UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

ISO 27002 y cumplimiento normativo en las sentencias de los juicios de los juzgados de familia, Lima 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Rumiche Huamani Ruben Eduardo (orcid.org/0000-0002-6864-131X)

ASESORES:

Mg. Poletti Gaitan Eduardo Humberto (orcid.org/0000-0002-2143-4444)

Dr. Pereyra Acosta, Manuel Antonio (orcid.org/0000-0002-2593-5772)

LÍNEA DE INVESTIGACIÓN :

Auditoría De Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA - PERÚ

2024

DEDICATORIA:

La presente investigación la dedico a mis padres maravillosos, Juan quien partió a la eternidad hace poco más de un año, el cual siempre me inculcó los estudios y esforzarme por lograr mis metas y quien desde el cielo debe estar muy feliz de ver que seguí sus consejos, a mi señora madre Martha quien siempre me alienta en mi día a día, a mi esposa Sandra quien me inspira a seguir adelante y está al pendiente de mis avances académicos, profesionales y personales, a mis hijos Ackerley y Hillary quienes son el motivo de mi lucha diaria y quienes ven en mí, una figura de ejemplo de superación, a mis hermanos y amigos quienes me brindaron siempre todo su apoyo incondicional.

AGRADECIMIENTOS

Quiero agradecer en primer lugar a Dios, quien me dio las fuerzas, salud y sabiduría para poder llegar hasta este nivel académico, así como también a mi asesor ing. Eduardo Poletti, y demás docentes de mi maestría quienes demostraron su profesionalismo y volcaron sus conocimientos hacía mi persona para poder culminar satisfactoriamente esta investigación a quienes les merezco mi profundo respeto y admiración por siempre, y a la universidad César Vallejo por permitirme lograr otra de mis metas personales y profesionales.

DECLARATORIA DE AUTENTICIDAD DEL ASESOR

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, POLETTI GAITAN EDUARDO HUMBERTO, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "ISO 27002 y cumplimiento normativo en las sentencias de los juicios de los juzgados de familia, Lima 2023", cuyo autor es RUMICHE HUAMANI RUBEN EDUARDO, constato que la investigación tiene un índice de similitud de 12.00%, 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, 04 de Enero del 2024

Apellidos y Nombres del Asesor:	Firma
POLETTI GAITAN EDUARDO HUMBERTO **DNI:** 18073124 **ORCID:** 0000-0002-2143-4444	Firmado electrónicamente por: EPOLETTIG el 07-01-2024 17:25:51

Código documento Trilce: TRI - 0719737

INVESTIGA UCV

DECLARATORIA DE ORIGINALIDAD DEL AUTOR

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Originalidad del Autor

Yo, RUMICHE HUAMANI RUBEN EDUARDO estudiante de la ESCUELA DE POSGRADO del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "ISO 27002 y cumplimiento normativo en las sentencias de los juicios de los juzgados de familia, Lima 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

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

Nombres y Apellidos	Firma
RUMICHE HUAMANI RUBEN EDUARDO : 10381603 **ORCID:** 0000-0002-6864-131X	Firmado electrónicamente por: RRUMICHEH el 07-01-2024 23:54:49

Código documento Trilce: INV - 1461030

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente estudio de investigación se avocó en analizar las buenas prácticas que se enfocan en la norma ISO 27002, así como verificar si se ejecuta el cumplimiento normativo en la expedición de sentencias en los juicios llevados a cabo en la institución de administración de justicia en este caso, los juzgados de familia de Lima, 2023. La investigación fue de tipo aplicada dado que se inclinó en la búsqueda de sinceramiento de conocimientos buscando las soluciones a la problemática del presente estudio, se utilizó un diseño no experimental transversal descriptivo correlacional causal; se trabajó con una población de 7,300 expedientes judiciales de diferentes materias en la especialidad de familia del primer semestre del año 2023, utilizando una muestra de 366 expedientes, y se utilizó la ficha de datos como instrumento de recolección de información. Se obtuvo como resultado un nivel de confiabilidad de 0.778 en el Alfa de Cronbach lo que indica una fuerte confiabilidad con 44 indicadores evaluados, por otro lado; en los resultados de pruebas de normalidad se utilizó pruebas no paramétricas. Como conclusión se tuvo que la incorporación de la ISO 27002 y el cumplimiento normativo en los juzgados de Lima, tuvieron un impacto significativo en la expedición de las sentencias judiciales de los juicios de los procesos judiciales en la especialidad de familia de Lima, 2023.

Palabras clave: Norma ISO, cumplimiento, juicios, sentencias, seguridad.

ABSTRACT

The present research study focused on analyzing the good practices that focus on the ISO 27002 standard, as well as verifying whether regulatory compliance is executed in the issuance of sentences in the trials carried out in the institution of administration of justice in this case, the family courts of Lima, 2023. The research was of an applied type since it was inclined towards the search for sincerity of knowledge seeking solutions to the problems of this study, a non-experimental transversal descriptive causal correlational design was used; We worked with a population of 7,300 judiciales files of different subjects in the family specialty from the first semester of the current year, using a sample of 366 files, and the data sheet was used as a data collection instrument. The result was a reliability level of 0.778 in Cronbach's Alpha, which indicates strong reliability with 44 indicators evaluated, on the other hand; Non-parametric tests were used in the results of normality tests. In conclusion, it was concluded that the incorporation of ISO 27002 and regulatory compliance in the courts of Lima had a significant impact on the issuance of judicial rulings in the trials of judicial processes in the family specialty of Lima, 2023.

Keywords: ISO Standard, compliance, trials, sentences, security.

I. INTRODUCCIÓN

Según Rodríguez et al., (2020). Sostiene que muchas instituciones a nivel mundial, invierten grandes presupuestos en la puesta en producción de diversos sistemas informáticos con la finalidad de atender los procesos de sus negocios buscando tener un mejor lugar en el mercado, así como una excelencia con sus clientes y proveedores, los problemas recurrentes que afrontan las corporaciones públicas y privadas, es la seguridad de la información, a través, de diversas modalidades de intentos de intrusiones a sus sistemas, buscando vulnerabilidades tecnológicas así como humanas, uno de ellas es la falta de normas de seguridad en dichas organizaciones, Llano et al., (2018) indica que la responsabilidad de la aplicabilidad de una normativa, está en el chequeo constante y evaluación sobre el cumplimiento de estas.

Los constantes cambios de los procesos, en los diversos tipos de negocios como modificaciones, derogaciones, creación de nuevas leyes, decretos, resoluciones, directivas y otros, están expuestos también a nuevos riesgos en lo que compete a la seguridad de la información, dada la variedad de ataques que surgen, estas podrían buscar las debilidades del negocio con la finalidad de causar daños o pérdida de información. Para afrontar o reducir esto, es importante unas políticas de seguridad de la información buscando proteger al negocio frente a estos riesgos latentes.

A nivel nacional muchas organizaciones no se preocupaban por la seguridad de sus activos antes de la aparición de la pandemia del COVID19, dado que el porcentaje de los ataques de ciberdelincuentes no era frecuente, razón por la cual, sus inversiones las destinaban en otros temas sin mucha relevancia, pero con la aparición de la pandemia se vieron en la obligación de informatizar y automatizar sus procesos de negocio y este cambio fue afectado en la seguridad de la información por variados ataques por parte de los ciberdelincuentes quienes se han esforzado para buscar las vulnerabilidades informáticas de las organizaciones con la finalidad de causar graves daños, así como robo de información, entre otros (Rossi, 2021).

En el ámbito local ocurrió el mismo procedimiento, la aparición de la pandemia resaltó las vulnerabilidades de las instituciones, razón por la cual la actual investigación nació ante la falta de políticas, directivas o normativas del cuidado de los datos en los juzgados de familia de una entidad estatal, ya que se detectó en reiteradas oportunidades, ataques informáticos por parte de los colaboradores institucionales mal intencionadas, mal uso de los equipos y dispositivos informáticos, así como mala praxis de la información sensible de la entidad, para esto se planteó el uso de la norma ISO 27002 buscando regular, ayudar y reducir los riesgos que vienen afectando los procesos de la sentencias que expiden dichos juzgados, invocando a los usuarios a la utilización de mejores costumbres y prácticas para una correcta seguridad de la documentación en la institución. Asimismo, se investigó si la institución estatal contaba con procedimientos normativos relacionados a normas de seguridad, buenas prácticas, catálogos de seguridad, con la finalidad de ver su cumplimiento y eficacia en dichos estándares que pudieran existir.

Las diversas entidades tienen claro que la información es el bien más importante y de vital importancia para continuar con su negocio de acuerdo al rubro que desempeñen, para lo cual deben realizar un correcto control de acceso a ella, garantizando la integridad, confidencialidad y disponibilidad. El propósito de establecer el uso de la norma ISO ha sido, otorgar las medidas necesarias de control de seguridad a través de políticas que mejor se adapten a sus necesidades.

La entidad estatal encargada de administrar justicia en el Perú, es totalmente autónoma, la cual tiene por encargo de la carta magna, administrar justicia aplicando las normas y códigos vigentes con el fin de resolver con sus sentencias y fallos, conflictos judiciales entre sus diferentes especialidades; entre estas está la especialidad de familia, que se encarga de resolver problemas de sociedad conyugal, derecho alimentario, violencia familiar, autorización para disponer bien de menor, procesos no contenciosos, separación convencional, régimen de visitas, unión de hecho, tenencia, constitución de patrimonio familiar, autorizaciones de viaje de menor, infracciones de niños y adolescentes, entre otros.

Los juzgados de familia tutelar, penal y civil objeto de esta investigación, no contaban con una guía de seguridad de la información, situación que ha llevado en muchas ocasiones a ser vulnerables ante ataques voluntarios e involuntarios por parte del personal de la institución, tales como, fácil acceso a las áreas laborales, pantallas no bloqueadas, falta de seguridad en el ambiente donde se almacenan los expedientes, sistemas defectuosos, servidores deficientes, entre otros.

Por otro lado, se pretendió que la norma ISO 27002, sus controles y sus buenas prácticas puedan reducir significativamente los riesgos de ataques informáticos, así como los otros tipos de seguridad que invoca la norma en bien de la institución estatal de administración de justicia, así como el cumplimiento normativo de algunos estándares que pudiera tener la institución.

Como justificación de la investigación, se destaca la importancia de poner en práctica las regulaciones que se indican en la referida norma, lo cual tuvo como consecuencias mejoras considerables en el resguardo y custodia de la información de los expedientes judiciales, así como en los ambientes físicos de los juzgados de familia de Lima y creó una mejor conciencia de seguridad de la información con el personal que integra dichos órganos jurisdiccionales, por otro lado; la revisión de los estándares normativos que tiene la institución y su cumplimiento, reflejó un mejor control y manejo de la documentación, bienes materiales y otros, lo cual tuvo resultados positivos en la expedición de las sentencias judiciales.

La presente investigación aportará en lo sucesivo a los futuros investigadores, la importancia de tener un dispositivo tal como una norma ISO, el estándar ITIL, el marco de trabajo COBIT u otro que sirva como utilidad en la prevención y respuesta ante anomalías, ataques y/o falta de algún medio de resguardo a la parte más importante de toda organización que es la información, en este caso, nos enfocamos en la norma ISO; así como a la importancia que tienen las normativas organizacionales y su cumplimiento.

Bajo los puntos antes referidos se identifica como problema general lo siguiente: ¿La norma ISO 27002 y el cumplimiento normativo se relacionan en las sentencias de los juicios de los juzgados de familia de Lima 2023?

Como problemas específicos tenemos: ¿En qué medida las directrices de la seguridad de la información, se relacionan con las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023? y, ¿Cómo los procedimientos y vigencia se relacionan con las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023?

El objetivo general investigado fue: Determinar la relación de la ISO 27002 y el cumplimiento normativo en las sentencias de los juzgados de familia en una entidad judicial de lima, 2023. Y como objetivos específicos tenemos: Determinar la relación que existe en las directrices de la seguridad de la información, en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023. y como segundo objetivo: Determinar la relación que existe con los procedimientos y vigencia en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023.

Como hipótesis general se planteó lo siguiente: Existe una relación significativa entre la ISO 27002 y el cumplimiento normativo en las sentencias de los juicios de los juzgados de familia, en una entidad judicial de Lima, 2023; y como hipótesis específicas: Existe una relación significativa entre las directrices de la seguridad de la información en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023; y Existe una relación significativa con los procedimientos y vigencia en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023.

II. MARCO TEÓRICO

Se indican algunos antecedentes con relación a las variables identificadas en la presente investigación:

En el campo internacional el investigador Gumucio (2021) en su estudio realizado en el país sureño de Chile, determinó como objetivo las estrategias en la evolución de la ciberseguridad para evitar fugas de información financiera, para esto se apoyó en el uso de mejoras continuas en seguridad de la información, así como en la evaluación de riesgos, manejó la metodología cuantitativa para los campos observables y estadísticos, y llegó a la conclusión de que existe una grieta perceptible entre los países que conforman Latinoamérica, para la valoración y ordenamiento en la seguridad de la información.

Según Joshi (2017) dicta que los datos se consideran extremadamente importantes y la universidad debe prevenir violaciones de seguridad. Este artículo analiza las amenazas de seguridad específicas que existen en las redes universitarias y propone un marco de extremar la seguridad de los datos para entornos de redes universitarias en respuesta a estas cuestiones. El marco propuesto reduce el riesgo de violaciones de seguridad al respaldar tres pasos; la primera fase evalúa amenazas y vulnerabilidades para identificar debilidades en el entorno educativo, la segunda fase se centra en los riesgos más altos y desarrolla planes de mitigación viables, y la tercera fase, el Modelo de Evaluación de Riesgos, reconoce los requisitos de cumplimiento para la gestión de vulnerabilidades para mejorar el cumplimiento en el entorno educativo. Seguridad Universitaria. El marco propuesto se implementó en el entorno informático de la Universidad Vikram de Ujjain, India, y el producto del análisis demuestra que el marco propuesto mejora el nivel de seguridad de las redes del campus. Los analistas de riesgos y administradores de seguridad de las universidades pueden utilizar el modelo para realizar análisis de riesgos confiables y repetibles de una manera realista y rentable.

Según Díaz (2021), estudios previos a nivel nacional muestran que este estudio examina la asociación de la norma ISO 27001:2014 (la cual se relaciona con la ISO 27002 donde se detallan las buenas prácticas que sirven para un desempeño adecuado de los datos), en los centros gubernamentales peruanos. El problema son los ataques informáticos cada vez más complicados. El método

utilizado fue cuantitativo, examinando una muestra de 76 colaboradores públicos, y se encontró que aproximadamente el 50% pensó que la norma estaba incluida. Se destacó la necesidad de la ciberseguridad y cuidado de la información en diversas entidades, teniendo presente que cada vez se presentan amenazas de mayor riesgo integral.

Muñoz (2018), en un estudio sobre la seguridad y evaluación de peligros de las políticas del SI, mencionó que su investigación fue básica, utilizó un diseño no experimental e intentó dos estudios transversales de antes y después para recopilar lecciones aprendidas. La población y la muestra analizada utilizan los 11 fundamentos de dominios de seguridad de TI del estándar ISO 27002. La conclusión también se aplica a las dimensiones del proyecto, a saber, la disponibilidad, confidencialidad e integridad en 6 instituciones, ya que son partes esenciales e importantes para la evolución de la empresa y, por lo tanto, mejoran el acatamiento de las políticas buscando corregir las etapas de mitigación de riesgos o la gestión de riesgos hasta un nivel aceptable, o los denominados riesgos aceptados.

Según Mucha y Lora (2019) en su estudio se centra en la experiencia de la formación profesional en las aulas de pregrado y posgrado, así como en el desarrollo de la estadística y temas de investigación. Los métodos de muestreo en la investigación cuantitativa tienen un objetivo básico: garantizar la representatividad. En este sentido, deben interpretarse según un enfoque cognitivo para comprender su significado. Asimismo, su clasificación también se relaciona con las variables de investigación en función de su carácter cuantitativo y cualitativo. ¿Pero es necesario asignar una probabilidad a las unidades muestrales? Si las variables de investigación son cuantitativas y cualitativas, las muestras se obtendrán mediante modelos matemáticos finitos e infinitos. En ambos modelos se determinó el tamaño de muestra óptimo que se debe aplicar para las pruebas de muestreo.

Castillo (2022) Indica que desarrollar aplicaciones web y móviles para la tarea de peligros de los activos utilizando métodos adecuados en el marco de las reglas de control de la información de la unidad de negocio de consultoría de sistemas. El estudio recomienda gestionar y proteger los datos de la empresa

contra los riesgos de pérdida, fuga, indisponibilidad o alteración. Para ello se estudiaron los métodos que se enfocan con el resguardo de la data existente y los estándares internacionales de calidad, se eligió el método MAGERIT y se examinaron las normas ISO, luego se desarrollaron aplicaciones web y móviles para tratar de contrarrestar los ataques informáticos. La elaboración de la aplicación se realizó utilizando métodos ágiles de elaboración de software, siguiendo el proceso de fortalecimiento del programa, el cual se detalla junto con los aspectos técnicos y funcionales en este estudio. Luego del desarrollo de la aplicación, se implementó la propuesta en una empresa consultora de sistemas que desarrolló políticas y actividades para la valoración de peligros de la información, donde se utilizó como prueba piloto del sistema la implementación de la aplicación propuesta por la empresa consultora. El sistema INFORISK propuesto fue evaluado a través de un estudio de usuarios, y se logró una calificación aceptable para el soporte del sistema, logrando así los objetivos del estudio.

Según Gonzales y Sarmiento (2019). Indicaron que el motivo de su estudio fue verificar cómo la ejecución de la norma NTP/ISO 27001 mejoró los métodos de custodia de la información en las oficinas de telemática del ejército del Perú. El análisis evaluado es de tipo aplicada, ya que busca dar solución al problema propuesto, y de nivel explicativo, ya que su finalidad es esclarecer la causa y efecto de la búsqueda del problema, por lo que su diseño es pre experimental. La población para dicho estudio fueron todas las etapas del departamento de telemática y como muestra se tomó el proceso de la prevención de datos y el método de muestreo fue aleatorio simple. Se utilizó la norma técnica peruana mencionada líneas arriba. El resultado del estudio fue una mejora considerable en los procesos de prevención en el área descrita. Se desarrollaron 15 entregables estandarizados, la implementación de la norma referida, mejoró significativamente los casos materia de investigación en la entidad castrense.

Según Silva et al.,(2017) el propósito de su estudio fue examinar en qué medida las PYMES llevan a cabo la prevención de ataques informáticos y descubrir los factores que influyen en la adopción de medidas de gestión para la seguridad de las entidades. Se realizó un estudio descriptivo exploratorio con diseño de encuesta. La muestra está compuesta por 43 industrias manufactureras de

productos metálicos ubicadas en la gran región ABC. Con base en la literatura de gestión del resguardo de la información y los estándares brasileños, las herramientas o técnicas se identifican y dividen en tres niveles: físico, lógico y humano. Las investigaciones han descubierto que el aspecto humano es el aspecto más ignorado por las empresas, seguido del aspecto lógico. El antivirus es la herramienta/tecnología más utilizada por las empresas encuestadas para asegurar la confianza de la información. Las investigaciones muestran que el 59% de las empresas encuestadas tienen un nivel satisfactorio de seguridad, y el principal factor impulsor es "evitar posibles pérdidas financieras". Todos los inhibidores resultaron ser importantes para las empresas encuestadas: falta de conocimiento, valor de la inversión, dificultad para evaluar costos/beneficios y cultura organizacional.

Viena (2020), Indica que su estudio tuvo como tarea poder indicar la relación entre el cumplimiento de la norma y la satisfacción de los usuarios del segundo hospital de Tarapoto, Essalud en el año 2020. Se recomendó un diseño de correlación descriptivo básico, transversal y no experimental, Se incluyeron 20 pacientes que fueron encontrados en el servicio de urgencias del nosocomio en los primeros meses de 2020. Se utilizó una muestra aleatoria de 20 pacientes, utilizamos encuestas como técnicas de recolección de datos y cuestionarios como herramientas; Concluyó que existe correlación entre el cumplimiento de la norma y la satisfacción entre los usuarios del segundo hospital de Essalud Tarapoto en el año 2020 debido a la correlación de Pearson. El coeficiente es 0,746 (correlación altamente positiva) y el valor es igual a 0,000 (valor $p \leq 0,05$).

Según Lykhova et al., (2022), Dicta que su estudio se centró en la seguridad de la información como estado social, sus aspectos y características, los estándares y su impacto en la mejora de los procesos en cuestión. Enfatizar el carácter interdisciplinario, la investigación utiliza una diversidad de métodos, incluida la lógica formal y la estructura sistemática, métodos de generalización y métodos comparativos. El análisis de documentos se utiliza para comprobar el desempeño legal y los estándares internacionales y nacionales más importantes en este campo. Hay tres niveles: personal, social y nacional. La conclusión es que estos niveles difieren según su nivel en el espacio de información.

Stoica (2018), indica que el objetivo del cuidado de los datos informáticos es recopilar, organizar, limpiar y manipular eficazmente la totalidad de la información disponible de la empresa. Durante el pasar de los años la ciencia ha evolucionado desde simples sistemas de informes hasta sistemas integrados a medida que las empresas se esfuerzan por utilizar la información empresarial de forma eficaz.

Según Otoya (2018) El propósito de seguir trabajando es garantizar la personalización de los riesgos de la tecnología de la información, es decir, se debe realizar una "gestión de riesgos" adecuada del Informe sobre el desarrollo de la producción agrícola de 2017. La Gestión de Riesgos en TI proporcionará a los profesionales de TI una mejor gestión de la tecnología al tener las herramientas para tomar mejores decisiones en escenarios de riesgo y amenazas. Incluye los motivos y fuentes de los riesgos de TI, sus resultados positivos y negativos y la contingencia que puedan ocurrir. Este tipo de gestión de riesgos de TI le permitirá determinar el valor y el tamaño de los activos y la probabilidad de impacto de amenaza o riesgo de ejecución para implementar completamente la prevención y garantizar la continuidad del negocio. Por lo tanto, este estudio midió el impacto de la gestión de riesgos de tecnologías de la información en proyectos de desarrollo rural en 2017.

Según Carvajal et al., (2019) Nos dice que la información hoy en día es lo más importantes en las entidades como parte principal para los procesos, sino también como un recurso que, si se gestiona apropiadamente, puede definir la estrategia de una organización lo que no es ninguna novedad en el sector público. El propósito de este artículo es aplicar varios estándares que tengan que ver con seguridad de la información (ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 27003:2010 e ISO/IEC 27005:) después de su revisión y su situación específica en Colombia, desde los lineamientos desarrollados por una entidad pública. Como resultado, se desarrolló un enfoque adaptado a las necesidades de las entidades públicas, que incluye medidas e indicadores de gestión de riesgos y controles relacionados para reducir los peligros invasivos en la información. El valor agregado de este trabajo tiene que ver con la unificación de estándares en la SI y su concreción en entornos gubernamentales, que cumplen con los requisitos de las leyes regulatorias y brindan el avance metodológico relacionado luego de la

finalización de su implementación, permitiendo a las organizaciones públicas promover tareas periódicas en seguridad de la información.

Atencio (2019) planteó que los cambios tecnológicos y su uso en la administración general de las tecnologías de la información y las estadísticas se ven afectados por software malintencionados e incluso por colaboradores de la institución que carecen de conocimiento, y esta queda expuesta a grandes amenazas que podría comprometer la transferencia de los datos de las redes informáticas de la organización. La investigación es no experimental, por lo que la información se recopila en base a un estudio de 8 socios comerciales del sector de TI en general, considerados tanto como población como muestra. Asimismo, los resultados arrojan resultados previos a la implementación del SGSI, el conocimiento era del 9.1%, mientras que después alcanzó el 90% del conocimiento en seguridad de la información se logró mediante la creación de documentos normativos. Por último, se concluyó que, al elaborar un módulo de gestión de la seguridad de la información, el objetivo debe ser aminorar la complejidad de la seguridad de la información, y sus activos, así como no solo deben centrarse en los factores que la afectan. Puestos de seguridad, así como recursos de información estratégica y cultura organizacional.

Según Chopra, et al., (2020), proteger la información es un gran desafío. Esto incluye proteger no sólo sus datos, sino también de las entidades cuyos sistemas almacenan gran cantidad de información. Aceptamos que las organizaciones conserven nuestra información y ellos a su vez, tienen la responsabilidad de resguardarla para que no sea utilizada por terceros mal intencionados. Además, los competidores pueden robar la información de la organización. Los sectores particularmente vulnerables son la banca, el sector automovilístico, la aviación y las telecomunicaciones en la venta de software y hardware.

Mientras que Ortiz (2018) mencionó que el objetivo es poner en función progresivamente la norma ISO 27002 para la gestión de los datos en la universidad de la amazonia Peruana. En su análisis utilizó un diseño cuasiexperimental porque el grupo de control se realizó en el mismo conjunto de estudios. Se puede confirmar con un 95% de confianza en la gestión de los datos en la universidad indicada se

puede mejorar mediante la ejecución de componentes de seguridad de establecidos en la norma ISO.

Fernández (2021) Indica que, su análisis fue dirigido en el entorno de justicia penal y tuvo como objetivo verificar si la práctica del estándar de cumplimiento normativo puede reducir la alteración en el municipio distrital de Nuevo Chimbote. Para esto, se escogió la mencionada entidad distrital como unidad de análisis; la muestra fue de 7 colaboradores. Dado que la investigación fue básica, el enfoque se desarrolló como descriptivo y explicativo, utilizando un diseño no experimental y un enfoque fenomenológico, además, se utilizó técnicas de entrevista como guía. La conclusión que se logró como resultado, es que los colaboradores opinan que la corrupción es un daño constante dentro de la Municipalidad por lo que la idea de poder practicar el cumplimiento normativo sería necesaria para que se obedezcan y cumplan las normas legales ya dictadas y puedan ser castigados los que la incumplan.

Astudillo (2021) propuso un grupo de elementos que permitan un acercamiento conceptual y teórico al principio de transparencia como directriz para el manejo de las funciones públicas y al derecho de poder acceder a la información dentro de las instituciones democráticas como expresión directa de este principio.

Beramendi (2021) se enfocó en el transporte público que requiere regulación y libertad de control de los usuarios para establecer un ambiente adecuado. Las desviaciones sociales crean un ambiente incómodo y estresante para los pasajeros. El propósito de esta tarea es narrar las reglas conocidas por los pasajeros del metro de Buenos Aires, explorar las percepciones de desistimiento de dichas reglas y analizar la interacción entre los pasajeros y cómo se relaciona con el incumplimiento. Los colaboradores experimentaron altos niveles de incumplimiento, el inconformismo refleja la existencia de reglas informales que rigen el comportamiento de los pasajeros que va en contra de lo establecido. Esto genera problemas durante el trayecto del viaje y ocasiona negativamente las interacciones de los pasajeros y crea una atmósfera social de malestar y tensión.

Manihuari y Vergaray (2022) afirman que el objetivo de su estudio fue fortalecer la información de la compañía CGS MÁXIMA S.A.C, ofreciendo un

modelo de protección informática; su análisis fue de tipo aplicada y diseño preexperimental. La muestra fue de 10 trabajadores. Los resultados muestran que el grado de confidencialidad de la información aumentó en 3,03 puntos (60,60%), el nivel de integridad, aumentó en 2,96 puntos (59,20%), el Nivel de disponibilidad, se acrecentó en 3,23 puntos (64,60%), lo que es un buen efecto al implementar la solución expuesta. Se estableció que el modelo de protección informática propuesto, optimizó la seguridad en los datos de la empresa mencionada.

Bonilla (2021) investigó las consecuencias del uso de las normas ISO 27001 y 27002 y la información eficaz en la un área administrativa de la autoridad policial Peruana. La pesquisa se enfocó en un diseño cuasiexperimental ya que el estudio se realizó en dos grupos, el primer grupo fue una prueba previa y el segundo grupo fue una prueba posterior.

Agüero et al., (2022) comentan que el propósito de su artículo es mostrar tres condiciones que afectan la claridad del lenguaje y de las decisiones judiciales, principalmente en dos áreas: medidas de protección y falta de servicio. La primera es la falta de una estructura fija de razonamiento que sirva como principio para una correcta organización. La segunda es la ausencia de una tarea asignada a los considerandos que forman la sentencia. El tercero es la falta de explicación de las técnicas de interpretación e integración jurídica utilizadas por los jueces. Se ofrecen soluciones para cada uno de estos problemas.

Zambrano et al., (2022) considera que los casos judiciales suelen resolverse a través de una sentencia, textos que son géneros típicos de discurso en el ámbito jurídico (Agüero, 2014). Estos argumentos son orgánicamente legítimos e imputan diferentes tipos de sanciones a sus destinatarios. Es más, siempre dicen algo sobre una persona o un evento (Van Dijk, 1980), porque contienen hechos que justifican el uso de normas jurídicas. Por lo tanto, son instrumentos de diversos conceptos y opiniones que encarnan la forma en que el derecho entiende y define la sociedad.

Gutiérrez et al., (2022) la información denominada ESG (Gobernanza Social Ambiental) especificada en los objetivos de desarrollo sostenible está adquiriendo cada vez más importancia en la economía mundial y ayuda a aumentar la transparencia organizacional. En consecuencia, la normativa europea y española

obliga a las organizaciones a incluir en sus informes sobre aspectos medioambientales, sociales y de gobierno corporativo. Este estudio se enfocó en revisar las normas de las empresas españolas en cuestiones medioambientales, sociales desde una perspectiva interdisciplinaria jurídica y económica. Mediante investigación exploratoria, descriptiva y analítica, se realizó un estudio cualitativo entre diciembre de 2015 y diciembre de 2019 sobre la relación entre las prácticas comerciales adversas que constituyen actividades delictivas y su impacto en los objetivos de sostenibilidad. Los resultados en la prevención de riesgos en los procedimientos de presentación de informes y auditorías que cumplan con la legislación de gobernanza social ambiental (ESG). Al analizar las sentencias del Tribunal Supremo (TS) español, es evidente el impacto negativo de la delincuencia empresarial en una serie de ODS y objetivos que afectan a las cinco áreas principales del programa de desarrollo (las cinco P´s). Una valiosa fuente de información cuantitativa y cualitativa para incluir en los "estados financieros" y los informes globales de una empresa.

Vivanco y Quintana (2019) indicaron que existen problemas en la administración de los activos de la Universidad Iberoamericana en Ecuador, debido a la falta de documentación adecuada que ayude a encontrar la mejor solución para evitar la alteración de la información financiera y académica. Por lo tanto, se considera un estudio descriptivo, ya que se identifican los riesgos de los medios de información y se determinan los métodos de tratamiento adecuados. Además, se estima que el tipo de población restringida cubre un total de 44 personas en la unidad administrativa, de las cuales 27 personas fueron informadas sobre el uso de medios de información durante el muestreo rutinario o intencional. Los resultados de la información, a su vez, permiten identificar debilidades y fortalezas que afectan la implementación de un sistema seguro. Para ello, comenzamos con la cultura empresarial de seguridad informática de los empleados y su impacto. Este es el caso cuando las amenazas integran activos de información. A juzgar por el porcentaje de resultados basados en las vulnerabilidades descubiertas, el 81% del conocimiento sobre los problemas de la información se obtuvo que, a partir del 19% de existencia inicial y el 100% de las amenazas existentes se mitigaron. La conclusión final es que el diseño del SGSI mejora la calidad y la competitividad del proceso en función de los riesgos.

Nacipucha (2019) señala que, como realidad problemática, la organización Arte Hogar no brinda una gestión de la información basada en estándares de seguridad de la información, ya que esto la hace vulnerable a las amenazas existentes, planteando los siguientes interrogantes: Cómo implementarlo utilizando la aplicación ISO 27001: ¿estándar de diseño del modelo SGSI? El tipo de investigación es de campo, pues se avoca a la recopilación de datos por medio de la observación, donde cada proceso se desarrolla en interacción con los empleados. Además, el tipo de población se consideró limitado. Se consideraron 40 contribuyentes en 8 muestras, por lo tanto, los hallazgos del estudio fueron que la empresa era vulnerable a ataques debido a la desinformación de los empleados sobre cuestiones de seguridad informática, y las entrevistas con los coordinadores de TI revelaron que la empresa carecía de una política de seguridad. Cabe señalar que este porcentaje se logra porque el 75% de las personas considera de importancia crítica la seguridad de la información. Finalmente, se señaló que Arte Hogar debe proteger constantemente todos los activos relacionados con la información definiendo métodos de seguridad.

Martínez (2019) Indica en su publicación en España, sobre el análisis del efecto de la IA en la legislación y los derechos básicos fundamentales enfrentando opiniones nada positivas, reactivas o desastrosas; propone una solución enfocada en un cumplimiento normativo, desde sus bases iniciales, optando por la metodología en enfoques de diseño y estándar de protección de datos.

Según Motii (2017) refiere que, a pesar del gran número de opciones disponibles, ha habido considerable confusión sobre los diferentes métodos utilizados por el administrador de TI debido a su falta de información. En su artículo tuvo como objetivo estudiar la importancia del gobierno de TI y proponer un nuevo enfoque para agrupar las referencias ITIL, COBIT con ISO/IEC 27002 para un mejor uso del gobierno de tecnologías de la información en el parlamento Marroquí. Este último es considerado como un conjunto de organizaciones con la tarea de responsabilidades legislativas, control gubernamental, evaluación de políticas públicas, diplomacia y fortalecimiento de las relaciones parlamentarias con instituciones constitucionales, buena gobernanza, desarrollo regional avanzado talleres, sociedad civil y ciudadanía. Asimismo, su investigación arrojó la respuesta

a una pregunta clave: ¿si el gestor de la información debería depender de las funciones del parlamento Marroquí o debería prever objetivos más amplios y evolutivos que afectan a todo el gobierno?

Ortiz (2018) indica que su finalidad fue implementar paulatinamente la ISO 27002, la cual estableció las pautas preventivas en los datos de una Universidad de la región selvática Peruana. Este estudio utilizó un diseño cuasiexperimental porque el grupo de control se realizó en el mismo conjunto de estudios. Pudo confirmar un 95% de confianza que la gestión de seguridad en la universidad en mención se puede mejorar mediante la práctica de los controles de la norma acotada.

Según Jufri (2017) refiere que la seguridad de los activos es esencial para salvaguardar la seguridad de la información debido a las amenazas a la confidencialidad, la integridad y la disponibilidad en el almacenamiento y uso de estos activos. La Universidad Langlangbuana exige protección de su activo de información, su sistema de información académica (AIS), que gestiona principalmente información confidencial con fines académicos. El objetivo del estudio fue realizar una estimación de riesgos en el activo AIS utilizando el marco OCTAVE Allegro, así como en las aplicaciones de control de seguridad utilizando las cláusulas de la norma ISO 27002. Como resultado, las políticas recomendadas por este estudio podrían ser útiles para la universidad y sus mejoras futuras.

Según Gonzales y Macedo (2020). Indican que los grupos sociales han abierto nuevas oportunidades para el tratamiento de la información, el alto contenido que se produce diariamente, trae desafíos en los diseños e indicadores, procedimientos y técnicas para medir la información, detrás de estos temas se reflejan teorías y muestras de con origen en las ciencias de la información, de las comunicaciones y de la informática, estos tres campos convergen en el diseño de las TI y las telecomunicaciones con relación a las personas.

Triana y Moreno (2021) advierten que la gestión documental es un factor clave que ayuda a decidir sobre los activos de las instituciones, esto con la finalidad de colaborar en el uso de los datos y una mejor posición económica y social, competitivo y adaptado a los cambios, con un diseño descriptivo con enfoque mixto,

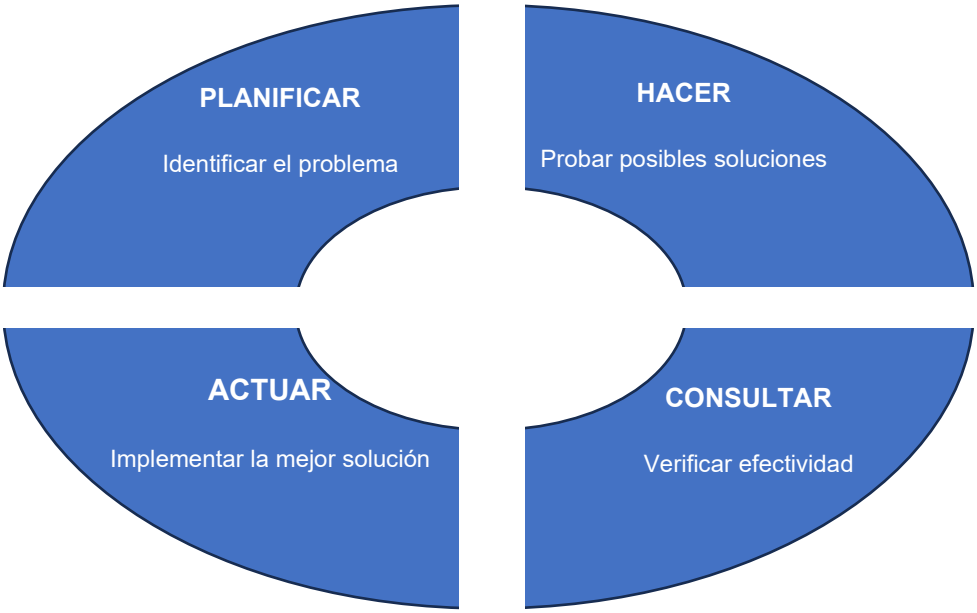
enfocándose en las buenas prácticas para armonizar íntegramente sus sistemas, y teniendo como resultado la identificación de zonas de inflexión y un modelo de procedimientos de armonización.

Fonseca (2022) indica que la preocupación principal de las entidades que administran justicia denominados órganos jurisdiccionales, tiene como objetivo descubrir la calidad de las medidas judiciales dictadas y para esto deben tener en cuenta la eficiencia, productividad, el grado de satisfacción y otros indicadores por parte de los litigantes, así como de sus usuarios en general, tomando el diseño de calidad argumentativa lo cual dio como resultados que el grado de calidad, no es óptimo por la falta de claridad y razonamientos débiles.

Leguizamón et al., (2020) manifiesta en su investigación sobre el análisis de ataques informáticos con “sistemas trampa” conocidos también como honeypots en la universidad distrital de Colombia, que dicho procedimiento tuvo como objetivo una alternativa complementaria a la seguridad informática en la organización para lo cual se trabajó utilizando el ciclo PDCA (Planificar – Hacer – Verificar – Actuar). Lo que es un modelo de diseño enfocado en técnicas de mejoras, con aplicaciones fáciles de usar y muy útiles en actividades productivas y administrativas, y tuvo como resultados luego de la implementación de dichos “señuelos” poder identificar diferentes modalidades de ataques informáticos, lo cual permitió crear reglas y encontrar fallas para poder establecer soluciones efectivas.

Figura 1.

El ciclo Planificar Hacer Consultar y Actuar



Fuente: https://safetyculture.com/es/temas/ciclo-pdca/

El uso del ciclo PDCA proporciona pautas simples para gestionar actividades y procesos. Es la estructura básica del sistema y puede usarse en cualquier organización.

Alarcón, et al., (2020) señala en su investigación que el progreso tecnológico global ha permitido procesar información crucial y relevante para los objetivos estratégicos de la organización. La razón de la investigación es verificar el impacto de la aplicación de la norma ISO 27001 en la seguridad de la información en una organización privada de Lima Perú. Basado en la aplicación de métodos cuantitativos, se realizó un diseño pre experimental donde se determina el impacto de la aplicación de la mencionada norma. Para ello se tuvo en cuenta una muestra de 30 colaboradores de la organización. Los resultados cuantitativos muestran que el empleo de dicha normativa afecta la seguridad de la información, así como las confidencialidad, integridad y disponibilidad.

Farida et al., (2021) mencionan que un sistema robusto de una corporación contable puede agregar su valor mejorando la eficiencia y eficacia de la cadena de suministro, optimizando y mejorando la toma de decisiones. En este estudio, se utilizó el método de muestreo intencional como punto de partida y se realizó una encuesta entre 51 empleados de unidades contables de ministerios e instituciones.

Los datos se analizaron mediante modelado de operaciones estructurales utilizando el software Lisrel 8.80. Los resultados muestran que la implementación de sistemas de datos contables tiene un buen desempeño de la organización a través de la calidad financiera.

Sandoval (2019) en su investigación del modelo de buenas prácticas utilizando la norma ISO 27002 en la red Wncor con el objetivo busca implementar de un modelo de buenas prácticas de la norma ISO 27002 en beneficio de las redes de la empresa investigada, El método que se utilizó fue científico y de investigación, el nivel apropiado de estudio y el diseño del estudio es pre experimental. El estudio se realizó con 500 individuos de los cuales se expuso una muestra probabilística de 40 usuarios. El resultado fue que se mejoró el manejo de incidentes en las redes de Wncor implementando un diseño de buenas prácticas utilizando la citada norma.

Ormaza (2020) en su estudio denominado Ataques informáticos en tiempos de pandemia indica que el objetivo es realizar una investigación sobre intrusiones informáticas más frecuentes que se suscitaron durante la pandemia del Covid19 en América Latina, tuvo un diseño de investigación bibliográfica con una tarea importante donde se establecieron diversas opiniones de búsqueda concernientes a la seguridad de la información, ciberdelincuencia y riegos digitales a fin de establecer qué documentación debería ser revisadas, lo cual trajo como resultado la identificación de los ataques y posteriormente un oportuno estudio de la información obtenida y con esto se observó la terrible situación que venían padeciendo los países, como resultado que se consiguió definir a través de esquemas, la frecuencia de ataques concentrados.

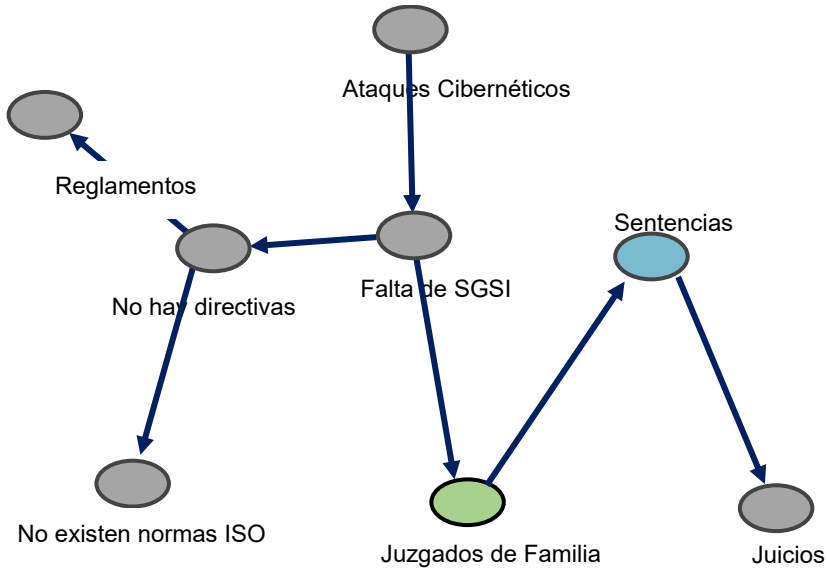
Infante, et al, (2021) su investigación se basa en una evaluación de cómo se manejan los casos de difamación en ausencia del acusado. Para solucionar este problema, se apoya en una serie de actividades educativas, que son herramientas ideales para mejorar este proceso en diversas instituciones jurídicas nacionales e internacionales, fueron usados los diversos métodos como: nivel teórico, deductivo, sintético y sistémico; a nivel empírico se encuentran la observación científica, la encuesta, asimismo se utilizó la estadística descriptiva e inferencial. La finalidad es valorar la certeza de las actividades educativas para favorecer los procesos legales de difamación en ausencia del demandado. Se utilizó un diseño pre experimental

utilizando una prueba inicial y otra final. En los alcances obtenidos, se pueden confirmar la necesidad de dicho estudio, que muestre el nivel de efectividad de las actividades educativas implementadas.

Para el desarrollo del marco teórico se evaluó los bienes informáticos que son utilizados en los juzgados de familia, así como el software con que cuentan, los dispositivos legales y herramientas que utilizan para la salvaguardar la seguridad de la información, se encontraron algunos equipos antiguos, sistemas operativos sin soporte técnico en línea de parte del fabricante, falta de actualizaciones, y antivirus deficiente administrado por un tercero. Sumado a ello, no se cuenta con directivas, normas, reglamentos u otro acto administrativo, donde se indique el procedimiento que se debe realizar para proteger la información de la empresa.

Figura 2.

Realidad problematica



FUENTE: Confeccionado por el autor – Software DAGitty

Asimismo, se encontraron gran parte de las computadoras que son utilizadas por los juzgados de familia, con un único usuario y contraseña para todos estos equipos, solo siendo su identificativo, el IP de cada terminal, lo cual es una puerta abierta para cualquier ciberataque que podrían estar expuestos estos equipos.

Bajo estos detalles antes descritos se pretendió ver cuál es el impacto de acotada norma antiguamente llamada ISO 17799, la cual es un estándar para la efectividad y control de la información que se basa como se muestra a continuación.

Figura 3.

Estructura Norma ISO 27002

Fuente: Elaborado por el autor

Figura 4.

Pilares de Seguridad de la Información

Fuente: https://pmi-levante.org/la-ciberseguridad-en-la-gestion-de-proyectos/

Se estableció la fórmula matemática simple para representar la relación entre la norma ISO 27002, el cumplimiento normativo y las sentencias judiciales de los órganos jurisdiccionales de la especialidad de familia. Supongamos que:

- N representa el grado de cumplimiento de la norma ISO,
- C es el nivel de cumplimiento normativo y
- S es el número de sentencias relacionadas con el incumplimiento normativo. Podríamos expresar la relación de la siguiente manera:

$$S = f\,(N, C)$$

Donde f es una función que describe la relación entre las variables. Esta función puede variar según la naturaleza específica de la relación que estás considerando. Podría ser algo como:

$$S = a \cdot N + b \cdot C$$

Aquí, a y b son coeficientes que determinan la contribución relativa de N y C a la variable S. Pueden ser valores positivos o negativos dependiendo de cómo influyen en el número de sentencias.

Posteriormente procedimos a desglosar a modo de ejemplo una variable en sus indicadores, para lo cual lo representamos de la siguiente manera:

- N es la variable que desglosaremos en dos indicadores I_1 e I_2. Lo cual se expresa de la siguiente forma:

$$N = w_1 \,.\, I_1 + w_2 \,.\, I_2$$

Aquí w_1 y w_2 son los pesos o coeficientes que representan la contribución relativa de I_1 e I_2 a la variable N. Estos pesos pueden ser positivos o negativos según la dirección de la influencia.

Esta fórmula es bastante simple y genérica. En aplicaciones del mundo real, la relación entre estas variables podría ser más compleja y requerir un modelo matemático más sofisticado.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

3.1.1 Tipo de investigación:

Se basó en una investigación aplicada ya que se abocó en la búsqueda y sinceramiento de conocimientos a fin de encontrar soluciones a la problemática que se encuentren en la presente investigación. Abarcó un enfoque cuantitativo ya que el método de investigación y procedimientos fue secuencial.

3.1.2 Diseño de Investigación:

Este estudio fue diseñado como no experimental transversal descriptivo correlacional causal. Esto se debe a que la investigación se llevó a cabo sin manipular las variables, lo que significa que este estudio examina casos ya existentes y no los creó el investigador (Hernández et al., 2014) y se enfoca en la observación de los datos y eventos para después revisarlos.

3.2 Variables y operacionalización

Variable 1: ISO 27002, es una variable independiente de tipo cuantitativa. En el anexo 1 se encuentra la matriz de operacionalización de esa variable.

Variable 2: Cumplimiento normativo, es una variable independiente de tipo cuantitativa. En el anexo 1 se encuentra la matriz de operacionalización de esa variable.

Variable 3: La variable dependiente de tipo cuantitativo es sentencias. La matriz de operacionalización de esa variable se encuentra en el anexo 1.

3.3 Población, muestra y muestreo

3.3.1 Población:

Según Arias et al., (2021) la población se concreta mediante el agrupamiento restringido o no restringido de sujetos o miembros con características similares. La población estuvo constituida por expedientes judiciales de la especialidad de familia pertenecientes al distrito judicial de Lima, entre los cuales se analizó su estado como apelación, archivo definitivo, con ejecución concluida, con ejecución consentida, en ejecución,

en calificación, en plazo de apelación, en plazo de impugnación, en trámite de ejecución, exhorto para diligenciar, para sentenciar, para resolución y sentenciado y/o resuelto entre otros. Para poder establecer el tamaño de la población se ha tomado algunos criterios que son los siguientes:

- Criterios de inclusión: Se analizó los expedientes que se encontraban en los ambientes de los juzgados de familia del distrito de Lima, en un rango de dos meses de antigüedad una vez calificados y mientras se ejecuta su proceso o trámite.
- Criterios de exclusión: Son excluidos de la presente investigación los expedientes de la especialidad de familia del distrito de Lima, que se encontraban en la mesa de partes, vale decir, desde su llegada a la sede judicial y permanecían en proceso de verificación, digitalización u otro trámite que se realice en dicha área, así como los expedientes que se encontraban en archivo definitivo o remitidos al banco de expedientes judiciales de la sede pública judicial.

los criterios de inclusión y exclusión ya descritos, se determinó el siguiente tamaño de la población:

N = 7,300 expedientes judiciales

3.3.2 Muestra

Según Hernández et al., (2014), señaló que la muestra es una porción de la población objetivo o universo y se usa para economizar los tiempos y recursos para obtener resultados.

Para determinar el volumen de una parte de la población conocida, se aplicó la fórmula de media poblacional, la cual tiene los siguientes parámetros:

n = tamaño muestra necesaria

Z = Nivel de confianza 95%

S = Desviación estándar

N = Tamaño de población

E = Error de precisión 5%

$$n = \frac{NZ^2S^2}{(\mathrm{N}-1)e^2 + Z^2S^2}$$

El siguiente tamaño de muestra se calculó utilizando la fórmula anterior y los parámetros mencionados:

n = 366 expedientes judiciales

3.3.3 Muestreo:

Probabilístico aleatorio simple.

Otzen y Manterola (2017) indican que los métodos de muestreo probabilístico permiten comprender la probabilidad de que cada sujeto sea incluido en la muestra mediante selección aleatoria; la selección aleatoria simple es porque garantiza que todos los participantes del grupo objetivo tengan las mismas posibilidades de ser tomados en cuenta para la muestra.

3.3.4 Unidad de análisis:

Expedientes judiciales.

3.4 Técnicas e instrumentos de recolección de datos.

Hernández et al., (2014) comenta que la confiabilidad de un elemento de comprobación del grado en que produce los mismos resultados cuando administra repetidamente la misma persona, universo u objeto.

Técnica: análisis documental.

Instrumento: Ficha de datos.

Validez de instrumento: Se validará por medio de los expertos, la misma que se presentará adecuadamente en su oportunidad.

3.5 Procedimientos

La presente investigación surgió debido a los frecuentes incidentes en los juzgados de familia en cuanto a la protección de la información, lo que

tiene un impacto significativo en los procesos judiciales y la toma de decisiones en ellos.

Se investigó si existían normativas de seguridad de la información que pudieran tener los juzgados de familia del distrito judicial de Lima, para esto se revisó la documentación tales como, reglamentos, directivas y otros, concernientes al tema.

Después de las reuniones con los magistrados más antiguos y el administrador de los órganos jurisdiccionales, se explicó la finalidad de la investigación y se evaluaron las dimensiones e indicadores de las variables, los funcionarios emitieron una opinión respecto a la seguridad integral en los procesos judiciales, desde que llega a las áreas donde son analizadas, evaluadas, procesadas, intervención de la partes (demandado y demandante), sus abogados (sólo en algunos procesos) y culmina con la expedición de una sentencia, que concluye al litis iniciado por ambas partes.

Por otro lado, se realizaron reuniones con el personal jurisdiccional de los juzgados investigados, con la finalidad de evaluar sus conocimientos y/o procedimientos que suelen accionar en lo que respecta a las buenas prácticas y cumplimiento normativo, donde se obtuvo resultados sobre capacitaciones, manuales, folletos, trípticos u otros, relacionados sobre el tema; con lo cual se dejó en evidencia si existe o se conoce sobre alguna normatividad relacionada al tema de investigación.

Asimismo, se hizo la consulta al administrador de la base de datos, sobre la cantidad de ingresos de expedientes judiciales en la especialidad de familia y la factibilidad de emitir un reporte de los mismos, indicando el rango de las fechas a estudiar.

Culminando estos encuentros con el personal antes mencionado, se planificó la estrategia que se utilizó, las herramientas que, usadas para la recolección de información, así como el software adecuado para el estudio estadístico de los resultados que se obtuvieron en el estudio.

Se utilizó la ficha de datos como instrumento de recolección de datos los cuales fueron ingresados al sistema SPSS para el análisis de datos a

través de gráficas y tablas estadísticas. Por último, se interpretó los resultados para el diseño de los cuadros con su debida explicación evaluando las hipótesis concernientes a la presente investigación.

3.6 Métodos de análisis de datos

Para el tema de confiabilidad del instrumento, se utilizó el método o análisis de homogeneidad utilizando la técnica Alfa de Cronbach.

En Normalidad se optó por el método de Kolmogorov-Smirnov ya que la muestra contiene más de 50 datos.

Para las pruebas estadísticas se utilizó un análisis paramétrico usando el coeficiente de correlación de Pearson

3.7 Aspectos éticos

El estudio investigativo se desarrolló conforme a lo mencionado en la resolución del vicerrectorado de investigación N.º 062-2023 -VI-UCV expedida en marzo del año 2023.

La información obtenida por ser de una entidad judicial, tiene un carácter de confidencial, razón por la cual, solo se entregan los resultados obtenidos en el procedimiento investigativo.

La recopilación de datos ha sido autorizada por la entidad de administración de justicia del distrito judicial de Lima.

IV. RESULTADOS

4.1 Resultados de pruebas de confiabilidad, normalidad

La presente investigación se sometió a un análisis utilizando el software IBM SPSS Statistics versión 29.0.1.0 (171), mediante el cual se obtuvo resultados de fiabilidad, normalidad, análisis de variables, hipótesis, regresión lineal, entre otros.

Pruebas de confiabilidad del instrumento de recopilación de datos

Tabla 1. Resultado de pruebas de fiabilidad

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
0.778	0.713	44

Fuente: Elaboración del autor.

La interpretación de los resultados de la tabla 1 son los siguientes:

1) Las estadísticas de fiabilidad del coeficiente alfa de Cronbach, proporciona información sobre la consistencia interna del cuestionario aplicado como recopilación de datos, una ventaja de esta medida es que nos permite estimar cuánto mejoraría o empeoraría la confiablidad de la prueba si se excluyera un determinado ítem.
2) Alfa de Cronbach: El coeficiente alfa de Cronbach es 0,778. Este valor está en el rango de 0 a 1, donde un valor más cercano a 1 indica una mayor consistencia interna entre los elementos del cuestionario. En este caso, un valor de 0,778 sugiere una buena consistencia interna, lo que implica que las preguntas están correlacionadas de manera positiva entre sí, y además que el instrumento usado tiene una fuerte confiabilidad, es decir que el instrumento de recopilación de datos ha permitido realzar mediciones estables y consistentes.

3) Alfa de Cronbach basada en elementos estandarizados: Este coeficiente alfa de Cronbach basado en elementos estandarizados es 0,713. La estandarización de los elementos implica que todas las puntuaciones individuales se convierten a puntuaciones “z” (con una media de 0 y una desviación estándar de 1) antes de calcular el alfa. Este valor también es alto, lo que indica una consistencia interna robusta.

Número de elementos: Son los 44 indicadores del instrumento de ficha de datos que se están evaluando para medir la consistencia interna; esto es, 40 indicadores de la variables independientes y 4 indicadores de la variable dependiente.

Pruebas de normalidad

Tabla 2. Formulación de hipótesis para pruebas de normalidad

Pruebas de Normalidad	**Norma ISO 27002**	**Cumplimiento normativo**	**Sentencias**
Ho: Distribución normal	Se tiene Ho, donde X es igual a N (μ, σ^2)	Se tiene Ho, donde X es igual a N (μ, σ^2)	Se tiene Ho, donde X es igual a N (μ, σ^2)
Ha: Distribución no normal	Se tiene Ha donde X es diferente de N (μ, σ^2)	Se tiene Ha donde X es diferente de N (μ, σ^2)	Se tiene Ha donde X es diferente de N (μ, σ^2)
Nivel de significancia: NC	0.95	0.95	0.95
Error: α	0.050	0.050	0.050
Prueba de normalidad	50 <= n Kolmogorov-Smirnov	50 <= n Kolmogorov-Smirnov	50 <= n Kolmogorov-Smirnov
	50 > n Shapiro-Wilk	50 > n Shapiro-Wilk	50 > n Shapiro-Wilk
Criterio de decisión	Se tiene que p-valor en menor a 0.050, por lo tanto, se acepta la Ha y rehúsa Ho	Se tiene que p-valor en menor a 0.050, por lo tanto, se acepta la Ha y rehúsa Ho	Se tiene que p-valor en menor a 0.050, por lo tanto, se acepta la Ha y rehúsa Ho
	Se tiene que p-valor es en mayor o igual a 0.050, por lo tanto, se acepta la Ho y rehúsa Ha	Se tiene que p-valor es en mayor o igual a 0.050, por lo tanto, se acepta la Ho y rehúsa Ha	Se tiene que p-valor es en mayor o igual a 0.050, por lo tanto, se acepta la Ho y rehúsa Ha

Fuente: Edición propia

Tabla 3. Resultado prueba de normalidad - variables

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	Gl	Sig.	Estadístico	gl	Sig.
ISO27002	0.110	366	0.000	0.962	366	0.000
CUMPLIMIENTO	0.263	366	0.000	0.810	366	0.000
SENTENCIAS	0.235	366	0.000	0.911	366	0.000

a. Corrección de significación de Lilliefors

Fuente: SPSS – Edición propia

En estos resultados que se observan en la tabla 3 los grados de libertad representan que los datos del numéricos de la muestra son 366 y como es mayor a 50 se utiliza la prueba de Kolmogorov-Smimov, el nivel de significancia es inferior de 0,050 en consecuencia, de acuerdo a la tabla 2 rechazamos la hipótesis nula y aceptamos la hipótesis alternativa, es decir, aceptamos que los datos no tienen, distribución normal, consecuentemente se utilizará pruebas no paramétricas.

Análisis descriptivo

Variables independientes y dependientes

Tabla 4. Resultado análisis descriptivo variable independiente 1 (ISO 27002) y Cumplimiento normativo

DESCRIPTIVOS

		ISO 27002		CUMPLIMIENTO	
		Estadístico	Error estándar	Estadístico	Error estándar
Media		83.8005	0.24316	25.3989	0.21210
95% de intervalo de confianza para la media	Límite inferior	83.3224		24.9818	
	Límite Superior	84.2787		25.8160	
Media recortada al 5%		84.0188		25.6928	
Mediana		84.0000		27.0000	
Varianza		21.640		16.465	
Desv. estándar		4.65183		4.05772	
Mínimo		69.00		14.00	
Máximo		93.00		30.00	
Rango		24.00		16.00	
Rango intercuartil		6.00		5.00	
Asimetría		-0.690	0.128	-1.169	0.128
Curtosis		0.237	0.254	0.077	0.254

Fuente: SPSS – Editado por el autor

La interpretación de los resultados de la estadística descriptiva de la Tabla 4, son:

1) Media (Promedio): La media es 83.8005 y 25.3989, lo que indican el valor típico de la variable. En este caso, representa un nivel moderado de la variable.
2) Error Estándar: El error estándar es 0.24316 y 0.21210. Este valor indica la variabilidad esperada en la media de las muestras. Cuanto menor sea el error estándar, más precisa será la estimación de la media. En este caso, un

error estándar relativamente bajo sugiere una estimación precisa de la media poblacional

3) Intervalo de Confianza al 95%: El intervalo de confianza proporciona un rango en el cual es probable que se encuentre la verdadera media de la población. En este caso, el intervalo va desde 83.3224 hasta 84.2787 y 24.9818 hasta 25.8160.
4) Media Recortada al 5%: La media recortada al 5% (84.0188) y (25.6928) se calcula eliminando el 5% de los valores extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.
5) Mediana: La mediana es 84.0000 y 27.0000, que es similar a la media. Indica que la distribución de los datos no está sesgada de manera significativa.
6) Varianza y Desviación Estándar: La varianza es 21.640 y 16.465 y la desviación estándar es 4.65183 y 4.05772. Ambas medidas proporcionan información sobre la dispersión de los datos alrededor de la media. En este caso, la desviación estándar muestra que hay una moderada dispersión alrededor de la media.
7) Mínimo y Máximo: El valor mínimo es 69.00 y 14.00 y el máximo es 93.00 y 30.00. Esto proporciona información sobre el rango total de la variable, que es 24.00 y 16.00.
8) Rango: El rango es la diferencia entre el máximo y el mínimo (24.00 - 6.00 = 18.00) y (16.00 – 5.00 = 11.00), mostrando la extensión total de los datos.
9) Rango intercuartil (IQR): Es la diferencia entre el tercer cuartil (Q3) y el primer cuartil (Q1). En este caso, es 6.00 y 5.00, lo que indica la dispersión central de los datos, excluyendo los valores extremos.
10) Asimetría: La asimetría es -0.690 y -1.169, lo que sugiere una ligera asimetría negativa. Los datos están ligeramente sesgados hacia la izquierda, pero no de manera significativa.
11) Curtosis: La curtosis es 0.237 y 0.077, lo que indica una ligera curva en la distribución. La curtosis positiva sugiere colas más ligeras y una distribución más aplanada en comparación con una distribución normal.

Estos datos estadísticos han proporcionado una descripción detallada de la distribución y la tendencia central de la variable independiente ISO 27002 y Cumplimiento. Con ello, se ha podido determinar la variabilidad y la forma de la distribución de los datos.

Tabla 5 Resultado análisis descriptivo variable Dependiente Sentencias

Descriptivos

			Estadístico	Error estándar
SENTENCIAS	Media		11.1667	0.08978
	95% de intervalo de confianza para la media	Límite inferior	10.9901	
		Límite superior	11.3432	
	Media recortada al 5%		11.2489	
	Mediana		11.0000	
	Varianza		2.950	
	Desv. Estándar		1.71762	
	Mínimo		6.00	
	Máximo		14.00	
	Rango		8.00	
	Rango intercuartil		1.00	
	Asimetría		-0.766	0.128
	Curtosis		0.665	0.254

Fuente: SPSS – Editado por el investigador.

La interpretación de los resultados de la estadística descriptiva de la Tabla 5, son:

1) Media (Promedio): La media es 11.1667, lo que indica el valor típico de la variable. En este caso, representa un nivel moderado de la variable.
2) Error Estándar: El error estándar es 0.08978. Este valor indica la variabilidad esperada en la media de las muestras. Cuanto menor sea el error estándar, más precisa será la estimación de la media. En este caso, un error estándar relativamente bajo sugiere una estimación precisa de la media poblacional
3) Intervalo de Confianza al 95%: El intervalo de confianza proporciona un rango en el cual es probable que se encuentre la verdadera media de la población. En este caso, el intervalo va desde 10.9901 hasta 11.3432.

4) Media Recortada al 5%: La media recortada al 5% (11.2489) se calcula eliminando el 5% de los valores extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.
5) Mediana: La mediana es 11.0000, que es similar a la media. Indica que la distribución de los datos no está sesgada de manera significativa.
6) Varianza y Desviación Estándar: La varianza es 2.950 y la desviación estándar es 1.71762. Ambas medidas proporcionan información sobre la dispersión de los datos alrededor de la media. En este caso, la desviación estándar muestra que hay una moderada dispersión alrededor de la media.
7) Mínimo y Máximo: El valor mínimo es 6.00 y el máximo es 14.00. Esto proporciona información sobre el rango total de la variable, que es 8.00.
8) Rango: El rango es la diferencia entre el máximo y el mínimo (14.00 - 6.00 = 8.00), mostrando la extensión total de los datos.
9) Rango intercuartil (IQR): Es la diferencia entre el tercer cuartil (Q3) y el primer cuartil (Q1). En este caso, es 1.00, lo que indica la dispersión central de los datos, excluyendo los valores extremos.
10) Asimetría: La asimetría es -0.766, lo que sugiere una ligera asimetría negativa. Los datos están ligeramente sesgados hacia la izquierda, pero no de manera significativa.
11) Curtosis: La curtosis es 0.665, lo que indica una ligera curva en la distribución. La curtosis positiva sugiere colas más ligeras y una distribución más aplanada en comparación con una distribución normal.

Estos datos estadísticos han proporcionado una descripción detallada de la distribución y la tendencia central de la variable dependiente Sentencias. Con ello, se ha podido determinar la variabilidad y la forma de la distribución de los datos.

4.2 RESULTADOS

4.2.1 Resultados del objetivo general

La formulación del objetivo general e hipótesis general conforme a lo formulado en la matriz de consistencia se encuentra en la siguiente tabla:

Tabla 6. Cuadro de formulación del objetivo e hipótesis general, y criterios de evaluación de la prueba de correlación.

Objetivo general	
Determinar la relación de la ISO 27002 y el cumplimiento normativo en las sentencias de los juzgados de familia en una entidad judicial de Lima 2023.	
Hipótesis general de investigación	
Existe relación significativa entre la ISO 27002 y el cumplimiento normativo en las sentencias de los juicios de los juzgados de familia de una entidad judicial de Lima, del año 2023.	
Formulación de hipótesis estadística	
Hipótesis nula	Ho: No existe relación significativa entre la ISO 27002 y el cumplimiento normativo en las sentencias de los juicios de los juzgados de familia de una entidad judicial de Lima, del año 2023.
Hipótesis alternativa	Ha: Existe relación significativa entre la ISO 27002 y el cumplimiento normativo en las sentencias de los juicios de los juzgados de familia de una entidad judicial de Lima, del año 2023.
Nivel de significancia: NC	0.950
Error: α	0.050
Prueba de correlación	Distribución normal: Prueba paramétrica Pearson
	Distribución no normal: Prueba no paramétrica Rho de Spearman
Criterio de decisión	Si p-valor es menor a 0.050 Entonces se declina Ho y se acepta Ha
	Si p-valor es mayor o igual a 0.050 se aceptar Ho y Declina Ha
Interpretación de coeficiente de correlación	La interpretación se registra en los anexos de la presente investigación.

Fuente: Elaboración propia.

Los resultados de la prueba de correlación de la hipótesis general se encuentran en la siguiente tabla:

Tabla 7. Prueba de correlación de la variable independiente ISO 27002 y la variable dependiente Sentencias

Correlaciones

			ISO27002	SENTENCIAS
Rho de Spearman	ISO27002	Coeficiente de correlación	1.000	.363**
		Sig. (bilateral)		0.000
		N	366	366
	SENTENCIAS	Coeficiente de correlación	.363**	1.000
		Sig. (bilateral)	0.000	
		N	366	366

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: SPSS

La interpretación de los resultados de la Tabla 7, son los siguientes:

- El Coeficiente de Correlación de Spearman (Rho) entre el ISO 27002 y Sentencias es 0.363. Este coeficiente indica la fuerza y dirección de la relación entre las dos variables.
- Significancia Estadística: La correlación es significativa a un nivel de significancia del 0.01 (bilateral).
- El p-valor es menor a 0.05, y conforme la Tabla 8, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, de que existe correlación de la variable independiente ISO 27002 en la variable dependiente Sentencias, en la entidad judicial de Lima 2023.
- La correlación de 0.363 sugiere una fuerte relación positiva entre la variable independiente ISO 27002 y la variable dependiente Sentencias en la muestra analizada. La significancia estadística respalda que las variables están relacionadas. Por lo tanto, existe una correlación positiva moderada entre la variable mencionadas.

Formulación de las hipótesis específicas

La formulación de las hipótesis específicas de investigación son las siguientes:

Tabla 8. Cuadro de formulación del objetivo 1 e hipótesis específica 1 de investigación, y criterios de evaluación de la prueba de correlación.

Objetivo específico 1	
Determinar la relación que existe en las directrices de la seguridad de la información, en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023.	
Hipótesis específica 1 de investigación	
Existe una relación significativa entre las directrices de la seguridad de la información en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023.	
Hipótesis estadística específica 1	
Hipótesis nula	Ho: No existe una relación significativa entre las directrices de la seguridad de la información en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023.
Hipótesis alternativa	Ha: Existe una relación significativa entre las directrices de la seguridad de la información en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023.
Nivel de significancia: NC	0.950
Error: α	0.050
Prueba de correlación	Distribución normal: Prueba paramétrica Pearson
	Distribución no normal: Prueba no paramétrica Rho de Spearman
Criterio de decisión	p-valor < 0.05 Rechazar Ho Aceptar Ha
	p-valor >= 0.05 Aceptar Ho Rechazar Ha
Interpretación de coeficiente de correlación	Los datos de la interpretación se encuentran en los anexos del presente estudio.

Fuente: Elaboración propia.

Tabla 9. Cuadro de formulación del objetivo 2 e hipótesis específica 2 de investigación, y criterios de evaluación de la prueba de correlación.

Objetivo específico 2	
Determinar la relación que existe con los procedimientos y vigencia en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023.	
Hipótesis específica 2 de investigación	
Existe una relación significativa con los procedimientos y vigencia en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023	
Hipótesis estadística específica 2	
Hipótesis nula	Ho: No existe una relación significativa con los procedimientos y vigencia en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023
Hipótesis alternativa	Ha: Existe una relación significativa con los procedimientos y vigencia en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023
Nivel de significancia: NC	0.950
Error: α	0.050
Prueba de correlación	Distribución normal: Prueba paramétrica Pearson
	Distribución no normal: Prueba no paramétrica Rho de Spearman
Criterio de decisión	Si p-valor es menor que a 0.050 Se rehúsa Ho y acepta Ha
	Si p-valor es menor o igual a 0.050 Se acepta Ho Y Declina Ha
Interpretación de coeficiente de correlación	Los datos de la interpretación se encuentran en los anexos de la presente investigación

Fuente: Elaboración propia.

Tabla 10. Prueba de correlación de la variable independiente cumplimiento normativo y la variable dependiente Sentencias.

Correlaciones

			SENTENCIAS	CUMPLIMIENTO
Rho de Spearman	SENTENCIAS	Coeficiente de correlación	1.000	.362**
		Sig. (bilateral)		0.000
		N	366	366
	CUMPLIMIENTO	Coeficiente de correlación	.362**	1.000
		Sig. (bilateral)	0.000	
		N	366	366

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaborado por el autor.

La interpretación de los resultados de la Tabla 10, son los siguientes:

- Coeficiente de Correlación de Spearman (Rho) entre el Cumplimiento y Sentencias es 0.362. Este coeficiente indica la fuerza y dirección de la relación entre las dos variables.
- Significancia Estadística: La correlación es significativa a un nivel de significancia del 0.01 (bilateral).
- El p-valor es menor a 0.05, y conforme la Tabla 8, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, de que existe correlación de la variable independiente Cumplimiento normativo en la variable dependiente Sentencias, en la entidad judicial de Lima 2023.
- La correlación de 0.362 sugiere una fuerte relación positiva entre la variable independiente Cumplimiento normativo y la variable dependiente Sentencias en la muestra analizada. La significancia estadística respalda que las variables están relacionadas. Por lo tanto, existe una correlación positiva moderada entre la variable mencionadas.

Tabla 11. Resultado del modelo de regresión lineal

Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	.578[a]	0.334	0.330	1.40557

a. Predictores: (Constante), CUMPLIMIENTO, ISO27002
b. Variable dependiente: SENTENCIAS

Fuente: SPSS

La interpretación de la tabla 11 indica el resumen del modelo se explica en que R es el grado de correlación y tiene un grado de .578; el modelo es Sentencia está en fusión con la ISO 27002 y cumplimiento, este modelo se explica en R cuadrado ajustado en 0.330 y R cuadrado 0.334 y el error estándar de la estimación es de 1.40557.

Más lecturas detalladas son las siguientes:

1) Modelo y Variables:

a) Se ha ajustado un modelo con la variable dependiente Sentencias como variable dependiente y varias variables predictoras ISO 27002, y Cumplimiento normativo.

2) Estadísticas del Modelo:

a) R: El coeficiente de correlación múltiple (R) es 0.578. Indica la fuerza y dirección de la relación global entre las variables predictoras y la variable dependiente.

b) R cuadrado (R^2): Es 0.334, lo que significa que aproximadamente el 33.4% de la variabilidad en la variable dependiente puede explicarse por las variables predictoras en el modelo.

c) R cuadrado ajustado: Es 0.330, ajusta el R cuadrado por el número de predictores en el modelo y proporciona una medida más precisa del ajuste.

3) Evaluación de la Calidad del Ajuste:

a) Un R cuadrado medio (en este caso, 0.334) indica que el modelo tiene una moderada capacidad para explicar la variabilidad en la variable dependiente

b) El Error estándar de la estimación (1.40557) proporciona una medida de la dispersión de los residuos del modelo.

4) Significancia del Modelo:

a) La letra "a" junto a las estadísticas indica que la significancia del modelo se ha evaluado, y se ha encontrado que el modelo en su conjunto es estadísticamente significativo.

5) Variables Predictoras:

a) Las variables predictoras incluidas en el modelo son: ISO 27002, y Cumplimiento normativo.

6) Consecuentemente, el modelo tiene un moderado ajuste, explicando alrededor del 33.4% de la variabilidad en la variable dependiente sentencias. Las variables predictoras incluidas en el modelo son todas estadísticamente significativas.

Tabla 12. Modelo de resultados Anova

ANOVA[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	359.680	2	179.840	91.029	<.001[b]
	Residuo	717.153	363	1.976		
	Total	1076.833	365			

a. Variable dependiente: SENTENCIAS

b. Predictores: (Constante), CUMPLIMIENTO, ISO27002

Fuente: Elaboración propia.

La interpretación de los resultados de la Tabla 12, es el siguiente

1) ANOVA General:

a) El ANOVA general evalúa si el modelo en su conjunto es estadísticamente significativo en la predicción de la variable dependiente: Sentencias.

2) **Componentes de la Suma de Cuadrados:**
   a) Regresión: La suma de cuadrados para la regresión es 359.680. Indica la variabilidad explicada por el modelo.
   b) Residuo: La suma de cuadrados para el residuo es 717.153. Indica la variabilidad no explicada por el modelo.
   c) Total: La suma de cuadrados total es 1076.833, que es la suma de la regresión y el residuo.

3) **Grados de Libertad (gl):**
   a) Para la regresión, hay 2 grados de libertad (uno para cada predictor).
   b) Para el residuo, hay 363 grados de libertad.
   c) En total, hay 365 grados de libertad.

4) **Media Cuadrática (Mean Square):**
   a) Para la regresión, la media cuadrática es 179.840 (suma de cuadrados dividida por grados de libertad).
   b) Para el residuo, la media cuadrática es 1.976.

5) **Estadística F y Significancia:**
   a) La estadística F es 91.029.
   b) La significancia (p-valor) es <001 (menos de 0.05).

6) **Conclusiones:**
   a) La estadística F significativa (p-valor < 0.05) indica que el modelo en su conjunto es estadísticamente significativo en la predicción de la *variable* sentencia.
   b) La regresión explica significativamente más variabilidad de la que se esperaría por azar.

7) Consecuentemente, el ANOVA indica que el modelo, que incluye las variables predictoras mencionadas, es estadísticamente significativo para predecir la variable dependiente sentencias. La regresión es significativamente mejor que

un modelo nulo, lo que sugiere que al menos una de las variables predictoras tiene un efecto significativo en la variable dependiente.

Tabla 13. Modelo de resultados de Coeficientes

Coeficientes[a]

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados			95.0% intervalo de confianza para B	
		B	Desv. Error	Beta	t	Sig.	Límite inferior	Límite superior
1	(Constante)	-2.492	1.427		-1.747	0.082	-5.297	0.313
	ISO27002	0.125	0.021	0.338	6.004	0.000	0.084	0.165
	CUMPLIMIENTO	0.127	0.024	0.299	5.316	0.000	0.080	0.173

a. Variable dependiente: SENTENCIAS

Fuente: Elaboración propia.

La interpretación de los resultados de la Tabla 13, es el siguiente

1) Constante:

a) Coeficiente: -2.492.
b) Desviación estándar del error del coeficiente (Desv. Error): 1.427.
c) La constante representa el valor esperado de la variable dependiente sentencias cuando todas las variables predictoras son cero.
d) Significancia (Sig.): 0.082 (p-valor < 0.05), lo que indica que la constante es estadísticamente significativa.

2) VARIABLE PREDICTORA 1: ISO 27002

a) Coeficiente no estandarizado (B): 0.125
b) Desviación estándar del error del coeficiente (Desv. Error): 0.021
c) Coeficiente estandarizado (Beta): 0.338
d) Un aumento de una unidad en la variable independiente ISO 27002 se asocia con un aumento de aproximadamente 0.125 unidades en la variable dependiente sentencias.
e) Significancia (Sig.): 0.082 (p-valor < 0.05), lo que indica que la variable es estadísticamente significativa.

3) **VARIABLE PREDICTORA 2: CUMPLIMIENTO**

   a) Coeficiente no estandarizado (B): 0.127.
   b) Desviación estándar del error del coeficiente (Desv. Error): 0.024.
   c) Coeficiente estandarizado (Beta): 0.299.
   d) Un aumento de una unidad en la variable independiente Cumplimiento se asocia con una disminución de aproximadamente 0.127 unidades en la variable dependiente Sentencias.
   e) Significancia (Sig.): 0.000 (p-valor < 0.05), lo que indica que la variable es estadísticamente significativa.

4) En conclusión, cada uno de los predictores ISO 27002 y Cumplimiento, tienen un impacto significativo y único en la variable dependiente Sentencias según el modelo de regresión.

V. DISCUSIÓN

La investigación fue un estudio cuantitativo de diseño no experimental descriptivo correlacional causal que utilizó de muestra 366 expedientes judiciales de la especialidad familia del distrito de Lima, también demostró que la implementación de las buenas prácticas establecidas en la norma ISO 27002, así como el cumplimiento normativo abarcó significativamente un mejor desempeño y control en la expedición de las sentencias judiciales de los procesos de la especialidad familia del distrito judicial de Lima, 2023. Se afirma que la norma en mención es uno de los estándares mundiales de seguridad de la información y tiene mucha relación con la familia de las demás normas de seguridad de la información, así como de la seguridad informática, tal como la ISO 27001, y a esto apunta el estudio llevado a cabo por Quintana (2019), quien indicó que la aplicación de dicha norma garantiza la disponibilidad y seguridad de la información.

Concuerdo con lo mencionado por el investigador Otoya (2018) quién indicó que el propósito de seguir trabajando es asegurarse de que se identifiquen y controlen los riesgos de la tecnología de la información. La Gestión de Riesgos en TI proporcionará a los profesionales de TI una mejor gestión de la tecnología al tener las herramientas para tomar mejores decisiones en escenarios de riesgo y amenazas. Por lo tanto, su estudio en 2017 analizó cómo la gestión de riesgos de TI afecta la seguridad en proyectos de desarrollo rural.

Concuerdo con la investigación de Chavarry (2021) quién argumenta que la ejecución de la ISO 27001 en un establecimiento requiere una gran auditoría de todos los procesos, por lo que se sugiere ejecutar los controles de la ISO 27002. La implementación de estos mecanismos ayuda al desarrollo de la corporación y de su entorno. No obstante, considerando la situación actual en Perú, es poco común encontrar profesionales especializados en la protección de los datos. Además, hay muy pocas instituciones educativas en el mercado que ofrezcan estudios en seguridad de información, así como en temas de auditoría informática. En consecuencia, si no hay profesionales en la línea de seguridad en una institución u organización, los colaboradores no serán capaces de afrontar los ataques que se podrían dar, por falta de dicha capacitación.

Coincido con los autores Sulistjowati et al., (2020) quienes, en la revista internacional sobre visualización informática, indican que, la seguridad de los datos en la actualidad es fundamental para cualquier organización y requiere atención. La gestión de la información organizacional es una parte integral de una buena gestión empresarial. El conocimiento de la ciberseguridad en los procesos comerciales a corto, mediano y largo plazo de una institución, particularmente en las áreas de TI y comunicación, se mide como un indicador de la adecuación de la defensa. Los expedientes judiciales son de gran importancia tanto para la entidad, así como para las partes intervinientes del proceso judicial.

Asimismo, la investigación realizada por el autor en el presente trabajo, coincide con lo indicado por el investigador Gumucio (2021), en su investigación en Chile, el investigador llegó a la conclusión de que las tácticas de ciberseguridad para prevenir la pérdida de datos deben basarse en la implementación de prácticas adecuadas en la seguridad de la información y en la evaluación de riesgos. En América Latina, los gobiernos han avanzado en la regulación de la seguridad para proteger a sus organizaciones de las amenazas, pero el desarrollo no es uniforme en términos de reglas y tecnología, por lo que aún hay una gran brecha entre otros países y esto puede tener un impacto en todo el sistema mundial, debido a la globalización. Por otra parte, en lo que compete al cumplimiento normativo, también se concuerda con el investigador referido quien indica, que en la legislación europea en especial la española, demuestran la importancia que los países desarrollados han dado al tema, creando metodologías y buenas prácticas, tipificación precisa de delitos en esta materia para prevenirlos y lograr una evaluación adecuada. Además, la Unión Europea ha creado leyes que deben aplicarse a todos los países miembros en temas específicos, asegurándose de que todos los países deben fortalecer sus respectivos sistemas de información, así como una adecuada cultura normativa.

Además, estoy de acuerdo con la investigación realizada por Muñoz (2018), la cual estimó un porcentaje de ejecución inicial del 52% de acuerdo con los 11 dominios de seguridad de la norma ISO 27002. Sin embargo, es importante destacar que hubo controles que solo tuvieron un porcentaje del 0% debido a las funciones de la corporación. La ISO 27002 está diseñada para cualquier tipo de

institución, ya sea pública, privada, pequeña o grande, se tiene en cuenta que este estudio no se enfoca en el cumplimiento de la normativa, por lo que no se emiten conclusiones.

Del mismo modo, convengo con la de opinión de Ortiz (2018) quién afirmó en su investigación que un 95% de nivel de confianza se obtiene tras la implementación de los controles que se indican en el estándar ISO 27002, lo cual permitió mejorar los controles de la seguridad de los activos de la universidad de la Selva Peruana, indicó que el uso de sus controles estratégicos subieron de 12% a 14%, los operativos de un 16% a un 20%, modo global de 28% a 34%, lo que se reflejó como un incremento del 6% tras la ejecución del contenido de la norma mencionada. Si bien es cierto, ambas instituciones detalladas en este ítem, son organismos públicos y se enfocan en materias distintas, los resultados son similares ya que se utilizó los diversos dominios, objetivos de control y controles de la citada norma.

Por otro lado, difiero en la investigación realizada por Ortiz (2020) sobre el grado del cumplimiento normativo quien comenta la efectividad de la política estatal para resolver un problema social, Los hallazgos indican que, debido a que las regulaciones no están claramente definidas, su impacto es ineficaz en muchos lugares, los hallazgos resaltan la importancia de llevar a cabo un análisis más exhaustivo de las decisiones relacionadas con la implementación de diversas regulaciones. El Gobierno reconoce que acortar el número de casas de apuestas en función no es suficiente para limitar la apertura de nuevas solicitudes. Según sus resultados, en un total de 11 municipios, hay un 28.94% de establecimientos de apuestas que no cumplen con la norma de tener un espacio mínimo de 250 metros de diámetro de alejamiento. En consecuencia, se deben establecer sanciones drásticas para reducir este incremento desproporcional y se evitaría con esto, la proliferación desmedida de estos locales. Esto puede ser regulado por una buena política de difusión y ejecución de la normativa establecida en la organización.

Del mismo modo, concuerdo con lo descrito por Zambrano et al., (2022) quién considera que los asuntos jurídicos suelen resolverse a través de sentencias, los textos son una forma típica de discurso en el ámbito del derecho, estos argumentos son de naturaleza jurídica y someten a sus sujetos a diversos tipos de

sanciones. A pesar de la aparente opacidad y neutralidad del campo jurídico, algunos estudios sugieren que los argumentos de los jueces deberían reflejar claramente (aunque no directamente) sus responsabilidades políticas y jurídicas. Una forma de acceder a las ideologías que rigen las decisiones judiciales es a través del estudio discursivo de las sentencias analizando las estrategias discursivas expresadas en el texto. Este tipo de investigación relaciona el contenido textual con diversos eventos sociales y muestra cómo los grupos poderosos entienden y valoran a los demás, especialmente ciertos grupos culturales minoritarios.

Concuerdo con lo demostrado con Alarcón et al., (2020) que demuestran el impacto de la implementación de ISO 27001 en la seguridad de la información en una corporación, desde un punto de vista cualitativo y confidencial, donde la información debe ser accesible solo a los usuarios autorizados, según su posición o roles en la organización. Para lograr esto, ISO 27001 establece estrategias para respaldar la confidencialidad y la seguridad de la información. Además, es esencial para la integridad proteger la información de cambios sin el consentimiento de la organización. ISO 27001 facilita la implementación de procedimientos para avalar la seguridad integral de los datos. Finalmente, en lo que respecta a la disponibilidad de información, debe estar disponible en todo momento para que el usuario en cuestión pueda tomar decisiones.

Convengo en opinión con lo descrito por Beramendi 2021) en cuanto al objetivo de intentar describir el uso de reglas y normas avaladas por los participantes; se observó que algunas reglas provenían de otras instituciones y fueron aprobadas. También existe una serie de normas de convivencia que las personas observan no para escribir, sino para aprender y compartir con los pasajeros, como mantener una distancia suficiente, no hablar en voz alta por teléfono, ocupar la posición adecuada en el asiento, etc. que la gente ya entiende. Existe consenso y creencia en que estas reglas deberían regir la interacción social, estas reglas se aprenden a través de la socialización en el espacio y rigen el comportamiento esperado y pueden causar malestar si no se siguen. Por ejemplo, como se muestra en la sesión de un participante, pidió permiso para moverse alrededor del auto, caminar hasta la puerta y luego salir del auto. Es decir, se

comporta en consecuencia, sin embargo, cuando nadie lo escuchó, se volvió físicamente agresivo, como empujar a otros pasajeros. En esta situación, el control social y las sanciones no funcionan, por lo que el individuo opta por recurrir a otro tipo de conductas que violan reglas implícitas y crean agresión. Además, había otro conjunto de reglas de seguridad que, según los participantes, no estaban relacionadas con las reglas regulatorias, como no estacionar entre autos, pero que fueron respaldadas informalmente. Asimismo, el análisis de la percepción de las autoridades policiales muestra que la mayoría de los participantes consideró graves las violaciones. Muchos jugadores conocen las reglas, pero no confían en que la gente las siga, esto sugiere que el incumplimiento no surge de la ignorancia o la desinformación como se mencionó anteriormente, sino del incumplimiento de las personas.

Apoyo lo redactado por Fernández (2021) quién indica que el objetivo general del estudio fue averiguar si la implementación del cumplimiento normativo (modelo de cumplimiento regulatorio preventivo) podría reducir la corrupción en la región de nuevo Chimbote en 2021 y los resultados fueron: Considerando las circunstancias de los propios participantes, según el comunicado en la región indicada, el cumplimiento de las normas, leyes, reglamentos, etc. Es una disposición perfectamente apropiada y necesaria ya que la corrupción ha aumentado significativamente debido a diversos factores de la pandemia. Por tanto, la corrupción pasa a ser un ámbito privado que incluye conductas inadecuadas, diferentes y ajenas a lo prescrito por las normas y supone una actitud injusta. También se encontró que la participación del cumplimiento normativo es crítica, ya que sería un medio muy eficaz para combatir la corrupción en las instituciones públicas debido a la alta vulnerabilidad. Por lo tanto, la inclusión del cumplimiento público será una acción adecuada para promover la ética y los estados de cuentas de los oficinistas, todo será liderado por un oficial de cumplimiento (una persona eficaz que pueda liderar). Esto está relacionado con el estudio de Madrid y Palomino (2020), ya que muestra cómo las altas tasas de corrupción se reducen debido al cumplimiento del gobierno, ya que crea más control ejecutivo que contra de estas prácticas corruptas.

Concuerdo con el autor Leguizamón et al., (2020) quien afirma que la cantidad de amenazas y vulnerabilidades en un entorno de información altamente sensible debe reducirse y limitarse para eliminar y prevenir cualquier fuga o mal manejo de la información. Por lo tanto, es necesario identificar cualquier error en los sistemas de información y hacer todo lo posible para protegerlos de personas malintencionadas que puedan tener prácticas delictivas, como las que se descubren previamente al dejar evidencia de mal uso. El modelado de la infraestructura honeypot implementada por una universidad Boliviana permitió descubrir vulnerabilidades de seguridad provocadas por ciberataques a los servidores del centro de investigación. El objetivo de difundir la nueva red es estudiar información sobre diversas amenazas y proporcionar soluciones rápidas y efectivas para la investigación y la innovación en la práctica académica de la universidad. La principal ventaja de lo mencionado en términos de adaptabilidad del sistema, son los requisitos mínimos para su implementación, lo que permite agregar más herramientas de este tipo a dispositivos físicos o máquinas virtuales, logrando diferenciar entre diferentes configuraciones de cada dispositivo de seguridad. Sin embargo, conviene recordar que dichos mecanismos son herramientas pasivas, lo que significa que, si no son atacados, no sirven para la tarea y no son herramientas para reparar ataques. La función de ataque es activa, no pasiva, y está destinada únicamente al análisis del ataque por parte de la computadora y sirve como base para futuras tomas de decisiones.

Resalto y concuerdo en lo mencionado por Sandoval (2019) Se cree que la implementación del modelo de buenas prácticas ISO 27002 puede mejorar la gestión de incidentes cibernéticos de Wncor basándose en los resultados demostrados al aplicar el modelo propuesto en el documento para aplicar de manera óptima los controles estándar ISO 27002. Más del 85% de los usuarios de la red ya no experimentaron estos problemas debido a los eventos previos. Sin embargo, se pudo confirmar que la implementación del modelo de buenas prácticas ISO 27002 a los usuarios estudiados aminoró los problemas de conexión a la red en un 80%, y se concluyó que la implementación del modelo de buenas prácticas ISO 27002 redujo los problemas de acceso de los usuarios a los servidores de archivos de la red en un 86%.

Por último, también estoy de acuerdo con lo investigado por Triana y Moreno (2021) quienes confirman el alto nivel de cumplimiento de los procesos, actividades y requisitos establecidos en los estatutos de archivos y las normas técnicas para el procedimiento de la clase y la ciberseguridad, particularmente en términos de compromiso, desarrollo de políticas y comprensión de la importancia del sistema. Asimismo, las oportunidades de mejora en cada norma se centran en un mismo aspecto, es decir, que para lograr su pleno cumplimiento es necesario mejorar la adquisición, desarrollo, uso y adquisición de herramientas, procedimientos y aplicaciones tecnológicas para una adecuada gestión y seguridad de la información.

VI. CONCLUSIONES

Primera: Invocando al objetivo general del estudio, se puede determinar que el uso de los registros de la ISO 27002, mejora significativamente la seguridad de la información en los juzgados de familia del distrito de Lima y esto a su vez, repercute en la expedición de las sentencias en los procesos judiciales llevados en dichos órganos jurisdiccionales, logrando la satisfacción de los litigantes y usuarios de esta entidad estatal. A su vez, la ejecución del cumplimiento normativo también tuvo relevancia en las sentencias judiciales, ya que, al aplicarse las normas ya expedidas con anterioridad, así como la aplicación de nuevas disposiciones, causaron un efecto aprobatorio con el personal jurisdiccional de dichos juzgados que desconocían estos dispositivos legales.

Segunda: En lo señalado por el objetivo específico uno se pudo determinar los resultados positivos que se efectivizaron en los ambientes de los juzgados de familia con relación a las directrices de la seguridad de la información en las sentencias de dichos tribunales de justicia, se observa que en la prueba de correlación Rho de Spearman de la variable independiente Cumplimiento normativo y la variable dependiente, se determinó que el coeficiente de correlación es de .362, lo cual indica la fuerza y dirección entre ambas variables, la significancia estadística de 0.000 (bilateral) con esto se llegó a determinar la asociación de la norma ISO 27002, cumplimiento normativo con las sentencias.

Tercera: En base al objetivo específico dos, se logró determinar la mejora progresiva en la relación que existe con los procedimientos y vigencia que se resaltan en la expedición de las sentencias, tal como se puede subrayar en la correlación Rho de Spearman el coeficiente de correlación es .363 sugirió una fuerte relación positiva moderada entre ambas variables, las significancias estadísticas están relacionadas,

por lo tanto, se pudo determinar la correlación positiva moderada entre las dos variables.

Cuarta: Se determinó que el uso de la norma ISO 27002 y el cumplimiento normativo tuvieron un impacto positivo en la expedición de las sentencias judiciales de los juzgados de la especialidad de familia, en el distrito de Lima del año 2023. Del mismo modo, las hipótesis planteadas en el trabajo de investigación para las tres variables encontradas, también fueron aceptadas en el análisis final. En concreto, en base a la prueba y ejecución de las buenas prácticas de la norma ISO 27002 y el cumplimiento normativo, en los órganos jurisdiccionales de la especialidad de familia del distrito de Lima, ahora ha mejorado significativamente la seguridad, adaptabilidad, disponibilidad, protección en los expedientes judiciales y en las sentencias que se expidan en estas entidades de administración de justicia.

VII. RECOMENDACIONES

Al Gerente de Administración Distrital

Primera: Incorporar paulatinamente estándares normativos y buenas prácticas en la institución judicial, en especial en los órganos jurisdiccionales de familia del distrito de Lima, que fueron objeto del presente estudio, en lo que respecta a los temas investigados.

Al Coordinador de Recursos Humanos y Prensa

Segunda: Dado que, en los hallazgos del estudio, se comprobó muy escasas pruebas del cumplimiento normativo, reglas, reglamentos, directivas y demás dispositivos legales de control, se recomienda que las áreas correspondientes se encarguen de publicitar por los distintos medios como correos electrónicos, afiches, campañas educativas y demás; los controles existentes, así como la actualización de la documentación que tenga que ver con la seguridad de los activos de la institución.

Al coordinador de Informática

Tercero: Se realicen campañas periódicas de prevención y seguridad informática y de la información, así como capacitaciones permanentes al personal nuevo que se integra a la organización.

A los Colaboradores de la institución

Cuarto: Tengan un mayor celo con la seguridad de los expedientes judiciales, y a su vez, celeridad y transparencia en los procesos que se ventilan en sus despachos asignados.

REFERENCIAS

Agüero, Claudio (2019). ¿Conforman las sentencias penales un género discursivo? Estudios Filológicos, 53, 7-26.

Agüero San Juan, Claudio, Silva Berríos, Valentina, Sepúlveda Arellano, Eduardo, Sologuren Insúa, Enrique, & Rajevic Mosler, Enrique. (2022). La estructura de las sentencias judiciales como un problema de lenguaje claro. Ius et Praxis, 28(3), 228-247. https://dx.doi.org/10.4067/S0718-00122022000300228

Alarcón, M., Cruzado, C., Mejía, C., & Rodríguez, L. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. Propósitos y Representaciones, 1-11.

Arias-Gómez, J., Villasís-Keever, M. Á., & Novales, M. G. M. (2021). El protocolo de investigación III: la población de estudio. Revista alergia mexico, 63(2), 201-206.

Astudillo Muñoz, J., (2021). Notes regarding transparency in the exercise of public functions and the right of accessto public information. Revista Facultad de Jurisprudencia, (9), 385-429. https://doi.org/rfj.vi9.302

Atencio, E. (2019). Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú. http://repositorio.undac.edu.pe/handle/undac/1474

Beramendi, M., (2021). An Analysis of the Normative (Non) Compliance and the Interactions among Passengers in the Buenos Aires Subway. Cuadernos de Vivienda y Urbanismo, 14, 1-17.

Castillo Romero, R. M. (2022). Desarrollo de una aplicación web y móvil para la gestión de riesgos de seguridad de la información aplicado a una empresa de consultoría de sistemas.

Carvajal, D. L., Cardona, A., & Valencia, F. J. (2019). Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana. Entre ciencia e ingeniería, 13(25), 68-76.

Chavarry Bonilla, S. (2021). Implementación de ISO 27001 y 27002 adaptadas para gestión de seguridad de información en secretaría ejecutiva de policía nacional del Perú".

Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System (Primera ed.). Nueva York: Apress.

Díaz, L. V. (2021). Percepción de la implementación de la NTP-ISO/IEC 27001:2014 en base a la información documentada del gobierno central del Perú.

Farida, I., Mulyani, S., Akbar, B., & Setyaningsih, S. (2021). Quality and efficiency of accounting information systems. Utopía y Praxis Latinoamericana, 26(2), 323-337. https://doi.org/10.5281/zenodo.4678910.

Fernández Arcela, M. S. (2021). Implementación del compliance público (cumplimiento normativo preventivo). Un instrumento contra la corrupción en la Municipalidad Distrital de Nuevo Chimbote, 2021.

Fonseca Luján, R. C. (2022). Calidad de las sentencias en el sistema penal acusatorio en la Ciudad de México. Estudios Socio-Jurídicos, 24(2), 1-32. [Publicación electrónica previa a la impresión] https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.11333

Gonzales Aybar, R. G., & Sarmiento Astudillo, G. F. (2019). Implementación de la NTP/ISO 27001 para mejorar el proceso de seguridad de información en el Departamento Telemática de la Oficina de Economía del Ejército del Perú.

González-Valiente, C. L., & Macedo, D. D. (2020). Data and information in online environments. https://doi.org/10.1590/2318-0889202032e200073e

Gumucio, J. (2021). Guía de implementación de un programa de gestión de riesgos de Ciberseguridad en entidades de Intermediación Financiera. Chile. https://repositorio.uchile.cl/handle/2250/180169

Gutiérrez, H., Chamizo, J. & Puentes, J. (2022): “Cumplimiento normativo sobre información sostenible de las empresas españolas y sus efectos en los avances de la Agenda 2030”, CIRIEC-España, Revista de Economía Pública, Social y Cooperativa, 105, 289-318. DOI: 10.7203/CIRIEC-E.105.21991.

Infante M, et al., (2021). Efecto de acciones educativas en los procesos judiciales en los delitos de injurias en ausencia del procesado. Revista Universidad y Sociedad, 13(4), 32-40.

Joshi C, Singh UK (2017) Information security risks management framework—a step towards mitigating security risks in university network. J Inf Secur Appl 35:128–137.

Jufri, M. T., Hendayun, M., & Suharto, T. (2017, November). Risk-assessment based academic information System security policy using octave Allegro and ISO 27002. In 2017 Second International Conference on Informatics and Computing (ICIC) (pp. 1-6). IEEE.

Leguizamón-Páez, M. A., Bonilla-Díaz, M. A., & León-Cuervo, C. A. (2020). Analysis of computer attacks through Honeypots in the District University Francisco José de Caldas.

Lykhova, S., Servatiuk, L., Shamsutdinov, O., Sysoieva, V., & Hurina, D. (2022). International and national standards on societal information security. Revista Científica General José María Córdova, 20. (38), 247-264. https://dx.doi.org/10.21830/19006586.898

Llano-Henao Y, Rivera-Cadavid M, Amariles P. Cumplimiento de la normatividad en la publicidad televisiva de medicamentos de venta libre en Colombia. Estudio descriptivo retrospectivo 2018. MÉD.UIS.2022;35(2):81-95. DOI: https://doi.org/10.18273/revmed.v35n2-2022008

Manihuari Arimuya, L. C., & Vergaray Pintado, W. F. (2022). Modelo de defensa informático para la Protección de los datos en la empresa CGS Maxima SAC, Lima 2022.

Martínez Martínez, Ricard. (2019). Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo. Revista Catalana de Dret Públic, (58). 64-81. https://doi.org/10.2436/rcdp.i58.2019.3317

Motii Malik, Semma Alami. 2017, “Towards a new approach to pooling COBIT 5 and ITIL V3 with ISO/IEC 27002 for better use of ITG in the Moroccan parliament”, International Journal of Computer Science Issues, Volume 14, Issue 3. https://doi.org/10.20943/01201703.4958

Morón Peredo, K. R. (2023). Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú SAC.

Mucha, L., & Lora, M. (2021). Técnica de muestreo para investigación cuantitativa: aplicación informática. http://www.scielo.org.bo/pdf/rpc/v09n08/v09n08a12

Muñoz Ñauta, J. D. (2018). Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación de la Universidad de Cuenca.

Nacipucha, J. (2019). Análisis y diseño para un modelo de gestión de seguridad de la información basados en normas ISO/IEC 27001:2013 para la empresa Artehogar en la ciudad de Guayaquil.

Ormaza J et al., (2020) Ataques informáticos en tiempos de pandemia COVID-19 en Latinoamérica: Revisión Bibliográfica.

Ortiz García J. (2020) La distancia, ¿importa? (I): el grado de cumplimiento normativo de la legislación sobre las distancias entre casas de apuestas y centros educativos. ARTÍCULO 4/2020 (N.º 192). Boletín Criminológico. Instituto Andaluz Interuniversitario de Criminología.

Ortiz Morales, Einstein Arnold. 2018. Controles de Seguridad según la Norma ISO/IEC 27002:2013 para el Mejoramiento de la Gestión de Seguridad de la Información.

Otoya Verástegui, M. R. (2018). Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. International journal of morphology, 35(1), 227-232.

Paniagua, D. G. C., Vilca, G. R. Q., Quispe, B. P., & Choquecota, H. F. (2021). Impacto del control ciudadano en el cumplimiento normativo de los portales de transparencia estándar en empresas de saneamiento del sur del Perú. Economía & Negocios, 3(2), 104-117.

Rodríguez Baca, Liset Sulay, Cruzado Puente de la Vega, Carlos Francisco, Mejía Corredor, Carolina, & Diaz, Mitchell Alberto Alarcón. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. Propósitos y Representaciones, 8(3), e786. https://dx.doi.org/10.20511/pyr2020.v8n3.786

Rossi, G. (2021). La seguridad y defensa en la era de la cuarta revolución industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas hibridas. [Tesis de maestría, Academia Diplomática del Perú Javier Pérez de Cuéllar]. http://repositorio.adp.edu.pe/handle/ADP/170

Sandoval Fernández, L. R. (2019). Modelo de buenas prácticas aplicando ISO 27002 para gestión de incidencias de la red Wncor.

Silva Netto, A. da ., & Silveira, M. A. P. da. (2017). Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. JISTEM - Journal of Information Systems and Technology Management, 4(3), 375–397

Stoica, L. (2018). Business Intelligence and Olap. Knowledge Horizons / Orizonturi Ale Cunoasterii. Volumen 10 N° 3, pp 68–76.

Sulistyowati D. et al., (2020) Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. International journal on informatics visualization. Vol 4 NO 4.

Talavera Díaz, R. M. (2020). Necesidad de implementar programas de cumplimiento normativo en empresas públicas del sector financiero frente a actos de corrupción. Análisis en el marco de la ley Nº 30424.

Triana Torres, J. W. y Moreno Rodríguez, I. C. (2021). Armonización entre la gestión documental, la calidad y la seguridad de la información en una institución de educación superior. Signos, Investigación en Sistemas de Gestión, 13 (2) https://doi.org/10.15332/24631140.66644

Van Dijk, Teun (1980). Algunas notas sobre la ideología y la teoría del discurso. Semiosis, 5, 37-53.

Viena Azang, S. I. (2020). Cumplimiento de normas y satisfacción en usuarios del Hospital II Essalud Tarapoto, 2020.

Vivanco, H y Quintana, A. (2019). Diseño de un modelo de gestión de seguridad de la información para la Universidad Iberoamericana del Ecuador.

Zambrano-Tiznado, Juan Pablo & Lira Rodríguez, Renato (2022). Aplicación de una propuesta teórica al estudio discursivo de sentencias judiciales: un estudio de caso. Athenea Digital, 22(1), e3037.

ANEXOS

Anexo 1. Matriz de operacionalización de variables

Variable	Definición conceptual	Definición operacional	Dimensión	Indicador	Escala de medición
Independientes: VI1. La norma ISO	Estándar internacional que proporciona directrices y prácticas recomendadas para la gestión de la seguridad de la información en una organización.	Se enfoca en la implementación de controles de seguridad para asegurar la confidencialidad, disponibilidad e integridad de la información	1. Políticas de seguridad de la información.	1. Número de políticas implementadas. 2. Efectividad de controles. 3. Nivel de concienciación del personal	• Intervalo
VI2.Cumplimiento normativo	El cumplimiento normativo consiste en asegurar que una organización cumpla con las leyes, estándares, reglamentos y otros en el desarrollo de sus actividades.	Esto implica seguir estándares regulados y específicos con la finalidad de cumplir con las leyes, reglamentos, directivas y otras normas establecidas.	1. Legal y Regulatorio.	1. Número de observaciones 2. Número de hallazgos 3. Número de subsanación de observaciones 4. Numero de subsanaciones de hallazgos	
Dependientes: Sentencias	Son decisiones emitidas por un tribunal o un juez como resultado de un proceso legal	Estas decisiones son el resultado de la interpretación y aplicación de la ley a un caso específico presentado ante el tribunal. Pueden ser objeto de apelación.	1. Resolución de sentencia	1. Numero de Apelaciones 2. Duración del proceso judicial 3. Cumplimiento de la sentencia.	

Matriz de consistencia

Título: "La norma ISO 27002 y cumplimiento normativo en las sentencias de los juicios de los juzgados de familia, Lima 2023"

Autor: Rumiche Huamaní Rubén Eduardo

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES / UA
Problema general ¿La ISO 27002 y el cumplimiento normativo se relacionan en las sentencias de los juicios de los juzgados de familia de Lima 2023? **Problemas específicos** 1. ¿En qué medida las directrices de la seguridad de la información, se relacionan con las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023? 2. ¿Cómo los procedimientos y vigencia se relacionan con las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023?	**Objetivo general** Determinar la relación de la ISO 27002 y el cumplimiento normativo en las sentencias de los juzgados de familia en una entidad judicial de Lima 2023 **Objetivos específicos** 1. Determinar la relación que existe en las directrices de la seguridad de la información, en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023. 2. Determinar la relación que existe con los procedimientos y vigencia en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023.	**Hipótesis general** Existe una relación significativa entre la ISO 27002 y el cumplimiento normativo en las sentencias de los juicios de los juzgados de familia de una entidad judicial de Lima 2023. **Hipótesis específicas** 1. Existe una relación significativa entre las directrices de la seguridad de la información en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023. 2. Existe una relación significativa con los procedimientos y vigencia en las sentencias de los juzgados de familia, en una entidad judicial de Lima, 2023.	**V. Independientes** VI1. ISO 27002 • Directrices de la dirección en seguridad de la información • Dispositivos para la movilidad y teletrabajo • Manejo de los soportes de almacenamiento • Requisitos de negocio para el control de acceso. • Control de acceso a sistemas y aplicaciones. • Áreas seguras • Seguridad de los equipos. • Copias de seguridad VI2. Cumplimiento normativo • Procedimientos. • Vigencia **V. Dependiente** VD. Sentencias • Sumaria **UNIDAD DE ANALISIS** • Juicios

Anexo 2. Ficha de datos

N.°	Código de expediente	Fecha de ingreso	Sede	Instancia	Distrito	Provincia	Proceso	Motivo	Materia	Especialidad	Sub especialidad	Tipo de expediente	Estado	Norma ISO 27002								Cumplimiento Normativo		Sentencias
														D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11

Variable independiente 1 – **NORMA ISO**

DIMENSIONES

D1	Directrices de la dirección en seguridad de la información
D2	Dispositivos para movilidad y teletrabajo
D3	Manejo de los soportes de almacenamiento
D4	Requisitos de negocio para el control de acceso
D5	Control de acceso a sistemas y aplicaciones
D6	Áreas seguras
D7	Seguridad de los equipos
D8	Copias de seguridad

Variable independiente 2

CUMPLIMIENTO NORMATIVO

D9	Procedimientos
D10	Vigencia

Variable Dependiente

SENTENCIAS

D11	Sumario

Anexo 3:

Modelo de Consentimiento y/o asentimiento informado, formato UCV

NO APLICA PARA ESTA INVESTIGACIÓN

Anexo 4. Matriz Evaluación por juicio de expertos

DOCUMENTOS PARA VALIDAR LOS INSTRUMENTOS DE MEDICIÓN A TRAVÉS DE JUICIO DE EXPERTOS

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor Ingeniero:

Marlon Frank Acuña Benites

Presente

Asunto: **VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO**.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante del Programa de Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información de la Escuela de Posgrado de la UCV, en la sede Lima norte 202302, requiero validar los instrumentos con los cuales se recogerá la información necesaria para poder desarrollar mi investigación y con la que sustentaré mis competencias investigativas en la experiencia curricular de diseño y desarrollo del trabajo de investigación.

Los nombres de mis variables son: ISO 27002, Cumplimiento normativo y Sentencias, siendo imprescindible contar con la aprobación de expertos del tema para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Formato de validación.
- Certificado de validez de contenido de los instrumentos.

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

.....

Rubén Eduardo Rumiche Huamaní
Alumno del programa de maestría grupo 202302
D.N.I 10381603

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento para medir las variables ISO 27002, cumplimiento normativo y sentencias. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradezco su valiosa colaboración.

1. Datos generales del juez:

Nombre del juez:	Marlón Frank Acuña Benites
Grado profesional:	Maestría ( ) Doctor (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	Educación
Institución donde labora:	Universidad César Vallejo sede Lima Norte
Tiempo de experiencia profesional en el área:	2 a 4 años (X) Más de 5 años ( )
Experiencia en Investigación (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Soporte teórico

Breve detalle de las variables de la investigación

VI1. Norma ISO 27002: Es un código de buenas prácticas detallados en controles de seguridad de la información, la cual es utilizada por diversas organizaciones y/o empresas a nivel mundial, buscando disminuir las amenazas y riesgos, así como una correcta protección de los datos.

VI2. Cumplimiento normativo: es la forma legal de los procesos y acciones que establecen las organizaciones para asegurar el buen desempeño de la empresa.

VD. Sentencias: Nos referimos netamente al tema judicial y se define a un mandato emitido por un juez o jueces, donde después de las evaluaciones correspondientes, aprueban o no, las exigencias del demandado.

Tabla detalle de desglose dimensión e indicadores

Variable	Dimensión	Indicador	Detalle
VI.1- Norma ISO 27002	D1. Directrices de la dirección en seguridad de la información	1. Clave de rendimiento 2. Clave de riesgo 3. Tiempo de detección y respuesta 4. Disponibilidad del sistema	Ayudan a medir el desempeño y evaluar los riesgos en el tema de la seguridad de la información
	D2. Dispositivos para movilidad y teletrabajo	1. Conexiones seguras 2. Actualización de dispositivos 3. Aplicaciones aprobadas. 4. Seguridad biométrica	Garantizar que los colaboradores accedan a los recursos de la organización de manera segura.
	D3. Manejo de los soportes de almacenamiento	1. Cifrado de datos 2. Políticas de uso y retención 3. Protección contra pérdida o robo 4. Capacitación en el uso correcto	Contribuir a garantizar los datos almacenados en dispositivos físicos, así como minimizar riesgos o acceso no autorizado.
	D4. Requisitos de negocio para el control de acceso	1. Gestión de identidades 2. Políticas de acceso 3. Autenticación 4. Gestión de incidentes	Contribuyen a establecer un sistema de control de acceso robusto y alineado a los objetivos de la organización

	D5. Control de acceso a sistemas y aplicaciones	1. Tiempo de respuesta de autenticación 2. Gestión de sesiones 3. Monitorización de intentos de acceso 4. Autorizaciones y permisos	Medir los tiempos, reducir el riesgo de accesos no autorizados
	D6. Áreas seguras	1. Control de acceso físico 2. Vigilancia 3. Gestión de visitantes 4. Firewalls y seguridad perimetral	Evaluar su efectividad y garantizar la seguridad
	D7. Seguridad de equipos	1. Seguridad física 2. Inventario de equipos 3. Antivirus y antimalware 4. Ciclo de vida de equipos	Protección física de dispositivos, e implementación de medidas de seguridad en el software.
	D8. Copias de seguridad	1. Frecuencia de copias 2. Éxito en las copias 3. Cifrado 4. Gestión de versiones	Evaluar la eficacia y confiabilidad y garantizar la capacidad de recuperación en situaciones criticas
VI2. CUMPLIMIENTO NORMATIVO	D9. Procedimientos normativos	1. Cumplimiento de políticas 2. Comunicación efectiva 3. Retroalimentación y mejora continua 4. Capacitación de personal	Asegurar que el procedimiento normativo este bien establecido, así como su efectividad en la implantación

	D10. Vigencia	1. Cumplimiento normativo 2. Actualización de políticas y procedimientos. 3. Revisión de contratos y acuerdos 4. Gestión de incidentes de cumplimiento	Cumplimiento y actualización de normas y regulaciones en una organización
VD. SENTENCIAS	D11. Sumario	1. Tiempo de resolución 2. Cumplimiento de procedimientos legales 3. Justicia y equidad 4. Transparencia del proceso	Ayudan a evaluar la efectividad y equidad en el manejo de sentencias sumarias.

Escala/ ÁREA	Subescala (dimensiones)	Definición
ORDINAL	Políticas de seguridad de la información	Son normas, reglamentos, directivas y otros, que la entidad establece como parte de las formas de regular el uso de la información en la organización.
	Legal y regulatorio	La documentación regulatoria, se enfocan en directivas y resoluciones emitidas por los funcionarios de la Gerencia de la entidad.
	Resolución de sentencia	Es la parte final de un proceso de conflicto resuelto luego de los argumentos y pruebas presentados por las partes sean naturales o jurídicos, esta resolución en algunos casos, es apelada por una de las partes cuando no se encuentra conforme con el resultado.

4. Presentación de instrucciones para el juez

A continuación, a usted le presento la ficha de datos conformada por las 3 variables de mi investigación detalladas con sus dimensiones numeradas del D1 al D11 con su detalle respectivo, elaborado por Rubén Rumiche Huamaní. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, esdecir, su sintácticay semántica son adecuadas.	1. No cumple con el criterio	El indicador no es claro.
	2. Bajo Nivel	El indicador requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica dealgunos de los términos del ítem.
	4. Alto nivel **(X)**	El indicador es claro, tiene semántica y sintaxisadecuada.
COHERENCIA El ítem tiene relación lógica conla dimensión o indicador que estámidiendo.	1. totalmente en desacuerdo (nocumple con el criterio)	El indicador no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El indicador tiene una relación tangencial /lejana conla dimensión.
	3. Acuerdo (moderado nivel)	El indicador tiene una relación moderada con ladimensión que se está midiendo.
	4. Totalmente de Acuerdo (altonivel) **(X)**	El indicador se encuentra está relacionado con ladimensión que está midiendo.
RELEVANCIA El ítem es esencialo importante, es decir debe ser incluido.	1. No cumple con el criterio	El indicador puede ser eliminado sin que se veaafectada la medición de la dimensión.
	2. Bajo Nivel	El indicador tiene alguna relevancia, pero otro ítempuede estar incluyendo lo que mide éste.
	3. Moderado nivel	El indicador es relativamente importante.
	4. Alto nivel **(X)**	El indicador es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel **(X)**

Dimensiones del Instrumento

- **Primera dimensión**: Directrices de la dirección en la seguridad de la información
  Objetivos de la Dimensión: Contiene indicadores clave de rendimiento (KPIs) e indicadores de clave de riesgo (KRIs) los cuales ayudan a medir el desempeño y evaluar los riesgos.

Indicadores	**Claridad**				**Coherencia**				**Relevancia**				
	1.No cumple con el criterio.	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**Observaciones/ Recomendaciones**
I1. Índice de incidentes de seguridad													
I2. Nivel de conciencia de seguridad del personal													
I3. Tiempo de detección y respuesta													
I4. Disponibilidad del sistema													

- **Segunda dimensión**: Dispositivos para movilidad y teletrabajo
  Objetivos de la Dimensión: Apoyar a las organizaciones a mantener un entorno de trabajo móvil seguro y eficiente.

Indicadores	**Claridad**				**Coherencia**				**Relevancia**				
	1.No cumple con el criterio.	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**Observaciones/ Recomendaciones**
I5. Conexiones seguras													
I6. Actualización de dispositivos													
I7. Aplicaciones aprobadas													
I8. Seguridad biométrica													

- **Tercera dimensión**: Manejo de soportes de almacenamiento
  Objetivos de la Dimensión: Garantizar que los datos almacenados en dispositivos físicos estén protegidos y que se minimicen los riesgos de pérdida o acceso no autorizado

Indicadores	**Claridad**				**Coherencia**				**Relevancia**				
	1.No cumple con el criterio.	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**Observaciones/ Recomendaciones**
I9. Cifrado de datos													
I10. Políticas de uso y retención													
I11. Protección contra pérdidas o robos													
I12. Capacitación en el uso correcto													

- **Cuarta dimensión**: Requisitos de negocio para el control de acceso.
  Objetivos de la Dimensión: Establecer un sistema de control de acceso robusto y alineado con los objetivos y requisitos específicos del negocio.

Indicadores	**Claridad**				**Coherencia**				**Relevancia**				
	1.No cumple con el criterio.	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**Observaciones/ Recomendaciones**
I13. Gestión de identidades													
I14. Políticas de acceso													
I15. Autenticación													
I16. Gestión de incidentes													

- **Quinta dimensión**: Control de acceso a sistemas y aplicaciones
  Objetivos de la Dimensión: Ayudan a mantener un control de acceso sólido y adaptado a las necesidades específicas de la organización

Indicadores	**Claridad**				**Coherencia**				**Relevancia**				
	1.No cumple con el criterio.	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**Observaciones/ Recomendaciones**
I17. Tiempo de respuesta de autenticación													
I18. Gestión de sesiones													
I19. Monitorización de intentos de acceso													
I20. Autorización y permisos													

- **Sexta dimensión**: Áreas seguras
  Objetivos de la Dimensión: Ayudan a mantener la integridad y seguridad tanto en áreas físicas como virtuales, proporcionando una visión completa de la postura de seguridad de la organización

Indicadores	**Claridad**				**Coherencia**				**Relevancia**				
	1.No cumple con el criterio.	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**Observaciones/ Recomendaciones**
I21. Control de acceso físico													
I22. Vigilancia													
I23. Gestión de visitantes													
I24. Firewalls y seguridad perimetral													

- **Sétima dimensión**: Seguridad de los equipos
  Objetivos de la Dimensión: Evaluar y mejorar constantemente la seguridad de los equipos en una institución.

Indicadores	**Claridad**				**Coherencia**				**Relevancia**				
	1.No cumple con el criterio.	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**Observaciones/ Recomendaciones**
I25. Seguridad física													
I26. Inventario de equipos													
I27. Antivirus y antimalware													
I28. Ciclo de vida de equipos													

- **Octava dimensión**: Copias de seguridad
  Objetivos de la Dimensión: Desde la protección física de dispositivos hasta la implementación de medidas de seguridad en el software y la gestión de activos.

Indicadores	**Claridad**				**Coherencia**				**Relevancia**				
	1.No cumple con el criterio.	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**Observaciones/ Recomendaciones**
I29. Frecuencia de copias													
I30. Éxito en las copias													
I31. Pruebas de restauración													
I32. Gestión de versiones													

- **Novena dimensión**: Procedimientos
  Objetivos de la Dimensión: Asegurar que los procedimientos normativos no solo estén bien establecidos, sino que también sean efectivamente implementados y seguidos.

Indicadores	**Claridad**				**Coherencia**				**Relevancia**				
	1.No cumple con el criterio.	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**Observaciones/ Recomendaciones**
I33. Cumplimiento de políticas													
I34. Comunicación efectiva													
I35. Retroalimentación y mejora continua													
I36. Documentación y archivo													

- **Décima dimensión**: Vigencia
  Objetivos de la Dimensión: Contribuyen a garantizar que la organización esté al tanto y cumpla de manera efectiva con las normas y regulaciones que afectan su operación

Indicadores	**Claridad**				**Coherencia**				**Relevancia**				
	1.No cumple con el criterio.	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**Observaciones/ Recomendaciones**
I37. Seguimiento de cambios legislativos													
I38. Actualización de políticas y procedimientos													
I39. Revisión de contratos y acuerdos													
I40. Gestión de incidentes de cumplimiento													

- **Onceava dimensión**: Sentencias
  Objetivos de la Dimensión: Ayudar a evaluar la efectividad y equidad en el manejo de sentencias sumarias, asegurando que se cumplan los principios fundamentales de la justicia.

Indicadores	**Claridad**				**Coherencia**				**Relevancia**				
	1.No cumple con el criterio.	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**1.No cumple con el criterio.**	**2.Bajo Nivel**	**3.Moderado Nivel**	**4.Alto Nivel**	**Observaciones/ Recomendaciones**
I41. Tiempo de resolución													
I42. Cumplimiento de procedimientos legales													
I43. Recursos legales													
I44. Transparencia del proceso													

Observaciones (precisar si hay suficiencia): El instrumento presenta suficiencia SÍ

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

Apellidos y nombres del juez validador: Marlon Acuña Benites

Especialidad del validador: Docente Investigador

Los olivos 07 de diciembre del 2023.

[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

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador