UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Tesis

Gestión del conocimiento y la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024

Asesor:

Dr. Baptista Velásquez, Adolfo Rafael

Autor:

Delgado Choquetaype, Ever

Para optar el título profesional de:

Ingeniero de Sistemas e Informática

Abancay- Apurímac - Perú

2025

Acta de sustentación

Universidad Tecnológica de los Andes

Transformando vidas

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE SUSTENTACIÓN DE TÍTULO PROFESIONAL Acta N°:001-2026

En la ciudad de **Abancay,** a los **21** días del mes de **noviembre** del 2025, siendo las **11:00** horas, se reunieron los integrantes del Jurado designado por Resolución Directoral **N° 062-2025-UTEA-FI-EPIS,** de la Escuela Profesional de **Ingeniería de Sistemas e Informática,** Facultad de **Ingeniería.**

Presidente:	Mg. Tintaya Zegarra Elvio
Dictaminante:	Mg. Chávez Vásquez Eduardo
Replicante:	Mg. Soria Donaires Fredy

Para evaluar la sustentación, en la modalidad de:

(X) Tesis ( ) Trabajo de suficiencia profesional

Titulado:

Campus de enseñanza virtual y las competencias de los docentes de la facultad de ingeniería de la Universidad Tecnológica de los Andes, Abancay - Apurímac 2024

Desarrollado por el (la) Bachiller:

Br. Delgado Choquetaype Ever

(Apellidos y Nombres)

Para optar el Título Profesional de:

Ingeniero de Sistemas e Informática

(Denominación del Título)

Concluido el acto, el Jurado dictaminó que el (la) mencionado(a) bachiller fue:
APROBADO(S) (X)

Por: **Unanimidad**

Emitiéndose la calificación final de:

Bachiller (Apellidos y Nombres)	**Calificación (**)**
Delgado Choquetaype Ever	Aprobado Notable

Siendo las **12:00** horas concluyó la sesión, firmando los integrantes del Jurado.

Presidente: Mg. Tintaya Zegarra Elvio — Firma

Dictaminante: Mg. Chávez Vásquez Eduardo — Firma

Replicante: Mg. Soria Donaires Fredy — Firma

(*): Mayoría: Dos Integrantes del Jurado aprueban o desaprueban; Unanimidad: Todos los integrantes del jurado aprueban y desaprueban
(**): 0 a 10: Desaprobado, 11 a 15: Aprobado, 16 a 18: Aprobado Notable, 19 y 20: Aprobado con Distinción, Art. A8 RGGAT.

Reporte de similitud

24% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 9 palabras)

Fuentes principales

20% Fuentes de Internet
5% Publicaciones
21% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Metadatos

Datos de los Autores		
Apellidos y Nombres	:	Br. Delgado Choquetaype, Ever
Tipo de Documento de Identidad	:	71692058
URL ORCID	:	------
Datos del asesor		
Apellidos y Nombres	:	Dr. Baptista Velásquez, Adolfo Rafael
Tipo de documento de Identidad	:	DNI
Numero de Documento de Identidad	:	45970028
URL ORCID	:	https://orcid.org/0000-0002-0475-0867
Datos de la Investigación		
Facultad	:	Ingeniería
Escuela Profesional	:	Ingeniería de Sistemas e Informática
Línea de Investigación	:	Informática, sociedad y gestión de conocimiento.
Rango de años en que se realizó la investigación	:	De noviembre de 2024 y finalizó en marzo de 2025.
Fuente de financiamiento	:	Financiado por el tesista
Porcentaje de similitud	:	24%
URL de OCDE	:	https://purl.org/pe-repo/ocde/ford # 2.02.04

Dedicatoria

A Dios, por ser el inspiro y darme fuerza para continuar con el proceso de obtener uno de los anhelos más deseados.

A mis padres por su amor, trabajo y sacrifico en todo este año gracia a ellos pude cumplir mis sueños de ser un gran profesional.

También a mi dulce princesa que es mi hija el motor y motivo de seguir adelante, mi princesita Itzel Yarucxi Delgado Chancahuaña.

Agradecimientos

Con profundo cariño y reconocimiento, extiendo mis más sinceros agradecimientos a mi asesor de tesis al Dr. Adolfo Rafael Baptista Velásquez quien con mucho cariño y paciencia me apoyo para el desarrollo de la presente investigación para así poder cumplir con mis sueños de optar mi título profesional de ingeniero de sistemas e informática.

Como también a todos mis familiares por haberme apoyado y acompañado en este proceso tan importante para mi formación profesional.

Resumen

El objetivo del estudio se basó en “establecer el nivel de asociación de la gestión del conocimiento con la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024”.

Considerando una metodología cuantitativa, tipo básica, correlacional y no experimental de corte transversal; siendo la población y muestra de 43 unidades de análisis establecida por el método no probabilístico, aplicando la encuesta y el cuestionario como técnica e instrumento respectivamente. Acciones que llevaron a los resultados, donde el 65.12% de los trabajadores asintieron de medio los procesos del tratamiento del conocimiento en virtud a la generación, transferencia y acopio, y aplicación y manejo del conocimiento, frente al 60.47% que afirmaron de medio las practicas aplicadas en la ciberseguridad garantizando su confidencialidad, su integridad y la disponibilidad de datos en la entidad municipal. Concluyendo que, el nivel de asociación en cuanto a la gestión del conocimiento es positiva, fuerte y significativa con la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024, evento establecido por *r* de Pearson 0.619 y el *p*-valor logrado de 0.000 estando por debajo del error de 0.05.

Palabras clave: Gestión del conocimiento, ciberseguridad, procesos operativos sistemáticos, prácticas de seguridad de la información.

Abstract

The objective of this study was to "establish the level of association between knowledge management and cybersecurity in the provincial municipality of Antabamba, Apurímac, in 2024."

Employing a quantitative, basic, correlational, and non-experimental cross-sectional methodology, the study included a population and sample of 43 units of analysis, selected using a non-probabilistic method. The survey and questionnaire were used as the data collection techniques and instruments, respectively. The results showed that 65.12% of the employees moderately agreed with the knowledge management processes related to knowledge generation, transfer, storage, application, and management, compared to 60.47% who moderately agreed with the cybersecurity practices applied, which guarantee confidentiality, integrity, and data availability within the municipal entity. In conclusion, the level of association between knowledge management and cybersecurity in the provincial municipality of Antabamba, Apurímac, in 2024 is positive, strong, and significant, as established by Pearson's r of 0.619 and a p-value of 0.000, which is below the error threshold of 0.05.

Key words: Knowledge management, cybersecurity, systematic operational processes, information security practices.

Índice

Índice de tablas

Índice de figuras

Índice de anexos

I. INTRODUCCIÓN

Las nuevas exigencias que surgen producto de la era de la información y la era digital, las organizaciones deben crear conocimientos nuevos, o los que ya se tienen, se deben nutrir y difundir en toda la organización, lo cual está dando paso a la nueva economía mundial (Copaz, 2022). Es así que, las organizaciones actuales tienden a moverse alrededor de una inmensa cantidad de información, donde una parte de esta información se encuentra estructurada y almacenada en los sistemas informáticos internos, y por otro lado se encuentra fuera de la organización, sirviendo ambas de soporte para la toma de decisiones y la competitividad de estas (Corma, 2018).

Para que la información llegue a todos los niveles de la organización y esta evolucione al ritmo que el contexto actual exige, de donde la existencia de la gestión del conocimiento, un proceso que fortalece a las organizaciones a encontrar, canalizar y difundir información pertinente para su personal, y a generar con ella formas innovadoras para resolver problemas y tomar decisiones (Briceño y colaboradores, 2020). Toda vez que, el conocimiento se ha convertido en uno de los activos más importantes para las instituciones a causa de que su gestión añade valor a los productos o servicios que ésta produce, permitiendo el fortalecimiento de estrategias metodologías y tecnologías, que facilita su inserción y consolidación en el mercado competitivo (Vitale y colaboradores, 2020).

Los países de América Latina y en especial el Perú han experimentado en años recientes una veloz transformación digital en el tratamiento de la información organizacional, situación que genero la proliferación de la ciberdelincuencia en las diferentes organizaciones. Observando que, conforme los gobiernos, las instituciones y los ciudadanos se ponen al día tecnológicamente, las amenazas de ciberseguridad aumentan en paralelo (Bustelo, 2024). Por lo que, las organizaciones demandan cambios constantes y respuestas precisas basadas en nuevas plataformas tecnológicas, nuevos tipos de

servicios, procesos y operaciones que se utilizan para el tratamiento y el resguardo de los datos, debiendo ser resuelto y habilitado rápidamente, y es aquí, donde la gestión del conocimiento y la ciberseguridad están siendo consideradas como alternativas para apoyar los numerosos cambios que deben aplicarse (Rodriguez, 2020).

En esa línea la investigación se configura en nueve capítulos que consideran: considerando el contexto introductorio; el diagnóstico del problema, con la descripción, la justificación, los problemas, objetivos e hipótesis de estudio; así como marco teórico, con los respectivos antecedente, las bases teóricas y los términos conceptualizados; la metodología manejada en la investigación; los resultados alcanzados; las conclusiones y recomendaciones determinadas; además de las fuentes de la literatura y los anexos del estudio.

II. Planteamiento del Problema

2.1. Descripción y formulación del problema

Evidentemente, en el entorno competitivo globalizado actual, las organizaciones a nivel mundial trazan grandes retos, donde la alta complejidad y la fuerte competitividad se imponen para adaptarse a diversas circunstancias, a un sin número de actividades dinámicas y cambiantes, que hacen necesario el rápido ajuste al tratamiento de información y a nuevas tendencias de la manera más efectiva para sobrevivir en el mercado, aplicando nuevos métodos, sistemas, tecnologías, enfoques, herramientas y teorías de manejo para generar y buscar novedosas oportunidades que puedan representar una ventaja competitiva con respecto a las demás organizaciones (Vitale y colaboradores, 2020).

Donde, las nuevas exigencias que surgen producto de la era de la información y la era digital, las organizaciones deben crear conocimientos nuevos, o los que ya se tienen, se deben nutrir y difundir en toda la organización, lo cual está dando paso a la nueva economía mundial (Copaz, 2022). Es así que, las organizaciones actuales tienden a moverse alrededor de una inmensa cantidad de información, donde una parte de esta información se encuentra estructurada y almacenada en los sistemas informáticos internos, y por otro lado se encuentra fuera de la organización, sirviendo ambas de soporte para la toma de decisiones y la competitividad de estas (Corma, 2018).

Por cuanto, para que la información llegue a todos los niveles de la organización y esta evolucione al ritmo que el contexto actual exige, existe la gestión del conocimiento, un proceso que fortalece a las organizaciones a encontrar, canalizar y difundir información pertinente para su personal, y a generar con ella formas innovadoras para resolver problemas y tomar decisiones (Briceño y colaboradores, 2020). Manifestando que, el conocimiento se ha convertido en uno de los activos más importantes para las organizaciones a causa de que su gestión añade valor a los productos o servicios que

ésta produce, permitiendo el desarrollo de tecnologías, metodologías y estrategias, lo que facilita su inserción y consolidación en el mercado (Vitale y colaboradores, 2020).

En Latinoamérica han ejercitado en los últimos años una veloz transformación digital en tratamiento de la información organizacional, lo que genero el aumento de ciberdelincuencia en las organizaciones. Observando que, conforme los gobiernos, las instituciones y los ciudadanos se ponen al día tecnológicamente, las amenazas de ciberseguridad aumentan en paralelo (Bustelo, 2024). Por lo que, demanda a las organizaciones a cambios constantes y respuestas oportunas, consecuentemente a ampliar la gama de tecnologías, nuevas plataformas, nuevos tipos de servicios, procesos y procedimientos que se utilizan para el tratamiento y el resguardo de los datos, debiendo ser resuelto y habilitado rápidamente, y es aquí, donde la gestión del conocimiento y la ciberseguridad están siendo consideradas como alternativas para apoyar los numerosos cambios que deben aplicarse (Rodriguez, 2020).

El Perú y toda Latinoamérica se llega a advertir que el estado latente de la ciberseguridad es preocupante siendo una de las más atacadas dentro el escenario mundial. La conjunción de la falta de estándares y regulaciones claras, la escasez de profesionales cualificados, la ausencia de una cultura de la gestión del conocimiento (GC), de seguridad cibernética en las empresas, gobiernos, usuarios y los recursos limitados para invertir en tecnologías para el manejo de la información y de seguridad convierten a la región en una zona del planeta singularmente vulnerable a las ciberamenazas (Bustelo, 2024). Encontrándose un 62% de organizaciones que sufrieron algún ataque y estando en peligro su información en años recientes, consecuentemente estas organizaciones deben diseñar acciones para garantizar el tratamiento de sus datos y no sean sujeto de algún ataque tecnológico y garantizar sus procesos operativos. (Ey México [EM], 2023).

Situación que no está ajena a la significativa importancia de la consecución de la investigación, en vista que las entidades del estado, como los gobiernos regionales,

locales y/o distritales, especialmente el gobierno provincial de Antabamba, que para diseñar una gestión pública efectiva, deben establecer procesos de cambios, innovaciones y modernización de la función pública, para mejorar su cercanía al ciudadano y la sociedad, bajo la finalidad de mejorar la legitimidad y la transparencia del tratamiento de datos tanto intrínseca como la extrínseca por intermedio de la generación de sistemas de información, transferencias, supervisión, transparencia y la administración del conocimiento, sin descuidar la trascendencia que representa la información confidencial, donde la organización, seguridad y la defensa informática se identifiquen como una de las tareas más importantes que requieren un mayor desarrollo e inversión en la entidad, puntualizando que el talento humano como el principal activo de la municipalidad, sustentará sus fortalezas en cuanto a su posicionamiento, productividad la fidelización y cumplimiento de los requerimientos organizacionales y de la zona de influencia.

Consecuentemente, la investigación consintió el tratamiento de la realidad de la GC y la concatenación que la misma contaba con la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac; permitiendo observar y conocer el proceso operacional y el potencial fomento para asegurar una adopción más amplia y efectiva de estas tecnologías para transformar el movimiento de la rueda de negocios y el crecimiento operacional de la entidad municipal, sociabilizarlo y aplicarlo entre los colaboradores para una toma de decisiones efectivas, proponiendo de manera integral una aplicación para la administración de los datos y del conocimiento, anidadas a las acciones de preservar la estabilidad y la creación de una estructura que pueda garantizar la seguridad de la información clasificada de cada uno de sus unidades funcionales para generar un fortalecimiento en el desempeño y satisfacción de las necesidades de la comunidad de Antabamba.

2.2. Formulación del problema de investigación

2.2.1 Problema General

¿Cuál es el nivel de asociación de la gestión del conocimiento y la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024?

2.2.2 Problemas Específicos

Pe1. ¿En qué medida la gestión del conocimiento se asocia con la confidencialidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024?

Pe2. ¿En qué medida la gestión del conocimiento se asocia con la integridad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024?

Pe3. ¿En qué medida la gestión del conocimiento se asocia con la disponibilidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024?

2.3 Justificación y delimitación

2.3.1 Justificación

Se justifica el estudio de manera oportuna a razón de los fenómenos de estudio que son significativos para el gobierno local, de cuyo desenlace se logró enriquecer y fortalecer el conocimiento de la gestión del conocimiento y de la ciberseguridad, anidados al reconocimiento, la observación e identificación de la adopción, tratamiento, compromiso, cumplimiento de las exigencias, disposiciones y las normas para la aplicación e implementación de los sistemas de administración de negocios anidados a las aplicación de búsqueda, observación y verificación del manejo público municipal, la gestión de intercambio de capacidades, datos y advertencias asociadas con la seguridad digital intrínseca y extrínseca de la entidad municipal provincial. Logrando posicionar al talento humano de la institución, siendo un recurso significativo y que sustenten sus capacidades de intercambiar los datos oportunamente y verídicamente, basadas en una cultura organizacional de participación activa, compromiso, motivación y

corresponsabilidad, concatenadas con las nuevas tecnologías de la información y la creación efectiva de las condiciones para una mejora continua de la municipalidad provincial en estudio.

2.3.2 Delimitación

Se consideró las distintas unidades orgánicas y colaboradores de la municipalidad provincial de Antabamba, departamento de Apurímac. Así mismo, el estudio se inició en noviembre del 2024 y finalizó en marzo del 2025. Además, el desarrollo de la investigación benefició al talento humano que cumplen diferentes funciones y actividades en las diferentes gerencias, direcciones y áreas operativas de la municipalidad objeto de estudio, y que repercutió en mejorar el servicio de oportunamente, la toma de decisiones y la satisfacción y cumplimiento de los requerimientos de los pobladores.

2.4 Objetivos

2.4.1 Objetivo General

Establecer el nivel de asociación de la gestión del conocimiento con la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

2.4.2 Objetivos Específicos

Oe1. Determinar el nivel de asociación de la gestión del conocimiento con la confidencialidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Oe2. Determinar el nivel de asociación de la gestión del conocimiento con la integridad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Oe3. Determinar el nivel de asociación de la gestión del conocimiento con la disponibilidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

2.5 Hipótesis

2.5.1 Hipótesis general

La gestión del conocimiento se asocia significativamente con la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

2.5.2 Hipótesis específicas

He1. La gestión del conocimiento se asocia elocuentemente con la confidencialidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

He2. La gestión del conocimiento se asocia elocuentemente con la integridad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

He3. La gestión del conocimiento se asocia elocuentemente con la disponibilidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

III. MARCO TEÓRICO

3.1 Antecedentes del problema

3.1.1 A nivel internacional

Efectuada las revisiones de las fuentes teóricas y bibliográficas de investigaciones previas sobre las variables problemáticas, entre los antecedentes internacionales se tiene a Payró y Fuentes (2021), en su estudio donde el objetivo fue describir una propuesta de GC para una organización de construcción de software. Con una metodología de un estudio de caso. Donde los resultados arrojaron un diseño de GC acorde a los requerimientos y aplicación de instrumentos de administración de conocimientos basados en las necesidades de la organización. Concluyendo que, las herramientas digitales de toda la organización y entre otros escenarios externos, demostraron la presencia de elementos de carencia de identidad por parte de los ejecutivos y una cultura anidad a la GC.

Por su parte Manzano y Mul (2020), en su investigación basado en el objetivo; analizar los procesos de GC en una empresa de servicios profesionales de consultoría en la ciudad de Mérida, Yucatán, México. Con la metodología de enfoque cualitativo. Donde los resultados fueron que, la entidad llegó a trabajar más en la apertura de datos y negocios y poco en garantizar su seguridad y la transferencia. Llegando a la conclusión que, entre las actividades sugeridas se determina evitar el cambio del talento humano, conservar y categorizar los datos, construir manuales, motivación, estimulaciones y garantizar los accesos a los datos de forma segura.

Considerando a Piñón et al. (2023), en el estudio bajo el objetivo analizar los programas de capacitación como herramienta para fortalecer la ciberseguridad en una empresa mexicana. Con una metodología de enfoque cuantitativo de carácter no experimental transeccional. Los resultados muestran que el 52.1% de empleados consideran que tienen el conocimiento necesario sobre las amenazas cibernéticas que pueden

enfrentar, pero el resto no consideran que conozcan dichas amenazas, siendo la ciberseguridad prioritaria para la organización y que no cuentan con la suficiente capacitación que les ayude a reducir las amenazas a las que están expuestos. Pudiendo concluir que, es necesario llevar a cabo la capacitación y concientización sobre seguridad mediante la elaboración de políticas, la definición de recursos y herramientas, la creación de campañas contra los ataques cibernéticos y la implementación de capacitación en línea o presencial.

En el estudio de Mera (2021), cuyo objetivo fue; analizar la gestión del conocimiento en el programa de fortalecimiento de emprendimientos e iniciativas productivas locales (PFEIPL) aplicado por el gobierno provincial de Imbabura. Aplicando una metodología tipo cualitativo, exploratoria y descriptiva. Pudiendo concluir que, deben realizar sistemáticamente acciones de GC, por intermedio de la ejecución de procedimientos lineamientos y formalidades para innovar GC, las que estén concatenados con el estratégico a poner en práctica.

3.1.2 A nivel nacional

Guevara (2023), en la investigación desarrollada con el objetivo de determinar el nivel de gestión del conocimiento en los trabajadores del municipio de JLO, 2022. Utilizando la metodología tipo básico, descriptivo, no experimental transversal. Logrando resultados 0.9 fiabilidad. Arribando a la conclusión que, el 4% de empleados muestran un bajo nivel, el 28,8% medio, y el 67,2% un alto nivel.

Además, en el estudio de Correa (2021), donde se logró el objetivo determinar la incidencia de la ciberseguridad en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021. Manejando la metodología de investigación aplicada, no experimental, transversal y correlacional – causal. Llegando a resultados del 39.4% consideraron que el manejo de información presente un nivel bueno frente al efecto de la ciberseguridad. Quién concluye que la ciberseguridad posee 0.256 y *p*

de 0.000 de Wald, señalando que entre ambas variables se presenta una incidencia significativa.

En consideración de Lazaro y Meza (2022), quienes plantearon el objetivo de analizar el grado de asociación entre GC y la efectividad organizacional en la Municipalidad de Punta Hermosa, 2021. Aplicando la metodología correlacional, fundamental, y no experimental. Obteniendo un resultado, donde Rho de Spearman es 0.885 con un p-logrado 0.000. Pudiendo concluir que, entre la GC y la efectividad organizacional hay una asociación evidente.

Sanchez (2021), en la investigación cuyo objetivo fue evaluar los diferentes niveles de seguridad informática que debe tener las entidades públicas, para lograr la continuidad de sus servicios informáticos, Con la metodología de estudio tipo descriptiva. Llegando a la conclusión que, la tecnología informática es vulnerables a los ataques de los ciber delincuentes, para el cual se diseñó estrategias de protección y asegurar las operaciones de las herramientas digitales institucional.

3.1.3 A nivel regional y local

En la investigación de Olarte (2021), se manejó el objetivo de conocer la importancia de los mecanismos de seguridad informática para evitar la vulnerabilidad del sistema de información inalámbrico. Con una metodología cuantitativa, descriptiva, no experimental y exploratorio. Quién concluye que, las acciones para garantizar la información deben estar basadas en la seguridad de las mismas y evitar la fragilidad de las tecnologías digitales.

3.2 Bases Teóricas

3.2.1 Gestión del conocimiento

De acuerdo a las manifestaciones de Zendesk (2023), la gestión del conocimiento (GC) “es un conjunto de actividades y procesos con el objetivo de facilitar la creación,

organización e intercambio de información entre los clientes y funcionarios de la organización".

De otra parte, la GC (KM, por sus siglas en inglés) "es el proceso de identificar, organizar, almacenar y difundir información dentro de una institución" (IBM, 2022).

3.2.1.1 Objetivos de la gestión del conocimiento

Para lograr una eficiente gestión del conocimiento se debe poner en práctica objetivos precisos que permitan a la organización cumplir con sus fines (Zendesk, 2023), a saber:

- Fortalecer la práctica de los usuarios y mejorar cada producto para la innovación de la organización.
- Generación y disponibilidad de datos.
- Hacer que las organizaciones estén más preparadas para su competitividad.
- Emplear herramientas y procesos de aprendizaje.
- Brindar soporte técnico a través de una base de conocimientos.
- Proveer instrumentos para operativizar el conocimiento en las organizaciones.
- Brindar servicio de atención ágil gracias al autoservicio (Zendesk, 2023).

3.2.1.2 Características de la gestión del conocimiento

Partiendo de lo afirmado por Flores (s.f.), entre los atributos a ser tomados en cuenta para una eficiente GC en la organización, y que son importantes para entender cómo se maneja y se utiliza la información en diferentes contextos, entre ellas están: a) la identificación del conocimiento clave organizacional, b) la generación y acopio de datos, c) el acceso y disponibilidad; garantiza que la información esté disponible para los empleados adecuados en el momento que sea requerida, bajo: Sistemas de búsqueda eficientes y plataformas accesibles para compartir información, d) las competencias para compartir y utilizar el conocimiento; implican habilidades para gestionar el conocimiento y entre ellas están: Compartir información de manera clara y efectiva,

utilizar el conocimiento disponible de forma adecuada y valorar su relevancia y asimilarlo correctamente y capacidad de colaborar con otros miembros de la empresa en la generación y aplicación del conocimiento, la transferencia y difusión; consiste en llevar el conocimiento desde donde es generado hasta donde se va a utilizar de forma efectiva, bajo una información oportuna entre los actores, por intermedio de: Capacitaciones, reuniones y plataformas en línea, y e) la creación de una cultura de aprendizaje; fomentar una mentalidad de aprendizaje continuo dentro de la organización, incentivando a los empleados a compartir lo que conocen y a aprender de los demás, promoviendo la mejora continua.

- Uso estratégico del conocimiento; permite tomar decisiones informadas y estratégicas, esto implica aplicar la información de manera efectiva para: Resolver problemas, innova y mejorar procesos (Flores, s.f.).

3.2.1.3 Procesos de la gestión del conocimiento

Krzyzanowski et al. (2024), sostiene que existen sistemas y pasos de procesos más comunes que una organización podría integrar con un proceso de gestión del conocimiento efectivo (párr. 1), señalando: a) el descubrimiento; considerando la apertura a información que permita integrar los procesos de la empresa basados en la minería de datos, b) la captura; lograr conocimientos entre los colaboradores que fortalezca el negocio institucional, c) la organización; constituida por todos los procesos hasta la indexación de los datos y compartir con los trabajadores, d) la evaluación; donde se llegará a mejorar efectivamente la toma de decisiones empresariales, e) la compartición; donde los datos se encuentren a disposición entre los colaboradores de la entidad, f), la reutilización/aplicación; asimilar toda información para que tome las decisiones en los diferentes niveles organizacionales, g) la creación; es cuando los individuos o equipos dentro de la empresa añaden lo que han aprendido—mediante la práctica, la navegación de procesos, interacciones internas y externas, investigación

independiente y otras experiencias—a el conocimiento colectivo de la organización (Krzyzanowski y colaboradores, 2024).

3.2.1.4 Estrategias de la gestión del conocimiento

Para aplicar una gestión del conocimiento eficiente existen distintas, estrategias, herramientas y proyectos que pueden ayudar a las empresas a fomentar el aprendizaje organizacional (Personio, 2024), siendo las estrategias siguientes a tener en cuenta:

- Contar con una herramienta digital; donde el personal pueda acceder a toda documentación significativa y compartir entre los miembros de la empresa.
- Acceder a información de la empresa; con la finalidad de realizar las respectivas consultas.
- Dar visibilidad a los diferentes proyectos que se desarrollen y que los colaboradores estén actualizados.
- Reconocimiento; valorar y recompensar todo compromiso del talento humano.
- Diseño de programas de capacitación; de acuerdo a las exigencias del entorno al mercado competitivo, así como de cada empleado generado por la unidad del talento humano.
- Fomentar el trabajo en equipo; permitiendo al talento humano aprender de sus compañeros y sus experiencias.
- La rotación de personal; el hecho de que un empleado cambie de unidad durante un tiempo le ayuda a adquirir nuevos conocimientos y aptitudes, y a ganar experiencia en tareas que son diferentes a las que realiza habitualmente (Personio, 2024).

3.2.1.5 Beneficios de la gestión del conocimiento

La gestión del conocimiento no solo es una herramienta estratégica, sino una inversión clave para el crecimiento sostenible y la competitividad de la organización en un entorno empresarial dinámico (Flores, s.f.), ofreciendo los siguientes beneficios:

- Acceso a información relevante; acceso más rápido y eficiente a la información relevante, por intermedio de la minería de datos, se pueden analizar grandes cantidades de información para obtener conocimientos valiosos, facilitando la toma de decisiones basadas en datos reales y actualizados.
- Colaboración y el trabajo en equipo; donde los colaboradores pueden intercambiar y manejar los conocimientos de forma eficaz, innovando y optimizando el rendimiento del equipo.
- Mejora toma de decisiones; al tener acceso rápido y fácil a una amplia gama de datos actualizados, reduciendo incertidumbres y riesgos.
- Satisfacción y retención de empleados; permitir que compartan y utilicen su conocimiento los empleados, y se sientan valorados y reconocidos en su trabajo, generando mayor satisfacción laboral y a una mayor retención de los empleados.
- Innovación continua; facilita el intercambio de ideas y conocimientos, estimulando la innovación dentro de la organización.
- Optimización de procesos; genera eficiencia operativa muy esencial para el rendimiento empresarial, por intermedio de la identificación y optimización de procesos internos, eliminando redundancias y mejorando la productividad.
- Desarrollo y retención del talento; no implica almacenar información, sino también compartir habilidades y experiencias entre colaboradores.

- Adaptación ágil al cambio; proporciona a la organización la agilidad necesaria al mantener al equipo informado sobre nuevas tendencias, tecnologías y mejores prácticas.
- Reducción de errores en los procesos; Accede a información precisa y actualizada ayudando a prevenir errores y malentendidos dentro de la entidad, estableciendo un sistema confiable para la distribución y actualización de información crítica (Flores, s.f.).

3.2.1.6 Herramientas de la gestión del conocimiento

Para Krzyzanowski et al. (2024a), las herramientas de gestión del conocimiento son esenciales para toda organización que buscan mejorar la eficiencia organizacional, simplificar la comunicación y fomentar la innovación (párr. 1), señalando:

- Las Bases de conocimiento; utilizando para capturar, gestionar y organizar información organizacional clave y ayudar a los equipos o clientes a encontrar la información que necesitan, cuando la necesitan.
- Los Sistemas de gestión del aprendizaje (LMS); ayudan a las organizaciones a construir una sólida fundación de gestión del conocimiento al permitirles crear programas de capacitación y educativos personalizados.
- El Servicio Centrado en el Conocimiento (KCS); apoyan el servicio centrado en el conocimiento, describiendo cómo los equipos de servicio al cliente y soporte acceden y utilizan el conocimiento para ofrecer un mayor valor a los clientes, empleados y partes interesadas.
- La Gestión del conocimiento AI; permite capturar, filtrar, representar o aplicar conocimientos, incluyendo aplicaciones que pueden seleccionar, analizar y clasificar texto; realizar razonamiento automatizado; y crear visualizaciones – todo lo cual puede mejorar las capacidades de toma de decisiones.

- La Gestión de relaciones con el cliente (CRM); ayuda a todos los equipos involucrados en marketing, ventas y servicio al cliente, los sistemas CRM rastrean información de prospectos y clientes a lo largo de las relaciones con los clientes.
- La Gestión de contenido; abarcan la creación, gestión y distribución del contenido organizacional en la intranet de la entidad o sitio web (Krzyzanowski y colaboradores, 2024a).

3.2.1.7 Dimensiones de la gestión del conocimiento

Para Tarí y García (2009), existen tres (03) dimensiones más comúnmente utilizadas en la gestión del conocimiento para una empresa (p. 142), estas son:

- **La creación del conocimiento**; ligada a la adquisición interna de conocimiento y a la capacidad de aprendizaje, así como la adquisición de información, diseminación de la información y la interpretación compartida (Tarí y García, 2009, p. 142).
- **El almacenamiento y transferencia del conocimiento**; constituida por almacenar conocimiento y transferir conocimiento en la organización, además de los flujos de aprendizaje, compartir conocimiento intraorganizativo, articulación del conocimiento y, stocks de conocimiento (Tarí y García, 2009, p. 142).
- **La aplicación y uso del conocimiento**; constituida por trabajo en equipo, empowerment, promover el diálogo, establecer sistemas para capturar y compartir el aprendizaje, relación entre distintos departamentos o áreas funcionales, compromiso con el aprendizaje, así como las prácticas de conocimiento, dominio personal, apertura y experimentación, visión compartida, cultura organizativa y, orientación al aprendizaje y de sistemas (Tarí y García, 2009, p. 142).

3.2.2 Ciberseguridad

De los aportes realizados por la Universidad Tecnológica del Perú (UTP 2023), considera que la ciberseguridad “es un conjunto de medidas y prácticas destinadas a proteger los sistemas informáticos, redes y dispositivos electrónicos de las amenazas cibernéticas” (párr. 1).

La ciberseguridad, llamada también seguridad digital, “es la práctica de proteger la información digital, dispositivos y activos de una organización, incluyendo información personal, cuentas, archivos, fotos e incluso los recursos económicos” (Microsoft, 2023).

3.2.2.1 Objetivos de la ciberseguridad.

Los objetivos de la ciberseguridad se encuentran clasificados en tres categorías (Ortega, 2024), tales como la prevención, detección y recuperación:

- Prevenir; generar escenarios para fortalecer la protección de los distintos competentes informáticos.
- La detección: conocer los factores que colocan en riesgo a los elementos y herramientas digitales frente a posibles ataques de ciber delincuentes.
- Recuperación: establecer métodos para aislar y expulsar las amenazas de los dispositivos de tal forma que se sufra el menor daño posible y ejecutar tareas de restauración y recuperación de información (Ortega, 2024).

3.2.2.2 Importancia de la ciberseguridad*.*

Para Age2 (2024), es de significancia y primordial proteger a las organizaciones, sus datos, sistemas y clientes, debiendo implantar y contar con sistemas de seguridad adecuados (párr. 1). Por cuanto y entre los motivos importantes que se debe considerar para invertir e implementar la ciberseguridad en una empresa son: a) preservación de información, b) autentificación de los servicios disponibles, c) la protección para el acceso a datos, d) proteger las operaciones de cada productos informático, e) mejora la competitividad de la empresa, f) protección de la

información frente a su manipulación, g) desarrollo de modelos de negocio innovadores, h) evitar la suplantación o el control de la información y los aplicativos, i) evitar el piratería de información digital, j) garantizar la automatización de procesos, y k) protección de competentes individuales.

Señalando además, que los integrantes de la organización conozcan y asuman buenas prácticas para garantizar la mayor seguridad y protección de los datos de la empresa, llegando a utilizar contraseñas fuertes y no compartirlas en aplicaciones o servicios, revisar la conexión de todas las redes y aplicaciones sociales, evitando aceptar a desconocidos en tu red de contactos, cuida lo que publicas en Internet, que sea siempre de fuentes fiables y navegación segura, instalar complementos de seguridad en el navegador, utilizar la navegación privada cuando sea necesario, las compras que se realicen a través de la red siempre en webs de confianza y que tengan un certificado digital válido, proteger la red WIFI adecuadamente, no reenviar cadenas, no todo lo que se publica online es fiable y revisar las opciones de seguridad de tu navegador (Age2, 2024).

3.2.2.3 Principios de la ciberseguridad.

Existen cuatro principios fundamentales de la ciberseguridad (Ortega, 2024), siendo: La integridad, la confidencialidad, la disponibilidad y la autenticación, las mismas permiten:

- Garantizar un grado de resiliencia y ciberseguridad de las herramientas tecnológicas.
- Promover la capacitación y competitividad de usuarios frente a los ataques de siber delincuentes.
- Inducir a que los instrumentos tecnológicos tengan la seguridad respectiva para garantizar el proceso de los datos de forma efectiva.
- Capacitar a los talentos humanos sobre los riesgos cibernéticos.

- Compartir y mantener los conocimientos, las habilidades y las capacidades tecnológicas que se requieren para ejercer la ciberseguridad (Ortega, 2024).

3.2.2.4 Características de la ciberseguridad.

La ciberseguridad estratégicamente debe proteger cada área y no solo enfocarse en tener herramientas para reaccionar ante los ataques, sino que debe brindar protección para evitar que los sistemas sean vulnerados (Bustamante, 2023), para los cuales debe cumplir las siguientes características: a) el control en el almacenamiento de la información, b) el acceso reducido a datos, c) el análisis y el tratamiento de riesgos; para conocer a qué son susceptibles y cómo pueden atacarlos, brindando protección en todos los niveles organizacionales, d) supervisión diario, e) las políticas seguras de BYOD (Bring Your Own Device); consiste en que los empleados trabajen desde sus propios dispositivos, generando políticas y acciones para que los usuarios utilicen sus equipos de forma segura sin comprometer los datos de la organización (Bustamante, 2023).

3.2.2.5 Tipos de ciberseguridad.

Según Infosecurity México (IM 2024), la ciberseguridad es determinante para la protección y gestión de la información de cualquier organización (párr. 1), siendo de gran importancia reconocer los tipos de ciberseguridad existentes contempladas en cuatro (04) áreas principales:

- Confidencialidad; acceden a los datos los usuarios autorizados (IM 2024).
- Integridad; usuarios autorizados son los que deben modificar la información (IM 2024).
- Disponibilidad; la información está disponible según sea necesario (IM 2024).
- Autenticación; verificar que realmente se está en comunicación con quién se están comunicando (IM 2024).

Por cuanto, según los elementos que se deben proteger se clasifican los tipos de ciberseguridad: a) la seguridad de hardware (HW) , b) la seguridad software (SW), y c) la seguridad en la red. Para eliminar las amenazas más comunes en la red que son: Virus, gusanos y caballos de troya, software espía y publicitario, ataques de día cero, también llamados ataques de hora cero, ataques de hackers, ataques de denegación de servicio, intercepción o robo de datos, y robo de identidad, aplicando antivirus y antispyware, cortafuegos, sistemas de prevención de intrusiones y redes privadas virtuales (Infosecurity México [IM] 2024).

3.2.2.6 Dimensiones de la ciberseguridad

Para abordar la ciberseguridad es fundamental comprender las dimensiones clave que sustentan la protección de la información y los sistemas digitales (Sánchez, 2024), señalando que para garantizar y preservar las dimensiones de seguridad se deben tomar en cuenta: la confidencialidad, integridad y disponibilidad, conocida como la tríada CID (o CIA en inglés):

- **Confidencialidad;** La violación de la confidencialidad pueden ser intencionados, como el robo de contraseñas, o ataques de fuerza bruta aplicando el método de prueba y error en un intento de descifrar una contraseña o nombre de usuario, la captura del tráfico de red interceptando y manipulando el tráfico, o ataques de phishing; Además de los no intencionados, como los accidentes comunes que incluyen el envío de información confidencial por correo electrónico a un destinatario equivocado, la publicación de datos privados en web públicas y redes sociales, o simplemente dejar información confidencial expuesta en el monitor de un ordenador desatendido (Sánchez, 2024).

- **Integridad;** asegurar que la información no sufra alteraciones no autorizadas. Siendo la integridad significativa para proporcionar confiabilidad en la información y los sistemas (Sánchez, 2024).
- **Disponibilidad;** uso de la información y de todos los procesos por los usuarios autorizados. Considerando los ataques no intencionados hacia los datos sean estos de naturaleza no intencionada, en cambio, los ataques maliciosos incluyen, ataques de denegación de servicio (DoS) en el que los hackers inundan un servidor con peticiones superfluas, saturando el servidor y degradando el servicio, u otras formas de sabotaje que impidan el acceso al sistema de información a los usuarios legítimos (Sánchez, 2024).

3.3 Definición de términos

Gestión del conocimiento

"Es un proceso sistemático que permite a las organizaciones crear, compartir, utilizar y gestionar su conocimiento y su información" (Cohen, 2024).

Ciberseguridad

"Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos (Kaspersky, 2024).

Conocimiento

"Conjunto de experiencias, valores, información en contexto y vivencias internalizadas, que provee un marco de trabajo para evaluar e incorporar nuevas experiencias e información (Quiroa, 2021).

Información

"Es un mensaje que se transmite a una persona o a un grupo de personas que forman parte de una organización" (Quiroa, 2021).

Conocimiento explícito

“Es el tipo de conocimiento que alcanza un grado de formalización en el momento en que se elaboran documentos, reglas, códigos y normas” (Quiroa, 2021).

Conocimiento tácito

“Es el conocimiento que posee cada persona que forma parte de la empresa y que se encuentra relacionado con la experiencia y habilidades adquiridas (Quiroa, 2021).

Educación corporativa

“Es un proceso formal de recibir los conocimientos” (Quiroa, 2021).

Gestión de habilidades

“Es un modelo estratégico en el que se determinan y gestionan las habilidades y actitudes que deben poseer los empleados de la organización” (Quiroa, 2021).

Gestión de información

“Se refiere a los sistemas de información que tienen ordenada y organizada la información, para que llegue de manera fácil a todos los que la requieran y con ello sea más fácil el proceso de la toma de decisiones” (Quiroa, 2021).

Aprendizaje en la organización

“Consiste en la motivación al aprendizaje colectivo, para que se genere un proceso de innovación constante” (Quiroa, 2021).

Inteligencia competitiva

“Se trata de mantenerse en contacto con los mercados para poder encontrar nuevas oportunidades de negocio” (Quiroa, 2021).

Activo de información

Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones” (Incibe, 2020).

Actualización de seguridad

Modificaciones que se aplican, de forma automática o manual, en el software de los sistemas operativos o aplicaciones instalado en los dispositivos electrónicos, con el objetivo de corregir fallos de seguridad, errores de funcionamiento o bien para dotar a los dispositivos de nuevas funcionabilidades, así como incorporar mejoras de rendimiento (Incibe, 2020).

Amenaza

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor (Incibe, 2020).

Análisis de riesgos

“Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo (Incibe, 2020).

Análisis de vulnerabilidades

“Consiste en la búsqueda y documentación de fallos, carencias o debilidades físicas (inundaciones, incendios, controles de acceso…) y lógicas (configuraciones, actualizaciones...) en un sistema informático, que puedan ser empleados por terceros con fines ilícitos, suponiendo un riesgo para la organización y los propios sistemas” (Incibe, 2020).

Antivirus

“Software de protección para evitar que ejecutemos algún tipo de software malicioso en nuestro equipo que infecte al equipo” (Incibe, 2020).

Antispyware

“Herramienta de software diseñada para detectar y eliminar programas maliciosos del tipo spyware cuyo objetivo es espiar y obtener de forma sigilosa información personal presente en el dispositivo sin consentimiento del usuario” (Incibe, 2020).

Autenticación

“Acción mediante la cual demostramos a otra persona o sistema que somos quien realmente decimos que somos, mediante un documento, una contraseña, rasgo biológico etc. (Incibe, 2020).

Backup

“Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados” (Incibe, 2020).

Borrado seguro

“Método de borrado de archivos que se caracteriza por sobrescribir los datos con el propósito de impedir su recuperación” (Incibe, 2020).

Brecha de seguridad

“Violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos (Incibe, 2020).

Ciberataque

“Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, el robo de información, extorsión del propietario o simplemente daños al sistema” (Incibe, 2020).

Ciberdelincuente

Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión” (Incibe, 2020).

Cifrado

“Proceso de codificación de información para poder evitar que esta llegue a personas no autorizadas” (Incibe, 2020).

Cifrado de extremo a extremo

“Es la propiedad de algunos sistemas de comunicación que hace que los mensajes intercambiados sean ilegibles durante la comunicación en caso de interceptación al estar cifrados” (Incibe, 2020).

Clave privada

“Son sistemas de criptografía asimétrica que se basan en la generación de una clave privada que sólo debe ser conocida por el usuario para el cifrado y descifrado de mensajes” (Incibe, 2020).

Clave pública

“Son sistemas de criptografía asimétrica, se basan en la generación, mediante una “infraestructura de clave pública”, que tienen la peculiaridad de que los mensajes cifrados con una de ellas sólo pueden ser descifrados utilizando la otra” (Incibe, 2020).

Contraseña

“Forma de autentificación de un usuario, a través de una clave secreta, para controlar el acceso a algún recurso o herramienta tecnológica” (Incibe, 2020).

IV. METODOLOGÍA

4.1 Tipo y nivel de investigación

4.1.1 Tipo de investigación

De tipo básica, caracterizada por “la indagación del contexto mismo de los fenómenos, con la finalidad de descubrir nuevos principios, teorías o hechos sin una aplicación inmediata en mente” (Stewart, 2024).

En esa línea, se realizaron un tratamiento básico científico de las respectivas variables, en donde se pudo observar el comportamiento de la gestión del conocimiento y de la ciberseguridad en la zona de influencia, y que generaron respuestas concretas para llegar comprender cómo los gerentes, ejecutivos y personal operacional de la municipalidad construyen la realidad organizacional en el cumplimiento de sus fines hacia la comunidad, profundizando en el modo en que la cultura institucional conforma la comprensión y manejo de la gestión del conocimiento y la ciberseguridad para solucionar los cuellos de botellas existentes y aportar conocimientos significativos sobre el cómo se forman las percepciones y participaciones del talento humano en la comprensión necesaria de los avances tecnológicos en las distintas áreas, para impulsar la innovación operativa en la municipalidad provincial objeto de investigación.

4.1.2 Nivel de investigación

Se establece un nivel correlacional, de donde según Hernández et al. (2014), las investigaciones de nivel correlacional “son estudios directamente de la realidad que brindarán y pondrán en conocimiento el nivel de asociación de dos o más variables independientes” (p. 93).

Por cuanto, en el estudio se lograron datos del ambiente natural, las que generaron la medición del comportamiento de la gestión del conocimiento y de la ciberseguridad a partir de las cuales se llegó a entender y evaluar el grado de correlación estadística entre ambos fenómenos, sin que exista influencia alguna de variables ajenas al de estudio.

4.2 Diseño de investigación

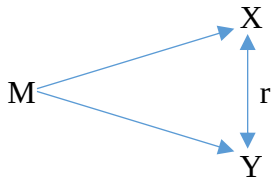
Parte del no experimental-transversal, donde los datos de las respectivas variables se lograron sin la necesidad de ejecutar experimento alguno, donde no existió manipulación intencional, que los mismos se obtuvieron en su ambiente natural y en un único momento para poder determinar de cómo las respectivas las variables se relacionan entre sí en un entorno ideal, donde no existan interferencias de otros fenómenos.

Señalando Hernández et al. (2014), que las investigaciones de diseño no experimental "son aquellos que se desarrollan donde no hay presencia de manipulación de las variables, observándose la situación en su entorno para luego analizar sus respectivos comportamientos" (p. 152).

Así mismo, los estudios transversales "son todos aquellos donde los datos se logran en un solo momento del contexto donde se maneja las respectivas variables" (Hernández y colaboradores, 2014, p. 154).

Figura 1

Tipología de la investigación



Nota: diseño de la estructura de la investigación

4.3 Operacionalización de variables

4.3.1 Variable X

Gestión del conocimiento.

4.3.2 Variable Y

Ciberseguridad.

4.3.3 Operacionalización de Variables

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores
Variable X: Gestión del conocimiento	"Es un conjunto de actividades y procesos con el objetivo de facilitar la creación, organización e intercambio de información entre los clientes y funcionarios de la organización" (Zendesk, 2023),	Son acciones concatenadas para el tratamiento de la información entre el talento humano para la creación, el almacenamiento y transferencia, y la aplicación y uso del conocimiento para la toma de decisiones en el cumplimiento de los objetivos corporativos.	Creación del conocimiento	Adquisición de conocimiento. Capacidad de aprendizaje. Adquisición de información. Diseminación de información. Interpretación compartida. Compartir información. Desempeño.
			Almacenamiento y transferencia del conocimiento.	Monopolización del conocimiento. Transferir conocimiento. Flujos de aprendizaje. Compartir conocimiento. Articulación del conocimiento. Stocks de conocimiento. Aplicación de conocimientos
			Aplicación y uso del conocimiento	Trabajo en equipo. Empowerment Promoción de diálogo. Sistemas para capturar el aprendizaje. Sistemas para compartir el aprendizaje. Prácticas del conocimiento. Dominio de personal. Visión compartida. Cultura organizativa.

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores
Variable Y: Ciberseguridad	"Es la práctica de proteger la información digital, dispositivos y activos de una organización, incluyendo información personal, cuentas, archivos, fotos e incluso los recursos económicos" (Microsoft, 2023).	Son acciones precisas para garantizar y preservar las información digital y demás activos de una empresa y que estén basadas en su confidencialidad, integridad y disponibilidad de los sistemas de información y tecnologías de información y comunicación con los que cuenta.	Confidencialidad	Protección de la información. Protección de los activos de accesos no autorizados. Protección de los activos de usos indebidos. Violación de confidencialidad. Robo de contraseñas. Ataques y descifrar contraseñas e usuarios Manipulación del tráfico. Ataques de phishing. Envío de información confidencial.
			Integridad	Integridad de los datos. Integridad de los sistemas. Garantía de los datos. Almacenamiento de datos. Procesamiento de los datos. Tratamiento de los datos. Modificaciones indebidas. Pérdidas de información. Confiabilidad de la información. Confiabilidad de los sistemas.
			Disponibilidad	Acceso a los datos. Servicios de información Usuarios autorizados. Asegurar y garantizar los niveles de disponibilidad. Ataques maliciosos de hackers. Saturación del servidor. Sabotaje de acceso a la información. Sabotaje de acceso al sistema.

4.4 Población y muestra

4.4.1 Población

Estuvo conformada por los gerentes, ejecutivos y personal operativo que cumplen sus funciones en las diversas unidades orgánicas de la municipalidad provincial de Antabamba, llegando a un total de 43 funcionarios municipales.

De donde una población de estudio “es la agrupación de cosas, eventos o sujetos que presentan atributos particulares y que encuentran en un espacio determinado a partir de las mismas se lograran información de manera generalizada” (Hernández y colaboradores, p. 174).

4.4.2 Muestra

La muestra de un estudio de acuerdo a lo manifestado por Hernández et al. (2014), “es un subconjunto de eventos exactamente representados de la totalidad que componen una población de la cual se logrará datos que representen el sentir del objeto de estudio” (p. 175).

Por cuanto, la muestra fue puntualizada por el método no probabilístico y la selección de la misma por el método por conveniencia, donde no se aplicaron ningún procedimiento probabilístico para la muestra, y fueron escogidos por sus atributos específicos que presentan cada talento humano, siendo considerados como parte del estudio al total de la población, y además porque la misma es pequeña. Es así que la muestra fueron 43 unidades de análisis.

Señalando, la Consultoría Estratégica de Investigación de Mercados (CIMEC 2023), que el método no probabilístico “es aquel que no da las mismas opciones de ser seleccionados a toda la población”. Además, la selección de los sujetos por conveniencia “es aquel en el cual se eligen a los miembros del estudio por proximidad, sin tener en cuenta si constituyen una muestra representativa o no” (CIMEC, 2023).

4.5 Técnicas e instrumentos para la recolección de datos

4.5.1 Técnica

Para el acopio de datos se manejó la encuesta, donde Pandey y Pandey, (2015) citado por Medina et al. (2023), “es un procedimiento sistemático utilizado para recopilar y analizar información con el fin de resolver un problema o responder a una pregunta de investigación”.

Por tanto, la encuesta fue aquel procedimiento donde las variables problemáticas a partir de sus correspondientes dimensiones fueron el medio para alcanzar a medir el contexto real de GC y de la ciberseguridad en la municipalidad, a partir de los cuales puntualizar el nivel de asociación que pueda existía entre los respectivos constructos en la zona de influencia.

4.5.2 Instrumentos

Fue el cuestionario, sosteniendo Hernández et al. (2014), que la misma “es un cumulo de interrogantes enfocadas a un, o más casos que se pretende medir” (p. 217).

De donde el cuestionario estuvo diseñado con un conjunto de ítems que permitieron evaluar las características específicas de la variable gestión del conocimiento y de la ciberseguridad que se vienen presentando en la municipalidad provincial de Antabamba. Para los cuales se construyeron dos cuestionarios, uno de ellos estaba estructurado para la GC, partiendo de las dimensiones: creación del conocimiento, almacenamiento y transferencia del conocimiento, y aplicación y uso del conocimiento, bajo una escala de medición de opción múltiple: 1: Nunca, 2: Casi nunca, 3: En ocasiones, 4: Casi siempre, y 5: Siempre. Así mismo para la ciberseguridad considerando sus dimensiones: Confidencialidad, Integridad, y Disponibilidad, manejando una escala valorativa de: 1: Nunca, 2: Casi nunca, 3: En ocasiones, 4: Casi siempre, y 5: Siempre.

4.6 Validación y confiabilidad de los instrumentos

4.6.1 Validación

Los instrumentos aplicados en el estudio, fueron sometidos a su respectiva validación por juicio de expertos, quienes analizaron la consistencia, contenido, criterio, concurrencia y predictividad del instrumento para la obtención de datos de la GC y la ciberseguridad que se estuvieron ejecutando en la entidad municipal.

4.6.2 Confiabilidad

Alcanzada la información producto del manejo de los instrumentos, se procedió a medir la consistencia y estabilidad de información, aplicando la prueba estadística de alfa de Cronbach y especificar el grado de confiabilidad de los datos que se reflejó en los resultados obtenidos, llegando a puntualizar la confiabilidad de los instrumentos aplicados que permitieron obtener datos consistentes y robustos para arribar a las conclusiones significativa y la resolución de las variables problemáticas.

Tabla 1

Fiabilidad de los instrumentos por Cronbach

Variable	Confiabilidad de Cronbach
Gestión del conocimiento	0.957
Ciberseguridad	0.948
Fiabilidad de variables	0.952

Nota: Nivel de confiabilidad de los instrumentos, elaboración propia

Al distinguir la tabla 1 se aprecia datos de fiabilidad de los instrumentos manejados, de donde la confiabilidad de alfa de Cronbach es 0.952 de ambos fenómenos problemáticos estudiados, señalando que la misma se encuentra muy cercano a la unidad (1), determinando un nivel de fiabilidad interna muy buena o excelente, indicador que permite sostener cuán consistentes son las preguntas diseñadas y que se encuentran interrelacionadas para medir las respectivas variables problemáticas, permitiendo interpretar los resultados de forma coherente..

4.7. Métodos y técnicas para la presentación y análisis de datos

Todos los datos alcanzados fueron tabulados sistemáticamente en sus correspondientes bases de datos de cada fenómeno y sus respectivas dimensiones, a partir de las cuales se presentan los resultados en tablas y figuras, las que permitieron desarrollar el análisis, interpretación y las discusiones de forma coherente, precisa, clara y concisa, para arribar a las conclusiones y recomendaciones pertinentes y consistentes. Para este procedimiento y entre otros se manejó el software estadístico SPSS 29, Microsoft Excel y Word.

Los procedimientos para el tratamiento de los datos, se efectuaron por intermedio de la estadística descriptiva, tanto para el constructo gestión del conocimiento y la ciberseguridad en mérito a sus correspondientes dimensiones e indicadores, y evaluar el comportamiento de las mismas. Así mismo se utilizó la estadística inferencial para determinar el nivel de asociación entre ambas variables, previamente se desarrolló la prueba de normalidad de los datos, con la intensión de observar la distribución normal o no normal de ellos, para puntualizar la aplicación de los estadísticos paramétricos o no paramétricos y contrastar la hipótesis de investigación.

V. RESULTADOS Y DISCUSIONES

5.1 Resultados descriptivos

5.1.1 Gestión del conocimiento: Variable X

Tabla 2

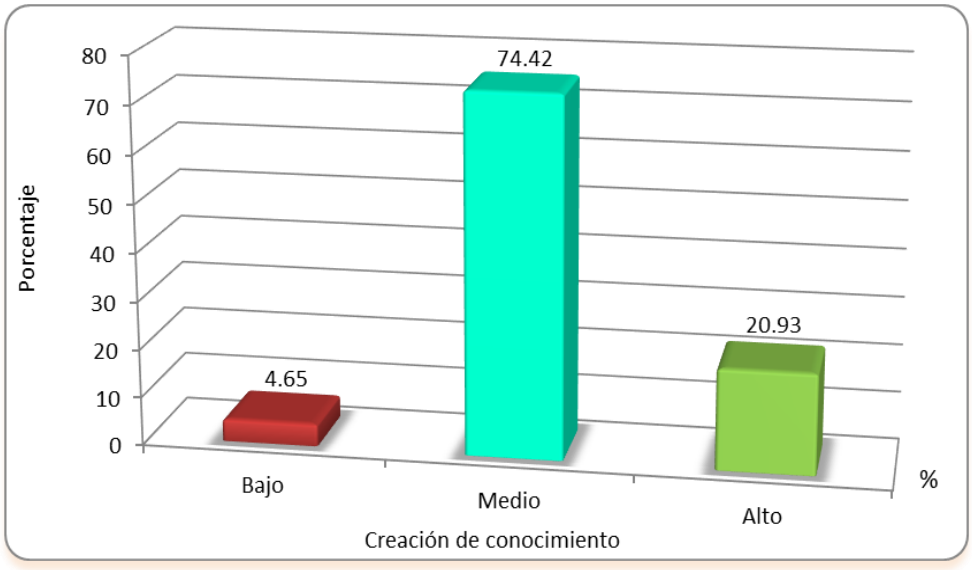
Dimensión creación de conocimiento

Afirmación	f	%	Porcentaje Acumulado
Bajo	2	4.65	4.65
Medio	32	74.42	79.07
Alto	9	20.93	100
Total	43	100	

Nota: Apreciación de creación de conocimiento

Figura 2

Estimación porcentual de la creación de conocimiento



Nota: Creación de conocimiento para la gestión del conocimiento

Análisis e interpretación

En la tabla y figura 2, se desprende que el 74.42% de los empleados supieron señalar medio, un 20.93% indicaron alto y el 4.65% afirmaron bajo la creación de conocimientos para los procesos y manejo de la información en la entidad municipal.

Tabla 3

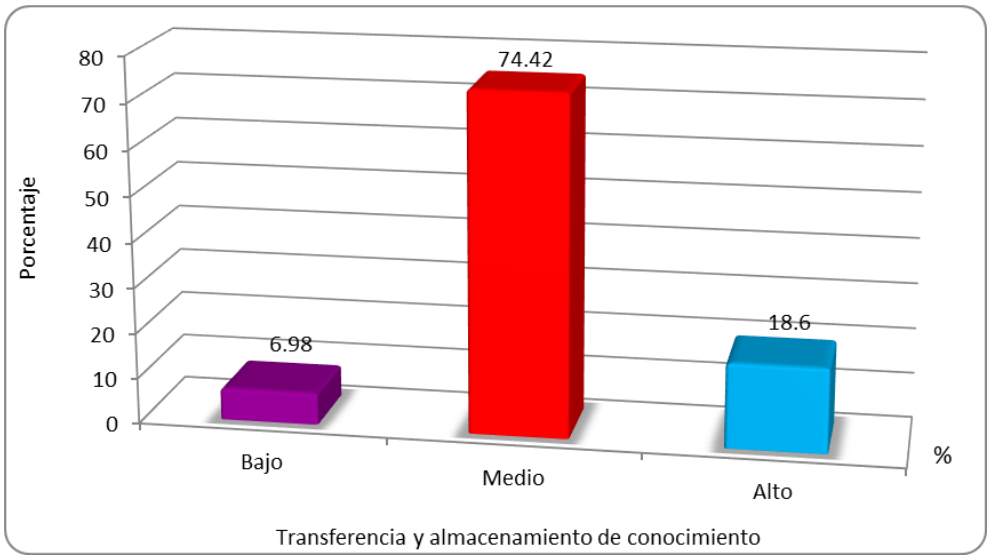
Dimensión transferencia y almacenamiento de conocimiento

Afirmación	f	%	Porcentaje Acumulado
Bajo	3	6.98	6.98
Medio	32	74.42	81.40
Alto	8	18.6	100
Total	43	100	

Nota: Valoración de transferencia y almacenamiento de conocimiento

Figura 3

Estimación porcentual de la transferencia y almacenamiento de conocimiento



Nota: Valor de la transferencia y almacenamiento de conocimiento

Análisis e interpretación

Al llegar a observar la tabla y la respectiva figura 3, se distingue que el 74.42% señalo medio, seguido del 18.6% que manifestó alto y un 6.98% que dijeron bajo la transferencia y almacenamiento de conocimientos entre las distintas dependencias municipales.

Tabla 4

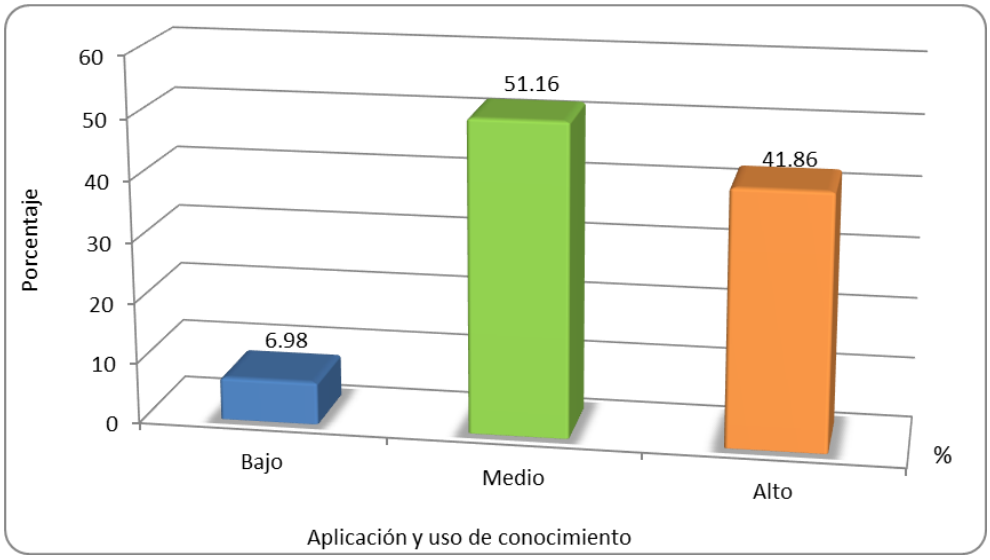
Dimensión aplicación y uso de conocimiento

Afirmación	f	%	Porcentaje Acumulado
Bajo	3	6.98	6.98
Medio	22	51.16	58.14
Alto	18	41.86	100
Total	43	100	

Nota: Evaluación de la aplicación y uso de conocimiento

Figura 4

Evaluación porcentual de la aplicación y uso de conocimiento



Nota: Valoración porcentual de la aplicación y uso de conocimiento

Análisis e interpretación:

La tabla 4 y la figura que antecede, presentan datos de donde el 51.16% de los empleados afirmaron medio, además del 41.86% que dijeron alto y sólo el 6.98% argumentaron bajo la aplicación y uso de conocimiento en los procesos operativos entre los grupos de interés en la entidad municipal.

Tabla 5

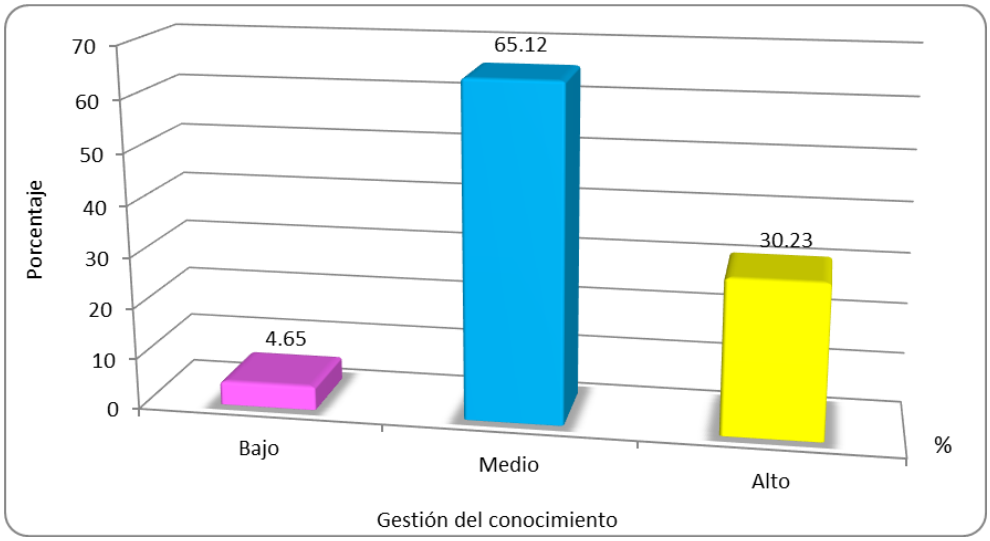
Estimación de la gestión del conocimiento

Afirmación	f	%	Porcentaje Acumulado
Bajo	2	4.65	4.65
Medio	28	65.12	69.77
Alto	13	30.23	100
Total	43	100	

Nota: Nivel de estimación de la gestión del conocimiento

Figura 5

Valoración porcentual de la gestión del conocimiento



Nota: Apreciación porcentual del a gestión de conocimiento

Análisis e interpretación:

En la tabla anterior y la figura 5, se desprende que el 65.12% de los trabajadores municipales afirmaron medio, después el 30.23% indicaron alto y un 4.65% señalo bajo la práctica de la gestión de conocimiento en la municipalidad distrital objeto de estudio.

5.1.2 Ciberseguridad: Variable Y

Tabla 6

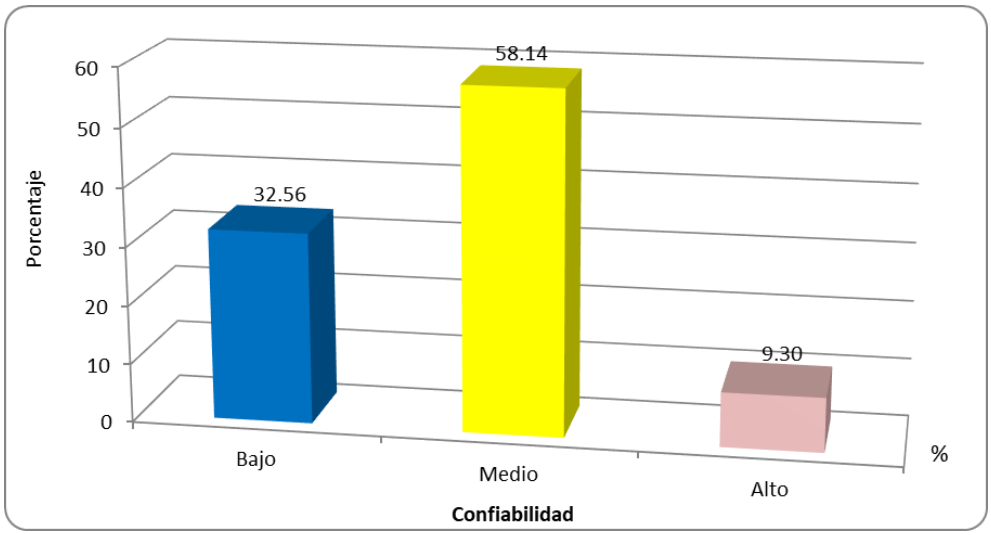
Dimensión confidencialidad de la ciberseguridad

Afirmación	f	%	Porcentaje Acumulado
Bajo	14	32.56	32.56
Medio	25	58.14	90.70
Alto	4	9.30	100
Total	43	100	

Nota: Estimación de la confidencialidad de la ciberseguridad

Figura 6

Valoración porcentual de confidencialidad de la ciberseguridad



Nota: Evaluación porcentual de la confidencialidad de la ciberseguridad

Análisis e interpretación:

Observando la tabla y figura 6, se distingue que el 58.14% del talento humano dijeron medio, así como el 32.56% expresaron bajo y el 9.30% mencionaron alto la confidencialidad de la información y activos de la municipalidad, usados en los procesos para la atención a los vecinos.

Tabla 7

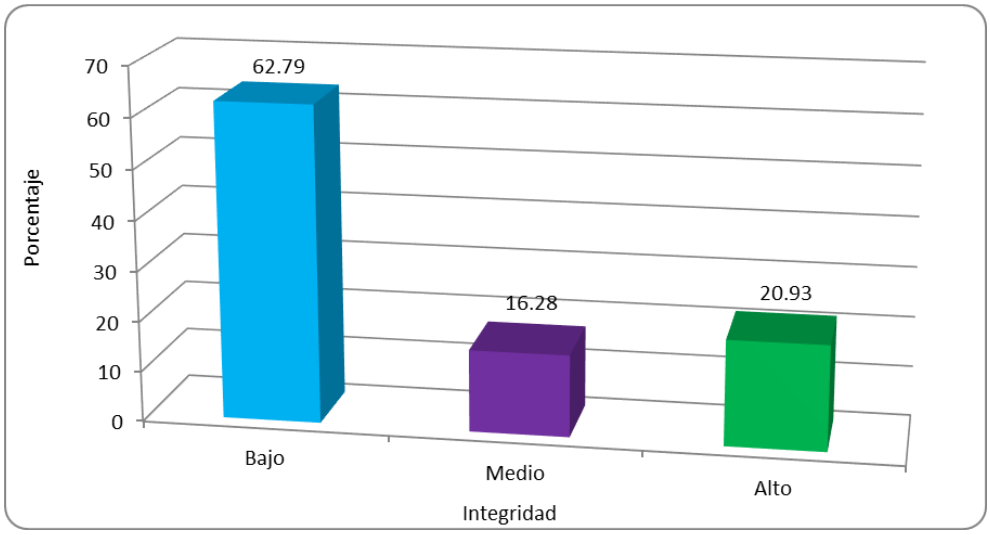
Dimensión de integridad de la ciberseguridad

Afirmación	f	%	Porcentaje Acumulado
Bajo	27	62.79	62.79
Medio	7	16.28	79.07
Alto	9	20.93	100
Total	43	100	

Nota: Apreciación de integridad de la ciberseguridad

Figura 7

Evaluación porcentual de integridad de la ciberseguridad



Nota: Valoración porcentual de integridad de la ciberseguridad

Análisis e interpretación:

Considerando a la tabla y figura que antecede, se expone que el 62.79% de los trabajadores mencionaron bajo, además el 20.93% dijeron alto y un 16.28% manifestaron medio las acciones que se consideran para mantener la integridad de la información municipal.

Tabla 8

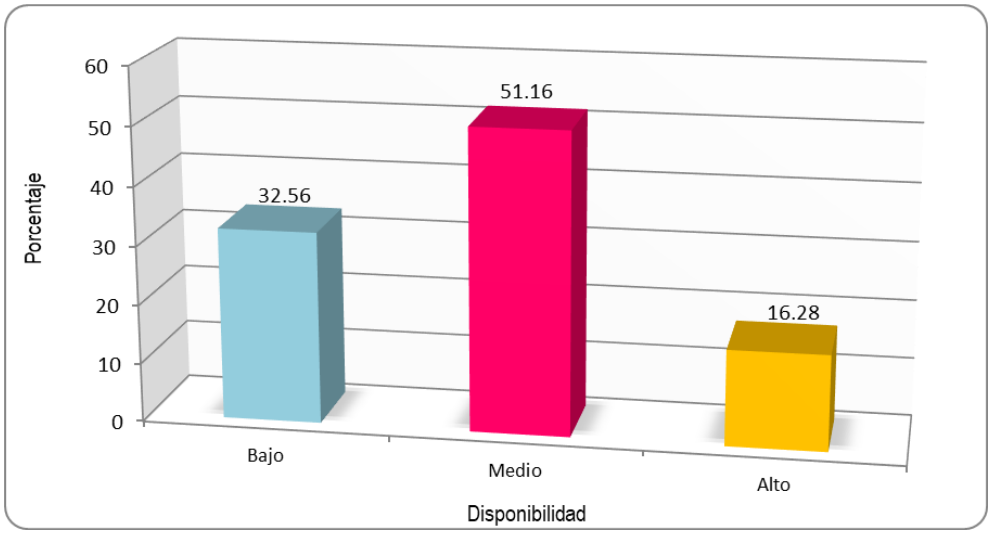
Dimensión disponibilidad de la ciberseguridad

Afirmación	f	%	Porcentaje Acumulado
Bajo	14	32.56	32.56
Medio	22	51.16	83.72
Alto	7	16.28	100
Total	43	100	

Nota: Estimación de la disponibilidad de la ciberseguridad

Figura 8

Valoración porcentual de disponibilidad de la ciberseguridad



Nota: Valor porcentual de disponibilidad de la ciberseguridad

Análisis e interpretación:

A partir de la tabla 8 y su respectiva figura que precede, se distingue que el 51.16% de los empleados apuntaron medio, luego el 32.56% revelaron bajo y el 16.28% indico alto la disponibilidad de los datos requeridos por las distintas áreas de la municipalidad y que se encuentran sujetos a su vulnerabilidad respectiva.

Tabla 9

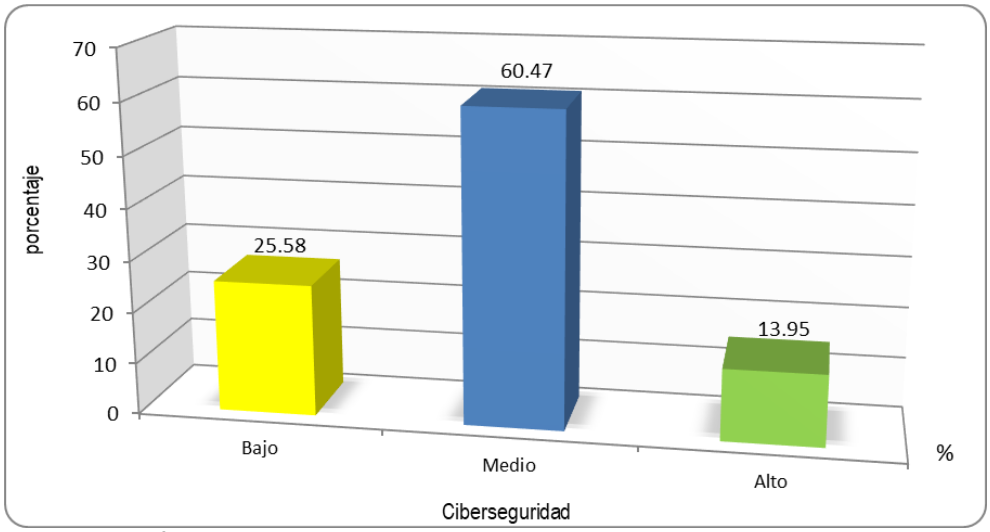
Percepción de la ciberseguridad

Afirmación	f	%	Porcentaje Acumulado
Bajo	11	25.58	25.58
Medio	26	60.47	86.05
Alto	6	13.95	100
Total	43	100	

Nota: Percepción de ciberseguridad

Figura 9

Evaluación porcentual de la ciberseguridad



Nota: Valoración porcentual de la ciberseguridad

Análisis e interpretación:

En la tabla y figura 9 se advierte que, el 60.47% de los trabajadores expusieron medio, además del 25.58% que sostuvo bajo y al final el 13.95% señalo alto las prácticas aplicadas sobre ciberseguridad para resguardar de la información en la entidad municipal distrital objeto de estudio.

5.2 Contrastación de hipótesis

a. Prueba de normalidad de datos del estudio

Tabla 10

Prueba de Shapiro-Wilk

	Shapiro-Wilk		
Variables	Estadístico	Gl	Sig.
Gestión del conocimiento	.969	43	.285
Ciberseguridad	.993	43	.995

Nota: Prueba de normalidad de datos por Shapiro-Wilk

Análisis e interpretación:

En la tabla 10, se aprecia datos de la prueba de normalidad de datos del estadístico de Shapiro-Wilk, en razón de que la muestra son 43 unidades muestrales, encontrándose por debajo de los 50 unidades muestrales consideradas para aplicar el respectivo estadístico; de donde los niveles de sig. de ambas variables son superiores al error 0.05 (sig. 0.285 y 0.995 > 0.05), que establece que los datos presentan el supuesto de distribución de normalidad y que para verificar las hipótesis de estudio se aplicó la prueba paramétrica *r* de Pearson.

b. Contrastación de hipótesis general

Tabla 11

Asociación de la gestión del conocimiento y la ciberseguridad

		Gestión del conocimiento	Ciberseguridad
Gestión del conocimiento	Correlación de Pearson	1	,619**
	Sig. (bilateral)		,000
	N	43	43
Ciberseguridad	Correlación de Pearson	,619**	1
	Sig. (bilateral)	,000	
	N	43	43

Nota: Rango de asociación de la gestión del conocimiento y la ciberseguridad

Análisis e interpretación:

Planteamiento de la hipótesis estadística: Hipótesis nula (Ho), Hipótesis alterna (Ha):

Ho: La gestión del conocimiento no se asocia significativamente con la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Ha: La gestión del conocimiento sí se asocia significativamente con la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Nivel de Significancia: 0.05

r de Pearson : 0.619**

Valor p calculado : 0.000

Conclusión: Toda vez que p < 0.05, se llega a rechazar la hipótesis nula (Ho) y aceptar la hipótesis alterna (Ha), por cuanto se llega a la conclusión que, la gestión del conocimiento sí se asocia significativamente con la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

c. Contrastación de hipótesis específicas

Tabla 12

Asociación de la gestión del conocimiento y la confidencialidad de la ciberseguridad

		Gestión del conocimiento	Confidencialidad
Gestión del conocimiento	Correlación de Pearson	1	,369**
	Sig. (bilateral)		,015
	N	43	43
Confidencialidad	Correlación de Pearson	,369**	1
	Sig. (bilateral)	,015	
	N	43	43

Nota: Rango de asociación de la gestión del conocimiento y la confidencialidad

Análisis e interpretación:

Planteamiento de la hipótesis estadística: Hipótesis nula (Ho), Hipótesis alterna (Ha):

Ho: La gestión del conocimiento no se asocia elocuentemente con la confidencialidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Ha: La gestión del conocimiento sí se asocia elocuentemente con la confidencialidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Nivel de Significancia: 0.05

r de Pearson : 0.369**

Valor p calculado : 0.015

Conclusión: Toda vez que p < 0.05, se llega a rechazar la hipótesis nula (Ho) y aceptar la hipótesis alterna (Ha), por cuanto se llega a la conclusión que, la gestión del conocimiento sí se asocia elocuentemente con la confidencialidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Tabla 13

Asociación de la gestión del conocimiento y la integridad de la ciberseguridad

		Gestión del conocimiento	Integridad
Gestión del conocimiento	Correlación de Pearson	1	,676**
	Sig. (bilateral)		,000
	N	43	43
Integridad	Correlación de Pearson	,676**	1
	Sig. (bilateral)	,000	
	N	43	43

Nota: Rango de asociación de la gestión del conocimiento y la integridad

Análisis e interpretación:

Planteamiento de la hipótesis estadística: Hipótesis nula (Ho), Hipótesis alterna (Ha):

Ho: La gestión del conocimiento no se asocia elocuentemente con la integridad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Ha: La gestión del conocimiento sí se asocia elocuentemente con la integridad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Nivel de Significancia: 0.05

r de Pearson : 0.676**

Valor p calculado : 0.000

Conclusión: Toda vez que p < 0.05, se llega a rechazar la hipótesis nula (Ho) y aceptar la hipótesis alterna (Ha), por cuanto se llega a la conclusión que, la gestión del conocimiento sí se asocia elocuentemente con la integridad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Tabla 14

Asociación de la gestión del conocimiento y la disponibilidad de la ciberseguridad

		Gestión del conocimiento	Disponibilidad
Gestión del conocimiento	Correlación de Pearson	1	,520**
	Sig. (bilateral)		,000
	N	43	43
Disponibilidad	Correlación de Pearson	,520**	1
	Sig. (bilateral)	,000	
	N	43	43

Nota: Rango de asociación de la gestión del conocimiento y la disponibilidad

Análisis e interpretación:

Planteamiento de la hipótesis estadística: Hipótesis nula (Ho), Hipótesis alterna (Ha):

Ho: La gestión del conocimiento no se asocia elocuentemente con la disponibilidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Ha: La gestión del conocimiento sí se asocia elocuentemente con la disponibilidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

Nivel de Significancia : 0.05

r de Pearson : 0.520**

Valor p calculado : 0.000

Conclusión: Toda vez que p < 0.05, se llega a rechazar la hipótesis nula (Ho) y aceptar la hipótesis alterna (Ha), por cuanto se llega a la conclusión que, la gestión del conocimiento sí se asocia elocuentemente con la disponibilidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024.

5.3 Discusiones

A partir de los resultados alcanzados se procede a realizar las discusiones oportunas y llegar al objetivo del estudio; establecer el nivel de asociación de la gestión del conocimiento con la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024. De donde por intermedio de la prueba de correlación r de Pearson cuyo rango fue 0.619 y el *p*-valor alcanzado de 0.000 siendo inferior al nivel de error 0.05, que especifica que la gestión del conocimiento presenta una relación positiva, fuerte y significativamente con la ciberseguridad en la entidad municipal distrital, validando la hipótesis general; ambiente señalado por el 65.12% de los empleados que afirmaron de medio los escenarios de la gestión del conocimiento, enmarcados en la creación, la transferencia y almacenamiento y, la aplicación y uso de conocimientos para que los archivos, informes y toda la información compartida, diseminada y transferida entre las unidades organizacional les permita adquirir conocimientos para cumplir con eficiencia las funciones encomendadas, así como la transferencia, la articulación de información y conocimientos de forma oportuna, concisa y verídica para el cumplimiento de los requerimientos de la comunidad, y las oportunidades brindades para el desarrollo de los escenarios de cooperación, trabajo en equipo y la cultura organizativa en busca de la promoción del personal, del conocimiento y el desarrollo institucional sostenido; contextos que se encuentran concatenadas al 60.47% de los trabajadores que indicaron de medio las prácticas ejecutadas sobre ciberseguridad, en mérito a la confidencialidad, integridad y disponibilidad de las normas, políticas y procedimientos para la protección de la información y activos contra violaciones a la seguridad y la manipulación del tráfico de datos que garanticen la seguridad de la información, además de las capacitaciones, los mecanismos previstos y las medidas de seguridad implementadas para proteger la integridad de los datos que afiancen la precisión, coherencia, exactitud y evitar las modificaciones indebidas de la información, así como de los sistemas y tecnologías de información de la entidad que son vulnerables a la

destrucción, el error, abuso y accesos no autorizados por parte de los internos y externos de la entidad que exige que se diseñen planes de contingencias ante sabotajes de acceso a la información y a los ciberataques.

Resultados encontrados y que se encuentra concordantes con lo señalado por Lazaro y Meza (2022), que, existe una relación muy fuerte de la gestión del conocimiento y la efectividad organizacional, basados en las capacidades, habilidades y conocimientos que ayudan a efectivizar el desempeño. De la misma manera se enmarca a los afirmado por Sanchez (2021), quién dice que, los activos informáticos presentan muchos riesgos debidos las vulnerabilidades con que cuenta y están expuestas al ataque cibernético, y que deben implementarse estrategias para asegurar la continuidad de los procesos y los sistemas informáticos.

Así mismo, los resultados conseguidos en el estudio se encuentran encuadrados a los hallazgos de Manzano y Mul (2020), quienes sostienen que, se deben aplicar estrategias para evitar la rotación del personal, mantener el orden y codificación de la información, desarrollar manuales, estableciendo además mecanismos formales de reconocimiento, y la obtención de un acceso controlado a la información. Así mismo los datos logrados se encuentran consentidos de acuerdo a lo indicado por Piñón et al. (2023), donde, afirman que es necesario llevar a cabo la capacitación y concientización sobre seguridad mediante la elaboración de políticas, la definición de recursos y herramientas y la creación de campañas contra los ataques cibernéticos.

Al final, los resultados encontrados están anidados a los señalados por Payró y Fuentes (2021), quienes asienten que, el perfil tecnológico de la organización, de su personal, y la intervención de un agente externos, fueron determinantes y que facilitaron el compromiso de la alta dirección y la adopción de la gestión de conocimiento en la entidad. Al igual de los resultados de Guevara (2023), donde manifiesta que, los estándares de administración

del saber de la gestión del conocimiento en los servidores revelan un 4% (5) con un nivel bajo, el 28,8% (36) con un nivel medio, y el 67,2% (84) presentaron un nivel alto. De otra parte, la información lograda en el estudio está anidada al de Correa (2021), donde indica que, la ciberseguridad presenta una relación de causalidad sobre la el tratamiento de datos con una estimación de 9.256 y un p valor de significancia de 0.000 de acuerdo a la prueba de Wald.

VI. Conclusiones

Primera.- Se concluye que, el nivel de asociación de la gestión del conocimiento es positiva, fuerte y significativa con la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024; en razón a *r* de Pearson de 0.619 y el *p*-valor encontrado 0.000 que es menor al error de significancia 0.05; contexto reflejado en el 65.12% de los empleados que manifestaron de bueno los procesos de la gestión del conocimiento en virtud a la creación, la transferencia y almacenamiento y, la aplicación y uso del conocimiento, concatenados al 60.47% que valorización de medio las prácticas de ciberseguridad desarrolladas en busca de la confidencialidad, integridad y disponibilidad de la información en la entidad municipal en el cumplimiento de los servicios que brinda a la comunidad.

Segunda.- Se llega a la conclusión que, la gestión del conocimiento se asocia positiva y moderadamente con la confidencialidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024, ambiente señalado por *r* de Pearson de 0.369 y el *p*-valor calculado 0.015 siendo inferior al error 0.05; toda vez que los procesos de la gestión del conocimiento para alcanzar los objetivos en la institución se encuentran interrelacionados al 58.14% de los trabajadores que valoraron de medio la confidencialidad en la seguridad de la información almacenada o en tránsito en la municipalidad.

Tercera.- Además se concluye que, la gestión del conocimiento se asocia positiva y elocuentemente con la integridad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024, entorno afirmado por *r* de Pearson de 0.676 y el *p*-valor logrado 0.000 estando por debajo del error 0.05; en vista que la sistematización de las operaciones de la gestión del conocimiento prácticos se hallan anidados al 62.79% del

talento humano que señalaron de bajo la integridad en la ciberseguridad de los datos desde su creación, captura y manipulación.

Cuarta.- Al final se llega a la conclusión que, la gestión del conocimiento se asocia positiva y moderadamente con la disponibilidad de la ciberseguridad en la municipalidad provincial de Antabamba, Apurímac 2024, ambiente sostenido por *r* de Pearson de 0.520 y el *p*-valor calculado 0.000 hallándose por debajo del error 0.05; en razón a que el tratamiento de la gestión del conocimiento para el logro de las metas organizacionales se encuentra correlacionadas con el 51.16% de los colaboradores que especificaron de medio la disponibilidad en la ciberseguridad de los datos se encuentren accesibles y operativos cuando estos sean requeridos en la entidad.

VII. RECOMENDACIONES

Primera.- A las autoridades del gobierno municipal provincial de Antabamba, se les recomienda establecer y poner en práctica planes de mejora continua para el fortalecimiento de la gestión del conocimiento asociadas a la ciberseguridad de los datos, fomentando la generación, aplicación y transferencia de conocimiento entre los colaboradores y garantizar la protección de la información personal, institucional, financiera y entre otros datos sensibles frente a accesos no autorizados, fraudes, malware y ataques cibernéticos, permitiendo ofrecer productos y servicios de mayor calidad.

Segunda.- A los gerentes y responsables de los sistemas y tecnologías de información, deben generar acciones para la expansión de la gestión del conocimiento que les permitirá optimizar el manejo y la reducción de tiempos dedicados a la búsqueda de información asociados directamente a la confidencialidad de datos para protegerlos contra accesos, la autenticación de usuarios, el cifrado y evitar el acceso no autorizado.

no autorizados datos en la ciberseguridad.

Tercera.- Al talento humano de la oficina de tecnologías de información, se recomienda generar estrategias tendientes a robustecer los procesos de la gestión del conocimiento implementando plataformas colaborativas que les permitirán la creación, el intercambio y uso de conocimientos y que estén concatenadas directamente con la integridad de la información para asegurar la fiabilidad, validez y protección de los datos contra cualquier variación o modificación no autorizadas y sean usadas de forma errónea y fines maliciosos.

Cuarta.- Al final se recomienda a los gobiernos locales provinciales y/o distritales, al talento humano de los mismos, a los responsables de las tecnologías de información y comunicación, deberán desarrollar programas enfocados en la innovación de la gestión del conocimiento y tener acceso al conocimiento oportuno, relevante y pertinente para la toma de decisiones más informadas y estratégicas, concordantes a la disponibilidad de

los recursos informáticos que garantizaran la seguridad de la información, evitando interrupciones o pérdida de datos y la continuidad de las procesos operativos, y la productividad de la entidad municipal.

VIII. REFERENCIAS

Age2 (2024). *Ciberseguridad: ¿Qué es y cuál es su importancia?* [Internet], [consultado el 22/11/2024] y disponible en: https://www.age2.es/noticias/ciberseguridad-que-es-y-cual-es-importancia/#:~:text=Tiene%20como%20funci%C3%B3n%20proteger%20de,trav%C3%A9s%20de%20servicios%20de%20ciberseguridad.

Bustamante, M. (2023). *Características de una buena estrategia de ciberseguridad*. [Internet], [consultado el 24/11/2024] y disponible en: https://ceupe.com.ar/blog/caracteristicas-de-una-buena-estrategia-de-ciberseguridad/

Bustelo, G. (2024). *Panorámica de la ciberseguridad en Latinoamérica: una coyuntura singular*. [Internet], [consultado el 18/11/2024] y disponible en: https://www.segurilatam.com/ciberilatam/ciberseguridad-ciberilatam/panoramica-de-la-ciberseguridad-en-latinoamerica-una-coyuntura-singular_20240612.html#:~:text=Los%20problemas%20de%20ciberseguridad%20en,invertir%20en%20tecnolog%C3%ADas%20de%20seguridad.

Briceño, B., Strand, K. y Marshall, M. (2020). *La gestión del conocimiento: recursos y oportunidades*. [Internet], [consultado el 11/11/2024] y disponible en: https://blogs.iadb.org/conocimiento-abierto/es/gestion-conocimiento-recursos/

Cohen, A. (2024). *Gestión del conocimiento: qué es, procesos y ejemplos*. [Internet], [consultado el 26/11/2024] y disponible en: https://blog.hubspot.es/marketing/gestion-del-conocimiento

Consultoría Estratégica de Investigación de Mercados (2023). *Muestreo probabilístico y no probabilístico*. [Internet], [consultado el 28/11/2024] y disponible en: https://www.cimec.es/muestreo-probabilistico-y-no-probabilistico/

Copaz, Arandia, R.A. (2022). *Análisis del concepto gestión del conocimiento: una mirada desde América latina en el último Quinquenio*. [Internet], [consultado el 15/11/2024] y disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2521-27372022000100010

Corma, P. (2018). *La gestión del conocimiento como asignatura pendiente en innovación*. [Internet], [consultado el 12/11/2024] y disponible en:

https://directivosygerentes.es/management/noticias-management/gestion-conocimiento-innovacion

Correa, Coronel, M.M. (2022). *Ciberseguridad y su incidencia en el Tratamiento de Datos Personales en una Municipalidad Distrital de Lima Sur, 2021*. [Internet], [consultado el 17/11/2024] y disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/85975/Correa_CMM-SD.pdf?sequence=1&isAllowed=y

Ey México (2023). *Panorama de ciberseguridad en Latinoamérica: ¿qué riesgos enfrentan las empresas?* [Internet], [consultado el 18/11/2024] y disponible en: https://www.ey.com/es_pe/insights/cybersecurity/panorama-ciberseguridad-latinoamerica-riesgos-enfrentan-empresas

Flores-Carretero, E. (s.f.). *7 características de la gestión del conocimiento que puedes aprovechar para tener una ventaja competitiva*. [Internet], [consultado el 20/11/2024] y disponible en: https://www.ieie.eu/la-gestion-del-conocimiento/

Guevara, Alarcon, T. D. (2023). *La gestión del conocimiento en los trabajadores de la municipalidad distrital de José Leonardo Ortiz, 2022*. [Internet], [consultado el 16/11/2024] y disponible en: https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/12702/guevara_atd.pdf?sequence=1&isAllowed=y

Hernández-Sampieri, R., Fernández-Collado, C. y Baptista-Lucio, P. (2014). *Metodología de la investigación*. sexta edición. Editorial McGraw-Hill Interamericana. México.

IBM (2022). *¿Qué es la gestión del conocimiento?* [Internet], [consultado el 20/11/2024] y disponible en: https://www.ibm.com/es-es/topics/knowledge-management

Incibe (2020). *Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario*. [Internet], [consultado el 27/11/2024] y disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Infosecurity México (2024). *Ciberseguridad: Una guía completa del concepto, tipos, amenazas y estrategias.* [Internet], [consultado el 23/11/2024] y disponible en: https://www.infosecuritymexico.com/es/ciberseguridad.html

Kaspersky (2024). *¿Qué es la ciberseguridad?* [Internet], [consultado el 26/11/2024] y disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?srsltid=AfmBOorWIiIu8ML7neRvtarx-IREKNbuxamrzQS1PY6IsaXKl5GtFla9

Krzyzanowski, A., Nucci, R. y Sevilla, D. (2024). *Qué es un proceso de gestión del conocimiento?* [Internet], [consultado el 21/11/2024] y disponible en: https://www.getguru.com/es/reference/knowledge-management-process

Krzyzanowski, A., Nucci, R. y Sevilla, D. (2024a). *Las mejores herramientas de gestión del conocimiento para usar en 2024*. [Internet], [consultado el 21/11/2024] y disponible en: https://www.getguru.com/es/reference/knowledge-management-tools

Lazaro, Cabanillas, A.J. y Meza-Garcia, O.Y. (2022). *Gestión del conocimiento y efectividad organizacional en la municipalidad distrital de punta hermosa – 2021*. [Internet], [consultado el 18/11/2024] y disponible en: https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/2216/Lazaro%20Cabanillas%2C%20A.%20J.%2C%20%26%20Meza%20Garcia%2C%20O.%20Y..pdf?sequence=1&isAllowed=y

Manzano, Santana, Á.G., Y Mul-Encalada, J. (2020). *La Gestión del Conocimiento en las Mipymes: Caso de una Consultora en Yucatán, México*. [Internet], [consultado el 16/11/2024] y disponible en: https://www.researchgate.net/publication/355513838_La_Gestion_del_Conocimiento_en_las_Mipymes_Caso_de_una_Consultora_en_Yucatan_Mexico

Medina, Romero, M., Rojas-León, R., Bustamante-Hoces, W., Loaiza-Carrasco, R. Martel-Carranza, Chr., y Castillo-Acobo, R. (2023). *Metodología de la investigación técnicas e instrumentos de investigación*. [Internet], [consultado el 28/11/2024] y disponible en: https://editorial.inudi.edu.pe/index.php/editorialinudi/catalog/download/90/133/157?inline=1

Mera, López, R.J. (2021). *La gestión del conocimiento en el Programa de Fortalecimiento de Emprendimientos e Iniciativas Productivas Locales del Gobierno Provincial de Imbabura*. [Internet], [consultado el 16/11/2024] y disponible en: https://repositorio.uasb.edu.ec/bitstream/10644/7992/1/T3464-MGD-Mera-La%20gestion.pdf

Microsoft (2023). *¿Qué es la ciberseguridad?*. [Internet], [consultado el 23/11/2024] y disponible en: https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-

ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390#:~:text=La%20ciberseguridad%2C%20tambi%C3%A9n%20conocida%20como,fotos%20e%20incluso%20el%20dinero.

Olarte, Quispe, P.B. (2021). *Seguridad informática y la vulnerabilidad del sistema de información inalámbrico en la Municipalidad Provincial de La Convención, periodo 2020.* [Internet], [consultado el 18/11/2024] y disponible en: http://repositorio.ulp.edu.pe/bitstream/handle/ULP/49/T142_73185092_B_PAUL%20OLARTE.pdf?sequence=1&isAllowed=y

Ortega, K. (2024). *¿Cuáles son los objetivos de la ciberseguridad?*. [Internet], [consultado el 22/11/2024] y disponible en: https://worldcampus.saintleo.edu/blog/estudiar-ciberseguridad-en-linea-objetivos-de-la-ciberseguridad

Payró, Campos, P. y Fuentes-Vasconcelos, F.I. (2021). *Gestión de conocimiento en una empresa de desarrollo de software.* [Internet], [consultado el 15/11/2024] y disponible en DOI: https://doi.org/10.46589/rdiasf.vi36.422

Personio (2024). *Gestión del conocimiento: ¿por qué es tan importante para las empresas?*. [Internet], [consultado el 20/11/2024] y disponible en: https://www.personio.es/glosario/gestion-del-conocimiento/#cul-es-la-importancia-de-una-adecuada-gestin-del-conocimiento.

Piñón, L.C., Sapién, A.L. y Gutiérrez. M. del C. (2023). *Capacitación en ciberseguridad en una empresa mexicana*. [Internet], [consultado el 16/11/2024] y disponible en: https://www.scielo.cl/pdf/infotec/v34n6/0718-0764-infotec-34-06-43.pdf

Quiroa, M. (2021). *Gestión del conocimiento*. [Internet], [consultado el 27/11/2024] y disponible en: https://economipedia.com/definiciones/gestion-del-conocimiento.html#google_vignette

Rodriguez, B. (2020). *¿Cómo contribuye la Gestión del conocimiento en la nueva realidad?*. [Internet], [consultado el 18/11/2024] y disponible en: https://www.djcs.com.ve/blog/2008-como-contribuye-la-gestion-del-conocimiento-en-la-nueva-realidad

Sanchez, Vela, M.A. (2021). *Elaboración de un plan de seguridad informática para mejorar la gestión de la información de la sub gerencia de tecnología de la información, de la municipalidad provincial de requena – 2021*. [Internet], [consultado el 19/11/2024] y

disponible en: http://repositorio.ucp.edu.pe/items/b1e67aa4-2b7b-460b-b8e8-305496114c31

Sánchez, Durán, J.A. (2024). *Introducción a la ciberseguridad: Capítulo 3*. [Internet], [consultado el 25/11/2024] y disponible en: https://club-ciso.aec.es/las-dimensiones-fundamentales-en-ciberseguridad/

Stewart, L. (2024). *Investigación básica vs. Aplicada*. [Internet], [consultado el 27/11/2024] y disponible en: https://atlasti.com/es/research-hub/investigacion-basica-vs-aplicada?_gl=1*nwkpnu*_up*MQ..*_ga*MTQ2NjczMDA4NC4xNzMzODQ0MTk5*_ga_K459D5HY8F*MTczMzg0NDE5OC4xLjAuMTczMzg0NDE5OC4wLjAuMA.

Tarí, Guillo, J.J. y García-Fernández, M. (2009). *Dimensiones de la gestión del conocimiento y de la gestión de la calidad: una revisión de la literatura*. [Internet], [consultado el 22/11/2024] y disponible en: https://www.researchgate.net/publication/43529442_Dimensiones_de_la_gestion_del_conocimiento_y_de_la_gestion_de_la_calidad_una_revision_de_la_literatura

Universidad Tecnológica del Perú (2023). *Ciberseguridad: ¿Qué es y en qué consiste?*. [Internet], [consultado el 22/11/2024] y disponible en: https://www.utp.edu.pe/blog/ingenieria-y-arquitectura/ciberseguridad-que-es-y-en-que-consiste?gad_source=1&gclid=Cj0KCQiAgdC6BhCgARIsAPWNWH0Yr6oNwWZhfgwJpo9ypDeQxVFwKHM3K3NROO8QJCDdz6bO9zTw20aAkHYEALw_wcB&gclsrc=aw.ds

Vitale, Alfonso, A.M., Fernández-Vidal, E. y Cabrera-Soto, M. (2020). *Importancia de la gestión del conocimiento para la creación de valor en las empresas cubanas.* [Internet], [consultado el 12/11/2024] y disponible en: https://portal.amelica.org/ameli/journal/129/1292434006/html/

Zendesk (2023). *¿Qué es la gestión del conocimiento?*. [Internet], [consultado el 20/11/2024] y disponible en: https://www.zendesk.com.mx/blog/que-es-gestion-del-conocimiento/

Los anexos, panel fotográfico y otros documentos están resguardados en la oficina de repositorio digital institucional en la Biblioteca Central de la Universidad Tecnológica de los Andes