre 0.308 y en el post 0,085; se usará la prueba no paramétrica de U Mann de Whitney.

Los resultados obtenidos para el indicador % de incidentes resueltas de seguridad de información de la dimensión Tratamiento de incidentes antes y después de la normativa ISO 27005 se observa en las siguientes tablas (ver tabla 12,13).

Tabla 12. *Resumen de % de incidentes resueltas de seguridad de información*

Resumen de procesamiento de casos						
	Casos					
	Válido		**Perdidos**		**Total**	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
INCIDENTES_PRE	20	100,0%	0	0,0%	20	100,0%
INCIDENTES_POST	20	100,0%	0	0,0%	20	100,0%

Fuente: Elaboración Propia

Tabla 13. *Prueba de normalidad de % de incidentes resueltas de seguridad de información*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
INCIDENTES_PRE	,913	20	,072
INCIDENTES_POST	,584	20	,000

Fuente: Elaboración Propia

Estos resultados indican el nivel de significancia respecto al porcentaje de incidentes resueltas de seguridad de información obteniendo en el pre 0.072 y en el post 0,000; se usará la prueba no paramétrica de U Mann de Whitney.

Contraste de hipótesis de porcentaje de riesgos mitigados

Formulación de hipótesis

Ho: $Me^1 = Me^2$: Marco referencial basado en la ISO 27005 no contribuyó en la reducción de riesgos en la gestión de riesgos de seguridad de información para empresas consultoras de TI

Ha: $Me^1 < Me^2$: Marco referencial basado en la ISO 27005 contribuyó en la reducción de riesgos en la gestión de riesgos de seguridad de información para empresas consultoras de TI

Nivel de confianza

El análisis tiene un grado de confianza de 0.95 y de significancia en un α=0.05

Regla de decisión

Rechazar la Ho, si el sig < α

Aceptar la Ho, si el sig > α

Prueba estadística:

Para la demostración estadística de la investigación luego de la observación de los supuestos de U de Mann- Whitney para grupos independientes se visualiza en la siguiente fórmula:

Es imprescindible medir el U1 Y U2 con los datos del indicador o variables según el grupo de comparación (pre y postest) y se usará la siguiente fórmula:

$$\boldsymbol{U_1 = n_1 n_2 + \frac{n_1(n_1+1)}{2} - R_1 \ ; \ U_2 = n_1 n_2 + \frac{n_2(n_2+1)}{2} - R_2 \ ; \ U = min(U_1, U_2)}$$

La prueba de U de Mann-Whitney se simboliza por medio de Z y su fórmula se presenta a continuación:

$$\boldsymbol{Z = \frac{U - \frac{n_1 n_2}{2}}{\sqrt{\frac{n_1 n_2 (n_1 + n_2 + 1)}{12}}} \sim N(0, 1)}$$

Resultados del estadístico de prueba utilizando SPSS

Se puede observar que los resultados del prestest arrojaron un 260,50 y en el postest fue de un 559,50 aumentado significativamente, de esta forma se concluye que estos resultados son favorables a la investigación. (ver tabla 14)

Tabla 14. *Rangos comparativos de número de % de riesgos mitigados*

Rangos				
	Grupo	N	Rango promedio	Suma de rangos
Riesgos	Pretest	20	13,03	260,50
	Postest	20	27,98	559,50
	Total	40		

Fuente: Elaboración Propia

De igual forma, se observa que existe una desigualdad en los grupos el resultado muestra que el valor de Z= -4,067; este valor ayuda al indicador % de riesgos mitigados; el valor de sig. = 0.000 < α = 0.05 indicando que los grupos evaluados exponen resultados diferentes y favorables para el estudio, es decir qué % de riesgos mitigados aumentó favorablemente después la implementación de la normativo ISO 27005 para la gestión de riesgos de seguridad de información. (ver tabla 15)

Tabla 15. *Estadísticos de prueba de U de Mann-Whitney*

Estadísticos de prueba	
Prueba estadística	% de riesgos mitigados
U de Mann-Whitney	50,500
W de Wilcoxon	260,500
Z	-4,067
Sig. asintótica(bilateral)	,000

Fuente: Elaboración Propia

Distribución de la estadística de prueba

Para realizar el análisis adecuado se utilizó la prueba de normalidad dividida como $z_{tab}(1-\propto /2)$ Reemplazando los valores que se alcanzó como resultado $z_{tab}(0.975)$ = 1.96. Por otro lado, el resultado se compara con Zcal =-4.067 y se representa a través del gráfico de gauss. Ver figura 8.

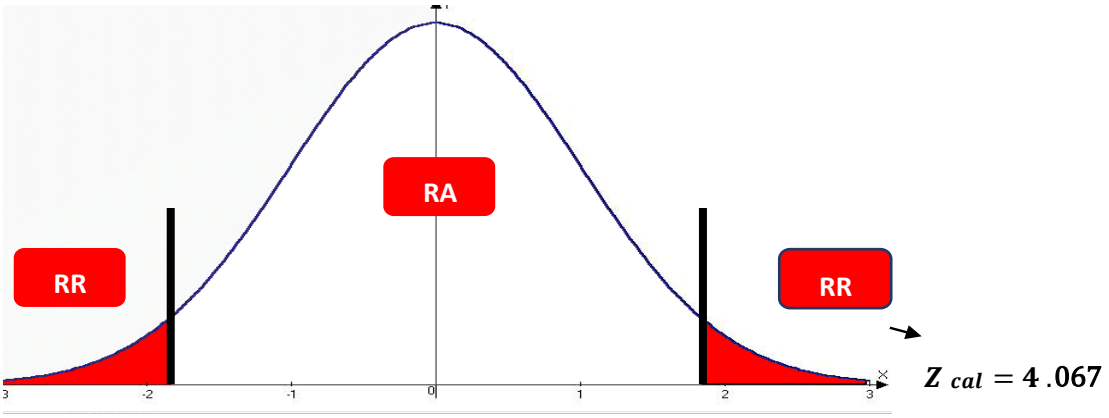


Figura 7. Prueba de hipótesis de % de riesgos mitigados

Como se muestra en la campana de gaus el resultado de Zcal se encuentra en la región de rechazo por lo tanto la Ho se rechaza a favor de Ha, concluyendo que los resultados son favorables. De modo que se acepta la Ha: Marco referencial basado en la ISO 27005 contribuyó en la reducción de riesgos en la gestión de riesgos de seguridad de información para empresas consultoras de TI. Evidenciando un incremento de porcentual en resolución de riesgos mitigados.

Contraste de hipótesis de % de incidentes resueltas de seguridad de información

Formulación de hipótesis

Ho: $Me^1 = Me^2$: Marco referencial basado en la ISO 27005 no contribuyó en la reducción de incidencias en la gestión de riesgos de seguridad de información para empresas consultoras de TI

Ha: $Me^1 < Me^2$: Marco referencial basado en la ISO 27005 contribuyó en la reducción de incidencias en la gestión de riesgos de seguridad de información para empresas consultoras de TI

Nivel de confianza

El análisis tiene un grado de confianza de 0.95 y de significancia en un α=0.05

Regla de decisión

Rechazar la Ho, si el sig < α

Aceptar la Ho, si el sig > α

Prueba estadística:

Para la demostración estadística de la investigación luego de la observación de los supuestos de U de Mann- Whitney para grupos independientes se visualiza en la siguiente fórmula:

Es imprescindible medir el U1 Y U2 con los datos del indicador o variables según el grupo de comparación (pre y postest) y se usará la siguiente fórmula:

$$U_1 = n_1 n_2 + \frac{n_1(n_1+1)}{2} - R_1 \;\; ; \;\; U_2 = n_1 n_2 + \frac{n_2(n_2+1)}{2} - R_2 \; ; \;\; U = min(U_1, U_2)$$

La prueba de U de Mann-Whitney se simboliza por medio de Z y su fórmula se presenta a continuación:

$$Z = \frac{U - \frac{n_1 n_2}{2}}{\sqrt{\frac{n_1 n_2 (n_1 + n_2 + 1)}{12}}} \sim N(0, 1)$$

Resultados del estadístico de prueba utilizando SPSS

Se puede observar que los resultados del prestest arrojaron un 311,50 y en el postest fue de un 508,50 aumentado significativamente, de esta forma se concluye que estos resultados son favorables a la investigación. (ver tabla 16)

Tabla 16. *Rangos comparativos de % de incidentes resueltas de seguridad de información*

Rangos				
Grupo de Análisis		N	Rango promedio	Suma de rangos
% de incidentes resueltas de seguridad de información	Pretest	20	15,58	311,50
	Postest	20	25,43	508,50
	Total	40		

Fuente: Elaboración Propia

De igual forma, el contraste del estudio de estadística de la tabla 17, se observa que existe una desigualdad entre los grupos el resultado muestra que el valor de Z= -2,784; este valor beneficia al indicador % de riesgos mitigados; el valor de sig. = 0.000 < α = 0.05 muestra que los grupos estudiados muestran resultados distintos y favorables para el estudio, es decir qué % de riesgos mitigados aumentó favorablemente después la implementación de la normativo ISO 27005 para la gestión de riesgos de seguridad de información.

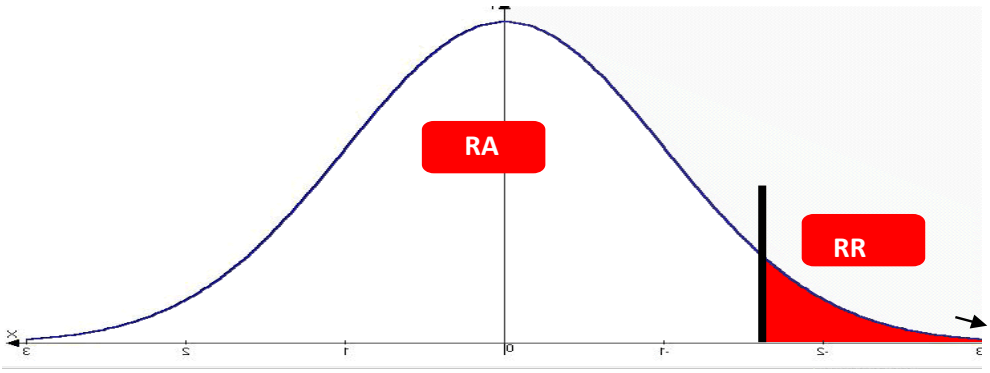
Tabla 17. *Estadísticas de la prueba U de Mann-Whitney de % de incidentes resueltas de seguridad de información*

Prueba estadística	% de incidentes resueltas de seguridad de información
U de Mann-Whitney	101.500
W de Wilcoxon	311.500
Z	-2.784
Sig. asintótica(bilateral)	.005

Fuente: Elaboración Propia

Distribución de la estadística de prueba

Para realizaron análisis adecuado se utilizó estudio de normalidad repartida como z_tab (1-∝/2) Reemplazando los valores que se obtuvo como resultados z_tab (0.975) = 1.96. Por otro lado, el resultado se compara con Zcal =-2.784 y se representa a través del gráfico de gauss, ver figura 9.



$Z_{cal} = 2.784$

$z_{tab} = -1.96$ $z_{tab} = 1.96$

Figura 8. Prueba de hipótesis de % de incidentes resueltas de seguridad de información

Analizando la campana de gaus el resultado de Zcal se encuentra en la región de rechazo por lo que se rechaza la Ho y se acepta él Ha, concluyendo que los resultados son favorables En consecuencia, se acepta la Ha: Marco referencial basado en la ISO 27005 contribuyó en la reducción de incidencias en la gestión de riesgos de seguridad de información para empresas consultoras de TI. Evidenciando un incremento de porcentual en resolución de incidencias resueltas.

V. DISCUSIÓN

Para esta investigación, respecto al primer indicador porcentaje de riesgos mitigados tuvo como finalidad determinar la eficacia del Marco de referencia basado en la ISO 27005 para los controles de seguridad para la gestión de riesgos de seguridad de la información en consultoras de TI. Se obtuvo como resultado sig = 0,000 < α=0.05) por la prueba no paramétrica de U Mann Whitney demostrando de igual forma se identifica que el valor inicial de la media del pretest paso de un 67.39% a un 86,91% demostrando un crecimiento de 19.51%, esto significa que gracias esta normativa se puedo identificar los riesgos a tiempo logrando dar un buen análisis situacional de los peligros. Demostrando que se rechaza la hipótesis nula y se acepta la hipótesis alterna, que la ISO 27005 fue eficaz en la gestión de riesgos de seguridad de información; De igual forma, Fahrurozi et al. (2020) en su artículo titulado "The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence)" señala que con la ejecución de controles informáticos logró aumentar el porcentaje sobre los riesgos mitigados en 75%. Por otra parte Hamit et al. (2020) En su artículo “Adopting an ISO/IEC 27005:2011-based Risk Treatment Plan to Prevent Patients from Data Theft” manifestó que esta normativa mejoró la seguridad de la información aumentando en un 65% respecto a los riesgos mitigados de la empresa. De esta forma es importante la utilización de la ISO 27005 con la cual se logra identificar los riesgos que afecten a la empresa y los activos logrando determinar los controles correspondientes y lograr mitigarlos.

Por otro lado, para el indicador porcentaje de incidentes resueltas de seguridad de información el cual tuvo como objetivo determinar la eficacia del Marco de referencia basado en la ISO 27005 en el tratamiento de incidentes en la gestión de riesgos de seguridad de la información en consultoras de TI. Se obtuvo como resultado como valor (sig = 0,005 < α=0.05) por la prueba no paramétrica de U Mann Whitney de igual forma se identifica que el valor inicial de la media del pretest paso de un 76,02% a un 90% demostrando un crecimiento de 13,97%. Demostrando que se rechaza la hipótesis nula y se acepta la hipótesis alterna, que la ISO 27005 fue eficaz en la gestión de riesgos de seguridad de información; Asimismo, Cruz (2019) En su investigación titulada "Modelo de gestión de riesgos de TI enfocado en estándares adaptados para contribuir en la protección del activo de ti en el sector de distribuidoras de la región Lambayeque" manifiesta que con la implementación de la normativa ISO 27005 logró la mejor toma de decisión y disminuir

los peligros encontrados esto ayudó a la empresa en un crecimiento de 68% de incidentes resueltas. De igual forma, García, Huamani y Alvarado (2018) en su artículo titulado "Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas" manifestó que pudo implementar los controles informáticos adecuados para la disminución de peligros logrando un aumento del 76% de incidentes resueltos respecto a la seguridad informática. En tal sentido se puede confirmar que esta normativa ayuda a la empresa con la identificación, evaluación de los activos en peligro determinando el grado de peligro en el que se encuentran y darles un tratamiento con los controles necesarios para la reducción de los incidentes

Por último, para el indicador nivel de satisfacción respecto a la gestión de riesgos de seguridad de información tuvo como finalidad determinar la eficacia del Marco de referencia basado en la ISO 27005 para el nivel de satisfacción en la gestión de riesgos de seguridad de la información en consultoras de TI. Los valores iniciales que arrojaron indicaron que el 53,3% indicaron que se encuentran totalmente desacuerdo, el 33,3% está en desacuerdo y un 13,3 % en neutral. Luego de la implementación los resultados mostraron que el 20% indica que está de acuerdo y el 80% indica que está totalmente de acuerdo respecto a la seguridad informática; demostrando que los controles de seguridad de información ayudaron con el nivel de satisfacción. Asimismo Carmona (2021) En su tesis titulada “Implementación de una Metodología de Gestión de Riesgos alineada a la ISO 27005 y Magerit para el proceso “OSE” de una empresa de facturación electrónica en la ciudad de Lima - 2021.” Indicó que, con la implementación de los controles necesarios para los peligros, el nivel de satisfacción de los trabajadores aumentó en 80% indicando que esta normativa favoreció en seguridad de información. En tal sentido con la implementación de los controles correctos frente a los peligros informáticos se puede aumentar el nivel de satisfacción con esto los trabajadores se sientan seguros sobre la protección de sus datos.

VI. CONCLUSIÓN

El Marco de referencial basado en la ISO 27005 es eficaz en la gestión de riesgos de seguridad de la información en consultoras de TI, puesto que incrementó el porcentaje de eficacia respecto a los indicadores (% de riesgos mitigados, % de incidentes resueltas de seguridad de información y Nivel de satisfacción respecto a la gestión de riesgos de seguridad de información), lo que permitió efectuar el objetivo de estudio.

El marco de referencial basado en la ISO 27005 favoreció al indicador % de riesgos mitigados dándose a observar que incrementó en un 19,51% esto ayudo a la empresa con la identificación de los activos que se encontraban en peligro para el uso de los controles respectivos para mitigación correspondiente de los peligros.

Por otro lado, el marco de referencial basado en la ISO 27005 favoreció al indicador % de incidentes resueltas de seguridad de información dándose a observar que incrementó en un 13,97%, esto fue beneficioso puesto que con la identificación de criticidad de los activos y controles respectivos se puedo dar un correcto tratamiento a los incidentes.

Finalmente, el marco de referencial basado en la ISO 27005 favoreció al indicador nivel de satisfacción respecto a la gestión de riesgos de seguridad de información donde el 80,0% de los encuestados indicó que se siente totalmente de acuerdo con los controles frente a los peligros informáticos aumentando el nivel de satisfacción beneficiosamente.

VII. RECOMENDACIONES

Se recomienda la actualización de los controles de seguridad de información con versiones de la ISO 27002:2022 o las próximas versiones a futuro con el propósito de mantener un constante cambio de las medidas de seguridad respecto a los nuevos peligros informáticos que se presenten en la compañía.

Se recomienda que el marco referencial basado en la ISO 27005 para la gestión de riesgos de seguridad de información sea implementado en un software que permita generar indicadores gráficos y la generación de escenarios y permita el ingreso de los datos, ingresando los datos respectivos obteniendo el grado de peligro de los activos.

Se recomienda capacitar periódicamente al personal sobre temas de seguridad de información con la finalidad que puedan identificar los posibles riesgos y puedan estar al tanto de las nuevas tendencias y no sean vulnerables.

Se recomienda que las consultoras de Ti implementen este tipo de normativas como la ISO 27005 ya que es beneficiosa en la gestión de riesgos de seguridad de la información obteniendo una identificación, estimación y tratamiento de los peligros informáticos.

REFERENCIAS

AL FIKRI, M., ADITYA, F., SURYANTO, Y. y RAMLI, K., 2019. Risk assessment using NIST and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency. Procedia Computer Science, vol. 161, pp. 1206-1215. ISSN 18770509. DOI 10.1016/j.procs.2019.11.234.

ARCE, Á., ZUÑA, E., ROMERO, W. y SOLEDISPA, C., 2019. Análisis de la seguridad de la información en las PYMES de la ciudad el Milagro. Revista Universidad y Sociedad [en línea], vol. 11, no. 2019, pp. 1-6. [Consulta: 28 abril 2022]. ISSN 2218-3620. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000400487.

ARÍAS, J., 2020. Proyecto de Tesis Guía para la elaboración [en línea]. S.l.: s.n. ISBN 9786120054161. Disponible en: www.agogocursos.com.

ARIAS, J., 2020. Técnicas e instrumentos de investigación científica [en línea]. Arequipa: s.n. ISBN 9786124844409. Disponible en: www.cienciaysociedad.org.

ARIAS, J., 2021. Diseño y metodología de la investigación. Enfoques Consulting EIRL [en línea], pp. 1-133. Disponible en: www.tesisconjosearias.com.

BARRIO, S., 2019. Nuevas tendencias en la gestión de riesgos del control interno. Auditoría Pública, pp. 43-51.

BERNAL, M., SALAMANCA, D., PEREZ, N. y QUEMBA, M., 2020. Validez de contenido por juicio de expertos de un instrumento para medir percepciones físico-emocionales en la práctica de disección anatómica. Educación Médica, vol. 21, no. 6, pp. 349-356. ISSN 1575-1813. DOI 10.1016/J.EDUMED.2018.08.008.

BEZERRA, E., ALCÁNTARA, F., MOTTA, A. y BOCA, J., 2018. Gestión del riesgo de las TI NTC 27005. Bogotá: Escuela Superior de Redes Red Cedia.

BURGDORF, M. y JENDRIA, K., 2022. ISO 27002 revisited. Datenschutz und Datensicherheit - DuD 2022 46:5 [en línea], vol. 46, no. 5, pp. 301-304. [Consulta: 22 junio 2022]. ISSN 1862-2607. DOI 10.1007/S11623-022-1607-6. Disponible en: https://link.springer.com/article/10.1007/s11623-022-1607-6.

CABALLERO, S. y HORACIO DANIEL, K., 2018. Análisis y Gestión de Riesgo en Proyectos Software Un nuevo modelo integrando la metodología SEI y Magerit2. , pp. 1-5.

CABEZAS, I., 2020. Implementación de un framework de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en lima [en línea]. Lima: Universidad San Martin de Porres. [Consulta: 14 junio 2022]. Disponible en: https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/7059/cabezas_jic.pdf?sequence=1&isAllowed=y.

CARMONA, L., 2021. Implementación de una Metodología de Gestión de Riesgos alineada a la ISO 27005 y Magerit para el proceso “OSE” de una empresa de facturación electrónica en la ciudad de Lima -2021. Lima: Universidad Tecnológica del Perú.

CARRASCO, S., 2019. Metodología de La Investigación Científica. [en línea]. [Consulta: 16 junio 2022]. Disponible en: https://www.academia.edu/26909781/Metodologia_de_La_Investigacion_Cientifica_Carrasco_Diaz_1_.

CASTILLO, M. y MOLINA, J., 2020. Análisis de riesgos al proceso de fiscalización de proyectos de ingeniería para una empresa que brinda servicios de ingeniería bajo la norma ISO/IEC 27005 [en línea]. Guayaquil: Escuela Superior Politécnica del litoral. [Consulta: 13 junio 2022]. Disponible en: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/50317.

CHAVARRIA ARAGÓN, A., GISELLA, L., CASTILLO, R. y CARLOS ARTURO, N., 2021. Arquitectura de seguridad de la información para la protección de activos digitales en Pymes [en línea]. Lima: Universidad Peruana de Ciencias Políticas. Disponible en: http://hdl.handle.net/10757/657808.

CISNEROS, A., URDÁNIGO, J., GUEVARA, A. y GARCÉS, J., 2022. Técnicas e Instrumentos para la Recolección de Datos que apoyan a la Investigación Científica en tiempo de Pandemia. núm. 1. Enero-marzo [en línea], vol. 8, pp. 1165-1185. DOI 10.23857/dc.v8i41.2546. Disponible en: http://dominiodelasciencias.com/ojs/index.php/es/index.

CRUZ, G., 2019. Modelo de gestión de riesgos de TI enfocado en estándares adaptados para contribuir en la protección del activo de ti en el sector de distribuidoras de la región Lambayeque [en línea]. Chiclayo: Universidad Católica Santo Toribio de Mogrovejo. [Consulta: 9 junio 2022]. Disponible en: https://orcid.org/0000-0002-9650-4427.

EL PERUANO, 2017. Ley de protección de datos personales N° 29733. Normas Legales. Lima: Editora Perú.

FAHRUROZI, M., TARIGAN, S., TANJUNG, M. y MUTIJARSA, K., 2020. The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence). ICITEE 2020 - Proceedings of the 12th International Conference on Information Technology and Electrical Engineering, pp. 86-91. DOI 10.1109/ICITEE49829.2020.9271748.

FAJARDO, R., 2021. Evaluación de riesgos de seguridad de la información para la empresa MAKOTO S.A.S basada en la norma ISO 27005:2018. Bogotá: Universidad Católica de Colombia.

FAYA, A., VENTURO, C., HERRERA, M. y HERNÁNDEZ, R., 2018. Autonomía del trabajador y Satisfacción laboral en trabajadores de un Universidad Peruana. Apuntes Universitarios, vol. 8, pp. 1-14.

GARCÍA PORRAS, J.C., HUAMANI PASTOR, S.C. y ALVARADO, R.F.L., 2018. Artículo de Contribución Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas Information security risk management model for Peruvian PYMES. Revista Peruana de ComPutaCión y sistemas [en línea], vol. 1, no. 1, pp. 47-56. ISSN 2617-2003. DOI 10.15381/xxxxxxs. Disponible en: http://dx.doi.org/10.15381/xxxxxxsRecibido28/02/2018-aceptado09/03/2018.

GUERRERO, M., MEDINA, A. y NOGUERIA, D., 2020. Procedimiento de gestión de riesgos como apoyo a la toma de decisiones Risk management procedure as a support to decisions making. [en línea], vol. 41, pp. 1-14. [Consulta: 13 mayo 2022]. Disponible en: http://www.rii.cujae.edu.cu.

GUEVARA, G., VERDESOTO, A. y CASTRO, N., 2020. Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción).

RECIMUNDO [en línea], vol. 4, no. 3, pp. 163-173. [Consulta: 16 junio 2022]. DOI 10.26820/recimundo/4.(3).julio.2020.163-173. Disponible en: https://www.recimundo.com/index.php/es/article/view/860.

HAMIT, L., SARKAN, M., FIRDAUS, N., AZMI, M., NAZ'RI MAHRIN, M., CHUPRAT, S. y YAHYA, Y., 2020. Adopting an ISO/IEC 27005:2011-based Risk Treatment Plan to Prevent Patients from Data Theft. , vol. 10, no. 3. ISSN 2088-5334.

HERNÁNDEZ, R. y MENDOZA, C., 2018. Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. ACADEMIA, pp. 1-745.

HUAURA, M., 2019. Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones. Lima: Universidad Nacional Mayor de San Marcos.

IBARRA, S., SEGREDO, S., JUÁRES, L. y TOBÓN, S., 2018. Study of content validity and reliability of an instrument to evaluate the socioformative methodology in the design of courses. Espacios [en línea]. [Consulta: 23 junio 2022]. Disponible en: https://www.revistaespacios.com/cited2017/cited2017-24.html.

INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2020. Protección de la información. , pp. 1-33.

INTERNACIONAL ORGANIZATION FOR STANDARDIZATION, 2017. NTP ISO/IEC 27002 2017.

JACOBO, R., PACHECO, P. y BERTHEAU, E.L., 2020. Validez y confiabilidad del instrumento determinante humano en la implementación del currículo de educación física. Educare [en línea], vol. 24, pp. 205-223. Disponible en: https://orcid.org/0000-0001-9293-5468.

JUÁREZ, L. y TOBÓN, S., 2018. Analysis of the elements implicit in the validation of the content of a research instrument., vol. 39, no. 53.

JURGENS, J. y BISSELL, K., 2022. Global Cybersecurity Outlook 2022 January 2022 In collaboration with Accenture.

LIU, X., CHANG, P., WU, Z., JIANG, M. y SUN, Q., 2022. Malicious data injection attacks risk mitigation strategy of cyber–physical power system based on hybrid measurements attack detection and risk propagation. International Journal of Electrical

Power and Energy Systems, vol. 142. ISSN 01420615. DOI 10.1016/j.ijepes.2022.108241.

MAGAÑA, M., 2020. Análisis y Diseño de Arquitecturas de Ciberseguridad en Distintos Sectores Empresariales [en línea]. Madrid: Universidad Politécnica de Madrid. [Consulta: 14 junio 2022]. Disponible en: https://oa.upm.es/67311/.

MELO, O., 2019. Aspectos a tener en cuenta para el análisis de riesgos con base en las normas ISO/IEC 27001, ISO/IEC 27005 e ISO/ IEC 31000. Universidad Polito de Colombia, pp. 1-11.

NARRO, S., 2021. El sistema de gestión de seguridad de la información y la gestión de riesgos en el área informática de una universidad pública, región Cajamarca 2020. Cajamarca: Universidad Privada del Norte.

ORTEGA, A., 2018. Enfoques de investigación. Enfoques De Investigación: Métodos Para El Diseño Urbano [en línea], pp. 1-34. [Consulta: 16 junio 2022]. Disponible en: https://www.researchgate.net/profile/Alfredo-Otero-Ortega/publication/326905435_ENFOQUES_DE_INVESTIGACION/links/5b6b7f9992851ca650526dfd/ENFOQUES-DE-INVESTIGACION.pdf.

PALTÁN, H., 2018. Desarrollo de un plan de mitigación de seguridad informática a una red inalámbrica de comunicación de datos para una institución privada, a través de la aplicación de hacking ético para la identificación de amenazas, riesgos y vulnerabilidades. [en línea]. Guayaquil: Escuela superior politécnica del litoral. [Consulta: 26 abril 2022]. Disponible en: http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/45975/D-106552.pdf?sequence=-1&isAllowed=y.

PINTO, J., 2017. Gestión y Riesgos de seguridad de la información en la Escuela de Suboficiales de la Policía Nacional del Perú, Puente Piedra 2016. Lima: Universidad Nacional de Educación Enrique Guzmán y Valle.

PUMA, M. y ESTRADA, E., 2020. La motivación laboral y el compromiso organizacional Job motivation and organizational commitment. [en línea], pp. 1-9. Disponible en: http://revistas.uap.edu.pe/ojs/index.php/CYD/index.

QUIJIJE, M. y RODRÍGUEZ, A., 2020. Auditoría informática a la empresa MSA CONSULTING GROUP basado en la norma ISO 27005. Guayaquil: Universidad de Guayaquil.

QUIJIJE ROMERO, M.C. y RODRÍGUEZ GONZÁLEZ, A.R., 2020. Auditoría informática a la empresa MSA Consulting Group basado en la norma ISO 27005 [en línea]. Guayaquil: Universidad de Guayaquil. [Consulta: 13 junio 2022]. Disponible en: http://repositorio.ug.edu.ec/handle/redug/49591.

RAMOS, C., 2021. Diseños de investigación experimental. CienciAmérica, vol. 10, no. 1, pp. 1-7. ISSN 1390-681X. DOI 10.33210/ca.v10i1.356.

REYES, O., 2019. Aspectos a tener en cuenta para el análisis de riesgos con base en las normas ISO/IEC 27001, ISO/IEC 27005 E ISO/ IEC 31000. Universidad Piloto de Colombia, pp. 1-11.

RIOS AGUDELO, C.A., 2020. Arquitectura para automatizar respuesta a incidentes de seguridad de la información relacionados con ataques internos mediante la ejecución de técnicas spoofing. S.l.: Institucion Universitaria.

ROBLES, B., 2018. Índice de validez de contenido: Coeficiente V de Aiken. Pueblo Continente, vol. 29, pp. 1-5.

SALAZAR, C. y CASTILLO, S., 2018. Fundamentos básicos de estadística. 1. S.l.: Fundamentos Básicos de Estadística.

SALGADO, D.C., 2019. Muestra probabilística y no probabilística. México: Universidad Autónoma del estado de México.

SALNYK, S., SYDORKIN, P., NESTERENKO, S., ZAYTCEV, A. y KONOTOPETC, M., 2020. Comparative analysis of the us ISO and NIST standards on assessing the risk of information leakage in communication systems. Journal of Scientific Papers «Social development and Security», vol. 10, no. 6, pp. 29-39. DOI 10.33445/sds.2020.10.6.4.

SANTOS, G., 2017. Validez y confiabilidad del cuestionario de calidad de vida SF-36 en mujeres con LUPUS, Puebla. Puebla: Benemérita Universidad Autónoma de puebla.

SCHIAVONNE, C., 2022. Propuesta de mitigación de riesgos en el sistema facturación de la empresa Pale Consultores haciendo uso de la adaptación de las metodologías

Pentesting Standart y NIST-2022 [en línea]. Cusco: Universidad Andina del Cusco. [Consulta: 14 junio 2022]. Disponible en: https://repositorio.uandina.edu.pe/handle/20.500.12557/4586.

SOLER, R., VALERA, P., OÑATE, A. y NARANJO, E., 2018. La gestión de riesgo: el ausente recurrente de la administración de empresas. Revista Ciencia Unemi [en línea], vol. 11, pp. 51-62. ISSN 2528-7737. Disponible en: https://orcid.

TAFUR, L., 2022. Gestión del Conocimiento para Mejorar la Gestión de Incidentes de Servicios TI - Gobierno Regional de Ancash - Huaraz - Año - 2021. Trujillo: Universidad Cesar Vallejo.

THANGAVELU, M., KRISHNASWAMY, V. y SHARMA, M., 2021. Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study. Computers and Security, vol. 109. ISSN 01674048. DOI 10.1016/j.cose.2021.102401.

TORRES, M., KARIM, P. y SALAZAR, F., 2019. Métodos de recolección de datos para una investigación. Facultad de Ingeniería, pp. 1-21.

UCV, 2017. Referencias estilo ISO 690 y 690-2 Adaptación de la norma de la International Organization for Standardization (ISO). Lima: Fondo Editorial UCV.

VAN DER KLEIJ, R., SCHRAAGEN, J.M., CADET, B. y YOUNG, H., 2022. Developing decision support for cybersecurity threat and incident managers. Computers and Security, vol. 113, pp. 1-15. ISSN 01674048. DOI 10.1016/j.cose.2021.102535.

VASQUEZ, F. y ALVA, J., 2018. Modelo de gestión de riesgos de ti para contribuir en la continuidad del negocio de las microfinancieras de la región Lambayeque. S.l.: s.n.

ANEXOS

Anexo 1. Matriz de operacionalización de variables.

Variable	Definición Conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
Marco referencial basados en la ISO 27005	**ISO 27005** Según Fajardo (2021, p.8) afirma que esta normativa proporciona requisitos para adaptar una evaluación de riesgos sobre los activos tecnológicos críticos en la empresa. De igual manera Quijije y Rodríguez (2020, p.21) está elaborado para ayudar a poner en práctica la seguridad de la información en función de un enfoque de gestión de riesgos.	**ISO 27005:** La ISO 27005 analiza el riesgo por medio de grados de detalle con respecto a la criticidad de los activos, determinando el alcance de las vulnerabilidades identificadas y los incidentes implicados en la organización.	-	-	-
Gestión de riesgos de seguridad de la información	Según Pinto (2017, p.52) Se entiende por gestión de riesgos de seguridad de la información a todas las disposiciones de precaución de las empresas que ayuden a defender y preservar la información logrando conservar la confidencialidad, disponibilidad e integridad de la misma. Según Huaura (2019, p.33) Los incidentes exponen a los activos de la organización generando la obligación de poner en práctica controles de seguridad a partir de un análisis de riesgo para la disminución de peligros.	Según Narro (2021, p. 41)Es el grupo de acciones que ayudan a identificar, analizar y cuantificar un riesgo por medio del uso de acciones de evaluación orientación y supervisión. Estas medidas permiten reducir o mitigar el impacto del peligro.	Controles de seguridad	• % de riesgos mitigados	Razón
			Tratamiento de incidentes	• % de incidentes resueltas de seguridad de información	
			Nivel de satisfacción	• Nivel de satisfacción respecto a la gestión de riesgos de seguridad de información	Ordinal

Fuente: Elaboración Propia

Anexo 2. Matriz de consistencia

<table>
<tr><th>Problema</th><th>Objetivos</th><th>Hipótesis</th><th>Variables e Indicadores</th><th>Métodos y técnicas de investigación</th></tr>
<tr>
<td>•PG: ¿En qué medida el Marco de referencia basado en ISO 27005 favorece en la gestión de riesgos de seguridad de la información en consultoras de TI?

•PE1: ¿En qué medida el Marco de referencia basado en la ISO 27005 favorece en los controles de seguridad para la gestión de riesgos de seguridad de la información en consultoras de TI?
•PE2: ¿En qué medida el Marco de referencia basado en la ISO 27005 favorece en el tratamiento de incidentes en la gestión de riesgos de seguridad de la información en consultoras de TI?
•PE3: ¿En qué medida el Marco de referencia basado en la ISO 27005 favorece con el nivel de satisfacción en la gestión de riesgos de seguridad de la información en consultoras de TI?</td>
<td>•OG: Determinar la eficacia del Marco de referencia basado en la ISO 27005 para la gestión de riesgos de seguridad de la información en consultoras de TI.

•OE1: Determinar la eficacia del Marco de referencia basado en la ISO 27005 para los controles de seguridad para la gestión de riesgos de seguridad de la información en consultoras de TI.
•OE2: Determinar la eficacia del Marco de referencia basado en la ISO 27005 en el tratamiento de incidentes en la gestión de riesgos de seguridad de la información en consultoras de TI.
•OE3: Determinar la eficacia del Marco de referencia basado en la ISO 27005 para el nivel de satisfacción en la gestión de riesgos de seguridad de la información en consultoras de TI.</td>
<td>•HG: El Marco de referencia basado en la ISO 27005 es eficaz en la gestión de riesgos de seguridad de la información en consultoras de TI.

•HE1: El Marco de referencia basado en la ISO 27005 es eficaz para los controles de seguridad en la gestión de riesgos de seguridad de la información en consultoras de TI.
•HE2: El Marco de referencia basado en la ISO 27005 es eficaz en el tratamiento de incidentes en la gestión de riesgos de seguridad de la información en consultoras de TI.

•HE3: El Marco de referencia basado en la ISO 27005 es eficaz en el nivel satisfacción en la gestión de riesgos de seguridad de la información en consultoras de TI.</td>
<td><u>Variable Dependiente:</u>
Gestión de riesgos de seguridad de la información

<u>Indicadores:</u>

D1. Controles de seguridad

1. % de riesgos mitigados

D2. Tratamiento de incidentes

1. % de incidentes resueltas de seguridad de información

D3. Nivel de satisfacción

1.Nivel de satisfacción respecto a la gestión de riesgos de seguridad de información</td>
<td>Métodos:
Tipo: Cuantitativo – Aplicado
Diseño: Experimental de tipo Pre-Experimental
<table>
<tr><th>Grupo</th><th>Antes</th><th>Intervención</th><th>Después</th></tr>
<tr><td>GE</td><td>0_1</td><td>X</td><td>0_2</td></tr>
</table>
GE: Empresas Consultoras de TI
O1: Aplicación de instrumentos en función a los indicadores antes de la ISO 27005

X: Marco referencial basados en la ISO 27005

O2: Aplicación de instrumentos en función a los indicadores después de la ISO 27005

Técnicas e Instrumentos:
De recolección de datos
• Fichaje por ficha de registro
• Encuesta por cuestionario de satisfacción</td>
</tr>
</table>

Fuente: Elaboración Propia

Anexo 3. Ficha de registro del indicador Pre Test: % de riesgos mitigados.

FICHA DE REGISTRO				
Autor	Capcha Da Costa, Gian Carlos	**Tipo de prueba**	Pre Test	X
			Post Test	
Empresa	CFR Business & Solutions E.I.R.L.			
Variable	Gestión de riesgos de seguridad de la información			
Dimensión	Controles de seguridad			
Periodo	20 días			
Fecha de Inicio	29/08/2022	**Fecha de Fin**	19/09/2022	

Indicador	**Descripción**	**Técnica**	**Unidad de Medida**	**Fórmula**
% de riesgos mitigados	La mitigación de riesgos es un proceso donde se ejecuta acciones la cual ayuda a reducir o eliminar el impacto de los incidentes (Liu et al. 2022, p. 2)	Fichaje	Porcentaje	$\%RM = \frac{TRS}{TRI}$ x 100
				%RM= % de riesgos mitigados
				TRS= Total de riesgos solucionados
				TRI= Total de riesgos identificados

N°	**Fecha**	**Total de riesgos Solucionados**	**Total de riesgos Identificados**	**% de riesgos mitigados**
1	29/08/2022	5	10	50,00%
2	30/08/2022	3	5	60,00%
3	31/08/2022	6	8	75,00%
4	01/09/2022	4	7	57,14%
5	02/09/2022	7	10	70,00%
6	03/09/2022	8	9	88,89%
7	05/09/2022	3	5	60.00 %
8	06/09/2022	7	12	58,33%
9	07/09/2022	9	11	81,82%
10	08/09/2022	3	5	60,00%
11	09/09/2022	8	10	80,00%
12	10/09/2022	4	6	66,67%
13	12/09/2022	4	7	57,14%
14	13/09/2022	6	7	85,71%
15	14/09/2022	7	10	70,00%
16	15/09/2022	6	9	66,67%
17	16/09/2022	6	8	75,00%
18	17/09/2022	4	5	80,00%
19	18/09/2022	5	9	55,56%
20	19/09/2022	3	6	50,00%
		Promedio		**67,40%**

Fuente: Elaboración Propia.

Anexo 4. Ficha de registro del indicador Post Test: % de riesgos mitigados.

FICHA DE REGISTRO					
Autor	Capcha Da Costa, Gian Carlos		**Tipo de prueba**	Pre Test	
				Post Test	X
Empresa	CFR Business & Solutions E.I.R.L.				
Variable	Gestión de riesgos de seguridad de la información				
Dimensión	Controles de seguridad				
Periodo	20 días				
Fecha de Inicio	10/10/2022	**Fecha de Fin**	02/11/2022		

Indicador	**Descripción**	**Técnica**	**Unidad de Medida**	**Fórmula**
% de riesgos mitigados	La mitigación de riesgos es un proceso donde se ejecuta acciones la cual ayuda a reducir o eliminar el impacto de los incidentes (Liu et al. 2022, p. 2)	Fichaje	Porcentaje	$\%RM = \frac{TRS}{TRI}$ x 100
				%RM= % de riesgos mitigados
				TRS= Total de riesgos solucionados
				TRI= Total de riesgos identificados

N°	**Fecha**	**Total de riesgos Solucionados**	**Total de riesgos Identificados**	**% de riesgos mitigados**
1	10/10/2022	6	7	85,71%
2	11/10/2022	7	8	87,50%
3	12/10/2022	5	6	83,33%
4	13/10/2022	4	5	80,00%
5	14/10/2022	4	4	100,00%
6	15/10/2022	5	5	100,00%
7	17/10/2022	5	6	83,33%
8	18/10/2022	3	3	100,00%
9	19/10/2022	5	5	100,00%
10	20/10/2022	5	6	83,33%
11	21/10/2022	4	4	100,00%
12	22/10/2022	5	5	100,00%
13	24/10/2022	3	4	75,00%
14	25/10/2022	5	6	83,33%
15	26/10/2022	4	5	80,00%
16	27/10/2022	3	3	100,00%
17	28/10/2022	3	4	75,00%
18	29/10/2022	4	5	80,00%
19	01/11/2022	2	3	66,67%
20	02/11/2022	3	4	75,00%
		Promedio		86,91%

Fuente: Elaboración Propia.

Anexo 5. Ficha de registro del indicador Pre Test: % de incidentes resueltas de seguridad de información.

FICHA DE REGISTRO				
Autor	Capcha Da Costa, Gian Carlos	**Tipo de prueba**	Pre Test	X
			Post Test	
Empresa	CFR Business & Solutions E.I.R.L.			
Variable	Gestión de riesgos de seguridad de la información			
Dimensión	Tratamiento de incidentes			
Periodo	20 días			
Fecha de Inicio	29/08/2022	**Fecha de Fin**	19/09/2022	

Indicador	**Descripción**	**Técnica**	**Unidad de Medida**	**Fórmula**
% de incidentes resueltas de seguridad de información.	Identifica el porcentaje de incidentes que ya se dio un tratamiento de este modo se puede determinar la buena gestión del riesgo (Thangavelu, Krishnaswamy and Sharma 2021, p. 15)	Fichaje	Porcentaje	$\%IRSI = \frac{\text{NIR}}{\text{NIP}} \text{ x } 100$
				%IRSI= % de incidentes resueltas de seguridad de información.
				NIR = N° de incidentes resueltos
				NIP = N° de incidentes presentados

N°	**Fecha**	**N° de incidentes resueltos**	**N° de incidentes presentados**	**% de riesgos mitigados**
1	29/08/2022	3	4	75,00%
2	30/08/2022	2	3	66,67%
3	31/08/2022	3	4	75,00%
4	01/09/2022	3	4	75,00%
5	02/09/2022	4	5	80,00%
6	03/09/2022	5	7	71,43%
7	05/09/2022	3	5	60,00%
8	06/09/2022	4	5	80,00%
9	07/09/2022	2	2	100,00%
10	08/09/2022	3	5	60,00%
11	09/09/2022	4	5	80,00%
12	10/09/2022	2	3	66,67%
13	12/09/2022	3	4	75,00%
14	13/09/2022	6	7	85,71%
15	14/09/2022	4	6	66,67%
16	15/09/2022	5	6	83,33%
17	16/09/2022	3	5	60,00%
18	17/09/2022	3	4	75,00%
19	18/09/2022	3	4	75,00%
20	19/09/2022	3	3	100,00%
		Promedio		75,52%

Anexo 6. Ficha de registro del indicador Post Test: % de incidentes resueltas de seguridad de información.

FICHA DE REGISTRO				
Autor	Capcha Da Costa, Gian Carlos	**Tipo de prueba**	Pre Test	
			Post Test	X
Empresa	CFR Business & Solutions E.I.R.L.			
Variable	Gestión de riesgos de seguridad de la información			
Dimensión	Tratamiento de incidentes			
Periodo	20 días			
Fecha de Inicio	10/10/2022	**Fecha de Fin**	02/11/2022	

Indicador	**Descripción**	**Técnica**	**Unidad de Medida**	**Fórmula**
% de incidentes resueltas de seguridad de información.	Identifica el porcentaje de incidentes que ya se dio un tratamiento de este modo se puede determinar la buena gestión del riesgo (Thangavelu, Krishnaswamy and Sharma 2021, p. 15)	Fichaje	Porcentaje	$\%IRSI = \frac{\text{NIR}}{\text{NIP}} \text{ x } 100$
				%IRSI= % de incidentes resueltas de seguridad de información.
				NIR = N° de incidentes resueltos
				NIP = N° de incidentes presentados

N°	**Fecha**	**N° de incidentes resueltos**	**N° de incidentes presentados**	**% de riesgos mitigados**
1	10/10/2022	2	3	66,67%
2	11/10/2022	2	2	100,00%
3	12/10/2022	1	2	50,00%
4	13/10/2022	1	1	100,00%
5	14/10/2022	0	0	100,00%
6	15/10/2022	0	0	100,00%
7	17/10/2022	1	1	100,00%
8	18/10/2022	1	2	50,00%
9	19/10/2022	1	1	100,00%
10	20/10/2022	1	1	100,00%
11	21/10/2022	1	1	100,00%
12	22/10/2022	1	1	100,00%
13	24/10/2022	2	2	100,00%
14	25/10/2022	2	3	66,67%
15	26/10/2022	0	0	100,00%
16	27/10/2022	1	1	100,00%
17	28/10/2022	2	3	66,67%
18	29/10/2022	1	1	100,00%
19	01/11/2022	0	0	100,00%
20	02/11/2022	2	2	100,00%
		Promedio		90,00%

Anexo 7.Cuestionario de nivel de satisfacción respecto a la gestión de riesgos de seguridad de información.

Instrucciones: Para responder las siguientes preguntas se responderá con una (x) considerando la siguiente escala de 1 a 5 donde:

Escala: Totalmente desacuerdo (1), Desacuerdo (2), Neutral (3), De acuerdo (4) y Totalmente de acuerdo (5)

N°	Ítem	1	2	3	4	5
1	¿La empresa evidencia mecanismos que le permitan una comunicación fluida entre sus áreas asegurando que los correos estén protegidos ante ataques cibernéticos (spam, fishing, Spyware, etc.					
2	¿La empresa cuenta con los protocolos de seguridad necesarios para mantener una navegación segura en internet?					
3	¿La empresa cuenta con protocolos de seguridad como contraseñas cifradas y firewall necesarios para resguardar la información de los trabajadores?					
4	¿La empresa establece o tiene políticas de seguridad ante las amenazas de violación de seguridad?					
5	¿La empresa cuenta con un plan de continuidad del negocio (BCP) ante incidencias como la caída del sistema?					
6	¿La empresa no tiene problemas de seguridad de información como filtrado de datos, caída del sistema, pérdida de acceso de información constantemente?					
7	¿La empresa cuenta con las herramientas necesarias para identificar los riesgos y su impacto?					
8	¿La empresa cuenta con un presupuesto necesario para la seguridad de la información?					
9	¿Los trabajadores son capaces de identificar el posible riesgo informáticos ya sea virus, malware, filtración de datos, encriptación, vulnerabilidad del sistema, denegación de servicios con las políticas de control de seguridad actual de la empresa?					
10	¿Los empleados cuentan con credenciales adecuadas para evitar la suplantación de identidad en los procesos de comunicación de la información (al ingresar al servidor, correo)?					

Fuente: Elaboración Propia.

Anexo 8.Resultados Pre Test del cuestionario de nivel de satisfacción respecto a la gestión de riesgos de seguridad de información

Pre Test										
N°	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
1	5	2	2	2	2	2	5	5	2	2
2	4	1	1	1	1	1	4	5	1	1
3	5	2	3	2	3	3	5	4	3	3
4	5	2	2	3	2	2	5	5	2	2
5	5	1	1	1	1	1	5	5	1	1
6	4	1	2	2	2	2	5	5	1	1
7	4	2	2	2	2	2	5	5	2	2
8	4	2	1	1	1	1	4	5	2	1
9	4	1	1	1	1	1	4	5	1	2
10	4	3	1	1	1	1	5	4	1	1
11	4	1	1	1	1	1	4	5	1	1
12	5	2	3	2	3	3	5	4	3	3
13	5	2	2	3	2	2	5	5	2	2
14	5	1	1	1	1	1	5	5	1	1
15	5	1	1	1	1	1	5	5	1	1

Fuente: Elaboración Propia.

Anexo 9. Resultados Post Test del cuestionario de nivel de satisfacción respecto a la gestión de riesgos de seguridad de información

Post Test										
N°	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
1	5	5	5	5	5	5	5	4	3	5
2	4	5	5	5	5	5	5	5	3	5
3	5	5	5	4	5	5	5	4	3	5
4	5	5	5	5	5	5	5	5	3	5
5	5	5	5	5	5	5	5	4	4	5
6	4	5	5	5	5	5	5	4	3	5
7	4	5	5	5	5	5	5	5	4	5
8	4	5	4	4	4	4	5	4	3	4
9	4	4	4	4	4	4	4	4	3	4
10	4	4	5	5	5	5	4	4	3	5
11	4	5	4	4	5	5	5	3	4	5
12	3	4	4	4	5	5	4	3	3	5
13	4	5	4	4	5	5	5	3	3	5
14	5	5	4	4	5	5	5	3	3	5
15	4	5	4	5	5	5	5	4	3	5

Fuente: Elaboración Propia.

Anexo 10. Carta de Presentación

UNIVERSIDAD CÉSAR VALLEJO

"Año del Fortalecimiento de la Soberanía Nacional"

CARTA DE PRESENTACION

Por el medio del presente documento, ofrecemos un saludo cordialmente al Gerente General de la empresa CFR Business & Solutions E.I.R.L., al señor Fernández Rivera Cristhian Luke, al cual nos dirigimos con el motivo de solicitarle que nos de el permiso necesario para realizar la elaboración de nuestro proyecto de investigación, el cual lleva como título: "Marco referencial basados en la metodología NIST e ISO 27005 para la gestión de riesgos de seguridad de la información para empresas consultoras de TI.", empleando la información necesaria de su empresa. Teniendo como objetivo "Determinar la eficacia del Marco de referencia basado en la metodología NIST e ISO 27005 en la seguridad de la información para empresas consultoras de TI.".

Asegurándole a usted y a sus trabajadores que la recolección de información será totalmente confidencial y anónima, le pedimos que tenga en consideración nuestro proyecto de investigación, y agradecerle por el tiempo tomado. Sin nada más que agregar, nos despedimos, deseándole que tenga un buen día.

Jueves 30 de junio del 2022

Nombre del investigador:

Capcha Da Costa, Gian Carlos

DNI: 74871990

Fuente: Elaboración Propia.

Anexo 11. Documento de consentimiento informado.

AUTORIZACIÓN PARA LA REALIZACIÓN Y DIFUSIÓN DE RESULTADOS DE LA INVESTIGACIÓN

Por medio del presente documento, Yo Fernández Rivera Cristhian Luke identificado con DNI N° 43431977 y representante legal de CFR Business & Solutions E.I.R.L. autorizo a Gian Carlos Capcha Da Costa identificado con DNI N° 74871990 a realizar la investigación titulada: "Marco referencial basado en la normativa ISO 27005 para la gestión de riesgos de seguridad de la información para empresas consultoras de TI" y a difundir los resultados de la investigación utilizando el nombre de CFR Business & Solutions E.I.R.L.

Lima,11 de octubre de 2022

Fernández Rivera Cristhian Luke

DNI N° 43431977

Gerente General

CFR Business & Solutions E.I.R.L.

Fuente: Elaboración Propia.

Anexo 12. Carta de Aceptación de la Empresa

"Año del Fortalecimiento de la Soberanía Nacional"

Señor:

Fernández Rivera Cristhian Luke

Presente:

De nuestra consideración:

Sirva la presente para saludarle cordialmente y a la vez comunicarle que su solicitud de autorización para realizar su proyecto de investigación, titulada "Marco referencial basados en la normativa ISO 27005 para la gestión de riesgos de seguridad de la información para empresas consultoras de TI.", ha sido aceptada por nuestra empresa.

Titulo del proyecto de investigación: "Marco referencial basados en la normativa ISO 27005 para la gestión de riesgos de seguridad de la información para empresas consultoras de TI."

Objetivo: Determinar la eficacia del Marco de referencia basado en la normativa ISO 27005 en la seguridad de la información para empresas consultoras de TI.

Es importante recordarle que se deberá mantenerse la confidencialidad de la información, la cual es propiedad de CFR Business & Solutions E.I.R.L, Esperamos que su investigación sea de gran aporte para nuestra institución. Sin otro particular, me despido.

Jueves 30 de junio del 2022

CFR BUSINESS & SOLUTIONS
Cristhian Fernandez R
GERENTE GENERAL

Firma del participante

Fuente: Elaboración Propia.

Anexo 13. Validación de % de riesgo mitigados por el Experto 1.

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: % DE RIESGOS MITIGADOS

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Mendoza Apaza, Fernando
Título y/o Grado Académico:	Ingeniero Electrónico / Dr. En Educación

Doctor (x) Magister ( ) Ingeniero (x) Licenciado ( ) Otro ( ).....

Universidad que labora:	Universidad César Vallejo
Fecha:	19/11/2022

Título de Investigación: Marco referencial basado en la ISO 27005 para gestión de riesgos de seguridad de información para empresas consultoras de TI

Autores:

- Capcha Da Costa Gian Carlos

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno(71-80%) Excelente(81-100%)

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.					90%
OBJETIVIDAD	Está expresado en conducta observable.					90%
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					90%
ORGANIZACION	Existe una organización lógica.					90%
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					90%
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					90%
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					90%
COHERENCIA	En los datos respecto al indicador.					90%
METODOLOGIA	Responde al propósito de investigación.					90%
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					90%
	TOTAL					90%

III. PROMEDIO DE VALIDACIÓN

90%

IV. OPCIÓN DE APLICABILIDAD

(x) El instrumento puede ser aplicado, tal como está elaborado
( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Fuente: Elaboración Propia.

Anexo 14. Validación de % de riesgo mitigados por el Experto 2.

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE VALIDACIÓN PARA EL EXPERTO: % de incidentes resueltas de seguridad de información

TESIS: Marco referencial basados en la normativa ISO 27005 para la gestión de riesgos de seguridad de la información para empresas consultoras de TI	Fecha 14/07/2022

Instrucciones: Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71 - 80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100% **(colocar el puntaje porcentual en el cuadro que considere)**. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

I. ASPECTOS DE VALIDACION

		VALORACION				
INDICADOR	CRITERIO	0-20%	21-50%	51-70%	71-80%	81-100%
Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
Objetividad	Está expresado en conducta observable.					X
Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
Organización	Existe una organización lógica.					X
Suficiencia	Comprende los aspectos de cantidad y calidad.					X
Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
Consistencia	Está basado en aspectos teóricos y científicos.					X
Coherencia	En los datos respecto al indicador.					X
Metodología	Responde al propósito de investigación.					X
Pertenencia	El instrumento es adecuado al tipo de investigación.					X
	Promedio Total	95%				

Sugerencia: _____

II. OPCIÓN DE APLICABILIDAD

El instrumento puede ser aplicado, tal como está elaborado (X)
El instrumento debe ser mejorado antes de ser aplicado ( )

IV. FIRMA DEL EXPERTO

Mg. Nemias Saboya Rios
DNI: 42001721

Fuente: Elaboración Propia.

Anexo 15. Validación de % de incidentes resueltos de seguridad de información por el Experto 1.

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: % DE INCIDENTES RESUELTAS DE SEGURIDAD DE INFORMACIÓN

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Mendoza Apaza, Fernando
Título y/o Grado Académico:	Ingeniero Electrónico / Dr. En Educación

Doctor (x) Magister ( ) Ingeniero (x) Licenciado ( ) Otro ( ).....

Universidad que labora:	Universidad César Vallejo
Fecha:	19/11/2022

Título de Investigación: Marco referencial basado en la ISO 27005 para gestión de riesgos de seguridad de información para empresas consultoras de TI

Autores:

- Capcha Da Costa Gian Carlos

Deficiente (0-20%) Regular (21-50%) Bueno(51-70%) Muy Bueno(71-80%) Excelente(81-100%)

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.					90%
OBJETIVIDAD	Esta expresado en conducta observable.					90%
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					90%
ORGANIZACION	Existe una organización lógica.					90%
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					90%
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					90%
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					90%
COHERENCIA	En los datos respecto al indicador.					90%
METODOLOGIA	Responde al propósito de investigación.					90%
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					90%
	TOTAL					90%

III. PROMEDIO DE VALIDACIÓN

90%

IV. OPCIÓN DE APLICABILIDAD

(x) El instrumento puede ser aplicado, tal como está elaborado
( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Fuente: Elaboración Propia.

Anexo 16. Validación de % de incidentes resueltos de seguridad de información por el Experto 2.

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE VALIDACIÓN PARA EL EXPERTO: % de incidentes resueltas de seguridad de información

TESIS: Marco referencial basados en la normativa ISO 27005 para la gestión de riesgos de seguridad de la información para empresas consultoras de TI	Fecha 14/07/2022

Instrucciones: Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71 - 80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100% **(colocar el puntaje porcentual en el cuadro que considere)**. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

I. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
Objetividad	Está expresado en conducta observable.					X
Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
Organización	Existe una organización lógica.					X
Suficiencia	Comprende los aspectos de cantidad y calidad.					X
Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
Consistencia	Está basado en aspectos teóricos y científicos.					X
Coherencia	En los datos respecto al indicador.					X
Metodología	Responde al propósito de investigación.					X
Pertenencia	El instrumento es adecuado al tipo de investigación.					X
	Promedio Total	**95%**				

Sugerencia: _____

II. OPCIÓN DE APLICABILIDAD

El instrumento puede ser aplicado, tal como está elaborado (X)
El instrumento debe ser mejorado antes de ser aplicado ( )

IV. FIRMA DEL EXPERTO

Mg. Alarcón Cajas Yohan
DNI: 46189705

Fuente: Elaboración Propia.

Anexo 17. Certificado de validez de los instrumentos por el experto 1.

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	INDICADOR: % de Riesgos Mitigados	Si	No	Si	No	Si	No	
1	$\%RM = \frac{TRS}{TRI} \times 100$	x		x		X		
	INDICADOR: % de incidentes resueltas de seguridad de información	Si	No	Si	No	Si	No	
2	$\%IRSI = \frac{\text{NIR}}{\text{NIP}} \times 100$	x		X		x		

Observaciones (precisar si hay suficiencia):_____

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Mendoza Apaza, Fernando **DNI: 10363032**

Especialidad del validador: Magíster en Administración, Ingeniero de Sistemas

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

19 de noviembre del 2022

Mgtr. Mendoza Apaza, Fernando
DNI: 10363032

Fuente: Elaboración Propia.

Anexo 18. Certificado de validez de las fórmulas por el experto 2.

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Dimensión: Controles de seguridad							
	INDICADOR: % de riesgos mitigados.	Si	No	Si	No	Si	No	
1	$\%RM = \frac{TRI}{TRS} \times 100$	X		X		X		
	Dimensión: Tratamiento de incidentes							
	INDICADOR: % de incidentes resueltas de seguridad de información.	Si	No	Si	No	Si	No	
2	$\%IRSI = \frac{NIP}{NIR} \times 100$	X		X		X		

Observaciones (precisar si hay suficiencia):

_____

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

Especialidad del validador:

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

14 de julio del 2022

Mg. Alarcón Cajas Yohan
DNI: 46189705

Fuente: Elaboración Propia.

Anexo 19. Validación del cuestionario de satisfacción respecto a la gestión de riesgos de seguridad de información por el experto 1.

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	¿La empresa evidencia mecanismos que le permitan una comunicación fluida entre sus áreas asegurando que los correos estén protegidos ante ataques de cibernéticos (spam, fishing, Spyware, ¿etc.)?	X		X		X		
2	¿La empresa cuenta los protocolos de seguridad necesarios como mantener una navegación segura en internet?	X		X		X		
3	¿La empresa cuenta con protocolos de seguridad como contraseñas cifradas y firewall necesarios para resguardar la información de los trabajadores?	X		X		X		
4	¿La empresa establece las políticas de seguridad ante las amenazas de violación de seguridad?	X		X		X		
5	¿La empresa cuenta con los medios requeridos como plan de continuidad del negocio (BCP) para seguir manteniendo sus servicios ante una incidencia?	X		X		X		
6	¿La empresa presenta problemas de seguridad de información como filtrado de datos, caída del sistema, perdida de acceso de información constantemente?	X		X		X		
7	¿La empresa cuenta con las herramientas necesarias como la matriz de riesgos para determinar el grado de impacto ante un riesgo?	X		X		X		
8	¿La empresa invierte el presupuesto necesario en la seguridad de información?	X		X		X		
9	¿Los trabajadores son capaces de identificar un virus o malware con las políticas de control de seguridad actual de la empresa?	X		X		X		
10	¿Los empleados cuentan con credenciales adecuadas para evitar la suplantación de identidad en los procesos de la empresa?	X		X		X		

Observaciones (precisar si hay suficiencia):_____

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. **Mendoza Apaza, Fernando** **DNI: 10363032**

Especialidad del validador: Magíster en Administración, Ingeniero de Sistemas

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

19 de noviembre del 2022

Mgtr. Mendoza Apaza, Fernando
DNI: 10363032

Fuente: Elaboración Propia.

Anexo 20.Validación del cuestionario de satisfacción respecto a la gestión de riesgos de seguridad de información por el experto 2.

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Cuestionario de nivel satisfacción respecto a la gestión de riesgos de seguridad de información

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	¿La empresa evidencia mecanismos que le permitan una comunicación fluida entre sus áreas asegurando que los correos estén protegidos ante ataques de cibernéticos (spam, fishing, Spyware, etc.)?	X		X		X		
2	¿La empresa cuenta los protocolos de seguridad necesarios para mantener una navegación segura en internet?	X		X		X		
3	¿La empresa cuenta con protocolos de seguridad como contraseñas cifradas y firewall necesarios para resguardar la información de los trabajadores?	X		X		X		
4	¿La empresa establece o tiene políticas de seguridad ante las amenazas de violación de seguridad?	X		X		X		
5	¿La empresa cuenta con un plan de continuidad del negocio (BCP) ante incidencias como la caída del sistema?	X		X		X		
6	¿La empresa no tiene problemas de seguridad de información como filtrado de datos, caída del sistema, perdida de acceso de información constantemente?	X		X		X		
7	¿La empresa cuenta con las herramientas necesarias para identificar los riesgos y su impacto?	X		X		X		
8	¿La empresa cuenta con un presupuesto necesario para la seguridad de información?	X		X		X		
9	¿Los trabajadores son capaces de identificar el posible riesgo informáticos ya sea virus, malware, filtración de datos, encriptación, vulnerabilidad del sistema, denegación de servicios con las políticas de control de seguridad actual de la empresa?	X		X		X		
10	¿Los empleados cuentan con credenciales adecuadas para evitar la suplantación de identidad en los procesos de comunicación de la información (al ingresar al servidor, correo)?	X		X		X		

Observaciones (precisar si hay suficiencia): _____

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

Especialidad del validador:

14 de julio del 2022

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

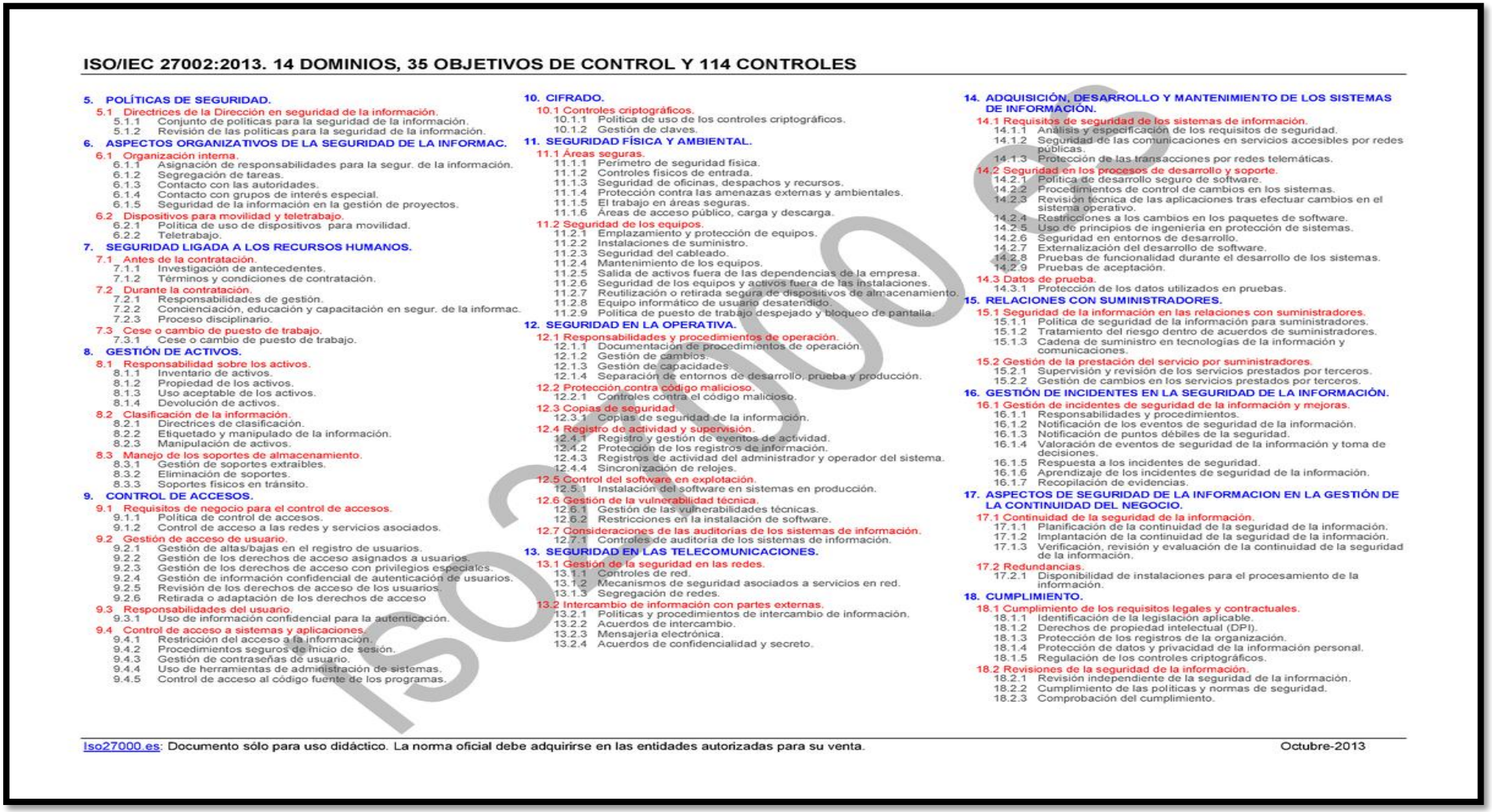
---

Mg. Yohan Roy Alarcón Cajas

DNI: 46189705

Fuente: Elaboración Propia.

Anexo 21. Controles del ISO 27002:2013



ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

 Octubre-2013

Fuente: ISO 27002:2013

Anexo 22. Resolución de cambio de titulo

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

RESOLUCIÓN DIRECTORAL N° 0342- 2022-EP-ING-SIS.UCV LIMA NORTE

Los Olivos, 18 de Noviembre del 2022

VISTO: El Dictamen **N° 0236-2022-EP-ING-SIS.UCV LIMA NORTE** de fecha **11 de Noviembre**, presentado por la comisión evaluadora de la Tesis designado por **coordinación de escuela** de Ingeniería de Sistemas, en el cual se establece la procedencia para el cambio de título de la Tesis **"MARCO REFERENCIAL BASADO EN LA ISO 27005 PARA GESTIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN PARA EMPRESAS CONSULTORAS DE TI** por el (los) estudiante (s) **GIAN CARLOS CAPCHA DA COSTA.**

CONSIDERANDO

Que, mediante **RESOLUCIÓN DIRECTORAL N° 0289-2022-EP-ING-SIS.UCV LIMA NORTE** de fecha **04 de Noviembre del 2022**, se designó a la comisión Evaluadora de la Tesis **"MARCO REFERENCIAL BASADO EN LA ISO 27005 PARA GESTIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN PARA EMPRESAS CONSULTORAS DE TI**(la)estudiante **GIAN CARLOS CAPCHA DA COSTA**; a los siguientes docentes:

Dr. YOHAN ROY ALARCON CAJAS
Dr. JORGE ISAAC NECOCHEA CHAMORRO
Dra. YESENIA DEL ROSARIO VÁSQUEZ VALENCIA

Estando a lo expuesto y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE

ARTÍCULO 1º: SE APROBO EL CAMBIO DE TITULO de la Tesis denominada: **"MARCO REFERENCIAL BASADO EN LA ISO 27005 PARA GESTIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN PARA EMPRESAS CONSULTORAS DE TI"** Presentada por el (los) estudiante (s) **GIAN CARLOS CAPCHA DA COSTA.**

Regístrese, comuníquese y archívese.

Dra. YESENIA DEL ROSARIO VÁSQUEZ VALENCIA
Coordinadora Académica
Escuela Profesional de Ingeniería de Sistemas
UCV Lima Norte

Anexo 23. Aplicación de la normativa ISO 27005 para la gestión de riesgos de seguridad de la información

Establecimiento del contexto

Según la Norma ISO/IEC 27005, el establecimiento del contexto se divide en: Contexto Interno y Contexto Externo en las cuales se determina el alcance de la gestión de riesgo dentro de la empresa, logrando identificar las metas de la empresa alineadas con las responsabilidades y los procesos.

Contexto Interno:

El sector en el que está Cfr. Business & Solutions E.I.R.L es el de Consultoría e Informática es un servicio profesional dirigido a empresas, instituciones u otro tipo de organizaciones, y que tiene como finalidad someter a examen sus procesos e identificar problemas, irregularidades o incumplimientos de algún marco normativo o legal, o aspectos técnicos que se pueden mejorar.

Objetivo de la Empresa:

Ser una empresa líder a nivel Nacional e Internacional en soluciones tecnológicas empresariales reconocidas de clase mundial. Para lograrlo, tenemos a nuestros Clientes en continua innovación de soluciones a través de servicios profesionales de excelencia, logrando con ellos una relación a largo plazo y superen sus desafíos empresariales.

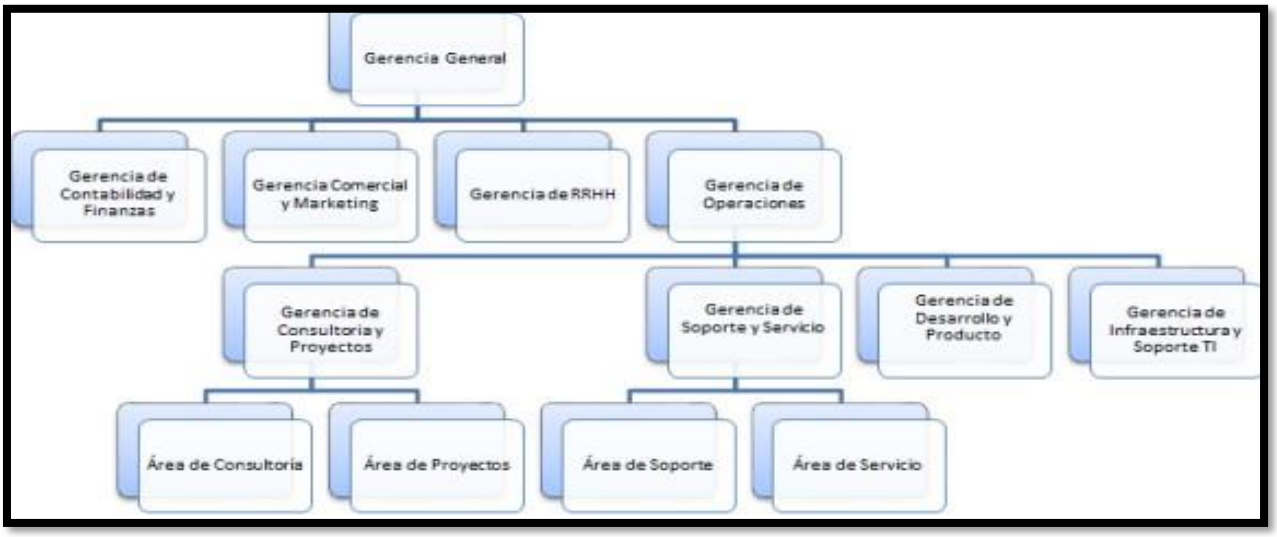
Misión

Ser la mejor opción en soluciones y consultoría SAP, con el mejor equipo de profesionales, satisfaciendo de manera eficiente las necesidades operativas y administrativas de nuestros clientes, logrando una adecuada rentabilidad de su empresa.

Visión

En el 2023 ser una empresa posicionada como una de las mejores opciones en soluciones y consultoría SAP Business One.

La empresa Cfr. Business & Solutions E.I.R.L encuentra constituida por las siguientes áreas:



Contexto Externo

En la siguiente tabla se puede apreciar un análisis FODA las cuales se podrá identificar las Fortalezas, Debilidades, Oportunidades y Amenazas de la empresa. Ver tabla 18.

Tabla 18: *análisis FODA de Cfr. Business & Solutions E.I.R.L.*

Fortalezas	Debilidades
• Experiencia en Sap Business One • Calidad de servicio prestado • Constante capacitación del personal	• Presencia en las redes sociales • Inversión tecnológica escasa • Inadecuado control de políticas de seguridad • Ubicación geográfica no favorable
Oportunidades	**Amenazas**
• Amplio mercado laboral • Nuevas tecnologías para trabajar • Buena relación con los clientes	• Competencia del mismo rubro de servicio • Inestabilidad económica • Ataques cibernéticos

Fuente: Elaboración Propia.

Evaluación del riesgo

En esta fase según la Norma ISO/IEC 27005 se identifica los riesgos que se puedan presentar dentro de la empresa CFR Business & Solutions E.I.R.L. de esta forma se reconoce las posibles amenazas, vulnerabilidades y efectos relacionados con los activos de la empresa de esta forma se logra identificar “El catálogo de Riesgos” o también conocido como lista de riesgos.

Identificación de activos

Para establecer los activos se deben tener en cuenta la fase preliminar “Establecimiento del contexto”, esta correlación ayuda a evaluar los activos importantes de la empresa incluyendo los procesos Core que necesitan ser protegidos ya que estos impactan al proceso general.

La norma ISO/IEC 27005 se divide En 2 categorías: Los activos principales (Activos primarios) y activos Secundarios (Activos de Apoyo)

Activos Primarios

A continuación, se muestra una lista de los activos Core (Activos Primarios) de la empresa. Ver tabla 19.

Tabla 19. *Activos Primarios de CFR Business & Solutions E.I.R.L.*

Procesos	Descripción
Consultoría y Proyectos	Encargada de la implementación de sistemas de información como Sap Business One, Odoo, Business Intelligence e interfaces e integración para SAP
Soporte y Servicios	Encargada de brindar soluciones a los clientes brindando reportes para temas de implementación y encargada de brindar productos y desarrollo que cumplan con la función de solucionar una problemática del cliente
Tecnología de Información	Encargada de desarrollo de addon, aplicaciones web con conexión a SAP, mantenimiento de servidores, páginas web, integraciones de sistemas.

Fuente: Elaboración Propia.

Activos Secundarios

A continuación, se muestra una lista de los activos de apoyo (Activos secundarios) de la empresa CFR Business & Solutions E.I.R.L., ver tabla 20.

Tabla 20. *Activos secundarios de CFR Business & Solutions E.I.R.L.*

Categoría	Descripción
Hardware	Laptops
	PC
	Impresoras
	Discos de almacenamiento externo
Software	Base de datos SQL
	BD de página web
	Sap Bussines one
	SAP HANA Cloud
	Página Web
	Data transfer workbench
Redes	Router
	Switch
Personal	Usuarios internos

Fuente: Elaboración Propia.

Valoración de los activos

Luego de la identificación de los activos es importante asignar un valor para determinar el grado de riesgo ante la posibilidad de pérdida, daño o difusión del activo de esta forma identificar lo valioso que será un activo y las pérdidas ocasionadas para la empresa de esta forma se dividirá en 3 dimensiones la valoración. Para la valoración se usará la escala de Likert en una escala de 1 al 5 para establecer la conformidad en las 3 dimensiones (Confidencialidad, Integridad, Disponibilidad).

Confidencialidad (C): Asegura la privacidad de la información por medio de la restricción de accesos a terceros de esta forma solo el personal autorizado a dichos datos (Instituto Nacional de Ciberseguridad 2020, p. 6).(ver tabla 21)

Integridad (I): Asegurar que la información sea precisa y confiable (Instituto Nacional de Ciberseguridad 2020, p. 6). (ver tabla 22)

Disponibilidad (D): Asegurar que la información sea accesible cuando sea requerida (Instituto Nacional de Ciberseguridad 2020, p. 6). (ver tabla 23)

Tabla 21. *Valores de criterios de Confidencialidad.*

Confidencialidad (C)	Valor	Criterio
	5	El perjuicio es catastrófico, fraude, pérdida de reputación y credibilidad
	4	El perjuicio es relevante, el incidente afecta a otros procesos
	3	El incidente no afecta a otros procesos
	2	El incidente no es tan grave
	1	No relevante

Fuente: Elaboración Propia.

Tabla 22. *Valores de criterios de Integridad.*

Integridad (I)	Valor	Criterio
	5	Debe se precisa y confiable al menos en un 95.5%
	4	Debe se precisa y confiable al menos en un 75%
	3	Debe se precisa y confiable al menos en un 50%
	2	No es precisa y confiable
	1	No relevante

Fuente: Elaboración Propia.

Tabla 23. *Valores de criterios de Disponibilidad.*

Disponibilidad (D)	Valor	Criterio
	5	Debe ser accesible al menos en el 95.5% del tiempo
	4	Debe ser accesible al menos en el 75% del tiempo
	3	Debe ser accesible al menos en el 50% del tiempo
	2	Debe ser accesible al menos en el 10% del tiempo
	1	No relevante

Fuente: Elaboración Propia.

El grado de criticidad de los activos se obtendrá de la sumatoria de las calificaciones hechas por cada criterio de seguridad (ver tabla 24) y obtendrá la siguiente clasificación:

Nivel de criticidad: Confidencialidad + Integridad + Disponibilidad

Tabla 24. *Niveles de criticidad de activos*

Rango	Nivel de Criticidad	Descripción		Criterio
1-3	1	Muy Bajo	MB	Insignificante en los procesos
4-6	2	Bajo	B	Afecta los procesos en un 10%, sin pérdida de información.
7-9	3	Medio	M	Afecta los procesos en un 50%, sin pérdida de información.
10-12	4	Alto	A	Afecta los procesos en un 75%, ocasiona casi poca pérdida de información.
13-15	5	Muy alto	MA	Afecta los procesos en un 95%, significativa pérdida de información.

Fuente: Elaboración Propia.

De esta forma se obtendrá el rango en el que se encuentra el activo frente al nivel de criticidad. Ver tabla 25.

Tabla 25. *Cuadro de Criterios de criticidad de activos*

N° Activo	Nombre de activo	Criterio de Seguridad			Total	Nivel de Criticidad
		C	I	D		
1	Consultoría y Proyectos	4	3	4	11	Alto [A]
2	Soporte y Servicios	3	4	5	12	Alto [A]
3	Tecnología de Información	5	4	4	13	Muy Alto [MA]
4	Laptops	4	4	4	12	Alto [A]
5	PC	4	5	4	13	Muy Alto [MA]
6	Impresoras	3	4	3	10	Alto [A]
7	Discos de almacenamientos externos	5	5	5	15	Muy Alto [MA]
8	Base de datos SQL	5	5	5	15	Muy Alto [MA]
9	BD de página web	3	3	4	10	Alto [A]
10	Sap Bussines one	4	5	5	14	Muy Alto [MA]
11	SAP HANA Cloud	5	5	5	15	Muy Alto [MA]
12	Página Web	4	4	4	12	Alto [A]
13	Data transfer workbench	3	3	3	9	Medio [M]
14	Router	4	5	4	13	Muy Alto [MA]
15	Switch	3	5	4	12	Alto [A]

Fuente: Elaboración Propia.

Identificación de vulnerabilidades, amenazas, consecuencias

Luego de la identificación los principales activos de la empresa es necesario determinar los posibles campos de acción logrando reconocer las posibilidades de riesgo, que área o proceso afectará, cual es el problema y los efectos si se llegase a materializar.

Para esto se elaboró una tabla para identificar los peligros de los activos primarios (ver tabla 26) y los activos secundarios (ver tabla 27) donde se analizó el riesgo, causas y posibles efectos, de esta forma la siguiente tabla está compuesta por (columna 1) Nombre del activo, (columna 2) Amenaza (columna 3) vulnerabilidades, (columna 4) Riesgo.

Tabla 26.*Identificación de peligros de los activos primarios*

Activo	Amenaza	Vulnerabilidad	Riesgo	
			Código	Consecuencia
Consultoría y Proyectos	Mala estimación de costos para la implementación	Mal manejo de los tiempos y mala comunicación de los costos para la implementación de Sap Business Ones	R1	Perdía de cliente potenciales, credibilidad e ingresos
Soporte y Servicios	Mal manejo de prioridad de requerimientos solicitados	Falta de conocimientos técnico	R2	Demora en el proceso de solución al cliente.
Tecnología de Información	Ataques de SQL Injection a las Base de datos	Mala activación de firewall, credenciales no modificadas, registros sin cifrado	R3	Hacking, pérdida de veracidad de la información de los clientes y pérdida de reputación.
	Robo de información	Mal manejo de privilegios en los usuarios	R4	Divulgación de datos, fraude, chantaje
	Vencimiento de licencias	Falta de gestión y seguimiento de las licencias en los equipos tecnológicos	R5	Hacking, Pérdida de confianza de los clientes

	Falla técnica sobre el monitoreo de las sentencias y programas desarrollados	El encargado de TI no verificó las sentencias ejecutadas, error de cambiar la IP de desarrollo al de producción	R6	Datos inconsistentes, merma de tiempo y retraso de las operaciones, pérdida de datos
	Corrupción de datos	Almacenamiento no protegido por falta de autenticación de privilegios en el servidor, Falta de copias de respaldo en las bases de datos o copias de seguridad incompletas	R7	Pérdida de datos, fraude, pérdida de reputación y credibilidad

Fuente: Elaboración Propia.

Tabla 27. *Identificación de peligros de los activos secundarios*

Activo	Amenaza	Vulnerabilidad	Riesgo	
			Código	Consecuencia
Laptops	Acceso no autorizado	Errores de configuración Errores en los sistemas de validación. Errores que permiten el acceso a directorios.	R8	Fuga de información importante y robo de contraseñas y cuentas de los clientes

	Infección de virus (cualquier tipo)	Ingresar a páginas inadecuadas, mal control sobre los correos electrónicos(spam) Errores de configuración	R9	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de datos personales
	Obsolescencia tecnológica de equipos de cómputo	Carencia de un plan de cambios de equipos de cómputo de acuerdo a su vida útil.	R10	Lentitud de las operaciones de venta debido a fallas de equipos de cómputo.
	Hurto o robo de activo	Falta de control en el listado de activos	R11	Pérdida de información importante
PC	Acceso no autorizado	Errores de configuración Errores en los sistemas de validación. Errores que permiten el acceso a directorios.	R12	Fuga de información importante y robo de contraseñas y cuentas de los clientes
	Infección de virus (cualquier tipo)	Ingresar a páginas inadecuadas, mal control sobre los correos electrónicos(spam) Errores de configuración	R13	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de datos personales
	Hurto de equipos	Deficiencia de procedimientos de control de salida e ingresos de equipos	R14	Pérdida del equipo por robo.

	Corte de Energía eléctrica	Corte de Energía eléctrica	R15	Interrupción de las operaciones por corte de energía eléctrica
	Fuego (Incendio)	Carencia de sistema de seguridad contra incendio, planes y procedimientos contra incendio	R16	Pérdida de equipos por eventos de fuego
	Agua (Inundaciones, fugas) Infraestructura inadecuada para instalación de equipos.	Infraestructura inadecuada para instalación de equipos	R17	Pérdida de equipos por eventos de agua.
	Obsolescencia tecnológica de equipos de cómputo	Carencia de un plan de cambios de equipos de cómputo de acuerdo a su vida útil.	R18	Lentitud de las operaciones de venta debido a fallas de equipos de cómputo.
Base de datos SQL	Acceso no autorizado	Contraseñas débiles Base de datos sin actualización	R19	Hackeo o robo de la cuenta para venderlo a terceros
	Robo de información por infección de virus	Datos sensibles sin cifrar Inyección de SQL	R20	Control de la base de datos, secuestro de información de los usuarios
	Abuso de privilegios de acceso.	Falta de políticas de acceso al servidor de BD.	R21	Robo de información
	Errores de mantenimiento y	Inadecuado control de mantenimientos y actualización de software	R22	Retraso en las operaciones

	actualización de software.			
	Error de configuración de hardware	Carencia de un plan de gestión de cambios.	R23	Fallas de operación del equipo.
	Agotamiento de recursos de hardware	Inadecuado dimensionamiento de hardware (disco duro, memoria ram, etc.,)	R24	Interrupción del sistema y lentitud de las operaciones
	Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (UPS, Generador eléctrico	R25	Interrupción de las operaciones por corte de energía eléctrica.
BD de página web	Acceso no autorizado.	Modificación no autorizada de BD y configuraciones	R26	Pérdida de integridad de datos
		Carencia de auditoría detallada de acceso y acciones ejecutadas a la base de datos.	R27	Robo de información
Impresoras	Perdida de documentos	Modificación de configuraciones de red	R28	Los documentos pueden ser expuestos en la bandeja de salida y sustraída por personas no autorizadas
	Hurto de equipos	Deficiencia de procedimientos de control de salida e ingresos de equipos	R29	Pérdida del equipo por robo.

	Corte de Energía eléctrica	Corte de Energía eléctrica	R30	Interrupción de las operaciones por corte de energía eléctrica
	Obsolescencia tecnológica de equipos de cómputo	Carencia de un plan de cambios de equipos de cómputo de acuerdo a su vida útil.	R31	Lentitud de las operaciones de venta debido a fallas de equipos de cómputo.
	Malware o virus	Infección por códigos maliciosos	R32	Infección a todos los equipos conectados a la misma red
Router	Acceso no autorizado	Mal cifrado de la clave Wi-Fi	R33	Toma de control del router, modificación de DNS, habilitación de entradas a otros dispositivos.
	Secuestro de DNS	Modificación de configuraciones de red	R34	Desvió de trafico de red manipulando la configuración de DNS para un posterior robo de dato
Switch	Malware o virus	Puertos abiertos	R35	Ingreso a la red y ejecución de servicios no autorizados en los puestos de red.
	Avería de equipos de comunicación	Falla del Switch core	R36	Pérdida de la conexión la red LAN
		Falla de equipos de radio enlaces	R37	Pérdida de la conexión de la red MAN
		Falla de equipos de enrutamiento WAN	R38	Pérdida de la conexión de la red WAN

		Ausencia de políticas de mantenimiento preventivo de los equipos de comunicación	R39	Deterioro del equipo e infraestructura de comunicación.
Página Web	Acceso no autorizado	Pérdida de control de accesos	R40	Ingreso de hacker al sistema con permiso de usuario y administrador teniendo accesos al registro, direcciones y archivos confidenciales para una posterior divulgación
		Carencia de auditoría detallada de acceso y acciones ejecutadas a la base de datos.	R41	Robo de información
		Modificación no autorizada de BD y configuraciones.	R42	Pérdida de integridad de datos
	Error de usuario.	Carencia de validación de datos de entradas del usuario.	R43	Pérdida de integridad de datos
	Redirección a sitios maliciosos	Inyección de códigos malicioso	R44	Redirección a otra página pudiendo descargar malwares, software malicioso y ataques de phishing, etc
Sap Bussines one	Acceso no autorizado	Errores en los sistemas de validación. Contraseñas débiles	R45	Alteración de documentos y robo de datos.

SAP HANA Cloud	Acceso no autorizado	Contraseñas débiles Base de datos sin actualización	R46	Hackeo o robo de la cuenta para venderlo a terceros
	Abuso de privilegios de acceso.	Falta de políticas de acceso al servidor de BD.	R47	Robo de información
	Errores de mantenimiento y actualización de software.	Inadecuado control de mantenimientos y actualización de software	R48	Retraso en las operaciones
	Error de configuración de hardware	Carencia de un plan de gestión de cambios.	R49	Fallas de operación del equipo.
	Agotamiento de recursos de hardware	Inadecuado dimensionamiento de hardware (disco duro, memoria ram, etc.,)	R50	Interrupción del sistema y lentitud de las operaciones
	Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (UPS, Generador eléctrico	R51	Interrupción de las operaciones por corte de energía eléctrica.
	Robo de información por infección de virus	Datos sensibles sin cifrar Inyección de SQL	R52	Control de la base de datos, secuestro de información de los usuarios
Data transfer workbench	Acceso no autorizado	Errores en los sistemas de validación. Contraseñas débiles	R53	Alteración de documentos y cargar erróneas de datos.

Usuarios internos	Ataque cibernético con o sin intención	Mala asignación de privilegios o permisos	R54	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios

Fuente: Elaboración Propia.

Análisis del riesgo

Para el siguiente análisis se evaluarán las consecuencias de los procesos, para posteriormente darle una evaluación del riesgo dependiendo su nivel de impacto que se encuentra. Esto proporcionará a encontrar la mejor toma de decisión frente al tratamiento del riesgo y las estrategias a realizar para la mitigación.

Evaluación de las consecuencias

Para la siguiente evaluación se tiene como datos las matrices de los activos primarios y secundarios para luego determinar el impacto (ver tabla 29) y la probabilidad (ver tabla 28) que este riesgo ocurra.

Matriz de riesgo por probabilidad

Tabla 28. *Escala de riesgo por probabilidad*

PROBABILIDAD		
Valor	**Clasificación**	**Descripción**
5	Casi Seguro	Se podría presentar mensualmente.
4	Probable	Se podría presentar mensualmente.
3	Posible	Se podría presentar hasta tres veces al año.
2	Improbable	Se podría presentar una vez al año.
1	Raro	No se presenta en varios años.

Fuente: Elaboración Propia.

Matriz de riesgo por impacto

Tabla 29. *Escala de riesgo por impacto*

	IMPACTO	
Valor	**Clasificación**	**Descripción**
5	Muy Alto	Tiene un efecto adverso grave o catastrófico que paraliza todas las operaciones o activos críticos de la organización
4	Alto	Tiene un efecto adverso grave o catastrófico que paraliza algunas operaciones o activos críticos de la organización
3	Moderado	Tiene un efecto adverso considerable que ralentiza operaciones o activos de la organización.
2	Bajo	Tiene un efecto adverso limitado en las operaciones o activos, de la organización
1	Muy Bajo	Tiene un efecto adverso insignificante en las operaciones o activos de la organización.

Fuente: Elaboración Propia.

Luego de identificar las escalas predefinidas anteriormente para determinar los niveles del activo, el nivel de probabilidad de una amenaza, el nivel de las consecuencias para cada activo en peligro se podrá calcular la medida del riesgo multiplicando (probabilidad x impacto) = Medida del riesgo

Evaluación del riesgo

La evaluación del riesgo es el desarrollo de los resultados del análisis del riesgo con los criterios de riesgo para definir si el riesgo, su magnitud o ambos son aceptables o tolerables. (Melo, 2019, pag. 9)

Los criterios que se para la priorización del riesgo, se presenta a continuación:

Tabla 30. *Criterios de criticidad*

		Valor					
PROBABILIDAD	Casi Seguro	5	5	10	15	20	25
	Probable	4	4	8	12	16	20
	Posible	3	3	6	9	12	15
	Improbable	2	2	4	6	8	10
	Raro	1	1	2	3	4	5
		Valor	1	2	3	4	5
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
			IMPACTO				

Fuente: Elaboración Propia.

Escala de Priorización del riesgo

Tabla 31. *Escala de criticidad*

Nivel de Riesgo	Calificación
Muy Alto	15 a 25
Alto	9 a 14
Moderado	4 a 8
Bajo	1 a 3

Fuente: Elaboración Propia.

A continuación, se mostrará una matriz con la valoración de los activos primarios (ver tabla 32) evaluado por activo, la probabilidad, el impacto, determinación del nivel del riesgo y la clasificación de prioridad del riesgo.

Tabla 32. *Matriz de valoración de los activos*

Código	Riesgo	Probabilidad		Impacto		Evaluación del Riesgo	Categoría
		Nivel	Descripción	Nivel	Descripción		
R1	Perdía de cliente potenciales, credibilidad e ingresos	1	Raro	2	Bajo	2	Bajo
R2	Demora en el proceso de solución al cliente.	1	Raro	2	Bajo	2	Bajo
R3	Hacking, pérdida de veracidad de la información de los clientes y pérdida de reputación.	1	Raro	2	Bajo	2	Bajo
R4	Divulgación de datos, fraude, chantaje	3	Posible	4	Alto	12	Alto
R5	Hacking, Pérdida de confianza de los clientes	3	Posible	3	Moderado	9	Alto
R6	Datos inconsistentes, merma de tiempo y retraso de las operaciones, pérdida de datos	1	Raro	2	Bajo	2	Bajo
R7	Perdida de datos, fraude, pérdida de reputación y credibilidad	2	Improbable	4	Alto	8	Moderado
R8	Fuga de información importante y robo de contraseñas y cuentas de los clientes	3	Posible	5	Muy Alto	15	Muy Alto
R9	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de datos personales	2	Improbable	5	Muy Alto	10	Alto

R10	Lentitud de las operaciones de venta debido a fallas de equipos de cómputo.	4	Raro	4	Alto	16	Muy Alto
R11	Pérdida de información importante	4	Probable	4	Alto	16	Muy Alto
R12	Fuga de información importante y robo de contraseñas y cuentas de los clientes	3	Posible	4	Alto	12	Alto
R13	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de datos personales	2	Improbable	4	Alto	8	Moderado
R14	Pérdida del equipo por robo.	3	Posible	2	Bajo	6	Moderado
R15	Interrupción de las operaciones por corte de energía eléctrica	2	Improbable	5	Muy Alto	10	Alto
R16	Pérdida de equipos por eventos de fuego	1	Raro	4	Alto	4	Moderado
R17	Pérdida de equipos por eventos de agua.	3	Posible	2	Bajo	6	Moderado
R18	Lentitud de las operaciones de venta debido a fallas de equipos de cómputo.	1	Raro	4	Alto	4	Moderado
R19	Hackeo o robo de la cuenta para venderlo a terceros	3	Posible	3	Moderado	9	Alto
R20	Control de la base de datos, secuestro de información de los usuarios	3	Posible	5	Muy Alto	15	Muy Alto
R21	Robo de información	4	Probable	4	Alto	16	Muy Alto
R22	Retraso en las operaciones.	2	Improbable	5	Muy Alto	10	Alto

R23	Fallas de operación del equipo.	1	Raro	5	Muy Alto	5	Moderado
R24	Interrupción del sistema y lentitud de las operaciones	1	Raro	4	Alto	4	Moderado
R25	Interrupción de las operaciones por corte de energía eléctrica.	2	Improbable	5	Muy Alto	10	Alto
R26	Pérdida de integridad de datos	1	Raro	3	Moderado	3	Bajo
R27	Robo de información	1	Raro	3	Moderado	3	Bajo
R28	Los documentos pueden ser expuestos en la bandeja de salida y sustraída por personas no autorizadas	2	Improbable	2	Bajo	4	Moderado
R29	Pérdida del equipo por robo.	3	Posible	2	Bajo	6	Moderado
R30	Interrupción de las operaciones por corte de energía eléctrica	2	Improbable	5	Muy Alto	10	Alto
R31	Lentitud de las operaciones de venta debido a fallas de equipos de cómputo.	1	Raro	4	Alto	4	Moderado
R32	Infección a todos los equipos conectados a la misma red	3	Posible	3	Moderado	9	Alto
R33	Toma de control del router, modificación de DNS, habilitación de entradas a otros dispositivos.	1	Raro	2	Bajo	2	Bajo

R34	Desvió de trafico de red manipulando la configuración de DNS para un posterior robo de dato	1	Raro	2	Bajo	2	Bajo
R35	Ingreso a la red y ejecución de servicios no autorizados en los puestos de red.	2	Improbable	2	Bajo	4	Moderado
R36	Pérdida de la conexión la red LAN	2	Improbable	5	Muy Alto	10	Alto
R37	Pérdida de la conexión de la red MAN	3	Posible	4	Alto	12	Alto
R38	Pérdida de la conexión de la red WAN	2	Improbable	5	Muy Alto	10	Alto
R39	Deterioro del equipo e infraestructura de comunicación.	2	Improbable	3	Moderado	6	Moderado
R40	Ingreso de Hacker al sistema con permiso de usuarios y administrar teniendo acceso al registro, direcciones y archivos confidenciales para la divulgación.	2	Improbable	4	Alto	12	Alto
R41	Robo de información.	1	Raro	3	Posible	3	Bajo
R42	Pérdida de integridad de datos	1	Raro	3	Posible	3	Bajo
R43	Pérdida de integridad de datos	3	Posible	2	Bajo	6	Moderado
R44	Redirección a otra página pudiendo descargar malwares, software malicioso y ataques de phishing, etc	2	Improbable	4	Alto	12	Alto
R45	Alteración de documentos y robo de datos.	3	Posible	3	Moderado	9	Alto

R46	Hackeo o robo de la cuenta para venderlo a terceros	3	Posible	2	Bajo	6	Moderado
R47	Robo de información	4	Probable	4	Alto	16	Muy Alto
R48	Retraso en las operaciones.	2	Improbable	5	Muy Alto	10	Alto
R49	Fallas de operación del equipo.	1	Raro	5	Muy Alto	5	Moderado
R50	Interrupción del sistema y lentitud de las operaciones	1	Raro	4	Alto	4	Moderado
R51	Interrupción de las operaciones por corte de energía eléctrica.	2	Improbable	5	Muy Alto	10	Alto
R52	Control de la base de datos, secuestro de información de los usuarios	3	Posible	4	Alto	12	Muy Alto
R53	Alteración de documentos y cargar erróneas de datos.	3	Posible	2	Bajo	6	Moderado
R54	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios	3	Posible	3	Moderado	9	Alto

Fuente: Elaboración Propia.

Luego de la identificación del riesgo y la identificación según su categoría se representará en una gráfica el impacto de los riesgos identificados en la fase de evaluación del riesgo con el propósito de facilitar la toma de decisión con respecto al tratamiento que se tomará para peligros encontrados, en la siguiente matriz se observa la información resultante de los cuadros de valoración del riesgos estos ubicados en un mapa de calor donde el eje x representa la probabilidad del riesgo y el eje y representa el impacto del riesgo. Ver tabla 33

Tabla 33. *Matriz de calor*

PROBABILIDAD					
5					
4				R11, R21, R47, R10	
3		R14, R29, R43, R46, R53, R17	R5, R19, R32, R45, R54	R4, R12, R37, R52	R8,20
2		R28, R35	R39	R7, R13, R40, R44	R9, R15, R22, R25, R30, R36, R48, R51
1		R1, R2, R3, R33, R34	R6, R26, R27, R41, R42	R16, R18, R24, R31, R50	R23, R49
	1	2	3	4	5
	IMPRACTO				

Fuente: Elaboración Propia.

Tratamiento del riesgo

Luego de dar una valoración oportuna a los riesgos identificados, es importante planificar en qué forma se le va a contrarrestar aquellos escenarios que dieron un valor alto mediante un tratamiento del peligro con acciones oportunas para la mitigación y lograr riesgos residuales aceptables por la empresa, dentro de estas acciones se tomarán en cuenta:

Evitar el riesgo: Se implementan las acciones para hacer que las condiciones o los factores que pueden generar el riesgo desaparezcan, y con ellos, el riesgo.

Reducir el riesgo: El riesgo se reduce a través de la prevención por medio de la implementación de controles.

Aceptar el riesgo: Decisión generada por la entidad de aceptar las consecuencias y probabilidad de un riesgo**.**

Transferir el riesgo: El riesgo puede ser transferido a otra empresa que tenga más capacidad de tratarlo.

Donde, E= Evitar el riesgo, R= Reducir el riesgo, A= Aceptar el riesgo, T = Transferir el riesgo

A continuación, se muestra un plan de tratamiento de los riesgos (ver tabla 34) sobre los activos de valoración media, alta y muy alta:

Tabla 34. *Tratamiento del riesgo*

Código	Riesgo	Evaluación del Riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002	Responsable de implementación	Actividades
R8	Fuga de información importante y robo de contraseñas y cuentas de los clientes	15	Muy Alto	R	**9.4.1 Restricción de acceso a la información** El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de acceso.	controlar los datos que pueden ser accedidos por un usuario en particular; controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar; controlar los derechos de acceso de otras aplicaciones; limitar la información contenida en las salidas; proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicación o sistemas.	Jefe de TI	-Creación de contraseñas que tengan como mínimo 9 caracteres y contemplar mayúsculas, minúsculas, números y caracteres especiales

R10	Pérdida de información importante	16	Muy Alto	R	**8.2.1 Clasificación de la información** Los propietarios de los activos deberían revisar los derechos de acceso de usuario a intervalos regulares.	los derechos de acceso de los usuarios deberían ser revisados en intervalos regulares y después de cualquier cambio, tal como la promoción, la degradación o la terminación del empleo, los derechos de acceso de usuario deberían ser revisados y reasignados al pasar de un rol a otro dentro de la misma organización; las autorizaciones de los derechos de acceso privilegiados deberían revisarse a intervalos más frecuentes.	Jefe de TI	-Clasificación de información, restricción de accesos a los usuarios que no tengan que ver en esa área
R11	Fuga de información importante y	16	Muy Alto	R	**9.2.5 Revisión de derechos de**	los derechos de acceso de los usuarios deberían	Jefe de TI	-Gestión de contraseñas y control de

	robo de contraseñas y cuentas de los clientes				**acceso de usuarios** Los propietarios de los activos deberían revisar los derechos de acceso de usuario a intervalos regulares.	ser revisados en intervalos regulares y después de cualquier cambio, tal como la promoción, la degradación o la terminación del empleo, los derechos de acceso de usuario deberían ser revisados y reasignados al pasar de un rol a otro dentro de la misma organización; las autorizaciones de los derechos de acceso privilegiados deberían revisarse a intervalos más frecuentes.		las cuentas de los usuarios, revisión de los accesos
R20	El hacker puede actuar en el sistema con permiso de usuario y	15	Muy Alto	R	Brindar credenciales según roles y funciones a los usuarios de las bases de datos.	Software de control de acceso, análisis de logs e informes gerenciales, control de acceso físico	Jefe de TI	-Revisión de los accesos del personal

	administrador teniendo accesos al registro, direcciones y archivos confidenciales para una posterior divulgación				Separar o independizar las funciones de los usuarios de los sistemas de información, con el fin de evitar la incompatibilidad ad entre las mismas, los fraudes y los errores ocasionados por accesos autorizados o no autorizados			
R21	Redirección a otra página pudiendo descargar malwares, software malicioso y ataques de phishing, etc	16	Muy Alto	R	**9.4.5 Control de acceso al código fuente de los programas** El acceso al código fuente de los programas debería estar restringido. **12.2.1 Controles contra software**	El acceso al código de los programas fuente y elementos asociados deberían estar estrictamente controlados, con el fin de prevenir la introducción de funcionalidades no autorizadas y evitar cambios no intencionales, así como para mantener la confidencialidad de la propiedad	Desarrollador Web	-Manejo de guardado de códigos -Acceso solo al personal autorizado

					malicioso (malware) Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concientización apropiada de los usuarios.	intelectual de valor Establecimiento de una política formal que prohibida el uso de software no autorizado; implementación de controles que previenen o detectan el uso de software no autorizado		
R47	Pérdida de datos, fraude, pérdida de reputación y credibilidad	16	Muy Alto	R	**6.1.3 Contacto con autoridades** Contactos apropiados con autoridades relevantes deberían ser mantenidos.	Las organizaciones deberían tener procedimientos vigentes que especifiquen cuándo y con qué autoridades (por ejemplo, las fuerzas policiales, organismos reguladores y autoridades de supervisión) deberían contactarse y cómo	Jefe de TI	-Acceso solo al personal autorizado

						identificar los incidentes de seguridad de la información que deberían reportarse en el momento oportuno (por ejemplo, si se sospecha que se está incumpliendo la ley).		
R5	Hacking, Pérdida de confianza de los clientes	9	Alto	R	**12.2.1 Controles contra software malicioso** Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concientización apropiada de los usuarios.	Establecimiento de una política formal que prohibida el uso de software no autorizado; implementación de controles que previenen o detectan el uso de software no autorizado	Jefe de TI	Clasificación de información, restricción de accesos a los usuarios que no tengan que ver en esa área

R19	Ingreso a la red y ejecución de servicios no autorizados en los puestos de red.	9	Alto	R	**13.1.2 Seguridad de servicios de red** Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deberían ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.	Las medidas de seguridad necesarias para los servicios particulares, tales como características de seguridad, niveles de servicio y los requisitos de gestión, deberían estar identificadas. La organización debería asegurarse que los proveedores de los servicios de red implementan estas medidas.	Jefe de TI	Clasificación de información, restricción de accesos a los usuarios que no tengan que ver en esa área
R32	Infección a todos los equipos conectados a la misma red	9	Alto	R	**13.1.3 Segregación en redes** Grupos de servicios de información, usuarios y sistemas de información deberían estar	El perímetro de cada dominio debería estar bien definido. Se permite el acceso entre dominios de la red, pero debería ser controlado en el perímetro utilizando una puerta de	Jefe de TI	Protección de red por vpn

					segregados en redes.	enlace (por ejemplo, cortafuegos, router con capacidad de filtrado).		
R45	Alteración de documentos y robo de datos	9	Alto	R	**8.2.1 Clasificación de la información** La información debería ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.	La clasificación y los controles de protección asociados a la información deberían tener en cuenta las necesidades del negocio para compartir o restringir la información, así como los requisitos legales	Jefe de TI	-Manejo de documentación -Restricción de accesos
R54	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios	9	Alto	R	**9.4.3 Sistema de gestión de contraseñas** Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar que	La política debería incluir los requisitos para la gestión de claves. La contraseña deberá tener mínimo 9 caracteres y contemplar mayúsculas, minúsculas, números y	Jefe de TI	Clasificación de información, restricción de accesos a los usuarios que no tengan que ver en esa área

					las contraseñas sean de calidad.	caracteres especiales.		
R4	Divulgación de datos, fraude, chantaje	12	Alto	R	**13.2.4 Acuerdos de confidencialidad o no divulgación** Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deberían estar identificados, revisados regularmente y documentados	Los acuerdos de confidencialidad o de no divulgación deberían abordar la necesidad de proteger la información confidencial usando términos legalmente exigibles. Los acuerdos de confidencialidad o de no divulgación son aplicables a las partes externas o empleados de la organización.	Jefe de TI	Clasificación de información, restricción de accesos a los usuarios que no tengan que ver en esa área
R12	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de	12	Alto	R	**9.2.2 Aprovisionamiento de acceso a usuario** Un proceso formal de aprovisionamiento de acceso a usuarios	obtener la autorización del propietario del sistema o servicio de información para el uso del sistema o servicio de información; la aprobación	Jefe de TI	Clasificación de información, restricción de accesos a los usuarios que no tengan que ver en esa área

	datos personales				debería ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.	separada para los derechos de acceso de administración también puede ser apropiado; verificar que el nivel de acceso concedido sea apropiado a las políticas de acceso y es consistente con otros requisitos, tales como la segregación de funciones.		
R37	Pérdida de la conexión de la red MAN	12	Alto	T	**13.1.3 Segregación en redes** Grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en redes.	El perímetro de cada dominio debería estar bien definido. Se permite el acceso entre dominios de la red, pero debería ser controlado en el perímetro utilizando una puerta de enlace (por ejemplo, cortafuegos, router con capacidad de filtrado).	Soporte técnico	Protección de red por vpn

R52	Control de la base de datos, secuestro de información de los usuarios	12	Alto	R	**9.1.1 Política de control de acceso** Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Los propietarios de activos deberían determinar las reglas de control de acceso apropiadas, los derechos de acceso y restricciones para las funciones específicas de los usuarios con respecto a sus activos, con el nivel de detalle y el rigor de los controles que reflejan los riesgos de seguridad de información asociados.	Jefe de TI	Clasificación de información, restricción de accesos a los usuarios que no tengan que ver en esa área y eliminado de accesos a trabajadores que ya no pertenezcan a esta área
R9	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de datos personales	10	Alto	R	**9.4.1 Restricción de acceso a la información** El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia	controlar los datos que pueden ser accedidos por un usuario en particular; controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar; controlar los derechos de	Jefe de TI	eliminado de accesos a trabajadores que ya no pertenezcan a esta área

					con la política de control de acceso.	acceso de otras aplicaciones; limitar la información contenida en las salidas; proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicación o sistemas.		
R15	Los documentos pueden ser expuestos en la bandeja de salida y sustraída por personas no autorizadas	4	Alto	R	**13.2.3 Mensajes electrónicos** La información involucrada en mensajería electrónica debería estar protegida apropiadamente.	Proteger los mensajes de acceso no autorizado, modificación o denegación de servicio acorde con el sistema de clasificación adoptado por la organización; garantizar la dirección correcta y el transporte del mensaje; la fiabilidad y disponibilidad del servicio; las	Jefe de TI	Control y supervisión de los activos

						consideraciones legales, por ejemplo, la obligación para las firmas electrónicas.		
R22	Alteración de documentos y robo de datos.	9	Alto	R	**8.2.1 Clasificación de la información** La información debería ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.	La clasificación y los controles de protección asociados a la información deberían tener en cuenta las necesidades del negocio para compartir o restringir la información, así como los requisitos legales	Jefe de TI	eliminado de accesos a trabajadores que ya no pertenezcan a esta área
R25	Alteración de documentos y cargar erróneas de datos.	10	Alto	R	**8.2.3 Manejo de activos** Los procedimientos para el manejo de activos deberían ser Los procedimientos para el manejo	las restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación; el mantenimiento de un registro formal de los destinatarios autorizados de los	Jefe de TI	Control de accesos Manejo de información

					de activos deberían ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.	activos; la protección de las copias temporales o permanentes de información a un nivel consistente con la protección de la información original.		
R30	Interrupción de las operaciones por corte de energía eléctrica	10	Alto	R	**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	controles para reducir al mínimo el riesgo de amenazas físicas potenciales, como: hurto, fuego, explosivos, humo, inundaciones (o falta de suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética y vandalismo	Soporte técnico	Supervisión constante de los equipos y interruptores eléctricos

R36	Pérdida de la conexión la red LAN	10	Alto	T	**13.1.3 Segregación en redes** Grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en redes.	El perímetro de cada dominio debería estar bien definido. Se permite el acceso entre dominios de la red, pero debería ser controlado en el perímetro utilizando una puerta de enlace (por ejemplo, cortafuegos, router con capacidad de filtrado).		Protección de red por vpn
R48	Retraso en las operaciones .	10	Alto	R	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad	se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo	Soporte técnico	Clasificación de información, restricción de accesos a los usuarios que no tengan que ver en esa área

R51	Interrupción de las operaciones por corte de energía eléctrica	10	Alto	R	**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	controles para reducir al mínimo el riesgo de amenazas físicas potenciales, como: hurto, fuego, explosivos, humo, inundaciones (o falta de suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética y vandalismo	Soporte técnico	Supervisión constante de los equipos y interruptores eléctricos
R14	Control de la base de datos, secuestro de información de los usuarios	6	Moderado	R	**9.4.1 Restricción de acceso a la información** **9.4.3 Sistema de gestión de contraseñas**	controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar permitir a los usuarios seleccionar y cambiar sus propias	Jefe de TI	eliminado de accesos a trabajadores que ya no pertenezcan a esta área

						contraseñas e incluir un procedimiento de confirmación para tener en cuenta errores de entrada		
R17	Pérdida de equipos por evento de agua	6	Moderado	T	**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	El equipamiento debería situarse de manera que minimice el acceso innecesario a las áreas de trabajo; Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	Soporte técnico	Supervisión constante de los equipos y cañerías
R29	Pérdida del equipo por robo.	6	Moderado	R	**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para	Las instalaciones de almacenamiento deberían asegurarse para evitar el acceso no autorizado; las instalaciones de procesamiento de	Soporte técnico	Manejo de lista de activos empresariales

					reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	la información que manejan datos sensibles deberían colocarse cuidadosamente para reducir el riesgo de que la información sea vista por personas no autorizadas durante su uso		
R43	Pérdida de integridad de datos	6	Moderado	R	**12.3.1 Respaldo de la información** Copias de respaldo de la información, del software y de las imágenes del sistema deberían ser realizadas y verificadas regularmente en concordancia con una política de respaldo acordada.	Debería establecerse una política de respaldo para definir los requisitos de la organización para los respaldos de la información, software y sistemas. La política de respaldo debería definir los requisitos de retención y protección. Deberían proporcionarse instalaciones adecuadas de respaldo para garantizar que toda	Jefe de TI	eliminado de accesos a trabajadores que ya no pertenezcan a esta área

						la información y software esenciales se pueden recuperar después de un desastre o falla de medios.		
R46	Hackeo o robo de la cuenta para venderlo a terceros	6	Moderado	R	**12.2.1 Controles contra software malicioso (malware)** Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concientización apropiada de los usuarios.	La protección contra software malicioso debería basarse en el empleo de software de detección de código malicioso y reparación, en la creación de conciencia de la seguridad de información y en apropiados controles de acceso al sistema y gestión de cambios	Jefe de TI	eliminado de accesos a trabajadores que ya no pertenezcan a esta área
R53	Alteración de documentos y cargar	6	Moderado	R	**8.2.1 Clasificación de la información**	La clasificación y los controles de protección asociados a la	Jefe de TI	eliminado de accesos a trabajadores que ya no

	erróneas de datos.				La información debería ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.	información deberían tener en cuenta las necesidades del negocio para compartir o restringir la información, así como los requisitos legales		pertenezcan a esta área
R28	Los documentos pueden ser expuestos en la bandeja de salida y sustraída por personas no autorizadas	4	Moderado	R	**13.2.2 Acuerdo sobre transferencia de información** Los acuerdos deberían dirigir la transferencia segura de información del negocio entre la organización y partes externas**.**	las responsabilidades de gestión para el control y la notificación de transmisión, despacho y recepción; b) los procedimientos para garantizar la trazabilidad y el no repudio; c) las normas técnicas mínimas para el empaquetado y transporte	Jefe de TI	Control y supervisión de los activos
R35	Ingreso a la red y ejecución servicios no	4	Moderado	R	**13.1.1 Controles de la red**	las responsabilidades y procedimientos	Soporte técnico	Protección de red por vpn

	autorizados en los puestos de red.				Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	para la gestión de equipos de red debería estar establecida; la responsabilidad operacional de las redes debería separarse de las operaciones de cómputo donde sea apropiado; deberían establecerse controles especiales para resguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas o sobre las redes inalámbricas y para proteger los sistemas conectados y aplicaciones; controles especiales también pueden ser necesarios para mantener la		

						disponibilidad de los servicios de red y computadoras conectadas; los sistemas en la red deberían estar autenticados; la conexión de sistemas a la red debería ser restringida		
R39	Deterioro del equipo e infraestructura de comunicación.	6	Moderado	R	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	sólo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo	Soporte técnico	Mantenimiento semanal de los equipos
R7	Perdida de datos, fraude, perdida de	8	Moderado	R	Configuración de firewall en las bases de datos y canales	Configuración de firewall en las bases de datos y canales de enlace	Jefe de TI	eliminado de accesos a trabajadores que ya no

	reputación y credibilidad				de enlace por sitios públicos, encriptación de información sensible.	por sitios públicos, encriptación de información sensible.		pertenezcan a esta área
R13	Hackeo o robo de la cuenta para venderlo a terceros	8	Moderado	R	**9.4.1 Restricción de acceso a la información** El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de acceso.	controlar los datos que pueden ser accedidos por un usuario en particular; controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar; controlar los derechos de acceso de otras aplicaciones; limitar la información contenida en las salidas; proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicación o sistemas.	Jefe de TI	eliminado de accesos a trabajadores que ya no pertenezcan a esta área

R40	Ingreso de Hacker al sistema con permiso de usuarios y administrar teniendo acceso al registro, direcciones y archivos confidenciales para la divulgación.	8	Moderado	R	**9.2.1 Registro y baja de usuarios** Un proceso formal de registro y baja de usuarios debería estar implementado para permitir la asignación de derechos de acceso.	Utilizar la identificación única de usuario (ID´s) para que los usuarios puedan estar vinculados y sean responsable de sus acciones; el uso de identificaciones compartidas debería sólo ser permitido cuando sean necesarios por razones de negocios o de funcionamiento y debería estar aprobados y documentados; deshabilitar o quitar inmediatamente los ID de usuario a los usuarios que han dejado la organización	Jefe de TI	eliminado de accesos a trabajadores que ya no pertenezcan a esta área
R44	Redirección a otra página pudiendo descargar malwares,	8	Moderado	R	**9.4.5 Control de acceso al código fuente de los programas**	El acceso al código de los programas fuente y elementos asociados (tales como diseños, especificaciones,	Desarrollador Web	Protección de los códigos Acceso solo al personal autorizado

	software malicioso y ataques de phishing, etc				El acceso al código fuente de los programas debería estar restringido.	planos de verificación y planos de validación) deberían estar estrictamente controlados, con el fin de prevenir la introducción de funcionalidades no autorizadas y evitar cambios no intencionales, así como para mantener la confidencialidad de la propiedad intelectual de valor		
R10	Pérdida de información importante	4	Moderado	R	**9.2.5 Revisión de derechos de acceso de usuarios** Los propietarios de los activos deberían revisar los derechos de acceso de usuario a intervalos regulares.	los derechos de acceso de los usuarios deberían ser revisados en intervalos regulares y después de cualquier cambio, tal como la promoción, la degradación o la terminación del empleo, los derechos de	Jefe de TI	Acceso solo al personal autorizado

						acceso de usuario deberían ser revisados y reasignados al pasar de un rol a otro dentro de la misma organización; las autorizaciones de los derechos de acceso privilegiados deberían revisarse a intervalos más frecuentes.		
R16	Infección a todos los equipos conectados a la misma red	4	Moderado	R	**13.1.1 Controles de la red** Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	las responsabilidades y procedimientos para la gestión de equipos de red debería estar establecida; la responsabilidad operacional de las redes debería separarse de las operaciones de cómputo donde sea apropiado; deberían establecerse controles	Jefe de TI	Clasificación de información, restricción de accesos a los usuarios que no tengan que ver en esa área

						especiales para resguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas o sobre las redes inalámbricas y para proteger los sistemas conectados y aplicaciones; controles especiales también pueden ser necesarios para mantener la disponibilidad de los servicios de red y computadoras conectadas; los sistemas en la red deberían estar autenticados; la conexión de sistemas a la red debería ser restringida		
R18	Lentitud de las operaciones	4	Moderado	R	**11.2.4 Mantenimiento de equipos**	sólo el personal de mantenimiento debidamente	Soporte técnico	Mantenimiento de los equipos

	de venta debido a fallas de equipos de cómputo.				Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo		
R24	Control de la base de datos, secuestro de información de los usuarios	4	Moderado	R	**9.2.1 Registro y baja de usuarios** Un proceso formal de registro y baja de usuarios debería estar implementado para permitir la asignación de derechos de acceso	Utilizar la identificación única de usuario (ID´s) para que los usuarios puedan estar vinculados y sean responsable de sus acciones; el uso de identificaciones compartidas debería sólo ser permitido cuando sean necesarios por razones de negocios o de funcionamiento y debería estar	Administrador de Bases de Datos	eliminado de accesos a trabajadores que ya no pertenezcan a esta área

						aprobados y documentados; deshabilitar o quitar inmediatamente los ID de usuario a los usuarios que han dejado la organización; periódicamente identificar y eliminar o desactivar los ID de usuario redundantes; asegurarse de que los ID de usuario redundantes no se otorguen a otros usuarios.		
R31	Lentitud de las operaciones de venta debido a fallas de equipos de cómputo.	4	Moderado	T	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	sólo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos; se debería mantener registros de todos los fallos, reales o sospechados, así	Jefe de TI	Mantenimiento de los equipos

						como de todo el mantenimiento preventivo y correctivo		
R50	Interrupción del sistema y lentitud de las operaciones	4	Moderado	R	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	sólo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo	Jefe de TI	Mantenimiento de los equipos
R23	Hackeo o robo de la cuenta para venderlo a terceros	5	Moderado	R	**9.4.3 Sistema de gestión de contraseñas** Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar que	La política debería incluir los requisitos para la gestión de claves. La contraseña deberá tener mínimo 9 caracteres y contemplar mayúsculas, minúsculas, números y	Jefe de TI	eliminado de accesos a trabajadores que ya no pertenezcan a esta área

					las contraseñas sean de calidad.	caracteres especiales.		
R49	Fallas de operación del equipo.	5	Moderado	R	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	sólo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo	Soporte técnico	Mantenimiento semanal de los equipos

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, MENDOZA APAZA FERNANDO, 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 Completa titulada: "MARCO REFERENCIAL BASADO EN LA ISO 27005 PARA GESTIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN PARA EMPRESAS CONSULTORAS DE TI", cuyo autor es CAPCHA DA COSTA GIAN CARLOS, constato que la investigación tiene un índice de similitud de 30.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 22 de Diciembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
MENDOZA APAZA FERNANDO **DNI:** 10363032 **ORCID:** 0000-0001-7981-8291	Firmado electrónicamente por: FEMENDOZAAPA el 29-12-2022 10:52:35

Código documento Trilce: TRI - 0499008

INVESTIGA UCV