UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIOS DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Auditoría informática basada en Ciclo de Vida ITIL v4 y seguridad de la información en la Caja Piura, Huaraz 2024

Tesis para obtener el título profesional de Ingeniero en Informática y de Sistemas

Autor

Ramírez Vidal Michell

Asesor

Carrasco Alvarado Wilmer Pasión

Código ORCID 0000-0003-3138-9808

Huaraz – Perú

2024

ÍNDICE GENERAL

ÍNDICE DE TABLAS

PALABRAS CLAVE:

Auditoría Informática, Sistemas de información

KEYWORDS:

Computer Audit, Information systems

LÍNEA DE INVESTIGACIÓN:

Línea	Sistema de Gestión
Área	Ciencias Sociales
Sub Área	Economía y Negocios
Disciplina	Negocios y Management

CONSTANCIA DE ORIGINALIDAD

USP UNIVERSIDAD SAN PEDRO | VICERRECTORADO DE INVESTIGACIÓN

CONSTANCIA DE ORIGINALIDAD

El que suscribe, Vicerrector de Investigación de la Universidad San Pedro:

HACE CONSTAR

Que, de la revisión del trabajo titulado **"Auditoría informática basada en Ciclo de Vida ITIL v4 y seguridad de la información en la Caja Piura, Huaraz 2024"** del (a) estudiante: **RAMIREZ VIDAL MICHELL** , identificado(a) con Código N° **1411100336**, se ha verificado un porcentaje de similitud del **20%**, el cual se encuentra dentro del parámetro establecido por la Universidad San Pedro mediante resolución de Consejo Universitario N° 5037-2019-USP/CUpara la obtención de grados y títulos académicos de pre y posgrado, así como proyectos de investigación anual Docente.

Se expide la presente constancia para los fines pertinentes.

Chimbote, 30 de diciembre de 2024

UNIVERSIDAD SAN PEDRO
VICERRECTORADO DE INVESTIGACIÓN
Dr. JAVIER MARTÍNEZ CARRIÓN
VICERRECTOR

NOTA: Este documento carece de valor si no tiene adjunta el reporte del Software TURNITIN.

TÍTULO

Auditoría informática basada en Ciclo de Vida ITIL v4 y seguridad de la información en la Caja Piura, Huaraz 2024

RESUMEN

Este estudio tuvo como objetivo principal estimar en qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la seguridad de la información en la Caja Piura, Huaraz 2024.

Se trabajó investigación básica, no experimental, trasversal y correlacional, aplicó encuesta.

La Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona positiva, moderada y significativa con valor de 0.678 con la seguridad de la información en la Caja Piura, Huaraz 2024, el p valor fue de 0.000. La Auditoría basada en el Ciclo de Vida ITIL v4 tuvo relación positiva, moderada y significativa con valor de 0.645 con la confiabilidad. La correlación encontrada entre Auditoría Informática basada en ITIL v4 y la dimensión Integridad fue positiva, moderada y significativa con valor de 0.584. Se encontró correlación positiva, moderada y significativa con valor de 0.510 entre la Informática basada en ITIL v4 y la dimensión Disponibilidad. Concluyó que la auditoría aplicada tuvo relación positiva, moderada y significativa entre las dos variables estudiadas.

ABSTRACT

The main objective of this study was to estimate to what extent the Audit based on the ITIL v4 Life Cycle is related to information security in the Caja Piura, Huaraz 2024.

Basic, non-experimental, cross-sectional and correlational research was carried out, and a survey was applied.

The Audit based on the ITIL v4 Life Cycle relates positive, moderate and significant with a value of 0.678 with information security in the Caja Piura, Huaraz 2024, the p value was 0.000. The ITIL v4 Lifecycle Based Audit had a positive, moderate and significant relationship with a value of 0.645 with reliability. The correlation found between ITIL v4 based Computer Audit and the Integrity dimension was positive, moderate and significant with a value of 0.584. A positive, moderate and significant correlation was found with a value of 0.510 between ITIL v4-based Computing and the Availability dimension. It concluded that the audit applied had a positive, moderate and significant relationship between the two variables studied.

I. INTRODUCCIÓN

La seguridad es una de las variables de suma importancia para cualquier sistema de información debido a que garantizan la sostenibilidad del desarrollo de los procesos operativos y administrativos, en ese sentido, el presente estudio propone realizar la auditoría informática fundamentada en el Ciclo de Vidad ITIL v4 enfocado en garantizar la seguridad de la infromación en la Caja Piura de la ciudad de Huaraz, 2024, con el propósito conocer cómos se están llevando a cabo los procesos se seguridad de la informácion; por otro lado, se alcanzan las investigaciones antecedentes que van a permitir conocer el estado situacional de las variables en estudio.

A nivel internacional, Alvarez (2023) en la tesis de grado elaborada en una institución universitaria privada ecuatoriana, se trazó el objetivo de realizar estudios técnicos avanzados de análisis de datos como auditoría informática en el sistema informático académico universitario. Aplicó metodología CRISP DM de IBM, modelamiento, trabajó estudio no experimental, transversal, descriptiva, aplicó observación y ficha de verificación. Encontró que con la aplicación de minería de datos en el análisis de la data se pudo identificar patrones de notas rectificadas fuera del calendario indicado con promedio de 15% de datos imprecisos. La Auditoría informática fue evaluada mediante el método MAIIES en índices de calidad con promedio de 69%, seguridad de la información con promedio de 79% y cumplimiento con promedio de 86%. Concluyó que el uso de técnicas de proceso y análisis de datos fue aceptable.

Chuquilla (2022) en la tesis de maestría elaborada en la Universidad de las Fuerzas Armadas, Ecuador; se trazó el objetivo de efectuar un plan de mejora de gestión de servicio de TI Service Desk y Field Support basada en ITIL 4. Trabajó investigación descriptiva no experimental, mixta. Encontró que el control informático aplicando ITIL4; marcos de referencia, COBIT e ISO20000 con ISO9001 tuvo resultado positivo para el desarrollo de planes de acción, planeamiento de proyectos nuevos, procesos ejecutados I&T que ayudaron en el

cumplimiento de los objetivos. Se encontró el tiempo en la ejecución del proceso, posibles mejoras de ejecución de optimización del proceso, en tiempo y costo. Se encontró que la cartera de servicios en el área IT respecto a Infraestructura y comunicaciones, donde se mostró específicamente el catálogo de servicios en el área de IT, matriz de prioridad y acuerdos de niveles de servicio que tiene IT. Se realizó proceso de auditoría de los modelos de gestión de servicio sobre incidentes y requerimientos de servicio. Concluyó que se mejoró la Gestión de servicio TI

Sánchez (2022) en la tesis de grado desarrollada en la Universidad Privada Antenor Orrego, Trujillo Perú, se planteó el objetivo de aplicar auditoría informática en una central de tráfico en la institución edil trujillana. Trabajó investigación descriptiva documental, transversal, población y muestra conformada por los procesos de gestión de la central de tráfico, aplicó observación y análisis. Encontró como resultados que las Normas de Control Interno en función a las TIC se formularon 7 comentarios que facilitaron a identificación de 19 controles y 13 disposiciones de Directiva de Videovigilancia; formularon 6 objetivos de auditoría para evaluar los procesos críticos, se tuvo cumplimiento de normas y directivas actualizadas, la disponibilidad de servicios de comunicación, integridad de la información, confidencialidad, plan de mantenimiento preventivo y el plan de la prevención con la finalidad de instituir adecuada y pertinente Gestión de TI. Elaboró 7 artefactos de auditoría para facilitar la evaluación y acopio de información de la gestión de TI, también identificaron 4 puntos fuertes y 8 débiles lo cual permitió encontrara que la Gestión de TI se calificó como deficiente por falta de apoyo edil.

Galeano y González (2020) en el artículo científico desarrollado en la Universidad Nacional del Este en Paraguay, abordó el objetivo de realizar auditoría informática cimentada en ITIL y COBIT. Trabajo estudio descriptivo, transversal, no experimental, la muestra estuvo estructurada por 24 procesos, aplicaron observación, y métodos de investigación bibliográfica y documentaria, la muestra estuvo conformada por cuatro salas de máquinas de 20 máquinas. Los

resultados indicaron que con la aplicación del modelo de madurez de ITIL se utilizó el ciclo de vida en el análisis del estado situacional de la gestión de TI del Laboratorio objeto de estudio conformado por el diseño, transición, operación, mejora continua y estrategia del servicio. Encontró que el modelo de madurez fue del nivel 4, con 87,5% de los 24 procesos analizados se logró resultado aceptable. En nivel de madurez en ITIL se encontró optimizado ningún proceso 0%, gestionado 21 procesos, 87.5%, definido 3 procesos 12.5%, repetible, inicial y no existe ningún proceso 0%.

A nivel nacional, Rabanal, M. C. (2024) en la tesis de grado realizada en la Universidad Señor de Sipán, en Pimentel Perú; abordó el objetivo de realizar el diseño de un modelo de auditoría de TI para garantizar con eficiencia el cumplimiento de políticas TI en el objeto de estudio. Trabajó estudio cuantitativo, cuasi experimental, continua, trabajó con las políticas como muestra y población, aplicó encuesta y cuestionario. Los resultados de auditoría cumplieron los objetivos planteados, el resultado de 3.98 para juicio de expertos indicó que el modelo fue suficientemente adecuado. Concluyó que el modelo permitió el cumplimiento de las políticas y normas en 95.5%. También encontró que 62% de riesgos fueron controlables, 38 % fueron riesgos intermedios, en ambos casos tubo que aplicar un plan de mitigación. Se encontró que la institución se encontró con nivel de madurez de grado 3, con 86% de cumplimiento de políticas de TI y COBIT, se encontró que se contó con políticas y controles internos, tuvieron que implementar pruebas de seguridad para proteger la información generada, las capacitaciones realizadas fueron. Respecto a la norma ISO 19011 y COBIT 2019, se instituyeron criterios delimitados y enfocados en el control interno y las auditorias TI.

Calderon (2020) en la tesis de grado elaborado en la Universidad Jorge Basadre Grohmann de Tacna Perú; abordó el objetivo de establecer la relación entre la Auditoría Interna y el Sistema de Gestión de Seguridad de la Información de la Caja Municipal de Ahorro y Crédito de Tacna S.A. El estudio fue no experimental, transversal, correlacional y mixta, trabajó con 164 colaboradores como población y 115 de ellos como muestra, aplicó encuesta y cuestionario.

Los resultados indicaron que la eficacia, eficiencia y satisfacción tuvo nivel de acuerdo en 62 %, 56 % y 50 %; respecto a seguridad de personal y privacidad de la información se tuvo 50 % en casi siempre y 52 % siempre; sobre seguridad lógica, seguridad física y ambiental, gestión de incidentes en seguridad de información se tuvo 44 % casi siempre, 59 %, 48 % y 48 % siempre; respecto a disponibilidad fue 56%. En confiabilidad, integridad y disponibilidad se encontraron 48 %, 48 % y 54 % con casi siempre. Concluyó que existió relación positiva moderada significativa de 0.496 entre auditoría interna y el sistema de gestión de seguridad de la información; existió relación positiva baja de 0.338 entre auditoría interna y la confiabilidad del sistema.

A nivel local, Mejía (2022) Díaz (2018) en la tesis de maestría desarrollada en la Universidad Privada del Norte, en Trujillo Perú, abordó el objetivo de establecer la medida en que la auditoría informática se relaciona con la seguridad de la información en una institución financiera. Trabajó estudio descriptivo correlacional, transversal, con población muestral de 10 colaboradores, aplicó encuesta y cuestionario. Los resultados indicaron que el nivel de auditoría estuvo en nivel ineficiente en 70%, en justificación estuvo en un nivel ineficiente en 80%; en adecuación, estuvo en nivel de inicio en 40%, en formalización en 70% estuvo en nivel ineficiente y, sobre desarrollo estuvo en nivel ineficiente en 60%. La confiabilidad de seguridad informática estuvo en nivel ineficiente en 40%, en integridad en nivel de inicio en 40%, disponibilidad estuvo en nivel satisfactorio medio en 40%. Concluyó que existió correlación positiva media de 0.640 entre la auditoría informática y seguridad de la información

Chávez (2017) en la tesis realizada en una institución universitaria estatal en Chimbote, se planteó el objetivo de realizar mejoramiento de procesos del Banco Financiero local aplicado específicamente en al área de crédito mediante auditoría informática. Trabajó investigación contínua, cuantitativo, pre experimental, aplicó observación, análisis, entrevistas y ficha de análisis documental y bibliográfica. La muestra estuvo constituida por 30 colaboradores. Los resultados indicaron que respecto al uso de la página web de la entidad

financiera por parte de los clientes, 75% consideró que no estaba actualizada, y 25% actualizada; 63% no podían hacer consultas y 37% si podían hacerlo; para el 28% satisfizo sus expectativas, para 55% debería ser actualizada con más frecuencia y 18% manifestaron otros detalles. Previo a la auditoría hizo análisis del contexto del área mediante entrevistas y aplicación de normas, se analizaron los procesos y aplicó auditoría aplicando el estándar COBIT con la cual se logró incrementar la satisfacción de los usuarios. Concluyó que la auditoría informática mejoró los procesos del área de crédito.

Fundamento teórico de la Auditoría Informática. La auditoría informática tiene como fundamento la evaluación de los procesos operativos y administrativos en función al desarrollo de las actividades y en comparación con las políticas y normas establecidas para el desarrollo y aplicación de dichas actividades. hoy consiste en una revisión profunda de que los operarios y colaboradores desarrollan con la finalidad de cumplir cada uno de los procesos de la cual está conformado la función operativa y administrativa de la institución (The University of Texas at Austin, 2023; Sabillón & Cano, 2019). Implica la participación de personal seleccionado con el propósito de promover confianza y transparencia en el desarrollo de las actividades (Macias et al., 2021).

La auditoría informática es aquella evaluación que es desarrollado por un equipo profesional, con experiencia y amplio conocimiento de la computación e informática, así como también, de los procesos que son realizados con el sistema de información (Mora, 2017). La auditoría informática aplicada desde la perspectiva de la seguridad de la información tiene el propósito de que dichos sistemas sean operados mediante control eficiente para que se genere un ambiente en donde se garantiza la seguridad de la información y de los recursos hardware y software (Garavit, 2020). Específicamente en la seguridad de la información trata de garantizar la confiabilidad, integridad y accesibilidad a la información de la institución (González, 2018. El proceso operativo de la auditoría informática consiste en la verificación y evaluación pertinente y

adecuada sobre el uso del sistema de información en cada uno de los procesos y actividades, tanto operativos como administrativos, que los colaboradores desarrollan para cumplir su desempeño laboral, esta verificación y evaluación se realiza mediante la observación y análisis de las actividades realizadas usando el sistema de información y comparándolo con lo indicado en las políticas y normas establecidas y teniendo como resultado cumplimiento e incumplimiento de la aplicación de dichas políticas (Jifan & Muhammad, 2021).

Esta auditoría se realiza para decidir la mejora sobre el uso adecuado del sistema de información y cómo se garantiza la seguridad de la información durante el uso de esta tecnología. El proceso de desarrollo o aplicación de la auditoría informática consiste en recabar estatus e información, hacer uso de las normas o políticas establecidas de uso de la información, planificación de la auditoría, organización del personal y las personas habilitadas, generación de presupuesto, implementación o aplicación del proceso de auditoría, generación de estadísticas, interpretaciones de los resultados, recomendaciones y elaboración del informe de auditoría hacia la institución. (Garavit, 2020; González, 2018). Por lo tanto, se entiende la auditoría informática como un conjunto de actividades de análisis y evaluación de cómo se están utilizando el sistema de información en función de la seguridad de los datos información que la institución genera y distribuye con su entorno (Díaz, 2018).

Bases de la Auditoría Informática. Este tipo de auditoría se basa específicamente en los principios fundamentales de la auditoría común otra adicional, específicamente en los enfoques y perspectivas de la auditoría contable, así mismo, se cimenta en los enfoques conductuales de los usuarios del sistema de información y de quién aplica la auditoría, debido a que quienes desarrollan o aplican la auditoría, necesariamente deben adoptar conductas objetivas y pragmáticas durante la evaluación del objeto que se audita, también se fundamenta en los principios fundamentales de los sistemas de computación e informática, específicamente, en su aplicación de acuerdo a las funciones que desarrolla la institución (Pacheco, 2018; Muño, 2017).

Objetivos de la Auditoría informática. Este tipo de auditoría se basa específicamente en los principios fundamentales de la auditoría común otra adicional, específicamente en los enfoques y perspectivas de la auditoría contable, así mismo, se cimenta En los enfoques conductuales de los usuarios del sistema de información y de quién aplica la auditoría, debido a que quienes desarrollan o aplican la auditoría, necesariamente deben adoptar conductas objetivas y pragmáticas durante la evaluación del objeto que se audita, también se fundamenta en los principios fundamentales de los sistemas de computación e informática, específicamente, en su aplicación de acuerdo a las funciones que desarrolla la institución (Jiménez & Ayala, 2019; Nuño, 2017). La auditoría informática tiene como objetivo conocer los procesos de uso digestión de los activos informáticos y su relación con la seguridad con la que se está trabajando con el sistema de información. Otro objetivo de la auditoría informática es garantizar la seguridad de la información y mejorar las conductas de los usuarios respecto al uso del sistema de información, los resultados obtenidos y las políticas establecidas por la organización (Julca, 2019; Pacheco, 2018).

Funciones de la Auditoría Informática. Consiste en verificar el estado situacional del sistema de información, observar y analizar cada uno de los procesos que desarrolla cada usuario de dicho sistema, generar una estadística de cumplimiento e incumplimiento del uso del sistema en comparación con las normas establecidas, desarrollar el informe de auditoría, revisar sugerencias y recomendaciones de mejoramientos el desarrollo de actividades y de cumplimiento de las normas, realizar evaluaciones profundas del uso de normas que se aplican para el uso adecuado de los sistemas de información, examinar los procesos realizados, desarrollar una auditoría objetiva, identificar procesos de mal uso, generación de pérdidas, acciones de fraudes, robos, ataques informáticos, etc. (Urquizo, 2021; Piattini, 2017).

Auditoría. Se conceptúa como el proceso de evaluar objetivamente a cada una de las actividades y procesos que desarrolla uno o más usuarios informáticos en comparación con las políticas y normas establecidas, informar a las autoridades sobre lo encontrado, recomendar y sugerir mejoras para que pueda se puedan tomar decisiones oportunas impertinentes (Díaz, 2020; Vanegas, 2014).

Metodología de desarrollo de la Auditoría Informática. La aplicación metodológica de la auditoría informática consiste en el desarrollo de varias fases bien definidas y que en cada de una de ellas exige la aplicación objetiva del conocimiento de los profesionales de la auditoría; las fases son las siguientes (Imbaquingo et al., 2020; ISACA, 2018):

Fase 1. Planificación. Como todos los tipos de auditoría, la auditoría informática, en su fase de planificación, primeramente, desarrolla un cronograma de actividades que se tienen que desarrollar En las siguientes fases, en esta fase de planificación se identifica el alcance de la auditoría, las técnicas que se van a aplicar, los instrumentos y herramientas a utilizar, los medios, presupuestos y otras consideraciones pertinentes (Imbaquingo & Díaz, 2023). La fase de planificación también implica conocer los procesos y actividades, las normas y políticas con las cuales se van a comparar las actividades desarrolladas, identificación de generalidades y particularidades que pueda tener el desarrollo de las actividades y la aplicación de la auditoría, tomar en cuenta ciertas complejidades que puedan aparecer en el desarrollo de la auditoría, desarrollar un presupuesto habituado y cronograma el tiempo para un adecuado desarrollo de la misma (Felix, 2028; Forense, 2028). También se identifica el porqué de la realización de la auditoría, se desarrollan las visitas al objeto auditado, fue identifican los objetivos de dicha auditoría, significan las áreas críticas de evaluación, se establecen las técnicas y métodos de auditoría, se identifican los procesos e instrumentos necesarios para su desarrollo (Blázquez, 2018; Aponte, 2018).

Fase 2. Ejecución. La fase de aplicación o ejecución del proceso de auditoría consiste en que el equipo auditor observar, analiza y evalúa el uso del sistema de información en cada área de trabajo, ya sea por cada persona o equipo de trabajo, y los compara con lo establecido en las políticas alcanzadas por la institución. en esta fase se desarrolla las estadísticas de cumplimiento e incumplimiento de dichas políticas (Chávez, 2017; Carrizo, 2013). Esta es una de las fases que exige al equipo auditor ser lo más objetivo posible en la obtención de los resultados y en la evaluación que realiza a cada trabajador o equipo de trabajo (Imbaquingo & Díaz, 2023). Es la fase en donde se aplican de los instrumentos y las pruebas con las cuales se recopila los datos e información con el propósito de procesarlos e interpretar la evidencia encontrada y para establecer las recomendaciones pertinentes (Bailon, 2019). Es la fase en donde se aplican de los instrumentos y las pruebas con las cuales se recopila los datos e información con el propósito de procesarlos e interpretar la evidencia encontrada y para establecer las recomendaciones pertinentes (Alexiou, 2017).

Fase 3. Comunicación de resultados. Las conformidades e inconformidades encontradas en la fase de ejecución son comunicadas como resultados en la fase de comunicación, para ello, el equipo auditor elabora un informe en donde se describe que interpretan cada uno de los problemas encontrados, el informe se divide en dos partes, informe preliminar y final; el desarrollo del informe se debería ser de manera objetiva alcanzando las conclusiones y recomendaciones dirigidas a la gerencia correspondiente, así como también debe alcanzar novedades encontradas que no han sido identificadas en el desarrollo del proceso y por las normas o políticas establecidas. el informe debe ser expuesto ante la autoridad pertinente y aprobado por dicha autoridad (The University of Texas at Austin, 2023; Mora, 2017).

Fase 4. Validación. En esta cuarta fase se califica la eficiencia y eficacia de los controles internos realizados, así como el cumplimiento adecuado de la aplicación de las recomendaciones de la auditoría realizada, implica desarrollar otras actividades con la finalidad de dar cumplimiento con los objetivos

establecidos por la auditoría (The University of Texas at Austin, 2023). La fase de validación necesariamente debe ser valorada por las personas que no han sido involucradas en el proceso de auditoría respeto a la calidad de la evaluación desarrollada, evaluación del cumplimiento y evaluación de la seguridad de la información, la auditoría se valida en función a los resultados y en función a la aplicación de las sugerencias establecida (Forense, 2018).

Fase 5. Seguimiento. El desarrollo de la auditoría ya en su última fase, denominada seguimiento, consiste en controlar por un periodo de medio año a un año después de terminado el proceso de auditoría con el informe final, para ello se tiene que analizar el desarrollo de las actividades por los usuarios del sistema de información y ver los cambios recomendados en la auditoría si están siendo aplicadas o no se están cumpliendo adecuadamente tal como fueron los titulados en las recomendaciones, encendimiento consiste en que las recomendaciones establecidas se cumplan para poder lograr el objetivo final de la auditoría (Imbaquingo & Díaz, 2023).

Ciclo de vida ITIL. Proviene del acrónimo Information Technology Infraestructure Library que traducido al español equivale a Biblioteca de Infraestructura de Tecnologías de la Información (BITI), es conceptuado como la agrupación internacional de las mejores prácticas relacionados con la gestión de servicios de tecnologías de información, se concibe como un marco de referencia, una norma de consulta de prácticas que ya han sido comprobadas, y que tiene como objetivo fundamental mejorar la calidad de los servicios cuando se emplea la tecnología de información, lo cual conlleva la reducción de los costos provenientes de una inadecuada gestión de dicha tecnología. Lleva el nombre de ciclo de vida debido a que utiliza el ciclo de vida del servicio mejorando adecuadamente ciertos procesos hasta llegar a convertirlos en procesos conocidos como especializados (Veritier, 2020; Axleos, 2019).

Fundamentos de ITIL. Esta metodología se fundamenta en el estudio y descripción sistemático y organizado u conjunto de prácticas adecuadas que se han desarrollado en la administración y uso de los servicios de la tecnología de

la información a nivel internacional, y por lo tanto, con el compendio de estos conocimientos busca apoyar a todas las instituciones del mundo en una gestión y administración adecuada de los sistemas de información, específicamente en los temas de seguridad informática, ITIL se constituye como una biblioteca de sugerencias y apoyo tecnológico en la gestión y aplicación de la tecnología de la información y los aspectos operativos y administrativos que toda empresa en el mundo desarrolla (Amón & Zhindón, 2020).

Ciclo de Vida de ITIL. El ciclo de vida ITIL o BITI son etapas muy bien definidas y que constituye el elemento fundamental de la estrategia de negocio con la finalidad de realizar procesos de mejora continua en la gestión administrativa del uso y aplicación de la tecnología de la información en los aspectos operativos y administrativos de la organización. el ciclo de vida y ITIL se divide en cinco partes fundamentales, estas son la estrategia de servicio, el diseño de servicios y la transición del servicio. **Estrategia.** Consiste en definir perspectivas, el posicionamiento, modelos y planificación que un proveedor de servicios tiene que ejecutar con la finalidad de alcanzar resultados y requerimientos de la organización. **Diseño.** Consiste en realizar el diseño de servicio ITIL en función a la estrategia establecida, el diseño debe ajustarse a las políticas, procesos y practicas informáticas. **Transición.** En esta fase se planifica la introducción, transformación y salida del servicio, también organiza los medios requeridos y necesarios. **Operación.** Consiste en coordinar y efectuar los procesos y actividades necesarios para administrar los servicios. **Mejora continua**. Consiste en actualizar los servicios ITIL en función a la dinámica cambiante del giro del negocio, se trata de identificar y adoptar mejoras continuas en los procesos que implica el uso de ITIL (Veritier, 2020; Axleos, 2019).

Dimensiones de Auditoría Informática. Esta variable tiene tres dimensiones, Diagnóstico, planificación, implementación e informes. En el diagnostico se tienen los siguientes indicadores: Negocio, informática, uso de normas y matriz de riesgos. En la dimensión Planificación, los indicadores son: Política de

auditoría informática, procesos a evaluar, técnicas y herramientas, equipo de trabajo y presupuesto. En la dimensión Implementación se ha considerado a los indicadores: Análisis de procesos, análisis de riesgos de seguridad, evaluación de procesos y normas y, resultados. En la dimensión Informes, los indicadores son: Presentación, recomendaciones, toma de decisiones y cambios realizados (Veritier, 2020).

Fundamento teórico de la seguridad de la información. El mundo virtual, específicamente el mundo de la computación y la informática tiene una cierta similitud con el mundo real, en dónde, la seguridad es un problema latente y cotidiano, y que la seguridad no se puede garantizar en su totalidad. Todo el capital y la información generada y recibida dentro de un sistema de información está sujeto a diversos tipos de ataques interno y externos, debido al valor e importancia que tienen estos capitales para la organización y los atacantes, la seguridad informática se entiende una condición en donde los activos se encuentra seguros frente a diversos ataques, pero para que ello suceda, los usuarios del sistema de información deben estar adecuadamente capacitados para no autogenerar riesgos y saber enfrentar los diversos tipos de ataques proveniente el exterior y el interior de la institución (Viguri, 2021).

La seguridad informática requiere especial atención por quién dispone el sistema de información, la misma que puede estar o no conectada a una red de computadoras, la seguridad no puede ser cubierta al 100%, pero pueden adoptarse políticas y actividades que pueden contribuir a la reducción significativa de los ataques externos e internos que puedan afectar las dimensiones de integridad, accesibilidad y confiabilidad de la información. Garantizar la seguridad de la información en un sistema informático no solo basta con disponer de todo el hardware de seguridad, tales como, firewall, sistema de actualización de software, disponibilidad de programas antivirus, sistema de detección de ataques o intrusos, etc., sino también de que el personal que usa el sistema de información debe estar debidamente preparado para

enfrentar conscientemente los diversos ataques que se puedan generar dentro del sistema (Peña & Anias, 2020).

La definición semántica del término seguridad los señala como un conjunto de normas técnicas y actividades que consiste en resguardar, prevenir y proteger el capital informático de la institución, la cual puede ser objeto de pérdida, daño y robo mediante ataques informáticos. generalmente los atacantes realizan este tipo de acciones por el valor de la información, por prestigio de haber atacado a un sistema informático, para exigir recompensas económicas mediante el secuestro de la información de importancia institucional. El personal que usa todo tipo de sistema de información como parte del cumplimiento de su desempeño laboral debe ser consciente de que los atacantes buscar la mínima oportunidad me descuido y de generación de vulnerabilidades con la finalidad de atacar al sistema, modificar información, borrar datos o secuestrar toda la información con la finalidad de lograr beneficios económicos posteriores (Imbaquingo & Díaz, 2023).

Seguridad informática. Se entiende como una disciplina cuya función fundamental es garantizar la integridad de la información, lo cual implica, que la documentación se mantenga integra, sin variaciones ni cambios realizados por agentes externos o no autorizados; garantizar la confidencialidad, esto significa que, el contenido de la documentación sólo debe ser conocido por personal autorizado; y garantizar la accesibilidad de la documentación, lo cual consiste, en qué ningún cliente externo o interno, principalmente personal no autorizado pueda acceder en modo lectura o escritura a los archivos importantes y confidenciales de la organización. No se puede garantizar la seguridad informática al 100%, pero se puede minimizar los riesgos y las vulnerabilidades provenientes de ataques de agentes externos o internos (Sabillón & Cano, 2019).

Seguridad de la información. Se entiende a la seguridad de la información como un conjunto de responsabilidades que conllevan a la realización de procedimientos, actividades, disponibilidad de recursos tecnológicos, disponibilidad de conocimientos de seguridad, entre otros recursos, con la

finalidad de gestionar y administrar la seguridad de los datos e información, así como del hardware y software, y de esta manera, garantizar la sostenibilidad operativa y administrativa de la organización (Calderon, 2020)

Definición de riesgo. Se define como la exposición en un determinado nivel para que una amenaza interna o externa se pueda concretizar sobre cualquier parte de un sistema de información generando el juicio a los activos informáticos de la institución, también se entiende al riesgo como una probabilidad de exposición a los ataques informáticos y a la probabilidad de éxito que estos tengan (Sánchez, 2022).

Seguridad Física: Consiste en general barreras físicas y procesos que van a gestionar el control del sistema de información, pueden ser, medidas para prevenir amenazas al hardware, software y documentos relevantes, información confidencial; implica proteger al sistema de información de riesgos sobre altas temperaturas, inundaciones, robo de hardware, proteger al sistema de eventos sísmicos, y otros tipos de eventos que puedan causar daño físico al sistema (Chávez, 2017).

Seguridad Lógica. La seguridad lógica hace referencia a todos los procesos y actividades que se puedan realizar con la finalidad de proteger los datos, archivos de información, diversos tipos de software, sistema operativo, sistemas transaccionales, etc. consiste en generar barreras y procesos tecnológicos que permitan que los atacantes internos o externos no puedan deteriorar a los activos de información en sus dimensiones, integridad, accesibilidad y confiabilidad. la seguridad lógica implica asignar permisos de acceso a los usuarios, generar perfiles de acceso de acuerdo al nivel de autoridad disponga el usuario. La seguridad lógica también implica quién sistema de información deba disponer de hardware y software que proteja específicamente la parte blanda del sistema de información (Chávez, 2017).

Principios básicos de la Seguridad de la Información. Estos principios se fundamentan en las tres dimensiones identificadas del sistema de información y

que consiste en de todos los activos de información deben tener seguros respeto a su integridad, disponibilidad y confidencialidad (Díaz, 2018).

Confidencialidad. Es un atributo de la información que consiste en que el conocimiento el contenido de la documentación o archivos no deben ser conocidos ni divulgados por personal no autorizado, la dimensión confidencialidad quién es relación directa con la accesibilidad hacia el sistema de información, es por ello que se debe asegurar el acceso, tanto hardware como software, en los sistemas de información (Díaz, 2018).

Integridad. La integridad indica que los datos y la información no han sido variados ni cambiados en todo o parte, y que la información se encuentra totalmente íntegra y sin variación en su contenido, indica que no se ha manipulado ni cambiado a la documentación por agentes externos o internos (Chávez, 2017).

Disponibilidad. Hace referencia a que los datos e información debe de estar siempre disponibles para el personal autorizado no disponibles para personal no autorizado, esta disponibilidad indica que el usuario correspondiente debe acceder en cualquier tiempo y en cualquier espacio (Chávez, 2017).

Dimensiones de la seguridad de información. La variable seguridad de información dispone de tres dimensiones qué caracterizan precisamente a todo tipo de información, estos son la disponibilidad, utilidad y confidencialidad. Para esta investigación, la dimensión Confiabilidad tiene como indicadores a la confiabilidad de archivos de gerencia, confiabilidad de archivos de créditos, confiabilidad de archivos de ahorros y confiabilidad de archivos en general. Sobre la dimensión Integridad, se tiene como indicadores a la integridad de archivos de gerencia, integridad de archivos de créditos, integridad de archivos de ahorros y la integridad de archivos en general. Para la dimensión Disponibilidad, se tiene como indicadores a la disponibilidad de archivos de

gerencia, disponibilidad de archivos de créditos, disponibilidad de archivos de ahorros y disponibilidad de archivos en general (Díaz, 2018.

Este estudio científico se justifica en la dimensión social dado que con Auditoría informática basada en Ciclo de Vida ITIL v4 se va a contribuir en garantizar la seguridad de la información en la Caja Piura, Huaraz 2024. En el aspecto social se va a beneficiar a los usuarios del sistema de información con conocimientos de auditoría informática y su respectiva aplicación, conocimientos del siglo de vida ITIL v4, Mientras que la institución financiera se va a beneficiar con la aplicación de esta auditoría, sus resultados que consiste en mejoras de luz en el sistema de información y mejoras en la atención tecnológica al cliente financiero.

Por otro lado, esta investigación es justificada en el aspecto económico debido a que se van a reducir los procesos deficientes que se han venido ejecutando antes de la implementación de la auditoria informática, se van a reducir significativamente las actividades que estaban generando riesgos de seguridad de la información, como resultado de ello, se va a tener en el corto plazo, la reducción de los costos concernientes con demoras, pérdidas de tiempo y costos de repetición de procesos deficientes.

Planteamiento del problema. Debido a la naturaleza de los servicios que prestan los sistemas financieros, entre ellos las cajas de las instituciones civiles en el mundo, siempre van a estar expuestos a ataques internos y externos y que puedan reducir y afectar la seguridad de la información relevante para este tipo de organizaciones financieras. Ninguna institución financiera del mundo se salva de los ataques informáticos, debido a que los atacantes siempre están al acecho de poder vulnerar la seguridad es implementadas en el sistema de información, esto se debe generalmente, a la deficiencia en capacitaciones en seguridad de la información, incumplimiento de las políticas establecidas para el uso de estos

sistemas; estas deficiencias generan las pérdidas de tiempo, demoras, quejas y reclamos por parte de los usuarios, cada institución debe evaluar y calificar los procesos realizados por los usuarios, deben realizar procesos de auditoría dado que es fundamental para garantizar la seguridad en el sistema de información, la cual puede ser interna o externa. De acuerdo con las estadísticas internacionales, en Latinoamérica se concretó un aproximado de 91,000 millones de intentos de ataques informáticos en el 2022 haciendo uso de Internet y software malino como ransomware, esta estadística remarca la importancia que se le debe de dará la seguridad informática en los sistemas financieros, específicamente en las cajas municipales (Universidad Autónoma del Perú, 2023).

A nivel nacional, existen once cajas municipales que se dedican a la microfinanzas, para ello utilizan el sistema de información y las tecnologías modernas, los servicios e internet y los servicios de las redes sociales, estos espacios tecnológicos son muy propicios para cualquier tipo de ataque informáticos que pueda poner en riesgo a la información financiera de las cajas municipales del país, en donde se efectúan los procesos operativos y administrativos concernientes con la atención de los requerimientos de los clientes financieros, específicamente en la prestación de servicio de créditos y ahorros; en este caso, las cajas municipales contratan a personal especializado y profesional en el uso de las tecnologías informáticas. A nivel nacional, estas instituciones constantemente enfrentan diversos tipos de ataques informáticos poniendo en riesgo a la información financiera de las cajas municipales (Díaz 2018). Según Forbes Perú (2023), en el país se dieron 4,700 millones de intentos de ataques por internet en los primeros meses del año y que las empresas pueden pagar entre 10000 a 100000 dólares por el rescate de información secuestrada. Cada día los ataques se modernizan y actualizan, por lo tanto, las cajas municipales se encuentran expuestas a diferentes tipos de ataques informáticos, esto se da porque los clientes financieros efectúan cientos de miles de transacciones presenciales y en línea para compras y ventas, así como, realizar comunicación con personas jurídicas y naturales.

A nivel local, la Caja Piura de la ciudad de Huaraz se encuentra ubicada en la ciudad de Huaraz y tiene como giro del negocio prestar servicios de finanzas y prestación de servicios de ahorros en diversas modalidades, tiene instalado un sistema de información moderno conectado a Internet con disponibilidad de página web, asimismo, hace usos de las redes sociales como medio de distribución de información institucional y financiera a los clientes financieros y su contexto principalmente. Esta caja municipal tiene el área de ahorro y el área de crédito. Actualmente, esa institución presenta problemas de seguridad de información, específicamente en que se desconoce la relación entre la variable Auditoría informática con la seguridad de la información en la Caja Piura, Huaraz 2024, se desconoce cómo se está relacionado la auditoria informática con la confiabilidad de la información y, cómo se está relacionando la Auditoría con la integridad y la Auditoría con la disponibilidad de la información en la Caja Piura, Huaraz 2024.

Ante esta realidad problemática, se plantea determinar las relaciones que pudieran existir entre la auditoría informática basada en el ciclo de vida ITIL v4, las relaciones entre la Auditoría informática con la confidencialidad, integridad y accesibilidad de la información. De no resolverse este problema en el mediano plazo, se espera que la organización financiera podría recaer en costos innecesarios y considerables por desconocimiento de las relaciones entre las variables indicadas y la variable con las dimensiones de la variable seguridad de la información. Con este estudio científico, se plantea efectuar una auditoría informática basada en el ciclo de vida ITIL v4 y seguridad de información en la Caja Piura SAC, Huaraz 2024.

Ante los problemas indiacdos, se ha planteado el problema general que consiste en ¿En qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la seguridad de la información en la Caja Piura, Huaraz 2024? Los problemas específicos considerados son: ¿En qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la confiabilidad de la información en la Caja Piura, Huaraz 2024? ¿En qué medida la Auditoría basada en el Ciclo de Vida ITIL v4

se relaciona con la integridad de la información en la Caja Piura, Huaraz 2024? ¿En qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la disponibilidad de la información en la Caja Piura, Huaraz 2024?

Con la finalidad de lograr los objetivo planteados en este estudio, se desea conocer las relaciones que pudieran existir enre la auditoría infromática basada en el ciclo de vida ITIL v4 en la seguridad de la información en la Caja Piura de la ciudad de Huaraz en donde se instituyan las actividades la investigación, en función a ello, se conceptualizan y operacionalizan las variables en estudio.

Respecto a la conceptualizacion y operacionalizacion de las variables se presenta:

Auditoría Informática: Se conceptúa como el proceso de evaluar, comparar y analizar procesos y actividades desarrollados con el uso de un determinado sistema de información basado en el modelo para auditar la gestión y control de cómo se están usando el sistema de información de la perspectiva del hardware, software e información (Imbaquingo et al., 2020).

Seguridad de información: Se define como las actividades desarrolladas de forma técnica y metodológica para que los usuarios del sistema de información puedan ser usado de forma segura en función a las políticas de seguridad establecidas (Díaz, 2018).

Dimensiones de la Auditoría Informática. en esta investigación se han considerado las dimensiones para esta varibale la dimesión Diagnóstico con los indicadores negocio, informática, uso de norma y matriz de riesgos. La dimensión planificación con los indicadores politica de auditoría informática, procesos a evaluar, técnicas y herramientas, equipod e trabajo, y presupuesto. La dimesión implemntación con los indicadores analiside procesos, analisis de riesgos de seguridad, evaluación de procesos y normas, y resultados. La dimensión informes con los indiacdores presnetación, recomendaciones, toma de decisiones y cambios realziados.

Dimensiones de la Seguridad de la información. Tiene como dimensiones a Confiabilidad con los indicadores onfiabilidad de archivos de gerencia, Confiabilidad de archivos de créditos, Confiabilidad de archivos de ahorros y Confiabilidad de archivos en general, la dimensión Integridad con los indicadores, Integridad de archivos de gerencia, Integridad de archivos de créditos, Integridad de archivos de ahorros y Integridad de archivos en general. La dimensión Disponibilidad con los indicadores Disponibilidad de archivos de gerencia, Disponibilidad de archivos de créditos, Disponibilidad de archivos de ahorros y Disponibilidad de archivos en general.

En la investigación se plantea como hipótesis: La Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona positivamente con la seguridad de la información en la en la Caja Piura, Huaraz 2024.

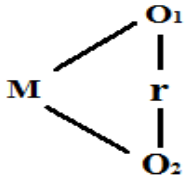
Asimismo, se formuló el objetivo general: Determinar en qué medida la Auditoría basada en EL Ciclo de Vida ITIL v4 se relaciona con la seguridad de la información en la Caja Piura, Huaraz 2024. Así mismo. Los objetivos específicos:

- Determinar en qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la confiabilidad de la información en la Caja Piura, Huaraz 2024.
- Establecer en qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la integridad de la información en la Caja Piura, Huaraz 2024.
- Determinar en qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la disponibilidad de la información en la Caja Piura, Huaraz 2024.

II. METODOLOGÍA

En este estudio científico no se manipulará a la variable Seguridad de la Información mediante la variable Auditoría Informática basada en el ciclo de vida ITIL v4 con el propósito de alcanzar resultados de mejoramiento, en tal sentido, el tipo de estudio va a ser no experimental. Teniendo en cuenta la obtención de datos, el tipo de estudio será transversal debido a que se realizará una única medición en todo el proceso de la investigación. Mientras que el enfoque a aplicar será cuantitativo dado que se va a trabajar con variables, dimensiones e indicadores que constituyen datos numéricos (Hernández et al., 2019).

Respecto al diseño de investigación será descriptivo correlacional, descriptivo debido a que se describirán las variables Auditoría informática fundamentada en el ciclo de vida ITIL v4 y seguridad de la información y sus relaciones que se pudieran encontrar (Ñaupas et al., 2018). El esquema para esta investigación es:



Dónde:

M = Sistema informático de la Caja Piura SAC de la ciudad de Huaraz 2024

O1 = Observación de la Auditoría informática basada en ITIL v4

O2 = Observación de la variable Seguridad de Información

r = Relación entre las variables y las dimensiones de la primera con la segunda variable

Población: La población es un conjunto de elementos conformadoscolaboradores usuarios animales, procesos, etc., cuyos atributos y características similares serán investigados científicamente (Hernández &

Mendoza, 2019), para esta investigación, la población estará conformada por 26 colaboradores usuarios del sistema de información de la Caja Piura SAC de la ciudad de Huaraz, quienes con el uso del sistema genera un determinado nivel de seguridad de la información que generan y comparten, la siguiente tabla muestra la cantidad de colaboradores usuarios del sistema de información por cada área de atención al cliente.

Tabla 2

Población de usuarios

N°	Unidad o área	Cantidad de usuarios
01	Area de créditos	13
02	Area de ahorros	6
03	Otros	7
	TOTAL	**26**

Fuente: Elaboracion propia

Muestra: Es una parte representativa de la poblacion, en el proceso investigativo se toma la muestra cuando la población es significativamente grande por cuestiones de tiempo de estudio y costos (Hernández & Mendoza, 2019). Estará conformada por 26 colaboradores usuarios del sistema de información de la caja Piura SAC de la ciudad de Huaraz, esto significa que tendrá el mismo tamaño de la población.

Técnica: La técnica que se va a aplicar en este estudio será la observación de la seguridad de la información, la investigación documentaria de la auditoría informática basada en ITIL v4 y análisis en ambas variables de estudio.

Instrumento: El instrumento a utilizar en las dos variables de estudio serán la ficha de registros de datos. Dado que estos instrumentos van a ser diseñados por el investigador, necesariamente tendrá que comprobarse la confiabilidad y validez de dichos instrumentos; respecto a la confiabilidad, se aplicará el método de Alfa de Cronbach, en este caso, el instrumento será aplicado si el valor es

mayor a 0.80, en el caso de la validez se aplicará el Juicio de Expertos, la cual deberá ser muy aceptable o excelente para que el instrumento sea aplicado

Metodología de la auditoría. La aplicación del ciclo de vida ITIL o BITI dispone de etapas muy bien definidas y que constituye el elemento fundamental de la estrategia de negocio con la finalidad de realizar procesos de mejora continua en la gestión administrativa del uso y aplicación de la tecnología de la información en los aspectos operativos y administrativos de la Caja Piura SAC. El ciclo de vida y ITIL se divide en cinco partes fundamentales, estas son la estrategia de servicio, el diseño de servicios y la transición del servicio.

Fase 1: Estrategia. Consiste en definir las perspectivas, el posicionamiento, modelos y planificación sobre la seguridad de la información, para ello se debe seleccionar al personal comprometido con la seguridad de información y concientizar a los demás sobre la importancia de la seguridad de la información en el uso del sistema, todos debe tener una perspectiva adecuada de la mejora continua sobre el uso adecuado del sistema de información y su relación con la seguridad de la información. Los participantes deben enfocarse en el valor e importancia de los conocimientos tecnológicos para enfrentar los ataques informático y el valor de la seguridad de la información y de la información sensible e importante de la entidad financiera.

Fase 2: Transición. En esta fase se planifica como debe ser el nivel de seguridad de la información, se identifican las transformaciones o cambios que se deben de realizar y cuáles son los objetivos a alcanzar en un determinado tiempo que debe ser anualmente, en esta fase se deben organizar los recursos humanos y los medios materiales mediante la elaboración de un presupuesto anual para aplicar la metodología. En esta fase se comunica a los participantes la importancia de los archivos de trabajo, el sistema de información, los procesos realizados y su respectiva seguridad.

Fase 3: Diseño. Consiste en realizar el diseño de servicio ITIL en función a la estrategia establecida, el diseño debe ajustarse a las políticas, procesos y practicas informáticas. El diseño contempla la habilidades y competencias iniciales en el uso del sistema, conocimientos de seguridad informática, de los procesos que realiza con el sistema y las tecnologías de ataques y sus características dinámicas y cambiantes en el tiempo. Luego el diseño debe contemplar el progreso de forma iterativa aplicando retroalimentaciones, todos los participantes deben colaborar con sus conocimientos y experiencias en el diseño de cómo se deberá llegar a un nivel aceptable de seguridad de la información.

Fase 4: Operación. Consiste en coordinar y efectuar los procesos y actividades necesarios para administrar los servicios. En esta fase se desarrolla o aplica el ciclo de vida ITIL teniendo en cuenta la estrategia establecida, se desarrollan los procesos de uso del sistema de información teniendo en cuenta la seguridad de la información, al inicio, se debe comenzar desde donde está, se identifican las capacidades iniciales de cada usuario en el uso del sistema, se identifican los conocimientos de seguridad informática de cada uno de ellos, así como de los procesos que realiza con el sistema, y las tecnologías de ataques y sus características dinámicas y cambiantes en el tiempo. Luego fase operativa tiene en cuenta el progreso iterativo de los usuarios, aplica las retroalimentaciones, todos los participantes colaborar con sus conocimientos y experiencias respecto al uso del sistema de información y su respectiva seguridad.

Fase 5: Mejora contínua. Consiste en actualizar los servicios ITIL en función a la dinámica cambiante del giro del negocio, se trata de identificar y adoptar mejoras contínuas en los procesos que implica el uso de ITIL. la mejora continua se sostiene con el control de la mejora en el uso del sistema de información y en la mejora de la seguridad de la información, específicamente en las dimensiones de integridad, accesibilidad y confidencialidad.

III. RESULTADOS

Objetivo específico 1

Determinar en qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la confiabilidad de la información en la Caja Piura, Huaraz 2024.

Tabla 3

Correlación entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Confiabilidad.

			Auditoría Informática basada en ITIL v4	Confiabilidad
Rho de Spearman	Auditoría Informática basada en ITIL v4	Coeficiente de correlación	1,000	,645**
		Sig. (bilateral)	.	,000
		N	26	26
	Confiabilidad	Coeficiente de correlación	,645**	1,000
		Sig. (bilateral)	,000	.
		N	26	26

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

Nota: Esta tabla contiene los valores de correlación entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Confiabilidad, así como el valor de significancia.

La correlación que se encontró entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Confiabilidad fue positiva, moderada y significativa con valor de 0.645, mientras que el p valor fue de 0.000, lo cual fue menor a 0.05, en ese sentido, se confirmó que los datos no correspondieron a una curva normal y se aplicó prueba no paramétrica.

Objetivo específico 2

Establecer en qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la integridad de la información en la Caja Piura, Huaraz 2024.

Tabla 4

Correlación entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Integridad.

			Auditoría Informática basada en ITIL v4	Integridad
Rho de Spearman	Auditoría Informática basada en ITIL v4	Coeficiente de correlación	1,000	,584**
		Sig. (bilateral)	.	,002
		N	26	26
	Integridad	Coeficiente de correlación	,584**	1,000
		Sig. (bilateral)	,002	.
		N	26	26

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

Nota: Esta tabla contiene los valores de correlación entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Integridad, así como el valor de significancia.

La correlación que se encontró entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Integridad fue positiva, moderada y significativa con valor de 0.584, mientras que el p valor fue de 0.002, lo cual fue menor a 0.05, en ese sentido, se confirmó que los datos no correspondieron a una curva normal y se aplicó prueba no paramétrica.

Objetivo específico 3

Determinar en qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la disponibilidad de la información en la Caja Piura, Huaraz 2024.

Tabla 5

Correlación entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Disponibilidad.

			Auditoría Informática basada en ITIL v4	Disponibilidad
Rho de Spearman	Auditoría Informática basada en ITIL v4	Coeficiente de correlación	1,000	,510**
		Sig. (bilateral)	.	,008
		N	26	26
	Disponibilidad	Coeficiente de correlación	,510**	1,000
		Sig. (bilateral)	,008	.
		N	26	26

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

Nota: Esta tabla contiene los valores de correlación entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Disponibilidad, así como el valor de significancia.

La correlación que se encontró entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Disponibilidad fue positiva, moderada y significativa con valor de 0.510, mientras que el p valor fue de 0.008, lo cual fue menor a 0.05, en ese sentido, se confirmó que los datos no correspondieron a una curva normal y se aplicó prueba no paramétrica.

Objetivo general

Determinar en qué medida la Auditoría basada en EL Ciclo de Vida ITIL v4 se relaciona con la seguridad de la información en la Caja Piura, Huaraz 2024.

Tabla 6

Correlación entre la variable Auditoría Informática basada en ITIL v4 y la variable Seguridad de la Información.

			Auditoría Informática basada en ITIL v4	Seguridad de la Información
Rho de Spearman	Auditoría Informática basada en ITIL v4	Coeficiente de correlación	1,000	,678**
		Sig. (bilateral)	.	,000
		N	26	26
	Seguridad de la Información	Coeficiente de correlación	,678**	1,000
		Sig. (bilateral)	,000	.
		N	26	26

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

Nota: Esta tabla contiene los valores de correlación entre la variable Auditoría Informática basada en ITIL v4 y la variable Seguridad de la Información, así como el valor de significancia.

La relación que se encontró entre la variable Auditoría Informática basada en ITIL v4 y la variable seguridad de la Información fue positiva, moderada y significativa con valor de 0.678, mientras que el p valor fue de 0.000, lo cual fue menor a 0.05, en ese sentido, se confirmó que los datos no correspondieron a una curva normal y se aplicó prueba no paramétrica.

IV. ANÁLISIS Y DISCUSIÓN

Esta investigación tuvo como resultado general que el Ciclo de Vida ITIL v4 se relaciona positiva, moderada y significativa con valor de 0.678 con la seguridad de la información en la Caja Piura, estos resultados tuvieron significativa coincidencia con los resultados de la investigación antecedente de Alvarez (2023) debido a que trató la correlación desde otra perspectiva, encontró que con la aplicación de la metodología propuesta pudo identificar patrones de notas rectificadas con promedio de 15% de datos imprecisos, encontró que la Auditoría informática evaluada en índices de calidad se encontró promedio de 69%, seguridad de la información con promedio de 79% y cumplimiento con promedio de 86%, concluyendo que el uso de técnicas de proceso y análisis de datos fue aceptable. También coincide ligeramente con los resultados de Chuquilla (2022) en donde se encontró que el tiempo en la ejecución del proceso presentó mejoras de ejecución de optimización del proceso, en tiempo y costo y que se mejoró la Gestión de servicio TI. Coincidió parcialmente con los resultados de Rabanal (2024) en donde concluyó que el modelo permitió el cumplimiento de las políticas y normas en 95.5%. También encontró que 62% de riesgos fueron controlables, 38 % fueron riesgos intermedios, en ambos casos tubo que aplicar un plan de mitigación. Calderon (2020) quién concluyó que existió relación positiva moderada significativa de 0.496 entre auditoría interna y el sistema de gestión de seguridad de la información. Mejía (2022) concluyó que existió correlación positiva media de 0.640 entre la auditoría informática y seguridad de la información. Chávez (2017) concluyó que la auditoría informática mejoró los procesos del área de crédito.

Los resultados en el primer objetivo específico indicaron que la Auditoría basada en el Ciclo de Vida ITIL v4 tuvo relación positiva, moderada y significativa con valor de 0.645 con la confiabilidad; este resultado coincidió con los resultados de la investigación antecedente de Sánchez (2022) porque encontró que las Normas de Control Interno en función a las TIC existió cumplimiento de normas y directivas actualizadas, la disponibilidad de servicios de comunicación, integridad de la información. No obstante. se encontró diferencias debido a que encontró 4 puntos

fuertes y 8 débiles lo cual permitió encontrará que la Gestión de TI se calificó como deficiente por falta de apoyo edil. Asimismo, coincidió con los resultados de la investigación antecedente de Sánchez (2022) quien encontró como resultados que se tuvo cumplimiento de normas y directivas actualizadas y la confidencialidad de la información. Calderon (2020) quién concluyó que existió relación positiva baja de 0.338 entre auditoría interna y la 48% en confiabilidad del sistema de información. Mejía (2022) tuvo como resultados que la confiabilidad de seguridad informática estuvo en nivel ineficiente en 40%.

En el segundo objetivo específico se encontró que la correlación encontrada entre Auditoría Informática basada en ITIL v4 y la dimensión Integridad fue positiva, moderada y significativa con valor de 0.584; estos resultados coinciden significativamente con los resultados de la investigación antecedente de Sánchez (2022) en donde se encontró que las Normas de Control Interno en función a las TIC existió cumplimiento de normas y directivas actualizadas, la disponibilidad de servicios de comunicación, integridad de la información. Coincidió con oso resultados de Sánchez (2022) quien tuvo como resultado que se cumplieron las normas y directivas actualizadas y la integridad de la información, plan de mantenimiento preventivo y el plan de la prevención con la finalidad de instituir adecuada y pertinente Gestión de TI. Coincide también con la investigación antecedente de Calderon (2020) quien encontró integridad de la información en 48%. Mejía (2022) en integridad en nivel de inicio en 40%.

Para el tercer objetivo se tuvo correlación positiva, moderada y significativa con valor de 0.510 entre la Informática basada en ITIL v4 y la dimensión Disponibilidad, estos resultados coinciden significativamente con los resultados de la investigación antecedente de Sánchez (2022) debido a que encontró que las Normas de Control Interno en función a las TIC existió cumplimiento de normas y directivas actualizadas, la disponibilidad de servicios de comunicación. Coincidió parcialmente con los resultados de la investigación antecedente de Sánchez (2022) quien tuvo como resultado que se cumplieron las normas y directivas actualizadas, la disponibilidad de

servicios de comunicación, integridad de la información, confidencialidad, plan de mantenimiento preventivo y el plan de la prevención con la finalidad de instituir adecuada y pertinente Gestión de TI, pero no coincidió en que en la evaluación y acopio de información de la gestión de TI encontraron que la Gestión de TI se calificó como deficiente por falta de apoyo edil. La investigacion de Calderon (2020) encontró en disponibilidad 54 %. Mejía (2022) disponibilidad estuvo en nivel satisfactorio medio en 40%.

V. CONCLUSIONES

Se concluyó a nivel general que la relación que se encontró entre la variable Auditoría Informática basada en ITIL v4 y la variable Seguridad de la Información en la Caja Piura fue positiva, moderada y significativa con valor de 0.678, con p valor de 0.000, lo cual fue menor a 0.05, confirmando que los datos no correspondieron a una curva normal. este resultado indica influencia media de la variable Auditoría Informática basada en ITIL v4 sobre la variable Seguridad de la Información.

Se determinó que existió correlación entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Confiabilidad de tipo positiva, moderada y significativa con valor de 0.645, con p valor fue de 0.000, lo cual fue menor a 0.05, confirmandose que los datos no correspondieron a una curva normal.

Se estableció que la correlación que se encontró entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Integridad fue positiva, moderada y significativa con valor de 0.584, mientras que el p valor fue de 0.002, lo cual fue menor a 0.05, en ese sentido, se confirmó que los datos no correspondieron a una curva normal.

Se determinó que la correlación que se encontró entre la variable Auditoría Informática basada en ITIL v4 y la dimensión Disponibilidad fue positiva, moderada y significativa con valor de 0.510, mientras que el p valor fue de 0.008, lo cual fue menor a 0.05, en ese sentido, se confirmó que los datos no correspondieron a una curva normal.

.

VI. RECOMENDACIONES

La Gerencia de la empresa financiera Caja Piura de la ciudad de Huaraz debe implementar procesos de auditoría basada en ITIL v4 y la variable Seguridad de la Información con frecuencia semestral con la finalidad de mejorar la Seguridad de la Información, para ello, deben contratar profesionales expertos en ambas variables y que hayan realizado auditorías en instituciones financieras. Estos procesos deben contar con la participación responsable y decidida de todos los involucrados, especialmente de los colaboradores operativos de créditos y ahorros.

La Gerencia de la empresa financiera Caja Piura de la ciudad de Huaraz debe cuidar la dimensión de Confiabilidad mediante la aplicación de la Auditoría Informática basada en ITIL v4, en tal sentido, la gerencia debe capacitar a los usuarios del sistema de información para identificar las informaciones relevantes y confidenciales de la institución financiera, especificamente de las áreas de ahorros, creditos y la gerencia financiera.

La Gerencia de la empresa financiera Caja Piura de la ciudad de Huaraz debe cuidar la dimensión de Integridad mediante la aplicación de la Auditoría Informática basada en ITIL v4, por lo tanto, la gerencia debe capacitar a los usuarios en el uso del sistema de información cuidando que la información solo sea accedida por los usuarios debidamente asignados, que la información no se cambiada o alterada en su contenido por agentes sin permiso a la documentación relevante de la empresa financiera.

La Gerencia de la empresa financiera Caja Piura de la ciudad de Huaraz debe cuidar la dimensión de Disponibilidad mediante la aplicación de la Auditoría Informática basada en ITIL v4, por lo tanto, la gerencia debe capacitar a los usuarios del sistema de información en los principios básicos del marco de referencia ITIL v4, especificamente de las áreas de ahorros, creditos y la gerencia financiera.

VII. AGRADECIMIENTOS

A Dios por permitirme el objetivo de ser profesional, a la Caja Piura de la ciudad de Huaraz por el espacio, los datos e información alcanzada, a la Universidad San Pedro por todo el apoyo recibido a través sus docentes quienes supieron darme la formación y enseñanza, a todos mis compañeros quienes contribuyeron en el logro de mi objetivo, ser profesional.

Michell

VIII. REFERENCIAS BIBLIOGRÁFICAS

Alexiou, S. (2017). *Advanced Data Analytics for IT Auditors*. ISACA, Vol 6, https://www.isaca.org/es-es/resources/isaca-journal/issues/2016/volume-6/advanced-data-analytics-for-it-auditors.

Alvarez, F. (2023). *Estudio de técnicas avanzadas de análisis de datos para el proceso de auditoría informática en el módulo del sistema académico de la Universidad Técnica del Norte*. [Tesis de grado, Universidad Técnica del Norte]. Ecuador.

Amón, J. P., & Zhindón Mora, M. G. (2020). *Modelo de Gobierno y Gestión de TI, basado en COBIT 2019 e ITIL 4, para la Universidad Católica de Cuenca*. Revista Científica FIPCAEC, 5, 239.

Aponte. (2018). *Planeación de la Auditoría Informática - Auditoría Informática*. https://sites.google.com/site/navaintegdesign/temario/1-2

Axleos, L. (2019). *Capacitación de ITIL® 4 Foundation. Manual de Capacitación de ITIL®*. Ferrero, D. (2021). Reporte Gestión de TI. Ferrero, Sistemas. Tumbaco: Reporte

Bailon, W. A. (2019). *Auditoria informática al control y mantenimiento de una infraestructura tecnológica.* CIENCIAMATRIA Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología, 15.

Blázquez Hernández, J. (2018). *Auditoria & Co el portal de la auditoría. Obtenido de La aplicación del Big Data y el Data Analytics en auditoría*: https://auditoria-auditores.com/articulos/articulo-auditoria-la-aplicaci-n-del-big-data-y-el-data-analytics-en-auditor-a/

Calderon, L. D. (2020). *Auditoría interna y el sistema de gestión de seguridad de la información de la Caja municipal de ahorro y crédito de Tacna S.A., 2020*. [Tesis de grado, Universidad Jorge Basadre Grohmann]. Tacna Perú.

Carrizo. (2013). *Auditoria Informática: Un Enfoque Metodológico y Práctico*. México: Continental.

Chávez, N. M. (2017). *Auditoría informática para el área de gestión de créditos Del banco financiero – oficina Chimbote*. [Tesis de grado, Universidad del Santa]. Chimbote. Perú.

Chuquilla, V. A. (2022). *Plan de mejora para La Gestión de Servicio TI - Service Desk & Field Support de La Empresa Ferrero Región Sudamérica Mediante Auditoria Informática Basada en ITIL 4, Cobit 2019 E ISO20000*. [Tesis de maestría, Universidad de las Fuerzas Armadas]. Ecuador.

Díaz Limay, Rudy. (2018). *La auditoría informática y la seguridad de la información en el área de sistemas de la caja del santa, Chimbote 2018*. [Tesis de maestría]. Universidad Privada del Norte. Trujillo. Perú.

Díaz, Rudy. (2018). *La auditoría informática y la seguridad de la información en el área de sistemas de la caja del santa, Chimbote 2018*. [Tesis de maestría, Universidad Privada del Norte]. Trujillo Perú.

Forbes Perú (2024). *¿Qué tanto han avanzado los ciberataques y qué estrategias pueden adoptar las empresas que operan en Perú para enfrentarlos?* https://forbes.pe/especiales/2024-02-15/que-tanto-han-avanzado-los-ciberataques-y-que-estrategias-pueden-adoptar-las-empresas-que-operan-en-peru

Forense, I. (2018). Auditorías Informáticas. https://informatico-forense-madrid.es/como-hacer-auditoria-informatica.

Galeano, P. y González, O. M. (2020). *Auditoría informática basada en combinación de normas ITIL y COBIT aplicada al sistema de gestión del Laboratorio de Informática, FPUNE.* [Artículo científico, Universidad Nacional del Este]. Paraguay.

Garavit, J. (2020). *La Auditoría en la Gestión de Datos*. *Universidad*, 5.

González Mataix, P. (2018). *Auditoría TI en la Asociación APSA. Universidad de Alicante*, 64.

Hernández, R., & Mendoza, C. (2019). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. McGraw-Hill*. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_d e_Abuso/Articulos/SampieriLasRutas.pdf

Hernández, R., Fernández, C., & Baptista, L. (2019). *Metodología de la Investigación*. Valencia: Sexta Edición. México.

Imbaquingo, D., & Díaz, J. (2023). *Quality and security as key factors in the development of Computer Audits in Higher Education Institutions*. Journal of Technology and Science Education. *In Review*.

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., Torre, J. D., & Jácome, J. (2020). *Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura*. RISTI: Revista Ibérica de Sistemas y Tecnologias de Información (E32). https://media.proquest.com/media/hms/PFT/1/YWfNH?_s=NOsfrJmgv8WbV%2FTdqPf5wzusmtU%3D

ISACA (2018) *Basic IS audit: Innovation in the IT audit process*. ISACA Journal, vol. 2, 2018. https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-2/is-audit-basics-innovation-in-the-it-audit-process

Jifan, C., & Muhammad, T. (2021). *Audit Data Analysis and Application Based on Correlation Analysis Algorithm*. Computational and Mathematical Methods in Medicine, 1748-670, https://doi.org/10.1155/2021/2059432.

Jiménez, D. A. & Ayala, J. C. (2019). *Estado del Arte de la Auditoría informática y su importancia para las empresas. Universidad Nacional de Piura*, Escuela profesional de contabilidad, Piura. Perú. https://repositorio.unp.edu.pe/bitstream/handle/UNP/1971/FCC-JIM-ORT-2019.pdf?sequence=1&isAllowed=y

Julca, L. (2019). *Propuesta de un modelo de auditoría de sistemas de información para entidades públicas*, Universidad Nacional de Piura.

Macias, M., Macias, R., Navarrete, M., & Navarrete, J. (2021). *Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática*. Revista científica arbitrada multidisciplinaria pentaciencias, 5(4). doi: https://doi.org/10.59169/pentaciencias.v5i4.700

Mora, E. (2017). *Auditoría Informática*. Costa Rica.

Nuño, P. (2017). *Auditoría de sistemas ¿Qué es una auditoría de sistemas?", Emprende Pyme, 2017*. [Online]. Available: https://www.emprendepyme.net/auditoria-de-sistemas.html. [Accessed: 29- Oct- 2019].

Ñaupas, H.; Valdivia, M. R.; Palacios, J. J. y Romero, H. E. (2018). *Metodología de la Investigación. Cuantitativa - cualitativa y redacción de la tesis*. Quinta edición. Bogotá: Ediciones de la U. ISBN. 978-958-762-876-0

Pacheco Curi, O. E. (2018). *Auditoría de sistemas*. En O. E. Pacheco Curi, *Auditoria De Sistemas* (pág. 12). Lima: OEPC.

Peña, M., & Anias, C. (2020). *Integración de marcos de referencia para gestión de Tecnologías de la Información*. Revista Ingeniería Industrial, 41(1). https://www.redalyc.org/journal/3604/360464918003/html/

Piattini, M. (2017). *Auditoría Informática*. Obtenido de Un Enfoque Práctico. España: computec RAMA.

Rabanal, M. C. (2024). *Diseño de un Modelo de Auditoría de TI para el Cumplimiento de Normas y Políticas de una Empresa Retail peruana*. [Tesis de grado, Universidad Señor de Sipán]. Pimentel Perú.

Sabillón, R., & Cano, J. (2019). *Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones*. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação (32), 33-48. doi: https://doi.org/10.17013/risti.32.33-48

Sánchez, D. A. (2022). *Auditoría informática a la gestión de las tecnologías de información de la central de tráfico, riesgo y monitoreo de la*

Municipalidad Provincial de Trujillo, del período enero-marzo del 2022. [Tesis de grado, Universidad Privada Antenor Orrego]. Trujillo Perú.

The University of Texas at Austin. (2023). *Audit Process.* Office of Internal Audits: https://audit.utexas.edu/audit-process#reporting

Universidad Autónoma del Perú (2023). *Ciberataques: Sector financiero de Latinoamérica expuesto*. https://www.autonoma.pe/blog/ciberataques-el-sector-financiero-de-america-latina-en-estado-vulnerable/

Urquizo Córdova, Ángel Polibio. (2021). *Auditoría informática para la protección de la información digital a la COAC acción y desarrollo Ltda*. *Ciudad de Riobamba período 2018.* [Tesis de grado]. Universidad Nacional de Chimborazo. Ecuador.

Vanegas, L. y Murillo, J. (2014). *Auditoria Informática: Un Enfoque Práctico*. España: computec RAMA. 2016. España: Dreams Magnet. ISBN-13: 978-1940600482

Veritier, C. (2020*). ITIL e ISO / IEC 20000 análisis, comparación y su relación con Agile.* Universidad de Cantabria, máster oficial en empresa y tecnologías de la información. https://repositorio.unican.es/xmlui/bitstream/handle/10902/20750/VERITIER%2cCARLOS.pdf?sequence=1&isAllowed=y

Viguri Cordero, J. A. (2021) *The use of Certification Mechanisms as an efficient guarantee of personal data protection*. Revista Catalana de Dret Públic. 2021;(62):160-176. doi:10.2436/rcdp.i62.2021.3571

ANEXOS Y APÉNDICES

Anexo 01: Matriz de Operacionalización de variables

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala
Auditoría Informática	Se conceptúa como el proceso de evaluar, comparar y analizar procesos desarrollados con uso de un determinado sistema de información basado en el modelo para auditar la gestión y control de cómo se están usando el sistema de información de la perspectiva del hardware, software e información (Imbaquingo et al., 2020)	La variable Auditoría Informática se va a medir en función de los índices, indicadores de cada una de las dimensiones diagnóstico, planificación, implementación e informas	Diagnóstico	Negocio Informática Uso de normas Matriz de riesgos	Ordinal Malo (1) Regular (2) Normal (3) Bueno (4) Excelente (5)
			Planificación	Política de auditoría informática Procesos a evaluar Técnicas y herramientas Equipo de trabajo Presupuesto	
			Implementación	Análisis de procesos Análisis de riesgos de seguridad Evaluación de procesos y normas	
			Informes	Resultados Presentación Recomendaciones Toma de decisiones Cambios realizados	
Seguridad de la información	Se define como las actividades desarrolladas de forma técnica y metodológica para que los usuarios del sistema de información puedan ser usado de forma segura en función a las políticas de seguridad establecidas (Díaz, 2018).	La variable Seguridad de la información se va a medir mediante sus indicadores de las dimensiones confiabilidad integridad y disponibilidad	Confiabilidad	Confiabilidad de archivos de gerencia Confiabilidad de archivos de créditos Confiabilidad de archivos de ahorros Confiabilidad de archivos en general	Ordinal Malo (1) Regular (2) Normal (3) Bueno (4) Excelente (5)
			Integridad	Integridad de archivos de gerencia Integridad de archivos de créditos Integridad de archivos de ahorros Integridad de archivos en general	
			Disponibilidad	Disponibilidad de archivos de gerencia Disponibilidad de archivos de créditos Disponibilidad de archivos de ahorros Disponibilidad de archivos en general	

Anexo 02: Matriz de consistencia

PROBLEMA DE INVESTIGACIÓN	OBJETIVOS	HIPÓTESIS	METODOLOGÍA
Problema General ¿En qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la seguridad de la información en la Caja Piura, Huaraz 2024? **Problemas específicos** ¿En qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la confiabilidad de la información en la Caja Piura, Huaraz 2024? ¿En qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la integridad de la información en la Caja Piura, Huaraz 2024? ¿En qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la disponibilidad de la información en la Caja Piura, Huaraz 2024?	**Objetivo General** Determinar en qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la seguridad de la información en la Caja Piura, Huaraz 2024. **Objetivos Específicos** Determinar en qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la confiabilidad de la información en la Caja Piura, Huaraz 2024. Establecer en qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la integridad de la información en la Caja Piura, Huaraz 2024. Determinar en qué medida la Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona con la disponibilidad de la información en la Caja Piura, Huaraz 2024.	**Hipótesis General** La Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona positivamente con la seguridad de la información en la en la Caja Piura, Huaraz 2024. **Hipótesis Específicas** La Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona positivamente con la confiabilidad de la información en la Caja Piura, Huaraz 2024. La Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona positivamente con la integridad de la información en la Caja Piura, Huaraz 2024. La Auditoría basada en el Ciclo de Vida ITIL v4 se relaciona positivamente con la disponibilidad de la información en la Caja Piura, Huaraz 2024.	Se considera que la investigación es de tipo no experimental. **Diseño de la Investigación** **Diseño:** Descriptivo correlacional. **Enfoque:** Cuantitativo **Población y Muestra:** Los elementos de la población reconformarán 26 trabajadores de la Caja Piura, Huaraz 2024. **Instrumentos de investigación** Encuesta

ANEXO 03: ENCUESTA

Bach. Ramírez Vidal Michell

Estimado encuestado: Sírvase responder con absoluta sinceridad la siguiente encuesta que corresponde al estudio de la Auditoría informática basada en Ciclo de Vida ITIL v4 y seguridad de la información en la Caja Piura, Huaraz 2024. Sírvase responder la encuesta con responsabilidad y honestidad. Este proceso es totalmente anónimo, se reitera el pedido de absoluta honestidad en sus respuestas. Muchas Gracias por su participación.

N°	DIM	FICHA DE REGISTRO DE DATOS	ESCALA				
			1	2	3	4	5
AUDITORÍA INFORMÁTICA BASADA EN ITIL v4							
1	Diagnóstico	Diagnóstico del negocio de la Auditoría informática basada en Ciclo de Vida ITIL v4 en la Caja Piura, Huaraz 2024					
2		Diagnóstico de la informática de la Auditoría informática basada en Ciclo de Vida ITIL v4 en la Caja Piura, Huaraz 2024					
3		Diagnóstico de uso de normas de la Auditoría informática basada en Ciclo de Vida ITIL v4 en la Caja Piura, Huaraz 2024					
4		Diagnóstico de matriz de riesgos de la Auditoría informática basada en Ciclo de Vida ITIL v4 en la Caja Piura, Huaraz 2024					
5	Planificación	Planificación de la Auditoría informática basada en Ciclo de Vida ITIL v4 en la Caja Piura, Huaraz 2024					
6		Planificación de los procesos a evaluar de la Auditoría informática basada en Ciclo de Vida ITIL v4					
7		Planificación de las técnicas y herramientas de la Auditoría informática basada en Ciclo de Vida ITIL v4					
8		Planificación del equipo de trabajo de la Auditoría informática basada en Ciclo de Vida ITIL v4					
9		Planificación del presupuesto de la Auditoría informática basada en Ciclo de Vida ITIL v4					
10	Implementación	Implementación del análisis de procesos de la Auditoría informática basada en Ciclo de Vida ITIL v4					
11		Implementación del análisis de riesgos de seguridad de la Auditoría informática basada en Ciclo de Vida ITIL v4					
12		Implementación de evaluación de procesos y normas de la Auditoría informática basada en Ciclo de Vida ITIL v4					

13		Implementación de los resultados de la Auditoría informática basada en Ciclo de Vida ITIL v4					
14	Informes	Presentación del informe de la Auditoría informática basada en Ciclo de Vida ITIL v4					
15		Recomendaciones del informe de la Auditoría informática basada en Ciclo de Vida ITIL v4					
16		Toma de decisiones en los informes de la Auditoría informática basada en Ciclo de Vida ITIL v4					
17		Cambios realizados en los informes de la Auditoría informática basada en Ciclo de Vida ITIL v4					

Leyenda: Malo 2. Regular 3. Normal 4. Bueno 5. Excelente

N°	DIM	FICHA DE REGISTRO DE DATOS	ESCALA				
			1	2	3	4	5
SEGURIDAD DE LA INFORMACIÓN							
1	Confiabilidad	Confiabilidad de archivos de gerencia respecto a seguridad de la información en la Caja Piura, Huaraz 2024					
2		Confiabilidad de archivos de créditos sobre seguridad de la información en la Caja Piura, Huaraz 2024					
3		Confiabilidad de archivos de ahorros sobre seguridad de la información en la Caja Piura, Huaraz 2024					
4		Confiabilidad de archivos en general respecto a seguridad de la información en la Caja Piura, Huaraz 2024					
5	Integridad	Integridad de archivos de gerencia respecto a seguridad de la información en la Caja Piura, Huaraz 2024					
6		Integridad de archivos de créditos sobre seguridad de la información en la Caja Piura, Huaraz 2024					
7		Integridad de archivos de ahorros sobre seguridad de la información en la Caja Piura, Huaraz 2024					
8		Integridad de archivos en general respecto a seguridad de la información en la Caja Piura, Huaraz 2024					
9	Disponibilidad	Disponibilidad de archivos de gerencia de la Auditoría informática basada en Ciclo de Vida ITIL v4					
10		Disponibilidad de archivos de créditos de la Auditoría informática basada en Ciclo de Vida ITIL v4					
11		Disponibilidad de archivos de ahorros de la Auditoría informática basada en Ciclo de Vida ITIL v4					
12		Disponibilidad de archivos en general de la Auditoría informática basada en Ciclo de Vida ITIL v4					

Leyenda: Malo 2. Regular 3. Normal 4. Bueno 5. Excelente

ANEXO 04: ALFA DE CRONBACH

N°	Auditoría Informática basado en ciclo de vidad ITIL v4																				
	Diagnóstico				TOT	Planificación					TOT	Implementación				TOT	Informes				TOT	TOT
	1	2	3	4		5	6	7	8	9		10	11	12	13		14	15	16	17		
1	2	1	3	2	8	2	2	1	2	1	8.0	1	2	5	2	10.0	1	2	4	2	6	32.0
2	2	1	1	1	5	1	1	1	1	1	5.0	1	1	3	1	6.0	1	2	3	1	4	20.0
3	3	4	4	5	16	3	5	3	5	4	20.0	5	5	4	3	17.0	3	5	3	5	8	61.0
4	1	2	3	1	7	4	2	2	1	2	11.0	4	2	1	1	8.0	5	2	4	5	9	35.0
5	2	3	3	2	10	2	1	1	3	2	9.0	1	1	2	2	6.0	1	1	3	2	5	30.0
6	2	2	4	5	13	5	2	5	2	4	18.0	2	4	4	5	15.0	3	5	5	4	9	55.0
7	4	3	3	2	12	3	4	3	5	2	17.0	3	3	3	3	12.0	2	3	3	3	6	47.0
8	1	1	1	2	5	1	1	2	1	2	7.0	1	1	1	1	4.0	1	1	1	2	3	19.0
9	3	5	3	4	15	1	2	1	3	1	8.0	1	2	3	2	8.0	1	4	2	2	4	35.0
10	2	5	4	1	12	3	3	2	4	1	13.0	2	1	5	2	10.0	1	2	1	3	4	39.0
Var					1.64						24					15.2					4.84	
																				Suma de varianzas	46.9	
																				Varianza General	169.81	
																				Valor de Alfa	0.965	

N°	SEGURIDAD DE LA INFORMACIÓN															
	Confiabilidad				TOT	Integridad				TOT	Disponibilidad				TOT	TOT
	1	2	4	5		6	7	9	10		11	12	14	15		
1	1	3	2	5	11.0	1	2	4	2	9.0	1	4	1	1	2	22.0
2	2	1	1	1	5.0	2	1	3	1	7.0	2	1	4	1	5	17.0
3	2	1	3	5	11.0	2	4	2	2	10.0	1	2	2	1	3	24.0
4	1	1	1	2	5.0	1	2	1	1	5.0	1	2	1	1	2	12.0
5	2	1	2	1	6.0	1	1	2	2	6.0	1	1	2	2	4	16.0
6	3	2	2	5	12.0	4	5	4	4	17.0	5	2	5	4	9	38.0
7	3	3	3	2	11.0	3	3	3	3	12.0	2	3	3	3	6	29.0
8	1	5	1	4	11.0	1	5	1	4	11.0	3	5	4	5	9	31.0
9	1	2	2	2	7.0	1	2	1	2	6.0	1	3	4	1	5	18.0
10	3	1	1	1	6.0	5	5	5	5	20.0	3	4	5	4	9	35.0
Var					7.65					22					7.82	
														Suma de varianzas	24.47	
														Varianza General	68.76	
														Valor de Alfa	0.966	

Anexo 05

Base de datos

N°	AUDITORÍA INFORMÁTICA BASADA EN ITIL v4																
	Diagnóstico				Planificación					Implementación				Informes			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	2	3	1	1	1	1	2	2	1	2	1	1	1	2	2	1	1
2	4	5	4	3	5	3	2	5	4	2	4	5	2	4	5	5	5
3	1	1	1	2	1	1	1	2	3	1	1	1	3	1	1	1	3
4	2	2	3	3	2	2	3	3	2	2	3	1	1	2	2	1	1
5	3	3	2	3	2	3	3	3	3	3	2	3	3	3	2	3	3
6	1	2	1	1	1	2	1	1	1	2	1	1	1	2	1	1	2
7	4	5	5	5	3	5	5	5	4	5	5	5	5	4	5	5	4
8	2	2	2	3	3	3	3	3	2	2	2	3	3	3	3	3	3
9	2	1	2	1	2	1	1	1	1	1	2	2	1	1	1	2	1
10	3	3	3	2	3	3	2	2	3	3	3	2	2	2	2	2	2
11	3	2	3	3	3	3	3	3	2	2	3	2	3	3	3	2	3
12	3	3	2	3	3	3	2	2	3	3	2	3	3	3	3	3	3
13	1	3	2	3	3	2	3	3	3	3	3	3	3	2	3	3	3
14	1	2	1	1	2	1	1	2	1	2	1	3	2	3	2	3	2
15	1	3	1	3	3	4	3	2	5	3	2	2	4	3	4	4	4
16	4	3	4	3	4	3	4	3	4	3	4	4	3	3	4	5	5
17	1	2	3	1	3	2	1	1	1	2	3	1	2	2	3	1	2
18	2	3	2	2	3	3	3	4	3	3	5	2	3	3	5	2	3
19	2	2	2	3	3	3	3	3	2	2	2	3	3	3	3	3	3
20	2	1	2	1	2	1	1	1	5	1	2	2	1	1	1	2	1
21	5	5	4	5	5	4	5	5	3	3	3	5	2	5	2	2	5
22	3	2	5	3	2	2	3	3	2	2	3	1	1	2	2	1	1
23	2	2	2	1	3	1	1	1	2	1	2	1	2	1	2	1	2
24	3	3	3	3	3	2	3	3	3	2	3	3	3	2	3	3	3
25	5	4	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5
26	1	3	1	2	3	5	3	2	1	3	2	1	3	1	1	2	1

N°	SEGURIDAD DE LA INFORMACIÓN											
	Confiabilidad				Integridad				Disponibilidad			
	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	1	2	2	2	2	2	3	3	2	2
2	5	4	5	5	5	5	5	5	5	5	5	5
3	1	1	1	2	1	1	1	3	1	1	1	1
4	1	1	2	1	1	2	1	1	2	1	1	1
5	2	3	2	2	2	3	2	2	2	3	2	2
6	1	1	1	1	2	1	2	1	1	2	1	1
7	4	4	3	2	4	5	2	2	3	4	4	4
8	3	4	2	3	2	3	3	4	2	4	3	3
9	2	1	3	2	2	4	2	1	2	2	2	3
10	3	2	2	2	2	2	3	2	2	2	1	2
11	3	4	3	5	4	4	4	4	5	5	5	4
12	2	3	2	1	2	3	2	3	2	2	3	2
13	4	4	3	4	5	5	5	2	5	5	4	5
14	2	2	1	2	2	3	3	1	3	2	1	2
15	4	4	4	5	4	3	4	4	3	4	4	4
16	5	4	5	5	5	3	5	4	5	5	4	5
17	1	1	1	2	1	2	1	1	2	2	1	2
18	2	3	2	2	3	3	3	3	3	3	2	3
19	2	2	2	2	2	2	2	2	2	2	2	3
20	2	4	3	2	3	3	2	3	3	3	3	3
21	3	2	2	2	2	3	2	2	1	2	1	1
22	1	1	1	2	1	1	1	2	1	1	1	1
23	2	1	2	2	3	1	2	2	1	2	3	2
24	3	1	2	1	1	1	2	1	1	1	2	1
25	3	4	4	4	4	3	3	5	4	4	5	4
26	3	1	1	2	1	1	2	1	2	2	1	2

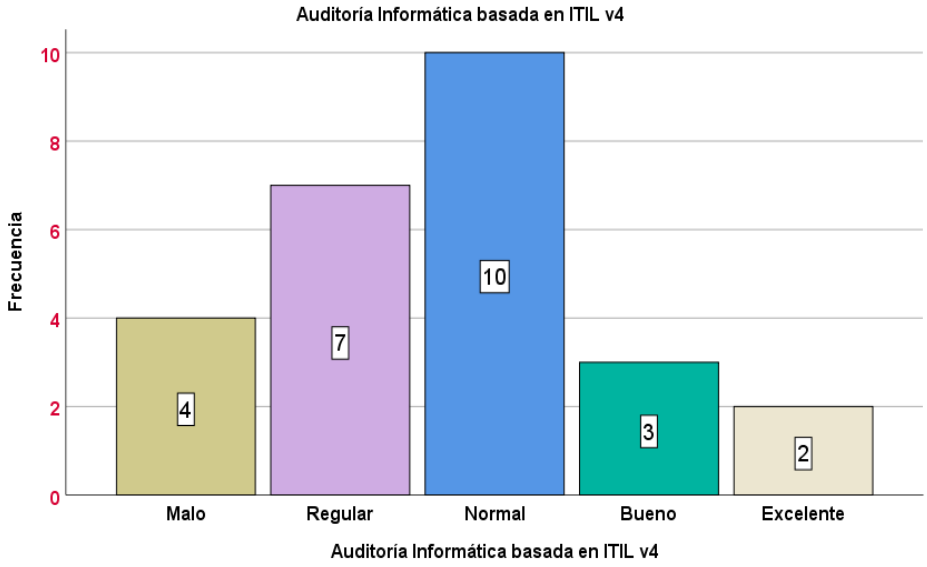
Anexo 06

Resumen de tabla de frecuencias

Tabla de frecuencia

Auditoría Informática basada en ITIL v4

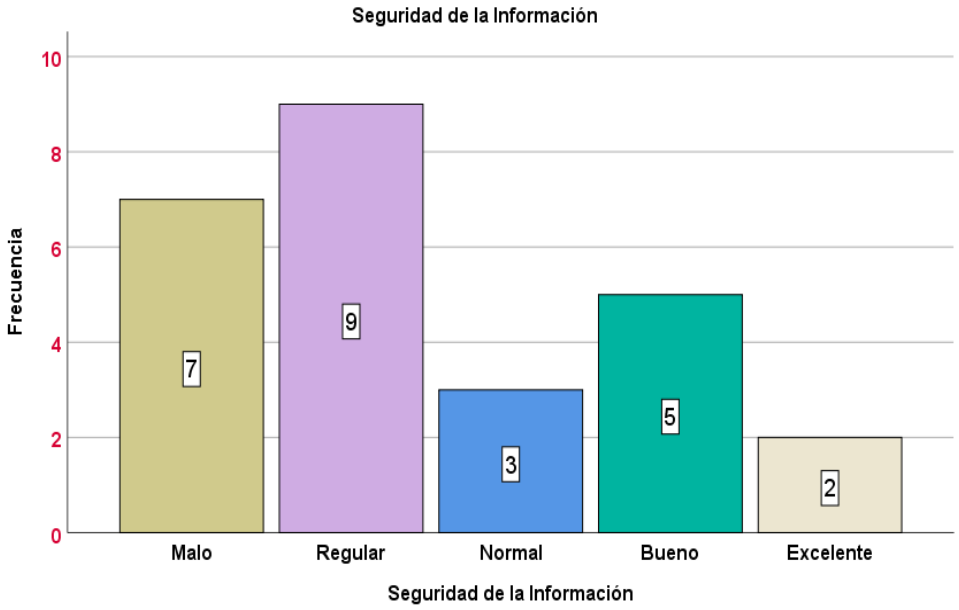
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	15,4	15,4	15,4
	Regular	7	26,9	26,9	42,3
	Normal	10	38,5	38,5	80,8
	Bueno	3	11,5	11,5	92,3
	Excelente	2	7,7	7,7	100,0
	Total	26	100,0	100,0	



Con referencia al resumen de la variable Auditoría informática basada en ITIL v4, en la Caja Piura, Huaraz 2024, se observó que en 4 casos (15.4%) se encontraron en nivel malo, 7 casos (26.9%) se encontró en nivel regular, 10 casos (38.5%) se encontraron en nivel normal, 3 casos (11.5%) se encontraron en nivel bueno, y, 2 casos (7.7%) se encontró en nivel excelente.

Seguridad de la Información

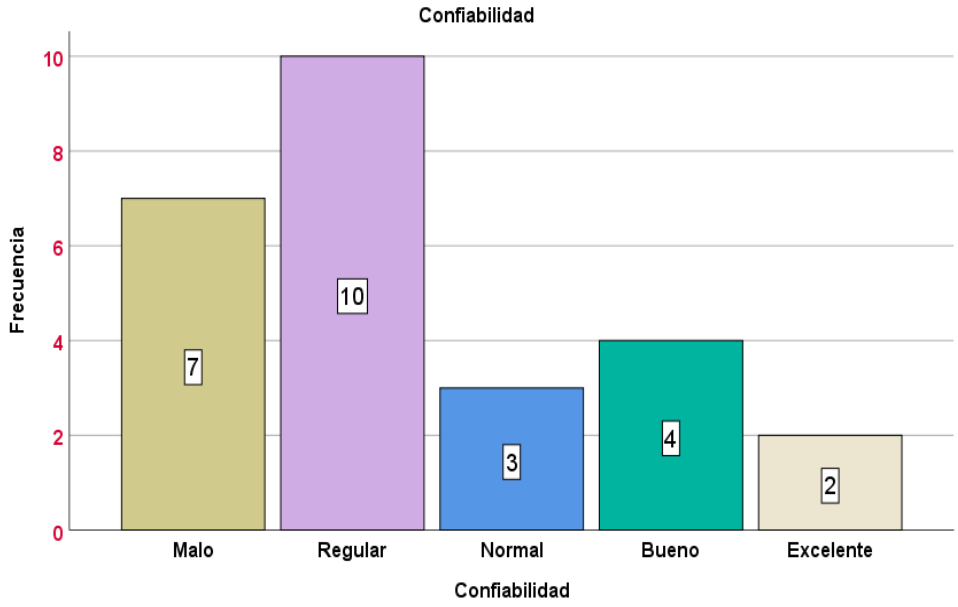
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	26,9	26,9	26,9
	Regular	9	34,6	34,6	61,5
	Normal	3	11,5	11,5	73,1
	Bueno	5	19,2	19,2	92,3
	Excelente	2	7,7	7,7	100,0
	Total	26	100,0	100,0	



Con referencia al resumen de la variable Seguridad de la Información en la Caja Piura, Huaraz 2024, se observó que en 7 casos (26.9%) se encontraron en nivel malo, 9 casos (34.6%) se encontró en nivel regular, 3 casos (11.5%) se encontraron en nivel normal, 5 casos (19.2%) se encontraron en nivel bueno, y, 2 casos (7.7%) se encontró en nivel excelente.

Confiabilidad

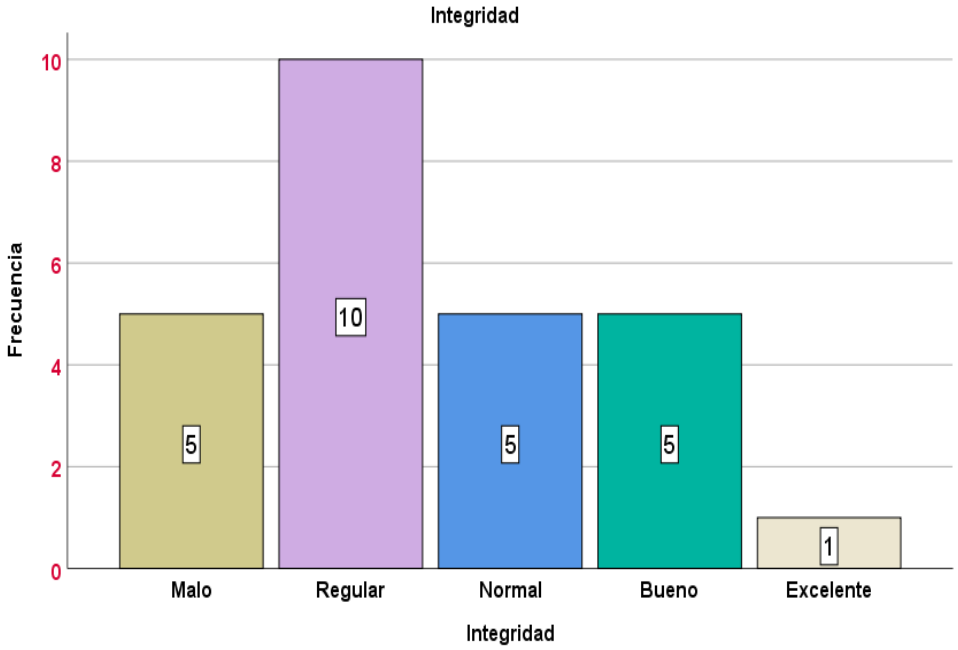
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	26,9	26,9	26,9
	Regular	10	38,5	38,5	65,4
	Normal	3	11,5	11,5	76,9
	Bueno	4	15,4	15,4	92,3
	Excelente	2	7,7	7,7	100,0
	Total	26	100,0	100,0	



Sobre el resumen de la dimensión Confiabilidad de la variable Seguridad de la Información en la Caja Piura, Huaraz 2024, se observó que en 7 casos (26.9%) se encontraron en nivel malo, 10 casos (38.5%) se encontró en nivel regular, 3 casos (11.5%) se encontraron en nivel normal, 4 casos (15.4%) se encontraron en nivel bueno, y, 2 casos (7.7%) se encontró en nivel excelente.

Integridad

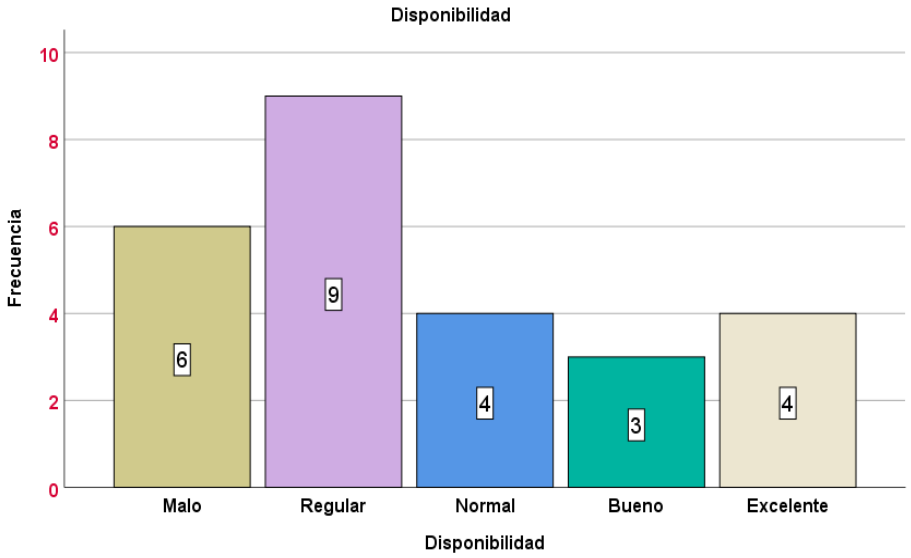
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	19,2	19,2	19,2
	Regular	10	38,5	38,5	57,7
	Normal	5	19,2	19,2	76,9
	Bueno	5	19,2	19,2	96,2
	Excelente	1	3,8	3,8	100,0
	Total	26	100,0	100,0	



Sobre el resumen de la dimensión Integridad de la variable Seguridad de la Información en la Caja Piura, Huaraz 2024, se observó que en 5 casos (19.2%) se encontraron en nivel malo, 10 casos (38.5%) se encontró en nivel regular, 5 casos (11.5%) se encontraron en nivel normal, 5 caso (19.2%) se encontró en nivel bueno, y, 1 caso (3.8%) se encontró en nivel excelente.

Disponibilidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	23,1	23,1	23,1
	Regular	9	34,6	34,6	57,7
	Normal	4	15,4	15,4	73,1
	Bueno	3	11,5	11,5	84,6
	Excelente	4	15,4	15,4	100,0
	Total	26	100,0	100,0	



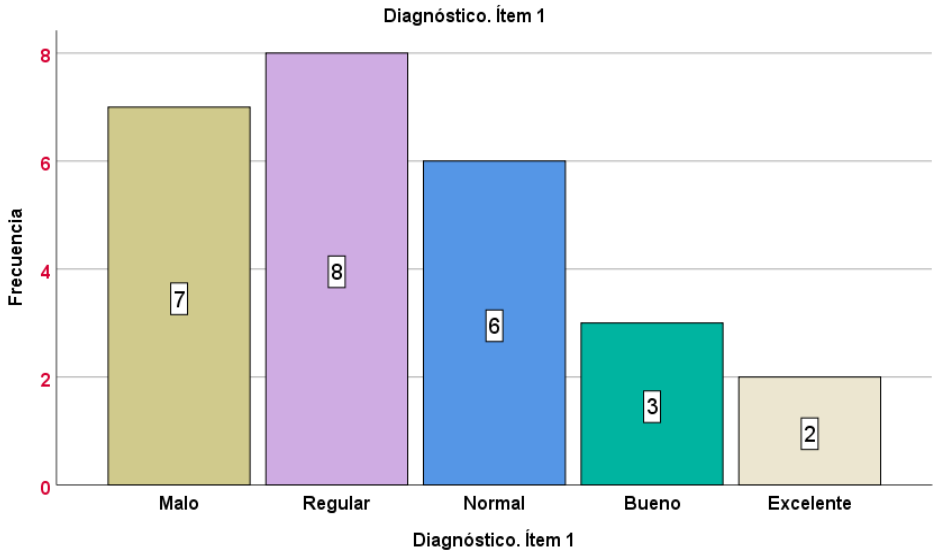
Sobre el resumen de la dimensión Disponibilidad de la variable Seguridad de la Información en la Caja Piura, Huaraz 2024, se observó que en 6 casos (23.1%) se encontraron en nivel malo, 9 casos (34.6%) se encontró en nivel regular, 4 casos (15.4%) se encontraron en nivel normal, 3 casos (11.5%) se encontró en nivel bueno, y, 4 casos (15.4%) se encontró en nivel excelente.

Anexo 7:

Procesamiento de datos en tablas de frecuencias

Diagnóstico. Ítem 1

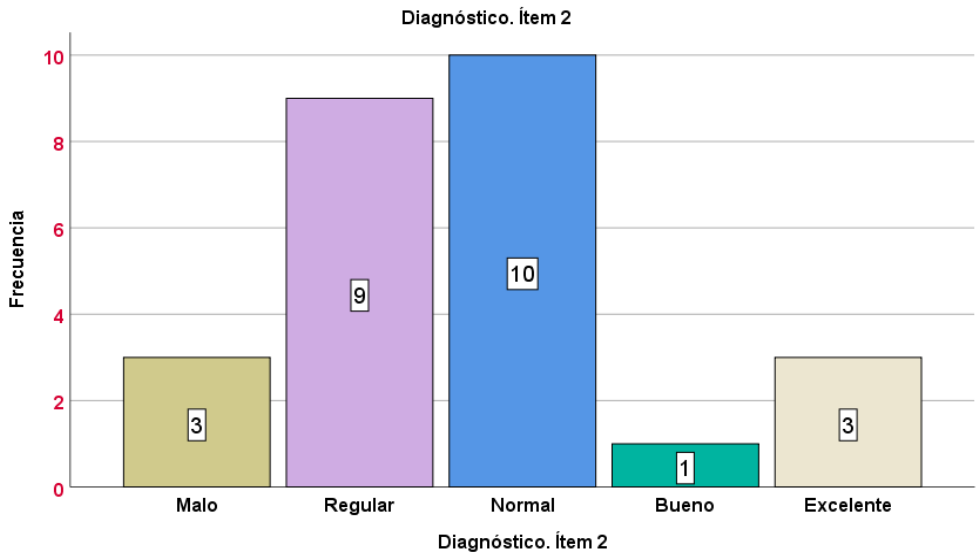
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	26,9	26,9	26,9
	Regular	8	30,8	30,8	57,7
	Normal	6	23,1	23,1	80,8
	Bueno	3	11,5	11,5	92,3
	Excelente	2	7,7	7,7	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 1 sobre el diagnóstico del negocio de la Auditoría informática basada en Ciclo de Vida ITIL v4 en la Caja Piura, Huaraz 2024, en el Ítem 1 de la dimensión Diagnostico, se observó que en 7 casos (26.9%) se encontraron en nivel malo, 8 casos (30.8%) se encontró en nivel regular, 6 casos (23.1%) se encontraron en nivel normal, 3 casos (11.5%) se encontraron en nivel bueno, y, 2 casos (7.7%) se encontró en nivel excelente.

Diagnóstico. Ítem 2

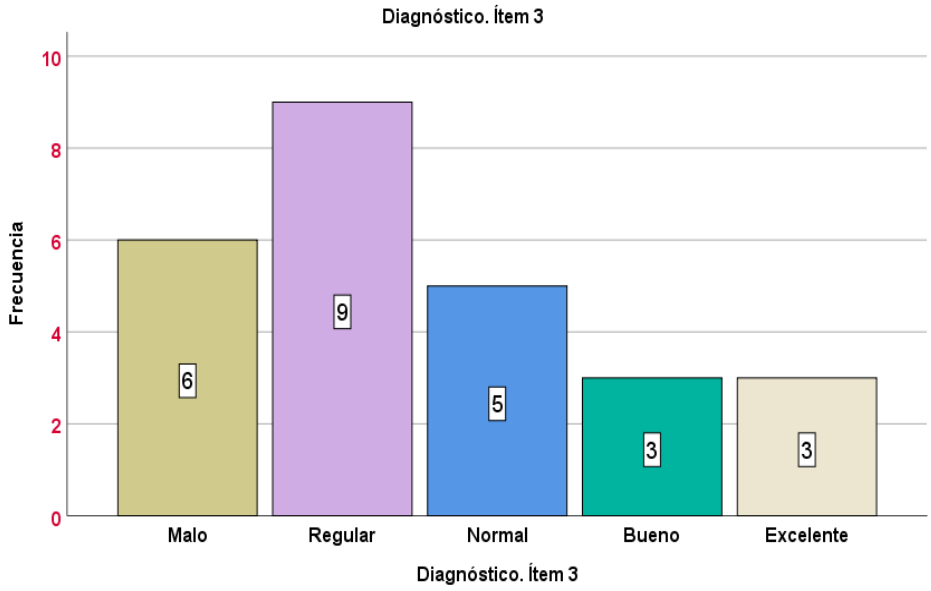
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	3	11,5	11,5	11,5
	Regular	9	34,6	34,6	46,2
	Normal	10	38,5	38,5	84,6
	Bueno	1	3,8	3,8	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 2 Diagnóstico de la informática de la Auditoría informática basada en Ciclo de Vida ITIL v4 en la Caja Piura, Huaraz 2024, en el Ítem 2 de la dimensión Diagnostico, se observó que en 3 casos (11.5%) se encontraron en nivel malo, 9 casos (34.6%) se encontró en nivel regular, 10 casos (38.5%) se encontraron en nivel normal, 1 casos (3.8%) se encontraron en nivel bueno, y, 3 casos (11.5%) se encontró en nivel excelente.

Diagnóstico. Ítem 3

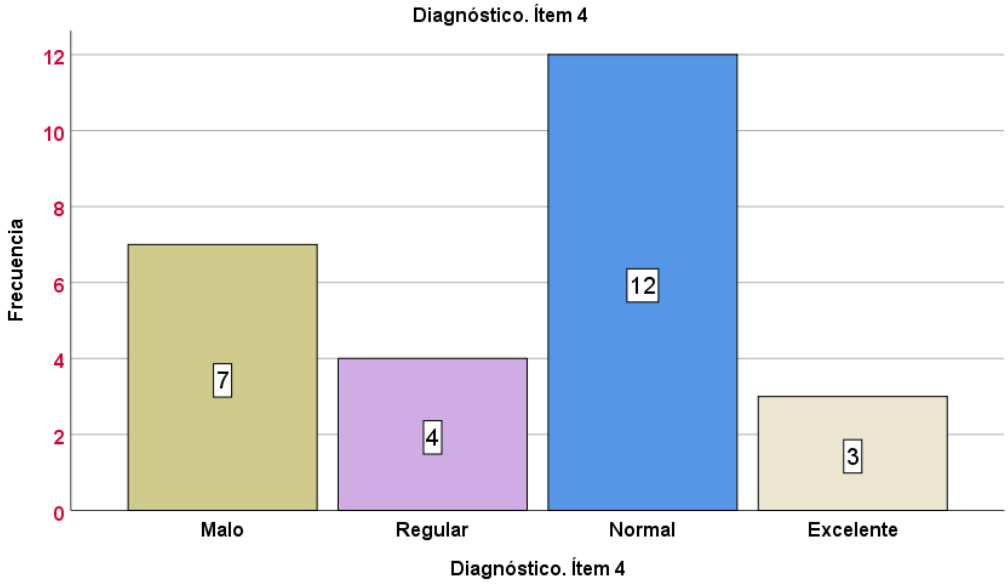
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	23,1	23,1	23,1
	Regular	9	34,6	34,6	57,7
	Normal	5	19,2	19,2	76,9
	Bueno	3	11,5	11,5	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 3 Diagnóstico de uso de normas de la Auditoría informática basada en Ciclo de Vida ITIL v4 en la Caja Piura, Huaraz 2024, en el Ítem 3 de la dimensión Diagnostico, se observó que en 6 casos (23.1%) se encontraron en nivel malo, 9 casos (34.6%) se encontró en nivel regular, 5 casos (19.2%) se encontraron en nivel normal, 3 casos (11.5%) se encontraron en nivel bueno, y, 3 casos (11.5%) se encontró en nivel excelente.

Diagnóstico. Ítem 4

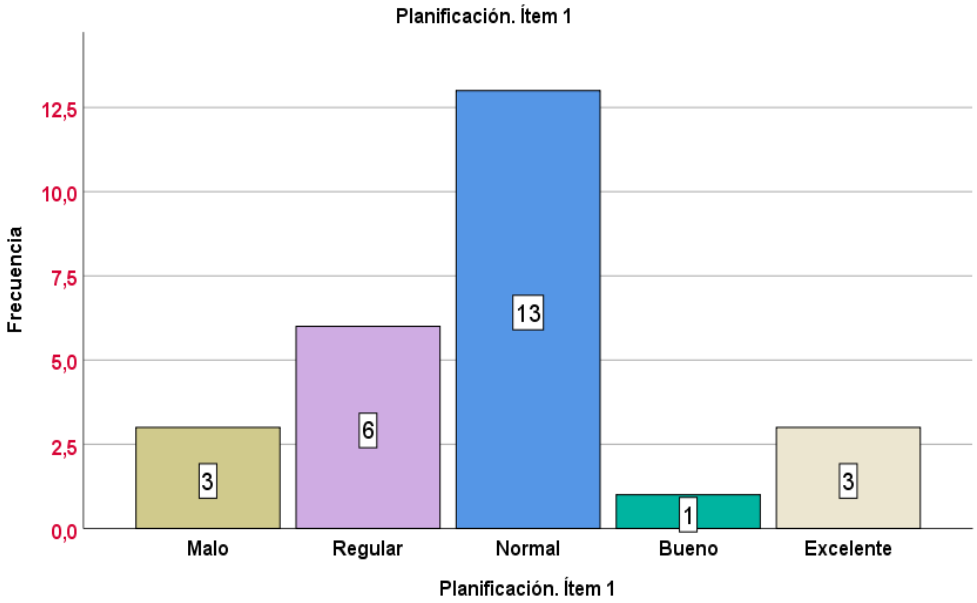
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	26,9	26,9	26,9
	Regular	4	15,4	15,4	42,3
	Normal	12	46,2	46,2	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 4 Diagnóstico de matriz de riesgos de la Auditoría informática basada en Ciclo de Vida ITIL v4 en la Caja Piura, Huaraz 2024, en el Ítem 4 de la dimensión Diagnostico, se observó que en 7 casos (26.9%) se encontraron en nivel malo, 9 casos (34.6%) se encontró en nivel regular, 12 casos (46.2%) se encontraron en nivel normal y, 3 casos (11.5%) se encontró en nivel excelente.

Planificación. Ítem 1

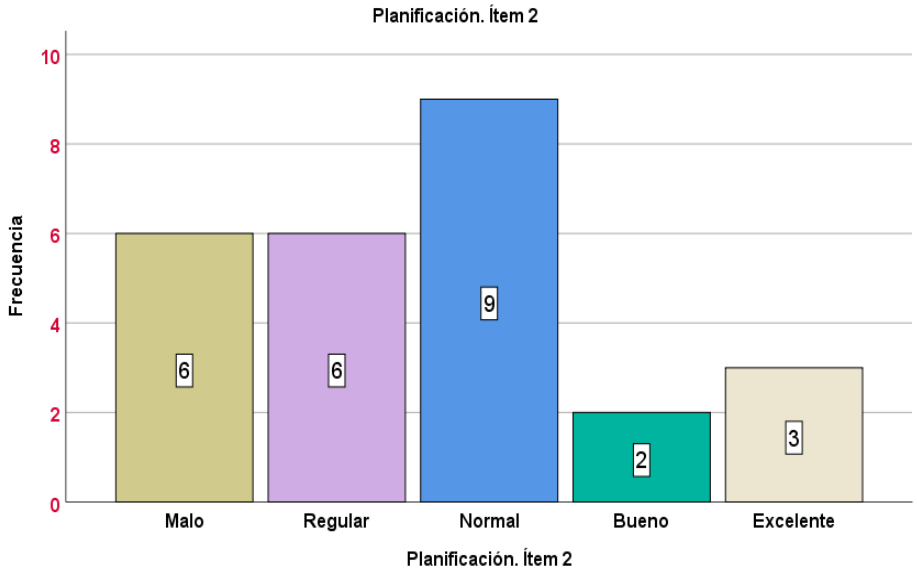
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	3	11,5	11,5	11,5
	Regular	6	23,1	23,1	34,6
	Normal	13	50,0	50,0	84,6
	Bueno	1	3,8	3,8	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 1 Planificación de la Auditoría informática basada en Ciclo de Vida ITIL v4 en la Caja Piura, Huaraz 2024, en el Ítem 1 de la dimensión Planificación, se observó que en 3 casos (11.5%) se encontraron en nivel malo, 6 casos (23.1%) se encontró en nivel regular, 13 casos (50.0%) se encontraron en nivel normal, 1 casos (3.8%) se encontraron en nivel bueno, y, 3 casos (11.5%) se encontró en nivel excelente.

Planificación. Ítem 2

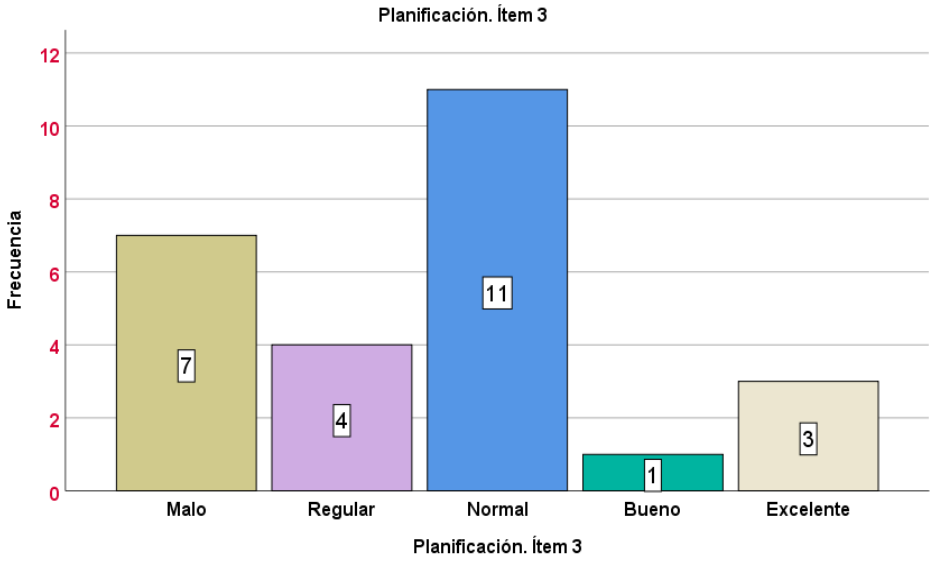
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	23,1	23,1	23,1
	Regular	6	23,1	23,1	46,2
	Normal	9	34,6	34,6	80,8
	Bueno	2	7,7	7,7	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 2 Planificación de los procesos a evaluar de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 2 de la dimensión Planificación, se observó que en 6 casos (23.1%) se encontraron en nivel malo, 6 casos (23.1%) se encontró en nivel regular, 9 casos (34.6%) se encontraron en nivel normal, 2 casos (7.7%) se encontraron en nivel bueno, y, 3 casos (11.5%) se encontró en nivel excelente.

Planificación. Ítem 3

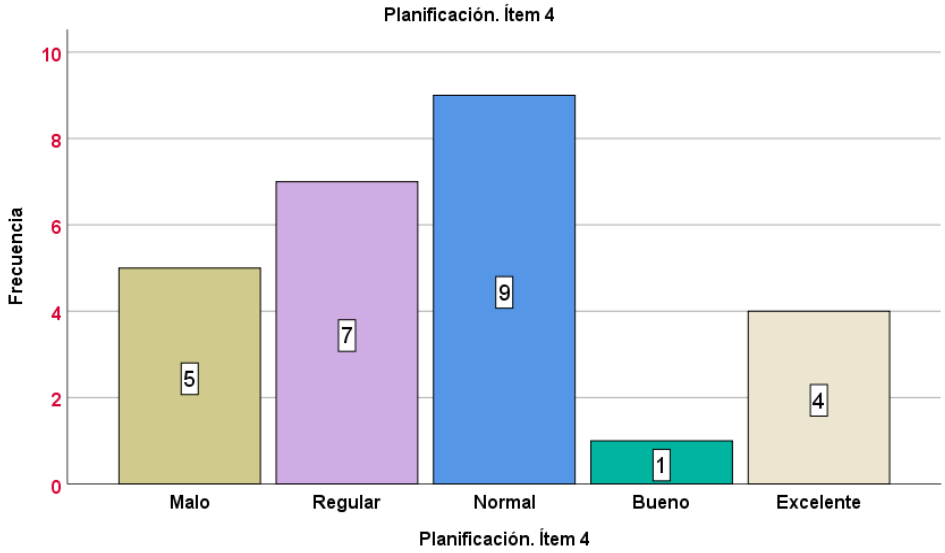
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	26,9	26,9	26,9
	Regular	4	15,4	15,4	42,3
	Normal	11	42,3	42,3	84,6
	Bueno	1	3,8	3,8	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 3 Planificación de las técnicas y herramientas de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 3 de la dimensión Planificación, se observó que en 7 casos (26.9%) se encontraron en nivel malo, 4 casos (15.4%) se encontró en nivel regular, 11 casos (42.3%) se encontraron en nivel normal, 1 casos (3.8%) se encontraron en nivel bueno, y, 3 casos (11.5%) se encontró en nivel excelente.

Planificación. Ítem 4

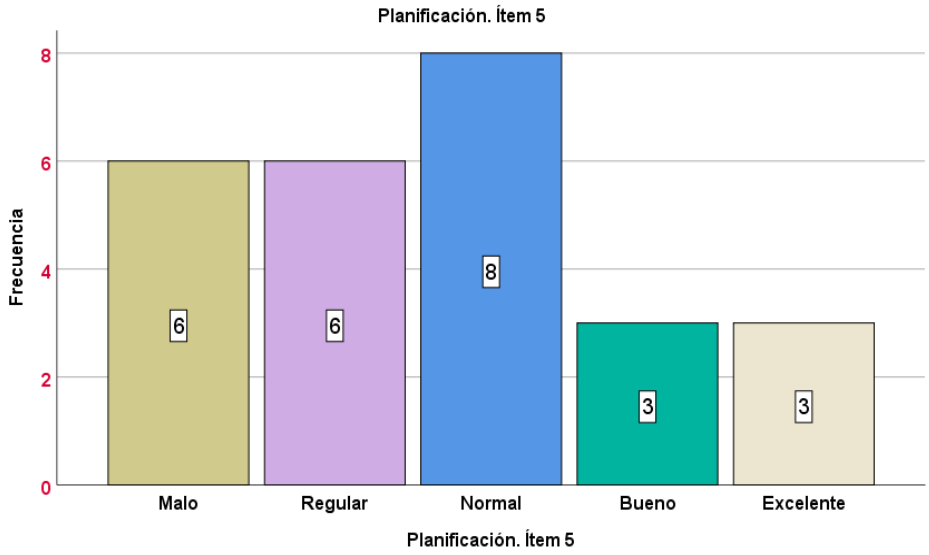
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	19,2	19,2	19,2
	Regular	7	26,9	26,9	46,2
	Normal	9	34,6	34,6	80,8
	Bueno	1	3,8	3,8	84,6
	Excelente	4	15,4	15,4	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 4 Planificación del equipo de trabajo de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 4 de la dimensión Planificación, se observó que en 5 casos (19.2%) se encontraron en nivel malo, 7 casos (26.9%) se encontró en nivel regular, 9 casos (34.6%) se encontraron en nivel normal, 1 casos (3.8%) se encontraron en nivel bueno, y, 4 casos (15.4%) se encontró en nivel excelente.

Planificación. Ítem 5

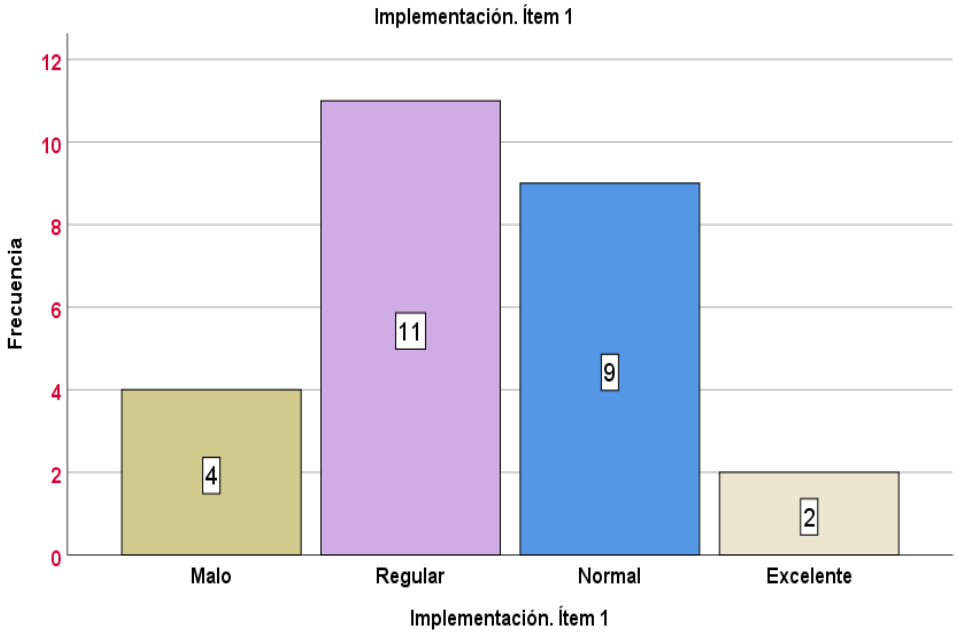
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	23,1	23,1	23,1
	Regular	6	23,1	23,1	46,2
	Normal	8	30,8	30,8	76,9
	Bueno	3	11,5	11,5	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 5 Planificación del presupuesto de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 5 de la dimensión Planificación, se observó que en 6 casos (23.1%) se encontraron en nivel malo, 6 casos (23.1%) se encontró en nivel regular, 8 casos (30.8%) se encontraron en nivel normal, 3 casos (11.5%) se encontraron en nivel bueno, y, 3 casos (11.5%) se encontró en nivel excelente.

Implementación. Ítem 1

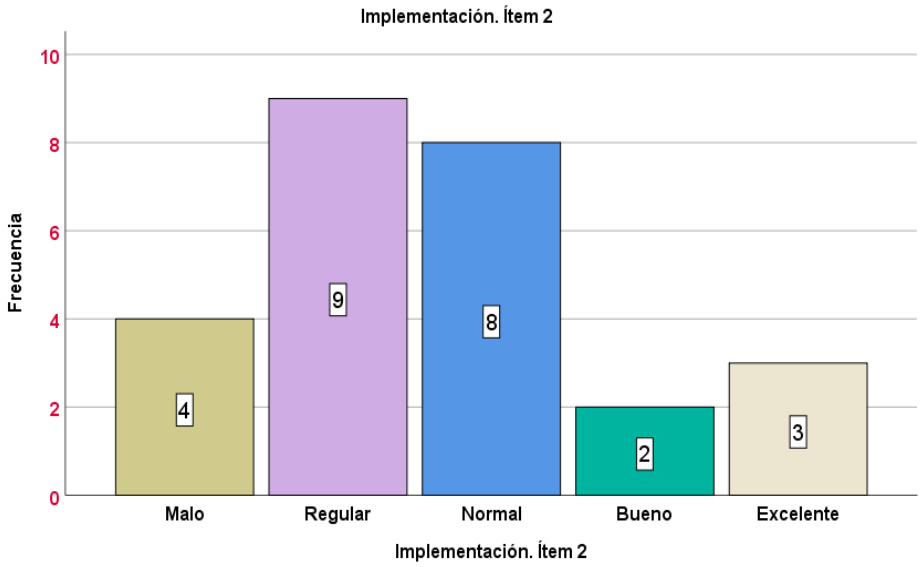
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	15,4	15,4	15,4
	Regular	11	42,3	42,3	57,7
	Normal	9	34,6	34,6	92,3
	Excelente	2	7,7	7,7	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 1 Implementación del análisis de procesos de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 1 de la dimensión Implementación, se observó que en 4 casos (15.4%) se encontraron en nivel malo, 11 casos (42.3%) se encontró en nivel regular, 9 casos (34.6%) se encontraron en nivel normal y, 2 casos (7.7%) se encontró en nivel excelente.

Implementación. Ítem 2

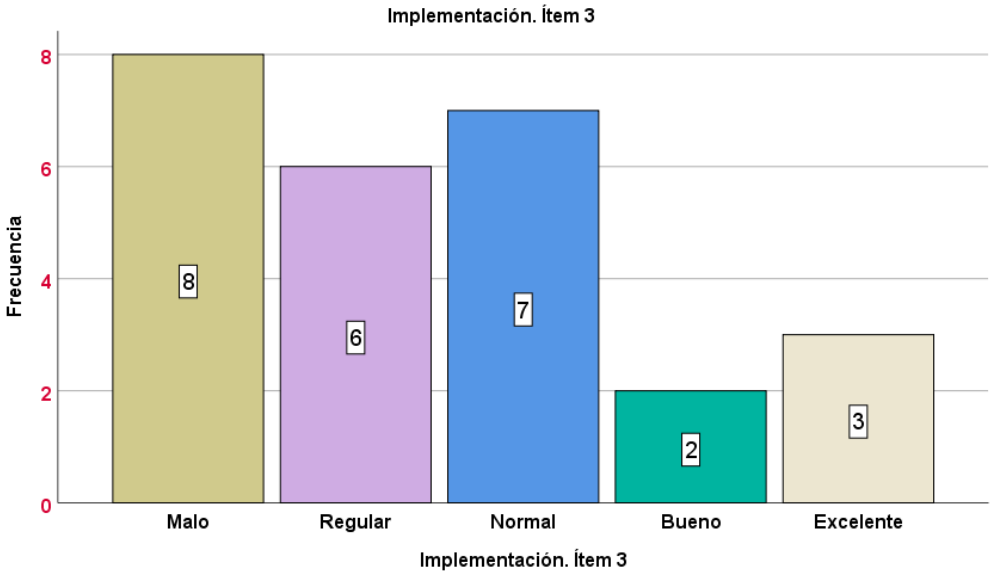
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	15,4	15,4	15,4
	Regular	9	34,6	34,6	50,0
	Normal	8	30,8	30,8	80,8
	Bueno	2	7,7	7,7	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 2 Implementación del análisis de riesgos de seguridad de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 2 de la dimensión Implementación, se observó que en 4 casos (15.4%) se encontraron en nivel malo, 9 casos (34.6%) se encontró en nivel regular, 8 casos (30.8%) se encontraron en nivel normal, 2 casos (7.7%) se encontraron en nivel bueno y, 3 casos (11.5%) se encontró en nivel excelente.

Implementación. Ítem 3

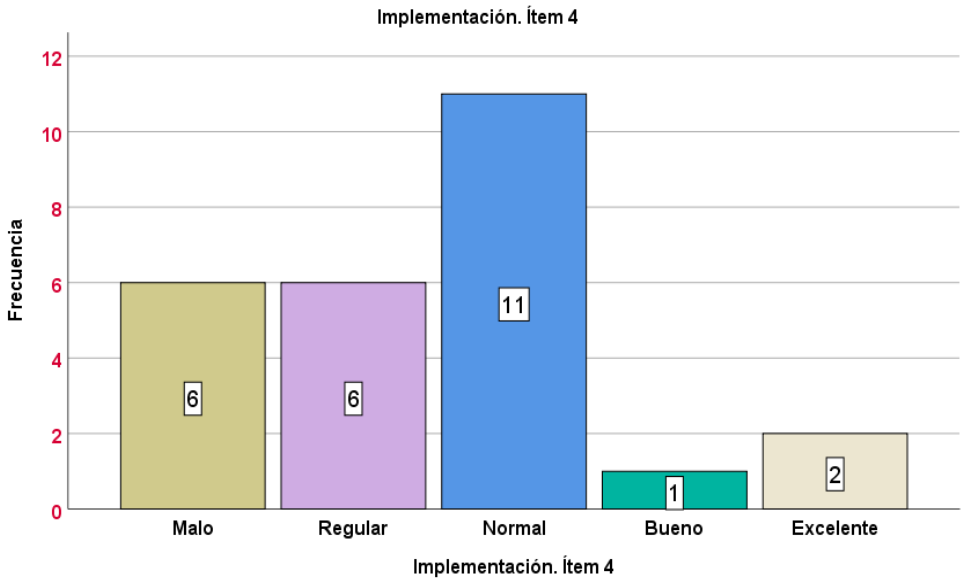
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	8	30,8	30,8	30,8
	Regular	6	23,1	23,1	53,8
	Normal	7	26,9	26,9	80,8
	Bueno	2	7,7	7,7	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 1 Implementación de evaluación de procesos y normas de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 3 de la dimensión Implementación, se observó que en 8 casos (30.8%) se encontraron en nivel malo, 6 casos (23.1%) se encontró en nivel regular, 7 casos (26.9%) se encontraron en nivel normal, 2 casos (7.7%) se encontraron en nivel bueno y, 3 casos (11.5%) se encontró en nivel excelente.

Implementación. Ítem 4

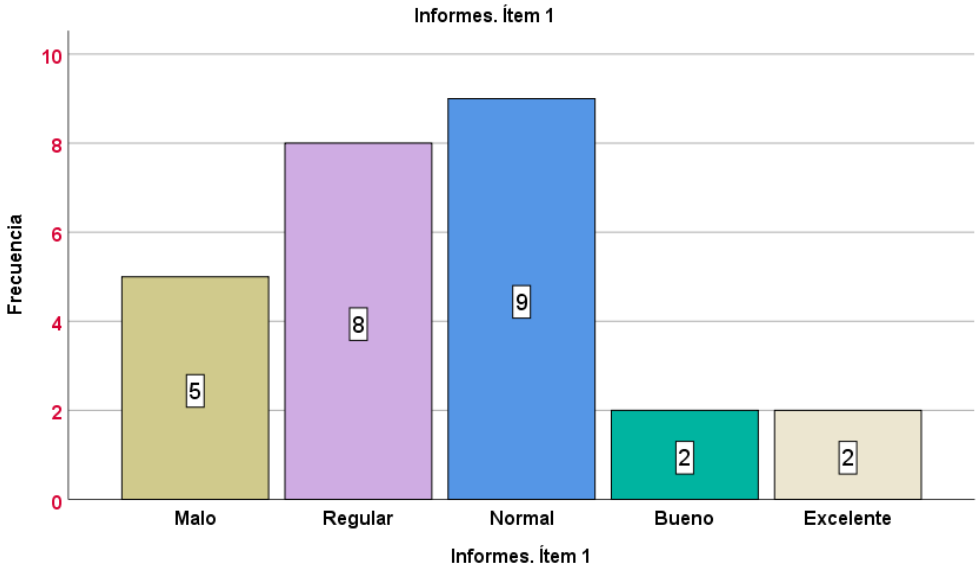
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	23,1	23,1	23,1
	Regular	6	23,1	23,1	46,2
	Normal	11	42,3	42,3	88,5
	Bueno	1	3,8	3,8	92,3
	Excelente	2	7,7	7,7	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 4 Implementación de los resultados de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 4 de la dimensión Implementación, se observó que en 6 casos (23.1%) se encontraron en nivel malo, 6 casos (23.1%) se encontró en nivel regular, 11 casos (42.3%) se encontraron en nivel normal, 1 casos (3.8%) se encontraron en nivel bueno y, 2 casos (7.7%) se encontró en nivel excelente.

Informes. Ítem 1

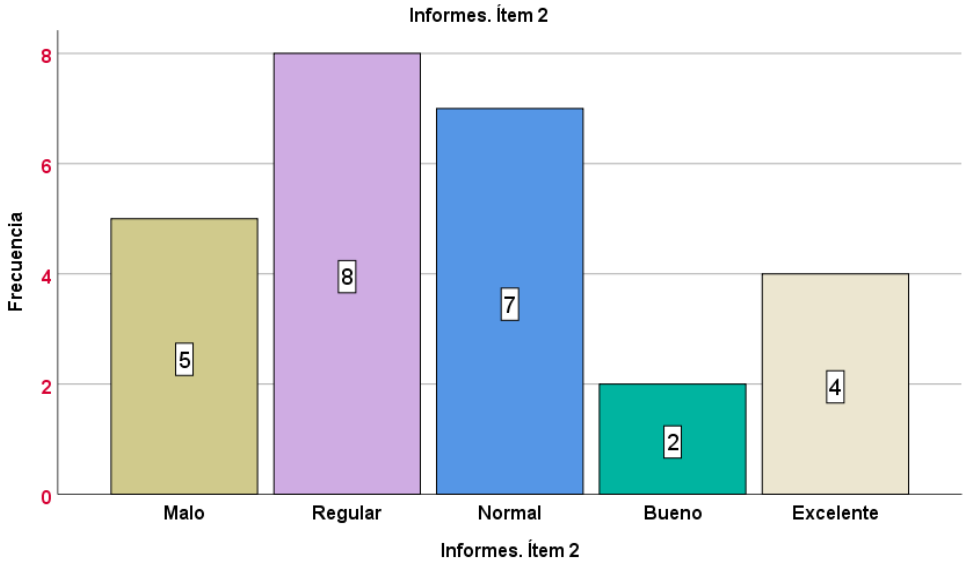
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	19,2	19,2	19,2
	Regular	8	30,8	30,8	50,0
	Normal	9	34,6	34,6	84,6
	Bueno	2	7,7	7,7	92,3
	Excelente	2	7,7	7,7	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 1 Presentación del informe de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 1 de la dimensión Informes, se observó que en 5 casos (19.2%) se encontraron en nivel malo, 8 casos (30.8%) se encontró en nivel regular, 9 casos (34.6%) se encontraron en nivel normal, 2 casos (7.7%) se encontraron en nivel bueno y, 2 casos (7.7%) se encontró en nivel excelente.

Informes. Ítem 2

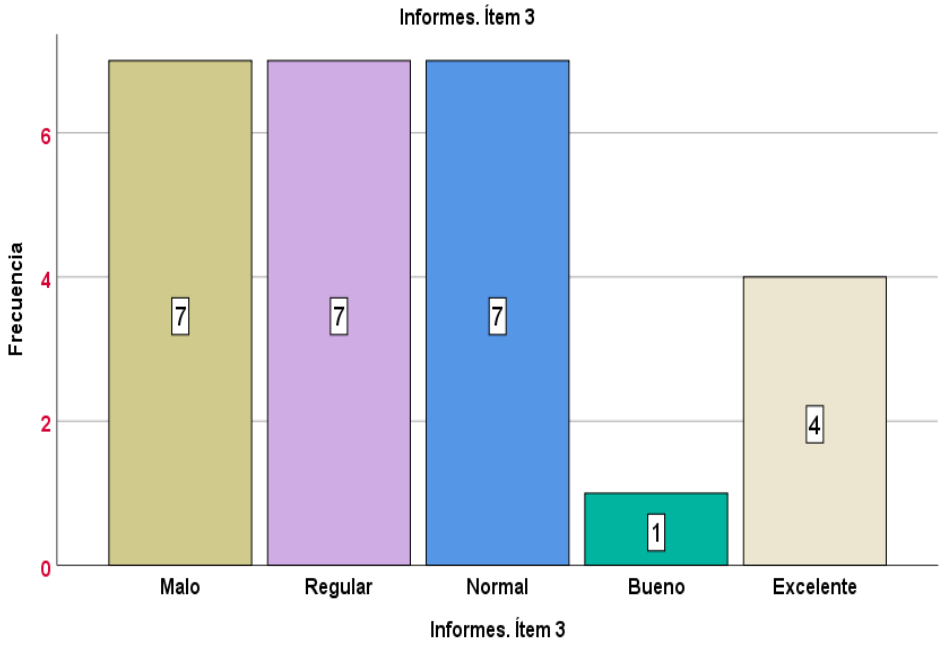
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	19,2	19,2	19,2
	Regular	8	30,8	30,8	50,0
	Normal	7	26,9	26,9	76,9
	Bueno	2	7,7	7,7	84,6
	Excelente	4	15,4	15,4	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 2 Recomendaciones del informe de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 2 de la dimensión Informes, se observó que en 5 casos (19.2%) se encontraron en nivel malo, 8 casos (30.8%) se encontró en nivel regular, 7 casos (26.9%) se encontraron en nivel normal, 2 casos (7.7%) se encontraron en nivel bueno y, 4 casos (15.4%) se encontró en nivel excelente.

Informes. Ítem 3

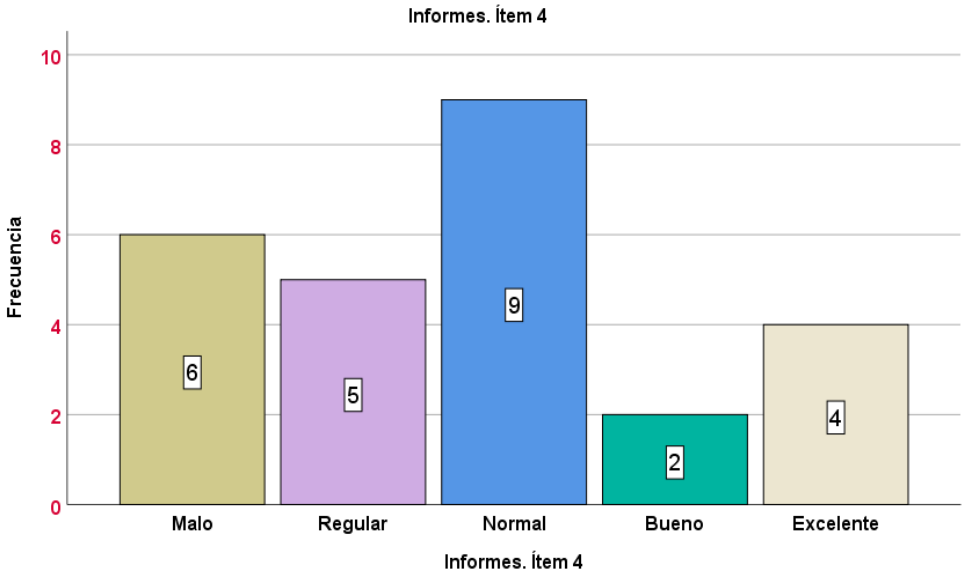
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	26,9	26,9	26,9
	Regular	7	26,9	26,9	53,8
	Normal	7	26,9	26,9	80,8
	Bueno	1	3,8	3,8	84,6
	Excelente	4	15,4	15,4	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 3 Toma de decisiones en los informes de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 3 de la dimensión Informes, se observó que en 7 casos (26.9%) se encontraron en nivel malo, 7 casos (26.9%) se encontró en nivel regular, 7 casos (26.9%) se encontraron en nivel normal, 1 caso (3.8%) se encontraron en nivel bueno y, 4 casos (15.4%) se encontró en nivel excelente.

Informes. Ítem 4

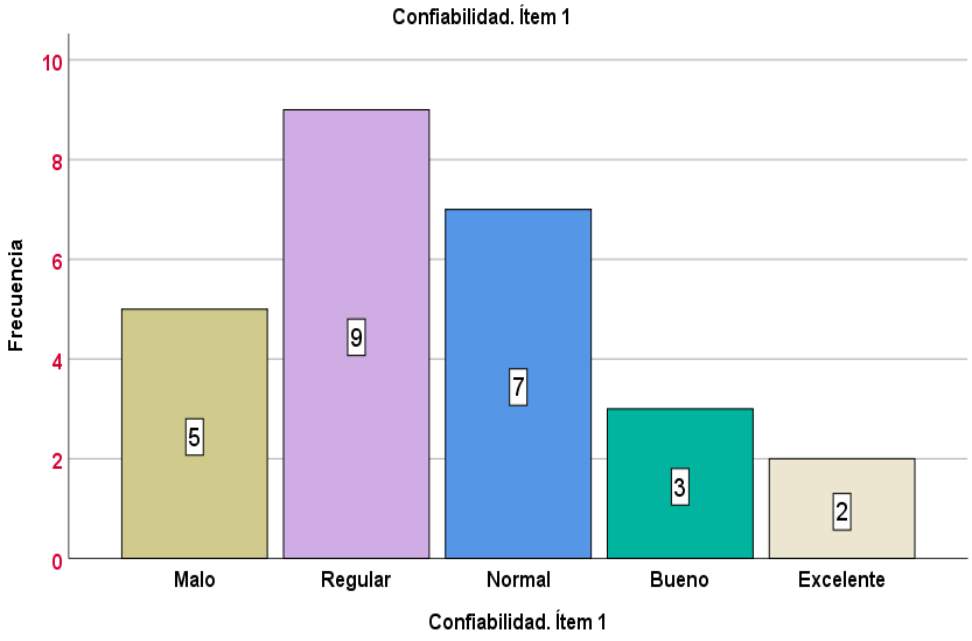
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	23,1	23,1	23,1
	Regular	5	19,2	19,2	42,3
	Normal	9	34,6	34,6	76,9
	Bueno	2	7,7	7,7	84,6
	Excelente	4	15,4	15,4	100,0
	Total	26	100,0	100,0	



Con referencia a la variable auditoría informática basada en ITIL v4, en la pregunta 4 Cambios realizados en los informes de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 4 de la dimensión Informes, se observó que en 6 casos (23.1%) se encontraron en nivel malo, 5 casos (19.2%) se encontró en nivel regular, 9 casos (34.6%) se encontraron en nivel normal, 2 caso (7.7%) se encontraron en nivel bueno y, 4 casos (15.4%) se encontró en nivel excelente.

Confiabilidad. Ítem 1

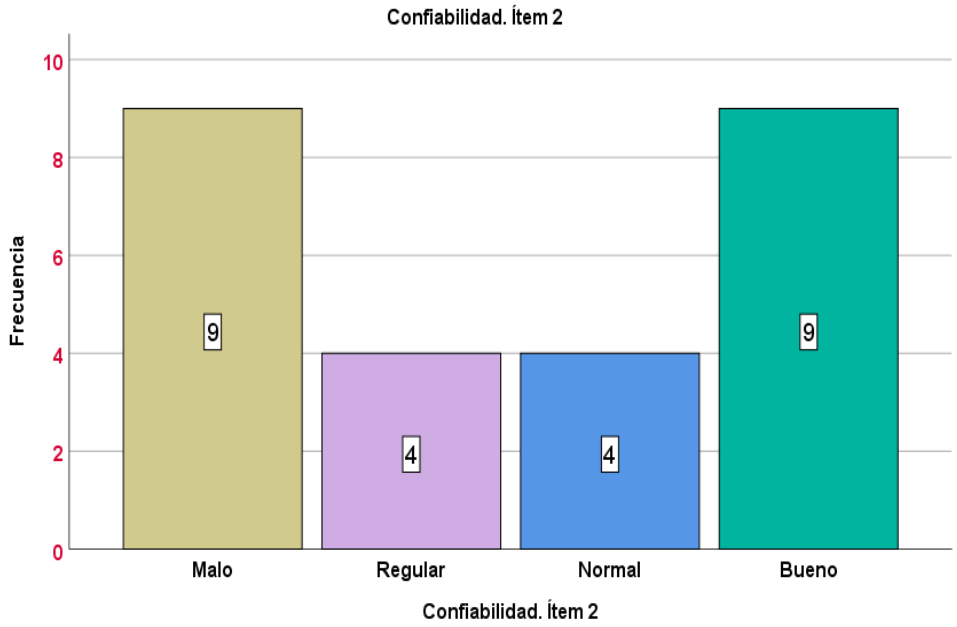
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	19,2	19,2	19,2
	Regular	9	34,6	34,6	53,8
	Normal	7	26,9	26,9	80,8
	Bueno	3	11,5	11,5	92,3
	Excelente	2	7,7	7,7	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 1 Confiabilidad de archivos de gerencia respecto a seguridad de la información en la Caja Piura, Huaraz 2024, en el Ítem 1 de la dimensión Confiabilidad, se observó que en 5 casos (19.2%) se encontraron en nivel malo, 9 casos (34.6%) se encontró en nivel regular, 7 casos (26.9%) se encontraron en nivel normal, 3 caso (11.5%) se encontraron en nivel bueno y, 2 casos (7.7%) se encontró en nivel excelente.

Confiabilidad. Ítem 2

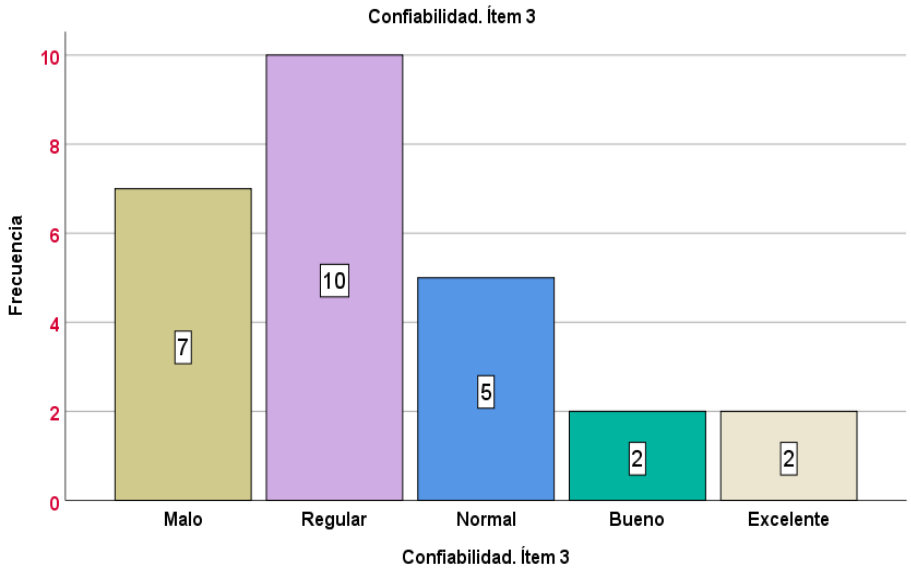
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	34,6	34,6	34,6
	Regular	4	15,4	15,4	50,0
	Normal	4	15,4	15,4	65,4
	Bueno	9	34,6	34,6	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 2 Confiabilidad de archivos de créditos sobre seguridad de la información en la Caja Piura, Huaraz 2024, en el Ítem 2 de la dimensión Confiabilidad, se observó que en 9 casos (34.6%) se encontraron en nivel malo, 4 casos (15.4%) se encontró en nivel regular, 4 casos (15.4%) se encontraron en nivel normal y 9 casos (34.6%) se encontró en nivel excelente.

Confiabilidad. Ítem 3

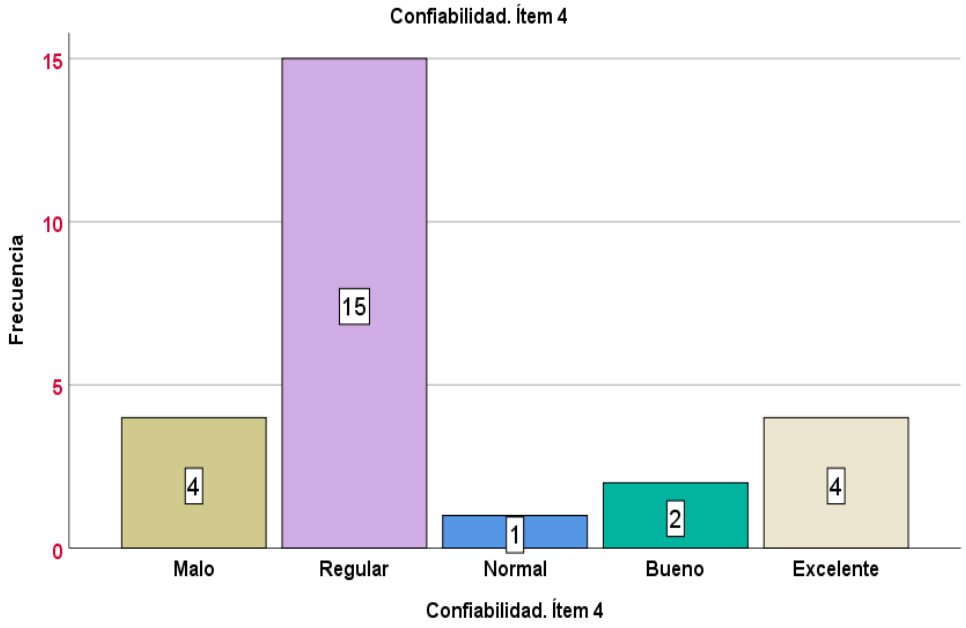
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	26,9	26,9	26,9
	Regular	10	38,5	38,5	65,4
	Normal	5	19,2	19,2	84,6
	Bueno	2	7,7	7,7	92,3
	Excelente	2	7,7	7,7	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 3 Confiabilidad de archivos de ahorros sobre seguridad de la información en la Caja Piura, Huaraz 2024, en el Ítem 3 de la dimensión Confiabilidad, se observó que en 7 casos (26.9%) se encontraron en nivel malo, 10 casos (38.5%) se encontró en nivel regular, 5 casos (19.2%) se encontraron en nivel normal, 2 caso (7.7%) se encontraron en nivel bueno y, 2 casos (7.7%) se encontró en nivel excelente.

Confiabilidad. Ítem 4

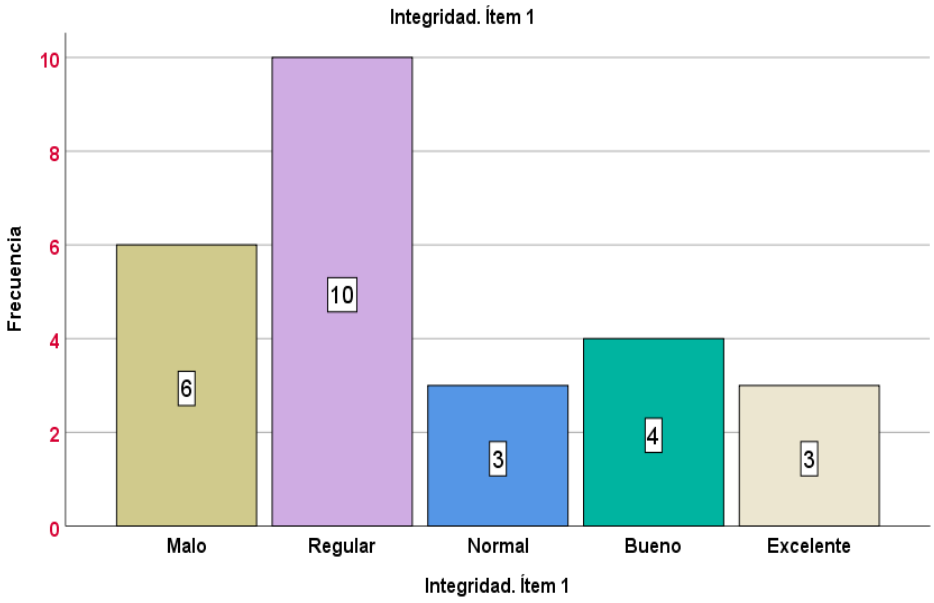
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	15,4	15,4	15,4
	Regular	15	57,7	57,7	73,1
	Normal	1	3,8	3,8	76,9
	Bueno	2	7,7	7,7	84,6
	Excelente	4	15,4	15,4	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 4 Confiabilidad de archivos en general respecto a seguridad de la información en la Caja Piura, Huaraz 2024, en el Ítem 4 de la dimensión Confiabilidad, se observó que en 4 casos (15.4%) se encontraron en nivel malo, 15 casos (57.7%) se encontró en nivel regular, 1 casos (3.8%) se encontraron en nivel normal, 2 caso (7.7%) se encontraron en nivel bueno y, 4 casos (15.4%) se encontró en nivel excelente.

Integridad. Ítem 1

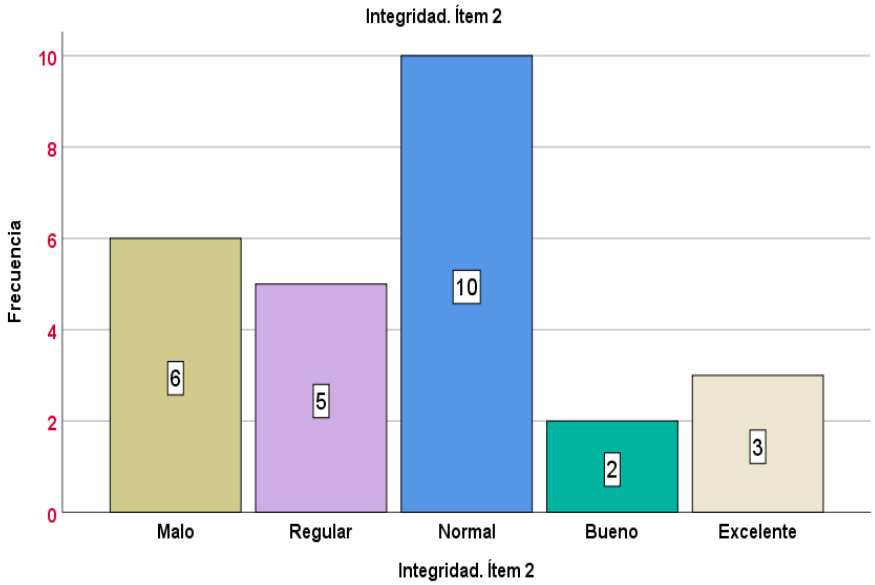
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	23,1	23,1	23,1
	Regular	10	38,5	38,5	61,5
	Normal	3	11,5	11,5	73,1
	Bueno	4	15,4	15,4	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 1 Integridad de archivos de gerencia respecto a seguridad de la información en la Caja Piura, Huaraz 2024, en el Ítem 1 de la dimensión Integridad, se observó que en 6 casos (23.1%) se encontraron en nivel malo, 10 casos (38.5%) se encontró en nivel regular, 3 casos (11.5%) se encontraron en nivel normal, 4 caso (15.4%) se encontraron en nivel bueno y, 3 casos (11.5%) se encontró en nivel excelente.

Integridad. Ítem 2

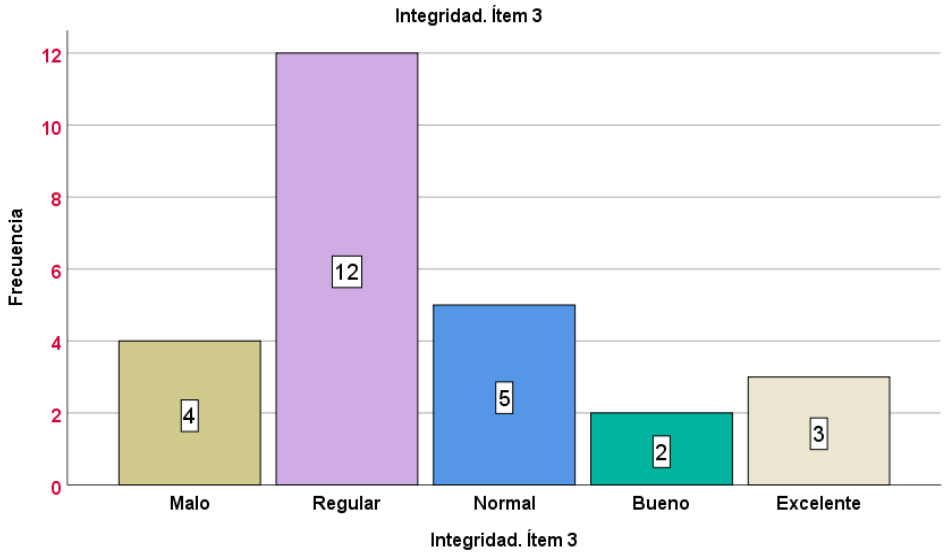
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	23,1	23,1	23,1
	Regular	5	19,2	19,2	42,3
	Normal	10	38,5	38,5	80,8
	Bueno	2	7,7	7,7	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 2 Integridad de archivos de créditos sobre seguridad de la información en la Caja Piura, Huaraz 2024, en el Ítem 2 de la dimensión Integridad, se observó que en 6 casos (23.1%) se encontraron en nivel malo, 5 casos (19.2%) se encontró en nivel regular, 10 casos (38.5%) se encontraron en nivel normal, 2 caso (7.7%) se encontraron en nivel bueno y, 3 casos (11.5%) se encontró en nivel excelente.

Integridad. Ítem 3

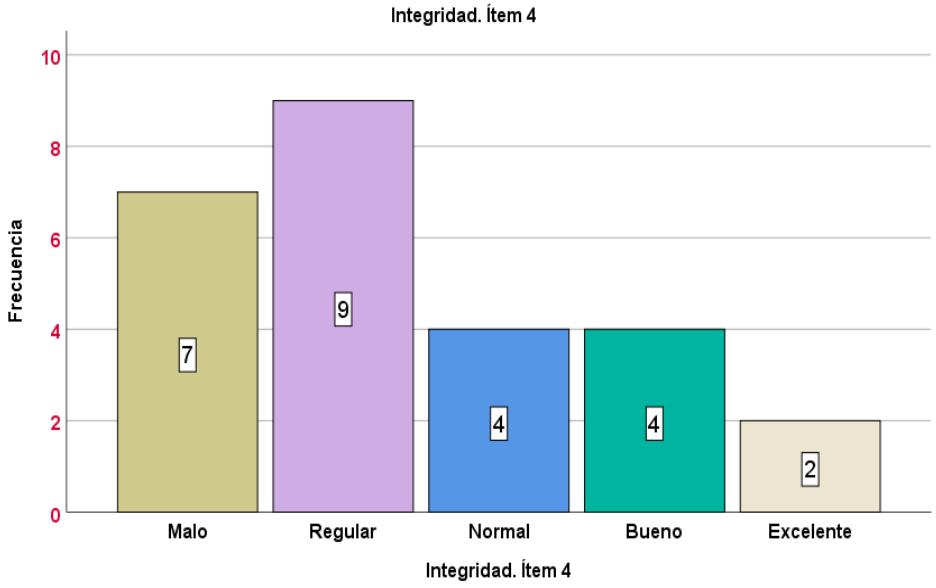
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	15,4	15,4	15,4
	Regular	12	46,2	46,2	61,5
	Normal	5	19,2	19,2	80,8
	Bueno	2	7,7	7,7	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 3 Integridad de archivos de ahorros sobre seguridad de la información en la Caja Piura, Huaraz 2024, en el Ítem 3 de la dimensión Integridad, se observó que en 4 casos (15.4%) se encontraron en nivel malo, 12 casos (46.2%) se encontró en nivel regular, 5 casos (19.2%) se encontraron en nivel normal, 2 caso (7.7%) se encontraron en nivel bueno y, 3 casos (11.5%) se encontró en nivel excelente.

Integridad. Ítem 4

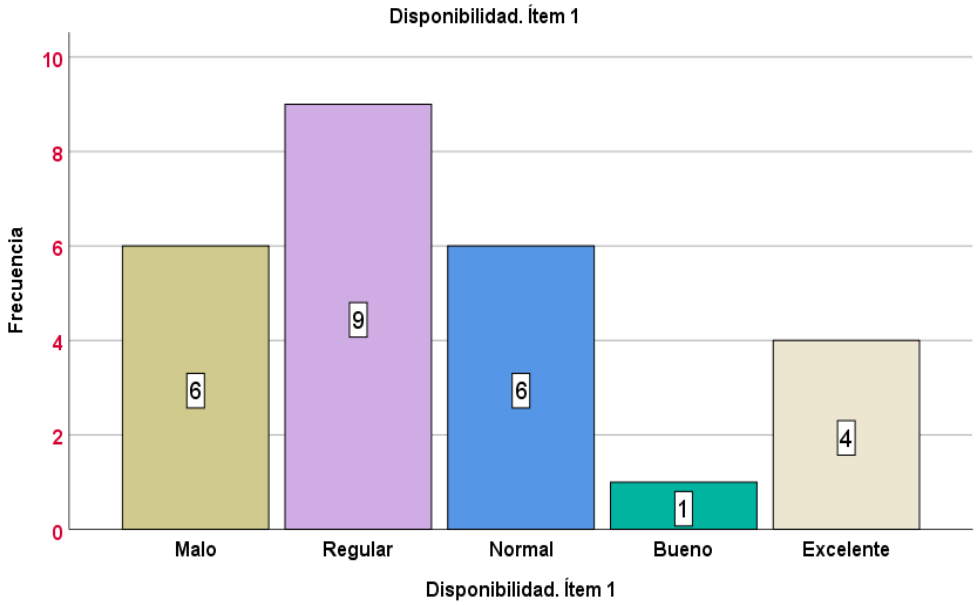
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	7	26,9	26,9	26,9
	Regular	9	34,6	34,6	61,5
	Normal	4	15,4	15,4	76,9
	Bueno	4	15,4	15,4	92,3
	Excelente	2	7,7	7,7	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 4 Integridad de archivos en general respecto a seguridad de la información en la Caja Piura, Huaraz 2024, en el Ítem 4 de la dimensión Integridad, se observó que en 7 casos (26.9%) se encontraron en nivel malo, 9 casos (34.6%) se encontró en nivel regular, 4 casos (15.4%) se encontraron en nivel normal, 4 caso (15.4%) se encontraron en nivel bueno y, 2 casos (7.7%) se encontró en nivel excelente.

Disponibilidad. Ítem 1

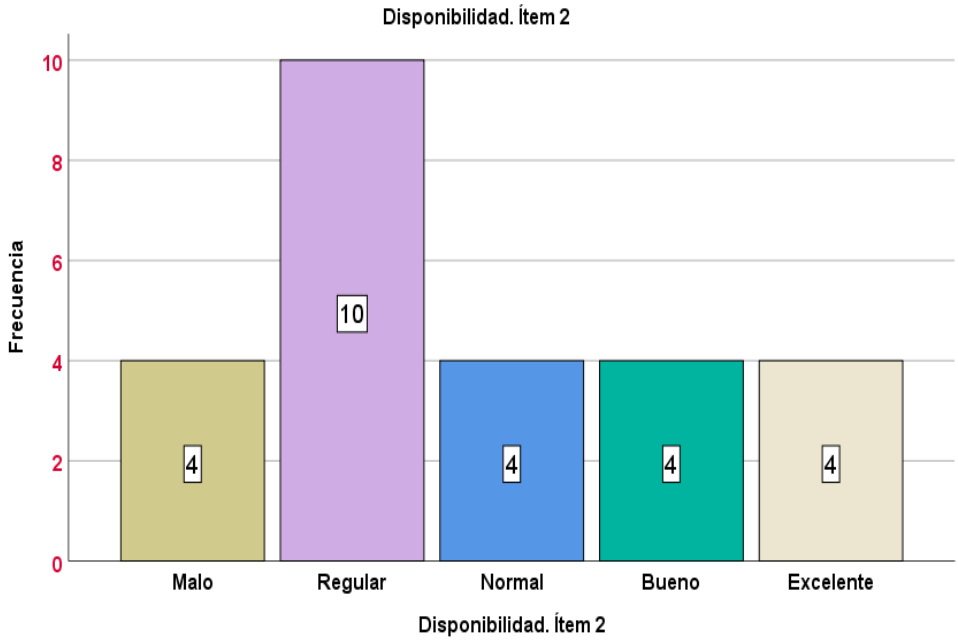
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	23,1	23,1	23,1
	Regular	9	34,6	34,6	57,7
	Normal	6	23,1	23,1	80,8
	Bueno	1	3,8	3,8	84,6
	Excelente	4	15,4	15,4	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 1 Disponibilidad de archivos de gerencia de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 1 de la dimensión Disponibilidad, se observó que en 6 casos (23.1%) se encontraron en nivel malo, 9 casos (34.6%) se encontró en nivel regular, 6 casos (23.1%) se encontraron en nivel normal, 1 caso (3.8%) se encontraron en nivel bueno y, 4 casos (15.4%) se encontró en nivel excelente.

Disponibilidad. Ítem 2

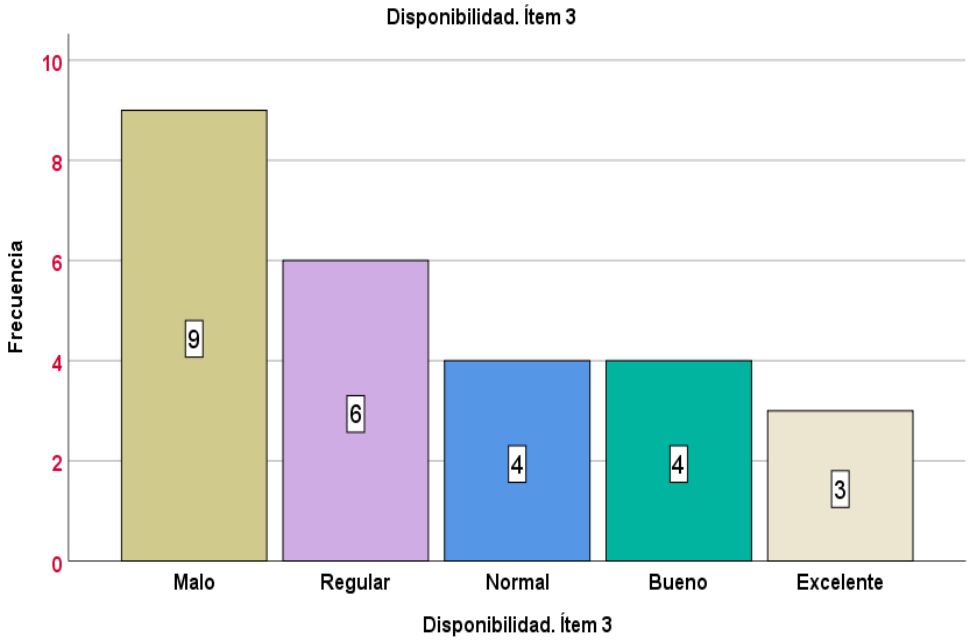
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	15,4	15,4	15,4
	Regular	10	38,5	38,5	53,8
	Normal	4	15,4	15,4	69,2
	Bueno	4	15,4	15,4	84,6
	Excelente	4	15,4	15,4	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 2 Disponibilidad de archivos de créditos de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 2 de la dimensión Disponibilidad, se observó que en 4 casos (15.4%) se encontraron en nivel malo, 10 casos (38.5%) se encontró en nivel regular, 4 casos (15.4%) se encontraron en nivel normal, 4 caso (15.4%) se encontraron en nivel bueno y, 4 casos (15.4%) se encontró en nivel excelente.

Disponibilidad. Ítem 3

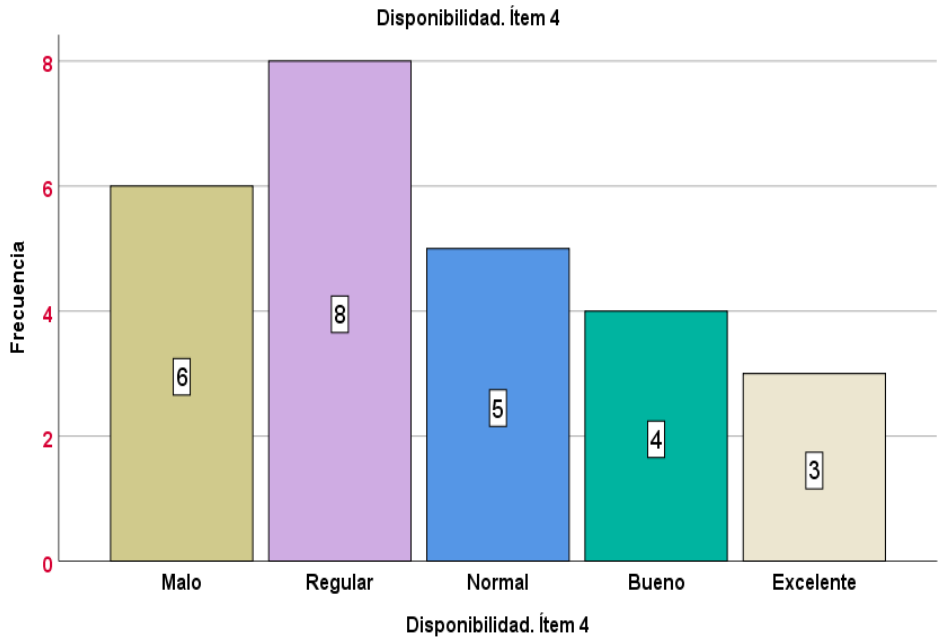
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	34,6	34,6	34,6
	Regular	6	23,1	23,1	57,7
	Normal	4	15,4	15,4	73,1
	Bueno	4	15,4	15,4	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 3 Disponibilidad de archivos de ahorros de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 3 de la dimensión Disponibilidad, se observó que en 9 casos (34.6%) se encontraron en nivel malo, 6 casos (23.1%) se encontró en nivel regular, 4 casos (15.4%) se encontraron en nivel normal, 4 caso (15.4%) se encontraron en nivel bueno y, 3 casos (11.5%) se encontró en nivel excelente.

Disponibilidad. Ítem 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	23,1	23,1	23,1
	Regular	8	30,8	30,8	53,8
	Normal	5	19,2	19,2	73,1
	Bueno	4	15,4	15,4	88,5
	Excelente	3	11,5	11,5	100,0
	Total	26	100,0	100,0	



Con referencia a la variable seguridad de la información, en la pregunta 4 Disponibilidad de archivos en general de la Auditoría informática basada en Ciclo de Vida ITIL v4, en el Ítem 4 de la dimensión Disponibilidad, se observó que en 6 casos (23.1%) se encontraron en nivel malo, 8 casos (30.8%) se encontró en nivel regular, 5 casos (19.2%) se encontraron en nivel normal, 4 caso (15.4%) se encontraron en nivel bueno y, 3 casos (11.5%) se encontró en nivel excelente.

Anexo 8: Formato de publicación en repositorio institucional

USP
UNIVERSIDAD SAN PEDRO

REPOSITORIO INSTITUCIONAL DIGITAL

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE DOCUMENTOS DE INVESTIGACIÓN

1. Información del Autor		
RAMIREZ VIDAL MICHELL	46307175	michrvm@gmail.com
Apellidos y Nombres	DNI	Correo Electrónico

2. Tipo de Documento de Investigación							
X	Tesis		Trabajo de Suficiencia Profesional		Trabajo Académico		Trabajo de Investigación

3. Grado Académico o Título Profesional [1]									
	Bachiller	X	Título Profesional		Título Segunda Especialidad		Maestría		Doctorado

4. Título del Documento de Investigación
Auditoría informática basada en Ciclo de Vida ITIL v4 y seguridad de la información en la Caja Piura, Huaraz 2024

5. Programa Académico
Ingeniería Informatica y de Sistemas

6. Tipo de Acceso al Documento			
X	Abierto o Público [3] (info:eu-repo/semantics/openAccess)		Acceso restringido [4] (info:eu-repo/semantics/restrictedAccess)(*)
	Embargo (Máximo 24 meses) (info:eu-repo/semantics/embargoedAccess)	Fecha de Liberación de embargo: ____ / ____ / ____ (Formato: día / mes / año)	
(*) En caso de restringido y embargo sustentar motivo			

A. Originalidad del Archivo Digital

Por el presente dejo constancia que el archivo digital que entrego a la Universidad, es la versión final del trabajo de investigación sustentado y aprobado por el Jurado Evaluador y forma parte del proceso que conduce a obtener el grado académico o título profesional.

B. Otorgamiento de una licencia CREATIVE COMMONS [5]

El autor, por medio de este documento, autoriza a la Universidad, publicar su trabajo de investigación en formato digital en el Repositorio Institucional Digital, al cual se podrá acceder, preservar y difundir de forma libre y gratuita, de manera integra a todo el documento. [6]

Ciudad	Día	Mes	Año
HUARAZ	06	06	2025

Huella Digital

Firma

Importante

1. Según Resolución de Consejo Directivo N° 033-2016-SUNEDU-CD, Reglamento del Registro Nacional de Trabajos de investigación para optar Grados Académicos y Títulos Profesionales, Art. 8, inciso 8.2.
2. Ley N° 30035. Ley que regula el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto y D.S. 006 -2015-PCM.
3. Si el autor eligió el tipo de acceso abierto o público, otorga a la Universidad San Pedro una licencia no exclusiva, para que se pueda hacer arreglos de forma en la obra y difundir en el Repositorio Institucional Digital. Respetando siempre los Derechos de Autor y Propiedad Intelectual de acuerdo y en el Marco de la Ley 822.
4. En caso de que el autor elija la segunda opción, únicamente se publicará los datos del autor y resumen de la obra de acuerdo a la directiva N° 004-2016-CUNCYTEC-DIDC (Numerales 5.2 y 6.7) que norma el funcionamiento del Repositorio Nacional Digital.
5. Las licencias Creative Commons (CC) es una organización internacional sin fines de lucro que pone a disposición de los autores un conjunto de licencias flexibles y de herramientas tecnológicas que facilitan la difusión de información, recursos educativos, obras artísticas y científicas, entre otros. Estas licencias también garantizan que el autor obtenga el crédito por su obra.
6. Según el inciso 12.2, del artículo 12° del Reglamento del Registro Nacional de Trabajos de investigación para optar grados académicos y títulos profesionales-RENATI "Las universidades, instituciones y escuelas de educación superior tienen como obligación registrar todos los trabajos de investigación y proyectos, incluyendo los metadatos en sus repositorios institucionales precisando si son de acceso abierto o restringido, los cuales serán posteriormente recolectados por el Repositorio Digital RENATI, a través del Repositorio ALICIA".

Nota - En caso de falsedad en los datos, se procederá de acuerdo a ley (Ley 27444, art. 32, núm. 32.3).

Anexo 9: Reporte de similitud

Auditoría informática basada en Ciclo de Vida ITIL v4 y seguridad de la información en la Caja Piura, Huaraz 2024

INFORME DE ORIGINALIDAD

20%	20%	2%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	8%
2	repositorio.ucv.edu.pe Fuente de Internet	2%
3	redi.unjbg.edu.pe Fuente de Internet	1%
4	repositorio.utn.edu.ec Fuente de Internet	1%
5	repositorio.usanpedro.edu.pe Fuente de Internet	1%
6	repositorio.espe.edu.ec Fuente de Internet	1%
7	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
8	dspace.unach.edu.ec Fuente de Internet	1%
9	editorialalema.org Fuente de Internet	

		<1 %
10	repositorio.uladech.edu.pe Fuente de Internet	<1 %
11	repositorio.upla.edu.pe Fuente de Internet	<1 %
12	Submitted to Universidad Privada San Pedro Trabajo del estudiante	<1 %
13	www.monografias.com Fuente de Internet	<1 %
14	www.hacienda.go.cr Fuente de Internet	<1 %
15	Submitted to Pontificia Universidad Catolica del Peru Trabajo del estudiante	<1 %
16	prezi.com Fuente de Internet	<1 %
17	alarcos.inf-cr.uclm.es Fuente de Internet	<1 %
18	www.estrategia.gobiernoenlinea.gov.co Fuente de Internet	<1 %
19	1library.co Fuente de Internet	<1 %
20	contadores-aic.org Fuente de Internet	

		<1 %
21	repositorio.uleam.edu.ec Fuente de Internet	<1 %
22	worldwidescience.org Fuente de Internet	<1 %
23	novascientia.delasalle.edu.mx Fuente de Internet	<1 %
24	repositorio.unesum.edu.ec Fuente de Internet	<1 %
25	pinpdf.com Fuente de Internet	<1 %
26	repositorio.upci.edu.pe Fuente de Internet	<1 %
27	blogs.imf-formacion.com Fuente de Internet	<1 %
28	cpl.thalesgroup.com Fuente de Internet	<1 %
29	www.captic.com Fuente de Internet	<1 %
30	www.sisbi.uba.ar Fuente de Internet	<1 %
31	dergipark.org.tr Fuente de Internet	<1 %

32	pt.scribd.com Fuente de Internet	<1 %
33	repositorio.uns.edu.pe Fuente de Internet	<1 %
34	servicios.fpune.edu.py:83 Fuente de Internet	<1 %
35	technologyrain.com.ar Fuente de Internet	<1 %
36	www.3ciencias.com Fuente de Internet	<1 %

Excluir citas	Apagado	Excluir coincidencias	< 10 words
Excluir bibliografía	Activo		