



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

**Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la
gestión de riesgos en el Sistema Integrado Judicial Supremo**

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Marquez Rodriguez, Maria de los Angeles (orcid.org/0000-0003-3792-7523)

Yarleque Aldana, Luis Miguel (orcid.org/0000-0002-0486-5277)

ASESOR:

Mg. Saboya Rios, Nemias (orcid.org/0000-0002-7166-2197)

LÍNEA DE INVESTIGACIÓN:

Auditoría y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2022

DEDICATORIA

A mi madre por apoyarme en los momentos difíciles y no dejar que me rinda. A Dios por darme la sabiduría y paciencia para resolver los problemas que se fueron generando. Y al ingeniero Nemias Saboya Rios por asesorarnos en el desarrollo de esta investigación.

Márquez Rodriguez, María

El presente trabajo está dedicado a mi familia que siempre ha sido la piedra angular en mi vida pues con su apoyo incondicional he conseguido seguir adelante en mi camino y continuar logrando mis objetivos y metas profesionales y personales que nos permiten seguir mejorando cada día.

Yarleque Aldana, Luis Miguel

AGRADECIMIENTO

A nuestros padres por apoyarnos en los momentos difíciles. A Dios por darnos la sabiduría y paciencia para resolver los problemas que se fueron generando. Al ingeniero Nemias Saboya Rios por asesorarnos en el desarrollo de esta investigación. Y al Poder Judicial por brindarnos la información necesaria para la realización de este estudio.

ÍNDICE DE CONTENIDOS

DEDICATORIA.....	ii
AGRADECIMIENTO.....	iii
ÍNDICE DE CONTENIDOS	iv
ÍNDICE DE TABLAS.....	v
ÍNDICE DE FIGURAS	vi
RESUMEN	vii
ABSTRACT	viii
I. INTRODUCCIÓN.....	1
II. MARCO TEÓRICO.....	5
III. METODOLOGÍA.....	10
3.1. Tipo y diseño de investigación	10
3.2. Variables y operacionalización	10
3.3. Población, muestra y muestreo	11
3.4. Técnicas e instrumentos de recolección de datos	11
3.5. Procedimientos.....	12
3.6. Método de análisis de datos	13
3.7. Aspectos éticos	13
IV. RESULTADOS.....	14
V. DISCUSIÓN	31
VI. CONCLUSIONES	33
VI. RECOMENDACIONES	33
REFERENCIAS.....	34
ANEXOS	36

ÍNDICE DE TABLAS

Tabla 1. Población de la Investigación	11
Tabla 2. Validez de los instrumentos.....	12
Tabla 3. Análisis descriptivos del % riesgos identificados	14
Tabla 4. Análisis descriptivos del tiempo de tratamiento de los riesgos identificados	15
Tabla 5. Análisis descriptivos del % incidencias del riesgo	16
Tabla 6. Análisis descriptivos del % riesgos tratados.....	17
Tabla 7. Análisis descriptivos del % de colaboradores que conocen los riesgos .	18
Tabla 8. Estadísticas de grupos de % riesgos identificados.....	20
Tabla 9. Estadístico de prueba para % riesgos identificados	20
Tabla 10. Rangos comparativos de la prueba de wilcoxon para el Tiempo de tratamiento de los riesgos identificados.....	22
Tabla 11. Estadísticos de prueba de Wilcoxon de Tiempo de tratamiento de los riesgos identificados.....	23
Tabla 12. Estadísticas de grupos de % incidencias del riesgo	25
Tabla 13. Estadístico de prueba para % incidencias del riesgo	25
Tabla 14. Estadísticas de grupos de % riesgos tratados.....	27
Tabla 15. Estadístico de prueba para % riesgos tratados	27
Tabla 16. Rangos comparativos de la prueba de Wilcoxon para el % de colaboradores que conocen los riesgos	29
Tabla 17. Estadísticos de prueba de Wilcoxon de % de colaboradores que conocen los riesgos.....	30

ÍNDICE DE FIGURAS

<i>Figura 1.</i> Proceso ISO/IEC 27005.....	8
<i>Figura 2.</i> Promedio de la media de % de riesgos identificados.....	14
<i>Figura 3.</i> Promedio de la media de % de riesgos identificados.....	15
<i>Figura 4.</i> Promedio de la media de % de incidencias del riesgo.....	16
<i>Figura 5.</i> Promedio de la media de % de riesgos tratados.....	17
<i>Figura 6.</i> Promedio de la media de % de colaboradores que conocen los riesgos.	18
<i>Figura 7.</i> Prueba de H. de % riesgos identificados.....	21
<i>Figura 8.</i> Prueba de H. de Tiempo de tratamiento de los riesgos identificados....	23
<i>Figura 9.</i> Prueba de H. de % incidencias del riesgo.....	25
<i>Figura 10.</i> Prueba de H. de % riesgos tratados.....	28
<i>Figura 11.</i> Prueba de H. de % de colaboradores que conocen los riesgos.....	30

RESUMEN

El estudio tuvo como finalidad conocer la influencia de un Marco de trabajo basado en el ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo; la medición se realizó por cinco indicadores: porcentaje de riesgos identificados, tiempo de tratamiento de los riesgos identificados, porcentaje de incidencias del riesgo, porcentaje de riesgos tratados y porcentaje de colaboradores que conocen los riesgos. El estudio tuvo como resultado el incremento en la identificación de los riesgos presentados en la Mesa de Partes Única de las diferentes salas supremas de justicia de la Corte Suprema, asimismo se minimizó el tiempo de respuesta y tratamiento de los riesgos identificados en el primer filtro de la Corte Suprema, finalmente la comunicación entre los servidores públicos basados en la estructura del marco de trabajo presentado obtuvo un mayor conocimiento de los riesgos, logrando la identificación rápida y la solución en un menor tiempo, de esta forma se agiliza la gestión del trámite documentario de las Mesas de Partes de la Corte Suprema. Finalmente concluimos que es fundamental implementar el marco de trabajo para la mejora de las funciones de los servidores públicos del Poder Judicial.

Palabras clave: Marco de trabajo, Sistema Integrado Judicial Supremo, ISO 27005, COBIT 2019

ABSTRACT

The purpose of the study was to know the influence of a Framework based on ISO 27005 and COBIT 2019 for risk management in the Supreme Judicial Integrated System; the measurement was carried out by five indicators: percentage of identified risks, treatment time of identified risks, percentage of risk incidents, percentage of risks treated and percentage of collaborators who are aware of the risks. The study resulted in an increase in the identification of risks presented in the Single Parties Table of the different supreme courtrooms of the Supreme Court, likewise the response time and treatment of risks identified in the first filter of the Supreme Court, finally the communication between public servants based on the structure of the framework presented obtained a greater knowledge of the risks, achieving rapid identification and solution in less time, thus speeding up the management of the documentary processing of the Parties Tables of the Supreme Court. Finally, we conclude that the implementation of the framework is essential to improve the functions of public servants in the Judiciary.

Keywords: Framework, Integrated Supreme Judicial System, ISO 27005, COBIT 2019

I. INTRODUCCIÓN

La seguridad de la información, actualmente, se puede determinar como un tema fundamental para las organizaciones, puesto que la gestión de la información es una parte esencial del gobierno corporativo y requiere una adecuada protección de los activos de información. Razón por la que se necesita utilizar el modelo de seguridad adecuado para cumplir con los requisitos y que permita asimilar el nivel de madurez de ciberseguridad. (Orellana y Álvarez, 2022)

Tanto las empresas privadas como las públicas están viviendo entornos dinámicos con el surgimiento y el cambio de TIs y la usabilidad de los datos aumenta en intensidad progresivamente. Al examinar las interrelaciones entre los procesos de su compañía y los recursos de información a los que accede, es importante examinar los nuevos riesgos que enfrenta su empresa. Esto requiere el desarrollo de un nuevo método para gestionar los riesgos que proporcionen el manejo, encontrar los riesgos que estén relacionados con los activos de información, analizarlos y encontrar formas de reducir los efectos negativos. En este tipo de escenario, tiene sentido utilizar un modelo de gestión de riesgo que sistematice estas tareas. (Zevallos, 2019)

Con el tiempo, la tecnología de la información ha evolucionado desde ofrecer soporte de transacciones hasta brindar una ventaja competitiva para el negocio. El creciente aumento del uso de TI dentro y entre las empresas ha requerido una variedad de procesos y estructuras de gobierno. En consecuencia, COBIT proporciona un entorno de trabajo integral que apoya a las industrias a conseguir sus metas, alinear sus objetivos de TI con sus objetivos comerciales, crear valor y generar ganancias en función de la implementación de procesos de administración y gobierno de TI dentro y fuera de la empresa, reduciendo el riesgo, midiendo el rendimiento de TI y gestionando los recursos disponibles de manera adecuada. (Hernández, 2019)

El poder judicial es un poder del estado peruano otorgado mediante la constitución Política del Perú, encargado de prestar el servicio de justificación social a través de sus jurisdicciones para determinar las inestabilidades y conflictos relacionados con la ley, proteger y fortalecer los derechos humanos

para alcanzar la paz pública y la seguridad jurídica, factor de desarrollo del país. Sobre la base de sus funciones es evidente que la información se convierte un recurso indispensable para el cumplimiento de sus objetivos y que por tanto una de sus principales responsabilidades debe ser la de asegurar su protección aceptando, reduciendo, evitando o transfiriendo riesgos que puedan afectar su confidencialidad, integridad y disponibilidad.

Actualmente el Sistema Integrado Judicial Supremo, no cuenta con un manual de procedimiento para la gestión de riesgos que estén basados en normas internacionales como ISO 27005 y COBIT 2019, que permitan asegurar una correcta gestión de los riesgos que se puedan presentar, como la pérdida y/o filtración de datos importantes para realizar el proceso sus actividades de justicia. Esta situación puede conllevar a tener problemas altamente perjudiciales para la institución, así como para los ciudadanos.

Esto lleva al problema general: ¿Cuál es la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo?

Así mismo, tenemos como específicos: ¿Cuál es la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en la evaluación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo?, ¿cuál es la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en el tratamiento del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo? y ¿cuál es la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en la comunicación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo?

Respecto a la justificación, Creswell (2009) describe una historia muy breve del desarrollo de métodos mixtos, incluyendo definiciones, ya que estos métodos son relativamente nuevos en la ciencia.

Justificación Metodológica:

El presente proyecto de investigación, busca seguir los pasos o lineamientos que se deben cumplir a través del marco de trabajo basado en ISO 27005 y COBIT 2019 para la Gestión de Riesgos en el Sistema Integrado Judicial Supremo. Con el desarrollo e implementación del cuestionario para cada una de las capacidades de la competencia de estudio, pueden dar soluciones futuras para investigadores, demostrando su validez y confiabilidad.

Justificación Práctica:

Este trabajo se realiza porque existe la necesidad de investigar el marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo, con el uso de los lineamientos.

Justificación Teórica:

Este estudio se realiza con el propósito de dar a conocer a todo el personal que hace uso del Sistema Integrado Judicial Supremo, los mejores instrumentos y correcto uso de la norma ISO 27005 y COBIT 2019, demostrando mejor los resultados, para ser incorporados una vez el estudio sea aceptado y aprobado.

También, se tiene como objetivo general: Identificar la influencia del marco de trabajo basado en el ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo.

Los Objetivos específicos están determinados de la siguiente manera: Estimar la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en la evaluación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo; identificar la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en el tratamiento del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo; y determinar la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en la comunicación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo.

Y como hipótesis del presente estudio, con respecto a lo general, tenemos: El marco de trabajo basado en la ISO 27005 y COBIT 2019 influye significativamente en la gestión de riesgos en el Sistema Integrado Judicial Supremo.

Así mismo, las específicas: El marco de trabajo basado en la ISO 27005 y COBIT 2019 influye significativamente en la evaluación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo; el marco de trabajo basado en la ISO 27005 y COBIT 2019 influye significativamente en el tratamiento del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo; y el marco de trabajo basado en la ISO 27005 y COBIT 2019 influye significativamente en la comunicación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo.

II. MARCO TEÓRICO

Se investigó sobre trabajos previos que apoyen de forma teórica a la presente investigación, entre las nacionales tenemos:

Abanto (2021), en su investigación titulada Modelo de gestión de riesgos de tecnologías de información para la generación de valor en el control de la corrupción de funcionarios y servidores en las municipalidades provinciales de Lambayeque, tuvo el objetivo de plantear un modelo de gobierno de riesgos de TI a los gobiernos locales de la región Lambayeque para agregar valor a la lucha contra la corrupción; el estudio es cuantitativo y experimental. Obteniendo como resultado que un MGR-TI crearía valor para frenar la corrupción entre agentes o funcionarios públicos en el gobierno provincial de la región Lambayeque; dado que accede determinar los riesgos que pueden provocar una práctica corrupta. De la misma forma, se obtuvo un MGR-TI dinámico, realista y ágil, ha sido recogido de formatos y repositorios, verificado por expertos y con buenos resultados basados en indicadores estadísticos.

Otoya (2018) en su investigación titulada Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. En diversas instituciones nacionales donde Agro Rural no es ajena, poco importa planificar sistemáticamente las actividades de planificación que se requieren por los estándares en el marco del SGSI, de acuerdo con las políticas y objetivos del SGSI. Tuvo como finalidad el llegar a conclusiones sobre el impacto del riesgo informático en la seguridad de la información en el momento de planear el desarrollo de la producción agrícola rural. En el estudio cuantitativo se usó el método hipotético deductivo de tipo básico. Como resultado se obtuvo que la importancia es 0.035 y la dependencia de la seguridad de la información con la administración de riesgos de TI llega al 44%. Esto demuestra que una buena gestión de riesgos puede conducir a una eficaz seguridad de la información, pero si hubiera una errónea administración de riesgos habría una seguridad de la información inadecuada.

Con respecto a los trabajos previos internacionales:

Fajardo (2021), en su investigación titulada *Evaluación de riesgos de seguridad de la información para la empresa Makoto S.A.S. basada en la norma ISO 27005:2018*. Tiene como problemática que no se ha evaluado los riesgos en los activos, los cuales están expuestos constantemente y son el pilar fundamental para el proceso de estructuración corporativa y de seguridad. Teniendo como objetivos específicos: efectuar una evaluación de activos y una valoración del impacto comercial y generar recomendaciones donde se evidencian hallazgos que permitan definir estrategias de gestión de riesgo. Fue un estudio cuantitativo y la población del estudio fueron los encargados del área de IT. Se obtuvo como resultado que se realizó una evaluación a los activos de información que nos permitió gestionar en el área de TI, sus procesos de tecnología, instalaciones y el factor humano que se armonizó con los objetivos estratégicos trazados por la junta, estos factores tienen el equilibrio en la cadena de seguridad de la información y de acuerdo a eso la administración de ellos dependía el nivel de aseguramiento a los activos.

Hernández (2021), en su investigación titulada *Propuesta para el mejoramiento de procesos y gestión de riesgos TI del área programación y control de la compañía EMTELCO S.A.S., basada en las buenas prácticas de ITIL 4 Y COBIT 2019*. Tuvo como finalidad presentar una propuesta de mejora de procedimientos y el gobierno de riesgos en el área de control y programación de la empresa, basada en COBIT 2019 e ITIL 4. Este trabajo posee un enfoque cualitativo y es un proyecto de tipo investigativo. Se obtuvo como resultado que se comprobó que no existe una adecuada infraestructura para implementar la propuesta, lo que indica la necesidad de una asignación adecuada por el área de gestión de TI y que los lineamientos para el gobierno de riesgos propuesto forman parte de una posible solución. Además, los resultados permiten afirmar que las prácticas del modelo del adecuado manejo de riesgos y la orientación del proyecto forman parte de una resolución factible y práctica.

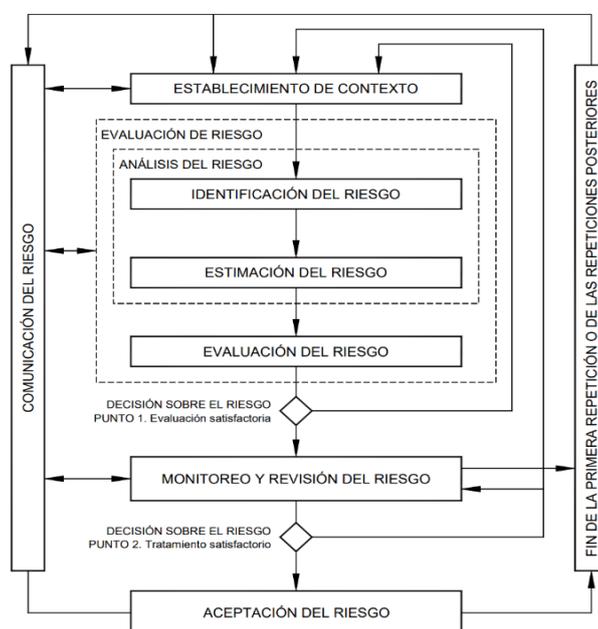
Polo (2020), en su investigación titulada *Implementación de los procesos de Gobierno de COBIT 2019 en la Dirección de Tecnologías de la Información y Comunicaciones del Ejército del Ecuador*. Tiene como problemática que no existe un proceso bien definido y documentado debido a varios factores, como la falta de rotación del personal técnico y una adecuada gestión. Teniendo como objetivo aplicar los procesos de gobierno de COBIT 2019 en la Dirección de TIC del ejército del Ecuador, permitiendo una conveniente gestión de los procesos de TI. La investigación es realizada mediante un enfoque cuantitativo. Se obtuvo como resultado que se aplicó el modelo para delimitar qué tan bien DTIC está alineado con los objetivos estratégicos de la institución y se descubrió que es un 80% consistente con los objetivos estratégicos que han tenido un impacto significativo en el área.

Navarro (2019), en su investigación titulada *Aplicación de Gestión de Riesgos Tecnológicos basada en la norma ISO/IEC 27005 en el área de base de datos y sistema operativo de la Dirección de Informática y Sistemas de la DGI*. Los sistemas que encontraba el contribuyente no estaban disponibles antes de la fecha límite del pago de impuestos, lo que provocaba interrupciones en las intervenciones comunes y demoras en el pago de impuestos. Teniendo como objetivo, para el manejo de riesgos técnicos en el área de BD y SO de la Dirección de informática y sistemas de la DGI, el implementar la norma ISO 27005 a fin de mitigar los efectos de dichos riesgos físicos, lógicos y organizacionales. Como resultado, la norma ISO 27005 adoptada brinda orientación sobre la gestión de riesgos escenario por escenario, centrándose en activos, procesos, amenazas y vulnerabilidades al analizar riesgos efectivamente, reduciendo el tiempo de ejecución, el consumo de recursos y optimizando las operaciones de reprocesamiento para evitar el aumento de amenazas. Así mismo, puede sugerir planes de recuperación global ante situaciones de riesgo.

En consideración a las bases teóricas, tenemos a las variables de investigación:

Para definir **el marco de trabajo basado en la ISO 27005 y COBIT 2019**, Moreno (2022) nos indica que fue desarrollada por el Comité Técnico Conjunto ISO JTC 1, técnicas de seguridad en la TI. La 1era edición de la ISO/IEC 27005 anula y sustituye a normas ISO anteriores, las cuales son revisiones técnicas. Establecer contexto, evaluar y manejar los riesgos, tratar y comunicar los riesgos, y el monitoreo de dichos riesgos, son actividades de la administración de riesgos en la seguridad de la información.

Figura 1. Proceso ISO 27005.



Fuente: Moreno (2022)

En la actividad de creación de contexto inicial, se recomienda que desarrolle o seleccione un punto de vista sobre la gestión de riesgos adecuado que tenga en cuenta los criterios básicos de la valoración de riesgos, impacto y criterios de tolerancia al riesgo. Además, las organizaciones cuentan con los recursos que se necesitan para poner en práctica y delimitar políticas y procedimientos, incluida la realización de evaluaciones de riesgos, el desarrollo de planes de respuesta a riesgos y la ejecución de controles seleccionados, controles de monitoreo y monitoreo de procesos de gestión de riesgos de seguridad. (Moreno, 2022)

Tal como se toman en las actividades de evaluación de riesgos, las decisiones se basan en niveles de riesgo aceptables. Por otra parte, es prudente considerar el

impacto, el potencial y la confianza en identificar y analizar riesgos. Los múltiples riesgos bajos o medios agrupados pueden tener un riesgo global mucho más alto y deben abordarse en consecuencia. Las opciones de manejo de riesgos deben seleccionarse en función del producto de la valoración de riesgos, el costo de implementarlas y sus beneficios (Moreno, 2022).

Se recomienda la especificación y desarrollo de criterios de tolerancia al riesgo, que a menudo dependen de los objetivos, las políticas y las partes interesadas de su organización. De manera similar, la comunicación de riesgos permite llegar a un consenso sobre cómo gestionar el riesgo mediante el intercambio de información entre los tomadores de decisiones y otras partes interesadas. Esta información puede incluir la gravedad, probabilidad, existencia, naturaleza y tratamiento del riesgo (Moreno, 2022).

Finalmente, se necesita un seguimiento y una revisión continuos para garantizar que la situación, la evaluación de riesgos y los resultados del tratamiento, y los planes de gestión sean relevantes para el contexto y pertinentes (Moreno, 2022).

Se define la variable: **Gestión de Riesgo** en la seguridad de la información, la cual según Moreno (2022), debería ser un proceso continuo en el que el riesgo debe abordarse utilizando planes de tratamiento para definir el contexto, evaluar el riesgo e implementar sugerencias. La gestión de riesgos examina lo que está sucediendo y sus consecuencias antes de decidir cómo proceder y cuándo realizar una reducción del riesgo para que sea más aceptable.

El adecuado manejo de riesgos en la seguridad de la información implica identificar riesgos, evaluarlos en términos de impacto y potencial de ocurrencia, comunicar y comprender el potencial y las consecuencias de estos riesgos, priorizar el manejo de riesgos y abordarlos. Disminuir las ocurrencias de riesgos, involucrar a las partes interesadas en las decisiones, informarles sobre el estado de la gestión de riesgos, monitorear la efectividad de la gestión de riesgos y monitorear y revisar regularmente los procesos de gestión de riesgos. Los empleados capacitan a los directores y toman riesgos y medidas para reducirlos (Moreno, 2022).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

En el presente trabajo se aplicó un diseño preexperimental que para Margarita Chávez Valdez et al., (2020) esto facilita el aproximarse al fenómeno que se está evaluando, tratar o impulsar al grupo para producir hipótesis, valorar 1 o más variables y estudiar sus efectos.

Con el enfoque cuantitativo y el método de la inferencia hipotética, Hernández [et al.] (2014) asegura que es un enfoque basado en la inferencia o inferencia lógica, partiendo de la parte teórica y deduciendo argumentos lógicos de ella. La hipótesis, que el investigador prueba, se llama; es el tipo aplicado para ayudar a dar solución a los problemas en cuestión.

3.2. Variables y Operacionalización

Variable Independiente:

Marco de trabajo basado en la ISO 27005 y COBIT 2019 que el Comité Técnico Conjunto ISO JTC 1, técnicas de seguridad en la TI, desarrolló anteriormente. La 1era edición de la norma ISO 27005 anula y sustituye a normas ISO anteriores, las cuales son revisiones técnicas. Establecer contexto, evaluar y manejar los riesgos, tratar y comunicar los riesgos, y el monitoreo de dichos riesgos, son actividades de gestión de riesgos en la seguridad de la información.

Variable Dependiente:

Gestión de riesgos en la seguridad de la información, la cual según Moreno (2022), debería ser un proceso continuo en el que el riesgo debe abordarse utilizando planes de tratamiento para definir el contexto, evaluar el riesgo e implementar recomendaciones y decisiones. Con el apoyo de la gestión de riesgos se puede examinar lo que está sucediendo y sus consecuencias antes de decidir cómo proceder y cuándo realizar una reducción del riesgo para que sea más aceptable.

3.3. Población, muestra y muestreo

Según Sucasaire (2022), la población se puede precisar como el conjunto de todos los elementos en los cuales se procede a analizar variables. La población tomada para la presente investigación **son todos los registros de expedientes emitidos** por el Sistema Integrado Judicial Supremo.

Otzen y Manterola (2017) afirman que se considera que una muestra representa una población si las distribuciones y valores de las diversas variables son reproducibles dentro de un margen de error predecible. La muestra de la presente investigación es de los **registros de expedientes emitidos durante un periodo de tiempo** por el Sistema Integrado Judicial Supremo.

Tabla 1. *Población de la Investigación*

Dimensiones	Indicadores	Población
Evaluación del riesgo	Porcentaje de riesgos identificados	Registros de expedientes emitidos durante un periodo de tiempo
Tratamiento del riesgo	Tiempo de tratamiento de los riesgos identificados	
	Porcentaje de incidencias del riesgo	
	Porcentaje de riesgos tratados	
Comunicación del riesgo	Porcentaje de colaboradores que conocen los riesgos	

Fuente: Elaboración propia

3.4. Técnicas e instrumentos de recolección de datos

Con respecto a la recolección de datos se usaron herramientas y técnicas de registro de gráficos observacionales, donde Carrasco (2006) se refiere a registrar o registrar datos de interés para el investigador y sus intereses, a través de publicaciones de diferentes tamaños o tapas duras denominadas notas, que sirven para registrar los datos. Se visualiza el resultado del contacto entre el observador y la realidad.

La validación de un instrumento radica en el hecho de realizar la medición de lo que corresponda. Hay 3 tipos de importancia: el valor del contenido se refiere a si la herramienta indica un atributo específico del contenido que debe medirse; la

importancia predictiva hace referencia a los procesos en los que los resultados de las pruebas de un grupo de individuos se comparan con puntajes, calificaciones u otras medidas de desempeño; y el constructivismo es un concepto unificado que combina consideraciones sustantivas y de valor en un contexto común para probar hipótesis sobre conexiones teóricas (Carhuacho et al., 2019).

3.5. Procedimientos

Cuando nos referimos al procedimiento en el desarrollo de una variable hacemos referencia a la manera en que se realiza la transformación entre la expresión final de la variable y su definición conceptual. Este estado final indica que al menos pueden realizar la función básica por la que se crearon. Para esto, también se necesita pasar por la conversión de la variante a un formato específico de la máquina de grabación, para que se puedan producir las grabaciones que la acompañan. O el evento completo, la expresión de la realidad que queremos experimentar (Cohen & Gómez, 2019).

Se le pidió a la compañía llenar fichas de registro con datos cuantitativos sobre cómo realizan la gestión de riesgos actualmente. Estas fichas se aplicaron a 50 colaboradores, con la finalidad de obtener datos para su posterior análisis. Así mismo, la valoración de la validez del instrumento fue realizada por 3 expertos que coincidieron en su aplicabilidad en este estudio. Se puede enfatizar la importancia del marco de trabajo basado en la ISO 27005 y COBIT 2019 para la mejora de la gestión de riesgos en el Sistema Integrado Judicial Supremo. Las pruebas se ejecutaron antes y después de la implementación, con lo que se deseó representar el logro de los objetivos planteados.

Tabla 2. *Validez de los instrumentos*

N°	Expertos	Grado académico	Puntaje a cada ficha de registro					
			1	2	3	4	5	6
1	Nemias Saboya	Magíster	85	85	85	85	85	85
2	Yohan Alarcón	Magíster	85	85	85	85	85	85

Fuente: Elaboración propia

3.6. Método de análisis de datos

En cuanto al momento de analizar los datos se usó fichas de registro que para Arias (2020), siempre conduce a probar una hipótesis que el investigador ha planteado previamente. Una de esas características importantes es que están estandarizados y todas las preguntas conducen a un solo objetivo.

Asimismo, para la medición de los datos se utilizará la escala de Likert que Matas (2018), la define como una herramienta psicométrica que requiere que los encuestados muestran su consentimiento o desacuerdo con un ítem. Esto se hace en una escala unidimensional ordenada. Estos instrumentos generalmente se usan con mayor frecuencia para la medición en ciencias sociales.

3.7. Aspectos éticos

Para Cohen y Gómez (2019) es esencial incorporar principios éticos básicos en el desarrollo de investigaciones en las que intervienen personas. Este principio de investigación ética es global y trasciende fronteras legales, geográficas, económicas, culturales y políticas.

Los tesisistas se comprometieron a cumplir con todos los acuerdos de confidencialidad de la empresa y de utilizar de forma responsable las referencias que han sido usadas en esta investigación. También respeta la Resolución N° 110-2022-VI-UCV del vicerrectorado de investigación de la UCV.

IV. RESULTADOS

Resultados descriptivos de la evaluación del riesgo

Resultados descriptivos del % riesgos identificados

Se logró obtener datos del primer indicador de % riesgos identificados, posteriormente a la utilización del marco de trabajo basado en la ISO 27005 y COBIT 2019 se señala una disminución del 0.131. Por otro lado, el nivel de variabilidad que se encontró en el pre-test, fue del 0.064, siendo superior al 0.044 obtenido en el post-test, además los valores mínimos y máximos consiguieron una disminución del 0.09 y 0.16 respectivamente, demostrando que el marco de trabajo, disminuye el % riesgos encontrados. (Ver tabla 3)

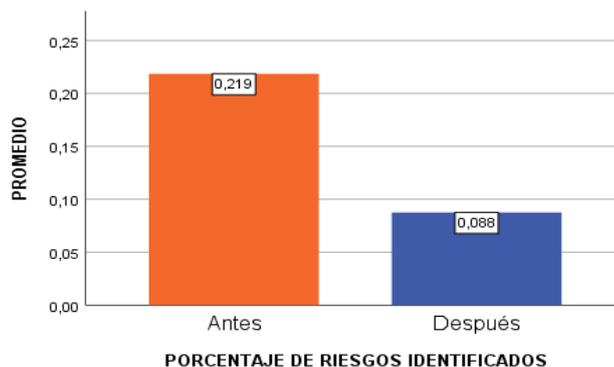
Tabla 3. Análisis descriptivos del % riesgos identificados

Estadísticos	Pre-test	Post-test
N	20	20
Media	0,2185	0,0875
Mediana	0,2300	0,0700
Moda	0,25	0,07
Desv. Desviación	0,06418	0,04471
(>)	0,09	0,00
(<)	0,33	0,17

Fuente: Elaboración propia

En la figura 2, se puede visualizar el puntaje de comparación del promedio del indicador % riesgos identificados, el pre-test consiguió un resultado del 0.22, mientras que los datos obtenidos en el post-test fue el valor del 0.88, de esta manera, se evidencia la disminución en el porcentaje de riesgos identificados.

Figura 2. Promedio de la media de % de riesgos identificados.



Resultados descriptivos del tratamiento del riesgo

Resultados descriptivos del tiempo de tratamiento de los riesgos identificados

Se logró obtener datos del Tiempo de tratamiento de los riesgos identificados, posteriormente a la utilización del marco de trabajo para la gestión de riesgos se señala una disminución del 717 del promedio. Por otro lado, el nivel de variabilidad que se encontró en el pre-test, fue del 658.8, siendo un resultado superior al 205 obtenido después del post-test, además el valor máximo disminuyó en 1560, demostrando que el marco de trabajo ayuda a decrecer el tiempo de tratamiento de los riesgos identificados. (Ver tabla 4)

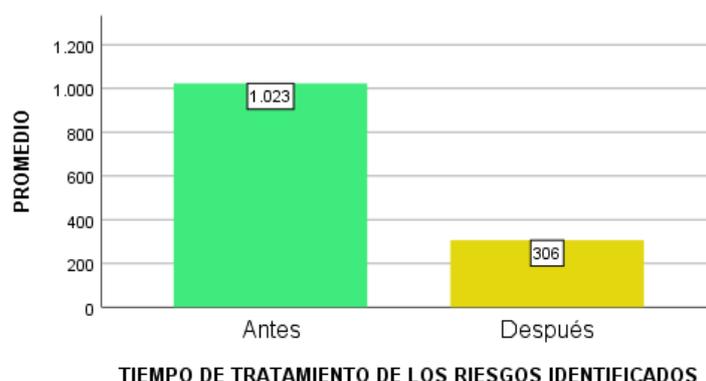
Tabla 4. Análisis descriptivos del tiempo de tratamiento de los riesgos identificados

Estadísticos	Antes	Después
N	20	20
Media	1023	306
Mediana	900	300
Moda	720	300
Desv. Desviación	658,843	205,001
Mínimo	0	0
Máximo	2160	600

Fuente: Elaboración propia

En la siguiente figura, se puede ver la comparación del promedio del tiempo de tratamiento de los riesgos identificados, el pre-test consiguió un resultado del 1023, mientras que los datos del post-test fue el valor del 306, evidenciándose la disminución en el tiempo de tratamiento de los riesgos identificados.

Figura 3. Promedio de la media de % de riesgos identificados.



Resultados descriptivos del % incidencias del riesgo

Se logró obtener datos del % incidencias del riesgo, posteriormente a la utilización del marco de trabajo para la gestión de riesgos se señala una disminución del 0.0485. Por otro lado, el nivel de variabilidad que se encontró en el pre-test, fue del 0.182, siendo superior al 0.138 obtenido en el post-test, además el valor máximo consiguió una disminución del 0.25, demostrando que el marco de trabajo, disminuye el % riesgos encontrados.

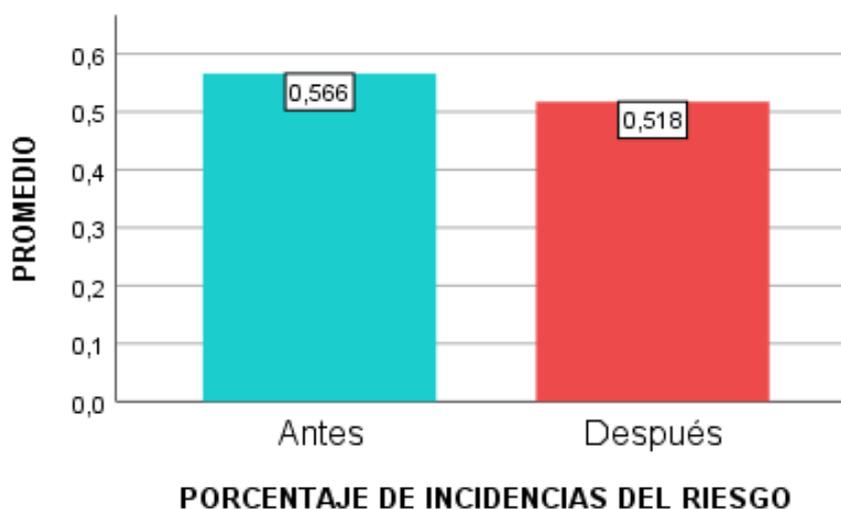
Tabla 5. Análisis descriptivos del % incidencias del riesgo

Estadísticos	Pre-test	Post-test
N	20	20
Media	0,5660	0,5175
Mediana	0,6000	0,5300
Moda	0,67	0,50
Desv. Desviación	0,18234	0,13845
(>)	0,27	0,28
(<)	1,00	0,75

Fuente: Elaboración propia

En la figura 4, se puede visualizar el puntaje de comparación del promedio del % de incidencias del riesgo, el pre-test consiguió un resultado del 0.57, mientras que los datos obtenidos en el post-test fue el valor del 0.52, de esta manera, se evidencia la disminución en el % incidencias del riesgo.

Figura 4. Promedio de la media de % de incidencias del riesgo.



Resultados descriptivos del % riesgos tratados

Se logró obtener datos del % riesgos tratados, posteriormente a la utilización del marco de trabajo para la gestión de riesgos se señala un aumento del 0.126. Por otro lado, el nivel de variabilidad que se encontró en el pre-test, fue del 0.045, siendo superior al 0.042 obtenido en el post-test, además los valores mínimos y máximos consiguieron un aumento del 0.13 y 0.14 respectivamente, demostrando que el marco de trabajo, aumenta el % riesgos tratados.

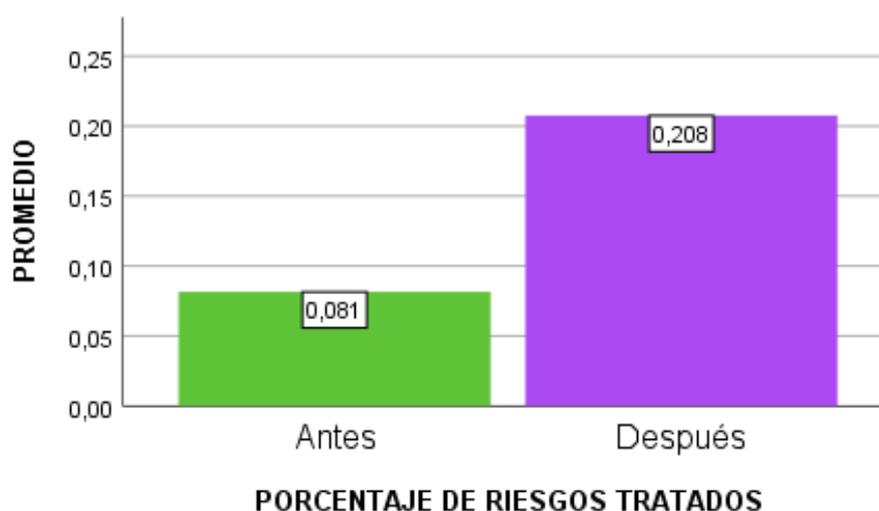
Tabla 6. Análisis descriptivos del % riesgos tratados

Estadísticos	Pre-test	Post-test
N	20	20
Media	0,0815	0,2075
Mediana	0,0800	0,2100
Moda	0,08	0,21
Desv. Desviación	0,04499	0,04191
(>)	0,00	0,13
(<)	0,17	0,31

Fuente: Elaboración propia

En la figura 5, se puede visualizar el puntaje de comparación del promedio del % de riesgos tratados, el pre-test consiguió un resultado del 0.08, mientras que los datos obtenidos en el post-test fue el valor del 0.21, de esta manera, se evidencia el aumento en el % de riesgos tratados.

Figura 5. Promedio de la media de % de riesgos tratados.



Resultados descriptivos de la comunicación del riesgo

Resultados descriptivos del % de colaboradores que conocen los riesgos

Se logró obtener datos del % de colaboradores que conocen los riesgos, posteriormente a la utilización del marco de trabajo para la gestión de riesgos se señala un aumento del 0.068. Por otro lado, el nivel de variabilidad que se encontró en el pre-test, fue del 0.109, siendo superior al 0.061 obtenido en el post-test, además el valor mínimo consiguió un aumento del 0.20 respectivamente, demostrando que el marco de trabajo, aumenta el % de colaboradores que conocen los riesgos.

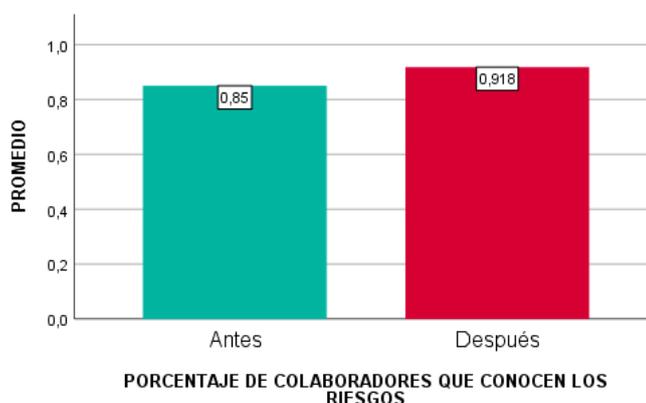
Tabla 7. Análisis descriptivos del % de colaboradores que conocen los riesgos

Estadísticos	Pre-test	Post-test
N	20	20
Media	0,8500	0,9180
Mediana	0,8850	0,9150
Moda	0,80	0,90
Desv. Desviación	0,10897	0,06101
(>)	0,60	0,80
(<)	1,00	1,00

Fuente: Elaboración propia

En la siguiente figura, se puede visualizar el puntaje de comparación del promedio del % de colaboradores que conocen los riesgos, el pre-test consiguió un resultado del 0.85, mientras que los datos obtenidos en el post-test fue el valor del 0.92, de esta manera, se evidencia el aumento en el % colaboradores que conocen los riesgos.

Figura 6. Promedio de la media de % de colaboradores que conocen los riesgos.



Contraste de hipótesis de Evaluación del riesgo

Contraste de hipótesis de Porcentaje de riesgos identificados

$H_0: \mu_1 = \mu_2$: El número de incidencias registradas antes de aplicar el Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo, no redujo después de la implementación del mismo.

$H_a: \mu_1 \neq \mu_2$: El número de incidencias registradas antes de la aplicación Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo, redujo después de la implementación del mismo.

Nivel de confianza: 0,95

Se acepta la H_a si sig sea mayor a α

Se rechaza la Hipótesis Nula si sig sea menor a α

El análisis relacionó el estadístico de prueba paramétrica T para las muestras pareadas porque la variable de prueba logró el supuesto de normalidad.

$$t = \frac{\sum_1^n \frac{x_{i1} - x_{i2}}{n}}{\sqrt{\frac{\sum_1^n (d_1 - \bar{X}_d)^2}{n-1}}}$$
$$\frac{\sqrt{\frac{\sum_1^n (d_1 - \bar{X}_d)^2}{n-1}}}{\sqrt{n}}$$

\bar{X}_d = Media aritmética de las diferencias

S_d = Desv. estándar de las diferencias

n = Número de sujetos de la muestra

El resultado descriptivo del porcentaje de riesgos identificados 2 veces (antes-Despues) se muestra en la tabla 8, donde el producto evidencia que las frecuencias pre-test fueron en promedio ($\bar{x} = 8.0580$), resultado que es menor al pos-test ($\bar{x} = 11.3435$). lo que involucra que una vez aplicado el Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo el porcentaje aumento significativamente de manera

que las incidencias en la organización están siendo mejor atendidas y controladas ya que se puede identificar con mayor agudeza los riesgos presentados día a día.

Tabla 8. Estadísticas de grupos de % riesgos identificados

% riesgos identificados	Promedio	N	Desv. Desviación	Desv. Error promedio
Pre - test	8,0580	20	4,42337	0,98910
Postest	11,3435	20	4,58758	1,02581

Fuente: Elaboración propia

De igual modo, se muestra los resultados de inferencia de la prueba paramétrica T para muestras relacionadas donde el estadístico de prueba $\text{sig} = 0.000 < \alpha = 0.05$ en la tabla 9, el resultado demuestra la existencia de diferencias significativas entre los promedios de las incidencias de ambos momentos (pretest-Postes) en 3.28 incidencias. Un resultado que conduce a la investigación positiva para el investigador que respalda la hipótesis presentada en el trabajo de investigación.

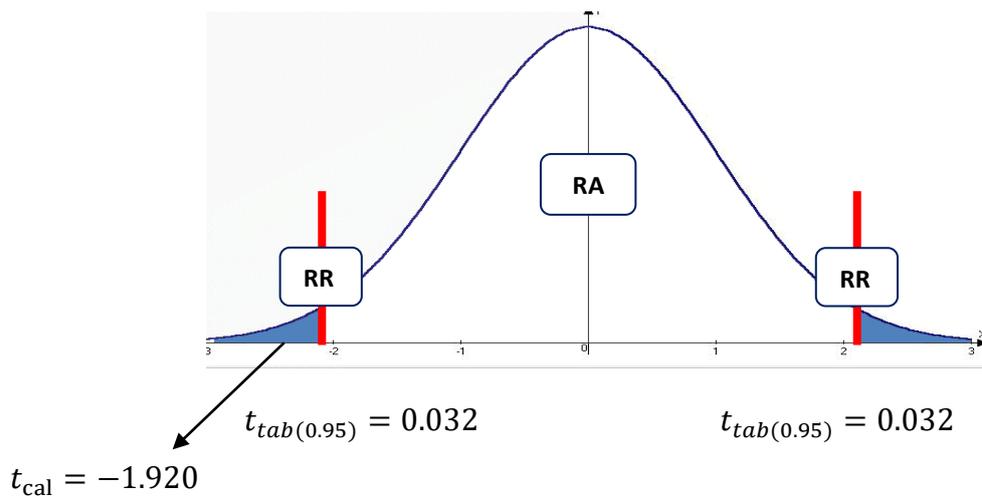
Tabla 9. Estadístico de prueba para % riesgos identificados

Indicador	Diferencias emparejadas					T	gl	Sig.
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza				
				Inferior	Superior			
Pre-Postest	-3.285	7,651	1,711	-6,866	0,295	-1,920	19	0,07

Fuente: Elaboración propia

Para determinar el contraste, fue fundamental utilizar una prueba distribuida como $t_{tab}(1-\alpha/2; n-1)$. En este caso, se reemplazó los valores y se obtuvo $t_{tab}(0,95; 19) = 0.032$, el cual se mostró en la campana de Gaus a continuación.

Figura 7. Prueba de H. de % riesgos identificados.



Fuente: Elaboración propia

Se indica que el resultado de Z_{cal} cayó dentro de la región de rechazo, de forma que se rechaza a la hipótesis nula a favor de la alternativa, en resumen existe suficiente evidencia estadística para manifestar que el Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo contribuyó favorablemente en la Porcentaje de riesgos identificados del Poder Judicial con un 95% de confianza.

Contraste de hipótesis de Tratamiento del riesgo

Contraste de hipótesis de Tiempo de tratamiento de los riesgos identificados

H_0 : $Me^1 = Me^2$: El Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo no contribuyo en la reducción de Tiempo de tratamiento de los riesgos identificados en el Poder Judicial.

H_a : $Me^1 < Me^2$: El Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo contribuyo en la reducción de Tiempo de tratamiento de los riesgos identificados en el Poder Judicial.

Estadística de prueba:

El análisis relacionó el estadístico de prueba t para muestras pareadas porque la variable de prueba logró el supuesto de normalidad.

$$T = \text{Min}[T(+), T(-)]$$

Donde establece que T se adapta una distribución normal, por consiguiente se debe usar la fórmula:

$$Z = \frac{T - n(n + 1)/4}{\sqrt{n(n + 1)(2n + 1)/24}}$$

El resultado descriptivo comparando los 2 momentos de estudio del indicador Tiempo de tratamiento de los riesgos identificados (antes - después), indica que en promedio el rango negativo fue de ($\bar{x} = 0,00$), resultado inferior al positivo ($\bar{x} = 4,00$). Es decir, los resultados del pos-test fueron inferiores en 7 casos, demostrando de esta manera que el Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo ayudó a reducir el tiempo de tratamiento generado en el Poder Judicial, y ningún caso no fueron favorables. Asimismo, la suma de rango inclina el resultado a favor de estudio (ver tabla 10).

Tabla 10. Rangos comparativos de la prueba de wilcoxon para el Tiempo de tratamiento de los riesgos identificados

Tiempo de tratamiento de los riesgos identificados		N	Rango promedio	Suma de rangos
Pretest - Postest	(-)	0	0,00	0,00
	(+)	7	4,00	28,00
	Empates	13		
	Total	20		

Fuente: Elaboración propia

Por otra parte, la tabla 11 muestra los resultados del contratos de la prueba de wilcoxon a través de una aproximación de la normal Z, donde el sig = 0.000 < α =

0.05, demostrando de esta manera que los datos respecto a las reincidencias al antes y el después presentan diferencia significativa favorables al estudio.

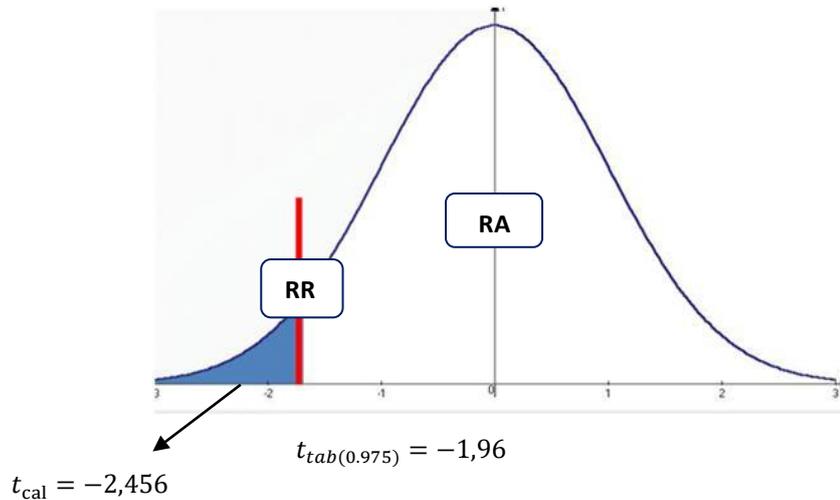
Tabla 11. Estadísticos de prueba de Wilcoxon de Tiempo de tratamiento de los riesgos identificados

Prueba	VELOCIDAD DE DESCARGA
Z	-2,456 ^b
Sig. asintótica(bilateral)	0,014

Fuente: Elaboración propia

Para determinar contrastes hipotéticos, fue fundamental utilizar una prueba distribuida como $Z_{tab}(1-\alpha/2)$. En este caso, se reemplazó los valores y se obtuvo $z_{tab}(0,975) = 1.96$. Por otro lado, el resultado de decisión se relacionó con el valor de $Z_{cal} = -2.456$ y se mostró en la campana de Gaus el que se enseña a continuación.

Figura 8. Prueba de H. de Tiempo de tratamiento de los riesgos identificados.



Fuente: Elaboración propia

Se indica que el resultado de Z_{cal} cayó dentro de la RR, de manera que se rechaza al H_0 a favor de la H_a , concluyendo que el Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo contribuyó en la reducción Tiempo de tratamiento de los riesgos identificados del Poder Judicial con un 95% de confianza.

Contraste de hipótesis de Tratamiento del riesgo

Contraste de hipótesis Porcentaje de incidencias de los riesgo

Ho: $\mu^1 = \mu^2$: El número de incidencias registradas antes de la aplicación Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo, no redujo después de la implementación del mismo

Ha: $\mu^1 \neq \mu^2$: El número de incidencias registradas antes de la aplicación Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo, redujo después de la implementación del mismo

Nivel de confianza: 0,95

Se rechaza la H. Nula si sig sea menor a α

Se acepta la H_a si sig sea mayor a α

La investigación relacionó el estadístico de prueba t para muestras pareadas porque la variable de prueba logró el supuesto de normalidad.

$$t = \frac{\frac{\sum_1^n x_{i1} - x_{i2}}{n}}{\frac{\sqrt{\frac{\sum_1^n (d_1 - \bar{X}_d)^2}{n-1}}}{\sqrt{n}}}$$

\bar{X}_d = Media aritmética de las diferencias

S_d = Desv. estándar de las diferencias

n = Número de sujetos de la muestra

El resultado descriptivo del porcentaje de riesgos identificados en los dos momentos (antes-Despues) se presenta en la tabla 12, donde los resultados evidencia que en promedio las incidencias en el pretest fueron ($\bar{x} = 16,7515$), resultado que es menor al postest ($\bar{x} = 6,9925$). Lo que implica que después de la aplicación Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la

gestión de riesgos en el Sistema Integrado Judicial Supremo el porcentaje aumento significativamente de manera que las incidencias en la organización están siendo mejor atendidas y controladas ya que se puede identificar con mayor agudeza los riesgos presentados día a día.

Tabla 12. Estadísticas de grupos de % incidencias del riesgo

% incidencias del riesgo	Promedio	N	Desv. Desviación	Desv. Error Promedio
Pretest	16,7515	20	10,30600	2,30449
Posttest	6,9925	20	7,83529	1,75203

Fuente: Elaboración propia

Además, la tabla 13 muestra los resultados de inferencia de la prueba t para muestras relacionadas donde el estadístico de prueba sig = 0.000 < α = 0.05, resultado que demuestra que existen diferencias significativas entre los promedios de las incidencias de ambos momentos (pretest - posttest) en 9,759 incidencias.

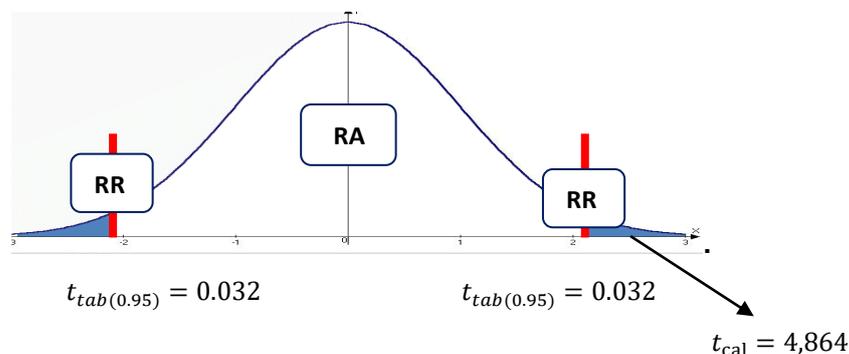
Tabla 13. Estadístico de prueba para % incidencias del riesgo

Indicador	Diferencias emparejadas					T	gl	Sig. (bilateral)
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza				
				Inferior	Superior			
Pre-Post	9,759	7,972	2,006	5,559	13,958	4,864	19	0,00

Fuente: Elaboración propia

Para determinar contrastes hipotéticos, la prueba aproximada de normalidad se da como $t_{tab}(1-\alpha/2; n - 1)$. En esta ocasión, se reemplazó los valores y se obtuvo como resultados $t_{tab}(0,95; 19) = 0.032$. Además, el resultado de decisión se mostró en la campana de Gaus el que se enseña a continuación.

Figura 9. Prueba de H. de % incidencias del riesgo.



Fuente: Elaboración propia

Se indica que el Zcal cayó dentro de RR, de forma que se rechaza la hipótesis nula a favor de la alternativa, concluyendo que el Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo contribuyó en el Porcentaje de incidencias de los riesgos en la organización con un 95% de confianza.

Contraste de hipótesis de Tratamiento del riesgo

Contraste de hipótesis de Porcentaje de riesgos tratados

Ho: $\mu^1 = \mu^2$: El número de incidencias registradas antes de la aplicación Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo, no redujo después de la implementación del mismo

Ha: $\mu^1 \neq \mu^2$: El número de incidencias registradas antes de la aplicación Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo, redujo después de la implementación del mismo.

Nivel de confianza: 0,95

Se rechaza la Hipótesis Nula si sig sea menor a α

Se acepta la H_a si sig sea mayor a α

El análisis relacionó el estadístico de prueba t para muestras pareadas porque la variable de prueba logró el supuesto de normalidad.

$$t = \frac{\sum_1^n \frac{x_{i1} - x_{i2}}{n}}{\sqrt{\frac{\sum_1^n (d_1 - \bar{X}_d)^2}{n-1}}}$$
$$\sqrt{n}$$

\bar{X}_d = Media aritmética de las diferencias

S_d = Desv. estándar de las diferencias

n = Número de sujetos de la muestra

El resultado descriptivo del porcentaje de riesgos identificados en los dos momentos (antes-Despues) se presenta en la tabla 14, donde los resultados evidencia que en promedio las incidencias en el pretest fueron ($\bar{x} = 14,1270$), resultado que es menor al pos-test ($\bar{x} = 40,6945$). lo que involucra la aplicación del Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo el porcentaje aumento significativamente de manera que las incidencias en la organización están siendo mejor atendidas y controladas ya que se puede identificar con mayor agudeza los riesgos presentados día a día.

Tabla 14. Estadísticas de grupos de % riesgos tratados

% riesgos tratados	Promedio	N	Desv. Desviación	Desv. Error Promedio
Pre - test	14,1270	20	8,23129	1,94057
Postest	40,6945	20	9,49443	2,12302

Fuente: Elaboración propia

Así mismo, la tabla 15 demuestra los resultados de inferencia de la prueba t para muestras relacionadas donde el estadístico de prueba sig = 0.000 < $\alpha = 0.05$, resultado que demuestra que existen diferencias significativas entre los promedios de las incidencias de ambos momentos (pretest- Postes) en -26,56 incidencias. Resultado que conlleva a que la investigación sea favorable al investigador apoyando la hipótesis planteada en el estudio.

Tabla 15. Estadístico de prueba para % riesgos tratados

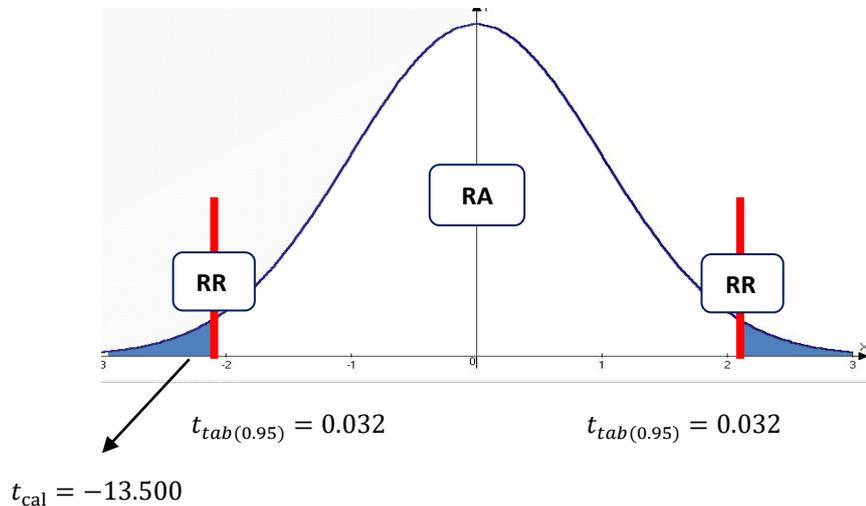
Indicador	Diferencias emparejadas					T	gl	Sig. (bilateral)
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza				
				Inferior	Superior			
Pre-Post	-26.56	8,800	1,9678	-30,686	-22,448	-13,500	19	0,00

Fuente: Elaboración propia

Para determinar contrastes hipotéticos, fue fundamental utilizar una prueba distribuida como $t_{tab}(1-\alpha/2; n - 1)$. En este caso, se reemplazó los valores y se

obtuvo $t_{tab}(0,95; 19) = 0.03$, el cual se mostró en la campana de Gaus a continuación.

Figura 10. Prueba de H. de % riesgos tratados.



Fuente: Elaboración propia

Se señala que el resultado de Z_{cal} cayó dentro de la RR, debido a lo cual se rechaza al H_0 a favor de la H_a , finalizando que el Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo contribuyo en el Porcentaje de riesgos tratados del riesgo en la organización con un 95% de confianza.

Contraste de hipótesis de Comunicación del riesgo

Contraste de hipótesis de Porcentaje de colaboradores que conocen los riesgos

$H_0: Me^1 = Me^2$: El Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo no contribuyo en la reducción de Tiempo de tratamiento de los riesgos identificados en el Poder Judicial.

$H_a: Me^1 < Me^2$: El Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo contribuyo en la reducción de Tiempo de tratamiento de los riesgos identificados en el Poder Judicial.

Nivel de confianza: 0,95

Se acepta la H_a si sig sea mayor a α

Se rechaza la Hipótesis Nula si sig sea menor a α

La investigación examinó el estadístico de prueba t para muestras pareadas porque la variable de prueba logró el supuesto de normalidad.

$$T = \text{Min}[T(+), T(-)]$$

Donde establece que T se adapta a una distribución normal por lo que se debe usar la fórmula:

$$Z = \frac{T - n(n + 1)/4}{\sqrt{n(n + 1)(2n + 1)/24}}$$

El resultado descriptivo relacionando los dos momentos del análisis del Tiempo de tratamiento de los riesgos identificados (antes-Despues), señala que en promedio el rango negativo fue de ($\bar{x} = 6.00$), resultado que es inferior al positivo ($\bar{x} = 0,00$). Lo que involucra que los resultados del postest fueron inferiores en 9 casos, evidenciando de esta manera que el Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo ayudó a reducir el tiempo de tratamiento generado en el Poder Judicial, y ningún caso no fueron propicios. De igual modo, la suma de rango inclina el resultado a favor de estudio (ver tabla 16).

Tabla 16. Rangos comparativos de la prueba de Wilcoxon para el % de colaboradores que conocen los riesgos

% colaboradores que conocen los riesgos		N	Rango promedio	Suma de rangos
Pretest – Postest	(-)	11	6,00	66,00
	(+)	0	0,00	0,00
	Empates	9		
	Total	20		

Fuente: Elaboración propia

Asimismo, la tabla 17 demuestra los resultados de la evaluación de Wilcoxon a través de una aproximación de la normal Z, donde el sig = 0.000 < $\alpha = 0.05$, demostrando de esta manera que los datos respecto a las reincidencias al antes y el después presentan diferencia significativa favorables al estudio.

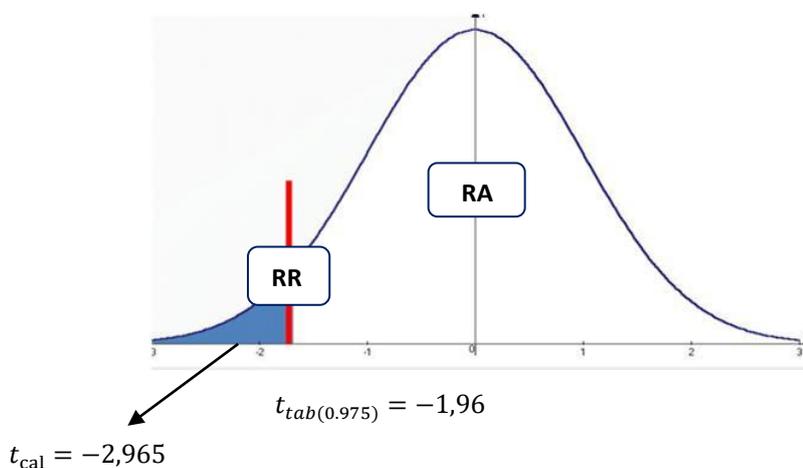
Tabla 17. Estadístico de prueba de Wilcoxon de % de colaboradores que conocen los riesgos

Prueba	VELOCIDAD DE DESCARGA
Z	-2,965 ^b
Sig. asintótica	0,03

Fuente: Elaboración propia

Para determinar contrastes hipotéticos, fue fundamental utilizar una prueba distribuida como $Z_{tab}(1-\alpha/2)$. Se reemplazó los valores y se obtuvo $z_{tab}(0,975) = 1.96$. Por otra parte, el resultado de decisión se relacionó con el valor de $Z_{cal} = -2.965$ el cual se mostró en la campana de Gaus.

Figura 11. Prueba de H. de % de colaboradores que conocen los riesgos.



Fuente: Elaboración propia

Se indica que el resultado de Z_{cal} cayó dentro de la RR, debido a lo cual se rechaza al H_0 a favor de la H_a , finalizando que el Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo contribuyó favorablemente en la reducción de las reincidencias del Poder Judicial con un 95% de confianza.

V. DISCUSIÓN

El propósito de este análisis fue conocer el impacto de un marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo para el Poder Judicial, se alcanzó como resultado valor ($p_value = 0.000 < \alpha = 0.05$), por medio de la evaluación no paramétrica de Wilcoxon. Lo que señala que colaboró propiciamente al tratamiento de los riesgos presentados ante la Corte Suprema de Justicia. Dicho de otro modo, gracias al marco de trabajo y al orden que este conlleva se logró una mejor identificación de los riesgos en los expedientes judiciales, mayor atención por parte del servidor público respecto de sus funciones y acortar la brecha de tiempo que estos demandan para la solución de los mismos; se logró tomar decisiones acertadas a corto tiempo identificando de manera fácil algún intento de sabotear o inferir al error de los servidores públicos al realizar sus funciones. Es factible el rechazo de la Hipótesis Nula a favor de la alterna, lo que claramente manifiesta que el modelo influyó significativamente a toma de decisiones frente a los riesgos presentados en la Corte Suprema de Justicia. Nuestros resultados corroboran el estudio de Abanto (2021) dado que permite determinar los riesgos que pueden provocar una práctica corrupta.

De la misma forma, se obtuvo un MGR-TI dinámico, realista y ágil, ha sido recogido de formatos y repositorios, verificado por expertos y con buenos resultados basados en indicadores estadísticos. Esto implica que para poder tener una buena estrategia ante riesgos institucionales es preciso tener un buen sistema que apoye en las decisiones, en tal caso un correo marco de trabajo que facilite el correcto funcionamiento de las actividades diarias.

De la misma manera Otoyá (2018) demuestra que una buena gestión de riesgos puede conducir a una eficaz seguridad de la información, pero si hubiera una inadecuada administración de riesgos habría una mala seguridad de la información. Por lo que se puede indicar, tomando en cuenta las observaciones previas, que la influencia de un Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo, es necesario y sumamente importante para el correcto progreso de las funciones

laborales de la Corte Suprema del Poder Judicial maximizando la atención y el reconocimiento de riesgos eventuales y frecuentes, así como también, minimizando el tiempo de respuesta y tratamiento de los riesgos identificados en el primer filtro de la Corte Suprema correspondiente a la Mesa de Partes Única.

VI. CONCLUSIONES

Con respecto a las conclusiones en los informes de investigación con enfoque cuantitativo y apoyados en el sistema estadístico SPSS versión 26:

Se determina que el marco de trabajo influye en gran medida ya que se demostró que maximiza el conocimiento frente a los tratamientos de los riesgos y minimiza el tiempo de respuesta frente al tratamiento de los riesgos identificados.

Se determina que la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en la evaluación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo aporta gran manejo de los riesgos identificados en el primer filtro de las Salas Supremas.

Se logro identificar con ayuda del marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo, los puntos vulnerables y de mayor atención para el tratamiento y conocimiento de los riesgos en el uso de expedientes judiciales.

Se determino que influye en gran medida el uso del marco de trabajo basado en la ISO 27005 y COBIT 2019 en la comunicación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo, toda vez que el trámite documentario se agilizó en el último estudio realizado con el sistema SPSS versión 26.

VI. RECOMENDACIONES

1.- Se recomienda mayor investigación o ampliar los estudios realizados con mayor rango de tiempos. Ya que los procesos son cambiantes y las nuevas y métodos de realizar engaños a la entidad publica como es el poder judicial están latentes día con día.

2.- Se recomienda ampliar el estudio a las diferentes cortes superiores de la región Lima, tales como Lima Sur, Lima Norte, Lima Este y Lima Oeste, replicando el uso del marco de trabajo en estudio para evaluar el alcance de las mejoras o requerimientos que se logren obtener.

3.- Se recomienda un mayor uso de variables, con lo que se agudice el estudio y lograr replicar esta investigación a los diferentes departamentos de la nación

REFERENCIAS

- ABANTO, R., 2021. *Modelo de gestión de riesgos de tecnologías de información para la generación de valor en el control de la corrupción de funcionarios y servidores en las municipalidades provinciales de la región de Lambayeque* [en línea]. S.I.: Universidad Católica Santo Toribio de Mogrovejo. Disponible en https://tesis.usat.edu.pe/bitstream/20.500.12423/3832/1/TM_AbantoOrtizRogerGustavo.pdf
- CARRASCO, S., 2006. *Metodología de la investigación científica*. 1. Lima: s.n. ISBN 9972-34-242-5
- CRESWELL, J.W. (2009). *Research design: Qualitative, quantitative, and mixed approaches*. Thousand Oaks, CA: Sage
- 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* [en línea]. S.I.: Universidad Católica de Colombia. Disponible en: [https://repository.ucatolica.edu.co/bitstream/10983/27059/1/EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.pdf](https://repository.ucatolica.edu.co/bitstream/10983/27059/1/EVALUACIÓN_DE_RIESGOS_DE_SEGURIDAD_DE_LA_INFORMACIÓN.pdf)
- FONSECA, O., 2019. *Modelo de un sistema de gestión de seguridad de la información en la organización GEOCONSULT CS* [en línea]. S.I.: Universidad EAN. Disponible en: <https://repository.ean.edu.co/bitstream/handle/10882/9521/FonsecaOmar2019.pdf;jsessionid=470DCC9D6A72E7BA542717B167D3A87F?sequence=1>
- HERNÁNDEZ, A., 2021. *Propuesta para el mejoramiento de procesos y gestión de riesgos ti del área programación y control de la compañía EMTELCO S.A.S., basada en las buenas prácticas de ITIL 4 Y COBIT 2019* [en línea]. S.I.: Universidad Santo Tomás. Disponible en: <https://repository.usta.edu.co/bitstream/handle/11634/34928/2021andreshernandez.pdf?sequence=1>
- HERNÁNDEZ, J., 2019. COBIT , una metodología que genera valor en las empresas. *Universidad Piloto de Colombia* [en línea], pp. 1-8. Disponible en: <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4677/00004999.pdf?sequence=1&isAllowed=y>
- HERNÁNDEZ, R., FERNÁNDEZ, C. y BAPTISTA, P., 2014. *Metodología de la investigación*. 6. México: s.n. ISBN 9781456223960
- MARGARITA CHÁVEZ VALDEZ, S., ESPARZA DEL VILLAR, A. y MORENO, L.R., 2020. Pre-experimental and quasi-experimental designs applied to social sciences and education. *Enseñanza e Investigación* [en línea], vol. 2, no. 2, pp. 167-178. Disponible en: https://www.researchgate.net/profile/Oscar-Villar/publication/347441005_DISENOS_PREEXPERIMENTALES_Y_CUASI_EXPERIMENTALES_APLICADOS_A_LAS_CIENCIAS_SOCIALES_Y_LA_EDUCACION/links/5fdbfb4592851c13fe9596df/DISENOS-PREEXPERIMENTALES-Y-CUASIEXPERIMENTALES-APLICAD

- MORENO, F., 2022. Proyecto de Norma Técnica Colombiana NTC-ISO 27005. [en línea], Disponible en: file:///C:/Users/Miguel/Downloads/topaz.info-iso-27005-espanol-pr_e0ded52f75ffe8e6f96d54e8a76fd3bd.pdf
- NAVARRO, J., 2019. *Aplicación de Gestión de Riesgos Tecnológicos basada en la norma ISO/IEC 27005 en el área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI*. [en línea]. S.I.: Universidad Nacional de Ingeniería de Nicaragua. Disponible en: <https://core.ac.uk/download/pdf/288314661.pdf>
- ORELLANA, X. y ÁLVAREZ, M., 2022. Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019. [en línea], vol. 7, no. 3, pp. 706-723. DOI 10.23857/pc.v7i3.3758. Disponible en: <https://polodelconocimiento.com/ojs/index.php/es/article/download/3758/8667>
- OTOYA, M., 2018. *Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017* [en línea]. S.I.: Universidad César Vallejo. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/16120/Otoya_VM.pdf?sequence=4&isAllowed=y
- OTZEN, T. y MANTEROLA, C., 2017. Sampling techniques on a population study. *International Journal of Morphology* [en línea], vol. 35, no. 1, pp. 227-232. ISSN 0717-9502. DOI 10.4067/S0717-95022017000100037. Disponible en: <https://scielo.conicyt.cl/pdf/ijmorphol/v35n1/art37.pdf>
- POLO, J., 2020. *Implementación de los procesos de Gobierno de COBIT 2019 en la Dirección de Tecnologías de la Información y Comunicaciones del Ejército del Ecuador* [en línea]. S.I.: Universidad de las Fuerzas Armadas de Ecuador. Disponible en: <http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/22560/T-ESPE-043874.PDF?sequence=1&isAllowed=y>
- SUCASAIRE, J., 2022. *Orientación para la selección y el cálculo del tamaño de la muestra de investigación* [en línea]. 1. Lima: Depósito Legal en la Biblioteca Nacional del Perú. ISBN 9786120075470. Disponible en: http://repositorio.concytec.gob.pe/bitstream/20.500.12390/3096/1/Orientacion_es_para_seleccion_y_calculo_del_tamaño_de_muestra_de_investigacion.pdf
- TICONA, O., 2022. *Modelo de seguridad de la información basado en la normativa ISO/IEC 27001 :2013 para mitigar los riesgos de los activos de la información en la entidad privada Severox Perú SAC, Arequipa, 2021* [en línea]. S.I.: Universidad César Vallejo. Disponible en: http://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47102/Gutierrez_RS-SD.pdf?sequence=1&isAllowed=y
- ZEVALLLOS, M., 2019. Artículo de revisión Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte Information security risk management model: A state of the art review. [en línea], vol. 2, no. 1, pp. 43-60. ISSN: 2617-2003. Disponible en: <http://dx.doi.org/10.15381/rpcs.v2i2.17103>

ANEXOS

Anexo 01: Matriz de Consistencia

TÍTULO	MARCO DE TRABAJO BASADO EN LA ISO 27005 Y COBIT 2019 PARA LA GESTIÓN DE RIESGOS EN EL SISTEMA INTEGRADO JUDICIAL SUPREMO				
PROBLEMA	OBJETIVO	HIPÓTESIS	OPERACIONALIZACIÓN DE VARIABLES		DISEÑO METODOLÓGICO
Problema general	Objetivo general	Hipótesis general	VARIABLE 1: Independiente	Dimensiones e Indicadores	Método
¿Cuál es la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo?	Determinar la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo.	El marco de trabajo basado en la ISO 27005 y COBIT 2019 influye significativamente en la gestión de riesgos en el Sistema Integrado Judicial Supremo.	Marco de trabajo basado en la ISO 27005 y COBIT 2019	<ul style="list-style-type: none"> • Evaluación del riesgo - Porcentaje de riesgos identificados • Tratamiento del riesgo - Tiempo de tratamiento de los riesgos identificados - Porcentaje de incidencias de los riesgos - Porcentaje de riesgos tratados • Comunicación del riesgo - Porcentaje de colaboradores que conocen los riesgos 	<p style="text-align: center;">Enfoque: Cuantitativo</p> <p style="text-align: center;">Tipo de investigación: Aplicada.</p> <p style="text-align: center;">Diseño: Pre-experimental</p> <p style="text-align: center;">Técnicas: Fichas</p> <p style="text-align: center;">Instrumento de recaudación de datos: Cuestionario</p> <p style="text-align: center;">Población: Registros de expedientes emitidos</p> <p style="text-align: center;">Muestra: Registros de expedientes emitidos durante un periodo de tiempo</p>
Problemas específicos	Objetivos específicos	Hipótesis específicas	VARIABLE 2: Dependiente		
<p>¿Cuál es la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en la evaluación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo?</p> <p>¿Cuál es la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en el tratamiento del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo?</p> <p>¿Cuál es la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en la comunicación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo?</p>	<p>Inferir la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en la evaluación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo.</p> <p>Identificar la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en el tratamiento del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo.</p> <p>Establecer la influencia del marco de trabajo basado en la ISO 27005 y COBIT 2019 en la comunicación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo.</p>	<p>El marco de trabajo basado en la ISO 27005 y COBIT 2019 influye significativamente en la evaluación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo.</p> <p>El marco de trabajo basado en la ISO 27005 y COBIT 2019 influye significativamente en el tratamiento del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo.</p> <p>El marco de trabajo basado en la ISO 27005 y COBIT 2019 influye significativamente en la comunicación del riesgo para la gestión de riesgos en el Sistema Integrado Judicial Supremo.</p>	Gestión de riesgos		

ANEXO 02: INSTRUMENTOS DE INVESTIGACIÓN PRE-TEST

FICHA DE REGISTRO DEL PORCENTAJE DE RIESGOS IDENTIFICADOS

Instrucción: La ficha se llenará con los respectivos datos almacenados en la base de datos del sistema multiplataforma que se implementará en la institución. Así mismo, los datos serán extraídos con el respectivo permiso de los administradores de la Corte Suprema de Justicia de la República.

FICHA DE REGISTRO			
Autor	Márquez Rodríguez, María		Tipo de Prueba
	Yarleque Aldana, Luis Miguel		
Empresa	Corte Suprema de Justicia de la República		
Variable	Marco de Trabajo basado en la ISO 27005 y COBIT 2019		
Dimensión	Evaluación del Riesgo		
Fecha de Inicio	02/09/2022	Fecha de Cierre	29/09/2022

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Porcentaje de Riesgos Identificados	Porcentaje de expedientes en los que se encontró riesgos	Observación	Porcentaje	$\%RI = \frac{RI}{ER} \times 100$

N°	Fecha	Cantidad de Expedientes con Riesgos (RI)	Cantidad de Expedientes Revisados (ER)	% de Riesgos Identificados (%RI)
1	02/09/2022	4	21	0.19
2	05/09/2022	3	15	0.20
3	06/09/2022	4	15	0.27
4	07/09/2022	3	14	0.21
5	08/09/2022	3	16	0.19
6	09/09/2022	4	12	0.33
7	12/09/2022	4	16	0.25
8	13/09/2022	1	10	0.10
9	14/09/2022	3	13	0.23
10	15/09/2022	3	12	0.25
11	16/09/2022	3	15	0.20
12	19/09/2022	4	17	0.24
13	20/09/2022	3	9	0.33
14	21/09/2022	1	11	0.09
15	22/09/2022	3	12	0.25
16	23/09/2022	1	9	0.11
17	26/09/2022	4	16	0.25
18	27/09/2022	3	12	0.25
19	28/09/2022	3	13	0.23
20	29/09/2022	3	15	0.20



FICHA DE REGISTRO DEL TIEMPO DE TRATAMIENTO DE RIESGOS IDENTIFICADOS

Instrucción: La ficha se llenará con los respectivos datos almacenados en la base de datos del sistema multiplataforma que se implementará en la institución. Así mismo, los datos serán extraídos con el respectivo permiso de los administradores de la Corte Suprema de Justicia de la República.

FICHA DE REGISTRO			
Autor	Márquez Rodríguez, María	Tipo de Prueba	Pre Test
	Yarleque Aldana, Luis Miguel		
Empresa	Corte Suprema de Justicia de la República		
Variable	Marco de Trabajo basado en la ISO 27005 y COBIT 2019		
Dimensión	Tratamiento del Riesgo		
Fecha de Inicio	02/09/2022	Fecha de Cierre	29/09/2022

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Tiempo de Tratamiento de Riesgos Identificados	Tiempo aproximado en que dura el tratamiento de un riesgo	Observación	Tiempo	$TTRI = RI \times TTR$

N°	Fecha	Cantidad de Expedientes con Riesgo (RI)	Cantidad de Tiempo en que Tratan un Riesgo (TTR)	Tiempo de Tratamiento de Riesgos Identificados (TTRI)
1	02/09/2022	4	8	1920
2	05/09/2022	3	4	720
3	06/09/2022	4	8	1920
4	07/09/2022	3	5	900
5	08/09/2022	3	5	900
6	09/09/2022	4	8	1920
7	12/09/2022	4	7	1680
8	13/09/2022	1	0	0
9	14/09/2022	3	4	720
10	15/09/2022	3	4	720
11	16/09/2022	3	4	720
12	19/09/2022	4	7	1680
13	20/09/2022	3	5	900
14	21/09/2022	1	0	0
15	22/09/2022	3	4	720
16	23/09/2022	1	0	0
17	26/09/2022	4	9	2160
18	27/09/2022	3	6	1080
19	28/09/2022	3	5	900
20	29/09/2022	3	5	900



FICHA DE REGISTRO DEL PORCENTAJE DE INCIDENCIAS DE LOS RIESGOS

Instrucción: La ficha se llenará con los respectivos datos almacenados en la base de datos del sistema multiplataforma que se implementará en la institución. Así mismo, los datos serán extraídos con el respectivo permiso de los administradores de la Corte Suprema de Justicia de la República.

FICHA DE REGISTRO				
Autor	Márquez Rodríguez, María		Tipo de Prueba	Pre Test
	Yarleque Aldana, Luis Miguel			
Empresa	Corte Suprema de Justicia de la República			
Variable	Marco de Trabajo basado en la ISO 27005 y COBIT 2019			
Dimensión	Tratamiento del Riesgo			
Fecha de Inicio	02/09/2022	Fecha de Cierre	29/09/2022	

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Porcentaje de Incidencias de los Riesgos	Porcentaje de expedientes que tienen mayor probabilidad de tener riesgos	Observación	Porcentaje	$\%IR = \frac{RR}{ER} \times 100$

N°	Fecha	Cantidad de Expedientes con Riesgos Repetitivos (RR)	Cantidad de Expedientes Revisados (ER)	% de Incidencias de Riesgos (%IR)
1	02/09/2022	7	21	0.33
2	05/09/2022	9	15	0.60
3	06/09/2022	10	15	0.67
4	07/09/2022	4	14	0.29
5	08/09/2022	8	16	0.50
6	09/09/2022	6	12	0.50
7	12/09/2022	9	16	0.56
8	13/09/2022	7	10	0.70
9	14/09/2022	8	13	0.62
10	15/09/2022	5	12	0.42
11	16/09/2022	9	15	0.60
12	19/09/2022	6	17	0.35
13	20/09/2022	7	9	0.78
14	21/09/2022	8	11	0.73
15	22/09/2022	8	12	0.67
16	23/09/2022	9	9	1.00
17	26/09/2022	7	16	0.44
18	27/09/2022	8	12	0.67
19	28/09/2022	8	13	0.62
20	29/09/2022	4	15	0.27



FICHA DE REGISTRO DEL PORCENTAJE DE RIESGOS TRATADOS

Instrucción: La ficha se llenará con los respectivos datos almacenados en la base de datos del sistema multiplataforma que se implementará en la institución. Así mismo, los datos serán extraídos con el respectivo permiso de los administradores de la Corte Suprema de Justicia de la República.

FICHA DE REGISTRO			
Autor	Márquez Rodríguez, María	Tipo de Prueba	Pre Test
	Yarleque Aldana, Luis Miguel		
Empresa	Corte Suprema de Justicia de la República		
Variable	Marco de Trabajo basado en la ISO 27005 y COBIT 2019		
Dimensión	Tratamiento del Riesgo		
Fecha de Inicio	02/09/2022	Fecha de Cierre	29/09/2022

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Porcentaje de Riesgos Tratados	Porcentaje de expedientes con riesgos tratados a tiempo	Observación	Porcentaje	$\%RT = \frac{ET}{ER} \times 100$

N°	Fecha	Cantidad de Expedientes Tratados (ET)	Cantidad de Expedientes Revisados (ER)	% de Riesgos Tratados (%RT)
1	02/09/2022	2	21	0.10
2	05/09/2022	1	15	0.07
3	06/09/2022	2	15	0.13
4	07/09/2022	1	14	0.07
5	08/09/2022	1	16	0.06
6	09/09/2022	2	12	0.17
7	12/09/2022	2	16	0.13
8	13/09/2022	0	10	0.00
9	14/09/2022	1	13	0.08
10	15/09/2022	1	12	0.08
11	16/09/2022	1	15	0.07
12	19/09/2022	2	17	0.12
13	20/09/2022	1	9	0.11
14	21/09/2022	0	11	0.00
15	22/09/2022	1	12	0.08
16	23/09/2022	0	9	0.00
17	26/09/2022	2	16	0.13
18	27/09/2022	1	12	0.08
19	28/09/2022	1	13	0.08
20	29/09/2022	1	15	0.07



FICHA DE REGISTRO DEL PORCENTAJE DE COLABORADORES QUE CONOCEN LOS RIESGOS

Instrucción: La ficha se llenará con los respectivos datos almacenados en la base de datos del sistema multiplataforma que se implementará en la institución. Así mismo, los datos serán extraídos con el respectivo permiso de los administradores de la Corte Suprema de Justicia de la República.

FICHA DE REGISTRO			
Autor	Márquez Rodríguez, María	Tipo de Prueba	Pre Test
	Yarleque Aldana, Luis Miguel		
Empresa	Corte Suprema de Justicia de la República		
Variable	Marco de Trabajo basado en la ISO 27005 y COBIT 2019		
Dimensión	Comunicación del Riesgo		
Fecha de Inicio	02/09/2022	Fecha de Cierre	29/09/2022

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Porcentaje de Colaboradores que Conocen los Riesgos	Porcentaje de colaboradores que saben identificar los riesgos	Observación	Porcentaje	$\%CCR = \frac{CCR}{TC} \times 100$

N°	Fecha	Cantidad de Colaboradores que Conocen los Riesgos (CCR)	Cantidad Total de Colaboradores (TC)	% de Colaboradores que Conocen los Riesgos (%CCR)
1	02/09/2022	8	10	0.80
2	05/09/2022	9	10	0.90
3	06/09/2022	8	10	0.80
4	07/09/2022	10	15	0.67
5	08/09/2022	9	15	0.60
6	09/09/2022	12	15	0.80
7	12/09/2022	9	10	0.90
8	13/09/2022	10	10	1.00
9	14/09/2022	10	10	1.00
10	15/09/2022	9	10	0.90
11	16/09/2022	14	15	0.93
12	19/09/2022	12	15	0.80
13	20/09/2022	7	10	0.70
14	21/09/2022	8	10	0.80
15	22/09/2022	10	10	1.00
16	23/09/2022	9	10	0.90
17	26/09/2022	9	10	0.90
18	27/09/2022	13	15	0.87
19	28/09/2022	12	15	0.80
20	29/09/2022	14	15	0.93



ANEXO 03: INSTRUMENTOS DE INVESTIGACIÓN POST-TEST

FICHA DE REGISTRO DEL PORCENTAJE DE RIESGOS IDENTIFICADOS

Instrucción: La ficha se llenará con los respectivos datos almacenados en la base de datos del sistema multiplataforma que se implementará en la institución. Así mismo, los datos serán extraídos con el respectivo permiso de los administradores de la Corte Suprema de Justicia de la República.

FICHA DE REGISTRO			
Autor	Márquez Rodríguez, María	Tipo de Prueba	Post Test
	Yarleque Aldana, Luis Miguel		
Empresa	Corte Suprema de Justicia de la República		
Variable	Marco de Trabajo basado en la ISO 27005 y COBIT 2019		
Dimensión	Evaluación del Riesgo		
Fecha de Inicio	03/10/2022	Fecha de Cierre	03/11/2022

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Porcentaje de Riesgos Identificados	Porcentaje de expedientes en los que se encontró riesgos	Observación	Porcentaje	$\%RI = \frac{RI}{ER} \times 100$

N°	Fecha	Cantidad de Expedientes con Riesgos (RI)	Cantidad de Expedientes Revisados (ER)	% de Riesgos Identificados (%RI)
1	03/10/2022	2	18	0.11
2	04/10/2022	1	14	0.07
3	05/10/2022	2	16	0.13
4	06/10/2022	2	14	0.14
5	10/10/2022	1	15	0.07
6	11/10/2022	1	14	0.07
7	12/10/2022	1	17	0.06
8	13/10/2022	0	9	0.00
9	14/10/2022	2	15	0.13
10	17/10/2022	1	14	0.07
11	18/10/2022	2	15	0.13
12	19/10/2022	2	13	0.15
13	20/10/2022	1	15	0.07
14	21/10/2022	1	11	0.09
15	24/10/2022	1	14	0.07
16	25/10/2022	2	12	0.17
17	26/10/2022	0	14	0.00
18	27/10/2022	1	13	0.08
19	28/10/2022	1	15	0.07
20	03/11/2022	1	14	0.07



FICHA DE REGISTRO DEL TIEMPO DE TRATAMIENTO DE RIESGOS IDENTIFICADOS

Instrucción: La ficha se llenará con los respectivos datos almacenados en la base de datos del sistema multiplataforma que se implementará en la institución. Así mismo, los datos serán extraídos con el respectivo permiso de los administradores de la Corte Suprema de Justicia de la República.

FICHA DE REGISTRO			
Autor	Márquez Rodríguez, María		Tipo de Prueba
	Yarleque Aldana, Luis Miguel		
Empresa	Corte Suprema de Justicia de la República		
Variable	Marco de Trabajo basado en la ISO 27005 y COBIT 2019		
Dimensión	Tratamiento del Riesgo		
Fecha de Inicio	03/10/2022	Fecha de Cierre	03/11/2022

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Tiempo de Tratamiento de Riesgos Identificados	Tiempo aproximado en que dura el tratamiento de un riesgo	Observación	Tiempo	$TTRI = RI \times TTR$

N°	Fecha	Cantidad de Expedientes con Riesgo (RI)	Cantidad de Tiempo en que Tratan un Riesgo (TTR)	Tiempo de Tratamiento de Riesgos Identificados (TTRI)
1	03/10/2022	2	5	600
2	04/10/2022	1	4	240
3	05/10/2022	2	5	600
4	06/10/2022	2	5	600
5	10/10/2022	1	5	300
6	11/10/2022	1	5	300
7	12/10/2022	1	4	240
8	13/10/2022	0	0	0
9	14/10/2022	2	4	480
10	17/10/2022	1	4	240
11	18/10/2022	2	4	480
12	19/10/2022	2	5	600
13	20/10/2022	1	5	300
14	21/10/2022	1	0	0
15	24/10/2022	1	4	240
16	25/10/2022	2	0	0
17	26/10/2022	0	6	0
18	27/10/2022	1	5	300
19	28/10/2022	1	5	300
20	03/11/2022	1	5	300



FICHA DE REGISTRO DEL PORCENTAJE DE INCIDENCIAS DE LOS RIESGOS

Instrucción: La ficha se llenará con los respectivos datos almacenados en la base de datos del sistema multiplataforma que se implementará en la institución. Así mismo, los datos serán extraídos con el respectivo permiso de los administradores de la Corte Suprema de Justicia de la República.

FICHA DE REGISTRO				
Autor		Márquez Rodríguez, María	Tipo de Prueba	Post Test
		Yarleque Aldana, Luis Miguel		
Empresa		Corte Suprema de Justicia de la República		
Variable		Marco de Trabajo basado en la ISO 27005 y COBIT 2019		
Dimensión		Tratamiento del Riesgo		
Fecha de Inicio		03/10/2022	Fecha de Cierre	
			03/11/2022	
Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Porcentaje de Incidencias de los Riesgos	Porcentaje de expedientes que tienen mayor probabilidad de tener riesgos	Observación	Porcentaje	$\%IR = \frac{RR}{ER} \times 100$
N°	Fecha	Cantidad de Expedientes con Riesgos Repetitivos (RR)	Cantidad de Expedientes Revisados (ER)	% de Incidencias de Riesgos (%IR)
1	03/10/2022	5	18	0.28
2	04/10/2022	7	14	0.50
3	05/10/2022	9	16	0.56
4	06/10/2022	5	14	0.36
5	10/10/2022	8	15	0.53
6	11/10/2022	6	14	0.43
7	12/10/2022	9	17	0.53
8	13/10/2022	6	9	0.67
9	14/10/2022	5	15	0.33
10	17/10/2022	8	14	0.57
11	18/10/2022	9	15	0.60
12	19/10/2022	6	13	0.46
13	20/10/2022	10	15	0.67
14	21/10/2022	8	11	0.73
15	24/10/2022	8	14	0.57
16	25/10/2022	9	12	0.75
17	26/10/2022	7	14	0.50
18	27/10/2022	8	13	0.62
19	28/10/2022	6	15	0.40
20	03/11/2022	4	14	0.29



FICHA DE REGISTRO DEL PORCENTAJE DE RIESGOS TRATADOS

Instrucción: La ficha se llenará con los respectivos datos almacenados en la base de datos del sistema multiplataforma que se implementará en la institución. Así mismo, los datos serán extraídos con el respectivo permiso de los administradores de la Corte Suprema de Justicia de la República.

FICHA DE REGISTRO				
Autor		Márquez Rodríguez, María	Tipo de Prueba	Post Test
		Yarleque Aldana, Luis Miguel		
Empresa		Corte Suprema de Justicia de la República		
Variable		Marco de Trabajo basado en la ISO 27005 y COBIT 2019		
Dimensión		Tratamiento del Riesgo		
Fecha de Inicio		03/10/2022	Fecha de Cierre	03/11/2022
Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Porcentaje de Riesgos Tratados	Porcentaje de expedientes con riesgos tratados a tiempo	Observación	Porcentaje	$\%RT = \frac{ET}{ER} \times 100$
N°	Fecha	Cantidad de Expedientes Tratados (ET)	Cantidad de Expedientes Revisados (ER)	% de Riesgos Tratados (%RT)
1	03/10/2022	5	18	0.28
2	04/10/2022	3	14	0.21
3	05/10/2022	4	16	0.25
4	06/10/2022	3	14	0.21
5	10/10/2022	2	15	0.13
6	11/10/2022	3	14	0.21
7	12/10/2022	3	17	0.18
8	13/10/2022	2	9	0.22
9	14/10/2022	3	15	0.20
10	17/10/2022	3	14	0.21
11	18/10/2022	3	15	0.20
12	19/10/2022	3	13	0.23
13	20/10/2022	2	15	0.13
14	21/10/2022	2	11	0.18
15	24/10/2022	3	14	0.21
16	25/10/2022	2	12	0.17
17	26/10/2022	3	14	0.21
18	27/10/2022	4	13	0.31
19	28/10/2022	3	15	0.20
20	03/11/2022	3	14	0.21



FICHA DE REGISTRO DEL PORCENTAJE DE COLABORADORES QUE CONOCEN LOS RIESGOS

Instrucción: La ficha se llenará con los respectivos datos almacenados en la base de datos del sistema multiplataforma que se implementará en la institución. Así mismo, los datos serán extraídos con el respectivo permiso de los administradores de la Corte Suprema de Justicia de la República.

FICHA DE REGISTRO				
Autor		Márquez Rodriguez, María	Tipo de Prueba	Post Test
		Yarleque Aldana, Luis Miguel		
Empresa		Corte Suprema de Justicia de la República		
Variable		Marco de Trabajo basado en la ISO 27005 y COBIT 2019		
Dimensión		Comunicación del Riesgo		
Fecha de Inicio		03/10/2022	Fecha de Cierre	
			03/11/2022	
Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Porcentaje de Colaboradores que Conocen los Riesgos	Porcentaje de colaboradores que saben identificar los riesgos	Observación	Porcentaje	$\%CCR = \frac{CCR}{TC} \times 100$
N°	Fecha	Cantidad de Colaboradores que Conocen los Riesgos (CCR)	Cantidad Total de Colaboradores (TC)	% de Colaboradores que Conocen los Riesgos (%CCR)
1	03/10/2022	9	10	0.90
2	04/10/2022	10	10	1.00
3	05/10/2022	9	10	0.90
4	06/10/2022	14	15	0.93
5	10/10/2022	13	15	0.87
6	11/10/2022	13	15	0.87
7	12/10/2022	10	10	1.00
8	13/10/2022	10	10	1.00
9	14/10/2022	10	10	1.00
10	17/10/2022	9	10	0.90
11	18/10/2022	14	15	0.93
12	19/10/2022	14	15	0.93
13	20/10/2022	8	10	0.80
14	21/10/2022	8	10	0.80
15	24/10/2022	10	10	1.00
16	25/10/2022	9	10	0.90
17	26/10/2022	9	10	0.90
18	27/10/2022	14	15	0.93
19	28/10/2022	13	15	0.87
20	03/11/2022	14	15	0.93

ANEXO 04: VALIDACIÓN DE EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	indicador: porcentaje de riesgos identificados	Si	No	Si	No	Si	No	
1	$\%RI = \frac{RI}{ER} \times 100$	X		X		X		
	indicador: tiempo de los riesgos identificados	Si	No	Si	No	Si	No	
2	$TTRI = RI \times TTR$	X		X		X		
	indicador: porcentaje de incidencias de los riesgos	Si	No	Si	No	Si	No	
3	$\%IR = \frac{RR}{ER} \times 100$	X		X		X		
	indicador: porcentaje de riesgos tratados	Si	No	Si	No	Si	No	
4	$\%RT = \frac{ET}{ER} \times 100$	X		X		X		
	indicador: porcentaje de colaboradores que conocen los riesgos	Si	No	Si	No	Si	No	
5	$\%CCR = \frac{CCR}{TC} \times 100$	X		X		X		

Observaciones (precisar si hay suficiencia): _____

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

Especialidad del validador:

15 de julio

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



Mgtr. Nemias Saboya Ríos
DNI: 42001721

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	indicador: porcentaje de riesgos identificados	Si	No	Si	No	Si	No	
1	$\%RI = \frac{RI}{ER} \times 100$	X		X		X		
	indicador: tiempo de los riesgos identificados	Si	No	Si	No	Si	No	
2	$TTRI = RI \times TTR$	X		X		X		
	indicador: porcentaje de incidencias de los riesgos	Si	No	Si	No	Si	No	
3	$\%IR = \frac{RR}{ER} \times 100$	X		X		X		
	indicador: porcentaje de riesgos tratados	Si	No	Si	No	Si	No	
4	$\%RT = \frac{ET}{ER} \times 100$	X		X		X		
	indicador: porcentaje de colaboradores que conocen los riesgos	Si	No	Si	No	Si	No	
5	$\%CCR = \frac{CCR}{TC} \times 100$	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



15 de julio

Mgtr. Yohan Roy Alarcón Cajas
DNI: 46189705

TABLA DE VALIDACIÓN PARA EL EXPERTO: PORCENTAJE DE RIESGOS IDENTIFICADOS

TESIS: Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo	Fecha 15/07/2022
--	----------------------------

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

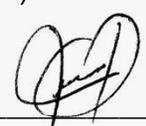
INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
1. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
4. Organización	Existe una organización lógica.					X
5. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
6. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
7. Consistencia	Está basado en aspectos teóricos y científicos.					X
8. Coherencia	En los datos respecto al indicador.					X
9. Metodología	Responde al propósito de investigación.					X
10. Pertenencia	El instrumento es adecuado al tipo de investigación.					x
Promedio Total		85				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

El instrumento puede ser aplicado, tal como está elaborado (x)

El instrumento debe ser mejorado antes de ser aplicado ()

III. FIRMA DEL EXPERTO



Mgtr. Nemias Saboya Rios



TABLA DE VALIDACIÓN PARA EL EXPERTO: TIEMPO DE TRATAMIENTO DE LOS RIESGOS IDENTIFICADOS

TESIS: Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo	Fecha 15/07/2022
--	----------------------------

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

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
1. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
4. Organización	Existe una organización lógica.					X
5. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
6. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
7. Consistencia	Está basado en aspectos teóricos y científicos.					X
8. Coherencia	En los datos respecto al indicador.					X
9. Metodología	Responde al propósito de investigación.					X
10. Pertenencia	El instrumento es adecuado al tipo de investigación.					X
Promedio Total		85				
Sugerencias						

II. OPCIÓN DE APLICABILIDAD

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

III. FIRMA DEL EXPERTO



Mgtr. Nemias Saboya Rios



TABLA DE VALIDACIÓN PARA EL EXPERTO: PORCENTAJE DE INCIDENCIAS DE LOS RIESGOS

TESIS: Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo	Fecha 15/07/2022
--	----------------------------

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

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
1. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
4. Organización	Existe una organización lógica.					X
5. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
6. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
7. Consistencia	Está basado en aspectos teóricos y científicos.					X
8. Coherencia	En los datos respecto al indicador.					X
9. Metodología	Responde al propósito de investigación.					X
10. Pertenencia	El instrumento es adecuado al tipo de investigación.					X
Promedio Total		85				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

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

III. FIRMA DEL EXPERTO



Mgtr. Nemias Saboya Rios

TABLA DE VALIDACIÓN PARA EL EXPERTO: PORCENTAJE DE RIESGOS TRATADOS

TESIS: Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo	Fecha 15/07/2022
--	----------------------------

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

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
11. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
12. Objetividad	Está expresado en conducta observable.					X
13. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
14. Organización	Existe una organización lógica.					X
15. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
16. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
17. Consistencia	Está basado en aspectos teóricos y científicos.					X
18. Coherencia	En los datos respecto al indicador.					X
19. Metodología	Responde al propósito de investigación.					X
20. Pertenencia	El instrumento es adecuado al tipo de investigación.					X
Promedio Total		85				
Sugerencias						

II. OPCIÓN DE APLICABILIDAD

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

III. FIRMA DEL EXPERTO


Mgtr. Nemias Saboya Rios



TABLA DE VALIDACIÓN PARA EL EXPERTO: PORCENTAJE DE COLABORADORES QUE CONOCEN LOS RIESGOS

TESIS: Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo	Fecha 15/07/2022
--	----------------------------

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

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
21. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
22. Objetividad	Está expresado en conducta observable.					X
23. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
24. Organización	Existe una organización lógica.					X
25. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
26. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
27. Consistencia	Está basado en aspectos teóricos y científicos.					X
28. Coherencia	En los datos respecto al indicador.					X
29. Metodología	Responde al propósito de investigación.					X
30. PERTENENCIA	El instrumento es adecuado al tipo de investigación.					X
Promedio Total		85				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

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

III. FIRMA DEL EXPERTO



Mgtr. Nemias Saboya Ríos

TABLA DE VALIDACIÓN PARA EL EXPERTO: PORCENTAJE DE RIESGOS IDENTIFICADOS

TESIS: Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo	Fecha 15/07/2022
--	----------------------------

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

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
11. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
12. Objetividad	Está expresado en conducta observable.					X
13. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
14. Organización	Existe una organización lógica.					X
15. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
16. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
17. Consistencia	Está basado en aspectos teóricos y científicos.					X
18. Coherencia	En los datos respecto al indicador.					X
19. Metodología	Responde al propósito de investigación.					X
20. Pertenencia	El instrumento es adecuado al tipo de investigación.					x
Promedio Total		85				
Sugerencias						

II. OPCIÓN DE APLICABILIDAD

El instrumento puede ser aplicado, tal como está elaborado (x)

El instrumento debe ser mejorado antes de ser aplicado ()

III. FIRMA DEL EXPERTO


Mgtr. Nemias Saboya Rios



TABLA DE VALIDACIÓN PARA EL EXPERTO: TIEMPO DE TRATAMIENTO DE LOS RIESGOS IDENTIFICADOS

TESIS: Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo	Fecha 15/07/2022
--	----------------------------

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

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
11. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
12. Objetividad	Está expresado en conducta observable.					X
13. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
14. Organización	Existe una organización lógica.					X
15. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
16. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
17. Consistencia	Está basado en aspectos teóricos y científicos.					X
18. Coherencia	En los datos respecto al indicador.					X
19. Metodología	Responde al propósito de investigación.					X
20. Pertenencia	El instrumento es adecuado al tipo de investigación.					X
Promedio Total		85				
Sugerencias						

II. OPCIÓN DE APLICABILIDAD

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

III. FIRMA DEL EXPERTO



Mgtr. Yohan Roy Alarcón Cajas



TABLA DE VALIDACIÓN PARA EL EXPERTO: PORCENTAJE DE INCIDENCIAS DE LOS RIESGOS

TESIS: Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo	Fecha 15/07/2022
--	----------------------------

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

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
31. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
32. Objetividad	Está expresado en conducta observable.					X
33. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
34. Organización	Existe una organización lógica.					X
35. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
36. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
37. Consistencia	Está basado en aspectos teóricos y científicos.					X
38. Coherencia	En los datos respecto al indicador.					X
39. Metodología	Responde al propósito de investigación.					X
40. Pertenencia	El instrumento es adecuado al tipo de investigación.					X
Promedio Total		85				
Sugerencias						

II. OPCIÓN DE APLICABILIDAD

El instrumento puede ser aplicado, tal como está elaborado (x)

El instrumento debe ser mejorado antes de ser aplicado ()

III. FIRMA DEL EXPERTO



Mgtr. Yohan Roy Alarcón Cajas



TABLA DE VALIDACIÓN PARA EL EXPERTO: PORCENTAJE DE RIESGOS TRATADOS

TESIS: Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo	Fecha 15/07/2022
--	----------------------------

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

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
41. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
42. Objetividad	Está expresado en conducta observable.					X
43. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
44. Organización	Existe una organización lógica.					X
45. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
46. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
47. Consistencia	Está basado en aspectos teóricos y científicos.					X
48. Coherencia	En los datos respecto al indicador.					X
49. Metodología	Responde al propósito de investigación.					X
50. Pertenencia	El instrumento es adecuado al tipo de investigación.					X
Promedio Total		85				
Sugerencias						

II. OPCIÓN DE APLICABILIDAD

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

III. FIRMA DEL EXPERTO

Mgtr. Yohan Roy Alarcón Cajas



TABLA DE VALIDACIÓN PARA EL EXPERTO: PORCENTAJE DE COLABORADORES QUE CONOCEN LOS RIESGOS

TESIS: Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo	Fecha 15/07/2022
--	----------------------------

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

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
51. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
52. Objetividad	Está expresado en conducta observable.					X
53. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
54. Organización	Existe una organización lógica.					X
55. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
56. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
57. Consistencia	Está basado en aspectos teóricos y científicos.					X
58. Coherencia	En los datos respecto al indicador.					X
59. Metodología	Responde al propósito de investigación.					X
60. PERTENENCIA	El instrumento es adecuado al tipo de investigación.					X
Promedio Total		85				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

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

III. FIRMA DEL EXPERTO



Mgtr. Yohan Roy Alarcón Cajas

ANEXO 05: MARCO DE TRABAJO PARA LA GESTIÓN DE RIESGOS

Según Sandoval y Pernaletе (2014) la construcción de un marco de trabajo consta de 3 etapas: investigación, construcción y evaluación. Para la construcción del marco de trabajo de gestión de riesgos en la seguridad de la información de la Corte Suprema de Justicia, se realizaron las siguientes etapas:

Figura 1. Construcción de Marco de Trabajo



Fuente: Elaboración propia

1. INVESTIGACIÓN

Según lo definido por Sandoval y Pernaletе (2014), la investigación fue la primera etapa que se realizó para la construcción del marco de trabajo para la gestión de riesgos en la seguridad de la información de la Corte Suprema de Justicia, y en ella se recopiló información sobre modelos de referencia para la construcción del marco de trabajo y se especificaron los elementos que se necesitan para la construcción de dicho marco de trabajo.

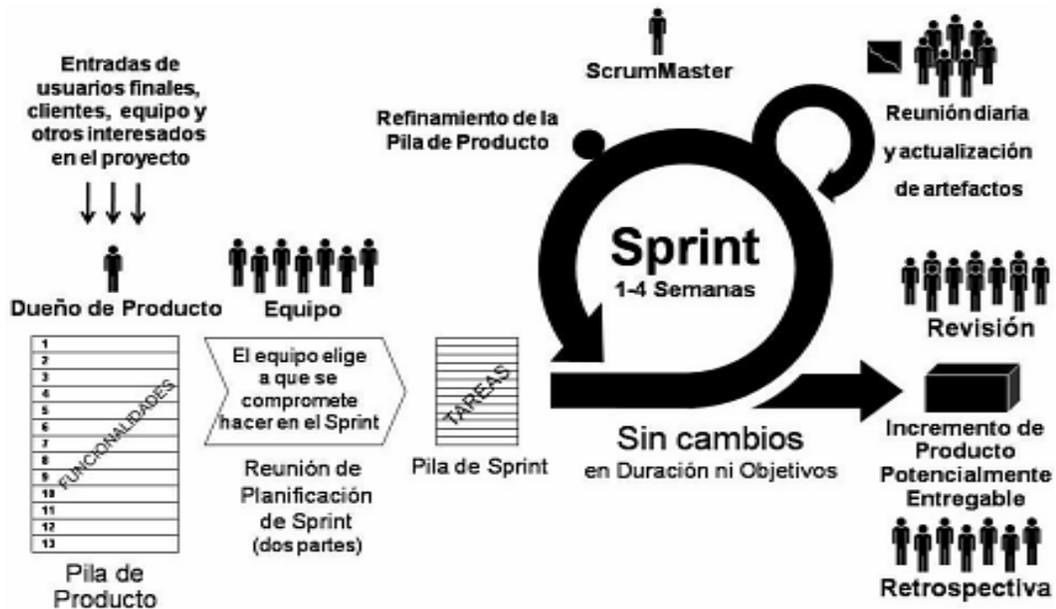
1.1. MODELOS DE REFERENCIA

El primer modelo que se pudo encontrar fue el marco de trabajo SCRUM, del cual se pudo entender que un framework necesita actores que puedan realizar los pasos que contiene el marco de trabajo. Además, cada actor tiene un rol, el cual describe todas las funciones que realiza dicho actor. También, en SCRUM, se habla de entregables que se presentan como los resultados de



cada ciclo de trabajo y que deben mostrarse a los interesados en el proyecto. Según Mariño y Alfonso (2014), el marco de trabajo SCRUM es fundamental para el desarrollo de proyectos y se estructura en ciclos de trabajo llamados Sprints, los cuales son iteraciones de 1 a 4 semanas y uno comienza cuando otro termina.

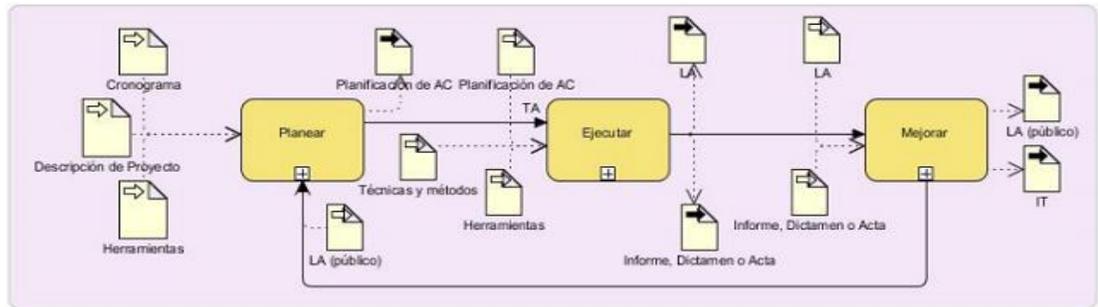
Figura 2. Framework SCRUM



Fuente: Información Básica de Scrum

Asimismo, se encontró el marco de trabajo para la gestión de actividades de calidad, del cual se pudo entender que un framework contiene etapas y pasos que deben seguirse para cumplir con el objetivo del marco de trabajo. En este sentido, Marin, Trujillo y Buedo (2018) realizaron un marco de trabajo para la gestión de actividades de calidad, el cual sugiere un enfoque a procesos sustentado sobre el Ciclo de Deming, permitiendo, de considerarse necesario, el mejoramiento continuo de las técnicas a utilizar y la inclusión de nuevas actividades a partir de lecciones aprendidas.

Figura 3. Framework para gestionar las actividades de calidad



Fuente: Framework to manage software quality activities

1.2. ESPECIFICAR ELEMENTOS

Después de analizar los modelos de referencia encontrados y siguiendo los pasos de Sandoval y Pernaletе (2014), se han podido especificar los siguientes elementos para la construcción del marco de trabajo:

- Actores: Se encargan de realizar las etapas del marco de trabajo.
- Roles: Funciones que tienen cada uno de los actores.
- Etapas: Partes en las que se divide el marco de trabajo.
- Paso: El camino a seguir de cada etapa del marco de trabajo.
- Entregables: Resultados de las etapas del marco de trabajo.

2. CONSTRUCCIÓN

En esta etapa se realizó la construcción del marco de trabajo para la gestión de riesgos en la seguridad de la información. Para ello, se especifica las etapas que tiene el marco de trabajo; los pasos y los entregables de cada etapa; los actores que realizan las etapas y los pasos; y los roles que son las funciones de cada actor (Sandoval y Pernaletе, 2014).

2.1. ESPECIFICAR ETAPAS

Para las etapas del marco de trabajo se han revisado artículos sobre ISO 27005 y COBIT 2019, de los cuales se han elegido 5 etapas:



- Establecimiento del Contexto: Esta etapa forma parte de ISO 27005 y en ella se establecen los criterios básicos que son necesarios para la gestión del riesgo, los cuales son criterios de evaluación, de impacto y de tratamiento. También, se define el alcance del marco de trabajo para la gestión de riesgos en la seguridad de la información (Hamita, Sarkanb, Azmib, Mahrinb, Chupratb y Yahya, 2020).
- Análisis del Riesgo: Esta etapa forma parte de COBIT 2019 y su propósito de esta etapa es determinar qué podría ocasionar una pérdida potencial y comprender cómo, dónde y por qué podría ocurrir esta pérdida (Alvarado-Sarango y Andrade-López, 2021).
- Evaluación del Riesgo: Esta etapa pertenece a ISO 27005, en ella, el grado de detalle depende de los activos, la amplitud de las vulnerabilidades y los incidentes anteriores que ocurrieron en la organización. Además, en ella se comparan los niveles de riesgo con los criterios de evaluación del riesgo que se definieron en el establecimiento del contexto (Espinosa, Martínez y Amador, 2014).
- Tratamiento del Riesgo: Esta etapa forma parte de ISO 27005 y en ella se desarrolla una lista de opciones de tratamiento para los riesgos que se encontraron en la etapa de identificación del riesgo (Hamita et al., 2020).
- Comunicación del Riesgo: Esta etapa forma parte de ISO 27005 y en ella se comparte la información de los riesgos para elegir la mejor forma de gestionar los riesgos (Espinosa, Martínez y Amador, 2014).

2.2. ESPECIFICAR PASOS Y ENTREGABLES

En el establecimiento del contexto existen 2 pasos:

- Especificar criterios básicos: Se desarrollan los criterios de evaluación del riesgo, los criterios de impacto del riesgo y especificarlos según el grado de daño, y los criterios de tratamiento del riesgo para las diferentes clases de riesgos (Hamita et al., 2020).



- Especificar alcance: Se define el alcance del proceso de gestión de los riesgos que se pueden presentar (Hamita et al., 2020).

En el análisis del riesgo existen 3 pasos:

- Identificación de los activos: Se identifican los activos dentro del alcance establecido, los cuales son aquellos que tienen valor para una organización (Alvarado-Sarango y Andrade-López, 2021).
- Identificación de las vulnerabilidades: Se identifican las vulnerabilidades que puedan causar daño a los activos o la organización (Alvarado-Sarango y Andrade-López, 2021).
- Identificación de las consecuencias: Se identifican las consecuencias que ocurrirían al ser explotadas las vulnerabilidades (Alvarado-Sarango y Andrade-López, 2021).

La evaluación del riesgo consta de 3 pasos:

- Evaluación de las consecuencias: Se evalúa el impacto de los posibles incidentes en la seguridad de la información de la organización tomando en cuenta la valoración de activos (Espinosa, Martínez y Amador, 2014).
- Evaluación de la probabilidad de incidentes: Se evalúa la probabilidad de cada escenario y su impacto en la organización (Espinosa, Martínez y Amador, 2014).
- Riesgo por prioridad: Se ordenan los riesgos de acuerdo con los criterios de evaluación (Espinosa, Martínez y Amador, 2014).

El tratamiento del riesgo consta de 1 paso:

- Opciones de tratamiento: Se realiza un listado con los posibles tratamientos para los riesgos de la seguridad de la información de la organización (Hamita et al., 2020).

En la comunicación del riesgo existe 1 paso:



- Compartir información de los riesgos: Se intercambia o comparte la información entre quienes toman las decisiones y las otras partes involucradas (Agrawal, 2017).

Después de especificar los pasos de cada etapa, se pasará a definir los entregables de estas etapas. Para ello, se realizó la siguiente tabla:

Tabla 1. Entregables por Etapas

ETAPAS	ENTREGABLES
Establecimiento del Contexto	- Lista de criterios básicos: evaluación, impacto y tratamiento del riesgo.
Análisis del Riesgo	- Lista de activos - Lista de vulnerabilidades - Lista de consecuencias de los riesgos
Evaluación del Riesgo	- Lista de incidentes con niveles de probabilidad - Perfil del riesgo
Tratamiento del Riesgo	- Lista de opciones de tratamiento
Comunicación del Riesgo	Sin entregable

Fuente: Elaboración propia

2.3. ESPECIFICAR ACTORES Y ROLES

Según las etapas, pasos y entregables especificados anteriormente, se han encontrado los siguientes actores y roles:

Tabla 2. Actores y sus roles

ACTORES	ROLES
Maestro de Gestión	Es quien se encargará de definir los criterios básicos que se necesitan para la gestión de riesgo y el alcance de dicha gestión. Además, es quien comparte la información con la organización.
Investigador de Riesgos	Es quién tendrá más contacto con la organización y se encargará de encontrar y analizar los riesgos.
Equipo de Tratamiento	Es un equipo que se encargará de buscar opciones de tratamiento para los riesgos encontrados por el Investigador de Riesgos. Asimismo, serán los encargados de implementar el tratamiento elegido por la organización.

Fuente: Elaboración propia

Luego de especificar cada etapa, paso y entregable, se pasará a unir el marco de trabajo para que se vea como la figura 4.

Figura 4. Marco de Trabajo para la Gestión de Riesgos



Fuente: Elaboración propia

1. ESTABLECIMIENTO DEL CONTEXTO

En esta etapa del marco de trabajo se han especificado los criterios básicos y el alcance del marco de trabajo para la gestión de riesgos en la seguridad de la información (Hamita et al., 2020).

1.1. ESPECIFICAR CRITERIOS BÁSICOS

Según Hamita et al. (2020), para establecer los criterios básicos, la organización debe evaluar si los recursos necesarios están disponibles para monitorear los procesos de gestión del riesgo en la seguridad de la información y realizar la evaluación y tratamiento del riesgo.

1.1.1. LISTA DE CRITERIOS DE EVALUACIÓN DEL RIESGO

Para desarrollar criterios de evaluación del riesgo se han tomado en cuenta los siguientes aspectos:



- El valor estratégico del proceso de información de la organización.

Figura 5. Valores Estratégicos



Fuente: Elaboración propia

- La importancia de los activos de información involucrados.

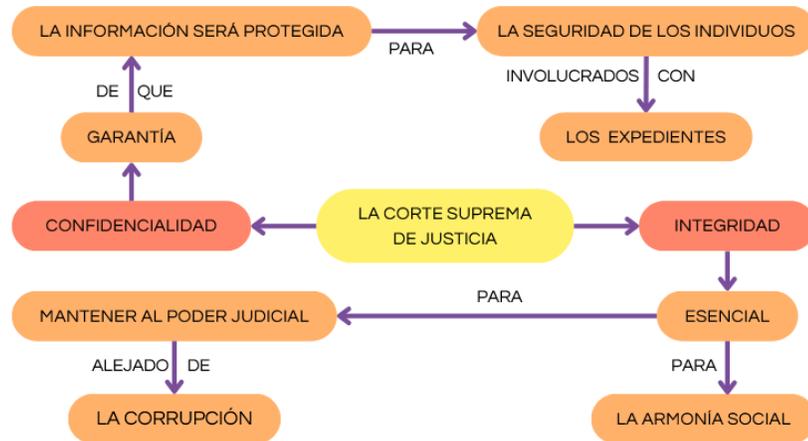
Figura 6. Los Activos



Fuente: Elaboración propia

- La importancia de la confidencialidad e integridad para las operaciones y la organización.

Figura 7. La Confidencialidad e Integridad



Fuente: Elaboración propia

- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación.

Figura 8. Expectativas y consecuencias negativas



Fuente: Elaboración propia

Siguiendo los aspectos mencionados, se han encontrado los siguientes criterios de evaluación:

- Se evaluarán los perfiles que pueden ingresar documentos a un expediente.
- Se tomará en cuenta, que perfiles pueden modificar los documentos de un expediente.
- Se evaluarán los perfiles que pueden elevar los expedientes.

- Se tomará en cuenta, que perfiles pueden eliminar documentos o delitos de un expediente.

1.1.2. LISTA DE CRITERIOS DE IMPACTO DEL RIESGO

Para desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la organización, se han tomado en cuenta los siguientes aspectos:

- Nivel de clasificación de los activos.

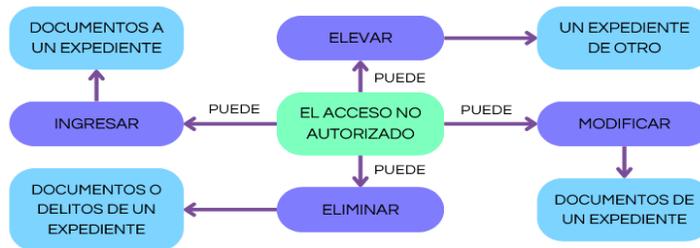
Figura 9. Clasificación de los Expedientes



Fuente: Elaboración propia

- Brechas en la seguridad de la información.

Figura 10. Brechas



Fuente: Elaboración propia

Siguiendo los aspectos mencionados, se han encontrado los siguientes criterios de impacto:

- Alto: Nivel alto de daño a la organización o alto costo para el tratamiento del riesgo.
- Medio: Nivel medio de daño a la organización o bajo costo para el tratamiento del riesgo.
- Bajo: Nivel bajo de daño a la organización o costo nulo para el tratamiento del riesgo.



1.1.3. LISTA DE CRITERIOS DE TRATAMIENTO DEL RIESGO

Para desarrollar criterios de tratamiento del riesgo, se han tomado en cuenta los siguientes elementos:

- Criterios del negocio

Figura 11. Criterios del Poder Judicial



Fuente: Elaboración propia

- Operaciones

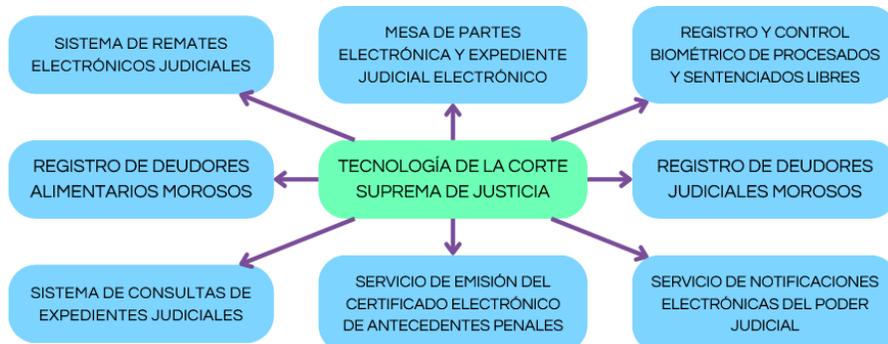
Figura 12. Operaciones de la Corte Suprema de Justicia



Fuente: Elaboración propia

- Tecnología

Figura 13. Tecnología de la Corte Suprema de Justicia



Fuente: Elaboración propia



Siguiendo los aspectos mencionados, se han encontrado los siguientes criterios de tratamiento:

- El perfil que puede ingresar documentos a un expediente, no pueda ingresar documentos a menos que cumpla con uno o más requisitos previos.
- El perfil que puede modificar documentos de un expediente, no pueda modificar a menos que cumpla con uno o más requisitos previos.
- El perfil que puede elevar un expediente, no pueda elevar un expediente a menos que un equipo este de acuerdo con la elevación de dicho expediente.
- El perfil que puede eliminar documentos o delitos de un expediente, no pueda eliminar a menos que cumpla con uno o más requisitos previos.

1.2. ESPECIFICAR ALCANCE

El alcance del proceso de gestión del riesgo permite establecer los límites y definir con precisión el objetivo y plazos de cada entregable. Para definir el alcance del proceso de gestión del riesgo en la seguridad de la información, se ha tomado en cuenta lo siguiente:

- Los objetivos de la organización.

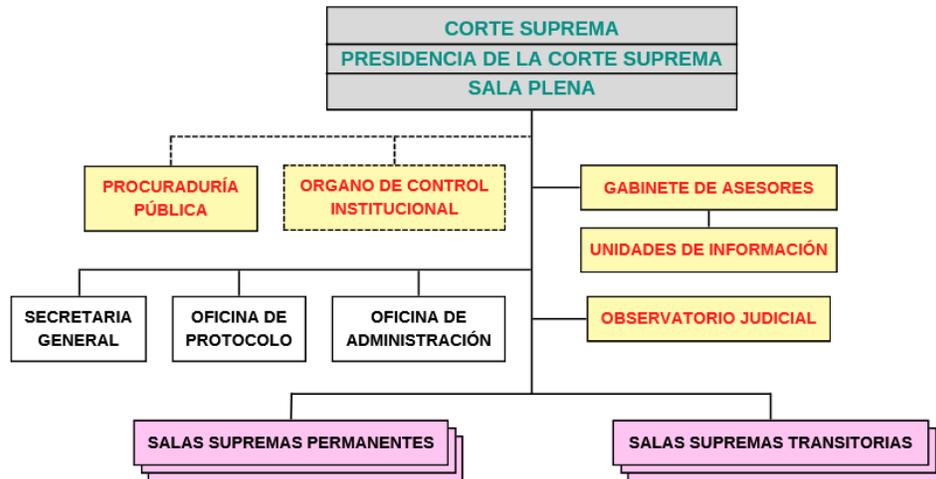
Figura 14. Objetivos de la Corte Suprema de Justicia



Fuente: Elaboración propia

- La estructura de la organización.

Figura 15. Organigrama de la Corte Suprema de Justicia

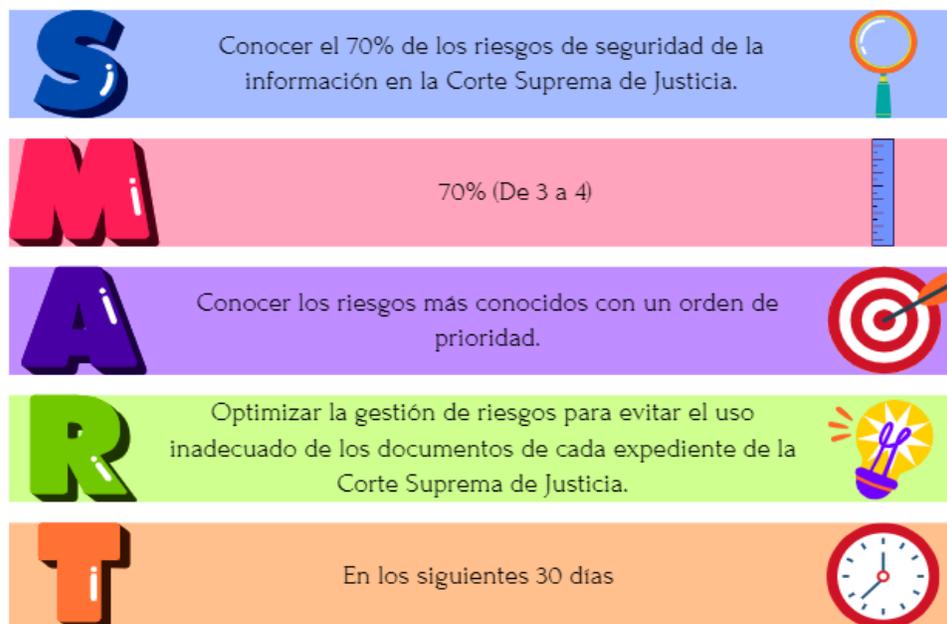


Fuente: Elaboración propia

Para establecer el alcance se deben definir objetivos SMART y definir los plazos y entregables con el diagrama de Gantt.

Siguiendo esta información, se ha definido el alcance de esta manera:

Figura 16. Objetivos SMART



Fuente: Elaboración propia

Tabla 3. Diagrama de Gantt

ENTREGABLES	1 SEMANA							2 SEMANA							3 SEMANA								
	1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7		



activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización.

2.1.1. LISTA DE ACTIVOS

Los activos se pueden identificar mediante la figura 17.

Figura 17. Activos de la Corte Suprema de Justicia



Fuente: Elaboración propia

En este caso, los activos de la Corte Suprema de Justicia vendrían a ser los expedientes. Según el Poder Judicial del Perú (2016) el expediente judicial es un instrumento público en forma de legajo que resulta de los actos procesales realizados en un juicio, que están ordenados cronológicamente en forma de libro.

2.2. IDENTIFICACIÓN DE LAS VULNERABILIDADES

Siguiendo lo indicado por Alvarado-Sarango y Andrade-López (2021), con respecto a identificar las vulnerabilidades que pueden ser explotadas, se ha realizado la siguiente lista:

2.2.1. LISTA DE VULNERABILIDADES

Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización, procesos y procedimientos
- Personal
- Configuración del sistema de información
- Hardware o software



Las vulnerabilidades pueden estar relacionadas con las propiedades de los activos que se pueden usar de una manera, o para un propósito, diferente del previsto cuando se adquirió o se elaboró el activo. Asimismo, para la identificación de vulnerabilidades se puede hacer uso de los siguientes métodos proactivos:

- Herramientas automatizadas para la búsqueda e identificación de las vulnerabilidades: software creado para pruebas de seguridad y descubrimiento de las vulnerabilidades de forma automática, generando informes detallados de los problemas y vulnerabilidades identificados en el sistema.
- Prueba de invasión: tiene como objetivo comprobar la resistencia del activo en relación a los métodos de ataque conocidos.
- Análisis crítico de código: la identificación de las vulnerabilidades en el código fuente.

En este caso, se identificaron las siguientes vulnerabilidades:

- Insuficiencia de requisitos previos para que el perfil adecuado pueda ingresar documentos a los expedientes.
- Insuficiencia de requisitos previos para que el perfil adecuado pueda modificar documentos de los expedientes.
- Insuficiencia de requisitos previos para que el perfil adecuado pueda elevar un expediente.
- Insuficiencia de requisitos previos para que el perfil adecuado pueda eliminar documentos o delitos de un expediente.

2.3. IDENTIFICACIÓN DE LAS CONSECUENCIAS

Siguiendo lo indicado por Alvarado-Sarango y Andrade-López (2021), con respecto a identificar las consecuencias de los riesgos en la seguridad de la información de la Corte Suprema de Justicia, se ha realizado la siguiente lista:



2.3.1. LISTA DE CONSECUENCIAS DE LOS RIESGOS

Un escenario de incidente ocurre cuando una vulnerabilidad determinada o un conjunto de vulnerabilidades son explotadas y se convierten en un incidente de seguridad de la información.

Para la identificación de riesgos se deben tomar en cuenta escenarios de incidentes en términos de:

- Tiempo de investigación y reparación.
- Pérdida de tiempo y oportunidades.
- Costo financiero de las habilidades específicas para reparar el daño.
- Imagen, reputación y buen nombre.

Además, se debe medir el impacto de los riesgos mediante la siguiente plantilla:

Tabla 4. *Plantilla para medir el impacto de los riesgos*

	Nivel de Impacto		
	Bajo	Medio	Alto

Fuente: Elaboración propia

Para saber las consecuencias de los riesgos se ha medido el impacto de cada riesgo utilizando la plantilla anterior.

Tabla 5. *Impacto de las consecuencias de los riesgos*

	Nivel de Impacto		
	Bajo	Medio	Alto
Una persona que no pertenece al perfil correspondiente ingresa documentos a un expediente	X		
Una persona que no pertenece al perfil correspondiente modifica documentos de un expediente		X	
Una persona que no pertenece al perfil correspondiente eleva un expediente			X



Una persona que no pertenece al perfil correspondiente elimina un documento o delito de un expediente			X
---	--	--	---

Fuente: Elaboración propia

Siguiendo estos aspectos, se ha podido identificar las siguientes consecuencias:

- Mala imagen de la Corte Suprema de Justicia.
- El empleado que se ve involucrado con uno de estos riesgos puede ser destituido.
- El empleado que se ve involucrado con uno de estos riesgos puede ir a la cárcel.

El empleado que se ve involucrado con uno de estos riesgos ya no podría ejercer su cargo.

3. EVALUACIÓN DEL RIESGO

En esta etapa del marco de trabajo se evaluará las consecuencias, se evaluará la probabilidad de incidentes y se ordenarán los riesgos por prioridad (Espinosa, Martínez y Amador, 2014).

3.1. EVALUACIÓN DE LAS CONSECUENCIAS

Según Espinosa, Martínez y Amador (2014), para la evaluación de las consecuencias, la organización debe evaluar las consecuencias del impacto en el negocio. Además, la evaluación de las consecuencias está relacionada con los activos. Por esta razón, se deben ordenar los activos de acuerdo con su importancia para la organización. Es posible hacer esto de dos maneras:

- A través del valor de reposición del activo: donde se determina el costo financiero de recuperación o reposición del activo y también del valor de la información que contenga.



- A través de las consecuencias al negocio: el valor se determina por el impacto de las consecuencias en los negocios. Normalmente este valor es más significativo que sólo el valor del activo.

Asimismo, se han encontrado las siguientes consecuencias para los riesgos identificados:

- Mala imagen de la Corte Suprema de Justicia.
- El empleado que se ve involucrado con uno de estos riesgos puede ser destituido.
- El empleado que se ve involucrado con uno de estos riesgos puede ir a la cárcel.
- El empleado que se ve involucrado con uno de estos riesgos ya no podría ejercer su cargo.

3.2. EVALUACIÓN DE LA PROBABILIDAD DE INCIDENTES

Siguiendo lo indicado por Espinosa, Martínez y Amador (2014), con respecto a evaluar la probabilidad de incidentes, se ha establecido lo siguiente:

3.2.1. LISTA DE INCIDENTES CON NIVELES DE PROBABILIDAD

Para la evaluación de la probabilidad de incidentes se han tomado en cuenta los siguientes aspectos:

- Para fuentes de amenaza deliberada: Motivación para explotar vulnerabilidades, conflictos con superiores, insatisfacción laboral, conocimiento de la vulnerabilidad y atracción de los activos.
- Para fuentes de amenaza accidental: Proximidad a lugares insalubres que pueden dañar los equipos, eventos climáticos y factores que pudieran tener influencia en los errores humanos y el mal funcionamiento del equipo.



Además, se debe medir la probabilidad de incidentes mediante la siguiente plantilla:

Tabla 6. *Plantilla para medir la probabilidad de incidentes*

	Nivel de Probabilidad		
	Baja	Media	Alta

Fuente: Elaboración propia

La presente tabla indica cual es la probabilidad de que suceda un incidente de seguridad de la información en la Corte Suprema de Justicia:

Tabla 7. *Probabilidad de Incidentes*

	Nivel de Probabilidad		
	Baja	Media	Alta
Una persona que no pertenece al perfil correspondiente ingresa documentos a un expediente		x	
Una persona que no pertenece al perfil correspondiente modifica documentos de un expediente			x
Una persona que no pertenece al perfil correspondiente eleva un expediente		x	
Una persona que no pertenece al perfil correspondiente elimina un documento o delito de un expediente	x		

Fuente: Elaboración propia

3.3. RIESGO POR PRIORIDAD

Siguiendo lo indicado por Espinosa, Martínez y Amador (2014), con respecto al orden de cada riesgo por su prioridad, se ha establecido lo siguiente:

3.3.1. PERFIL DEL RIESGO



Según Alvarado-Sarango y Andrade-López (2021), este entregable está definido en COBIT 2019 y en él se deben incluir un inventario de riesgos conocidos ordenados por prioridad, incluyendo la frecuencia esperada y el impacto potencial.

Para medir la evaluación del riesgo, nos guiamos de la tabla 8 para saber la prioridad de los riesgos, la cual relaciona el impacto de los riesgos y la probabilidad de que ocurran riesgos. En la tabla, 1 es el de mayor prioridad y 9 es la de menor prioridad.

Tabla 8. *Prioridad del riesgo*

IMPACTO	MATRIZ DE EVALUACIÓN DEL RIESGO		
Alto	1	2	4
Medio	3	5	7
Bajo	6	8	9
	Alta	Media	Baja
	PROBABILIDAD		

Fuente: Elaboración propia

Para medir el nivel de prioridad de riesgos se debe utilizar la siguiente plantilla:

Tabla 9. *Plantilla para medir el nivel de Prioridad de Riesgos*

Riesgos	Nivel de Prioridad

Fuente: Elaboración propia

Asimismo, se ha determinado el nivel de prioridad de los riesgos en la siguiente tabla:



Tabla 10. Nivel de Prioridad de Riesgos

Riesgos	Nivel de Prioridad
Una persona que no pertenece al perfil correspondiente ingresa documentos a un expediente	8
Una persona que no pertenece al perfil correspondiente modifica documentos de un expediente	3
Una persona que no pertenece al perfil correspondiente eleva un expediente	2
Una persona que no pertenece al perfil correspondiente elimina un documento o delito de un expediente	4

Fuente: Elaboración propia

Para realizar el perfil de riesgos se debe usar la siguiente plantilla:

Tabla 11. Plantilla para realizar el Perfil de Riesgos

Orden de Riesgos por Prioridad			
N°	Riesgos	Nivel de Impacto	Nivel de Probabilidad
1			
2			

Fuente: Elaboración propia

Finalmente, se realiza el perfil de riesgos ordenados por prioridad en la tabla 12.

Tabla 12. Perfil de Riesgos

Orden de Riesgos por Prioridad			
N°	Riesgos	Nivel de Impacto	Nivel de Probabilidad
1	Una persona que no pertenece al perfil correspondiente eleva un expediente	Alto	Media
2	Una persona que no pertenece al perfil correspondiente modifica documentos de un expediente	Medio	Alta
3	Una persona que no pertenece al perfil correspondiente elimina un documento o delito de un expediente	Alto	Baja



4	Una persona que no pertenece al perfil correspondiente ingresa documentos a un expediente	Bajo	Media
---	---	------	-------

Fuente: Elaboración propia

4. TRATAMIENTO DEL RIESGO

En esta etapa del marco de trabajo se presentarán las opciones de posibles tratamientos para los riesgos de seguridad de la información que se encontraron anteriormente (Hamita et al., 2020).

4.1. OPCIONES DE TRATAMIENTO

Según Hamita et al. (2020), existen 2 tipos de tratamientos del riesgo que se deben considerar al momento de buscar opciones de tratamiento:

- Reducir el Riesgo: Cuando los riesgos identificados se pueden reducir de tal manera que al reevaluarlos sean aceptables para la organización.
- Evitar el Riesgo: Cuando los riesgos identificados son muy altos o los costos para implementar el tratamiento exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo, mediante el retiro de una actividad o el cambio de las condiciones en las que se realiza dicha actividad.

También se debe considerar las siguientes restricciones al momento de elegir un tratamiento:

- Restricciones de tiempo
- Restricciones financieras
- Restricciones técnicas y operativas
- Restricciones éticas y legales

4.1.1. LISTA DE OPCIONES DE TRATAMIENTO



Para el tratamiento de los riesgos de seguridad de la información en el Sistema Integrado Judicial Supremo de la Corte Suprema de Justicia, se han encontrado las siguientes opciones:

- Para ingresar, modificar o eliminar un documento de un expediente, se solicite un código que será enviado al correo del trabajador de la Corte Suprema de Justicia. El código enviado tendrá una duración de 3 minutos para ser ingresado al sistema, sino se generará otro código.
- Para elevar un expediente del otro, que se envíe una solicitud con las razones para elevar expediente a un grupo de mínimo 3 personas. Si las 3 personas aceptan la solicitud, el sistema le permitirá elevar el expediente.
- Para saber quién está modificando los documentos del expediente, el sistema solicite tomar una foto en tiempo real con la cámara del dispositivo por el que ingresa al sistema.

5. COMUNICACIÓN DEL RIESGO

En esta etapa del marco de trabajo se compartirá y explicará la información encontrada sobre los riesgos (Agrawal, 2017).

5.1. COMPARTIR INFORMACIÓN DE LOS RIESGOS

En este paso se presenta, a la Corte Suprema de Justicia, los entregables que se realizaron en las etapas anteriores y se pasará a explicar detalladamente, en una exposición, cada entregable.

Después de finalizar la etapa de la construcción del marco de trabajo para la gestión de riesgos en la seguridad de la información de la Corte Suprema de Justicia, se realizará la tercera etapa.

3. EVALUACIÓN



La evaluación es la tercera y última etapa, aquí se evaluará el marco de trabajo construido, donde se identificarán los errores que se cometieron en la etapa de construcción y se identificarán las amenazas que puedan darse con el paso del tiempo (Sandoval y Pernalet, 2014).

3.1. IDENTIFICAR ERRORES

Después de analizar el marco de trabajo y el proceso de construcción del mismo, se han hallado los siguientes errores:

- Al momento de construir el marco de trabajo, se eliminaron algunas etapas que se habían previsto para el marco de trabajo de gestión de riesgos en la seguridad de la información.
- El marco de trabajo está basado en ISO 27005 y COBIT 2019, sin embargo se consultaron y encontraron más artículos sobre ISO 27008 que sobre COBIT 2019.
- Las etapas del marco de trabajo de gestión de riesgos están basadas más en ISO 27005 que en COBIT 2019.

Los errores hallados pueden solucionarse al realizar una mayor investigación sobre COBIT 2019.

3.2. IDENTIFICAR AMENAZAS

Se han identificado las siguientes amenazas:

- Encontrar nuevos riesgos al momento de implementar un tratamiento de la lista de opciones de tratamiento propuestas en el marco de trabajo.
- La Corte Suprema de Justicia puede considerar que los tratamientos de la lista de opciones, no son convenientes para sus trabajadores o para alguno de los procesos que realizan.
- La Corte Suprema de Justicia podría hallar otros marcos de trabajo sobre la gestión de riesgos en la seguridad de la información.



ALCANCES

1. Establecer los procedimientos que se llevaran a cabo en las diferentes áreas de la Corte Suprema de Justicia, en los cuales se ha implementado el Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo.
 2. Dar a conocer a los jueces y personal de apoyo a la función jurisdiccional que laboran en dicha corte, el procedimiento a seguir, desde el ingreso de los documentos, siguiendo con el tramite y finalizando en la entrega de los mismos.
 3. Propiciar la uniformidad de trabajo, permitiendo que los servidores puedan identificar sus funciones y responsabilidades, realizando aquellas de forma ordenada y sistemática.
 4. Evitar la duplicidad de funciones, y servir como indicador para detectar omisiones.
 5. Permitir la integración de todos los colaboradores, así como la funcionalidad integral del personal.
 6. Propiciar el ahorro de esfuerzos y recursos.
 7. Facilitar la inducción de los nuevos colaboradores de los diferentes puestos y áreas de la Corte Suprema.
1. PROCEDIMIENTO DE RECEPCION, REGISTRO Y DIGITALIZACION DE DEMANDAS, ESCRITOS Y OFICIOS.

N° Actividad	Unidad Orgánica/ Responsable	Acción a Seguir
1	Usuario	a) Entrega escrito, demanda u oficio.
2		Recepción y registro de escritos, demandas u oficios
2.1	Centro de distribución modular (CDG)/ Asistente Judicial	a) Recibe la documentación y verifica que sea dirigida o corresponda a los órganos jurisdiccionales. No corresponde b) Orienta al usuario para devolver documentación ¿El usuario esta conforme? No Continua actividad 2. 3.a. Si Continua actividad 2. 2.a.
2.2	Usuario	a) Recibe documento. Fin del procedimiento.
2.3	Centro de distribución modular (CDG)/	Si corresponde a) Verifica la conformidad y legibilidad de los documentos presentados por los justiciables o sus abogados; en

	Asistente Judicial	<p>particular aquellos que indiquen contener copias y procedimientos; y cuando corresponda, que contengan la respectiva tasa judicial.</p> <p>¿Es conforme? No es conforme b) Registra las observaciones correspondientes en el sistema,</p> <p>Si es conforme ¿La documentación es una demanda o escrito u oficio? Si la documentación ingresada es una demanda c) Registra y graba en el SIJ, generando automáticamente el numero de registro, el código de digitalización y la asignación aleatoria del órgano jurisdiccional competente y secretario judicial de la sub área de calificación del área de apoyo a las causas. Continúa actividad f.</p> <p>Si la documentación ingresada es un escrito u oficio d) Ubica en el SIJ el código que identifica a la documentación. e) Registra y graba en el SIJ y el sistema identifica al secretario asignado, responsable del documento. f) Imprime, en original y copia, un cargo de ingreso del escrito, demanda y oficio, el cual señala los datos del documento, la cantidad de folios recibidos, la cantidad y numeración de tasas judiciales adjuntas y otros. g) Coloca el sello correspondiente al documento impreso y lo adjunta al cargo de recepción del documento. h) Coloca documentos en bandeja física.</p>
3		Digitalización de demandas, escritos u oficios
3.1	Centro de distribución modular (CDG)/ Técnico Administrativo II	a) Recoge documentos de bandeja física. b) Compara las copias ingresadas con el escrito o demanda original, para verificar la coincidencia entre el numero de folios del documento original con el numero de folios de la copia. ¿Hay documentación digitalizada? No c) Llena formato de entrega de anexo no digitalizados. d) Entrega formato llenado con los anexos no digitalizados al Asistente Administrativo II. Continúa actividad 3.2.a Si e) Desglosa la documentación f) Coloca la copia de cada hoja de la documentación en el escáner para la digitalización. Se digitaliza anexos. g) Digita en el escáner el código de digitalización de cada documento.

		<ul style="list-style-type: none"> h) Realiza la digitalización en el escáner, asegurando su calidad. i) Sella la documentación digitalizada. j) Coloca documentación digitalizada en la bandeja física. <p>Continúa actividad 3.3.a</p>
3.2	Centro de distribución modular (CDG)/ Asistente Administrativo II	<ul style="list-style-type: none"> a) Recibe formato llenado correctamente y los anexos no digitalizados. b) Sella y firma físicamente y custodia la documentación. c) Entrega formato de anexos no digitalizados al administrador del área. <p>Fin del procedimiento.</p>
3.3	Centro de distribución modular (CDG)/ Técnico o auxiliar Administrativo	<ul style="list-style-type: none"> a) Recoge la documentación de la bandeja física. b) Descarga archivo digitalizado PDF en el sistema. c) Organiza mediante índices la documentación digitalizada en el sistema. d) Contrasta la documentación física con lo digitalizado en el sistema. <p>¿Conforme? No <ul style="list-style-type: none"> e) Comunica observaciones al técnico administrativo II. Si <ul style="list-style-type: none"> f) Entrega documentación original al usuario. Continúa actividad 3.5.a </p>
3.4	Centro de distribución modular (CDG)/ Asistente Administrativo II	<ul style="list-style-type: none"> a) Subsana observaciones. Continúa actividad 3.3.a
3.5	Usuario	<ul style="list-style-type: none"> a) Recepciona cargo. <p>Fin del procedimiento-</p>

2. PROCEDIMIENTO DE DISTRIBUCION DE ESCRITOS, DEMANDAS, OFICIOS Y MEDIDAS CAUTELARES A LOS SECRETARIOS JUDICIALES.

N° Actividad	Unidad Orgánica/ Responsable	Acción a Seguir
1		Distribución de escritos, escritos, demandas, oficios y medidas cautelares a los secretarios judiciales.
1.1	Centro de distribución modular (CDG)/ Asistente	<ul style="list-style-type: none"> a) Distribuye documentación de forma automática en el sistema. <p>Si es demanda Continúa actividad 1.2.a Si es escrito u oficio</p>

	Administrativo II	<p>Continúa actividad 1.3.a Si es una medida cautelar o un escrito presentado antes de la ejecución de la medida cautelar Continúa actividad 1.4.a Nota:</p> <ul style="list-style-type: none"> - Las medidas cautelares o escritos antes de la ejecución de la medida cautelar serán distribuidas en el sistema al secretario Judicial de apoyo al juez. - Cuando ingresa una medida cautelar y ya hay una sentencia descargada, el sistema distribuirá la medida cautelar al secretario judicial de ejecución.
1.2	Área de apoyo a las Causas/ secretario judicial de Calificación	<p>a) Recibe documentación en el sistema Fin del procedimiento</p>
1.3	Área de apoyo a las Causas/ secretario judicial de Calificación/ Tramite/ Ejecución/ Apoyo al Juez	<p>a) Recibe documentación en el sistema. b) Adjunta escrito al expediente digital Fin del procedimiento.</p>
1.4	Área de apoyo a las Causas/ secretario judicial de Apoyo al juez	<p>a) Recibe documentación en el sistema Fin del procedimiento.</p>

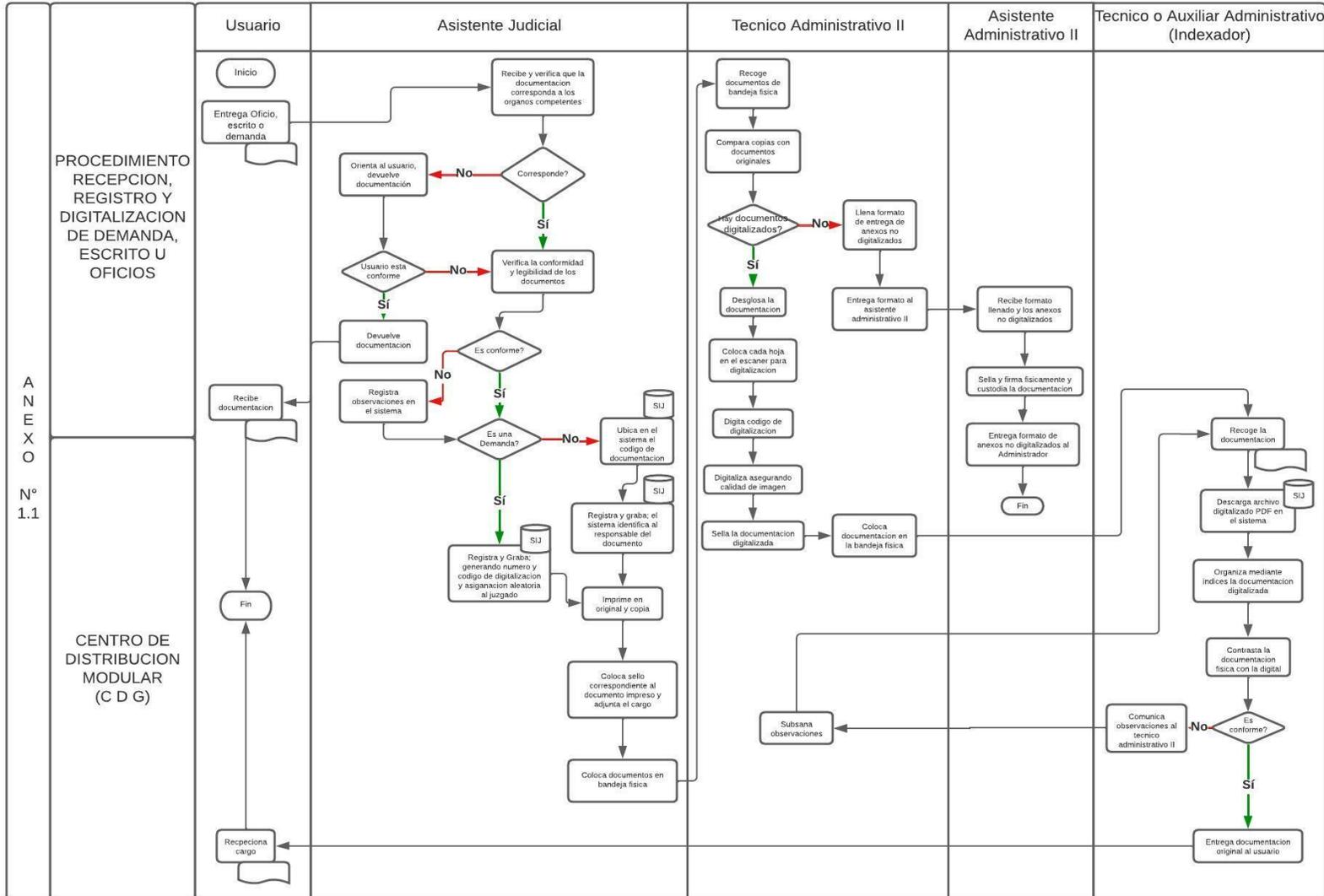
3. PROCEDIMIENTO DE CALIFICACION DE MEDIDA CAUTELAR.

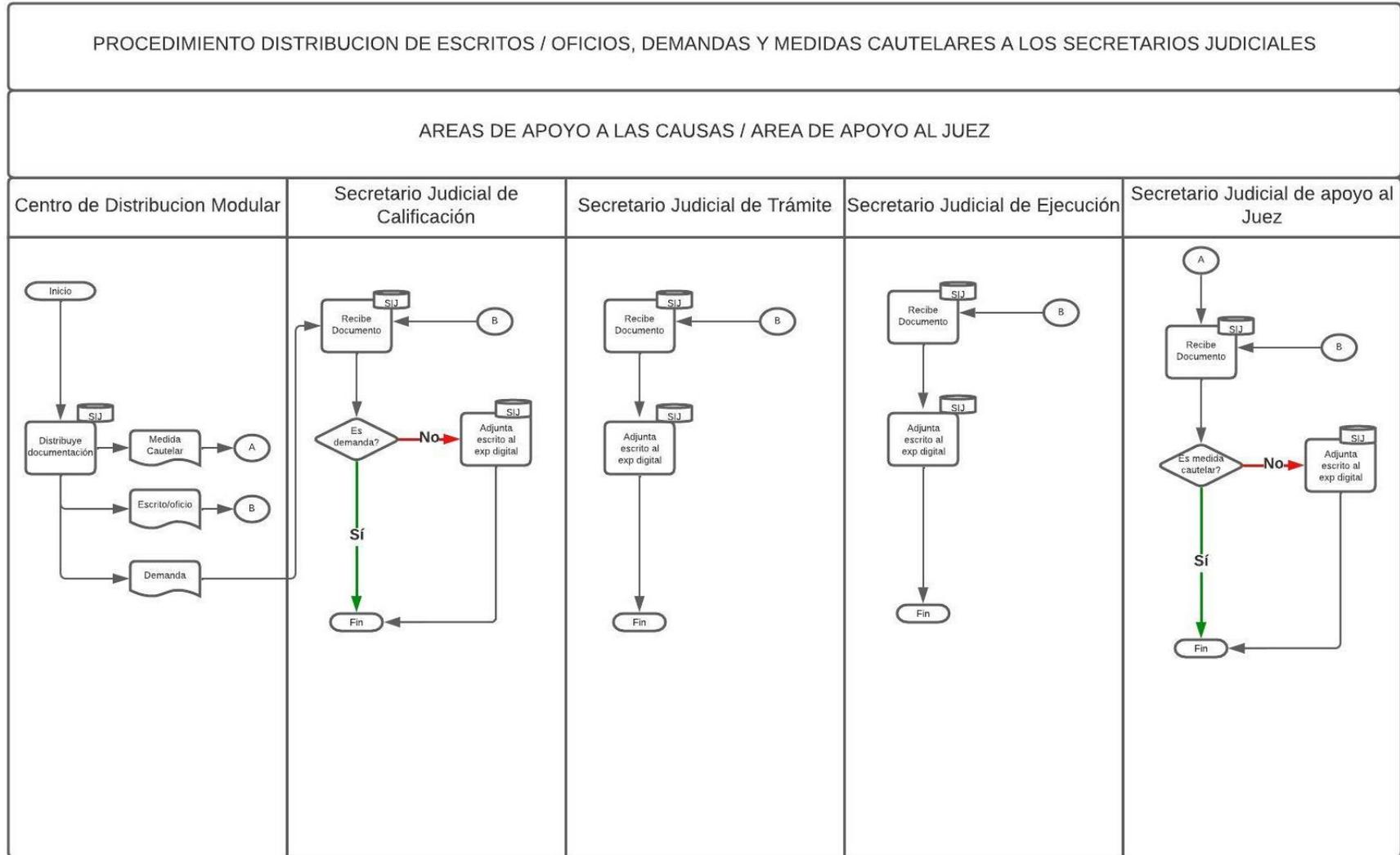
N° Actividad	Unidad Orgánica/ Responsable	Acción a Seguir
1		Calificación de medidas cautelares
1.1	Área de apoyo al Juez / secretario Judicial de Apoyo al Juez	<p>a) Recibe y revisa medida cautelar en el sistema. b) Da cuenta al Juez.</p>
1.2	Área Jurisdiccional / Juzgado	<p>a) Señala sentido y lineamientos para calificación.</p>

1.3	Área de apoyo al Juez / secretario Judicial de Apoyo al Juez	<ul style="list-style-type: none"> a) Elabora proyectos de resolución en el sistema b) Envía proyecto de resolución al juez en el sistema.
1.4	Área Jurisdiccional / Juzgado	<ul style="list-style-type: none"> a) Recibe por sistema y revisa proyecto de resolución. <p>¿Proyecto es conforme? Si. Continúa actividad 1.6. No</p> <ul style="list-style-type: none"> b) Devuelve proyecto. Continúa la actividad 1.3.a.
1.5	Área de apoyo al Juez / secretario Judicial de Apoyo al Juez	<ul style="list-style-type: none"> a) Corrige observaciones. Continúa la actividad 1.3.b.
1.6	Área Jurisdiccional / Juzgado	<p>El proyecto puede ser:</p> <ul style="list-style-type: none"> - Auto Inadmisibile. Continúa actividad 1.7.a. - Auto Improcedente. Continúa actividad 1.18.a. - Auto que concede medida cautelar con efecto solicitado/ Auto que concede medida cautelar con efecto distinto al solicitado. Continúa actividad 1.20.a
		El proyecto es un Auto Inadmisibile.
1.7	Área Jurisdiccional / Juzgado	<ul style="list-style-type: none"> a) Firma digitalmente.
1.8	Área de apoyo al Juez / secretario Judicial de Apoyo al Juez	<ul style="list-style-type: none"> a) Firma digitalmente. b) Realiza descargo en el sistema. c) Realiza notificación electrónica
1.9	Solicitante	<ul style="list-style-type: none"> a) Recibe notificación. <p>¿Subsana el auto de inadmisibilidat? No. Continúa actividad 1.13.a. Si.</p> <ul style="list-style-type: none"> b) Presenta escrito de subsanación. <p>Pasa al procedimiento de Recepción, registro y digitalización de demanda, escrito u oficios (Procedimiento N° 1.1)</p>
1.10	Área de apoyo al Juez / secretario Judicial de Apoyo al Juez	<ul style="list-style-type: none"> a) Recibe escrito por sistema anexo al cuaderno. b) Elabora proyecto de resolución de concesorio o rechazo de la medida cautelar. c) Envía proyecto de resolución al juez mediante el sistema.
1.11	Área Jurisdiccional / Juzgado	<ul style="list-style-type: none"> a) Recibe por sistema y revisa proyecto de resolución. <p>¿Proyecto es conforme? No.</p> <ul style="list-style-type: none"> b) Devuelve proyecto. Continúa actividad 1.12.a. <p>Si. El proyecto puede ser:</p>

		<ul style="list-style-type: none"> - Auto que concede medida cautelar: Continúa actividad 1.25.a. - Auto de rechazo de medida cautelar: Continúa actividad 1.14.b.
1.12	Área de apoyo al Juez / secretario Judicial de Apoyo al Juez	a) Corrige observaciones. Continúa actividad 1.10.c.
1.13	Área de apoyo al Juez / secretario Judicial de Apoyo al Juez	<ul style="list-style-type: none"> a) Elabora proyecto de resolución de rechazo de medida cautelar. b) Envía proyecto de resolución al juez mediante el sistema.
1.14	Área Jurisdiccional / Juzgado	<ul style="list-style-type: none"> a) Recibe en el sistema y revisa proyecto de resolución. <p>¿Proyecto es conforme?</p> <p>Si. Es auto de rechazo de la medida cautelar.</p> <ul style="list-style-type: none"> b) Firma digitalmente. Continúa actividad 1.16.a. <p>No.</p> <ul style="list-style-type: none"> c) Devuelve proyecto. Continúa actividad 1.15.a.
1.15	Área de apoyo al Juez / secretario Judicial de Apoyo al Juez	a) Corrige observaciones. Continúa actividad 1.13.b.
1.16	Área de apoyo al Juez / secretario Judicial de Apoyo al Juez	<ul style="list-style-type: none"> a) Firma digitalmente. b) Realiza descargo en el sistema. c) Realiza notificación electrónica.
1.17	Solicitante	<ul style="list-style-type: none"> a) Recibe notificación. <p>¿Apela?</p> <p>No. Fin de procedimiento.</p> <p>Si.</p> <ul style="list-style-type: none"> b) Presenta escrito de apelación. <p>Pasa al procedimiento de:</p> <ul style="list-style-type: none"> - (Procedimiento N° 1.1) <p>Fin del procedimiento</p>
1.18	Área Jurisdiccional / Juzgado	a) Firma digitalmente.
1.19	Área de apoyo al Juez / asistente Judicial	<ul style="list-style-type: none"> a) Firma digitalmente. b) Realiza descargo en el sistema. c) Realiza notificación electrónica. Continúa actividad 1.17.a.
		El proyecto es auto que concede medida cautelar

1.20	Área Jurisdiccional / Juzgado	a) Firma digitalmente.
1.21	Área de apoyo al Juez / secretario Judicial de Apoyo al Juez	a) Firma digitalmente. b) Realiza descargo en el sistema. Realiza notificación electrónica. Continúa actividad 1.22.a. Pasa a etapa de ejecución.
1.22	Solicitante	a) Recibe notificación- ¿Es con efecto distinto a lo solicitado? Si. ¿Apela? Si. Pasa al procedimiento de: - (Procedimiento N° 1.1) No Fin del procedimiento. No Fin del procedimiento.
1.23	Ejecutado	Una vez ejecutada la medida cautelar ¿Formula oposición? No. Fin del procedimiento. Si. a) Formula oposición. Pasa al procedimiento: - (Procedimiento N° 1.1) Fin del procedimiento.

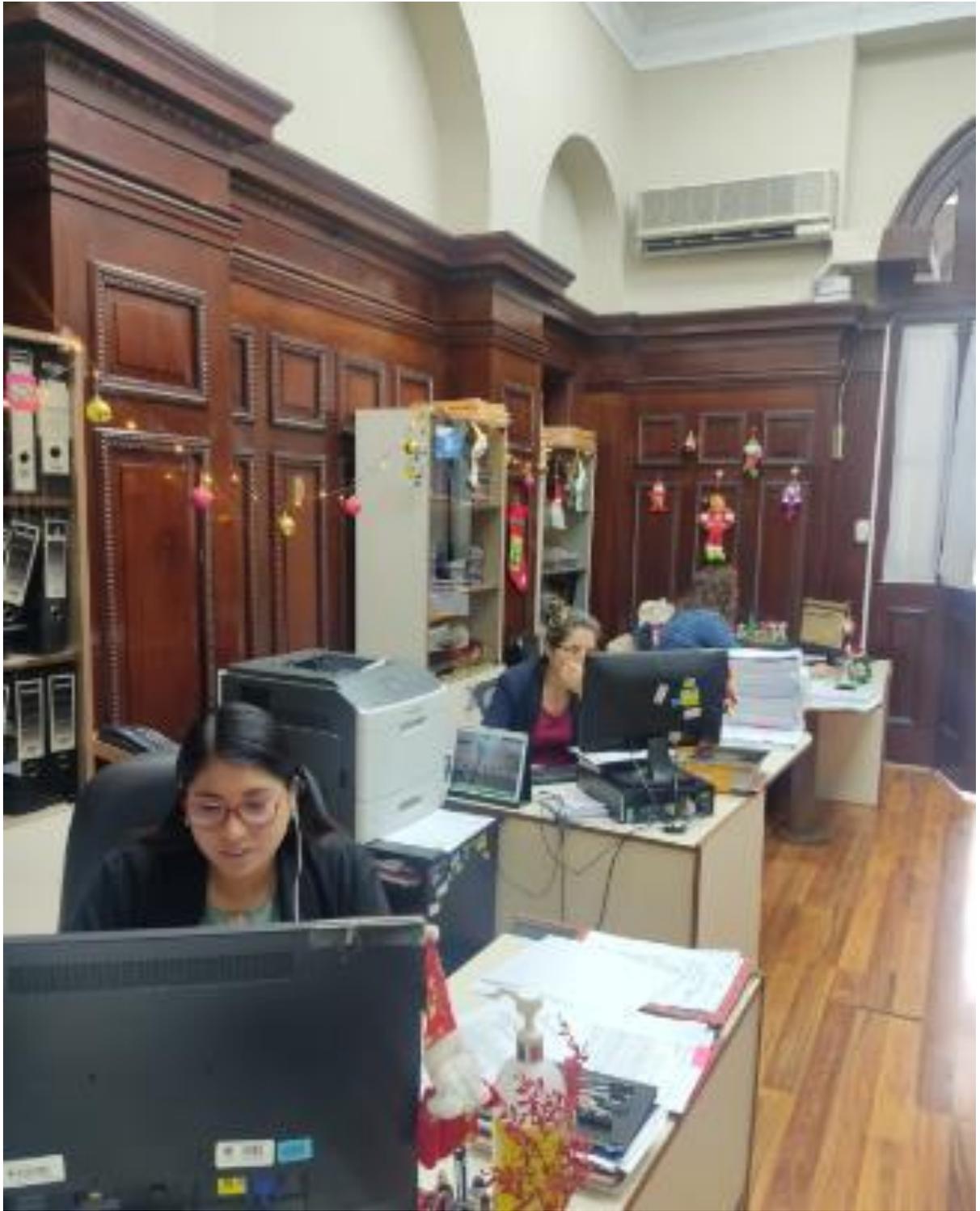




ANEXO 06: EVIDENCIAS









ANEXO 07: CARTA DE APLICABILIDAD DE LA CORTE SUPREMA DE JUSTICIA



"Año del Fortalecimiento de la Soberanía Nacional"

Miércoles, 23 de noviembre de 2022

Director(a) de la escuela de Ingeniería de Sistemas
Universidad Cesar Vallejo — Sede Lima Norte

AUTORIZACIÓN PARA LA REALIZACIÓN Y DIFUSIÓN DE RESULTADOS DE LA INVESTIGACIÓN

Por el presente documento, Yo **LUIS MIGUEL RIEGA MORALES** identificado con DNI N° 10792369 y siendo el Jefe Coordinador del Área de Innovación Judicial de la Corte Suprema de Justicia de la República, autorizo a MÁRQUEZ RODRÍGUEZ MARÍA y YARLEQUE ALDANA LUIS MIGUEL identificados con los DNI N° 75572838 y 42500429 a realizar la investigación titulada "Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo" y a difundir los resultados de la investigación utilizando el nombre de la Corte Suprema de Justicia de la República.

Atentamente.

Firma y Sello
LUIS MIGUEL RIEGA MORALES
COORDINADOR
Área de Innovación Judicial
Corte Suprema de Justicia de la República

Riega Morales, Luis Miguel
Jefe Coordinador del
Área de Innovación Judicial
DNI: 10792369



UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

Declaratoria de Autenticidad del Asesor

Yo, SABOYA RIOS NEMIAS, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo", cuyos autores son YARLEQUE ALDANA LUIS MIGUEL, MARQUEZ RODRIGUEZ MARIA DE LOS ANGELES, constato que la investigación tiene un índice de similitud de 24.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 20 de Diciembre del 2022

Apellidos y Nombres del Asesor:	Firma
SABOYA RIOS NEMIAS DNI: 42001721 ORCID: 0000-0002-7166-2197	Firmado electrónicamente por: NSABOYARI el 20- 12-2022 20:44:58

Código documento Trilce: TRI - 0497373