Universidad César Vallejo

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Modelo metodológico basado en la norma ISO 27001 para el desarrollo de software en empresas de TI

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES

Arca Prieto, Jose Daniel (orcid.org/0000-0002-9909-2384)

Castro Palacios, Joustin Arsenio Santiago (orcid.org/0000-0003-3649- 2257)

ASESOR:

Mg. Peña Cáceres, Oscar Jhan Marcos (orcid.org/0000-0002-8159-7560)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendiemiento

PIURA — PERÚ

2023

Dedicatoria

A nuestros padres , dedicamos este proyecto universitario a ustedes, quienes han sido una parte fundamental en su desarrollo. Agradecemos su colaboración, conocimientos compartidos y contribuciones que han enriquecido este trabajo. Esperamos que este proyecto sea un testimonio de nuestro esfuerzo conjunto y de la calidad de nuestra formación académica.

Agradecimiento

Queremos expresar nuestro sincero agradecimiento al Mg. Peña Cáceres Oscar por su invaluable orientación y apoyo. Gracias también a nuestras familias y amigos por su constante ánimo. Este trabajo no habría sido posible sin ustedes.

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

RESUMEN

La investigación se enfocó en diseñar una metodología basada en la norma ISO 27001 para mejorar la calidad en el desarrollo de sistemas tecnológicos en organizaciones de tecnologías de la información. Adoptando un enfoque cuantitativo y un diseño no experimental, se encuestó a 17 trabajadores de la oficina de tecnología de la Municipalidad Provincial de Sullana. El análisis detallado de metodologías existentes permitió identificar puntos clave para formular un enfoque metodológico integrador. El modelo resultante logró fusionar eficazmente las mejores prácticas de desarrollo y estándares de seguridad. Los resultados indican un cumplimiento exitoso, con un alto rendimiento en el indicador de cumplimiento de normas y regulaciones, alcanzando un 84.8% de respuestas positivas que respaldan la efectividad del modelo. La documentación, validación y difusión del modelo recibieron un respaldo significativo, especialmente en "coherencia y estructura de la documentación" (53%), destacando su viabilidad para la adopción generalizada en empresas de TI. En conclusión, el modelo metodológico ha mejorado notablemente la calidad en el desarrollo de sistemas tecnológicos, respaldado por el cumplimiento de normas y la aceptación positiva de su documentación, sugiriendo su potencial para una adopción extendida en empresas de tecnologías de la información.

Palabras clave: Modelo metodológico, Norma ISO 27001, Seguridad de la información, Software empresarial, TI

ABSTRACT

The research focused on designing a methodology based on the ISO 27001 standard to improve quality in the development of technological systems in information technology organizations. Adopting a quantitative approach and a non-experimental design, 17 workers from the technology office of the Provincial Municipality of Sullana were surveyed. A detailed analysis of existing methodologies identified key points needed to formulate an integrative methodological approach. The resulting model effectively merged best development practices and security standards. The results indicate successful compliance, with a high performance in the indicator of compliance with norms and regulations, reaching 84.8% positive responses that support the effectiveness of the model. The documentation, validation, and dissemination of the model received significant support, especially in "consistency and structure of documentation" (53%), highlighting its viability for widespread adoption in IT companies. In conclusion, the methodological model has significantly improved quality in the development of technological systems, supported by compliance with standards and positive acceptance of its documentation, suggesting its potential for widespread adoption in IT companies.

Keywords: Methodological model, ISO 27001 Standard, Information Security, Enterprise Software, IT

I. INTRODUCCIÓN

Hoy en día, las compañías de tecnología de la información (TI) se enfrentan a una competencia feroz y un buen software es esencial para la complacencia del usuario y mantener la posición en el mercado. Sin embargo, el desarrollo de software crea muchas condiciones de riesgo y flaquezas que atentan la seguridad de la información de las empresas y sus consumidores. Para manejar estas complicaciones, se han desarrollado varias técnicas y marcos para garantizar la confiabilidad del sistema y la protección de la información.

Según Sisti (2019) la información se posiciona como uno de los recursos más valiosos en manos de las empresas, desempeñando un papel esencial en la toma de decisiones, la gestión corporativa, la automatización de las operaciones, y se transforma en un elemento crucial para lograr el éxito en el ámbito organizacional, al generar ventajas competitivas significativas. Por eso es importante desarrollar sistemas de información utilizando metodologías que aseguren la calidad del código y la protección de la información, ya que esto garantiza una gestión más efectiva de este recurso vital y, a su vez, fortalece la posición de la empresa en un mercado cada vez más competitivo y digitalizado.

La elección de una metodología correcta para un proyecto de desarrollo de software es una decisión de gran importancia para llegar a un efecto significativo de sus resultados. Menéndez (2006) identificó una serie de requisitos esenciales para construir una metodología efectiva. Estos requisitos incluyen la capacidad de la metodología para permitir una comunicación efectiva, su adaptabilidad a entornos dinámicos orientados al usuario, la posibilidad de ser enseñada, su cobertura integral del ciclo de desarrollo de software, la integración de todas las fases del ciclo, la inclusión de validaciones, el soporte para determinar la exactitud del sistema a lo largo del proceso, la accesibilidad de herramientas CASE(Ingeniería de Software Asistida por Computadora), la alineación con los objetivos del proyecto, la especificación de responsabilidades, su aplicabilidad en una variedad de proyectos de software, la capacidad de soportar la evolución del sistema y la inclusión de actividades que contribuyan a la mejora constante del procedimiento de desarrollo. Estos requisitos demuestran ser fundamentales y de importancia al momento de seleccionar una metodología. Si queremos obtener eficiencia y calidad

de la entrega de proyectos de software en un entorno cada vez más exigente y competitivo, se debe tener cuidado en cada una de las fases que involucra el desarrollo de software.

Algunos autores como Tamayo y Tamayo (2003), definen al marco metodológico como una etapa que utiliza el método científico con el propósito de obtener informes significativos, validar, corregir o hacer uso de la información. Además, se aborda que la norma ISO 27001 aborda los desafíos expuestos y fomenta la excelencia en la producción de programas en compañías de tecnologías de la información. En palabras de NAQ Certificación (2015), la norma ISO 27001 establece los criterios y directrices de excelencia para la administración de la integridad de datos, integrándose con enfoques de creación de aplicaciones que refuerzan tanto la seguridad como la calidad del software.

A pesar de la existencia de diversas metodologías y marcos de trabajo para el desarrollo de software, aún persisten desafíos significativos en términos de asegurar la calidad y la protección de los datos en las empresas de TI. La falta de integración efectiva entre las prácticas de desarrollo de software y los parámetros de protección de la información, como la norma ISO 27001, ha llevado a generar brechas de seguridad y pérdida de información vital, afectando la competitividad y la confiabilidad de estas empresas en un mercado cada vez más digital y competitivo.

Ante esta problemática surge la siguiente interrogante: ¿Cómo mejora la calidad y seguridad en empresas de TI la aplicación de un modelo metodológico asentado en la norma ISO 27001?

Esta investigación se justifica por la necesidad de desarrollar metodologías de software eficientes y seguras, dada la escasez de enfoques centrados en la norma ISO 27001 y la prevalencia de procesos extensos y rígidos, inadecuados para pequeñas y medianas empresas (PYMEs). Desde una perspectiva práctica, abordará vacíos evidentes en metodologías que integran estándares de seguridad reconocidos, ofreciendo soluciones adaptativas a empresas de variados tamaños y sectores. Teóricamente, enriquecerá el cuerpo académico de conocimientos en desarrollo de software y gestión de seguridad de la información, proporcionando un marco empírico y conceptual para futuras investigaciones y perspectivas renovados sobre integración de prácticas de desarrollo y estándares de seguridad.

Socialmente, el estudio responde a crecientes preocupaciones sobre la privacidad y seguridad de la información, con el potencial de reforzar la confianza del consumidor en servicios y productos de TI mediante la garantización de la protección de datos personales y financieros. Metodológicamente, el enfoque propuesto supera las limitaciones de metodologías centradas en grandes corporativos, ofreciendo a las medias y pequeñas empresas una herramienta viable y flexible con el objetivo de aumentar tanto la calidad como la seguridad de sus sistemas tecnológicos, permitiendo su implementación en una variedad de contextos organizativos y contribuyendo a la innovación metodológica en el campo. Se propuso inicialmente validar su enfoque en un contexto público mediante la colaboración con una municipalidad. Esta validación permitió ajustar y refinar la metodología para cumplir con los requisitos y desafíos específicos de una entidad gubernamental. Sin embargo, la intención subyacente es que los resultados obtenidos en esta fase de validación no solo sean específicos para el ámbito público, sino que también sienten las bases para la aplicabilidad más amplia en empresas de TI.

Esta investigación tuvo como objetivo general, diseñar una metodología basado en la norma ISO 27001 para impulsar la eficiencia en la creación de aplicaciones informáticas en empresa de TI, y para lograrlo se plantearon objetivos específicos, realizar un análisis exhaustivo de las metodologías existentes en el desarrollo de sistemas tecnológicos en corporaciones de TI, diseñar un modelo metodológico que integre las mejores prácticas de desarrollo de sistemas tecnológicos y los estándares de seguridad de la información y por último documentar, validar y difundir el modelo metodológico para su adopción y uso en empresas de TI. Estos objetivos permitieron considerar la siguiente hipótesis, el modelo metodológico basado en la norma ISO 27001 en empresas de TI mejora la calidad y la seguridad de los sistemas tecnológicos, y como hipótesis específicas se detallan, 1) el análisis exhaustivo de las metodologías existentes en el desarrollo de sistemas tecnológicos en empresas de TI contribuirá en la mejora de la calidad y seguridad de los sistemas tecnológicos, 2) el desarrollo del modelo metodológico integra las mejores prácticas de desarrollo de sistemas tecnológicos y los estándares de seguridad de la información y 3) El modelo metodológico aportara facilidad en su documentación y difusión facilitando su adopción y uso en una empresa de TI.

II. MARCO TEÓRICO

En el estudio académico de Mora (2021), titulada “Propuesta metodológica para la gestión de la seguridad de la información alineada a la norma ISO 27001 y ciberseguridad”, propuso diseñar un modelo metodológico para el procedimiento de la protección de la seguridad según los estándares establecidos en la norma ISO 27001. Se llevó a cabo un examen exhaustivo de las debilidades presentes en los sistemas de datos, con el fin de lograr una gestión más efectiva y adecuada. La propuesta metodológica logró establecer las pautas normativas y los procedimientos relacionados con la seguridad informática. Además, se logró presentar de manera clara y concisa los beneficios asociados con la implementación de los protocolos de seguridad, los cuales fortalecen la seguridad informática y aseguran una contestación efectiva ante posibles riesgos de seguridad.

El título del trabajo de Robalino (2018) es “Propuesta metodológica y simulación de implementación SIEM basada en las normas ISO 27001 y/o 27002”. El principal fin de este fue desarrollar un marco metodológico y probar la implementación de SIEM basado en las normas ISO 27001 y/o 27002 en un entorno controlado y seguro, enfocándose en la comprobación de la tecnología de la información corporativa en redes de mediano tamaño. El desarrollo está guiado por una "metodología de creación" que utiliza cuidadosamente los conocimientos y técnicas de los modelos metodológicos "top-down" y "MSF" y asegura el seguimiento de la información a través de la "metodología de creación". Security Information and Event Management (SIEM)", la línea Deming, así como las directrices de las normas ISO 27001 e ISO 27002, constituyen elementos clave en este desarrollo que comprende cuatro etapas. Durante la fase inicial denominada "Teoría", el autor detalla exhaustivamente diversas clases de enfoques empresariales ligados a la tecnología de la información, clasificándolos en subclases y dando explicaciones detalladas. Esta etapa de Modelado, emplea la metodología de implementación SIEM como base para la formulación del plan. Por último, en la etapa de concreción, se lleva a cabo una valoración conceptual para medir la eficacia de las técnicas utilizadas en la aplicación de SIEM. Finalmente, se analiza la información recogida en la fase de resultados para determinar las posibilidades y limitaciones del método desarrollado.

Estos hallazgos conducen a los refinamientos y ajustes necesarios para llegar al enfoque final de implementación de SIEM mejorado y revisado.

En trabajo de Nacipucha (2019) titulado “Análisis y Desarrollo de Modelo de Gestión de Seguridad de la Información Basado en la Norma ISO/IEC 27001:2013 en la compañía Artehogar, Guayaquil”. Se estableció como propósito desplegar una estructura sistémica de gestión para salvaguardar la información de la empresa ArteHogar S.A., localizada en la ciudad de Guayaquil, basado en la norma internacional ISO/IEC 27001:2013. La investigación se realizó con base en las pautas establecidas en la norma y utilizó una combinación de métodos cualitativos y cuantitativos. Pueden ayudar a garantizar que la exactitud de la información del dispositivo no se haya visto comprometida por empleados que utilizan con frecuencia correos electrónicos personales para actividades oficiales, lo que puede facilitar la adquisición no autorizada de información empresarial a través de tácticas como el phishing, y han demostrado que los empleados carecen de conocimiento de los correos electrónicos maliciosos para Para su identificación se comprobó el estado actual de la compañía ArteHogar en materia de protección de datos, utilizando como sistema de referencia la norma ISO/IEC 27001:2013. Con base en los resultados del análisis, se concluyó que se debe implementar un marco de gestión de protección de la información. Dicha adición identifico sectores de precariedad y proporcionó implementos importantes para construir pasos de protección estable.

La investigación de Castillo (2019) titulado “Propuesta de lineamientos metodológicos basados en ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014 en seguridad de la información en la provincia de Recuay – 2015” presento el objetivo principal del marco metodológico de este estudiar el soporte ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014, complementando así la defensa de informes en la administración pública de la provincia de Recuay. Se realizó una investigación descriptiva no experimental con el propósito de examinar el impacto de las normas consideradas en la salvaguarda de la información en las entidades municipales. Se eligió como conjunto de investigación a un total de 48 funcionarios pertenecientes a provincias y municipios que emplean sistemas de información y gestionan datos. La muestra incluyó a 20 trabajadores. Para la redacción del trabajo, se aplicaron

las pautas establecidas por la norma ISO/IEC 27001:2013 y los lineamientos de la NTP ISO/IEC 27001:2014. Se concluyó que la evaluación de incertidumbres, vulnerabilidades y normas de seguridad en la salvaguardia de la información del gobierno provincial arrojó resultados satisfactorios. Además, las prácticas del estándar NTP ISO/IEC 27001:2014 tienen el impacto más beneficioso en las organizaciones de información.

En el estudio de grado de Cerezo (2022), titulado “Aplicación de la norma ISO 27001 para la gestión de seguridad de la información en la empresa plataforma de búsqueda académica BUSAC-ESTE en Ecuador”. Se incrementó la protección de la información. de las unidades estructurales de Guru-IT a través de la incorporación del estándar ISO 27001, empleando pautas de prueba para la adquisición de datos y la revisión estadística. El resultado de este estudio fue una mejora en el porcentaje de vulnerabilidades detectadas en la fase post-implementación, que disminuyó un 13,55% respecto a los datos obtenidos en la fase pre-implementación. Asimismo, el tiempo necesario para la implementación de protocolos de seguridad y detección de piezas expuestas se ha reducido significativamente un 5,65% y un 11,97%, en cada caso, respecto a los detalles recopilados en la fase inicial. Se concretó que la incorporación de la norma ISO 27001 podría optimizar sustancialmente la salvaguardia de la información de las unidades Guru-IT.

El estudio de Navarro (2021) “lmplementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 en el departamento de operación de Caja Sullana” brindó recomendaciones para la creación de aplicaciones de monitoreo de resguardo de datos. Los departamentos operativos de las respectivas unidades estructurales se basan en la norma ISO 27001. Para lograr esto se utiliza la información del Volumen 5 de la Guía de apoyo a la gestión de proyectos (PMBOK) constituye una norma globalmente reconocida que es aplicable a cualquier entidad. Esta decisión fue impulsada por incidentes previos en los que tanto ex empleados como actuales del área violaron las medidas de seguridad de datos de la empresa. Este proyecto se ejecutó con el propósito de recopilar información pertinente, se llenó un cuestionario a los gerentes regionales y equipos de operaciones, cuyos resultados sustentan el desarrollo del protocolo

estándar ISO 27001:2013. Al finalizar el proyecto, se formularon sugerencias con el objetivo de resguardar la protección de los colaboradores y usuarios, apoyadas por los fines de seguimiento dentro de la norma ISO 27001:2013, para identificar, coordinar, minimizar y documentar recursos de incidentes que puedan comprometer la información.

En el artículo de Rodríguez, Cruzado y otros (2020), titulado “Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana” tuvo como objetivo examinar el impacto de implementar la norma ISO 27001 en la protección de datos de una compañía privada en Lima (Perú). Se utilizó un enfoque cuantitativo y se llevó a cabo un análisis pre experimental para establecer el impacto de la implementación del ISO 27001. Se tomó en cuenta una selección de 30 empleados de la compañía para este estudio. Los resultados cuantitativos indican que efectivamente hay un impacto de la implementación del ISO en la protección de datos y en los aspectos de confidencialidad, integridad y disponibilidad. Los hallazgos logrados respecto a la solidez de la seguridad de la información corroboraron lo previamente señalado; dado que, sin la implementación de políticas o reglamentaciones por parte de una organización para la ejecución de sus procedimientos, estos operarán sin rumbo y estarán sujetos a elevados peligros. De igual manera, se destacó que la adopción de la norma ISO 27001 sí afecto la solidez de la información, ya que facilito la evaluación de qué estrategias, políticas y directrices se están instaurando para prevenir modificaciones no autorizadas de la información.

En el estudio llevado a cabo por Martelo, Medray, y otros (2018), titulado “Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI)”, tuvo como objetivo desarrollar un software que facilitara la administración de los documentos producidos durante la instauración de un Sistema de Gestión de Seguridad de la Información (SGSI).

Este módulo busca garantizar una organización, acceso y control efectivos del material documental crucial para auditorías y certificación del sistema de gestión, proporcionando una supervisión completa de cada documento y cumpliendo con los protocolos de la norma ISO 27001.El resultado del estudio fue un módulo

novedoso con características distintivas, integrando módulos de roles, actividades y comunicaciones que permiten un monitoreo constante de los documentos y promueven la participación de implementación. Además, el software proporciona una opción de almacenamiento cloud, especialmente diseñada para pequeñas y medianas empresas, y se personaliza según las necesidades de la organización que lo adquiere, resguardando así los fundamentos de seguridad de la información. Las conclusiones del estudio subrayan la utilidad del instrumento desarrollado para evaluar el estado de los documentos, evitar el uso de documentos anticuados, asegurar la disponibilidad y el monitoreo de los documentos delegados y alinearse con los procedimientos estrictos de la norma ISO 27001. Esto se realiza mediante un enfoque de trabajo repetitivo y fortaleciendo la responsabilidad a través de la administración de roles y la delegación de tareas.

La seguridad de la información se refiere a la salvaguardia frente amenazas y peligros capaces de violar la privacidad, la legitimidad o admisión. La finalidad de esta seguridad es afianzar que únicamente individuos autorizados logren tener acceso, para alterar la información y que los sistemas informáticos tengan la capacidad de sobrellevar posibles inconvenientes, errores o ataques. Whitman y Mattord (2011), la definen como la prevención del empleo no consentido, modificación, revelación, interrupción, alteración o supresión de datos y plataformas informáticas. Es necesario implementar una serie de medidas para asegurar un resguardo efectivo de la información, incluidas normas de protección, plataformas de entrada, tecnologías de encriptación y entornos de alerta y reacción. Es importante que estas medidas se diseñen, implementen y se mantengan para asegurar una defensa adecuada contra las amenazas y riesgos a lo largo del tiempo.

ISO 27001 especifica los requisitos indispensables para implementar un entorno efectivo de control de la inviolabilidad de los datos (SGSI) y eficiente. Este modelo se centra en proteger los valores de información, garantizar su reserva, integridad y accesibilidad, y gestionar los desafíos de salvaguardia de la información. ISO 27001 se hace referencia a la metodología de mejora continua PDCA (Planificar, Hacer, Controlar y Actuar) e incluye una serie de criterios relevantes como la verificación de información crítica, la evaluación de vulnerabilidades, la

implementación y pruebas de seguridad y desarrollo. ISMB. ISO 27001 es una herramienta importante para proteger la privacidad del público. Brinda un enfoque poderoso para la administración de la seguridad de la información permitiendo así a las empresas reconocer, examinar y administrar las posibles amenazas a la seguridad de la información.

(García, 2015). La implementación de un SGSI (Sistema de gestión de seguridad) certificado ISO 27001 proporciona a una organización ventajas, incluida una mayor seguridad, generalidad y disponibilidad de los datos, y una mayor suficiencia para prevenir y solucionar a vulneraciones de seguridad y cumplimiento de los estándares y regulaciones ajustables. Además, dichas implementaciones pueden crear una mayor confianza en la organización entre clientes, proveedores y socios comerciales.

La calidad de software, Según Pressman (2010) se refiere a la alineación entre los requerimientos funcionales y de desempeño claramente definidos, junto con los estándares de desarrollo bien documentados, y las características que se anticipan en todo software creado de manera profesional.

Según Smithson y Johnson (2010), un marco metodológico es un abordaje conformado que se emplea para dirigir y clasificar el procedimiento del estudio en un espacio o área particular. Estos modelos proporcionan un reglamento o pasos que deben seguirse sistemáticamente para lograr un objetivo.

Según estos mismos autores, el propósito de un modelo metodológico es radica en ofrecer un marco que guíe la investigación. un marco que oriente la investigación, desde el establecimiento de propósitos hasta la recolección de datos, la selección de métodos y técnicas sugeridas, la evaluación de data, la comprensión de los resultados y la propuesta de conclusiones. También incluye instrucciones sobre cómo realizar una revisión de la literatura, diseñar un experimento, realizar entrevistas o encuestas, etc.

El artículo 35 de la Constitución Política del Perú (1993) enfatiza que los municipios son reconocidos como empresas creadas por ley, constituidas por iniciativa del gobierno local. Estos municipios tienen la opción de utilizar diversas formas

especificadas en la normativa que regula las actividades empresariales y su principal objetivo es prestar servicios municipales al publico

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo de investigación

El tipo de investigación fue aplicada ya tuvo como propósito crear un modelo metodológico basado en la norma ISO 27001 para su aplicación práctica en un entorno definido. Para Murillo (2008) la investigación aplicada, también conocida como investigación empírica, se distingue por su enfoque en la utilización de saberes ya adquiridos, mientras que simultáneamente se obtienen nuevos conocimientos. Este proceso se lleva a cabo mediante la implementación y organización de prácticas fundamentadas en investigaciones previas.

La investigación tuvo un enfoque cuantitativo, según el sitio Qualtrics, esta forma de investigación emplea métodos matemáticos y estadísticos para detallar, comprender y anticipar eventos a través de información cuantitativa. En esta situación, se emplearon indicadores que puedan afectar la implementación de modelos metodológicos en el contexto del desarrollo de software de las empresas de tecnologías de la información.

3.1.2. Diseño de investigación

El diseño de la investigación fue no experimental de naturaleza observacional y descriptiva. Esta elección se basó en la decisión de observar y describir la implementación de un modelo metodológico fundamentado en la norma ISO 27001 y su impacto en empresas de tecnologías de la información. La validación del modelo metodológico se llevó a cabo mediante la selección cuidadosa de indicadores relevantes, estableciendo así un enfoque descriptivo y observacional para evaluar su rendimiento.

La investigación tiene un alcance aplicado, buscando proporcionar una visión práctica y contextualizada de la implementación del modelo en un entorno empresarial.

3.2. Variables y operacionalización

Variable independiente

Modelo metodológico: Según Creswell (2014): " Los modelos metodológicos se presentan como instrumentos tanto conceptivos como operativos que proporcionan un marco organizado y sistemático para realizar investigaciones y proporcionan pautas claras y coherentes para realizar investigaciones."

Dimensiones

Seguridad de la información: Según la publicación especial 800-30 (2012) del NIST del Instituto Nacional de Estándares y Tecnología de EE. UU., la orientación de la salvaguardia de datos es asegurar la salvaguarda de la confidencialidad, la seguridad y la asequibilidad de la información. Esto significa que está diseñado para evitar la entrada no permitida o la revelación de datos confidenciales, para garantizar que la información permanezca intacta, es decir, la modificación no autorizada, y para asegurar la disponibilidad de la información en el momento oportuno.

Eficiencia en el proceso de desarrollo: Se refiere a la capacidad de un equipo o una organización para producir software de manera efectiva y utilizar de manera óptima los recursos que se disponen. Consiste en alcanzar los objetivos deseados en cuanto a calidad, funcionalidad y tiempo, al mismo tiempo que se reducen los costos y se optimiza la utilización de los recursos humanos y tecnológicos disponibles. También la productora Digital, Software Factory (4r Soluciones) (2013), define la eficiencia como la correlación entre el desempeño del software y la cantidad de recursos utilizados en determinadas circunstancias.

Cobertura de la documentación: La cobertura de la documentación del modelo metodológico para el desarrollo de software debe englobar tanto los aspectos teóricos como los prácticos, brindando una orientación detallada a los equipos de desarrollo. Esto implica

presentar explicaciones precisas en las fases del ciclo de vida del software, los roles y responsabilidades asignados a los miembros del equipo, las actividades fundamentales, los artefactos y documentos requeridos, y los indicadores utilizados para evaluar la calidad y llevar a cabo las verificaciones necesarias.

Indicadores

Protección de datos confidenciales: La protección de datos confidenciales es un componente esencial en la protección de la información. Radica en la implementación de diversas acciones y estrategias con el propósito de preservar la integridad y confidencialidad de la información que se considera privada y sensible, evitando su acceso, divulgación o uso no autorizado. Según PowerData (2023) salvaguardar información comprende conceptos como el cifrado de datos, la tokenización y las técnicas de administración de contraseñas, que contribuyen a salvaguardar la información en todos los sistemas y plataformas de la entidad.

Cumplimiento de normas y regulaciones de seguridad: Según la definición proporcionada por Del Prado (2020), una norma puede ser caracterizada como una regla que no solo requiere ser comunicada y difundida de manera completa, sino que también debe ser acatada de forma estricta para prevenir cualquier posible perjuicio en el desarrollo de las tareas laborales. En otras palabras, una norma laboral implica la necesidad de transmitir y divulgar íntegramente las directrices establecidas, y su observancia rigurosa se vuelve fundamental para evitar eventuales consecuencias negativas en el rendimiento y la ejecución de las labores asignadas.

Tiempo de desarrollo: De acuerdo con Sharma (2022), el tiempo de desarrollo en el campo del software no se limita a una simple medida temporal, sino que implica una serie de procesos y tareas interconectadas que son esenciales para la creación de un producto. Este lapso abarca desde la noción inicial del proyecto y finaliza en su

implementación definitiva e implica actividades como el análisis de requisitos, el diseño, la codificación, las pruebas y la entrega.

Cumplimiento de plazos: En la investigación de FLOCERT (2017), se da a conocer que el cumplimiento de plazos se refiere al momento dentro del ciclo en el que se establece la aplicabilidad de un criterio específico de cumplimiento y, por lo tanto, se requiere su cumplimiento. En otras palabras, el plazo de cumplimiento determina el punto en el tiempo en el que un requisito o estándar particular debe ser satisfecho.

Adaptabilidad a cambios y mejoras: Según Rodríguez (2022), la adaptabilidad se refiere a la capacidad de un sistema para incorporar de manera factible y a un costo razonable nuevas funcionalidades que no se habían previsto inicialmente, así como para manejar gradualmente cargas mayores de las que se habían considerado en un principio. En otras palabras, la adaptabilidad implica la adaptabilidad y la capacidad de reacción de un sistema para hacer frente a cambios y desafíos inesperados al permitir la integración de nuevas características y soportar cargas adicionales de manera escalonada.

Coherencia y estructura de la documentación: Evalúa si la documentación del modelo metodológico presenta una estructura lógica y coherente, con secciones claramente definidas, instrucciones secuenciales y una presentación clara de los conceptos clave. Según Maida y Paciencia (2015) una documentación bien estructurada facilita la comprensión y aplicación del modelo.

Variable dependiente

Empresas de TI: Según Peter Weill y Jeanne W. Ross: " Las empresas de tecnología de la información son organizaciones que proporcionan servicios tecnológicos, soluciones y apoyo para atender las demandas de datos e interacciones de otras compañías y entidades. "

Dimensión

Calidad de los servicios de TI: Según (Molina, 2014). “La calidad de los servicios de TI significa la capacidad de una empresa de TI para satisfacer de manera confiable y rápida los deseos y necesidades de los usuarios. Esto significa brindar servicios tecnológicos fáciles de entender que estén disponibles cuando sea necesario y satisfagan las necesidades comerciales.”

Indicador

Nivel de satisfacción de los clientes: Los autores Anderson y Sullivan describen la satisfacción del cliente como una métrica singular que muestra en qué medida las vivencias y resultados de adquisición y utilización satisfacen o superan las expectativas del cliente.”

3.3. Población, muestra y muestreo

3.3.1 Población

La población fue de tipo infinita, ya que se realizó la investigación tomando en cuenta las oficinas o departamentos de tecnología de empresas que se encuentran en la región de Piura. Según Arias (2006), una población es un conjunto de elementos que comparten características comunes y puede ser finita o infinita. En el contexto del estudio, los resultados de la investigación de este grupo deben ser aplicables a todos los elementos y deben ser válidos independientemente de su número, porque su propósito es amplio.

- **Criterios de inclusión:** Oficinas o departamentos de tecnología y comunicaciones constituidas en la región de Piura.

- **Criterios de exclusión:** Oficinas o departamentos de tecnología y comunicaciones no constituidos y que no pertenecen a la región de Piura.

3.3.2 Muestra

El volumen de la muestra fue una Oficina de Tecnología y Comunicaciones de una organización en la región de Piura, basándose en los criterios de inclusión y exclusión. Esta oficina analizo el modelo metodológico para su respectiva evaluación. Según López-Roldán (2017), una muestra se refiere a una fracción o subconjunto de unidades características de un grupo mayor llamado población o universo. Estas unidades se determinan aleatoriamente y se estudian científicamente para producir resultados precisos que puedan generalizarse a todo el universo de estudio. Los resultados obtenidos están sujetos a tolerancias y probabilidades de error específicas que pueden determinarse caso por caso.

3.3.3 Muestreo

Este estudio utilizó un método de muestreo no probabilístico y la selección de individuos se basó en la conveniencia del equipo de investigación. Según Cuesta (2009), el muestreo no probabilístico se caracteriza por recoger una muestra sin asegurar una igualdad de oportunidades de elección para todos los miembros de la población.

3.3.4 Unidad de análisis

Oficinas o departamentos de tecnología y comunicaciones de empresas ubicadas en la región de Piura. Estas oficinas o departamentos constituyeron la población objetivo de estudio, y se eligió una de ellas para crear una muestra de forma cómoda.

3.4. Técnicas e instrumentos de recolección de datos

La técnica que se empleó en este estudio para recopilar datos fue la encuesta y consistió en utilizar como instrumento un cuestionario, el cual fue distribuido en 7 partes, una por cada indicador: “Protección de datos confidenciales”, “Cumplimiento de normas y regulaciones de seguridad”, “Tiempo de desarrollo”, “Cumplimiento de plazos”, “Adaptabilidad a cambios y mejoras”, “Coherencia y Estructura de la documentación” y “Nivel de satisfacción de los clientes”. Según Babbie (2016) una encuesta es un método de investigación en el que a un grupo específico de personas se le formula una serie de preguntas y luego sus respuestas se analizan

estadísticamente para obtener datos y detalles sobre la sociedad en la que se ubica la muestra. Se determinó la confiabilidad a través de la aplicación del método estadístico Alfa de Cronbach y su validez fue por medio de la valoración de Juicio de Expertos en la que tres profesionales del área de Ingeniería de Sistemas, corroboraron la validez del instrumento

Tabla 1. *Recolección de datos*

Dimensión	**Indicador**	**Técnica**	**Instrumento**	**Escala de medición**
Seguridad de la información	Protección de datos confidenciales	Encuesta	Cuestionario	Ordinal
	Cumplimiento de normas y regulaciones			
Eficiencia en el proceso de desarrollo	Tiempo de desarrollo			
	Cumplimento de plazos			
Cobertura de la documentación	Coherencia y estructura de la documentación			
Calidad de servicios de TI	Nivel de satisfacción de los clientes			

Validez Juicio de Expertos

VARIABLE: MODELO METODOLÓGICO

DIMENSION: SEGURIDAD DE LA INFORMACIÓN

INDICADOR: PROTECCIÓN DE DATOS CONFIDENCIALES

Tabla 2. *Validez del indicador protección de datos confidenciales*

Ítem	Esencial	Útil – No Esencial	No importante	CVR	CVR’
1	3	0	0	1.000	1.0000
2	2	1	0	0.333	0.6667
3	3	0	1	1.000	1.0000
4	2	0	0	0.333	0.6667
5	3	0	0	1.000	1.0000

La tabla de validez del indicador protección de datos confidenciales refleja la evaluación de cinco ítems o preguntas de una encuesta por un panel de tres jueces. Los ítems 1, 3 y 5 fueron considerados unánimemente como esenciales por todos los jueces, mostrando una fuerte concordancia en su importancia. Por otro lado, el ítem 2 presentó una opinión dividida, con dos jueces considerándolo esencial y uno viéndolo como útil pero no esencial. El ítem 4 fue visto como esencial por dos jueces. Cabe destacar que, aunque el ítem 3 fue considerado esencial por todos, hubo un voto en la categoría "No Importante", lo que podría sugerir un error en la recopilación o registro de datos. En general, la mayoría de los ítems fueron considerados esenciales, pero hay ciertas discrepancias en la percepción de la importancia entre algunos de ellos.

INDICADOR: CUMPLIMIENTO DE NORMAS Y REGULACIONES

Tabla 3. *Validez del indicador cumplimiento de normas y regulaciones*

Ítem	Esencial	Útil – No Esencial	No importante	CVR	CVR’
6	2	1	0	0.333	0.6667
7	3	0	0	1.000	1.0000
8	3	0	1	1.000	1.0000
9	3	0	0	1.000	1.0000
10	3	0	0	1.000	1.0000

En la tabla de Validez del indicador cumplimiento de normas y regulaciones, el ítem 6 tuvo una opinión variada, con dos jueces considerándolo esencial y uno considerándolo útil pero no esencial. En contraste, los ítems 7, 9 y 10 recibieron una concordancia total, con todos los jueces coincidiendo en su esencialidad. El ítem 8, aunque fue clasificado unánimemente como esencial, tuvo un voto en la categoría "No Importante", lo que puede indicar una inconsistencia o error en los datos, similar a lo observado anteriormente en el ítem 3 del conjunto anterior. En resumen, a excepción del ítem 6, la mayoría de los ítems en este conjunto fueron considerados esenciales por todos los jueces, pero la posible inconsistencia en el ítem 8 debería ser revisada.

DIMENSION: EFICIENCIA EN EL PROCESO DE DESARROLLO DE SOFTWARE
INDICADOR: TIEMPO DE DESARROLLO

Tabla 4. *Validez del indicador tiempo de desarrollo*

Ítem	Esencial	Útil – No Esencial	No importante	CVR	CVR'
11	2	1	0	0.333	0.6667
12	2	1	0	0.333	0.6667
13	3	0	0	1.000	1.0000

La tabla de validez del indicador tiempo de desarrollo, los ítems 11 y 12 presentan opiniones similares, con dos jueces calificándolos como esenciales y un juez considerándolos útiles, pero no esenciales. Esto sugiere que, aunque hay una inclinación hacia la esencialidad, existe cierta discrepancia en la percepción de estos dos ítems. Por otro lado, el ítem 13 fue unánimemente clasificado como esencial por todos los jueces, reflejando una total concordancia en su importancia.

INDICADOR: CUMPLIMIENTO DE PLAZOS

Tabla 5. *validez del indicador cumplimiento de plazos*

Ítem	Esencial	Útil – No Esencial	No importante	CVR	CVR'
14	2	1	0	0.333	0.6667
15	2	1	0	0.333	0.6667
16	3	0	0	1.000	1.0000
17	2	1	0	0.333	0.6667

En la tabla validez del indicador cumplimiento de plazos, los ítems 14, 15 y 17 tienen evaluaciones idénticas: dos jueces los consideraron esenciales mientras que un juez los vio como útiles, pero no esenciales. Esta repetición en las calificaciones sugiere una tendencia donde hay una ligera inclinación hacia la esencialidad, pero con una nota de divergencia entre los jueces sobre la importancia total de estos ítems. En contraste, el ítem 16 se destaca al ser clasificado unánimemente como esencial por todos los jueces, lo que indica una total concordancia en su relevancia.

INDICADOR: ADAPTABILIDAD A CAMBIOS Y MEJORAS

Tabla 6. *Validez del indicador adaptabilidad a cambios y mejoras*

Ítem	Esencial	Útil-No esencial	No importante	CVR	CVR’
18	2	1	0	0.333	0.6667
19	2	1	0	0.333	0.6667
20	2	1	0	0.333	0.6667

La tabla validez del indicador adaptabilidad a cambios y mejoras, los ítems 18, 19 y 20 al ser sometidos a evaluación En su análisis, dos de los expertos calificaron cada ítem como "Esencial", mientras que el tercer experto los consideró "Útil, pero no Esencial". Cabe destacar que ninguno de los expertos juzgó a estos ítems como "No Importante". En este caso, los tres ítems tienen un CVR' de 0.6667, superando claramente el umbral establecido. Por lo tanto, podemos concluir que los ítems 18, 19 y 20 están bien formulados y cuentan con la aprobación de los expertos, no siendo necesario su eliminación o revisión basándose en este criterio.

DIMENSION: COBERTURA DE LA DOCUMENTACIÓN

INDICADOR: COHERENCIA EN LA ESTRUCTURA DE LA DOCUMENTACIÓN

Tabla 7. *Validez del indicador coherencia en la estructura de la documentación*

Ítem	Esencial	Útil-No esencial	No importante	CVR	CV’R
21	2	0	1	0.333	0.6667
22	2	1	0	0.333	0.6667
23	2	1	0	0.333	0.6667
24	3	0	0	1.000	1.0000
25	2	1	0	0.333	0.6667

Continuando con la evaluación en la tabla validez del indicador coherencia en la estructura de la documentación, los ítems del 21 al 25 fueron también analizados por los tres expertos. El ítem 21 fue calificado mayoritariamente como "Esencial", aunque un experto lo consideró "No Importante". Los ítems 22, 23 y 25 tuvieron un consenso similar, siendo vistos principalmente como "Esencial". Notablemente, el ítem 24 fue unánimemente reconocido como "Esencial" por todos. Al igual que los ítems anteriores, todos estos superaron el umbral de CVR' de 0.5823, confirmando su adecuada formulación y aceptación por el panel de expertos.

VARIABLE: EMPRESAS DE TI

DIMENSIÓN: CALIDAD DE LOS SERVICOS DE TI

INDICADOR: NIVEL DE SATISFACCIÓN DE LOS CLIENTES

Tabla 8. *Validez del indicador nivel de satisfacción de los clientes*

Ítem	Esencial	Útil-No esencial	No importante	CVR	CV'R
1	2	1	0	0.333	0.6667
2	3	0	0	1.000	1.0000
3	2	0	1	0.333	0.6667
4	3	0	0	1.000	1.0000
5	3	0	0	1.000	1.0000
6	2	1	0	0.333	0.6667
7	2	1	0	0.333	0.6667
8	3	0	0	1.000	1.0000
9	2	0	1	0.333	0.6667
10	2	1	0	0.333	0.6667

En la tabla Validez del indicador nivel de satisfacción de los clientes dentro de la variable "Empresas de TI", se evaluaron los ítems del 1 al 10, que buscan medir el "NIVEL DE SATISFACCION DEL CLIENTE" en la dimensión "CALIDAD DE LOS SERVICIOS DE TI". Los ítems fueron evaluados por tres expertos. Los ítems 2, 4, 5 y 8 destacaron, siendo calificados unánimemente como "Esencial" por todos los expertos, lo que indica una alta relevancia en la satisfacción del cliente. Los ítems 1, 6, 7 y 10 fueron mayoritariamente considerados "Esenciales", aunque un experto los vio como "Útiles, pero no Esenciales". Por otro lado, los ítems 3 y 9 tuvieron una división de opiniones, con dos expertos calificándolos como "Esenciales" y uno como "No Importantes". A pesar de estas diferencias, todos los ítems superaron el umbral de CVR' de 0.5823, lo que sugiere que son adecuados para evaluar la calidad de los servicios de TI en términos de satisfacción del cliente. Por lo tanto, estos ítems son relevantes y no requieren modificación o eliminación basándose en esta evaluación.

Tabla 9. *Validez de instrumento para medir la variable Modelo metodológico*

N°	Experto	Grado académico	Puntaje
1	Castillo Jiménez Ivan Michell	Doctor en TIC	79.1
2	Juárez Nole Harry Smith	Ingeniero de Sistemas	82.3
3	Ublillus Farfán Segundo Williams	Magister en Ing. De sistemas	81.3
PROMEDIO			80.9

Fuente: elaboración propia

El resultado obtenido de la evaluación realizada por expertos para medir la variable "Modelo metodológico" arrojó un promedio de 80.9%. Esta cifra posiciona al instrumento en un rango de calificación de muy bueno. Esta evaluación refleja la apreciación positiva de los expertos respecto a la calidad y precisión del instrumento en cuestión.

Tabla 10. *Validez de instrumento para medir la variable Empresas de TI*

N°	Experto	Grado académico	Puntaje
1	Castillo Jiménez Ivan Michell	Doctor en TIC	72.2
2	Juárez Nole Harry Smith	Ingeniero de Sistemas	82.3
3	Ublillus Farfán Segundo Williams	Magister en Ing. De sistemas	83.1
PROMEDIO			79.2

Fuente: elaboración propia

El resultado obtenido de la evaluación realizada por expertos para medir la variable "Empresas de TI" mostró una media del 79.2%. Este valor sitúa la herramienta en un nivel de muy bueno. Dicha evaluación representa la valoración favorable de los especialistas sobre la exactitud y calidad de la herramienta analizada.

Confiabilidad de instrumentos

Hernández, Fernández y Baptista (2014) subrayan la importancia de evaluar la solidez de una herramienta de medición. Para hacerlo, es necesario recurrir a distintos métodos y técnicas. El criterio principal para determinar esta solidez se basa en la capacidad de la herramienta para, cuando se aplica de manera reiterada al mismo individuo o muestra, generar resultados que sean consistentes y comparables entre sí. Es decir, si se obtienen los mismos o muy similares resultados en mediciones repetidas, se puede inferir que el instrumento es confiable.

Alfa de Cronbach

Según Pérez (2023) el alfa de Cronbach es una evaluación de coherencia interna, lo que implica el nivel de relación cercana entre un grupo de elementos cuando se analizan como un colectivo. Este coeficiente es interpretado como un indicador de la confiabilidad de la medición.

Tabla 11. *Rangos del alfa de Cronbach*

CONFIABILIDAD	DESCRIPCIÓN
<MENOS-0.53]	Confiabilidad nula
[0.54-0.59]	Confiabilidad baja
[0.60-0.65]	Confiable
[0.66-0.71]	Muy confiable
[0.72-0.99]	Excelente confiabilidad
1	Confiablidad perfecta

Fuente: helpstats(2018)

La evaluación total se efectuó con un conjunto de 17 participantes, con el objetivo de profundizar en la fiabilidad del instrumento que mide la variable independiente. Utilizando el software SPSS para el análisis, se determinó un coeficiente de fiabilidad de 0,772. Este resultado respalda la premisa inicial de que el instrumento es altamente fiable.

Tabla 12. *Confiabilidad de la variable independiente*

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,772	,764	25

Para la evaluación de la confiabilidad de la variable dependiente se llevó a cabo con el mismo conjunto de 17 participantes, con el fin de determinar la fiabilidad del instrumento en este aspecto específico. Tras procesar los datos mediante el software SPSS, se alcanzó un coeficiente de fiabilidad de 0,806. Este valor sugiere que el instrumento presenta una alta fiabilidad.

Tabla 13. *Confiabilidad de la variable dependiente*

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,806	10

3.5. Procedimientos

Con el propósito de crear un modelo metodológico efectivo y aplicable para mejorar la calidad en el desarrollo de sistemas tecnológicos en empresas de TI, se estableció la obligatoriedad de seguir una serie de procedimientos. Estos procedimientos constituyen los pasos y acciones específicas que se llevarán a cabo para lograr el objetivo mencionado. Esta sección proporcionará una descripción detallada de los procedimientos propuestos, los cuales se fundamentan en un análisis minucioso de la norma ISO 27001, la revisión de metodologías existentes y la identificación de requisitos de seguridad específicos. Estos procedimientos serán la estructura central de nuestro estudio y nos permitirán diseñar un modelo metodológico que integre las mejores prácticas de seguridad de la información con los procesos de desarrollo de software. La implementación y evaluación de estos procedimientos nos facilitarán determinar su efectividad y realizar mejoras continuas para garantizar estándares de calidad y protección en el desarrollo de software en empresas de TI.

En la fase inicial, se llevó a cabo un análisis detenido de la normativa ISO 27001 con el objetivo principal de identificar y comprender a fondo los requisitos y prácticas

establecidos en dicha norma. Este análisis proporcionará una comprensión precisa de los principios y directrices de la norma.

Seguidamente, se llevó a cabo una evaluación de las metodologías existentes que se basan en la norma ISO 27001. Durante esta evaluación, se analizaron las fortalezas y debilidades de estas metodologías en términos de seguridad de la información y calidad del sistema. También se identificaron requisitos de seguridad de la información relevantes para el desarrollo de software en empresas de TI, cubriendo aspectos como la gestión de riesgos, la protección de datos y la seguridad en la arquitectura del software, entre otros.

Una vez completados el análisis y la evaluación, se definieron los procesos y actividades que formarán parte del modelo metodológico, con un enfoque especial en la seguridad de la información. Se elaboraron guías y documentación detallada que describieron de manera precisa los procesos, actividades y controles establecidos en el modelo metodológico.

Finalmente, se llevó a cabo una retroalimentación por parte de los equipos de desarrollo, permitiendo recopilar sus opiniones y sugerencias. Con base en esta retroalimentación, se realizaron ajustes necesarios en el modelo metodológico con el objetivo de optimizar su eficacia y asegurar su adecuación a las necesidades particulares de las empresas de tecnologías de información.

3.6. Método de análisis de datos

El análisis de datos en este estudio se realizó utilizando un enfoque estadístico descriptivo. De acuerdo con los autores Hernández, Fernández y Baptista (2014), este enfoque busca lograr una representación precisa de los elementos y características de un fenómeno o grupo. Su propósito principal es identificar y clasificar las variables de estudio, así como resumir y presentar los datos de manera objetiva.

Tras recopilar la información a través del cuestionario, se llevó a cabo un análisis destinado a obtener información relevante sobre los indicadores de seguridad, evaluación de riesgos y nivel de satisfacción de los clientes en la empresa

considerada en este estudio. Este proceso descriptivo permitirá una comprensión detallada de los datos recopilados, facilitando la identificación de patrones, tendencias y características fundamentales relacionadas con los aspectos mencionados.

3.7. Aspectos éticos

Consentimiento informado: Se logró la autorización de todos los individuos o grupos que formaron parte del estudio. Se les ha proporcionado información precisa y completa acerca del propósito, procedimientos, ventajas y posibles riesgos del estudio, permitiéndoles tomar decisiones informadas sobre su participación. En todo momento, se ha respetado su autonomía y privacidad.

Confidencialidad y anonimato: La privacidad y confidencialidad de los involucrados se ha resguardado de manera estricta. La información recopilada se ha procesado de manera segura, asegurando el carácter anónimo de los datos para prevenir el reconocimiento de las personas pertinentes.

Benevolencia y crueldad: Se han tenido en cuenta los posibles efectos del estudio en los individuos y en la sociedad en general. Se ha trabajado para optimizar las ventajas y reducir cualquier posible daño. Estos riesgos y beneficios han sido evaluados cuidadosamente para lograr un equilibrio ético apropiado.

Imparcialidad y equidad: Se ha garantizado que todos los procedimientos de investigación sean justos y equitativos. No se ha permitido ninguna forma de relegación o prejuicio en la elección de los individuos, la evaluación de la información y la comprensión de los hallazgos.

Divulgación y transparencia: La transparencia se ha preservado en todos los aspectos de la investigación. Los resultados se han expuesto de manera nítida y puntual, sin recurrir a manipulación ni distorsión de los datos. Todas las fuentes utilizadas se han citado debidamente, y se han reconocido las contribuciones de otros investigadores.

Revisión ética: Se ha procurado obtener la aprobación de un comité de ética de investigación u entidad equivalente cuando el proyecto de investigación incluye la participación de seres humanos, animales u otros aspectos sensibles. Se han seguido todas las regulaciones y reglas éticas pertinentes. Estos aspectos éticos se han considerado plenamente al diseñar el programa de investigación, asegurando el rigor científico y el respeto por todas las partes involucradas.

IV. RESULTADOS

4.1 Análisis estadístico descriptivo

En la etapa inicial del análisis sobre la protección de datos confidenciales en la empresa, se observó que no se ha implementado ningún modelo metodológico específico para el desarrollo de software. Esta falta de una estructura formal plantea desafíos significativos en varios aspectos cruciales para el funcionamiento eficiente y seguro de la empresa.

Primero y, ante todo, la ausencia de un modelo metodológico ha impactado notablemente en el tiempo de desarrollo de los proyectos de software. Sin una guía formal para seguir, el proceso de desarrollo carece de una estructura predefinida. Esto puede llevar a una mayor variabilidad en los tiempos de entrega, ya que los equipos de desarrollo pueden enfrentar dificultades al abordar los desafíos de manera coherente y eficiente. La falta de un método establecido puede conducir a retrasos imprevistos, ya que las decisiones y procesos no están estandarizados y pueden requerir más tiempo para su implementación.

Además, la falta de un modelo metodológico formal dificulta la adaptabilidad a cambios en los proyectos de desarrollo de software. La agilidad en la respuesta a las nuevas demandas del mercado o los requisitos cambiantes se ve comprometida debido a la falta de procesos flexibles y definidos. La ausencia de una estructura formal puede hacer que sea difícil ajustar las estrategias de desarrollo existentes para acomodar cambios significativos en los requisitos del proyecto.

En términos de cumplimiento de normas, la falta de un modelo metodológico específico puede resultar en un desafío para asegurar que los proyectos cumplan con las normativas y estándares relevantes en la industria. Sin una guía formal, la empresa puede tener dificultades para garantizar que sus prácticas de desarrollo se adhieran a las regulaciones de seguridad de datos y privacidad, lo que podría poner en riesgo la conformidad legal.

Finalmente, la carencia de un modelo metodológico formal también complica significativamente el cumplimiento de plazos. La falta de procesos estandarizados puede llevar a la falta de previsibilidad en los plazos de entrega. La falta de una estructura organizada para el desarrollo de software puede hacer que sea difícil establecer estimaciones realistas para la finalización de los proyectos, lo que puede afectar negativamente la puntualidad en las entregas.

En resumen, la ausencia de un modelo metodológico específico en la empresa tiene un impacto significativo en el tiempo de desarrollo, la adaptabilidad a cambios, el cumplimiento de normas y el cumplimiento de plazos en los proyectos de desarrollo de software. La falta de una estructura formal dificulta la eficiencia, la predictibilidad y la seguridad en el desarrollo de software, lo que subraya la importancia de implementar una metodología adecuada para abordar estos desafíos de manera efectiva.

A continuación, se presentan los resultados de las encuestas realizadas después de la evaluación del modelo metodológico en la empresa:

Tabla 14. *Alternativas de respuesta para las encuestas*

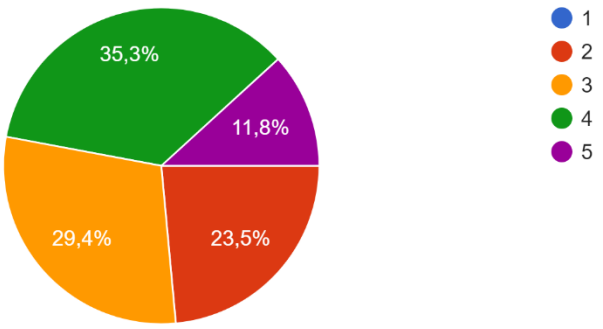
Alternativa de respuesta	Valor
Totalmente en desacuerdo	1
En desacuerdo	2
Neutro	3
De acuerdo	4
Totalmente de acuerdo	5

DIMENSION 1: Seguridad de la información

INDICADOR 1: Protección de datos confidenciales

1) El modelo metodológico basado en ISO 27001 ha mejorado la seguridad de la información en el desarrollo de software en la empresa

Figura 1. *Impacto del modelo metodológico en la seguridad de la información*

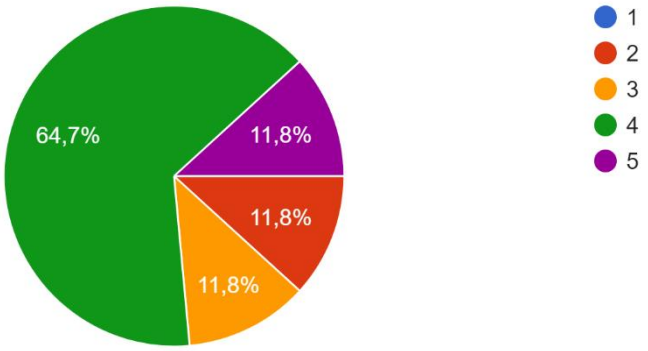


El análisis del primer ítem indica una percepción positiva general del modelo metodológico basado en ISO 27001. La mayoría de los expertos, específicamente el 35.3%, están de acuerdo en que el modelo ha mejorado la seguridad de la

información en el desarrollo de software en la empresa. Además, un 11.8% está totalmente de acuerdo con esta afirmación, lo que refuerza la validez y eficacia del modelo en cuestión. Si bien un 23.5% de los participantes marcó que estaban en desacuerdo, es importante resaltar que la proporción de expertos que valoran positivamente el modelo supera a aquellos con opiniones contrarias. Además, el 29.4% de los encuestados se mantuvo neutral, lo que puede interpretarse como una falta de experiencia directa o conocimiento completo sobre el impacto del modelo, más que como una percepción negativa del mismo. En resumen, el modelo metodológico basado en ISO 27001 ha recibido una acogida favorable entre los expertos, con una proporción significativa que reconoce sus beneficios en la mejora de la seguridad de la información en el desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

2) Proporciona medidas para prevenir el acceso no autorizado o la exposición de información en el desarrollo de software.

Figura 2. *medidas para prevenir el acceso no autorizado*

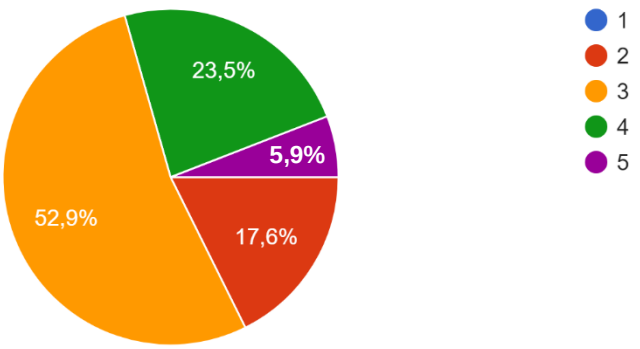


El análisis del ítem revela que la mayoría de los expertos reconocen y valoran las capacidades del modelo metodológico basado en ISO 27001 para prevenir el acceso no autorizado o la exposición de información en el desarrollo de software. De hecho, un contundente 64.7% de los expertos está de acuerdo con esta afirmación, lo que indica un respaldo significativo a las medidas de seguridad propuestas por el modelo. Además, un 11.8% de los encuestados se mostró

totalmente de acuerdo, enfatizando aún más la confianza en las fortalezas del modelo para proteger la información. Aunque un 11.8% de los participantes se mantuvo neutral y otro 11.8% expresó cierto desacuerdo, la abrumadora mayoría respalda la eficacia del modelo en cuanto a la prevención de accesos no autorizados. En resumen, el modelo metodológico basado en ISO 27001 es ampliamente reconocido entre los expertos como una herramienta efectiva que proporciona medidas robustas para salvaguardar la información en el proceso de desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

3) Evalúa y maneja los riesgos asociados con el desarrollo de software.

Figura 3. *Evalúa y maneja los riesgos asociados con el desarrollo de software.*

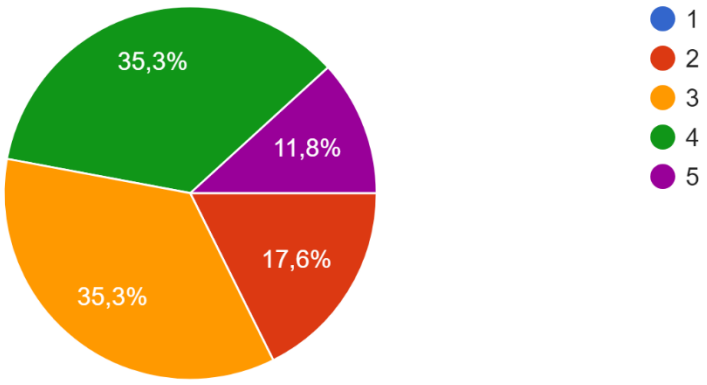


El análisis del tercer ítem destaca que una considerable proporción de expertos reconoce el potencial del modelo metodológico basado en ISO 27001 en la evaluación y gestión de riesgos asociados con el desarrollo de software. Un 23.5% de los expertos está de acuerdo en que el modelo cumple eficazmente con esta función, y un adicional 5.9% se muestra totalmente de acuerdo, reflejando un nivel de confianza elevado en sus capacidades. Aunque el 52.9% de los encuestados se posicionó de manera neutral, esto no necesariamente indica una visión negativa. Puede sugerir que algunos expertos no tienen experiencia directa con todas las características del modelo o desean ver más implementaciones prácticas antes de formarse una opinión definitiva. Solo un 17.6% expresó algún nivel de desacuerdo. Por lo tanto, es evidente que el modelo metodológico basado en ISO 27001 es

percibido por muchos expertos como una herramienta valiosa para abordar los desafíos relacionados con la evaluación y gestión de riesgos en el desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

4) El modelo ha mejorado la capacidad de anticiparse a posibles riesgos de seguridad en el desarrollo de software.

Figura 4. *Mejora en la anticipación de riesgos de seguridad*

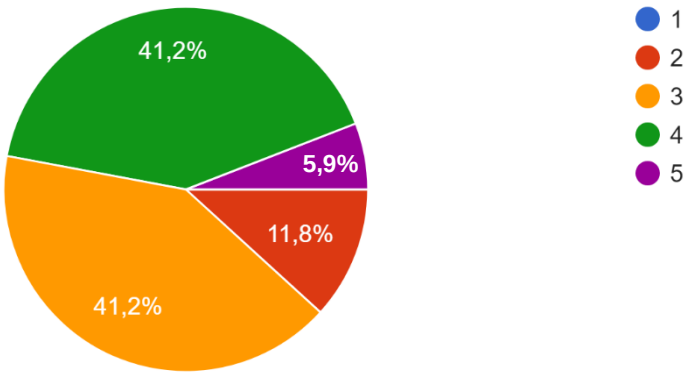


La evaluación del cuarto ítem revela un sentimiento predominante de confianza en el modelo metodológico basado en ISO 27001 en cuanto a mejorar la capacidad de anticipación frente a posibles riesgos de seguridad en el desarrollo de software. El 35.3% de los expertos está de acuerdo con esta afirmación, lo que indica una fuerte aprobación de las capacidades proactivas del modelo. Adicionalmente, un 11.8% de los participantes expresó un nivel de acuerdo total, subrayando aún más la eficacia del modelo en esta área. Es importante señalar que un 35.3% de los encuestados se mostró neutral; esto puede ser interpretado como una espera cautelosa para observar resultados a largo plazo o simplemente la necesidad de más información para tomar una posición firme. Con solo un 17.6% en desacuerdo, el consenso general es que el modelo metodológico basado en ISO 27001 posee herramientas y estrategias efectivas que permiten una mejor anticipación y gestión de los riesgos de seguridad en el desarrollo de software. Es relevante destacar que,

en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

5) Ha ayudado a mantener la integridad de la información durante el desarrollo de software.

Figura 5. *Mantenimiento de integridad de información.*



El análisis del quinto ítem resalta que muchos expertos valoran positivamente el papel del modelo metodológico basado en ISO 27001 en la preservación de la integridad de la información durante el desarrollo de software. Es evidente que un 41.2% de los expertos está de acuerdo con esta perspectiva, lo que indica una confianza notable en las capacidades del modelo para garantizar la integridad de los datos. Además, un 5.9% de los participantes se mostró totalmente convencido, reforzando la idea de que el modelo es altamente efectivo en este aspecto. Aunque un 41.2% de los encuestados optó por una postura neutral, esto no refleja necesariamente una percepción negativa; podría ser una señal de que algunos expertos desean más evidencia empírica o simplemente no han interactuado lo suficiente con todas las características del modelo. Con solo un 11.8% expresando desacuerdo, la interpretación global es que el modelo metodológico basado en ISO 27001 es ampliamente reconocido por su capacidad para mantener y proteger la integridad de la información en el proceso de desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

En lo que respecta a evaluar el primer objetivo “realizar un análisis exhaustivo de las metodologías existentes en el desarrollo de sistemas tecnológicos en empresas de TI”, se consideró el siguiente indicador:

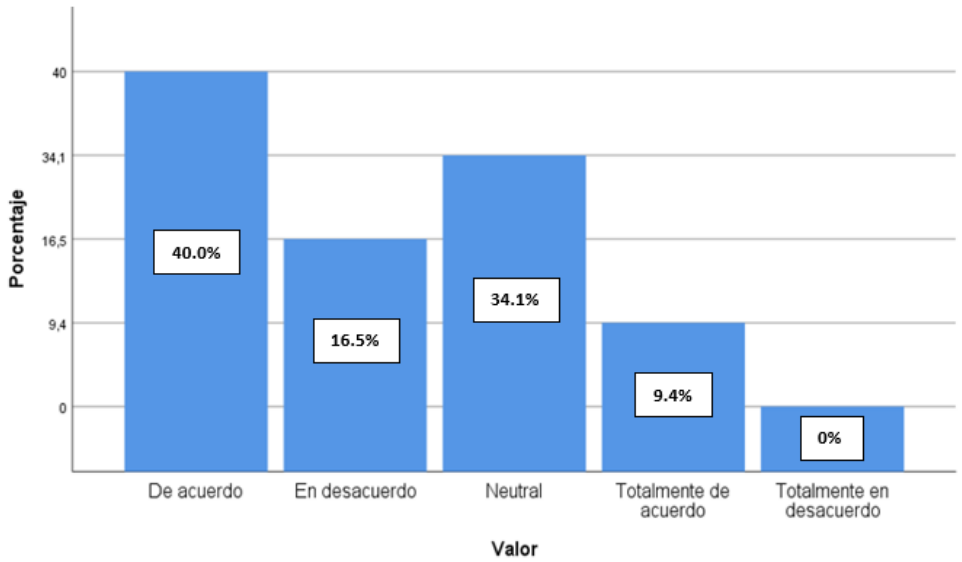
INDICADOR N°1: Protección de datos confidenciales

Tabla 15. *Protección de datos confidenciales*

Protección de datos confidenciales				
Valor	Frecuencia	Porcentaje	Porcentaje valido	Porcentaje acumulado
Totalmente en desacuerdo	0	0	0	0
En desacuerdo	14	16.5	16.5	16.5
Neutral	29	34.1	34.1	50.6
De acuerdo	34	40	40	90.6
Totalmente de acuerdo	8	9.4	9.4	100
Total	85	100	100	

En la evaluación del modelo metodológico respecto a la protección de datos confidenciales, la mayoría de los expertos mostraron una percepción neutral o positiva. Específicamente, un 74,1% se ubicó entre "Neutral" y "Totalmente de acuerdo". Aunque un 16,5% estuvo "En desacuerdo", ningún experto se posicionó en "Totalmente en desacuerdo". Estos resultados reflejan una aceptación generalizada del modelo en términos de protección de datos confidenciales, sugiriendo que, si bien puede haber áreas de mejora, el modelo ya posee una base robusta en este aspecto.

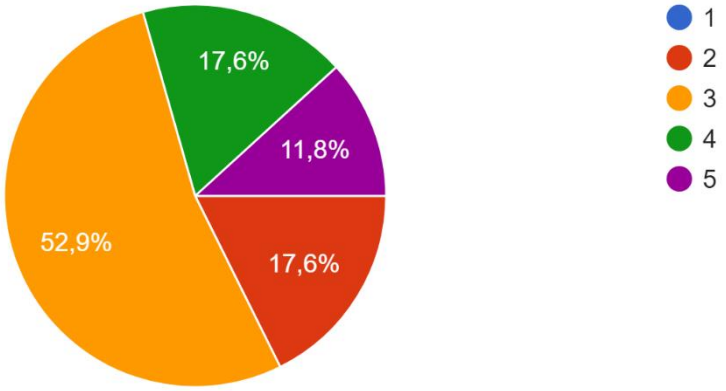
Figura 6. *Protección de datos confidenciales*



INDICADOR 2: Cumplimiento de normas y regulaciones

6) El cumplimiento de las normas y regulaciones de seguridad impacta positivamente en la calidad de los servicios de TI que ofrece la empresa.

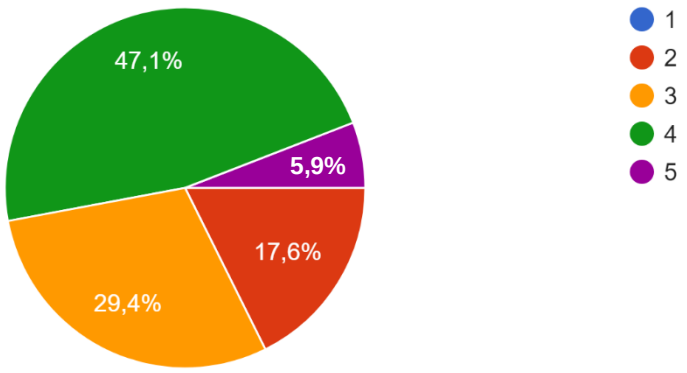
Figura 7. *Impacto del cumplimiento normativo en la calidad de servicios TI.*



El análisis del sexto ítem señala una apreciación general de la importancia del cumplimiento de normas y regulaciones en la calidad de los servicios de TI que ofrece la empresa. Un significativo 17.6% de los expertos está de acuerdo con la idea de que el cumplimiento de estas normas y regulaciones influye positivamente en la calidad de los servicios, mientras que un 11.8% está totalmente convencido de este impacto positivo, lo que subraya la relevancia de adherirse a estándares y regulaciones en el ámbito de TI. Es notable que más de la mitad de los encuestados, exactamente el 52.9%, se mantuvo neutral. Esta postura puede sugerir que, si bien muchos reconocen la importancia del cumplimiento, también podrían estar esperando evidencia más concreta o considerando otros factores que influyen en la calidad de los servicios. Sin embargo, con solo un 17.6% en desacuerdo, el consenso general tiende a favorecer la idea de que el modelo metodológico basado en ISO 27001, al enfatizar el cumplimiento de normas, contribuye de manera efectiva a elevar la calidad de los servicios de TI en la empresa. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

7) El Modelo metodológico basado en la norma ISO 27001 ha contribuido al cumplimiento de las normas y regulaciones de seguridad en el desarrollo de software

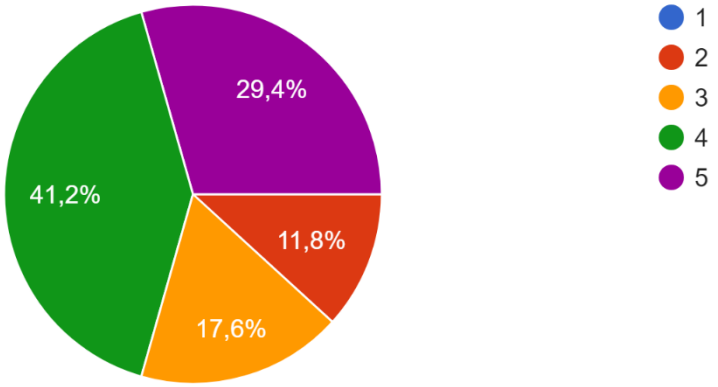
Figura 8. *Contribución al Cumplimiento de Normas de Seguridad.*



El análisis del séptimo ítem pone de manifiesto el reconocimiento de los expertos hacia el modelo metodológico basado en la norma ISO 27001 en su papel crucial para asegurar el cumplimiento de las normas y regulaciones de seguridad en el desarrollo de software. Un destacado 47.1% de los expertos está de acuerdo con la contribución del modelo en este ámbito, lo que refleja una confianza significativa en sus capacidades para guiar a las empresas hacia el cumplimiento de los estándares de seguridad. Además, un 5.9% de los encuestados enfatizó esta perspectiva, mostrándose totalmente de acuerdo, lo que refuerza aún más la percepción positiva de la eficacia del modelo. Aunque el 29.4% se mantuvo neutral, esto no necesariamente indica escepticismo; más bien, puede reflejar una postura cautelosa o la consideración de múltiples factores al evaluar el cumplimiento. Con una minoría del 17.6% en desacuerdo, la interpretación predominante es que el modelo metodológico basado en ISO 27001 es una herramienta valiosa y eficaz que facilita a las empresas de TI el cumplimiento de las normas y regulaciones esenciales de seguridad en el desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

8) El modelo metodológico ha facilitado la auditoría y la Demostración del cumplimiento de las normas y regulaciones de seguridad en el desarrollo de software según la norma ISO 27001

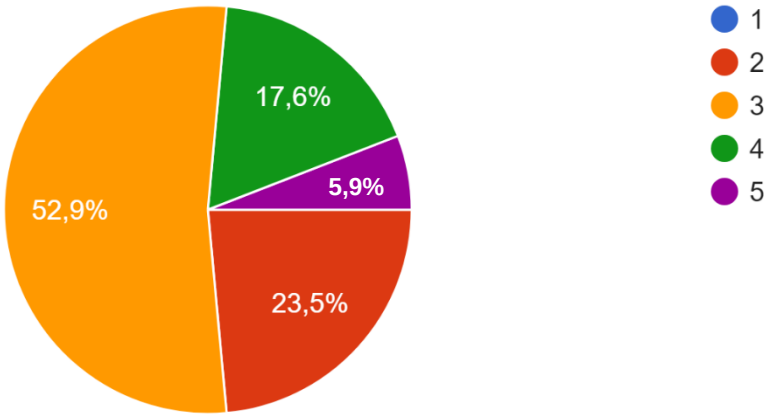
Figura 9. *Facilitación de Auditoría y Cumplimiento.*



El análisis del octavo ítem refleja un fuerte respaldo de los expertos hacia el modelo metodológico basado en la norma ISO 27001 en relación con su capacidad para facilitar la auditoría y demostración del cumplimiento de las normas y regulaciones de seguridad en el desarrollo de software. Una impresionante proporción del 41.2% de los encuestados está de acuerdo en que el modelo ha sido instrumental en este aspecto, evidenciando su eficacia en la facilitación de procesos de auditoría. Esta percepción positiva es aún más reforzada por el 29.4% de los expertos que se muestran totalmente convencidos de la utilidad del modelo en este contexto, subrayando su relevancia e impacto en el sector. Si bien un 17.6% adoptó una postura neutral, y solo un 11.8% expresó desacuerdo, el consenso general indica claramente que el modelo metodológico basado en ISO 27001 no solo es valioso para garantizar la seguridad en el desarrollo de software, sino que también es esencial para simplificar y optimizar los procesos de auditoría y demostración de cumplimiento, respaldando así la calidad y confiabilidad de las empresas de TI. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

9) El modelo metodológico ha optimizado la calidad de los servicios de TI

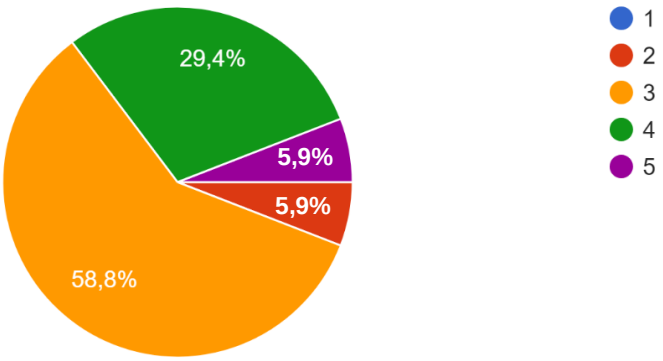
Figura 10. *Optimización de Calidad de Servicios de TI*



El análisis del noveno ítem destaca la percepción positiva que muchos expertos tienen del modelo metodológico basado en la norma ISO 27001 en relación con su influencia en la calidad de los servicios de TI. Un 17.6% de los expertos afirma estar de acuerdo con que el modelo ha jugado un papel vital en la optimización de la calidad de estos servicios. Esta perspectiva se ve reforzada por el 5.9% de los encuestados que se mostraron totalmente convencidos de la capacidad del modelo para elevar la calidad de los servicios de TI. Aunque más de la mitad, el 52.9%, adoptó una postura neutral, esto no implica necesariamente una visión negativa. Es posible que estos expertos estén considerando otros factores que influyen en la calidad o simplemente deseen más evidencia sobre el impacto directo del modelo. Con solo un 23.5% en desacuerdo, es evidente que, en general, el modelo metodológico basado en ISO 27001 es ampliamente reconocido como una herramienta que contribuye significativamente a mejorar y optimizar la calidad de los servicios de TI en la industria. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

10) El modelo metodológico basado en la norma ISO 27001 ha resultado en avances observables en la calidad de los servicios de TI ofrecidos por la empresa.

Figura 11. *Calidad de los Servicios de TI*



El análisis del décimo ítem resalta la confianza de los expertos en la capacidad del modelo metodológico basado en la norma ISO 27001 para generar mejoras palpables en la calidad de los servicios de TI ofrecidos por la empresa. Un notable 29.4% de los expertos está de acuerdo en que el modelo ha llevado a avances observables en este ámbito, lo que refleja una clara apreciación de las ventajas que aporta. Esta idea se ve aún más fortalecida por el 5.9% que está totalmente de acuerdo, subrayando la transformación positiva que el modelo ha impulsado en la industria. Es relevante destacar que la mayoría, un 58.8%, se mantuvo neutral, lo que puede sugerir que, si bien reconocen el potencial del modelo, están pendientes de más evidencia o implementaciones a largo plazo para consolidar su opinión. Con solo un 5.9% en desacuerdo, la tendencia general apunta a que el modelo metodológico basado en ISO 27001 es ampliamente valorado como un catalizador para elevar y renovar la calidad de los servicios de TI en las empresas. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

Con respecto a evaluar el segundo objetivo “diseñar un modelo metodológico que integre las mejores prácticas de desarrollo de sistemas tecnológicos y los estándares de seguridad de la información”, se consideró al siguiente indicador:

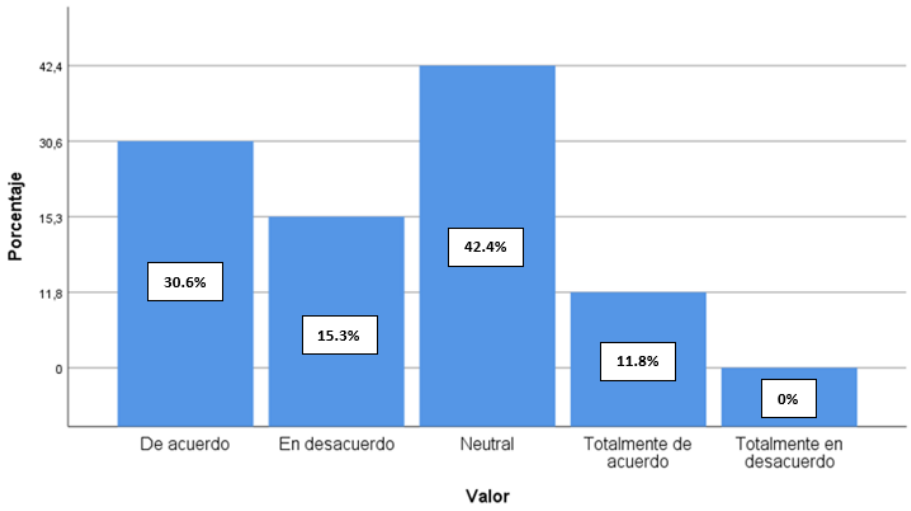
INDICADOR: Cumplimiento de normas y regulaciones de seguridad

Tabla 16. *Cumplimiento de normas y regulaciones de seguridad*

Cumplimiento de normas y regulaciones de seguridad				
Valor	Frecuencia	Porcentaje	Porcentaje valido	Porcentaje acumulado
Totalmente en desacuerdo	0	0	0	0
En desacuerdo	13	15.3	15.3	15.3
Neutral	36	42.4	42.4	57.7
De acuerdo	26	30.6	30.6	88.2
Totalmente de acuerdo	10	11.8	11.8	100
Total	85	100	100	

En la evaluación del modelo metodológico respecto al cumplimiento de normas y regulaciones de seguridad, la mayoría de los expertos mostraron una percepción neutral o afirmativa. Concretamente, un 84,8% de las respuestas osciló entre "Neutral" y "Totalmente de acuerdo". A pesar de que un 15,3% estuvo "En desacuerdo", ningún experto se mostró "Totalmente en desacuerdo". Estos datos refuerzan la idea de que el modelo ya está ampliamente alineado con las normativas de seguridad, y sugieren que las posibles mejoras a realizar serían mínimas y focalizadas.

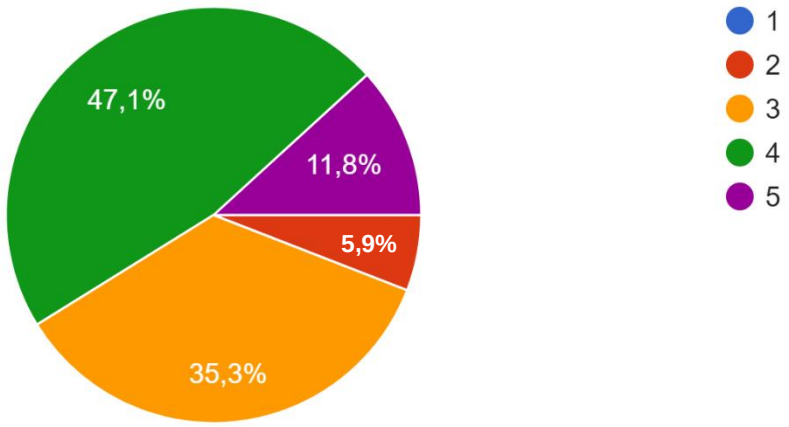
Figura 12. *Cumplimiento de normas y regulaciones de seguridad*



DIMENSIÓN: Cobertura de la documentación
INDICADOR: Coherencia y estructura de la documentación

11) La documentación del modelo metodológico tiene una estructura clara y organizada, con secciones bien definidas y un orden lógico de contenido.

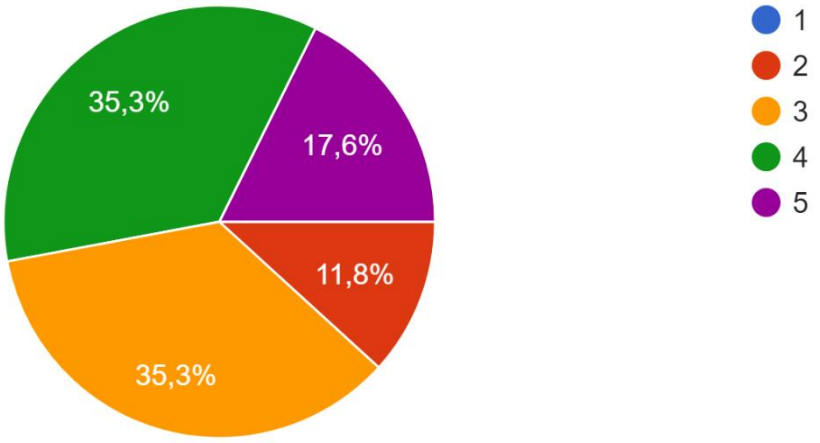
Figura 13. *Estructura de Documentación del Modelo Metodológico*



Al explorar las percepciones sobre la estructura y organización de la documentación del modelo metodológico, es destacable que casi la mitad, el 47,1% de los encuestados, siente que la documentación tiene una estructura clara y organizada. Esta afirmación es reforzada por un 11,8% adicional que está plenamente convencido de la coherencia y orden lógico del contenido. Juntos, estos datos reflejan que casi el 60% de los encuestados aprecia la claridad y estructura organizada de la documentación. Además, el 35,3% que adoptó una postura neutral puede ser interpretado como una oportunidad para resaltar aún más las características y beneficios de la estructura de la documentación, y para proporcionar más orientación sobre su uso eficiente. Con solo un 5,9% en desacuerdo, los resultados subrayan que la documentación del modelo metodológico es ampliamente reconocida por su claridad, organización y presentación lógica, facilitando su comprensión y aplicación en el ámbito del desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

12) Las secciones de la documentación están claramente definidas y abordan aspectos específicos del modelo metodológico de desarrollo de software.

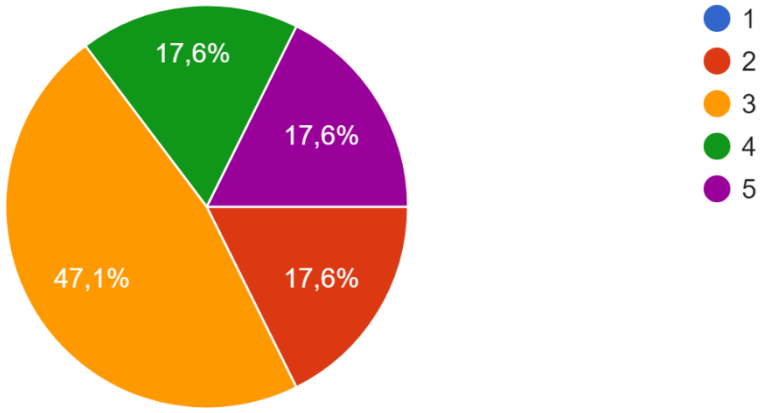
Figura 14. *Secciones Definidas en la Documentación del Modelo Metodológico*



Al evaluar las percepciones sobre las secciones de la documentación del modelo metodológico de desarrollo de software, es alentador encontrar que un 35,3% de los encuestados percibe que estas secciones están claramente definidas y abordan aspectos específicos del modelo. Esta visión es respaldada por un adicional 17,6% que está plenamente convencido de la precisión y definición de las secciones de la documentación. Sumados, estos porcentajes indican que más de la mitad de los encuestados aprecia la claridad y especificidad con la que se abordan los temas en la documentación. Además, el 35,3% que se mantiene neutral puede verse como una oportunidad para enfatizar aún más las ventajas de la estructura de la documentación y para ofrecer una mayor claridad sobre cómo cada sección se relaciona con aspectos específicos del modelo metodológico. Con solo un 11,8% en desacuerdo, los resultados resaltan que la documentación del modelo es ampliamente valorada por su claridad y enfoque detallado, facilitando su uso y comprensión en el ámbito del desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

13) La documentación proporciona instrucciones secuenciales y coherentes para aplicar el modelo metodológico.

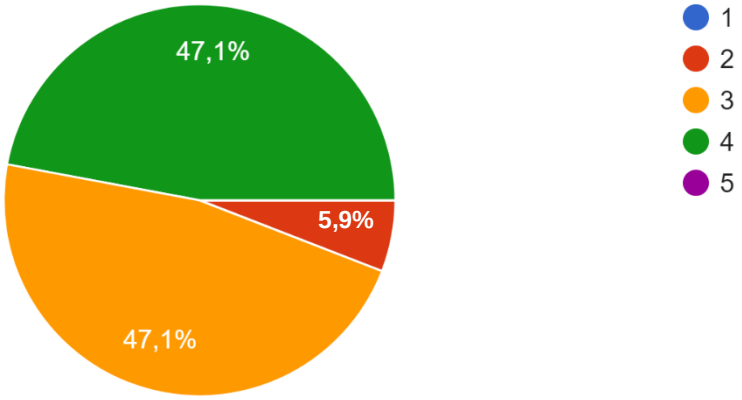
Figura 15. *Instrucciones Secuenciales en la Documentación*



Al considerar las percepciones sobre la coherencia y secuencia de instrucciones en la documentación del modelo metodológico, es positivo observar que un 17,6% de los encuestados siente que la documentación ofrece instrucciones coherentes y secuenciales para la aplicación del modelo. Esta perspectiva se refuerza con un 17,6% adicional que está plenamente convencido de la secuencialidad y coherencia de las instrucciones proporcionadas. Juntos, estos datos sugieren que más de un tercio de los encuestados encuentra valor en la forma en que la documentación guía la aplicación del modelo. Además, el 47,1% que optó por una respuesta neutral puede ser interpretado como una oportunidad para reforzar y destacar la estructura secuencial y coherente de las instrucciones en futuras revisiones de la documentación o en sesiones de capacitación. Con solo un 17,6% en desacuerdo, los resultados subrayan que la documentación es ampliamente percibida como una herramienta valiosa que ofrece una guía clara y ordenada para aplicar el modelo metodológico en el desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

14) La documentación presenta de manera clara los conceptos clave relacionados con el modelo metodológico.

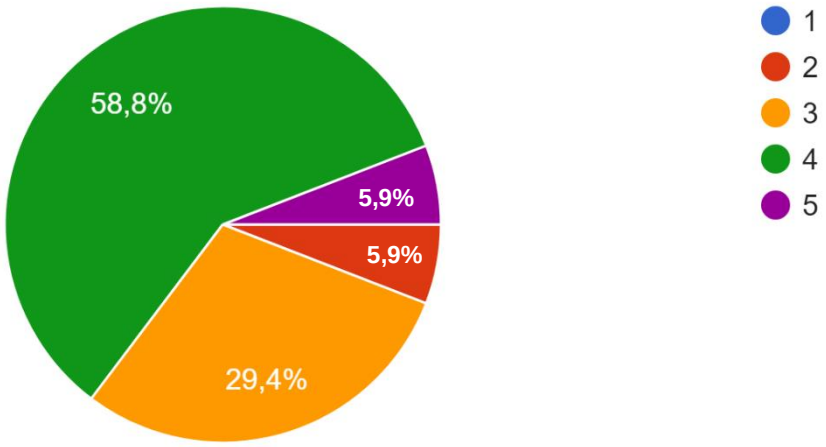
Figura 16. *Claridad en Conceptos Clave de la Documentación*



Al investigar las percepciones sobre la claridad con la que la documentación presenta los conceptos clave del modelo metodológico, es especialmente alentador que casi la mitad, el 47,1% de los encuestados, considere que la documentación presenta de manera clara y comprensible estos conceptos esenciales. Esta percepción es notable, ya que refleja que la documentación cumple eficazmente su papel en la transmisión de conocimientos fundamentales relacionados con el modelo. Además, el 47,1% que optó por una postura neutral puede ser visto no solo como una respuesta de indecisión, sino también como una oportunidad para mejorar aún más la claridad y enfatizar los conceptos clave en futuras versiones de la documentación o en sesiones de formación. Con solo un 5,9% en desacuerdo, los resultados demuestran que la documentación del modelo metodológico es ampliamente valorada por su capacidad para presentar de manera efectiva y clara los conceptos clave, facilitando la comprensión y aplicación de los mismos en el contexto del desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

15) La estructura y coherencia literaria de la metodología facilitan su implementación.

Figura 17. *Facilitación de Implementación con Estructura y Coherencia Literaria*



Al explorar cómo la estructura y coherencia literaria de la metodología impactan en su implementación, es destacable que más de la mitad, el 58,8% de los encuestados, siente que la coherencia y estructura literaria del material facilitan efectivamente su implementación. Este alto porcentaje refleja una percepción positiva sobre la legibilidad y lógica de la metodología, lo que es esencial para una implementación exitosa. Además, un 5,9% está plenamente convencido de las ventajas de la estructura y coherencia literaria en la facilitación de la implementación, subrayando aún más el valor de la metodología en este aspecto. Aunque el 29,4% se mantuvo neutral, esta respuesta puede interpretarse como una oportunidad para enfatizar aún más las características coherentes y estructuradas de la metodología en futuras sesiones de capacitación o revisiones del material. Con solo un 5,9% en desacuerdo, los resultados resaltan que la estructura y coherencia literaria de la metodología son ampliamente apreciadas y reconocidas como facilitadoras para su implementación en el ámbito del desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún

participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

En lo que respecta a evaluar el tercer objetivo “documentar, validar y difundir el modelo metodológico para su adopción y uso en empresas de TI” Se consideró el siguiente indicador:

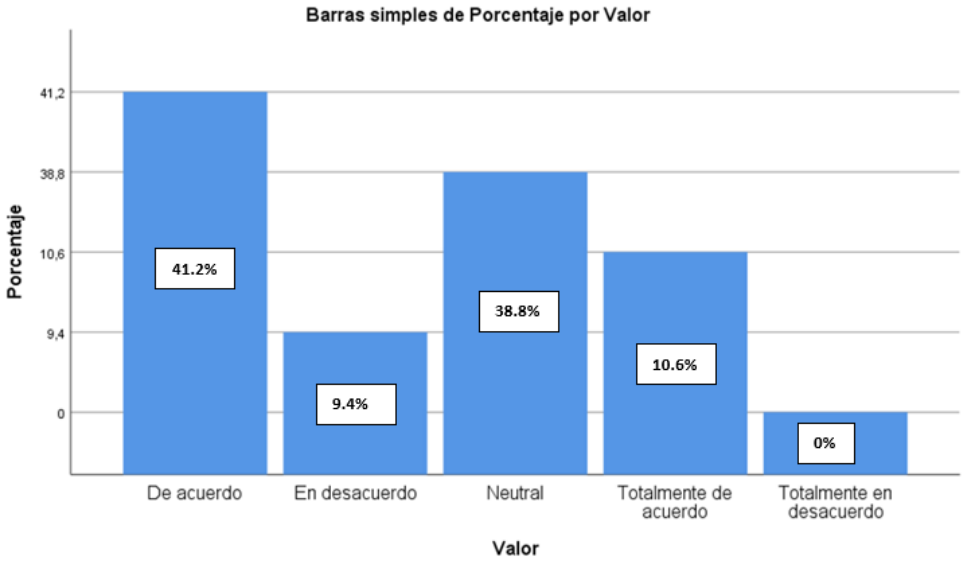
INDICADOR: Coherencia y estructura de la documentación

Tabla 17. *Coherencia y estructura de la documentación*

Coherencia y estructura de la documentación				
Valor	Frecuencia	Porcentaje	Porcentaje valido	Porcentaje acumulado
Totalmente en desacuerdo	0	0	0	0
En desacuerdo	8	9.4	9.4	9.4
Neutral	33	38.8	38.8	48.2
De acuerdo	35	41.2	41.2	89.4
Totalmente de acuerdo	9	10.6	10.6	100
Total	85	100	100	

En la evaluación del modelo metodológico sobre la coherencia y estructura de la documentación, el 90,6% de las respuestas de los expertos osciló entre "Neutral" y "Totalmente de acuerdo", evidenciando una percepción generalmente favorable. A pesar de que un 9,4% estuvo "En desacuerdo", la mayoría respaldó la calidad y estructura de la documentación del modelo, sugiriendo que las áreas de mejora serían específicas y no abarcadoras.

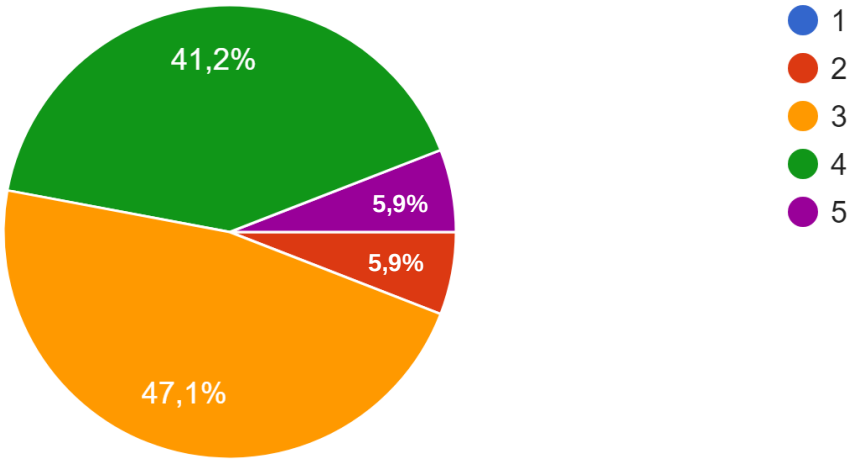
Figura 18. *Coherencia y estructura de la documentación*



VARIABLE DEPENDIENTE: Empresas de TI
DIMENSIÓN: Calidad de los servicios de TI
INDICADOR: Nivel de satisfacción de los clientes

1) El modelo metodológico basado en ISO 27001 ha mejorado la seguridad de la información en el desarrollo de software de la empresa

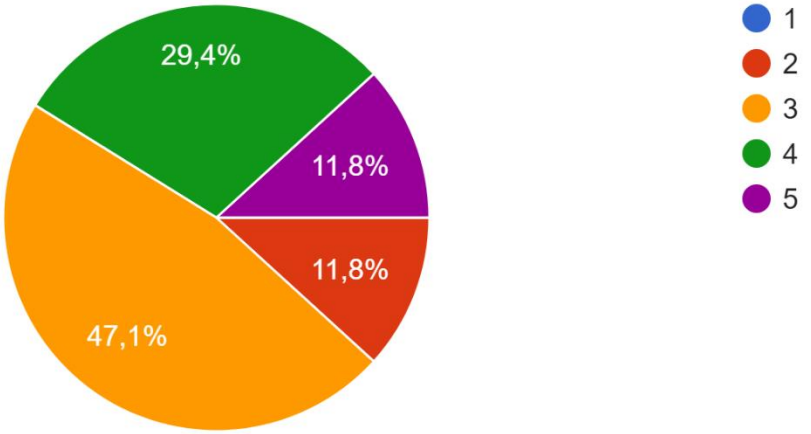
Figura 19. *Mejora de Seguridad de Información en Desarrollo de Software*



Al preguntar a los participantes si el modelo metodológico basado en ISO 27001 ha mejorado la seguridad de la información en el desarrollo de software de la empresa, resulta alentador ver que el 41,2% de los encuestados está de acuerdo con su efectividad, lo que refleja una percepción positiva del modelo. Además, es importante destacar que solo un pequeño porcentaje, el 5,9%, mostró desacuerdo, lo que sugiere que las críticas hacia el modelo son mínimas. Aunque el 47,1% de los participantes optó por una postura neutral, esto podría interpretarse como una oportunidad para brindar más información y formación sobre los beneficios del modelo, lo que podría inclinar aún más la balanza hacia una percepción favorable en futuras evaluaciones. Es evidente que el modelo ISO 27001 tiene un impacto positivo y es apreciado por una buena proporción de los encuestados. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

2) El modelo presenta claridad y coherencia al momento del desarrollo de software

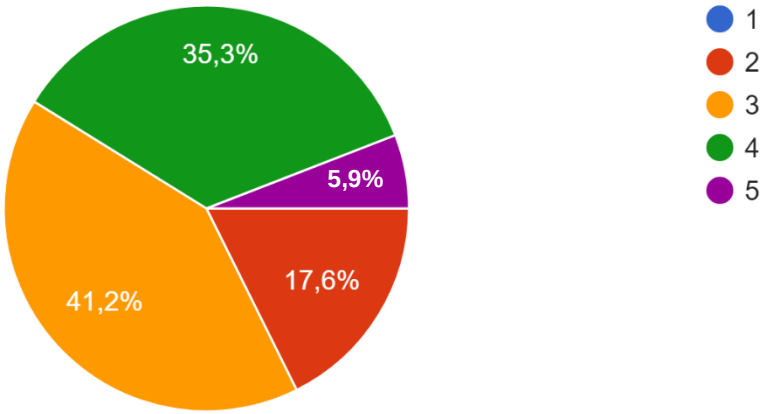
Figura 20. *Claridad y coherencia al momento del desarrollo de software*



Al abordar la percepción sobre si el modelo presenta claridad y coherencia durante el desarrollo de software, es notable que la mayoría de los encuestados tiene una percepción positiva o neutral. Específicamente, el 29,4% (5 de 17) de los encuestados considera que el modelo es claro y coherente, mientras que un adicional 11,8% (2 de 17) está totalmente de acuerdo con esta afirmación. Estas cifras suman un 41,2% que ve al modelo de manera favorable. Además, es alentador observar que la mayoría, el 47,1% (8 de 17), adopta una postura neutral, lo que podría interpretarse como una oportunidad para reforzar la claridad y coherencia del modelo a través de formación adicional. Solo una minoría, el 11,8% (2 de 17), expresó desacuerdo, lo que refleja que las críticas hacia la claridad y coherencia del modelo son limitadas. En conjunto, estos resultados demuestran que el modelo es percibido positivamente por una buena proporción de los encuestados en términos de claridad y coherencia en el desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

3) La metodología facilita la implementación efectiva de prácticas de seguridad en el desarrollo de software.

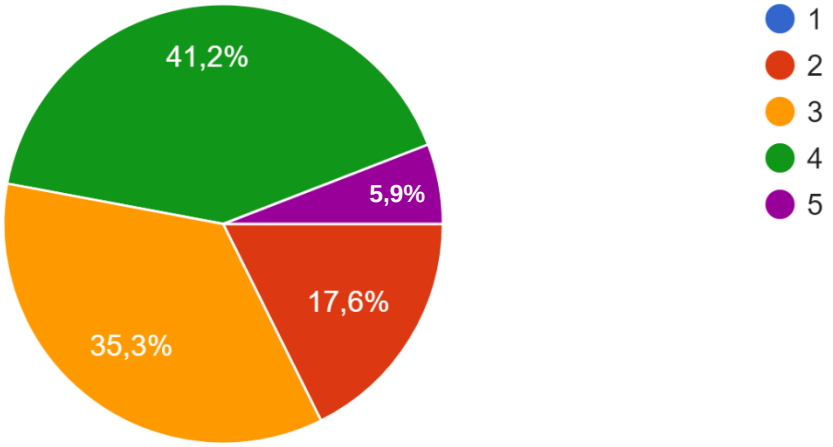
Figura 21. *Facilitación de Prácticas de Seguridad en Desarrollo de Software*



Al evaluar las percepciones sobre si la metodología facilita la implementación efectiva de prácticas de seguridad en el desarrollo de software, es alentador observar que un 35,3% de los encuestados siente que la metodología es facilitadora en este aspecto. Además, un 5,9% adicional está totalmente de acuerdo con esta perspectiva, lo que suma un 41,2% que ve a la metodología de manera favorable. Por otro lado, es positivo destacar que el 41,2% de los encuestados mantiene una postura neutral, lo que puede interpretarse como una oportunidad para reforzar aún más las ventajas de la metodología a través de formación o comunicación. Solo un 17,6% expresó desacuerdo y 0% totalmente en desacuerdo, lo que refleja que las críticas hacia la metodología en términos de facilitar prácticas de seguridad son limitadas. Estos resultados reflejan que la metodología es percibida de manera positiva por una buena proporción de los encuestados en cuanto a la implementación de prácticas de seguridad en el desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

4) Se adapta a las necesidades y características únicas de tu organización en el desarrollo de software.

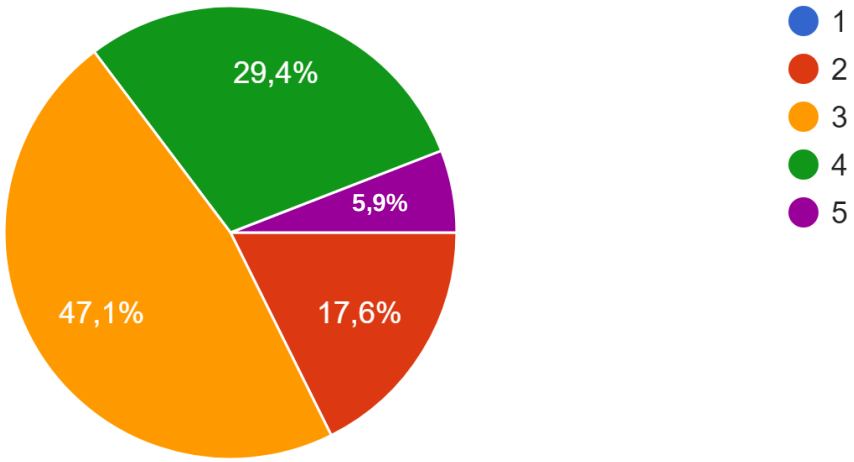
Figura 22. *Adaptación a las Necesidades en Desarrollo de Software*



sobre si la metodología se adapta a las necesidades y características únicas de su organización en el desarrollo de software, es alentador encontrar que un destacado 41,2% siente que la metodología se alinea bien con las especificidades de su organización. Además, un 5,9% adicional está plenamente convencido de esta adaptabilidad, lo que suma casi la mitad de los encuestados con una percepción favorable. Es también relevante destacar que el 35,3% tiene una postura neutral, lo que podría ser interpretado como una oportunidad para aclarar y reforzar cómo la metodología puede ser adaptada de manera más eficiente a las necesidades individuales de cada organización. Mientras que solo un 17,6% expresó desacuerdo, es evidente que la metodología es ampliamente vista como adaptable y adecuada para satisfacer las particularidades de las organizaciones en el ámbito del desarrollo de software. Estos resultados son un testimonio positivo de la flexibilidad y pertinencia de la metodología en el contexto organizacional. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

5) Brinda medidas para prevenir acceso no autorizado o exposición de información en el desarrollo de software.

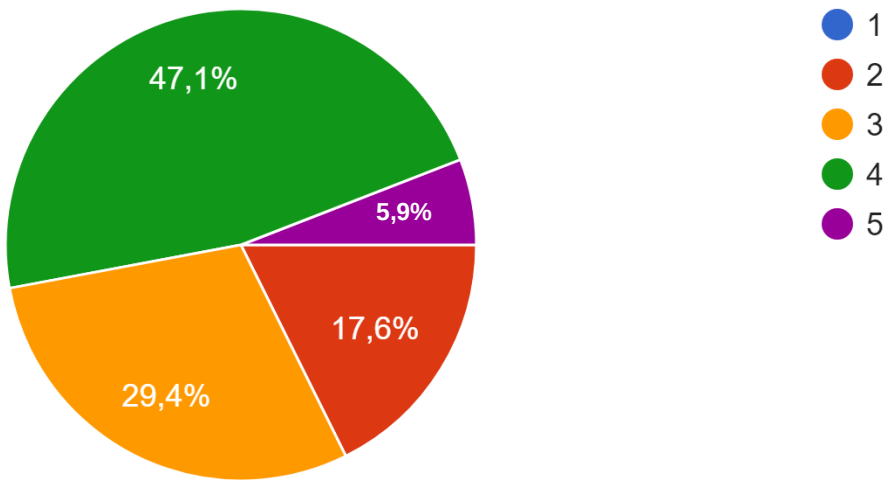
Figura 23. *Medidas de Prevención de Acceso No Autorizado*



Es alentador observar que una considerable proporción de encuestados, el 29,4%, siente que la metodología es compatible y se alinea adecuadamente con las singularidades de su organización. Además, un 5,9% de los participantes expresó total convicción en esta adaptabilidad, reflejando un fuerte respaldo a la metodología. Sumando ambas cifras, más de un tercio de los encuestados ve la metodología con una luz positiva en términos de adaptabilidad. Además, es destacable que el 47,1% adoptó una postura neutral. Esta respuesta, lejos de ser vista como indecisión, puede ser interpretada como una oportunidad para proporcionar más claridad y demostrar aún más cómo la metodología puede ser moldeada para satisfacer las demandas específicas de cada organización. Con solo un 17,6% en desacuerdo, los resultados resaltan que la metodología es ampliamente percibida como flexible y adecuada para las diferentes necesidades organizacionales en el desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

6) Ayuda a mantener la integridad de la información en el desarrollo de software.

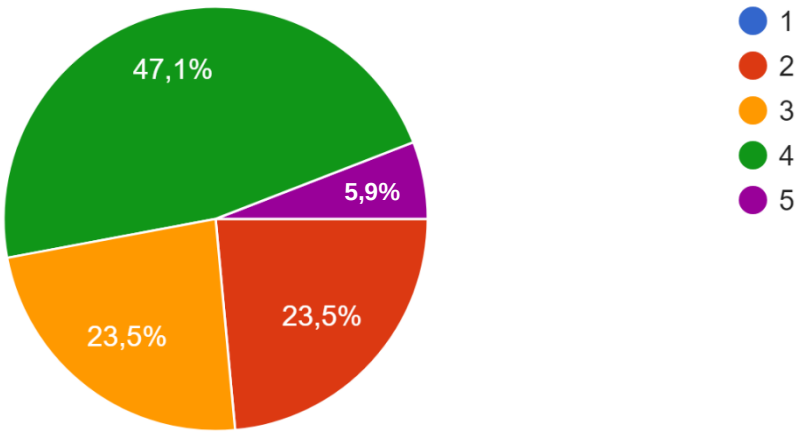
Figura 24. *Mantenimiento de Integridad de Información en Desarrollo de Software*



Al explorar la contribución de la metodología en el mantenimiento de la integridad de la información durante el desarrollo de software, es sumamente alentador descubrir que casi la mitad, el 47,1% de los encuestados, siente que la metodología desempeña un papel esencial en este aspecto. Esta percepción es reforzada por un adicional 5,9% que está completamente convencido de la capacidad de la metodología para asegurar la integridad de la información. Juntos, estos porcentajes reflejan que más de la mitad de los encuestados ven a la metodología como un instrumento valioso en la protección de la integridad de los datos. Aunque el 29,4% de los participantes se mantuvo neutral, esto puede verse como una oportunidad para enfatizar aún más los beneficios y características de la metodología que apoyan la integridad de la información. Con solo un 17,6% en desacuerdo, es evidente que la metodología es reconocida y valorada por su capacidad para mantener y resguardar la integridad de la información en el ámbito del desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

7) Fortalece la gestión de riesgos en el desarrollo de software en tu organización.

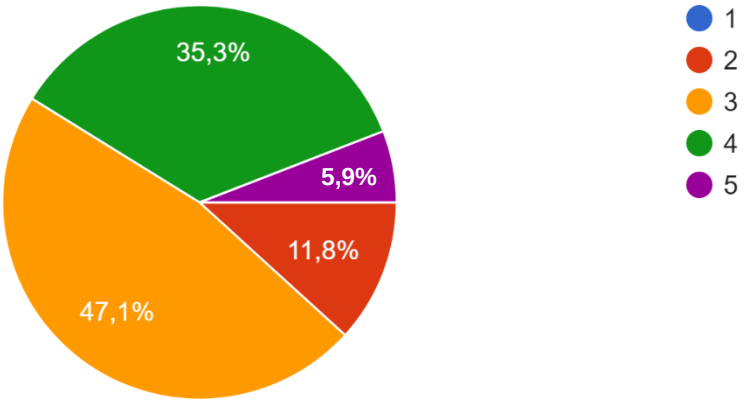
Figura 25. *Fortalecimiento en la gestión de riesgos*



Al analizar la eficacia de la metodología en el fortalecimiento de la gestión de riesgos durante el desarrollo de software, es destacable que casi la mitad de los encuestados, el 47,1%, reconoce que esta metodología juega un papel crucial en este proceso. Esta percepción positiva se ve reforzada por un 5,9% adicional de encuestados que están plenamente convencidos de las capacidades de fortalecimiento de la metodología en la gestión de riesgos. Estas cifras, juntas, indican que más del 50% de los encuestados ven a la metodología como una herramienta esencial para la gestión de riesgos en el desarrollo de software. Aunque el 23,5% se mantuvo neutral, esto no necesariamente indica indecisión, sino que puede reflejar una oportunidad para subrayar aún más los beneficios y ventajas de la metodología en este ámbito. Con un 23,5% en desacuerdo, es evidente que, a pesar de las diversas opiniones, una mayoría aprecia y valora la metodología por su capacidad para robustecer la administración de riesgos en el proceso de desarrollo de software en sus organizaciones. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

8) El modelo metodológico basado en ISO 27001 mejora la disponibilidad de la información en el desarrollo de software, es decir, se encuentra disponible cuando se necesita.

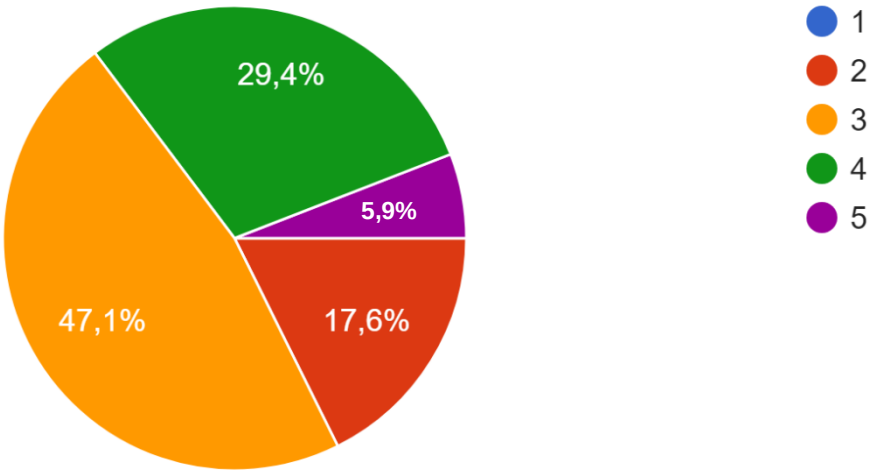
Figura 26. *Mejora de Disponibilidad de Información*



Cuando se explora la influencia del modelo metodológico basado en ISO 27001 en la mejora de la disponibilidad de la información durante el desarrollo de software, es inspirador observar que un 35,3% de los encuestados reconoce que el modelo es efectivo para asegurar que la información esté disponible cuando se necesita. Esta percepción se ve fortalecida por un 5,9% adicional que está totalmente convencido de las capacidades del modelo en este aspecto. Juntos, estos datos sugieren que casi el 41,2% de los encuestados ven al modelo metodológico basado en ISO 27001 como un pilar esencial para garantizar la disponibilidad oportuna de la información. Además, el 47,1% que se mantuvo neutral puede ser interpretado como una oportunidad para brindar más claridad sobre las ventajas del modelo, destacando aún más sus beneficios en la mejora de la disponibilidad de la información. Con solo un 11,8% en desacuerdo, es evidente que el modelo es ampliamente percibido como una herramienta valiosa para garantizar que los datos estén accesibles cuando se necesitan durante el proceso de creación de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

9) Evalúa y maneja los riesgos asociados con el desarrollo de software.

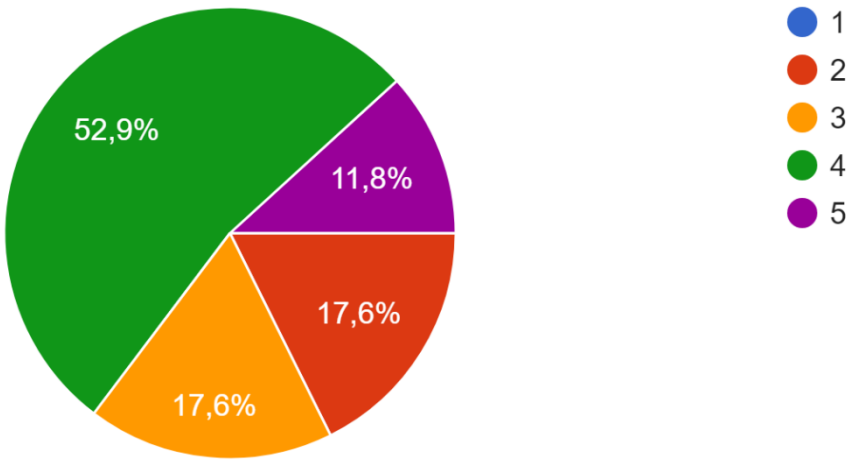
Figura 27. *Evalúa y maneja los riesgos asociados con el desarrollo de software.*



Al indagar sobre la capacidad de la metodología para evaluar y manejar los riesgos asociados con el desarrollo de software, es alentador ver que un 29,4% de los encuestados siente que la metodología es eficaz en esta tarea. Esta percepción positiva es respaldada por un 5,9% adicional que está plenamente convencido de la eficacia de la metodología en la evaluación y gestión de riesgos. Sumados, estos porcentajes reflejan que más de un tercio de los encuestados valora la metodología como un instrumento fundamental en la administración de riesgos. Además, el 47,1% que optó por una respuesta neutral puede ser visto como una oportunidad para resaltar y profundizar en las capacidades de la metodología en esta área, enfatizando aún más sus ventajas. Con solo un 17,6% en desacuerdo, queda claro que la metodología es ampliamente reconocida y apreciada por su capacidad para evaluar y manejar eficientemente los riesgos en el desarrollo de software. Es relevante destacar que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

10) Garantiza el cumplimiento de los estándares de seguridad de la información en el desarrollo de software.

Figura 28. *Garantía de Cumplimiento de Estándares de Seguridad*



Cuando se aborda la capacidad de la metodología para garantizar el cumplimiento de los estándares de seguridad de la información en el desarrollo de software, es notable y alentador que más de la mitad, específicamente el 52,9% de los encuestados, reconozca que la metodología es eficaz en garantizar dicho cumplimiento. Esta percepción se refuerza aún más con un 11,8% que está totalmente convencido de la capacidad de la metodología para garantizar la adherencia a los estándares de seguridad. Estas cifras, en conjunto, indican que casi dos tercios de los encuestados confían en la metodología como un medio fundamental para asegurar el cumplimiento de los estándares. Además, es relevante que el 17,6% que optó por una postura neutral puede representar una oportunidad para proporcionar más información y claridad sobre cómo la metodología garantiza el cumplimiento de estos estándares. Con solo un 17,6% en desacuerdo, los resultados resaltan que la metodología es ampliamente vista como un instrumento robusto y confiable para garantizar que el desarrollo de software esté en línea con los criterios de seguridad de la información. Es relevante destacar

que, en el análisis detallado, se observa que ningún participante, representando un 0% de los encuestados, expresó estar totalmente en desacuerdo.

INDICADOR: Nivel de satisfacción de los clientes

Tabla 18. *Nivel de satisfacción de los clientes*

Nivel de satisfacción de los clientes				
Valor	Frecuencia	Porcentaje	Porcentaje valido	Porcentaje acumulado
Totalmente en desacuerdo	0	0	0	0
En desacuerdo	27	15.9	15.9	15.9
Neutral	65	38.2	38.2	54.1
De acuerdo	66	38.8	38.8	92.9
Totalmente de acuerdo	12	7.1	7.1	100
Total	170	100	100	

Al explorar el nivel de satisfacción de los clientes con respecto a las empresas de TI, se observó una tendencia en su mayoría neutral o positiva. De las 170 respuestas recopiladas, ninguna se manifestó como "Totalmente en desacuerdo", lo que indica una ausencia de desaprobación extrema hacia los servicios prestados por estas empresas.

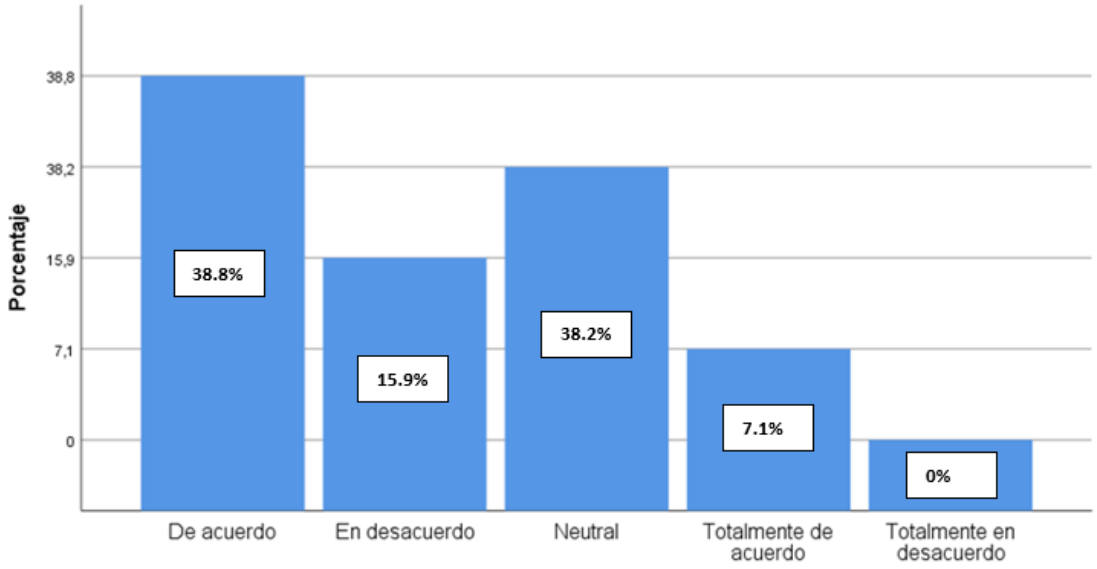
Un 15,9% de las respuestas se inclinaron hacia "En desacuerdo", lo que sugiere que hay ciertos aspectos que podrían ser revisados para mejorar la satisfacción del cliente. Sin embargo, es crucial resaltar que un notable 84,1% de las respuestas se agruparon entre "Neutral", "De acuerdo" y "Totalmente de acuerdo". Esto sugiere que la mayoría de los clientes tiene una percepción generalmente positiva o neutral de los servicios prestados por las empresas de TI.

El 38,8% de las respuestas se identificaron como "De acuerdo" y un 7,1% como "Totalmente de acuerdo", indicando un respaldo considerable a la excelencia de los servicios proporcionados.

En base a estos resultados, se pudo inferir que la implementación del modelo metodológico propuesto podría potenciar aún más la complacencia de los clientes

en las empresas de TI. Dado que la mayoría ya tiene una percepción favorable, la adopción de un modelo estructurado y eficiente como el propuesto podría consolidar y mejorar aún más esta percepción positiva, llevando a las empresas a alcanzar niveles de satisfacción aún más altos por parte de sus clientes.

Figura 29. *Nivel de satisfacción de los clientes*



V. DISCUSIÓN

Los resultados de esta investigación proporcionaron una visión retrospectiva esclarecedora sobre la efectividad del modelo metodológico desarrollado en el contexto de las empresas de TI. Los objetivos planteados en este estudio se centraron en evaluar cómo este modelo contribuyó a la mejora de la calidad y seguridad de los sistemas tecnológicos, su alineación con las mejores prácticas y regulaciones de seguridad, así como su capacidad para facilitar la documentación y su adopción en empresas de TI.

En lo que respecta al primer objetivo, que buscaba determinar si el análisis exhaustivo de las metodologías existentes contribuyó a la mejora de la calidad y seguridad de los sistemas tecnológicos, se consideró como indicador la protección de datos confidenciales. Los resultados de esta evaluación revelaron una percepción mayoritariamente positiva. Un sólido 74.1% de los expertos se posicionó entre "Neutral" y "Totalmente de acuerdo", lo que indicó que el modelo había logrado una aceptación generalizada en términos de la protección de datos confidenciales. Este hallazgo fue de gran relevancia en ese momento, ya que sugirió que el modelo metodológico se erigía como una herramienta efectiva en el contexto de la seguridad de la información. La falta de respuestas en la opción "Totalmente en desacuerdo" indicó que, si bien podía haber margen para mejoras, el modelo ya poseía una base sólida en este aspecto. Esto tenía implicaciones significativas en un entorno en el que la seguridad de datos era de importancia primordial, destacando la pertinencia del modelo en empresas de TI.

Al igual que la propuesta de Mora (2021), el modelo desarrollado en esta investigación reconoce la dinámica y cambiante naturaleza de las amenazas de seguridad en el entorno empresarial contemporáneo. En respuesta a esta realidad, se creó un enfoque que se adapta y fortalece continuamente, especialmente después de cada incidente potencial. Esta agilidad y capacidad de adaptación son esenciales para enfrentar los desafíos cada vez más complejos que presenta la ciberdelincuencia. Se cree firmemente que este enfoque proactivo y flexible, aplicado en el modelo, es crucial para salvaguardar la integridad y confidencialidad de la información en un mundo digital en constante cambio.

El segundo objetivo, que se centró en evaluar si el modelo metodológico se alineaba con las mejores prácticas y regulaciones de seguridad, se valió del indicador de "Cumplimiento de normas y regulaciones de seguridad". Los resultados de esta evaluación también fueron alentadores. Un sustancial 84.8% de las respuestas osciló entre "Neutral" y "Totalmente de acuerdo", lo que indicó que el modelo se encontraba ampliamente alineado con las normativas de seguridad.

La ausencia de respuestas en la categoría "Totalmente en desacuerdo" apuntó a que las mejoras necesarias podrían ser mínimas y específicas.
Este descubrimiento subrayó la importancia del modelo metodológico en la promoción de prácticas seguras y alineadas con las regulaciones de seguridad de la información. En un contexto en el que la ciberseguridad y la privacidad de los datos eran aspectos cruciales, este resultado reforzó aún más la relevancia del modelo y su capacidad para guiar a las empresas de TI en el cumplimiento de estándares y regulaciones.

En contraste al enfoque de Robalino (2018) de proponer varios modelos teóricos basados en las normas ISO 27001 y 27002, se optó por estudiar detenidamente otras metodologías ya existentes basadas en estas normas. Esta elección permitió examinar cómo estas metodologías se aplican en situaciones del mundo real y cómo son percibidas por los profesionales en este contexto específico. Es importante destacar que, aunque la metodología no fue aplicada directamente en este estudio, fue validada por profesionales de la población objetivo durante el proceso de validación de la investigación.

Finalmente, el tercer objetivo evaluó la facilidad en la documentación y difusión del modelo metodológico, utilizando como indicador "Coherencia y estructura de la documentación". Los resultados en esta área también respaldaron de manera contundente al modelo. Un destacado 90.6% de las respuestas de los expertos osciló entre "Neutral" y "Totalmente de acuerdo". A pesar del 9.4% que expresó desacuerdo, la mayoría confirmó la calidad y estructura de la documentación del modelo.

Este descubrimiento demostró que el modelo metodológico era una herramienta que se destacaba por su capacidad para ser documentada de manera clara y coherente. Esto tenía implicaciones significativas para su adopción en empresas de TI, ya que una documentación adecuada facilitaba la comprensión y el uso efectivo del modelo.

Así mismo el estudio de Castillo (2019) revela que la implementación de la Guía Metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014 en la Municipalidad Provincial de Recuay ha tenido un impacto positivo en la opinión de los usuarios acerca de la seguridad de los datos. Los resultados obtenidos indican que una parte significativa del personal calificó la guía como normal y bueno o excelente en términos de concientización, seguridad en la generación de documentos e incremento de la seguridad en el manejo de documentos en el sistema informático. Esta evaluación se alinea con los resultados obtenidos, donde se encontró una aceptación generalizada del modelo metodológico en términos de protección de datos confidenciales, alineación con las regulaciones de seguridad y facilidad en la documentación y adopción en empresas de TI.

En conjunto, los resultados de esta investigación reforzaron la validez de las hipótesis planteadas y subrayaron la efectividad del marco metodológico en la mejora de la calidad y seguridad de los sistemas tecnológicos en empresas de TI. Además, cabe mencionar que el modelo metodológico también deja espacio para mejoras y complementos futuros. Una posible dirección para fortalecer dicho marco metodológico es considerar la integración de tecnologías emergentes, como inteligencia artificial o blockchain, para reforzar aún más la seguridad de la información. Explorar la posibilidad de establecer alianzas estratégicas con expertos en ciberseguridad o llevar a cabo investigaciones adicionales para identificar nuevas amenazas podría enriquecer está metodología y hacerla aún más robusta. Estas consideraciones podrían proporcionar valiosas oportunidades para futuras investigaciones y mejoras en el modelo propuesto.

Además de las oportunidades ya mencionadas, existe un potencial adicional para el enriquecimiento del modelo metodológico. La consideración de mecanismos que

promuevan la conciencia continua sobre las prácticas de seguridad informática podría fortalecer la implementación efectiva del modelo en entornos de TI. Esto podría incluir programas de capacitación y simulacros de incidentes de seguridad, destinados a mantener a los profesionales actualizados y preparados para abordar amenazas emergentes. Asimismo, la expansión de la metodología para abordar aspectos específicos de la seguridad, como la gestión de accesos y la evaluación de riesgos, podría ser una vía para ampliar su aplicabilidad y relevancia en diversas áreas de las empresas de TI. Estas iniciativas podrían contribuir no solo a la mejora continua del modelo existente, sino también a su adaptación a las cambiantes dinámicas del panorama de seguridad cibernética y tecnológica.

VI. CONCLUSIONES

En el transcurso de esta investigación, se lograron alcanzar los objetivos propuestos, orientados a diseñar una metodología que impulse la calidad en el desarrollo de sistemas tecnológicos en empresas de TI, basada en la norma ISO 27001. De lo cual se han obtenido las conclusiones siguientes:

1. La metodología basada en la norma ISO 27001 para impulsar la calidad en el desarrollo de sistemas tecnológicos en empresa de TI ha demostrado cumplir con todos los indicadores al momento de su evolución, como se demuestra en los resultados obtenidos en las diferentes dimensiones.

2. En primer lugar, al cumplir el objetivo específico de llevar a cabo un análisis exhaustivo de las metodologías existentes que se emplean para el desarrollo de sistemas tecnológicos, se logró identificar aspectos y enfoques claves que describen sus fortalezas, debilidades, eficiencia, flexibilidad y adaptabilidad. Este análisis proporcionó una comprensión detallada de metodologías como DMAIC la cual proporciona un enfoque estructurado para la mejora de procesos, ITIL y su estándar reconocido por la gestión de servicios de TI, PDCA con su enfoque que promueve la mejora continua, entre otras. Estas metodologías resultaron fundamentales para la formulación de un enfoque metodológico basado en la norma ISO 27001.

3. En relación con el segundo objetivo específico, el modelo metodológico ha integrado las mejores prácticas en el desarrollo de sistemas tecnológicos y los estándares de seguridad de la información. Esta integración se evidencia en los resultados obtenidos productos de la evaluación del indicador "cumplimiento de normas y regulaciones", donde un 84,8% de las respuestas fluctúan entre "de acuerdo" y "totalmente de acuerdo". Este porcentaje indica que una amplia mayoría de los participantes respalda y confirma que el modelo metodológico cumple de manera efectiva con las normas y regulaciones establecidas. De este modo, el modelo desarrollado adopta los mejores estándares de seguridad de la información que proporciona la norma ISO 27001, impactando positivamente en la robustez y la seguridad

de los sistemas tecnológicos desarrollados. Esta adopción no solo fortalece la calidad del proceso de desarrollo, sino que también asegura la conformidad con las normativas vigentes, contribuyendo así a la seguridad y fiabilidad de los productos resultantes.

4. Finalmente, se logró cumplir con el tercer objetivo específico, el cual consistía en documentar, validar y difundir el modelo metodológico para su adopción y uso en empresas de tecnologías de la información. Al evaluar el indicador "Coherencia y estructura de la documentación", donde un 53% de las respuestas fueron positivas, se observó un respaldo significativo, evidenciado por el alto nivel de cumplimiento del indicador. La difusión activa de este modelo se considera crucial para su adopción y uso generalizado en empresas de TI. Para lograr esto, se llevarán a cabo diversas estrategias, como la organización de seminarios y talleres especializados para presentar y explicar el modelo a profesionales en el campo de las tecnologías de la información. Además, se elaborarán materiales informativos como manuales y guías, que se distribuirán entre la comunidad empresarial y académica. También se establecerán recursos en línea, como sitios web y blogs, para proporcionar acceso a la documentación y recursos adicionales relacionados con el modelo. Estas estrategias buscan asegurar una difusión efectiva del modelo metodológico, fortaleciendo su valor y aumentando su aplicabilidad en el ámbito empresarial de las tecnologías de la información.

5. Durante la investigación, se lograron los objetivos de diseñar y validar una metodología basada en ISO 27001 para mejorar la calidad en el desarrollo de sistemas tecnológicos en empresas de TI. La metodología ha demostrado eficacia en la evaluación, cumpliendo con indicadores clave. El análisis detallado de metodologías existentes contribuyó significativamente al desarrollo de un modelo adaptado a las necesidades de empresas de TI. La integración de mejores prácticas y estándares de seguridad fortaleció la calidad y seguridad de los sistemas tecnológicos, respaldado por una evaluación positiva del cumplimiento de normas. La documentación coherente facilita la difusión y prepara el terreno para la posible adopción del

modelo en empresas de TI. A pesar de estos logros, es esencial reconocer las limitaciones identificadas. Los indicadores de cumplimiento de plazos y adaptabilidad a cambios y mejoras presentan oportunidades de mejora. Para abordar estas limitaciones, futuras investigaciones pueden enfocarse en optimizar procesos y promover una mayor adaptabilidad continua.

VII. RECOMENDACIONES

1. Se sugiere a futuros investigadores establecer un proceso continuo de revisión y refinamiento del modelo metodológico basado en la norma ISO 27001 con el propósito de asegurar su adaptabilidad a diversos entornos tecnológicos y satisfacer las necesidades específicas de las organizaciones y empresas de tecnologías de la información. Esto facilitará mantener la relevancia del modelo en un entorno tecnológico en constante evolución, permitiendo su personalización para abordar los desafíos específicos de cada organización.

2. Dada la importancia y la urgencia de difundir la norma ISO 27001, se sugiere intensificar programas de formación que abarquen conductas de calidad y complementen los procesos de seguridad de la información. De esta manera se dispondrá de profesionales capaces e instruidos de emplear metodologías que contribuyan en el desarrollo de sistemas de información, salvaguardando la integridad de los datos y ampliando principios de seguridad de acuerdo a sus necesidades. La capacitación debería centrarse en la aplicación práctica de metodologías como DMAIC, ITIL y PDCA, en concordancia con los principios de la ISO 27001, asegurando un desarrollo de software robusto y seguro sin necesidad de una explicitación directa.

3. Se recomienda adoptar un enfoque proactivo hacia la investigación continua, buscando la integración constante de nuevas prácticas y tecnologías emergentes en la metodología. Mantenerse al tanto de los avances en el campo y ajustar la metodología de investigación de manera regular es fundamental para garantizar su pertinencia a largo plazo.

4. Se propone para futuras investigaciones explorar la integración de otras metodologías relevantes o metodologías ágiles, para mejorar la eficacia y adaptabilidad del modelo propuesto. Entre las metodologías que podrían considerarse se encuentran aquellas orientadas a la gestión ágil de proyectos, como Scrum, que podrían aportar flexibilidad y agilidad al proceso de desarrollo de software.

5. Aunque la validación inicial se propuso en colaboración con una municipalidad, se sugiere extender este enfoque a empresas de TI de diversos sectores. La adaptación y validación en entornos empresariales distintos permitirán evaluar la flexibilidad y aplicabilidad del modelo en situaciones variadas, fortaleciendo su utilidad y contribuyendo a un espectro más amplio de implementaciones exitosas.

REFERENCIAS

4RSOLUCIONES.*Calidad funcional software Archives | 4R Soluciones | Diseño, Desarrollo y Programación Web & Mobile. 4R Soluciones | Diseño, Desarrollo y Programación Web & Mobile [en línea]. Disponible en: https://www.4rsoluciones.com/tag/calidad-funcional-software/.*

ALEXANDER, A. y ANGÉLICA MURILLO GARZA. 2021. *Enfoques metodológicos en la investigación histórica: cuantitativa, cualitativa y comparativa. Debates por la Historia [en línea], vol. 9, no. 2, [consulta: 12 junio 2023]. Disponible en: https://www.redalyc.org/journal/6557/655768525006/html/.*

Mora, B., 2021*. Propuesta metodológica para la gestión de la seguridad de la información alineada a la norma ISO 27001 y ciberseguridad. Puce.edu.ec [en línea], [consulta: 9 julio 2023]. DOI https://doi.org/11639. Disponible en: http://repositorio.puce.edu.ec/handle/22000/21011.*

CASTILLO, L. 2019. *Propuesta de guía metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014 en la seguridad de la información en la Municipalidad Provincial de Recuay - 2015. Usanpedro.edu.pe [en línea], [consulta: 13 junio 2023]. DOI http://repositorio.usanpedro.edu.pe/handle/USANPEDRO/13634. Disponible en: http://repositorio.usanpedro.edu.pe/handle/USANPEDRO/13634.*

Ciclo de vida del software: todo lo que necesitas saber. Intelequia [en línea], 2023. [consulta: 9 julio 2023]. Disponible en: https://intelequia.com/blog/post/ciclo-de-vida-del-software-todo-lo-que-necesitas-saber.

CSIC, 2019. *Ética en la investigación. Consejo Superior de Investigaciones Científicas [en línea]. [consulta: 9 julio 2023]. Disponible en: https://www.csic.es/es/el-csic/etica/etica-en-la-investigacion#:~:text=La%20%C3%A9tica%20en%20la%20investigaci%C3%B3n,el%20progreso%20de%20la%20sociedad..*

DALLE, T., BONIOLO, SAUTU y ELBERT. *Manual de metodología. Construcción del marco teórico, formulación de los objetivos y elección de la metodología. [en línea]. S.l.: Disponible en: http://biblioteca.clacso.edu.ar/gsdl/collect/clacso/index/assoc/D1532.dir/sautu2.pdf.*

ESTHER, E. y ECHENIQUE, G. 2017. *Metodología de la Investigación. [en línea]. S.l.: Disponible en: https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf.*

FLORES, L., VILLEGAS HUAMANI, E. y ROSA, A. *La satisfacción del cliente como indicador de calidad. [en línea]. S.l.: Disponible en: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/628122/LizanoF_E.pdf?sequence=3.*

GLOBALSUITE SOLUTIONS. 2023. *¿Qué es la norma ISO 27001 y para qué sirve? GlobalSuite Solutions [en línea]. [consulta: 19 junio 2023]. Disponible en: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/.*

ISO 27001 - Sistemas de Gestión de Seguridad de la Información. Software ISO [en línea], 2023. [consulta: 9 julio 2023]. Disponible en: https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/.

JAVIER, 2022. *Aplicación de la norma ISO 27001 para la gestión de la seguridad de la información en la empresa Plataforma Buscador Académico BUSAC. S.A. en Ecuador. Ucv.edu.pe [en línea], [consulta: 19 junio 2023]. DOI https://hdl.handle.net/20.500.12692/102607. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/102607.*

JAVIER, F. y MAURICIO OROZCO ALZATE. 2017. *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação [en línea], no. 22, [consulta: 19 junio 2023]. DOI*

https://dialnet.unirioja.es/servlet/dcart?info=link&codigo=6672188&orden=0 *Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6672188.*

KRIPTOS. *La importancia del cumplimiento de regulaciones en la seguridad de información. Kriptos [en línea]. Disponible en: https://www.kriptos.io/es-post/la-importancia-del-cumplimiento-de-regulaciones-en-la-seguridad-de-informacion.*

LÓPEZ-ROLDÁN, P. y FACHELLI, S., [sin fecha]. METODOLOGÍA DE LA INVESTIGACIÓN SOCIAL CUANTITATIVA. [en línea]. S.l.: Disponible en: https://ddd.uab.cat/pub/caplli/2017/185163/metinvsoccua_cap2-4a2017.pdf.

Maida, Esteban Gabriel y Pacienzia, Julián. 2015. *Metodologías de desarrollo de software. [En línea] 2015. [Citado el: 18 de Junio de 2023.] https://repositorio.uca.edu.ar/bitstream/123456789/522/1/metodologias-desarrollo-software.pdf.*

Marco de ciberseguridad del NIST. Comisión Federal de Comercio [en línea], 2019. [consulta: 9 julio 2023]. Disponible en: https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist.

MARCO NIST.*CIBERSEGURIDAD Un abordaje integral de la Ciberseguridad. [en línea]. S.l.: Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf.*

METODOLOGIA DE LA INVESTIGACIÓN. [en línea. S.l.: Disponible en: http://virtual.urbe.edu/tesispub/0092660/cap03.pdf.

MIRANDA-CRUZ, M.B., TAPIA-HERMIDA, L.X., ROMERO-FLORES, M.L. y CHIRIBOGA-ZAMORA, P.A., 2021. *La calidad de los servicios y la satisfacción del cliente, estrategias del marketing digital. Caso de estudio hacienda turística rancho los emilio´s. Alausí. Dominio de las Ciencias [en línea], vol. 7, no. 4, Disponible en: http://dominiodelasciencias.com/ojs/index.php/es/indexhttps://orcid.org/0000-0002-5408-1200.*

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. [en línea]. 2019. Disponible en: https://1library.co/document/zpnew44y-analisis-diseno-gestion-seguridad-informacion-basados-artehogar-guayaquil.html.*
Normas ISO. Normas ISO [en línea], 2017. [consulta: 9 julio 2023]. Disponible en: https://www.normas-iso.com/iso-27001/.

Pentesting. *Slideshare.net [en línea], 2015. [consulta: 14 junio 2023]. Disponible en: https://es.slideshare.net/eventoscreativos/pentesting-4814058.*

Plazo de cumplimiento - FLOCERT. FLOCERT [en línea], 2017. [consulta: 9 julio 2023]. Disponible en: https://www.flocert.net/es/glossary/plazo-de-cumplimiento/.

Seguridad de datos: En qué consiste y qué es importante en tu empresa. Powerdata.es [en línea], 2018. [consulta: 18 junio 2023]. Disponible en: https://www.powerdata.es/seguridad-de-datos.
***SHARMA, P., 2022.** Estimación del tiempo de desarrollo de software: una guía práctica. Cynoteck [en línea]. [consulta: 20 junio 2023]. Disponible en: https://cynoteck.com/es/blog-post/software-development-time-estimation/#What_is_the_time_estimation_for_software_development.*

Tamayo y Tamayo, Mario - El Proceso de la Investigación Científica. *Scribd [en línea], 2023. [consulta: 19 junio 2023]. Disponible en: https://es.scribd.com/doc/12235974/Tamayo-y-Tamayo-Mario-El-Proceso-de-la-Investigacion-Cientifica.*

***TORO, R., 2018.** Confidencialidad, integridad y disponibilidad en los SG-SSI. PMG SSI - ISO 27001 [en línea]. [consulta: 14 junio 2023]. Disponible en: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/.*

What is ISO 27001 and How To Get an ISO 27001 Certification. Nqa.com [en línea], 2015. [consulta: 15 junio 2023]. Disponible en: https://www.nqa.com/es-pe/certification/standards/iso-

27001#:~:text=%C2%BFQu%C3%A9%20es%20la%20ISO%2027001,informaci%C3%B3n%2C%20as%C3%AD%20como%20cumplimiento%20legal.

WILLIAN, J., 2018. *Propuesta Metodológica y Simulación de la Implementación de un SIEM basado en la Norma ISO 27001 y/o 27002. Epn.edu.ec [en línea], [consulta: 15 junio 2023]. DOI https://doi.org/T-MVE/0698/CD%209078. Disponible en: https://bibdigital.epn.edu.ec/handle/15000/19672*.

ANEXOS

Anexo 1: Operacionalización de variables

VARIABLES DE ESTUDIO	DEFINICION CONCETUAL	DEFINICION OPERACIONAL	DIMENSION	INDICADORES	ESCALA DE MEDICION
Modelo metodológico	Según Creswell (2014): "Los modelos metodológicos son herramientas conceptuales y procedimentales que ofrecen un marco organizado y sistemático para abordar una investigación, proporcionando directrices claras y coherentes sobre cómo llevar a cabo un estudio."	La variable modelo metodológico tiene 3 dimensiones las cuales serán medidas mediante la técnica de la encuesta, aplicando el instrumento de cuestionario.	Seguridad de la información	Protección de datos confidenciales	ORDINAL
				Cumplimiento de normas y regulaciones de seguridad	
			Eficiencia en el proceso de desarrollo	Tiempo de desarrollo	
				Cumplimiento de plazos	
				Adaptabilidad a cambios y mejoras	
			Cobertura de la documentación	Coherencia y estructura de la documentación	
Empresas de TI	Según Peter Weill y Jeanne W. Ross: "Las empresas de TI son organizaciones que brindan servicios tecnológicos, soluciones y soporte para cumplir las demandas de	La variable empresas de TI tiene 1 dimensión las cuales serán medidas mediante la técnica de la encuesta, aplicando el instrumento de cuestionario.	Calidad de servicios de TI	Nivel de satisfacción de los clientes	ORDINAL

Anexo 2: Instrumentos de recolección de datos.

Alternativa de respuesta	Valor
Totalmente en desacuerdo	1
En desacuerdo	2
Neutral	3
De acuerdo	4
Totalmente de acuerdo	5

VARIABLE: Modelo metodológico							
DIMENSIÓN: SEGURIDAD DE LA INFORMACION							
INDICADOR	AFIRMACIÓN		ALTERNATIVAS DE RESPUESTA				
			1	2	3	4	5
Protección de datos confidenciales	1	El modelo metodológico basado en ISO 27001 ha mejorado la seguridad de la información en el desarrollo de software en la empresa.					
	2	Proporciona medidas para prevenir el acceso no autorizado o la exposición de información en el desarrollo de software.					
	3	Evalúa y maneja los riesgos asociados con el desarrollo de software.					
	4	El modelo ha mejorado la capacidad de anticiparse a posibles riesgos de seguridad en el desarrollo de software.					
	5	Ha ayudado a mantener la integridad de la información durante el desarrollo de software.					

Cumplimiento de normas y regulaciones de seguridad	6	El cumplimiento de las normas y regulaciones de seguridad impacta positivamente en la calidad					
		de los servicios de TI que ofrece la empresa					
	7	El modelo metodológico basado en la norma ISO 27001 ha contribuido al cumplimiento de las normas y regulaciones de seguridad en el desarrollo de software					
	8	El modelo metodológico ha facilitado la auditoría y la Demostración del cumplimiento de las normas y regulaciones de seguridad en el desarrollo de software según la norma ISO 27001					
	9	El modelo metodológico ha optimizado los servicios de TI después					
		El modelo metodológico					

	10	basado en la norma ISO 27001 ha resultado en avances observables en la calidad de los servicios de TI ofrecidos por la empresa.					

DIMENSIÓN: EFICIENCIA EN EL PROCESO DE DESARROLLO							
INDICADOR		**AFIRMACIÓN**	**ALTERNATIVAS DE RESPUESTA**				
			1	2	3	4	5
TIEMPO DE DESARROLLO	11	El tiempo de desarrollo de software se ha reducido gracias al modelo metodológico basado en la norma ISO 27001.					
	12	Se ha observado una optimización significativa en el tiempo de desarrollo de software después de aplicar el modelo metodológico basado en la norma ISO 27001.					
	13	El tiempo de desarrollo de software se vio afectado de manera positiva después aplicar el modelo metodológico basado en la norma ISO 27001.					

CUMPLIMIENTO DE PLAZOS	14	Los plazos establecidos para la finalización de proyectos de software se han cumplido de manera consistente desde el uso del modelo metodológico basado en la norma ISO 27001.					
	15	Los proyectos de desarrollo de software cumplen con los plazos establecidos de manera consistente y sin retrasos significativos.					
	16	Los hitos y las fechas de entrega intermedias se cumplen puntualmente durante el proceso de desarrollo de software.					
ADAPTABILIDAD A CAMBIOS Y MEJORAS	17	El modelo metodológico ha permitido realizar modificaciones y optimizaciones en el proceso de desarrollo de software de manera ágil, efectiva y adaptativa.					
	18	La metodología ha conllevado la incorporación de nuevas tecnologías y herramientas de seguridad de la información en el proceso de desarrollo de software, permitiendo la optimización continua en este aspecto.					

	19	el proceso de desarrollo de software ha presentado dificultades para adaptarse a los cambios y criterios requeridos en cuanto a seguridad de la información.					
	20	La propuesta ha logrado identificar y corregir de manera efectiva las debilidades en el proceso de desarrollo de software relacionadas con la seguridad de la información, generando resultados tangibles y significativos.					
DIMENSIÓN: COBERTURA DE LA DOCUMENTACIÓN							
INDICADOR	**AFIRMACIÓN**		**ALTERNATIVAS DE RESPUESTA**				
			1	**2**	**3**	**4**	**5**
COHERENCIA Y ESTRUCTURA DE LA DOCUMENTACIÓN	La documentación del modelo metodológico tiene una estructura clara y organizada, con secciones bien definidas y un orden lógico de contenido.						
	Las secciones de la documentación están claramente definidas y abordan aspectos específicos del modelo metodológico de desarrollo de software.						

	La documentación proporciona instrucciones secuenciales y coherentes para aplicar el modelo metodológico.					

	La documentación presenta de manera clara los conceptos clave relacionados con el modelo metodológico.					
	La estructura y coherencia literaria de la metodología facilitan su implementación.					

VARIABLE: Empresas de TI							
DIMENSIÓN: Calidad de los servicios de TI							
INDICADOR	**AFIRMACIÓN**		**ALTERNATIVAS DE RESPUESTA**				
			1	**2**	**3**	**4**	**5**
Nivel de satisfacción	1	El modelo metodológico basado en normas de calidad ha mejorado la satisfacción de los usuarios en relación con la calidad del software desarrollado por la empresa					
	2	El modelo presenta claridad y coherencia al momento del desarrollo de software					
	3	La metodología facilita la implementación efectiva de prácticas de seguridad en el desarrollo de software.					
	4	Se adapta a las necesidades y características únicas de tu organización en el desarrollo de software.					
	5	Brinda medidas para prevenir acceso no autorizado o exposición de información en el desarrollo de software.					

de los clientes	6	Ayuda a mantener la integridad de la información en el desarrollo de software.					
	7	Fortalece la gestión de riesgos en el desarrollo de software en tu organización.					
	8	El modelo metodológico basado en ISO 27001 mejora la disponibilidad de la información en el desarrollo de software, es decir, se encuentra disponible cuando se necesita.					
	9	Evalúa y maneja los riesgos asociados con el desarrollo de software.					
	10	Garantiza el cumplimiento de los estándaresde seguridadde la información en el desarrollo de software.					

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de la variable modelo metodológico". 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. Agradecemos su valiosa colaboración.

Anexo 3. Matriz Evaluación por juicio de expertos

Variable Independiente

1. Datos generales del juez

Nombre del juez:	CASTILLO JIMENEZ IVAN MICHELL
Grado profesional:	Maestría ( ) Doctor (x)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	
Institución donde labora:	UCV
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala

Nombre de la Prueba:	Cuestionario
Autores:	Arca Prieto José Daniel Castro Palacios Joustin Arsenio Santiago
Procedencia:	Piura
Administración:	Individual
Tiempo de aplicación:	30 min
Ámbito de aplicación:	Empresarial

ASPECTOS DE VALIDACIÓN.

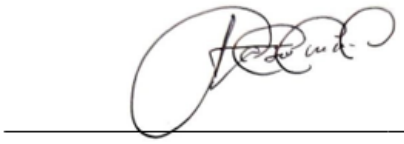
		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				**75**	
OBJETIVIDAD	Esta expresado en conducta observable.				**80**	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				**77**	
ORGANIZACIÓN	Existe una organización lógica.				**73**	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					**85**
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					**82**
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				**77**	
COHERENCIA	En los datos respecto al indicador.					**85**
METODOLOGÍA	Responde al propósito de investigación.				**77**	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				**80**	
TOTAL						

PROMEDIO DE VALIDACIÓN.

79.1

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

( ) El instrumento debe ser mejorado antes de ser aplicado.



Firma del experto informante

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento “Cuestionario de la variable modelo metodológico”. 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. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	JUAREZ NOLE HARRY SMITH
Grado profesional:	ING (X) Doctor ( ) Maestría ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (X)
Áreas de experiencia profesional:	
Institución donde labora:	MUNICIPALI DAD PROVINCIAL DE SULLANA
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala

Nombre de la Prueba:	Cuestionario
Autores:	Arca Prieto José Daniel Castro Palacios Joustin Arsenio Santiago
Procedencia:	Piura
Administración:	Individual
Tiempo de aplicación:	30 min
Ámbito de aplicación:	Empresarial

ASPECTOS DE VALIDACIÓN.

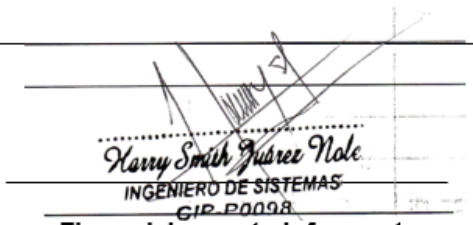
		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				**80**	
OBJETIVIDAD	Esta expresado en conducta observable.				**77**	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnolo					**92**
ORGANIZACIÓN	Existe una organización lógica.					**88**
SUFICIENCIA	Comprende los aspectos de cantidad y cali				**75**	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sist metodológico y científico.				**78**	
CONSISTENCIA	Está basado en aspectos teóricos y científi					**85**
COHERENCIA	En los datos respecto al indicador.				**79**	
METODOLOGÍA	Responde al propósito de investigación.					**84**
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					**85**
TOTAL						

I. PROMEDIO DE VALIDACIÓN.

82.3

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

( ) El instrumento debe ser mejorado antes de ser aplicado.



Firma del experto informante

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento “Cuestionario de la variable modelo metodológico”. 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. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	UBILLUS FARFAN SEGUNDO WILLIAMS
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (X)
Áreas de experiencia profesional:	
Institución donde labora:	MUNICIPALIDAD PROVINCIAL DE SULLANA
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala

Nombre de la Prueba:	Cuestionario
Autores:	Arca Prieto José Daniel Castro Palacios Joustin Arsenio Santiago
Procedencia:	Piura
Administración:	Individual
Tiempo de aplicación:	30 min
Ámbito de aplicación:	Empresarial

ASPECTOS DE VALIDACIÓN.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				**80**	
OBJETIVIDAD	Esta expresado en conducta observable.				**75**	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnolc					**90**
ORGANIZACIÓN	Existe una organización lógica.					**85**
SUFICIENCIA	Comprende los aspectos de cantidad y cali				**72**	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sist metodológico y científico.				**75**	
CONSISTENCIA	Está basado en aspectos teóricos y científic					**83**
COHERENCIA	En los datos respecto al indicador.				**80**	
METODOLOGÍA	Responde al propósito de investigación.					**88**
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					**85**
TOTAL						

I. PROMEDIO DE VALIDACIÓN.

81.3

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

( ) El instrumento debe ser mejorado antes de ser aplicado.

Firma del experto informante

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento “Cuestionario de la variable Empresas de TI”. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de este sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

Variable dependiente

1. Datos generales del juez

Nombre del juez:	**CASTILLO JIMENEZ IVAN MICHELL**
Grado profesional:	Maestría ( ) Doctor (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	
Institución donde labora:	UCV
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala

Nombre de la Prueba:	Cuestionario
Autores:	Arca Prieto José Daniel Castro Palacios Joustin Arsenio Santiago
Procedencia:	Piura
Administración:	Individual
Tiempo de aplicación:	30 min
Ámbito de aplicación:	Empresarial

ASPECTOS DE VALIDACIÓN.

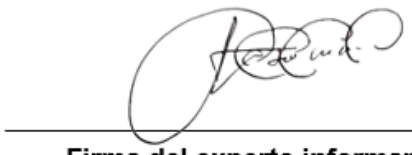
		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				**80**	
OBJETIVIDAD	Esta expresado en conducta observable.					**82**
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnolc				**80**	
ORGANIZACIÓN	Existe una organización lógica.					**85**
SUFICIENCIA	Comprende los aspectos de cantidad y calic				**75**	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sist metodológico y científico.					**81**
CONSISTENCIA	Está basado en aspectos teóricos y científic				**72**	
COHERENCIA	En los datos respecto al indicador.				**77**	
METODOLOGÍA	Responde al propósito de investigación.					**90**
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				**80**	
TOTAL						

I. PROMEDIO DE VALIDACIÓN.

72.2

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

( ) El instrumento debe ser mejorado antes de ser aplicado.



Firma del experto informante

de TI". 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. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	JUAREZ NOLE HARRY SMITH
Grado profesional:	ING (X) Doctor ( ) Maestría ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (X)
Áreas de experiencia profesional:	
Institución donde labora:	MUNICIPALI DAD PROVINCIAL DE SULLANA
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala

Nombre de la Prueba:	Cuestionario
Autores:	Arca Prieto José Daniel Castro Palacios Joustin Arsenio Santiago
Procedencia:	Piura
Administración:	Individual
Tiempo de aplicación:	30 min
Ámbito de aplicación:	Empresarial

ASPECTOS DE VALIDACIÓN.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				**80**	
OBJETIVIDAD	Esta expresado en conducta observable.				**77**	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnolc					**92**
ORGANIZACIÓN	Existe una organización lógica.					**88**
SUFICIENCIA	Comprende los aspectos de cantidad y cali				**75**	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sist metodológico y científico.				**78**	
CONSISTENCIA	Está basado en aspectos teóricos y científi					**85**
COHERENCIA	En los datos respecto al indicador.				**79**	
METODOLOGÍA	Responde al propósito de investigación.					**84**
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					**85**
TOTAL						

I. PROMEDIO DE VALIDACIÓN.

82.3

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

( ) El instrumento debe ser mejorado antes de ser aplicado.

Firma del experto informante

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento “Cuestionario de la variable Empresas de TI”. 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. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	UBILLUS FARFAN SEGUNDO WILLIAMS	
Grado profesional:	Maestría (x)	Doctor ( )
Área de formación académica:	Clínica ( ) Educativa ( )	Social ( ) Organizacional (X)
Áreas de experiencia profesional:		
Institución donde labora:	MUNICIPALIDAD PROVINCIAL DE SULLANA	
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)	
Experiencia en Investigación Psicométrica: (si corresponde)		

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala

Nombre de la Prueba:	Cuestionario
Autores:	Arca Prieto José Daniel Castro Palacios Joustin Arsenio Santiago
Procedencia:	Piura
Administración:	Individual
Tiempo de aplicación:	30 min
Ámbito de aplicación:	Empresarial

ASPECTOS DE VALIDACIÓN.

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.					**82**
OBJETIVIDAD	Esta expresado en conducta observable.				**75**	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnolo					**95**
ORGANIZACIÓN	Existe una organización lógica.					**85**
SUFICIENCIA	Comprende los aspectos de cantidad y cali				**77**	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sist metodológico y científico.				**79**	
CONSISTENCIA	Está basado en aspectos teóricos y científi					**88**
COHERENCIA	En los datos respecto al indicador.				**80**	
METODOLOGÍA	Responde al propósito de investigación.					**85**
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					**85**
TOTAL						

I. PROMEDIO DE VALIDACIÓN.

83.1

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

( ) El instrumento debe ser mejorado antes de ser aplicado.

CELLUS FARFAN SEGUNDO WILLIAMS
ING. EN INFORMATICA Y DE SISTEMAS
Reg. Colegio de Ingenieros CIP N° 167285

Firma del experto informante

Anexo 4. Carta de solicitud

MUNICIPALIDAD PROVINCIAL DE SULLANA

TICKET EXPEDIENTE N°: 032876 29/09/2023 11:08:21

PROCEDIMIENTO: AUTORIZACIÓN PARA INVESTIGACIÓN Y SE LES BRINDE FACILIDADES

REMITENTE: CASTRO PALACIOS JOUSTIN ARSENIO

DESTINO: OFICINA DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

RECEPCIONADO

RECEPCION: 29/09/2023 11.04

PLAZO DE RESPUESTA: 30 Dias

FOLIOS : 01

DNI / RUC 72912904

REFERENCIA CARTA

N°

AUTOMATICO: SI

USUARIO: LNAHUCHE

POR:.....

HORA:.....FIRMA:.....

Verificar el estado de su tramite en http://www.munisullana.gob.pe

La recepción de documentos no significa su aceptación y está sujeto a posterior revisión.

CIUDAD. -

ATT.: Oficina de Tecnología de la Información y Comunicaciones

***Jose Daniel Arca Prieta**, con D.N.I Nº 71459493 y **Joustin Arsenio Santiago Castro Palacios**, con D.N.I Nº 72912904, **Estudiantes de la Escuela Profesional de Ingeniería de Sistemas de la Facultad de Ingeniería y Arquitectura de la Universidad Cesar Vallejo-Piura**, ante usted con el debido respeto que se merece me presento y digo:*

Que, para lograr obtener nuestro título profesional en la carrera antes mencionada, requerimos desarrollar una investigación académica, la cual hemos creído conveniente realizarla en la Municipalidad Provincial de Sullana que Ud., dignamente dirige.

*Que, la Investigación que desarrollaremos lleva por título: "**Modelo metodológico basado en la norma ISO 27001 para el desarrollo de software en empresas de TI**" la cual será una investigación con enfoque cuantitativo de tipo aplicada con un diseño pre experimental, evaluando un único grupo, la cual se desarrollara en los meses de setiembre a diciembre del 2023, La cual cuenta con la Asesoría Académica del **Ingº Mg, Peña Cáceres Oscar Jhan Marcos** y tendrá como objetivo general : Diseñar una metodología basado en la norma ISO 27001 para impulsar la calidad en el desarrollo de sistema tecnológicas en empresa de TI.*

Por lo expuesto:

Solicitamos a usted le brinde la atención que merece la presente a fin de que nos otorgue la autorización correspondiente y se nos pueda brindar las facilidades para poder llevar a cabo dicha investigación académica.

Sullana, 29 de setiembre del 2023

JOSE DANIEL ARCA PRIETO
DNI Nº 71459492

JOUSTIN A. CASTRO PALACIOS
DNI Nº 72912904

Anexo 5. Carta de aceptación

MUNICIPALIDAD PROVINCIAL DE
SULLANA
Oficina de Tecnologías de la Información y Comunicaciones

Sullana, 02 de octubre del 2023

OFICIO N° 005-2023/MPS-OGAyF-OTIyC

Señor:
JOUSTIN ARSENIO SANTIAGO CASTRO PALACIOS
Estudiante de la Escuela Profesional de Ingeniería de Sistemas
De la Facultad de Ingeniería y Arquitectura de la
Universidad Cesar Vallejo
CIUDAD. -

ASUNTO : Dar respuesta a su Exp.032876 del 29.09.2023

El presente es para hacerle llegar el saludo institucional y el mío en particular.

En atención a su documento indicado en el asunto, mediante el cual solicita se le otorgue a usted y al Sr. José Daniel Arca Prieto, Estudiantes de la Escuela Profesional de Ingeniería de Sistemas de la Facultad de Ingeniería y Arquitectura de la Universidad Cesar Vallejo, la autorización para llevar a cabo una investigación académica la cual lleva por título "Modelo metodológico basado en la norma ISO 27001 para el desarrollo de software en empresas de TI", el mismo que cuenta con la Asesoría Académica del Ingª Mag. Peña Cáceres Oscar Jhan Marcos y tendrá como objetivo general: Diseñar una metodología basada en la norma ISO 27001 para impulsar la calidad en el desarrollo de sistema tecnológico en empresa TI.

Al respecto le comunico a usted que este despacho ha creído por conveniente aceptar su solicitud, para que lleven a cabo dicho Trabajo de Investigación Académica, debiendo respetar las normas, así como los horarios establecidos.

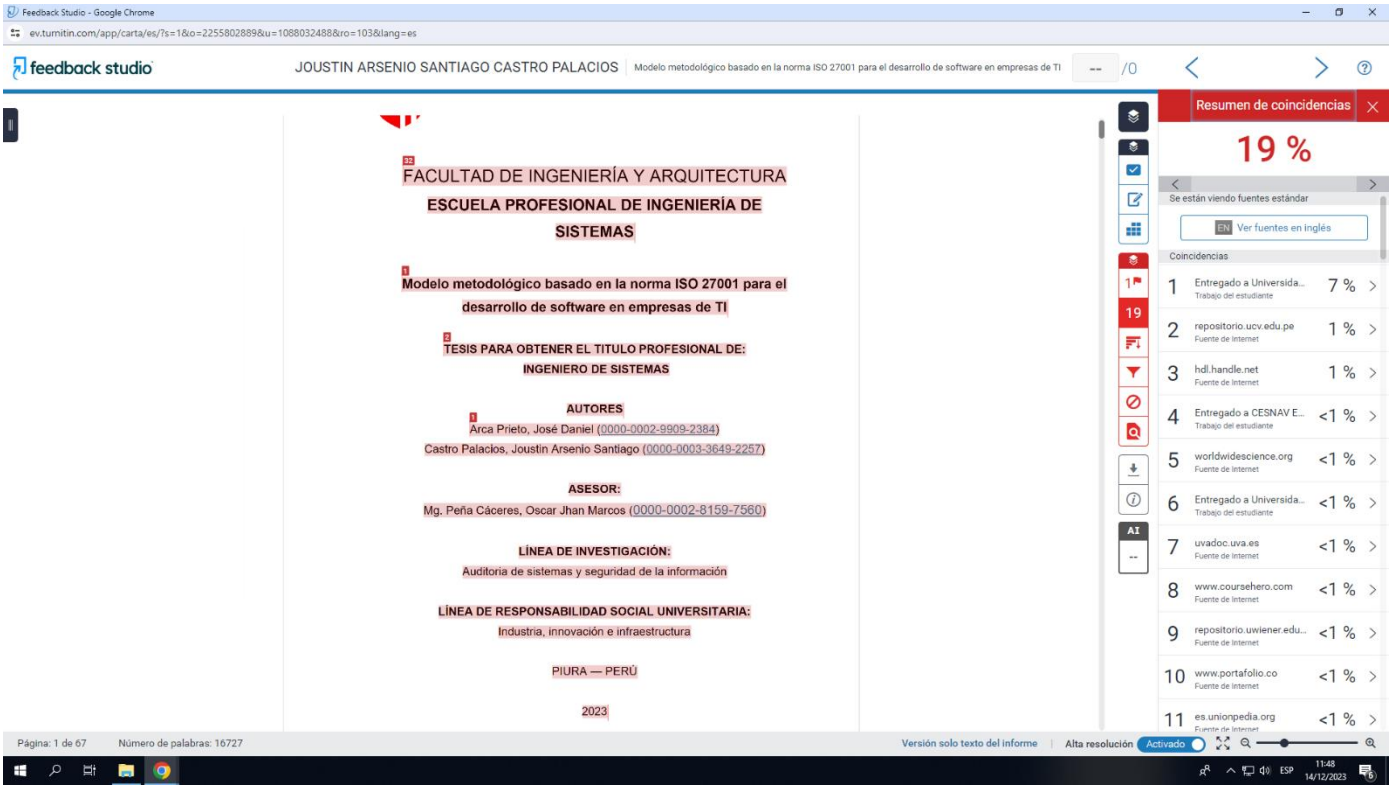
Sin otro particular, aprovecho la oportunidad para testimoniarle las muestras de mi especial consideración y estima.

Atentamente,

MUNICIPALIDAD PROVINCIAL DE SULLANA
ING° LUIS LEON LOAYZA
JEFE DE OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES
CIP: 120180

c.c
Archivo
extra
LLL/MO.V.

Anexo 6. Resultado de similitud del programa Turnitin.



Anexo 7. Valoración de los criterios de cada metodología

Metodología	Cobertura de la metodología	Enfoque de gestión de riesgos	Facilidad de implementación	Adaptabilidad	Evaluación y mejora continua
DMAIC	4	4	5	2	4
ITIL	3	4	3	3	5
PDCA	4	4	4	3	3
COSO	3	3	3	4	4
COBIT 5	4	5	3	3	2
CRAMM	3	3	4	3	3
MAGERIT	4	3	3	2	3
ISSAF	3	4	3	3	2

Anexo 8. Evaluación de los aspectos más resaltantes de cada metodología

Metodologías	Fortalezas	Debilidades	Eficacia	Flexibilidad	Adaptabilidad
DMAIC	Proporciona un enfoque estructurado para la mejora de procesos.(«Vista de Metodología DMAIC de Lean Seis Sigma: Una revisión en el contexto del ruido industrial - sector metalmecánico» 2022)	Puede ser demasiado rígida en entornos altamente dinámicos.(«Vista de Metodología DMAIC de Lean Seis Sigma: Una revisión en el contexto del ruido industrial - sector metalmecánico 2022)	Alta	Media	Baja
ITIL	Estándar reconocido internacionalmente para la gestión de servicios de TI. (Ángel y Villamizar 2017)	Requiere una curva de aprendizaje significativa para implementarla correctamente.(Ángel y Villamizar 2017)	Media	Media	Media
PDCA	Enfoque cíclico que promueve la mejora continua.(Becerra, Adrián y Orbe])	Requiere disciplina y compromiso para seguir el ciclo completo.(Becerra, Adrián y Orbe)	Alta	Alta	Media
COSO	Proporciona un marco integral para la gestión de	Requiere una comprensión profunda de los procesos y	Media	Media	Alta

	riesgos y control interno. (Santa Cruz Marín 2014)	riesgos de la organización. (Santa Cruz Marín 2014)			
COBIT 5	Enfoque integrado para la gestión y gobierno de TI. (De La Cruz Vélez De Villa y De La Cruz 2017)	Requiere un nivel de madurez organizacional para implementarla eficazmente. (De La Cruz Vélez De Villa y De La Cruz 2017)	Alta	Baja	Media

Anexo 9. Modelo metodológico MSI-D

METODOLOGÍA MSI-D

CONTENIDO

GLOSARIO DE TÉRMINOS

ISO 27001:

(GlobalSuite Solutions, 2023) La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma proporciona un marco para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva.

Seguridad de la información:

(Grupo ESGinnova, 2023) La seguridad de la información es el conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que se manejan dentro de la organización y asegurar que los datos no salgan del sistema que ha establecido la organización. Es una pieza clave para que las empresas puedan llevar a cabo sus operaciones, ya que los datos que maneja son esenciales para la actividad que desarrollan.

Requisitos de Seguridad:

(Grupo ESGinnova, 2015) Los requisitos de seguridad que se encuentran relacionados con el acceso a los activos de información de la organización por parte de los clientes pueden variar de forma considerable dependiendo del tipo de instalación que procese la información y el tipo de información a la que se pretende acceder. Los requisitos en seguridad se pueden encontrar anexados al acuerdo al que se ha llegado con el cliente, y éste contiene todos los riesgos perfectamente identificados y los requisitos de seguridad.

Evaluación de Riesgos:

(safetyculture, 2023) Una evaluación de riesgos es un proceso sistemático que implica identificar, analizar y controlar los peligros y riesgos en el lugar de trabajo para garantizar la salud y la seguridad de los trabajadores. Lo lleva a cabo una persona competente para determinar qué medidas están, o deberían estar, implementadas para eliminar o controlar el riesgo en el lugar de trabajo en cualquier situación potencial.

Plan de seguridad de la información:

(Grupo ESGinnova, 2015) El Plan de Seguridad se trata de realizar los objetivos estratégicos que se identificaron en la política de seguridad y en las normativas vigentes de seguridad en la organización, con el fin de situar a la entidad a nivel mundial en ambiente de riesgo tolerable.

Alcance del proyecto:

(RIVEROS, 2020) El alcance de un proyecto incluye todo el trabajo necesario para realizar el proyecto y todo lo que se requiere para que ese trabajo se completado satisfactoriamente. En definitiva, el alcance define qué se incluye y qué no se incluye en el proyecto. Por lo tanto, la correcta gestión del alcance del proyecto conduce al cumplimiento de las expectativas y al éxito del mismo.

Seguimiento y Mejora Continua:

(Páez Acosta, 2022) La gestión de procesos y mejora continua son todas las acciones realizadas para identificar, analizar, evaluar y tomar decisiones en las operaciones que realizan con miras a optimizar el desempeño y aumentar la competitividad de la empresa.

Pruebas de seguridad de aplicaciones

(Distillery, 2023) Las pruebas de seguridad de aplicaciones (AST) son un proceso de identificación, análisis y corrección de las vulnerabilidades de seguridad de una aplicación web. Incluye probar la aplicación para detectar vulnerabilidades conocidas y examinar el código para detectar posibles problemas de seguridad. El proceso consiste en probar el código de la aplicación y su entorno para detectar fallos de seguridad y posibles vulnerabilidades. Una vez identificados, los problemas se abordan y solucionan.

INTRODUCCION

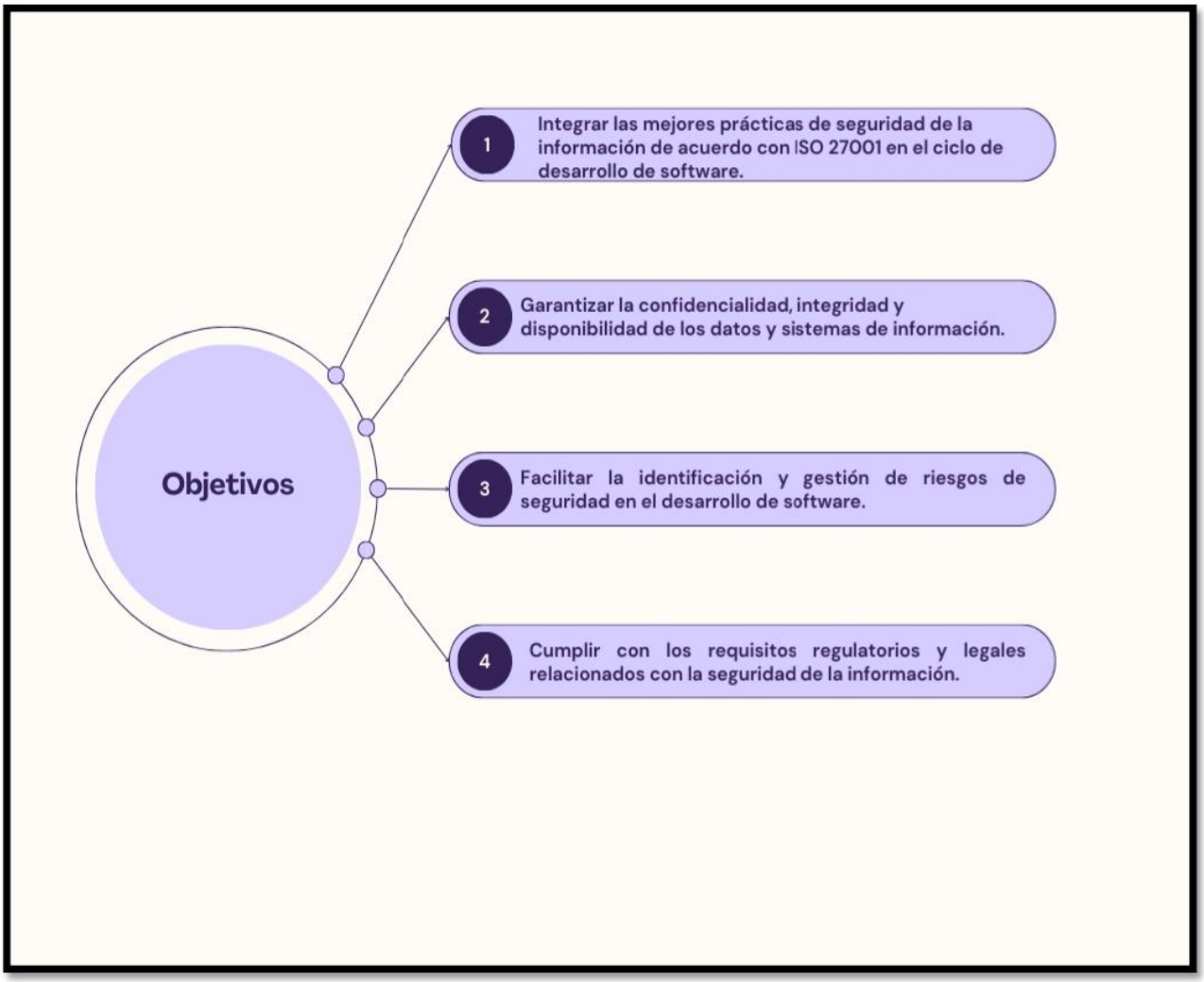
En un mundo cada vez más digitalizado, la seguridad de la información se ha convertido en una preocupación primordial para las organizaciones de tecnología de la información (TI). La necesidad de desarrollar software robusto y seguro es esencial para proteger datos confidenciales, garantizar la integridad de los sistemas y cumplir con las regulaciones de seguridad.

En esta metodología, se establecen fases y actividades específicas que abarcan desde la planificación inicial hasta la implementación y el monitoreo continuo. El objetivo principal es garantizar que el software desarrollado cumpla con los más altos estándares de seguridad, protegiendo la confidencialidad, integridad y disponibilidad de la información.

A lo largo de esta guía, exploraremos en detalle cada una de las fases, roles y responsabilidades, y los entregables claves de la metodología. Además, destacaremos la importancia de la colaboración entre equipos de desarrollo, seguridad de la información y gestión de proyectos para lograr un enfoque integral y efectivo en la seguridad del software.

1. OBJETIVOS DE LA METODOLOGÍA:

Figura 1. Objetivos de la metodología



2. FASES DE LA METODOLOGÍA:

2.1. Inicio:

- Definición del alcance del proyecto de desarrollo de software.
  La definición del alcance en un proyecto es esencial, especialmente en el contexto de la seguridad de la información. Esto implica identificar con precisión qué partes del sistema y qué activos de información están incluidos en el proyecto, lo que a su vez permite enfocar los esfuerzos de seguridad en las áreas críticas. Para lograrlo, es fundamental trabajar estrechamente con los interesados clave y llevar a cabo reuniones de inicio del proyecto para aclarar expectativas y limitaciones. Documentar de manera clara y accesible el alcance en un documento es crucial para garantizar que todos los miembros del equipo estén alineados y comprometidos en alcanzar los objetivos del proyecto de seguridad de la información.

- Identificación de las partes interesadas y sus requerimientos de seguridad.
  Identificar a todas las partes interesadas, tanto internas como externas, y comprender sus necesidades y preocupaciones en cuanto a seguridad es crucial. Esto permite adaptar las medidas de seguridad para satisfacer sus expectativas y garantizar que se aborden sus preocupaciones. Para lograrlo, se recomienda realizar entrevistas o encuestas con las partes interesadas, incluyendo tanto a las partes internas como a las externas. Esta información recopilada debe ser utilizada para crear un registro de interesados que esté siempre actualizado y que sirva como referencia clave para las decisiones relacionadas con la seguridad, garantizando así una gestión más efectiva de los riesgos y la protección de la información.
  Puntos clave en esta etapa:
  1-Definir el título del Proyecto.
  2-Descripción del Proyecto.
  3-Definir las partes Involucradas. (internas y externas)

Parte involucrado	*Función*
[Nombre]	[Función]

4-Definir el alcance del Proyecto (¿Qué está incluido y qué no está incluido?).

6-Requerimientos de seguridad de cada parte interesada.

Parte involucrado interna	*Requerimientos de Seguridad*
[Nombre de la Parte Interesada]	[Descripción de los Requerimientos de Seguridad]

Parte involucrado externa	*Requerimientos de Seguridad*
[Nombre de la Parte Interesada]	[Descripción de los Requerimientos de Seguridad]

2.2. Planificación:

- Identificación y evaluación de los riesgos de seguridad asociados al proyecto.

  La identificación y evaluación de riesgos desempeñan un papel fundamental en el marco de la ISO 27001, especialmente en proyectos de desarrollo de software. Al comprender los riesgos específicos que enfrenta el proyecto, es posible tomar decisiones informadas sobre las medidas de seguridad que deben implementarse. Esta comprensión facilita la priorización de recursos y la reducción de los riesgos a niveles aceptables. Para llevar a cabo esta tarea de manera efectiva, se recomienda utilizar técnicas de evaluación de riesgos, como el análisis de amenazas y vulnerabilidades, para identificar posibles problemas de seguridad. Asignar valores a los riesgos para determinar su impacto y probabilidad es esencial para establecer prioridades y determinar cuáles riesgos deben abordarse en primer lugar, garantizando así un enfoque más eficiente en la gestión de la seguridad del proyecto de desarrollo de software.

- Definición de controles de seguridad basados en ISO 27001 relevantes para el proyecto.

  La ISO 27001 proporciona un conjunto completo de controles de seguridad. Al seleccionar los controles pertinentes para el proyecto, puedes garantizar que las mejores prácticas de seguridad se apliquen de manera efectiva. Esto también simplifica la evaluación de la conformidad con la norma y facilita la comunicación con auditores y partes interesadas.

  Puntos clave de esta etapa:

  1- Definir lista de riesgos asociados al proyecto

Riesgo	*Impacto*	*Probabilidad*	*Medidas de Mitigación*
[Tipo de Riesgo]	[Alto/Medio/Bajo]	[Alta/Media/Baja]	[Descripción de Medidas]

  2- Definir los objetivos de seguridad relacionados con la norma ISO 27001

3- Desarrollo del plan de seguridad

Objetivo	*Responsable*	*Fecha de Implementación*
[Objetivo]	[Nombre]	[Fecha]

4- Requerimientos del sistema

N°	*Requerimiento*
[N°]	[Requerimiento]

2.3. Diseño:

2.3.1. Diseño de la base de datos

En la fase de diseño, se aborda la estructura y organización de la base de datos, un componente crítico en proyectos de desarrollo de software. El diseño de la base de datos debe satisfacer los requisitos del sistema, garantizar la integridad de los datos y facilitar un rendimiento eficiente. A continuación, se describen los pasos clave en el diseño de la base de datos:

Identificación de Requisitos de Datos:

Definir los tipos de datos necesarios para almacenar la información del sistema.

Identificar las relaciones entre diferentes conjuntos de datos.

Modelado de Datos:

Utilizar técnicas de modelado como el Modelo Entidad-Relación (ER) para representar visualmente las entidades y sus relaciones.

Crear diagramas que muestren las tablas de la base de datos, campos y claves primarias/foráneas.

Revisión Continua con Partes Interesadas:

Cómo hacerlo: Realiza reuniones regulares con todas las partes interesadas, incluyendo expertos en seguridad, para revisar y discutir los requerimientos. Solicita su retroalimentación específicamente en relación con los controles y directrices de la ISO 27001.

Documentación Detallada y Específica:

Cómo hacerlo: Al definir un requerimiento, asegúrate de ser lo más detallado y específico posible. Si un requerimiento está relacionado con la seguridad, referencia los controles o secciones específicas de la ISO 27001 que son relevantes. Además, considera utilizar herramientas o plataformas de gestión de requerimientos que permitan una fácil referencia y seguimiento de cada requerimiento a lo largo del ciclo de vida del proyecto.

2.3.2. Definición de requisitos de seguridad para el diseño del software

En esta etapa, es fundamental identificar los requisitos específicos de seguridad que deben incorporarse en el diseño del software. Esto implica determinar las

necesidades de confidencialidad, integridad, disponibilidad y otros aspectos de la seguridad de la información. Al definir estos requisitos desde el principio, se asegura que el diseño del software aborde adecuadamente las preocupaciones de seguridad y que se integren controles de seguridad apropiados.

2.3.3. Diseño de arquitectura segura

El diseño de una arquitectura segura implica crear una estructura de software que proteja los activos de información crítica y minimice las vulnerabilidades. Esto puede incluir la segmentación de componentes para limitar el acceso no autorizado, la implementación de cortafuegos, la separación de roles y privilegios, y la consideración de la resistencia a los ataques. El objetivo es establecer una base sólida que resista posibles amenazas.

Puntos clave

1-Diseño de la base de datos E-R

2-Definir requisitos de seguridad

Requisito de Seguridad	*Descripción*
[Requisito]	[Descripción]

3- Diseño de los prototipos funcionales

2.4. Desarrollo:

En esta fase, se procede con el desarrollo e implementación del software siguiendo los diseños y controles de seguridad definidos en las etapas anteriores. Es importante garantizar que se sigan las mejores prácticas de desarrollo seguro de software, como la revisión de código, la gestión de vulnerabilidades y la validación de la seguridad de terceros componentes o bibliotecas utilizados.

2.4.1. Implementación de Controles de Seguridad

Durante la implementación del software, se aplican los controles de seguridad definidos en las etapas anteriores. Estos controles pueden incluir medidas como la autenticación de usuarios, la encriptación de datos, la gestión de accesos y privilegios, y la validación de datos de entrada para prevenir vulnerabilidades comunes

2.4.2. Programación Segura:

Los desarrolladores deben seguir prácticas de programación segura, que incluyen el uso de funciones y bibliotecas de seguridad, la validación adecuada de datos, la gestión segura de sesiones y la protección contra ataques conocidos. También se debe asegurar que no haya información sensible o contraseñas en el código fuente en texto claro.

2.4.3. Gestión de Claves y Credenciales:

La gestión adecuada de claves y credenciales es esencial para garantizar la seguridad de la información. Se deben utilizar métodos seguros para almacenar y gestionar las claves de cifrado y las credenciales de acceso. Además, se debe evitar el almacenamiento de contraseñas en texto claro y en su lugar utilizar técnicas de almacenamiento seguro, como el hash y la sal.

2.4.4. Revisión de Código:

La revisión de código es un proceso continuo en el que se examina el código fuente para identificar posibles problemas de seguridad. Los desarrolladores y expertos en seguridad revisan el código para buscar vulnerabilidades, errores de programación y malas prácticas de seguridad. Las revisiones de código ayudan a identificar y corregir problemas antes de que lleguen a producción.

2.4.5. Control de Versiones:

Es importante utilizar sistemas de control de versiones para rastrear los cambios en el código fuente y mantener un historial de versiones. Esto facilita la colaboración entre desarrolladores y permite revertir cambios si se descubre un problema de seguridad en una versión posterior.

Puntos clave

1-Implementación de Controles de Seguridad

2-Programación

3-Revisión del código

4-Correccion de errores de código

2.5. Pruebas y Validación:

En esta etapa crítica del ciclo de desarrollo de software, se llevan a cabo actividades de prueba y validación específicas para garantizar que el software

sea resistente a amenazas y cumpla con los estándares de seguridad establecidos. Las dos principales áreas de enfoque son:

2.5.1. Ejecución de pruebas de seguridad:

Se realizan pruebas exhaustivas destinadas a identificar y evaluar posibles vulnerabilidades y debilidades en el software.

Validación de que los controles de seguridad funcionan según lo previsto: Además de las pruebas de seguridad, es fundamental verificar que los controles de seguridad implementados funcionen correctamente y proporcionen la protección esperada.

Punto claves

1- Ejecución de pruebas de aceptación

PRUEBA DE ACEPTACION						
FECHA DE EJECUCION:			****/**/******			
MODULO DEL SISTEMA:			****MODULO DEL SISTEMA****			
Código	**Funcionalidad**	**Escenario de prueba**	**Acción del usuario**	**Resultado esperado**	**Resultado obtenido**	**Estado de la prueba**


Fases de la metodología
Inicio
Planificación
Diseño
Desarrollo
Pruebas y Validación

3. DOCUMENTACIÓN Y ENTREGABLES:

3.1. Documentación de la seguridad:

Durante el desarrollo de software y el proceso de aseguramiento de la seguridad de la información, es esencial generar documentación que registre los aspectos clave relacionados con la seguridad. Esto incluye:

Configuración de seguridad: Detalles sobre cómo se ha configurado el software para garantizar la seguridad. Esto puede abarcar aspectos como la configuración de cortafuegos, configuración de autenticación, permisos de acceso, entre otros.

Controles de seguridad implementados: Una lista de los controles de seguridad específicos que se han implementado en el software. Esto puede incluir medidas técnicas, procesos operativos y políticas de seguridad.

Políticas de seguridad: Documentación de las políticas y procedimientos de seguridad que se aplican al software. Esto puede incluir políticas de gestión de contraseñas, políticas de acceso, políticas de cifrado, etc.

Procedimientos de seguridad: Descripción detallada de los procedimientos que deben seguirse en caso de incidentes de seguridad o situaciones de emergencia.

Diagramas de arquitectura de seguridad: Gráficos que ilustran la estructura de seguridad del software, incluyendo cómo se aplican los controles de seguridad en el diseño.

3.2. Entregables:

En esta fase, se determina qué documentación y registros de auditoría deben entregarse a las partes interesadas pertinentes. Esto puede incluir:

Informe de seguridad: Un resumen que describe la postura de seguridad del software, incluyendo los controles implementados y cualquier hallazgo importante de pruebas de seguridad.

Documentación técnica: Detalles técnicos sobre la implementación de los controles de seguridad y la arquitectura de seguridad del software. Esto puede ser útil para el personal de TI y desarrollo.

Políticas y procedimientos de seguridad: Para garantizar que todos los usuarios y administradores sigan las prácticas recomendadas de seguridad.

Registros de auditoría: Estos registros pueden ser requeridos por reguladores o auditores externos para demostrar el cumplimiento de las políticas de seguridad y las regulaciones aplicables.

La documentación y los entregables son esenciales para la transparencia, la revisión y la auditoría de la seguridad del software. Además, sirven como referencia para futuros desarrollos y actualizaciones del software, asegurando que la seguridad de la información siga siendo una prioridad.

3.3. Seguimiento y Mejora Continua:

3.3.1. Monitorización y respuesta: Monitorizar activamente el software en busca de signos de actividad maliciosa y tener un plan de respuesta a incidentes en caso de brechas de seguridad.

3.3.2. Revisiones periódicas: Realizar revisiones regulares del software y su entorno para identificar y abordar nuevas amenazas y vulnerabilidades.

4. ROLES Y RESPONSABILIDADES:

4.1. Oficial de Seguridad de la Información: Responsable de supervisar la estrategia general de seguridad y asegurarse de que se siguen las directrices de ISO 27001.

4.2. Desarrolladores: Responsables de escribir código seguro, revisar el código de otros y corregir cualquier problema de seguridad identificado.

4.3. Auditores: Responsables de revisar y validar que todos los controles de seguridad estén en su lugar y funcionen correctamente.

4.4. Equipo de respuesta a incidentes: Actúan rápidamente en caso de una brecha o incidente de seguridad para contener y remediar el problema.

REFERENCIAS

Distillery. 2023. Distillery. *Distillery.* [En línea] 30 de Enero de 2023. https://distillery.com/es/blog/que-son-las-pruebas-de-seguridad-de-las-aplicaciones-y-como-funcionan/.

GlobalSuite Solutions. 2023. GlobalSuite Solutions. *GlobalSuite Solutions.* [En línea] 22 de Setiembre de 2023. https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/.

Grupo ESGinnova. 2023. Grupo ESGinnova. *Grupo ESGinnova.* [En línea] 11 de Marzo de 2023. https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/.

—. 2015. Grupo ESGinnova. *Grupo ESGinnova.* [En línea] 29 de Abril de 2015. https://www.pmg-ssi.com/2015/04/iso-27001-requisitos-seguridad-tener-cuenta-clientes/.

—. 2015. isotools. *isotools.* [En línea] 2015. https://pe.isotools.us/iso-27001-plan-de-seguridad-informacion/.

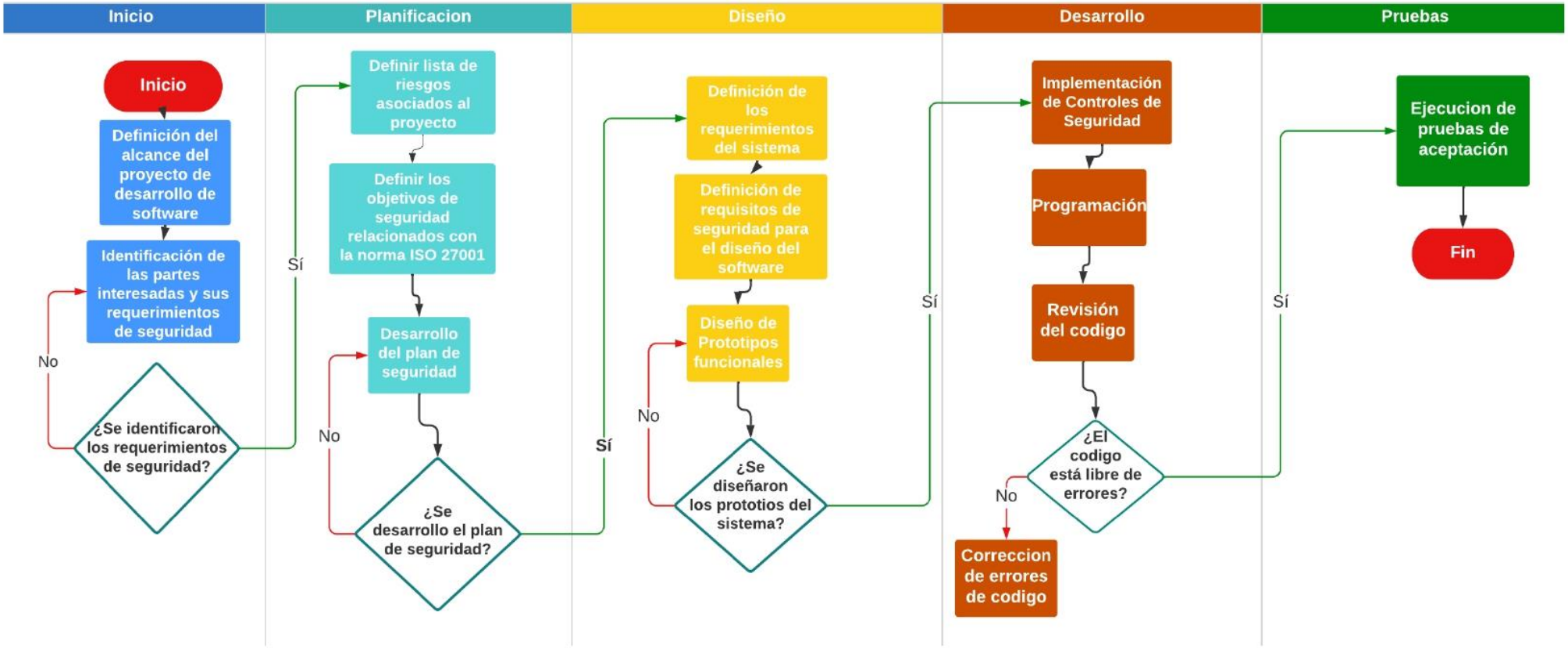
Páez Acosta, Nancy. 2022. lemontech. *lemontech.* [En línea] 18 de Julio de 2022. https://blog.lemontech.com/gestion-de-procesos-mejora-continua/#:~:text=La%20gesti%C3%B3n%20de%20procesos%20y%20mejora%20continua%20son%20todas%20las,la%20competitividad%20de%20la%20empresa..

RIVEROS, ALEJANDRO. 2020. Ealde. *Ealde.* [En línea] 17 de Noviembre de 2020. https://www.ealde.es/alcance-proyecto-gestion/.

safetyculture. 2023. safetyculture. *safetyculture.* [En línea] 25 de Julio de 2023. https://safetyculture.com/es/temas/evaluacion-de-riesgos/.

ANEXOS

Anexo 1. Diagrama de flujo



Anexo 2. Caso practico

1. INICIO

1.1 DESCRIPCIÓN DEL PROYECTO

1.1.1. TITULO DEL PROYECTO

SISTEMA WEB PARA EL CONTROL DE SUMINISTROS Y HERRAMIENTAS EN EL ÁREA DE SOPORTE TÉCNICO E INFORMÁTICO DE LA MUNICIPALIDAD PROVINCIAL DE SULLANA.

1.1.2 ANÁLISIS DEL PROBLEMA

La Municipalidad Provincial de Sullana, como muchas otras instituciones gubernamentales, depende en gran medida de la tecnología para llevar a cabo sus operaciones diarias. El área de soporte técnico e informático juega un papel crucial en garantizar que todos los sistemas y equipos funcionen correctamente. Sin embargo, con el aumento de la dependencia tecnológica, también ha aumentado la demanda de suministros y herramientas necesarias para el mantenimiento y reparación de estos sistemas.

Actualmente la gestión de estos suministros y herramientas se realiza de manera manual, lo que lleva a una falta de control preciso sobre el inventario, pérdida de tiempo en la búsqueda de herramientas o suministros específicos, dificultad para rastrear el uso y la disponibilidad de herramientas, retrasos en la atención de solicitudes de soporte debido a la falta de suministros necesarios y aumento de cotos debido a compras duplicadas o innecesarias.

1.1.3. DEFINICIÓN DE LAS PARTES INVOLUCRADAS

Parte involucrado	*Función*
Carlos Jobino Arámbulo Amaya	Jefe
Luis Felipe León Loayza	Supervisor de proyectos
Jean Gustavo Moran Navarro	Análisis y programación de sistemas
Marco Tulio Cobeñas Vega	Análisis y programación de sistemas
Ernesto Salomon Viela Zegarra	Análisis y programación de sistemas
William Matin Silva Zapata	Soporte Técnico
Carlos Enrique Yman Azcarate	Soporte Técnico
David Morante Carreño	Administrador de redes y ciberseguridad

1.1.4. ALCANCE

El proyecto se enfocó en el diseño y desarrollo de un sistema web para el control de suministros y herramientas en el área de Soporte Técnico e Informático de la Municipalidad Provincial de Sullana. Incluyó la creación de la estructura del sistema, funciones para el registro de suministros, herramientas, proveedores y empleados, así como la optimización de procesos y generación de informes detallados. El alcance abarca desde la concepción hasta la preparación para la futura integración y uso operativo.

Parte Involucrada	*Requerimientos de Seguridad*
Carlos Jobino Arámbulo Amaya	Acceso seguro al sistema mediante autenticación y autorización.
	Respaldo regular de la información para evitar pérdidas de datos.
Luis Felipe León Loayza	Acceso restringido a funciones y datos específicos según roles.
Jean Gustavo Moran Navarro	Encriptación de datos sensibles durante la transmisión y almacenamiento.
Marco Tulio Cobeñas Vega	Auditoría de actividades dentro del sistema para detectar posibles anomalías.
Ernesto Salomon Viela Zegarra	Implementación de cortafuegos y medidas de protección contra intrusiones.
William Matin Silva Zapata	Respaldo y recuperación eficientes de la información relacionada con el soporte técnico.
Carlos Enrique Yman Azcarate	Monitoreo constante de vulnerabilidades en el sistema y actualizaciones de seguridad.
David Morante Carreño	Configuración adecuada de permisos para garantizar la seguridad de la red.

2. PLANIFICACION

2.1. REQUERIMIENTOS DE SEGURIDAD

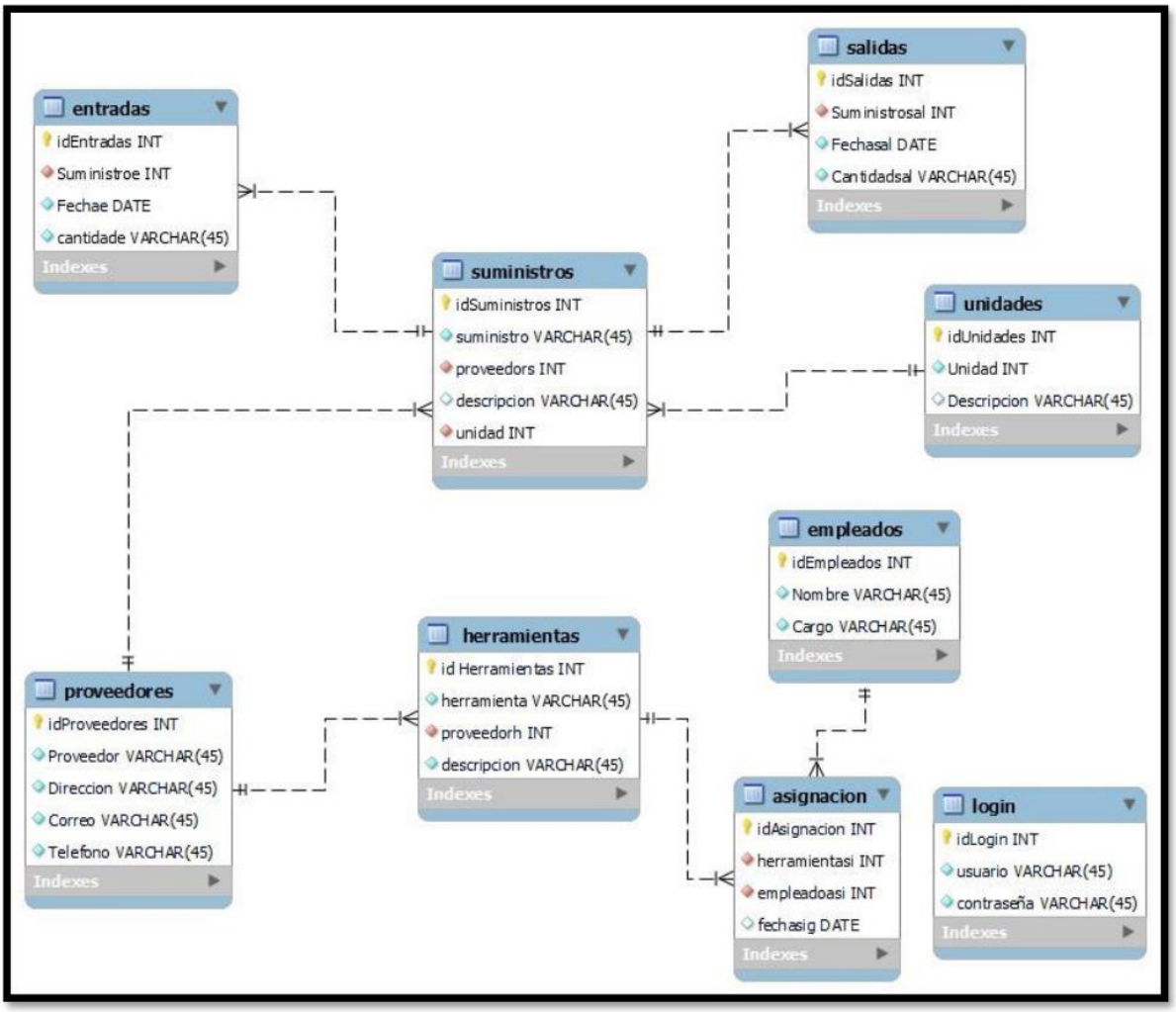
Riesgos	*Impacto*	*Probabilidad*	*Medidas de Mitigación*
Falta de Experiencia en nuevas tecnologías	Alto	Alta	Capacitación continua para el equipo de análisis y programación.
Dificultades técnicas en la implementación	Alto	Media	Realizar pruebas exhaustivas durante el desarrollo.
Cambio en los requerimientos	Medio	Media	Establecer un proceso formal para la gestión de cambios.
Retraso en la entrega de suministros	Alto	Alta	Establecer un cronograma realista y contingencias planificadas.
Problemas en la seguridad del sistema	Alto	Alta	Realizar pruebas de seguridad de forma regular.

2.2. OBJETIVOS DE SEGURIDAD

Objetivo	*Responsable*	*Fecha de Implementación*
Establecer un SGSI	Luis Felipe León Loayza - Supervisor de Proyectos	
Identificación de Activos y Evaluación de Riesgos	Jean Gustavo Moran Navarro - Análisis y Programación de Sistemas	
Control de Acceso	Marco Tulio Cobeñas Vega - Análisis y Programación de Sistemas	
Gestión de Cambios	Luis Felipe León Loayza - Supervisor de Proyectos	
Protección contra Malware y Amenazas	David Morante Carreño - Administrador de Redes y Ciberseguridad	
Concientización y Formación del Personal	Luis Felipe León Loayza - Supervisor de Proyectos	
Gestión de Incidentes de Seguridad	David Morante Carreño - Administrador de Redes y Ciberseguridad	
Monitoreo y Auditoría	Carlos Enrique Yman Azcarate - Soporte Técnico	

3. DISEÑO

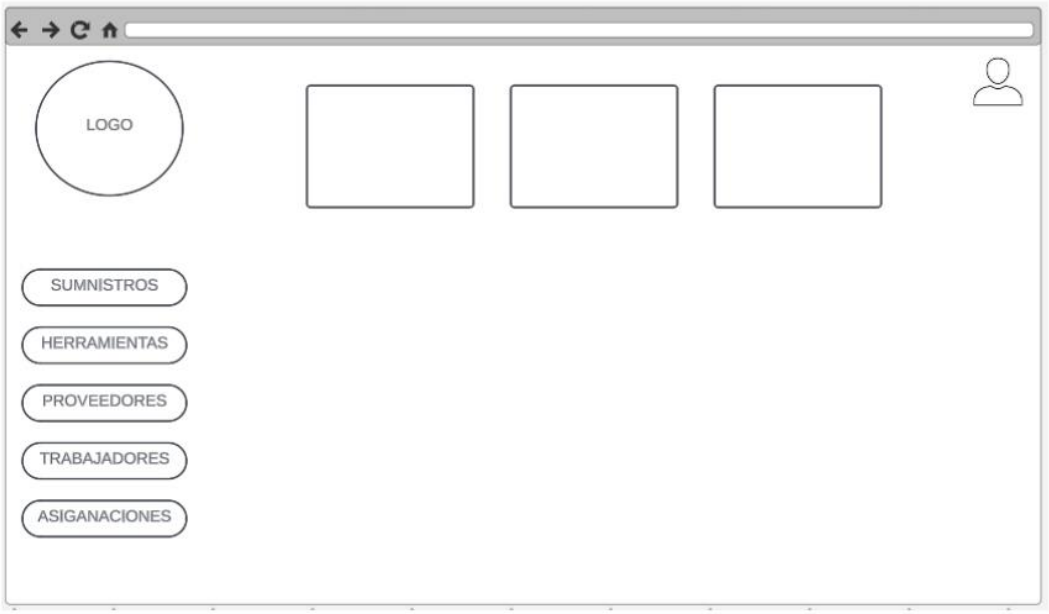
3.1. DISEÑO DE LA BASE DE DATOS E-R

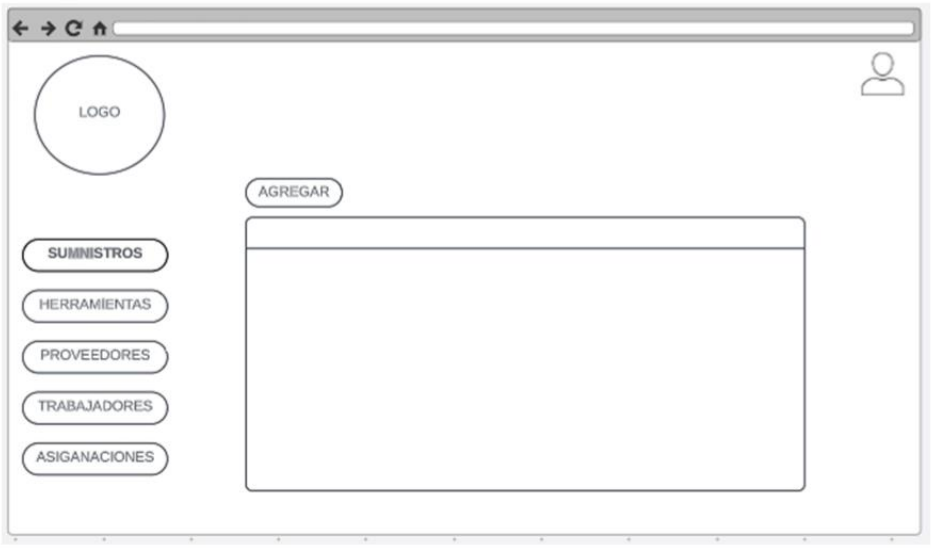


3.2. DEFINIR REQUISITOS DE SEGURIDAD

Requisito de Seguridad	***Descripción***
Política de Contraseñas	Establecer políticas para contraseñas robustas, incluyendo longitud, complejidad y rotación.
Control de Acceso	Implementar mecanismos de control de acceso basados en roles y privilegios.
Encriptación de Datos	Garantizar la encriptación de datos en reposo, en tránsito y durante su procesamiento.
Auditoría de Acceso	Registrar y auditar actividades de acceso al sistema para detectar posibles amenazas.
Respaldo Regular de Datos	Realizar respaldos regulares de la información crítica para la recuperación en caso de pérdida.
Protección contra Malware	Implementar soluciones antimalware y realizar escaneos periódicos en sistemas y redes.
Actualizaciones y Parches de Seguridad	Aplicar regularmente actualizaciones y parches de seguridad en sistemas y software.
Capacitación en Seguridad	Proporcionar formación continua al personal sobre prácticas seguras y concientización.
Gestión de Incidentes de Seguridad	Establecer un protocolo para la gestión y respuesta efectiva ante incidentes de seguridad.
Políticas de Uso Aceptable	Definir políticas claras sobre el uso aceptable de recursos informáticos y de red.
Monitoreo de Vulnerabilidades	Realizar monitoreo constante de vulnerabilidades y aplicar medidas correctivas.

3.3. ELABORACIÓN DE PROTOTIPOS DE INTERFACES




LOGO
AGREGAR
SUMNISTROS
HERRAMIENTAS
PROVEEDORES
TRABAJADORES
ASIGANACIONES

4. DESARROLLO

4.1. Codificación

Codificación módulo “Inicio de sesión”

login.php

```
<!doctype html>
<html lang="en">
  <head>

    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" type="text/css" href="resources/css/estilo.css">
    <link rel="icon"  href="resources/img/logo.png">
     <script src="https://unpkg.com/sweetalert/dist/sweetalert.min.js"></script>
  <script src="https://cdn.jsdelivr.net/npm/sweetalert2@11"></script>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/css/bootstrap.min.css" rel="stylesheet" integrity="
    sha384-EVSTQN3/azprG1Anm3QDgpJLIm9Nao0Yz1ztcQTwFspd3yD65VohhpuuCOmLASjC" crossorigin="anonymous">

    <title>Municipalidad de Sullana</title>
  </head>
  <body>
<br>
<br>
<br>
<br>
<br>
<div class="container px-5 my-5">
  <div class="row justify-content-center">
    <div class="col-lg-8">
      <div class="card border-0 rounded-3 shadow-lg">
        <div class="card-body p-4">
          <div class="text-center">

            <form action="<?php echo base_url('login/validateLogin');?>" method="post">


            <div class="h1 fw-light">INICIO DE SESION</div>
            <p class="mb-4 text-muted">Sistema de gestion de equipos informaticos</p>
          </div>



            <div class="form-floating mb-3">
              <input class="form-control" id="user" name="user" required="Ingrese un usuario" type="text" placeholder="Usuario"
              />
              <label for="user">Usuario</label>
            </div>


            <div class="form-floating mb-3">
              <input class="form-control" id="password" name="password" required="Ingrese una contraseña" type="password"
              placeholder="Contraseña"/>
              <label for="password">Contraseña</label>
```

Codificación módulo “Suministros”

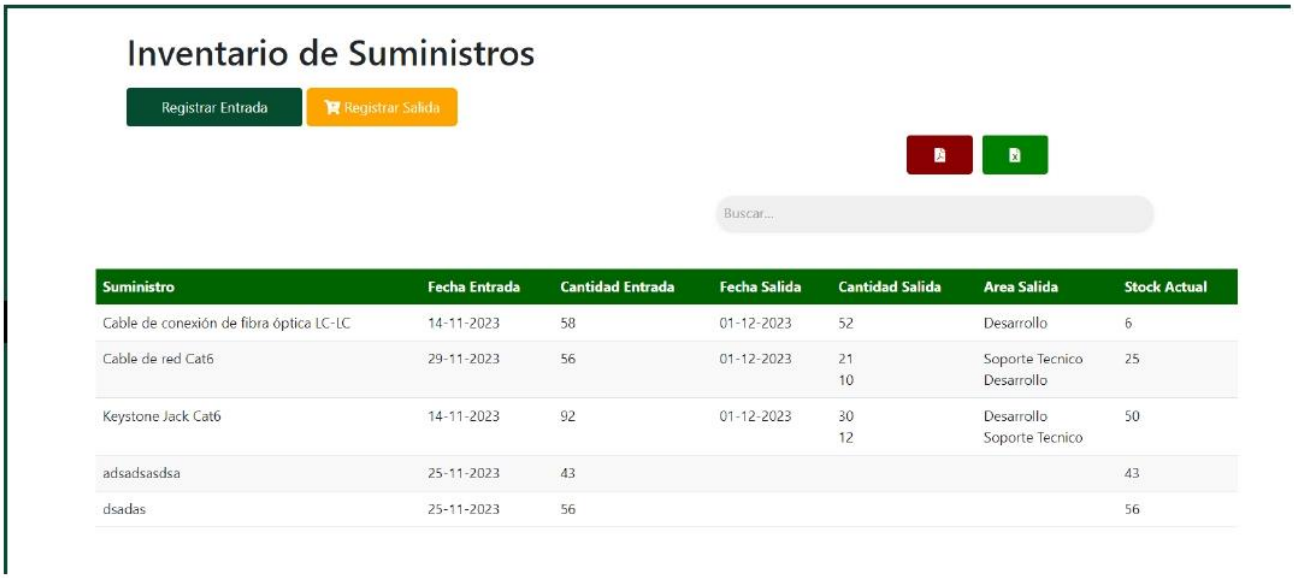
suministros.php

```
        <a href="<?php echo base_url();?>/Inventario" ><i class="fas fa-box-open"></i> Inventario</a>
        <a href="<?php echo base_url();?>/Herramientas"><i class="fas fa-tools"></i> Herramientas</a>
        <a href="<?php echo base_url();?>/Empleados"><i class="fas fa-users"></i> Empleados</a>
        <a href="<?php echo base_url();?>/Asignaciones"><i class="fas fa-tasks"></i> Asignaciones</a>

    </ul>
  </div>
  <div class="container">
      <div class="row">
          <div class="col-lg-6 offset-lg-3">
              <h1>Registro de Suministros</h1>
              <div>
              <button class="registrar-btn" id="registrar-btn">Registrar Suministro</button>
               <a href="<?php echo base_url();?>/Unidad" id="registrar-unidad-btn"><i class="fas fa-ruler"></i></a>

                      <div class="reporte-btn-container">
                      <a href="#" class="reporte-btn" id="reporte-btn" type="submit"><i class="fas fa-file-pdf"></i></a>
                      <a href="#" class="reporte-btn" id="reporte-btn-excel" type="submit"><i class="fas fa-file-excel"></i></a>
                    </div>
                    <br>
                            <div class="search-bar">

          <input type="text" id="search-input" placeholder="Buscar...">
      </div>
  <br>
              <table class="table">
      <thead>
          <tr>
              <th hidden>ID</th>
              <th>Suministro</th>
              <th>Proveedor</th>
              <th>Descripcion</th>
              <th>Unidad</th>
               <th>Editar</th>
              <th>Eliminar</th>
          </tr>

      </thead>
     <?php foreach ($suministros as $suministro) : ?>
              <tr>
                <td hidden><?= $suministro['idSuministros']; ?></td>
                  <td><?= $suministro['suministro']; ?></td>
                  <td><?= $suministro['proveedor']; ?></td>
                  <td><?= $suministro['descripcion']; ?></td>
                  <td><?= $suministro['unidad']; ?></td>
                   <td><a href="#" class="btn-editar" data-id="<?php echo $suministro['idSuministros']; ?>"><i class="fas fa-edit
                  "></i></a></td>
                  <td><a href="#" class="btn-eliminar" data-id="<?php echo $suministro['idSuministros']; ?>"><i class="fas
                  fa-trash"></i></a></td>
```

Codificación modulo “Inventario”

Inventario.php

```php
<?php

namespace App\Controllers;

use App\Models\EntradasModel;
use App\Models\SalidasModel;
use CodeIgniter\Controller;

class Inventario extends BaseController
{
    private $entradasmodel;
    private $salidasmodel;

    public function __construct()
    {
        helper(['form', 'url']);
        $this->entradasmodel = new EntradasModel();
        $this->salidasmodel = new SalidasModel();
    }

    public function index()
    {
        if (!session()->get('isLoggedIn')) {
            return redirect()->to(base_url('Login'));
        }

        $data['entradas'] = $this->entradasmodel
            ->select('entradas.idEntradas, entradas.Fechae, entradas.cantidade, suministros.suministro as suministro')
            ->join('suministros', 'suministros.idSuministros = entradas.Suministroe')
            ->findAll();

        $data['salidas'] = $this->salidasmodel
            ->select('salidas.idSalidas, salidas.Fechasal, salidas.Cantidadsal, suministros.suministro as suministro')
            ->join('suministros', 'suministros.idSuministros = salidas.Suministrosal')
            ->findAll();

        return view('inventario', $data);
    }
}
```



Inventario de Suministros

Registrar Entrada Registrar Salida

Buscar...

Suministro	Fecha Entrada	Cantidad Entrada	Fecha Salida	Cantidad Salida	Area Salida	Stock Actual
Cable de conexión de fibra óptica LC-LC	14-11-2023	58	01-12-2023	52	Desarrollo	6
Cable de red Cat6	29-11-2023	56	01-12-2023	21 10	Soporte Tecnico Desarrollo	25
Keystone Jack Cat6	14-11-2023	92	01-12-2023	30 12	Desarrollo Soporte Tecnico	50
adsadsasdsa	25-11-2023	43				43
dsadas	25-11-2023	56				56

5. PRUEBAS Y VALIDACIÓN

PRUEBA DE ACEPTACION						
FECHA DE EJECUCION:			**27/11/2023**			
MODULO DEL SISTEMA:			***HU-01***			
Código	**Funcionalidad**	**Escenario de prueba**	**Acción del usuario**	**Resultado esperado**	**Resultado obtenido**	**Estado de la prueba**
GI-01	Gestión de Suministros	Agregar unidad para registro del suministro	El usuario debe dar “clic” en el botón Registrar unidad, después procede a llenar todos los campos y por último debe dar “clic” en el botón Registrar	Se espera que la unidad sea registrada satisfactoriamente. La información de la unidad debería mostrarse en la tabla del sistema.	La unidad se registra exitosamente. Los datos de la unidad se visualizan en la tabla del sistema.	Aprobada
		Agregar un nuevo suministro	El usuario debe dar “clic” en el botón Registrar suministro, después procede a llenar todos los campos y por último debe dar “clic” en el botón Registrar	Se espera que el suministro sea registrado satisfactoriamente y se muestre en el sistema.	El suministro se registra exitosamente y se muestra en el sistema.	Aprobada
		Modificar detalles del suministro	El usuario da “clic” en el botón editar de la tabla, luego procede a cambiar los datos que considere, por último, guarda los datos.	Se espera que los cambios realizados en el suministro por el usuario sean guardados satisfactoriamente y se muestren en el sistema	Los datos editados en el suministro se guardan exitosamente después de hacer clic en el botón de guardar	Aprobada
		Eliminar un suministro registrado	El usuario da "clic" en el botón eliminar de la tabla	Se espera que el suministro seleccionado sea eliminado de la tabla de manera satisfactoria.	El suministro es eliminado exitosamente de la tabla después de hacer clic en el botón "Eliminar".	Aprobada
FIRMA						

PRUEBA DE ACEPTACION						
FECHA DE EJECUCION:			27/11/2023			
MODULO DEL SISTEMA:			*HU-02*			
Código	**Funcionalidad**	**Escenario de prueba**	**Acción del usuario**	**Resultado esperado**	**Resultado obtenido**	**Estado de la prueba**
GI-02	Gestión de inventario	Registrar la entrada de un suministro al inventario	El usuario da “clic” en el botón Registrar Entrada, posteriormente procede a llenar todos los campos y por último debe dar “clic” en el botón registrar	Se espera que la entrada del suministro sea registrada satisfactoriamente en el inventario.	Los datos de la entrada del suministro se almacenan adecuadamente y se muestran en el sistema.	Aprobada
		Modificar la entrada del suministro	El usuario da “clic” en el botón editar de la tabla, luego procede a modificar los datos que considere, por último, guarda los datos.	Se espera que los datos del suministro sean modificados de acuerdo con las ediciones realizadas por el usuario y se muestren en el sistema.	Las ediciones realizadas por el usuario se guardan y reflejan adecuadamente en la tabla del sistema	Aprobada
		Eliminar un suministro del inventario	El usuario hace clic en el botón "Eliminar" de la tabla correspondiente al suministro que desea eliminar.	Se espera que el suministro seleccionado sea eliminado de manera satisfactoria del inventario.	El suministro es eliminado con éxito de la tabla.	Aprobada
FIRMA						

PRUEBA DE ACEPTACION						
FECHA DE EJECUCION:			23/11/2023			
MODULO DEL SISTEMA:			*HU-03*			
Código	**Funcionalidad**	**Escenario de prueba**	**Acción del usuario**	**Resultado esperado**	**Resultado obtenido**	**Estado de la prueba**
GI-03	Autenticación de usuarios	Iniciar sesión	El usuario ingresa su nombre de usuario y contraseña.	El sistema valida las credenciales del usuario sean correctas y permite ingresar al sistema	Se validaron los datos del usuario y contraseña correctos y permitió el acceso al sistema	Aprobado

Firma:

Anexo 10. Información de la revista científica donde se postulará el articulo proveniente de los resultados de la presente investigación.

Título tentativo del articulo científico	Modelo metodológico basado en la norma ISO 27001 para el desarrollo de software en empresas peruanas
Nombre de la revista a postular	Thesai
Url de revista	https://thesai.org/Publications/IJACSA
Base de datos de Indización	Scopus
Cuartil	Q3
Idioma	Ingles
ISSN	2156-5570 (Online) 2158-107X (Print)
h-index	35

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, PEÑA CÁCERES OSCAR JHAN MARCOS, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - PIURA, asesor de Tesis titulada: "Modelo metodológico basado en la norma ISO 27001 para el desarrollo de software en empresas de TI", cuyos autores son CASTRO PALACIOS JOUSTIN ARSENIO SANTIAGO, ARCA PRIETO JOSE DANIEL, constato que la investigación tiene un índice de similitud de 19.00%, 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.

PIURA, 30 de Noviembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
PEÑA CÁCERES OSCAR JHAN MARCOS **DNI:** 76505884 **ORCID:** 0000-0002-8159-7560	Firmado electrónicamente por: OJPENAC el 10-12-2023 12:28:25

Código documento Trilce: TRI - 0673722

INVESTIGA UCV