



Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería Informática

Protección de datos y seguridad informática en los sistemas de gestión de la Municipalidad
del Distrito de Carquin – 2025

Tesis

Para optar el Título Profesional de Ingeniero Informático

Autor

Cesar Yair Melendez Panana

Asesor

Ing. Julio Enrique Guerrero Hurtado



Huacho – Perú

2026



Reconocimiento - No Comercial – Sin Derivadas - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

Reconocimiento: Debe otorgar el crédito correspondiente, proporcionar un enlace a la licencia e indicar si se realizaron cambios. Puede hacerlo de cualquier manera razonable, pero no de ninguna manera que sugiera que el licenciante lo respalda a usted o su uso. **No Comercial:** No puede utilizar el material con fines comerciales. **Sin Derivadas:** Si remezcla, transforma o construye sobre el material, no puede distribuir el material modificado. **Sin restricciones adicionales:** No puede aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros de hacer cualquier cosa que permita la licencia.



UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

(Resolución de Consejo Directivo N° 012-2020-SUNEDU/CD de fecha 27/01/2020)

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería Informática

INFORMACION DE METADATOS

DATOS DEL AUTOR (ES):		
APELLIDOS Y NOMBRES:	DNI	FECHA DE SUSTENTACIÓN
Cesar Yair Melendez Panana	70253713	20 de julio 2026
DATOS DEL ASESOR:		
Apellidos y Nombres:	DNI	CÓDIGO ORCID
Julio Enrique Guerrero Hurtado	15580855	https://orcid.org/0000-0001-5717-3648
DATOS DE LOS MIEMBROS DE JURADOS – PREGRADO:		
APELLIDOS Y NOMBRES:	DNI	CÓDIGO ORCID
Teodorico Jamanca Alberto	15604418	https://orcid.org/0000-0002-9739-6683
Erlo Wilfredo Lino Escobar	15608475	https://orcid.org/0000-0003-4889-6646
Ronald Demetrio Flores Flores	15300224	https://orcid.org/0000-0003-4211-7285

CESAR YAIR MELENDEZ PANANA

Protección de Datos y Seguridad Informática en los sistemas de gestión de la Municipalidad de Carquin - 2025

UNIDAD DE INVESTIGACIÓN FIISI - PREGRADO 2026
Unidad de Investigación de la FIISI - 2026
Facultad de Ingeniería Industrial, Sistemas e Informática

Detalles del documento

Identificador de la entrega

trn:oid::1:3601129200

Fecha de entrega

24 jun 2026, 7:00 p.m. GMT-5

Fecha de descarga

24 jun 2026, 7:07 p.m. GMT-5

Nombre del archivo

Melendez_Panana_Cesar_Yair.pdf

Tamaño del archivo

966.1 KB

88 páginas

17.567 palabras

107.795 caracteres



Página 1 de 90 - Portada

Identificador de la entrega: trn:oid::1:3601129200



Página 2 de 90 - Descripción general de integridad

Identificador de la entrega: trn:oid::1:3601129200

20% Similitud general

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

Filtrado desde el informe

- Bibliografía
- Coincidencias menores (menos de 10 palabras)

Exclusiones

- N.º de coincidencias excluidas

Fuentes principales

- 10% Fuentes de Internet
- 5% Publicaciones
- 11% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

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.

DEDICATORIA

A Dios, por ser el faro que ilumina mi camino y otorgarme la perseverancia necesaria para culminar esta meta profesional. A mis padres, por su inagotable sacrificio, amor incondicional y por ser el pilar fundamental en mi formación; este logro es el reflejo de todo su esfuerzo. A mi familia y amigos, que con sus palabras de aliento y compañía me motivaron a superar cada desafío en esta etapa universitaria.

Melendez Panana Cesar Yair

AGRADECIMIENTO

Agradezco profundamente a Dios por la sabiduría y fortaleza brindada en este camino, y a mi universidad, docentes y asesor, por su invaluable formación y guía profesional durante el desarrollo de esta investigación. Asimismo, extendiendo mi gratitud a los trabajadores de la Municipalidad de Carquin por las facilidades otorgadas para la recolección de información, y a mi familia por su apoyo incondicional y aliento constante, factores que hicieron posible la culminación de este importante logro académico.

Melendez Panana Cesar Yair

ÍNDICE

DEDICATORIA.....	II
AGRADECIMIENTO	III
INDICE	IV
INDICE DE TABLAS.....	VI
INDICE DE GRAFICOS.....	VII
RESUMEN	VIII
ABSTRACT.....	X
INTRODUCCIÓN	XII
I. CAPITULO I: PLANTEAMIENTO DEL PROBLEMA	13
1.1. Descripción de la realidad problemática	13
1.2. Formulación del problema	14
1.2.1. Problema general	14
1.2.2. Problemas específicos.....	15
1.3. Objetivos de la investigación	15
1.3.1. Objetivo general	15
1.3.2. Objetivos específicos	15
1.4. Justificación de la investigación	16
1.5. Delimitación del estudio.....	18
1.6. Viabilidad del Estudio.....	19
II. CAPITULO II: MARCO TEORICO	21
2.1. Antecedentes de la investigación	21
2.1.1. Investigaciones internacionales.....	21
2.1.2. Investigaciones nacionales.....	22
2.2. Bases teóricas	23
2.3. Definición de términos básicos.....	42
2.4. Hipótesis de investigación	48
2.4.1. Hipótesis general	48
2.4.2. Hipótesis específicas	48
2.5. Operacionalización de Variable e Indicadores.....	49
III. CAPITULO III: METODOLOGIA DE LA INVESTIGACION	50
3.1. Diseño metodológico	50

3.2.	Población y muestra.....	52
3.2.1.	Población.....	52
3.2.2.	Muestra.....	52
3.3.	Técnicas de recolección de datos	53
IV.	CAPITULO IV: RESULTADOS.....	55
4.1.	Análisis de Resultados	55
4.1.1.	Resultados de Protección de Datos y sus dimensiones.....	55
4.1.2.	Resultados de Seguridad Informática y sus dimensiones.....	61
4.2.	Contrastación de Hipótesis.....	67
4.2.1.	Contrastación de Hipótesis General.....	67
4.2.2.	Contrastación de Hipótesis Específica 1.....	68
4.2.3.	Contrastación de Hipótesis Específica 2.....	69
4.2.4.	Contrastación de Hipótesis Específica 3.....	71
V.	CAPITULO V: DISCUSIÓN.....	73
5.1.	Discusión de Resultados	73
VI.	CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES	75
6.1.	Conclusiones.....	75
6.2.	Recomendaciones	77
VII.	REFERENCIAS.....	77
7.1.	Fuentes bibliográficas.....	79
VIII.	ANEXOS	80
8.1.	MATRIZ DE CONSISTENCIA	80
8.2.	CUESTIONARIO.....	83

INDICE DE TABLAS

<i>Tabla 1</i>	<i>Protección de Datos</i>	<i>55</i>
<i>Tabla 2</i>	<i>Categoría Políticas de Protección de Datos.....</i>	<i>56</i>
<i>Tabla 3</i>	<i>Categoría Control de Acceso a la Información</i>	<i>58</i>
<i>Tabla 4</i>	<i>Categoría Manejo y Tratamiento de Datos</i>	<i>59</i>
<i>Tabla 5</i>	<i>Seguridad Informática</i>	<i>61</i>
<i>Tabla 6</i>	<i>Categoría Confidencialidad.....</i>	<i>62</i>
<i>Tabla 7</i>	<i>Categoría Integridad</i>	<i>64</i>
<i>Tabla 8</i>	<i>Categoría Disponibilidad.....</i>	<i>65</i>

INDICE DE GRAFICOS

<i>Gráfico 1</i>	<i>Protección de Datos</i>	55
<i>Gráfico 2</i>	<i>Políticas de Protección de Datos</i>	57
<i>Gráfico 3</i>	<i>Control de Acceso a la Información</i>	58
<i>Gráfico 4</i>	<i>Manejo y Tratamiento de Datos</i>	60
<i>Gráfico 5</i>	<i>Seguridad Informática</i>	61
<i>Gráfico 6</i>	<i>Confidencialidad</i>	63
<i>Gráfico 7</i>	<i>Integridad</i>	64
<i>Gráfico 8</i>	<i>Disponibilidad</i>	66

RESUMEN

El presente trabajo de investigación tuvo como objetivo principal determinar la relación entre la protección de datos y la seguridad informática en los sistemas de gestión de la Municipalidad de Carquin durante el año 2025. El estudio se desarrolló bajo un enfoque cuantitativo, con un diseño no experimental, de corte transversal y de nivel correlacional. La muestra poblacional estuvo conformada por 92 trabajadores de la institución, a quienes se les aplicó un cuestionario estructurado tipo Likert para evaluar su percepción sobre los mecanismos de resguardo y control de la información institucional. El análisis de los datos mediante el coeficiente de correlación de Spearman reveló una correlación positiva fuerte ($\rho = 0.612$; $p < 0.001$) entre las variables primarias. En el contexto de las dimensiones de seguridad de la información, la protección de datos muestra una relación correlacional significativa con la confidencialidad, integridad y una menor correlación con la disponibilidad de los sistemas. El análisis indica que el manejo adecuado de la información personal y sensible tiene un respaldo legal y sirve como una medida de protección para los sistemas de información de la organización. Considerando los resultados, se sugiere que las autoridades municipales lleven a cabo la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001, así como la adopción de “Zero Trust” para combatir las amenazas a la seguridad de la información y garantizar la operación ininterrumpida de las funciones del servicio público.

Palabras Clave

Protección de datos, seguridad informática, confidencialidad, integridad, disponibilidad, sistemas de gestión, ciberseguridad.

ABSTRACT

The main objective of this research work was to determine the relationship between data protection and information security in the management systems of the Municipality of Carquin during the year 2025. The study was developed under a quantitative approach, using a non-experimental, cross-sectional, and correlational design. The sample consisted of 92 institutional workers, who completed a structured Likert-type questionnaire designed to assess their perception of the safeguarding and control mechanisms of institutional information. The statistical results, analyzed using the Spearman correlation coefficient, demonstrated the existence of a moderate and highly significant positive relationship ($\rho = 0.612$; $p < 0.001$) between the main variables. When evaluating the dimensions of information security, it was found that data protection has a direct and significant link with confidentiality ($\rho = 0.592$), integrity ($\rho = 0.543$), and, to a lesser extent, system availability ($\rho = 0.424$). It is concluded that the proper management of personal and sensitive data is not only a legal requirement but a strategic component that strengthens the technical robustness of the entity. Based on the findings, it is recommended that the municipal administration institutionalize an Information Security Management System (ISMS) aligned with the ISO/IEC 27001 standard, as well as the adoption of a "Zero Trust" architecture to mitigate vulnerabilities and guarantee the continuity of public services.

Keywords

Data protection, information security, confidentiality, integrity, availability, management systems, cybersecurity.

INTRODUCCIÓN

Con la rápida transformación digital, el sector público equilibra la modernización tecnológica con la protección de la información en su posesión. Mientras que la digitalización ha agilizado los procesos del sector público, ha aumentado el riesgo de ciberataques. En consecuencia, la protección de la información y la salvaguarda de los canales digitales han pasado progresivamente de ser meramente una preocupación tecnológica a ser el núcleo de cualquier sistema de gobierno y confianza de los ciudadanos.

A nivel mundial y nacional, la mayoría de los gobiernos locales son víctimas de ciberataques debido a la falta de un marco, un control de acceso deficiente y la ausencia de una cultura de seguridad cibernética. El gobierno local de Carquín no es diferente y debe operar sistemas de gestión cargados de datos administrativos, financieros y personales que necesitan un espacio digital seguro para operar. La protección insuficiente del espacio digital es una amenaza importante para la privacidad de los usuarios, la integridad de los datos y registros, y la disponibilidad continua de servicios al público.

Ante este contexto, este estudio aspira a explorar el nexo entre la protección de la información y la protección cibernética de los sistemas de gestión del gobierno local de Carquín para el año 2025. Este estudio busca proporcionar datos preliminares sobre el estado actual de la protección cibernética en el gobierno local y, más importante aún, busca ofrecer una base para el diseño de sistemas formales de protección cibernética, mejorando así la gestión digital segura, ética y efectiva del gobierno local.

I. CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

Actualmente, las entidades públicas están digitalizando rápidamente sus sistemas de gestión. Esta digitalización implica el uso creciente de plataformas de tecnología de la información (TI) para gestionar recursos, brindar servicios a los ciudadanos, registrar información administrativa y apoyar la toma de decisiones institucionales. En consecuencia, las entidades públicas dependen cada vez más de los sistemas de TI. Por lo tanto, la protección de datos y la ciberseguridad son fundamentales para garantizar una gestión eficiente, transparente y confiable de los servicios públicos.

Desde una perspectiva global, muchos ciberataques, incidentes de hacking, robos de información y manipulación de datos se concentran en los gobiernos locales y municipales. Una protección de datos inadecuada puede poner en riesgo los datos personales sensibles de millones de ciudadanos y puede poner en peligro el sistema de gestión. Estos eventos generan costos económicos y operativos y, aún más importante, erosionan la confianza de los ciudadanos en los servicios públicos.

La situación existente en Perú a nivel nacional muestra un estado deficiente de ciberseguridad y una falta de protección de datos a nivel municipal. Numerosos informes y otros análisis realizados a nivel institucional muestran que muchos gobiernos locales no implementan políticas de protección y seguridad de datos, no disponen de protocolos de seguridad y no cuentan con medidas de control o capacitación suficientes en ciberseguridad básica para el personal. Estas carencias ponen en riesgo los sistemas de gestión del gobierno local ante brechas de información, modificaciones en los registros y accesos no autorizados.

La Municipalidad de Carquín no es ajena a estos asuntos a nivel local. Sus sistemas para administración, impuestos, logística, recursos humanos y servicios ciudadanos dependen del acceso constante a información digital. Sin embargo, se han detectado problemas con la protección de datos personales, la seguridad de la información digital, la integridad de la información y la disponibilidad constante de los servicios digitales. Estos problemas afectan negativamente al correcto funcionamiento de la institución y a la calidad de los servicios que se pueden brindar a la población.

Además, la falta de protección básica en ciberseguridad, como controles de acceso, copias de seguridad de la información, monitoreo de sistemas y recuperación de incidentes que afectan la información institucional, aumenta la probabilidad de errores en los procesos administrativos, de que se genere información no confiable o incompleta y de decisiones formuladas sin cuidado, lo que resulta en retrasos interminables en la gestión de la Municipalidad.

El problema principal es la ausencia de un marco de protección básico para los datos y la ciberseguridad en los sistemas de gestión que emplea la Municipalidad de Carquín. Esta falla abarca la protección de datos, la integridad y la disponibilidad, y resulta en una pérdida de confianza de los ciudadanos en la administración. Es necesario realizar una investigación en 2025 para analizar la protección de datos y la ciberseguridad de los sistemas de gestión municipal con el fin de apoyar la mejora de la gestión pública local.

1.2. Formulación del problema

1.2.1. Problema general

¿Qué relación existe entre la protección de datos y la seguridad informática en los sistemas de gestión de la Municipalidad de Carquin, 2025?

1.2.2. Problemas específicos

¿Cómo se relaciona la protección de datos con la confidencialidad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025?

¿De qué manera la protección de datos se relaciona con la integridad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025?

¿Qué relación existe entre la protección de datos y la disponibilidad de los sistemas de gestión de la Municipalidad de Carquin, 2025?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Determinar la relación entre la protección de datos y la seguridad informática en los sistemas de gestión de la Municipalidad de Carquin, 2025.

1.3.2. Objetivos específicos

Analizar la relación entre la protección de datos y la confidencialidad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025.

Evaluar la relación entre la protección de datos y la integridad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025.

Examinar la relación entre la protección de datos y la disponibilidad de los sistemas de gestión de la Municipalidad de Carquin, 2025.

1.4. Justificación de la investigación

La investigación actual se justifica por la importancia cada vez mayor que han alcanzado la seguridad informática y la protección de datos en las instituciones públicas, en particular en los gobiernos locales. En estos últimos, los sistemas de gestión informática son esenciales para administrar recursos, atender a los ciudadanos y tomar decisiones institucionales dentro del contexto de transformación digital. La Municipalidad de Carquín maneja información sensible y datos personales de los ciudadanos, además de registros financieros, administrativos y documentales.

Desde el campo académico, este estudio ayuda a reforzar el conocimiento teórico vinculado con la seguridad informática y la protección de datos en la administración pública municipal, posibilitando examinar cómo interactúan ambas variables en un contexto institucional real. La indagación expande las perspectivas conceptuales acerca de la ciberseguridad, la seguridad informativa y la gestión de sistemas informáticos en instituciones públicas. Esto produce pruebas empíricas que pueden ser utilizadas como fuente para investigaciones futuras vinculadas a la modernización del Estado, el manejo digital y la gestión de tecnologías de la información.

La investigación, en términos prácticos, ayudará a determinar las fortalezas y debilidades de los sistemas de gestión de la Municipalidad de Carquín con respecto a la seguridad informática y la protección de datos. Los resultados logrados ayudarán a diseñar propuestas de mejora enfocadas en mejorar la disponibilidad de los sistemas informáticos, la integridad de los registros, la protección de información sensible y el control de accesos. Así, se ayudará a disminuir los peligros vinculados con la pérdida de información, los accesos no autorizados, las

interrupciones del servicio y la violación de datos personales; esto reforzará la eficacia administrativa y operativa de la entidad.

Además, la importancia social de este estudio reside en que una protección y seguridad informática adecuadas tienen un impacto directo en la confianza que los ciudadanos tienen en el manejo municipal. Se fomenta la transparencia, la confiabilidad de las instituciones y la calidad de los servicios públicos cuando los sistemas de información aseguran una gestión responsable y segura de los datos. La defensa de los datos de los ciudadanos no es solamente un deber administrativo; también es un compromiso ético que ayuda a preservar la privacidad y garantizar la seguridad de las personas.

Desde una perspectiva institucional, los resultados permitirán a los responsables municipales tomar decisiones de manera más estratégica respecto a la planificación, implementación y consolidación de políticas de privacidad de datos y ciberseguridad. Además, el estudio contribuirá a fortalecer la cultura organizacional de seguridad de la información y promover la capacitación de los empleados en el uso adecuado y responsable de los sistemas de gestión. Esto servirá para mantener operativos los servicios municipales y mejorar la gestión pública a nivel local.

En última instancia, el estudio es justificado desde el punto de vista metodológico debido a que utiliza una perspectiva cuantitativa con un diseño correlacional y no experimental. Esto posibilita evaluar de forma objetiva la conexión entre la protección de datos y la seguridad informática en los sistemas de gestión del municipio de Carquin. Para que los resultados sean válidos y confiables, es necesario utilizar herramientas estructuradas y métodos estadísticos adecuados. Esto favorece la rigurosidad científica del estudio y la producción de información valiosa para potenciar la administración municipal durante el año 2025.

1.5. Delimitación del estudio

Delimitación espacial:

La presente investigación se delimita espacialmente en la Municipalidad de Carquin, considerando las áreas y dependencias que utilizan sistemas de gestión informática para el desarrollo de sus funciones administrativas, operativas y de atención al ciudadano. El estudio se enfoca en el análisis de los sistemas de información empleados en la gestión municipal, los cuales almacenan, procesan y resguardan datos institucionales y personales, constituyéndose en el objeto principal de evaluación en relación con la protección de datos y la seguridad informática.

Delimitación temporal:

En cuanto a la delimitación temporal, la investigación se circunscribe al periodo correspondiente al año 2025, etapa durante la cual se analizará la situación actual de la protección de datos y la seguridad informática en los sistemas de gestión de la Municipalidad de Carquin. Este periodo permitirá evaluar las prácticas vigentes, los mecanismos implementados y la percepción del personal respecto al manejo seguro de la información institucional durante dicho año.

Delimitación conceptual:

Desde el punto de vista conceptual, el estudio se centra en dos variables principales: la protección de datos y la seguridad informática. La protección de datos se entiende como el conjunto de medidas, políticas y procedimientos orientados a garantizar el adecuado tratamiento, resguardo y uso responsable de la información, especialmente de los datos personales y sensibles. Por su parte, la seguridad informática se concibe como el conjunto de mecanismos técnicos y organizacionales destinados a preservar la confidencialidad, integridad y disponibilidad de la información contenida en los sistemas de gestión municipal.

Delimitación metodológica:

La delimitación metodológica establece que la investigación se desarrollará bajo un enfoque cuantitativo, con un diseño no experimental, de tipo correlacional y de corte transversal. La información será recolectada en un solo momento del tiempo mediante la aplicación de un cuestionario estructurado dirigido al personal de la Municipalidad de Carquin, lo que permitirá analizar la relación entre las variables de estudio sin manipularlas y dentro de su contexto natural.

1.6. Viabilidad del Estudio**Viabilidad técnica:**

La presente investigación es viable desde el punto de vista técnico, debido a que se cuenta con los recursos necesarios para la recolección, procesamiento y análisis de la información. El investigador dispone de equipos informáticos, acceso a internet, herramientas de ofimática y software estadístico que permitirán aplicar el instrumento de investigación y procesar los datos obtenidos. Asimismo, la Municipalidad de Carquin cuenta con sistemas de gestión informática operativos, lo que facilita el acceso a la información requerida y la aplicación del cuestionario al personal involucrado en el uso de dichos sistemas.

Viabilidad económica:

El estudio resulta viable, ya que no requiere de una inversión elevada para su ejecución. Los costos asociados a la investigación se limitan principalmente a la impresión de documentos, acceso a material bibliográfico, conectividad a internet y eventual movilidad del investigador. Además, el uso de herramientas digitales para la aplicación de encuestas y el procesamiento de datos contribuye a reducir significativamente los gastos, lo que hace que el desarrollo de la investigación sea financieramente accesible.

Viabilidad temporal:

La investigación puede desarrollarse dentro del periodo establecido, ya que el cronograma propuesto permite ejecutar de manera ordenada cada una de las etapas del estudio, desde la revisión bibliográfica y el diseño del instrumento hasta la recolección, análisis e interpretación de los resultados. El periodo correspondiente al año 2025 resulta adecuado para cumplir con los objetivos planteados, sin que se generen retrasos significativos en el desarrollo del trabajo.

Viabilidad social y administrativa:

La investigación es viable desde el punto de vista social y administrativo, debido a la pertinencia del tema y a la disposición institucional para la realización de estudios académicos que contribuyan a mejorar la gestión municipal. La temática de protección de datos y seguridad informática es relevante para la Municipalidad de Carquin, ya que sus resultados podrán servir como insumo para la toma de decisiones y el fortalecimiento de los sistemas de gestión. Asimismo, la aplicación del instrumento no interfiere con las labores normales del personal, lo que garantiza un entorno favorable para el desarrollo del estudio.

II. CAPITULO II: MARCO TEORICO

2.1. Antecedentes de la investigación

2.1.1. Investigaciones internacionales

1. (Ávila-Coello, 2024)

Título: *Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano.* donde desarrolló la investigación Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano, en la que se identifica la necesidad de fortalecer las políticas y estrategias de protección de datos mediante el análisis de prácticas actuales en organismos del sector público y se concluye que las brechas regulatorias y la falta de capacitación técnica constituyen barreras significativas para la madurez de los sistemas de seguridad de la información en instituciones gubernamentales. (p. 140)

2. (Vasco Delgado, 2025)

Título: *Ciberseguridad y protección de datos personales: desafíos y perspectivas.* El estudio muestra que las brechas normativas y la implementación insuficiente de políticas de protección de datos siguen siendo desafíos prioritarios en la región, proponiendo la necesidad de armonizar enfoques regulatorios y fortalecer las capacidades institucionales para garantizar la seguridad de la información en el contexto gubernamental. (p. 5)}

3. (Mata García, 2025)

Título: *Ciberseguridad para todos. Aprende, protege y responde.* Los resultados mostraron una guía en español sobre conceptos y prácticas esenciales de ciberseguridad y

protección de datos aplicada al uso cotidiano y organizacional, explicando cómo identificar riesgos, proteger información personal y aplicar medidas de seguridad prácticas en entornos digitales. Es útil para contextualizar conceptual y práctico el tema de protección de datos y seguridad informática en entidades públicas. (p. 78)

2.1.2. Investigaciones nacionales

1. (Torres Montano, 2025)

Título: *Seguridad de la información y gestión administrativa en entidades del sector público.* Sus principales conclusiones de su artículo Gobierno digital y protección de datos personales en la administración pública peruana, examina cómo el proceso de transformación digital del Estado plantea desafíos para la protección de los datos personales de los ciudadanos, destacando las tensiones entre la expansión digital y los riesgos de brechas de seguridad, y proponiendo recomendaciones para fortalecer la institucionalidad y la cultura de protección de datos en el sector público peruano. (p. 28)

2. (Melgarejo Solórzano, 2023)

Título: *Las medidas de seguridad y la interceptación de datos informáticos en la regulación peruana 2021-2022.* El estudio que analiza cómo las medidas de seguridad limitan la interceptación de datos informáticos y muestra que, pese a la existencia de mecanismos normativos, su aplicación práctica aún presenta debilidades que impactan la protección efectiva de la información en el sector público. (p. 53)

3. (Díaz Sandoval, 2024)

Título: *Análisis del nivel de seguridad de la información de la oficina de informática y telecomunicaciones de la Municipalidad Distrital de San Juan Bautista – 2023.* El investigador identifica deficiencias tanto técnicas como organizacionales en los controles de seguridad, evidenciando la necesidad de fortalecer las prácticas de protección de datos dentro de las municipalidades peruanas para asegurar la integridad y disponibilidad de la información institucional. (p. 28)

2.2. Bases teóricas

1. Protección de datos (Variable Independiente)

1. Introducción

En la actualidad, la protección de datos personales se ha convertido en uno de los pilares fundamentales de la sociedad digital. Según el autor (Sevillano Jaén, 2022) el crecimiento acelerado del uso de tecnologías de la información, plataformas digitales, redes sociales y sistemas informáticos en instituciones públicas y privadas ha incrementado de manera significativa la recopilación, tratamiento y almacenamiento de datos personales. Esta realidad ha generado nuevos riesgos relacionados con la privacidad, la seguridad de la información y los derechos fundamentales de las personas. (p. 26)

En este contexto, la protección de datos surge como un conjunto de principios, normas y medidas destinadas a garantizar que la información personal sea tratada de forma lícita, segura y responsable. Según el investigador (T Montano, 2025) En países como el Perú, la protección de datos personales adquiere especial relevancia en la administración pública, donde el manejo de información sensible de los ciudadanos exige altos estándares de confidencialidad, integridad y disponibilidad. (p. 28)

La presente investigación tiene como objetivo desarrollar de manera sistemática el tema de la protección de datos, abordando sus conceptos fundamentales, dimensiones, principios, marco normativo, importancia, desafíos actuales y su relación con la ciberseguridad, proporcionando así un sustento teórico adecuado para trabajos académicos e investigaciones.

2. Marco Conceptual

Protección de Datos Personales

La protección de datos personales se refiere al conjunto de políticas, normas, procedimientos y medidas técnicas u organizativas que se establecen con el objetivo de salvaguardar la información que permite identificar a una persona, ya sea de manera directa o indirecta. Rodríguez indica que en este contexto, la protección de datos incluye las medidas dirigidas a proteger la seguridad y el manejo apropiado de la información privada, con el fin de impedir que terceros accedan a ella, la utilicen, divulguen o gestionen indebidamente. Además, su propósito principal es garantizar que los derechos esenciales de los propietarios de datos, la autodeterminación informativa y la privacidad sean respetadas, lo que les permite a ellos mantener el control sobre la información que les concierne y sobre cómo se recopila, almacena y utiliza (Rodríguez, 2021, p. 28).

Datos Personales

(Delgado Ramos, 2022) Los datos personales comprenden toda información de naturaleza numérica, alfabética, gráfica, fotográfica, acústica, biométrica o de cualquier otra índole que permita identificar a una persona natural de manera directa o indirecta. Se trata de información vinculada a una persona determinada o determinable, cuya utilización debe realizarse conforme a los principios y disposiciones establecidos para la protección de datos

personales. Dentro de esta categoría se encuentran datos como nombres y apellidos, números de documentos de identidad, domicilios, direcciones de correo electrónico, números telefónicos, imágenes, huellas dactilares, registros de voz, información financiera, antecedentes laborales y datos relacionados con la salud. Debido a su carácter personal, estos datos requieren medidas de protección que garanticen su tratamiento adecuado, evitando accesos no autorizados, divulgaciones indebidas o cualquier uso que pueda afectar la privacidad y los derechos de sus titulares. (p. 16)

Tratamiento de Datos

(Autoridad Nacional de Protección de Datos, 2021) El tratamiento de datos personales incluye cualquier operación o grupo de operaciones que se lleven a cabo sobre datos personales, sin importar si se hacen mediante procesos automatizados, semiautomatizados o manuales. Estas acciones incluyen la recolección, adquisición, registro, ordenamiento, almacenamiento, preservación, adaptación, puesta al día, consulta, uso, transferencia, comunicación y difusión de datos; así como su cancelación o eliminación. El tratamiento tiene la posibilidad de llevarse a cabo en cualquiera de las fases del ciclo de vida de los datos y debe realizarse de acuerdo con los principios de seguridad, confidencialidad, finalidad, legalidad y proporcionalidad. Además, supone adoptar acciones que aseguren el empleo apropiado de la información personal, previniendo accesos no autorizados, modificaciones inapropiadas o cualquier otro acto que pueda poner en riesgo los derechos de los propietarios de los datos. Así, se pretende garantizar que la información se maneje de un modo responsable, transparente y en cumplimiento con las normas vigentes sobre protección de datos personales. (p. 38)

3. Dimensiones de la Protección de Datos

1. Confidencialidad de la Información

La confidencialidad se refiere al deber de proteger la información y los datos personales frente a accesos, consultas, usos o divulgaciones no autorizadas. Este principio busca garantizar que la información sea conocida únicamente por aquellas personas que cuentan con la autorización correspondiente para acceder a ella en el ejercicio de sus funciones o responsabilidades. En ese sentido, Stallings (2021) señala que la confidencialidad implica restringir el acceso a la información exclusivamente a los usuarios autorizados, evitando que terceros puedan conocer, utilizar o difundir los datos de manera indebida. Asimismo, este principio contribuye a asegurar que la información sea empleada únicamente para los fines previamente establecidos, preservando la privacidad de los titulares de los datos y fortaleciendo la confianza en los sistemas y procesos encargados de su gestión. (p. 23)

En el ámbito institucional, la confidencialidad se asegura mediante políticas de acceso, uso de credenciales, acuerdos de confidencialidad y controles de seguridad lógica y física.

2. Integridad de los Datos

En la protección de datos personales, la integridad es un principio fundamental porque asegura que la información permanezca inalterada sin cambios no autorizados y sea precisa, completa y coherente a lo largo de todo su ciclo vital. El propósito de este principio es garantizar que los datos mantengan sus rasgos originales y representen con precisión la realidad que muestran. En esa línea, Whitman (2020) afirma que la integridad es crucial para evitar equivocaciones, manipulaciones o alteraciones inapropiadas que puedan comprometer la veracidad y la fiabilidad de los datos (p. 12). Del mismo modo, para mantener la integridad se requiere la aplicación de medidas de control enfocadas en identificar, prevenir y rectificar

cambios no autorizados. Las medidas incluyen los métodos de validación de datos, las copias de seguridad, los registros de auditoría y las herramientas de monitoreo que hacen posible el reconocimiento de modificaciones realizadas a la información, lo cual contribuye a asegurar su fiabilidad, consistencia y precisión.

3. Disponibilidad de la Información

La disponibilidad es la dimensión que asegura que los sistemas y la información personal estén a disposición de los usuarios autorizados y sean funcionales cuando estos lo requieran. Su objetivo es garantizar el acceso a la información necesaria para llevar a cabo las actividades institucionales con puntualidad, evitando interrupciones que puedan comprometer la ejecución de funciones organizacionales o la prestación de servicios. En las entidades públicas, esta dimensión es especialmente significativa, ya que la información se convierte en un recurso esencial para la administración, la toma de decisiones y el trato eficaz a los ciudadanos. Además, la disponibilidad requiere la aplicación de acciones con el objetivo de evitar que se pierda el acceso a la información y asegurar que las operaciones sigan funcionando frente a incidentes eventuales. Se distinguen entre estas medidas los planes de recuperación y respaldo de datos, las estrategias para recuperar información en caso de desastres, los planes de continuidad del negocio, los sistemas redundantes y otros procedimientos que facilitan la restauración de servicios y la reconstrucción de datos en situaciones imprevistas o fallas.

4. Legalidad y Licitud del Tratamiento

Esta dimensión se basa en el cumplimiento de las normas, reglamentaciones y leyes que rigen la gestión de los datos personales. Su propósito es asegurar que la recolección, almacenamiento, utilización, transferencia y demás procesos realizados en torno a los datos

personales se lleven a cabo de acuerdo con los principios y responsabilidades establecidos por la legislación actual. Por lo tanto, el manejo de los datos debe basarse en el consentimiento previo, libre, expreso e informado del propietario o en alguna base legal que autorice su procesamiento. Además, supone que la información se use solamente para los propósitos específicos, explícitos y legítimos para los cuales fue adquirida, evitando usos no autorizados o que no sean compatibles. El cumplimiento normativo incluye también la implementación de acciones que garanticen el respeto hacia los derechos de los propietarios de los datos, impulsando la transparencia, la responsabilidad institucional y el resguardo de la privacidad en todas las actividades vinculadas con el tratamiento de información personal.

5. Responsabilidad y Gestión de la Información

La responsabilidad es una dimensión esencial en la protección de los datos personales, puesto que supone el compromiso de las entidades de asegurar un manejo apropiado y seguro de la información que gestionan, acorde a las leyes vigentes. Este principio requiere que la organización implemente procedimientos, políticas, medidas de seguridad y mecanismos de control con el objetivo de evitar posibles riesgos que puedan perjudicar los datos personales de los titulares. También incluye la designación de tareas y responsabilidades específicas para manejar y supervisar la protección de datos, garantizando que haya individuos o áreas responsables de asegurarse del cumplimiento de las obligaciones legales y organizacionales. Asimismo, incluye la formación constante de los empleados, el seguimiento ininterrumpido de los procedimientos vinculados con el tratamiento de datos y la evaluación regular de las medidas puestas en marcha. Con estas medidas, la organización evidencia su diligencia en el manejo de datos personales y refuerza la transparencia institucional, la confianza de los ciudadanos en el tratamiento de sus datos y el cumplimiento normativo.

4. Principios de la Protección de Datos

Entre los principales principios que rigen la protección de datos personales se encuentran:

- Principio de legalidad: El tratamiento de datos debe realizarse conforme a la ley.
- Principio de consentimiento: El titular debe autorizar el uso de sus datos, salvo excepciones legales.
- Principio de finalidad: Los datos deben ser utilizados solo para fines específicos y legítimos.
- Principio de proporcionalidad: Solo se deben recopilar los datos estrictamente necesarios.
- Principio de seguridad: Se deben adoptar medidas técnicas y organizativas para proteger los datos.

5. Marco Normativo de la Protección de Datos

La protección de datos personales está respaldada por varios instrumentos jurídicos internacionales y nacionales que establecen derechos, principios y deberes para asegurar el manejo apropiado de la información personal. El Reglamento General de Protección de Datos (RGPD) de la Unión Europea es uno de los más relevantes a nivel global. Este reglamento define normas para la recolección, almacenamiento, uso y transmisión de datos personales, lo que refuerza el resguardo del derecho a la privacidad y el poder de los titulares sobre sus datos. En cuanto a Perú, la Ley N.º 29733, Ley de Protección de Datos Personales y su reglamento constituyen el marco legal más importante en este país. Estas son las normas que regulan cómo se manejan los datos personales en entidades públicas y privadas. Estas normas determinan los

principios que rigen el manejo de la información, los derechos de los propietarios de los datos, las responsabilidades de aquellos que gestionan dichos datos y las sanciones pertinentes en caso de incumplimiento. Su objetivo es asegurar una protección adecuada de la privacidad y un correcto tratamiento de la información personal.

6. Importancia de la Protección de Datos

La protección de datos es fundamental para:

- Proteger la privacidad y los derechos fundamentales de las personas.
- Generar confianza en el uso de servicios digitales.
- Prevenir delitos informáticos como el robo de identidad y el fraude.
- Fortalecer la transparencia y la gestión institucional.

7. Desafíos Actuales en la Protección de Datos

La salvaguarda de datos personales afronta varios retos que provienen del uso cada vez mayor de las tecnologías informáticas y de la digitalización de las organizaciones. El aumento continuo de los ciberataques, que tienen como objetivo obtener, alterar, sustraer o divulgar información ilegalmente y que amenazan la privacidad y seguridad de los datos, es uno de los principales desafíos. El uso generalizado de aplicaciones, servicios y plataformas digitales también ha hecho que el volumen de datos personales recolectados y procesados aumente, lo que ha extendido los contextos de exposición a potenciales vulneraciones. La cultura de seguridad limitada en la información que existe en numerosas entidades es otro importante reto, ya que puede propiciar prácticas inapropiadas en el tratamiento de datos personales. Además, la falta de capacitación adecuada del personal en cuanto a seguridad informática y protección de datos

aumenta las probabilidades de que ocurran fallos humanos y que no se cumplan las medidas de protección fijadas. Por último, la rápida evolución de las tecnologías digitales crea nuevos escenarios y riesgos que, a menudo, avanzan más rápidamente que la actualización de los marcos normativos y mecanismos de control actuales. Esto ha llevado a la necesidad de fortalecer constantemente las estrategias para proteger y gestionar los datos personales.

8. Relación entre Protección de Datos y Ciberseguridad

La ciberseguridad y la protección de datos personales son áreas complementarias que colaboran juntas para asegurar la información. La ciberseguridad ofrece los mecanismos de carácter técnico, tecnológico y operativo que son necesarios para resguardar la información ante riesgos y vulnerabilidades, mientras que la protección de datos se centra en aplicar los derechos, principios, obligaciones y disposiciones legales que están vinculados con la gestión de la información personal. En este contexto, la ciberseguridad se encarga de poner en marcha controles y acciones que tienen como finalidad evitar accesos no permitidos, identificar actividades maliciosas y reaccionar a tiempo frente a sucesos que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos. Por su parte, la protección de datos determina qué información debe estar protegida, cuáles son las condiciones para tratarla y cuáles son los derechos de sus titulares. Por lo tanto, las dos disciplinas tienen una conexión cercana y complementaria, porque la protección apropiada de los datos personales necesita de mecanismos eficaces de ciberseguridad, mientras que una estrategia de ciberseguridad efectiva debe tener en cuenta el acatamiento de las reglas y principios que rigen la protección de información personal.

9. Conclusiones

La protección de datos personales constituye un elemento esencial en la gestión moderna de la información, especialmente en el contexto digital y gubernamental. Su adecuada implementación requiere no solo el cumplimiento de normas legales, sino también la adopción de una cultura organizacional basada en la seguridad, la responsabilidad y el respeto por la privacidad. Fortalecer las políticas de protección de datos contribuye al desarrollo institucional, a la confianza ciudadana y a la sostenibilidad de los servicios digitales.

2. Seguridad informática (Variable Dependiente)

1. Introducción

La seguridad informática se ha convertido en un elemento esencial en la sociedad actual, caracterizada por el uso intensivo de tecnologías de la información y la comunicación. (Gómez Vieites, 2021) refiere que el crecimiento del internet, los sistemas informáticos, las bases de datos y las plataformas digitales ha generado múltiples beneficios para las organizaciones; sin embargo, también ha incrementado los riesgos asociados a ataques cibernéticos, pérdida de información, accesos no autorizados y vulneración de sistemas por otro lado en este contexto, la seguridad informática surge como un conjunto de políticas, procedimientos, normas y medidas técnicas orientadas a proteger los sistemas de información frente a amenazas internas y externas.

(p. 16)

La presente investigación tiene como finalidad desarrollar de manera integral el tema de la seguridad informática, abordando sus conceptos fundamentales, dimensiones, principios, tipos, amenazas, medidas de protección, marco normativo, importancia y desafíos actuales, constituyendo así una base teórica sólida para trabajos académicos e investigaciones.

2. Marco Conceptual

Seguridad Informática

La seguridad informática se define como el conjunto de estrategias, normas y controles destinados a proteger los sistemas informáticos, redes, aplicaciones y datos frente a accesos no autorizados, alteraciones, destrucción o interrupciones del servicio. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información.

Sistema de Información

Un sistema de información es el conjunto ordenado de recursos humanos, tecnológicos, procedimentales y de datos que colaboran para recolectar, procesar, almacenar, administrar y repartir información en una entidad. Su propósito es brindar información pertinente, confiable y a tiempo que ayude a planificar, tomar decisiones, controlar las operaciones y lograr los objetivos de la institución. Estos sistemas incorporan varios elementos, entre ellos personas, equipos informáticos, software, bases de datos, redes de comunicación y procedimientos laborales. Estos componentes hacen posible convertir los datos en información útil para todos los niveles administrativos. Del mismo modo, colaboran en incrementar la eficacia de los procesos organizativos, afinar el aprovechamiento de los recursos y robustecer la habilidad de respuesta que tiene la organización ante las exigencias externas e internas. Los sistemas de información, así, se convierten en un instrumento esencial para llevar a cabo las actividades estratégicas, administrativas y operativas en cualquier organización.

Amenaza Informática

Una amenaza informática es cualquier acontecimiento, situación, acción o actor que tiene la capacidad de aprovechar una debilidad presente en un sistema de información y causar impactos negativos sobre los activos tecnológicos de una empresa. La confidencialidad, la

integridad o la disponibilidad de los datos pueden verse comprometidas por estas amenazas, lo que podría perjudicar el desempeño habitual de los sistemas, servicios y procesos institucionales. Las amenazas pueden provenir de dentro o fuera y presentarse en diferentes formas, incluyendo fallas técnicas, desastres naturales, interrupciones en los servicios tecnológicos, errores humanos, ataques cibernéticos, acceso no autorizado o robo de datos. La concreción de la misma puede generar perjuicios a nivel operativo, pérdidas financieras, deterioro reputacional y violaciones a la seguridad de la información. Por lo tanto, reconocer y administrar las amenazas informáticas es una actividad fundamental para salvaguardar los sistemas de información y disminuir los riesgos en el interior de las organizaciones.

3. Dimensiones de la Seguridad Informática

1. Confidencialidad

Un aspecto esencial de la seguridad de la información es la confidencialidad, que asegura que sólo aquellas personas con el permiso adecuado puedan acceder a los datos, documentos y recursos informativos. Su objetivo es resguardar la información contra accesos, consultas, usos o divulgaciones no permitidas que puedan amenazar su privacidad o causar daños a la organización. Esta dimensión tiene como objetivo prevenir que personas ajenas consigan acceso a datos reservados, estratégicos o sensibles sin la autorización adecuada, disminuyendo así los riesgos relacionados con el espionaje, la filtración de información y otras maneras de divulgación inapropiada de información. Para esto, se establecen procedimientos de seguridad enfocados en limitar el acceso a la información según las responsabilidades y funciones de cada usuario, incluyendo mecanismos de control de acceso, autenticación de usuarios y administración de permisos. De este modo, la confidencialidad ayuda a mantener la privacidad, la confianza y la seguridad de los datos institucionales.

Se logra mediante el uso de contraseñas seguras, cifrado de información, autenticación de usuarios y políticas de control de accesos.

2. Integridad

La integridad es un aspecto esencial de la seguridad de la información, que asegura que los datos permanezcan precisos, íntegros, consistentes y sin modificaciones no autorizadas mientras son almacenados, procesados o transmitidos. Su objetivo es garantizar que la información mantenga sus rasgos originales y represente de manera precisa la realidad que representa, previniendo errores, incoherencias o cambios que puedan comprometer su fiabilidad y validez. Esta dimensión es fundamental para tomar decisiones correctas y para llevar a cabo las actividades institucionales, porque garantiza que se cuente con información confiable y precisa en todo momento. La integridad también tiene como objetivo evitar manipulaciones accidentales o deliberadas a través de la realización de controles, registros de auditoría, mecanismos de validación y otras acciones de seguridad que posibiliten la identificación, el registro y la corrección de cualquier modificación inapropiada en los datos. Así, se ayuda a mantener la calidad de los datos y a aumentar la confianza en los sistemas que los gestionan.

Se protege a través de controles de validación, registros de auditoría, firmas digitales y copias de seguridad.

3. Disponibilidad

La disponibilidad es un aspecto fundamental de la seguridad de la información que asegura que los sistemas, las aplicaciones, los servicios tecnológicos y la información institucional sigan siendo accesibles y funcionales cuando los usuarios con autorización lo requieran. Su objetivo es garantizar el acceso a la información necesaria para llevar a cabo las

actividades de la organización de manera oportuna, previniendo las interrupciones que pudieran comprometer la continuidad de los procesos y la provisión de servicios. La escasez de disponibilidad puede tener un gran impacto en la organización, incluyendo demoras en las operaciones, disminución de la productividad, problemas financieros y restricciones en el proceso de toma de decisiones. Por lo tanto, esta dimensión demanda la aplicación de medidas destinadas a evitar fallos y reducir el impacto de eventuales incidentes que afecten el acceso a los recursos tecnológicos. Los planes de contingencia, los procesos de recuperación frente a catástrofes, los sistemas de redundancia, las copias de respaldo y las labores de mantenimiento preventivo son algunas de las acciones más importantes para asegurar la disponibilidad. Estas ayudan a que la continuidad operativa y la fiabilidad de los sistemas informáticos se sostengan.4.

Autenticidad

La autenticidad es un aspecto de la seguridad de la información que posibilita corroborar y asegurar quiénes son los usuarios, además de la procedencia y legitimidad de los datos que se intercambian o procesan en los sistemas. Su objetivo es garantizar que las personas, entidades o dispositivos que acceden a los recursos informáticos sean de hecho quienes dicen ser y que la información provenga de fuentes autorizadas y confiables. Para evitar el uso indebido de credenciales, la suplantación de identidad y otros actos que pongan en riesgo la seguridad de los sistemas y la fiabilidad de los datos, esta dimensión es esencial. Además, la autenticidad posibilita que las acciones llevadas a cabo en los sistemas sean asignadas a usuarios concretos, lo cual potencia la trazabilidad y la responsabilidad en el manejo de los datos. Para asegurarla, se utilizan procedimientos como la verificación de usuarios a través de contraseñas, firma electrónica, certificados digitales, autenticación multifactor y diferentes sistemas de validación que posibilitan comprobar la identidad de los usuarios y la legitimidad de los datos procesados.

5. No Repudio

El no repudio es un aspecto de la seguridad de la información que asegura que una persona no pueda rechazar más adelante la ejecución de una acción, transacción o comunicación que tuvo lugar en un sistema informático. Su objetivo es ofrecer pruebas suficientes para evidenciar la participación de un usuario en una actividad específica, garantizando así la validez y trazabilidad de las operaciones efectuadas. Esta dimensión es especialmente relevante en contextos digitales en los que se llevan a cabo intercambios de información, transacciones electrónicas, procesos administrativos y procedimientos que exigen la acreditación fehaciente de la identidad del responsable de una acción. Además, el no repudio robustece la confianza en los sistemas de información porque posibilita la verificación del autor y del momento de una operación específica. Se utilizan métodos como los sellos de tiempo, las firmas digitales, los certificados electrónicos y los registros electrónicos de auditoría para asegurar este principio. Estos ofrecen evidencia comprobable acerca de la autoría, integridad y ejecución de las acciones realizadas en los sistemas informáticos.

4. Principios de la Seguridad Informática

Los principales principios que rigen la seguridad informática son:

- Prevención: Evitar la ocurrencia de incidentes de seguridad.
- Gestión del riesgo: Identificar, evaluar y tratar los riesgos informáticos.
- Defensa en profundidad: Aplicar múltiples capas de seguridad.
- Responsabilidad: Definir roles y responsabilidades claras.
- Mejora continua: Actualizar constantemente las medidas de seguridad.

5. Tipos de Seguridad Informática

- Seguridad física: Protección de los equipos e infraestructuras.
- Seguridad lógica: Protección del software y sistemas.
- Seguridad de redes: Protección de las comunicaciones y conexiones.
- Seguridad de la información: Protección de los datos en cualquier formato.

6. Amenazas Informáticas Comunes

Entre las principales amenazas se encuentran:

- Malware (virus, troyanos, ransomware).
- Phishing y ataques de ingeniería social.
- Ataques de denegación de servicio (DoS/DDoS).
- Accesos no autorizados.
- Fugas de información.

7. Medidas de Seguridad Informática

Las medidas más utilizadas incluyen:

- Uso de antivirus y firewalls.
- Actualización constante de sistemas.
- Copias de seguridad periódicas.
- Políticas de seguridad y capacitación del personal.

- Monitoreo y auditoría de sistemas.

8. Marco Normativo

Un grupo de estándares, normas y regulaciones respaldan la seguridad informática, y estos delinear las pautas para proteger los sistemas tecnológicos y la información contra amenazas y riesgos. La familia de normas ISO/IEC 27000 es una de las más destacadas a nivel mundial, ya que ofrece orientaciones para el manejo seguro de la información, la detección de riesgos, la aplicación de medidas de seguridad y el perfeccionamiento constante de los sistemas protectores. Estas normas son empleadas de manera extensa por entidades privadas y públicas con el propósito de reforzar la confidencialidad, integridad, disponibilidad y otros aspectos que garantizan la seguridad de los datos.

La Ley N.º 29733, que es la Ley de Protección de Datos Personales, y su reglamento tienen una relación estrecha con la seguridad informática en el Perú porque para proteger los datos personales es necesario establecer medidas organizativas y técnicas que aseguren su seguridad. Del mismo modo, está relacionada con las políticas, estrategias y directrices en materia de seguridad digital que impulsa el Estado peruano. Estas tienen como objetivo reforzar la salvaguarda de la información pública, mantener los servicios digitales y gestionar apropiadamente los riesgos cibernéticos. En general, este marco regulatorio ayuda a definir deberes y responsabilidades, así como prácticas adecuadas que buscan salvaguardar la seguridad de los sistemas de información y proteger los bienes digitales de las entidades..

9. Importancia de la Seguridad Informática

La seguridad informática es fundamental para:

- Proteger la información crítica.

- Garantizar la continuidad de los servicios.
- Prevenir pérdidas económicas y legales.
- Fortalecer la confianza de los usuarios.
- Cumplir con las normas legales vigentes.

10. Desafíos Actuales de la Seguridad Informática

La seguridad de la informática afronta múltiples retos debido a que las tecnologías digitales son cada vez más necesarias y al continuo cambio de los entornos tecnológicos. Uno de los mayores desafíos es el aumento de los ciberataques, que cada vez son más sofisticados y tienen como objetivo poner en riesgo la información, los sistemas y los servicios de las entidades. Igualmente, un factor de riesgo significativo es la ausencia de una cultura de seguridad apropiada entre los usuarios, puesto que numerosas vulnerabilidades surgen debido a equivocaciones humanas, desconocimiento de las mejores prácticas en términos de seguridad o violación de los procedimientos definidos.

La rápida evolución de la tecnología, que produce continuamente nuevas amenazas y vulnerabilidades, es otro desafío importante que requiere que las organizaciones actualicen sus mecanismos de protección de forma continua. Asimismo, la mayor utilización de dispositivos móviles, el acceso a los sistemas de manera remota y la conexión entre diversas plataformas incrementan el área expuesta a peligros de seguridad. En muchos casos, además, la escasa inversión en infraestructura, herramientas y formación especializada en ciberseguridad restringe la habilidad de las organizaciones para prevenir, identificar y reaccionar eficientemente ante incidentes de seguridad. En conjunto, estos retos demuestran que es preciso reforzar de forma

constante las tácticas de protección, manejo de riesgos y sensibilización para asegurar la seguridad de la información y el mantenimiento del funcionamiento institucional.11. Relación entre Seguridad Informática y Protección de Datos

La seguridad informática proporciona las herramientas técnicas necesarias para garantizar la protección de los datos personales. Sin seguridad informática, no es posible asegurar la confidencialidad, integridad y disponibilidad de la información.

12. Conclusiones

La seguridad informática es un componente fundamental para que las organizaciones funcionen correctamente en un ambiente cada vez más dependiente de las tecnologías de la información. Su objetivo es salvaguardar las redes, sistemas, aplicaciones y datos frente a riesgos que tengan el potencial de poner en peligro la disponibilidad, la confidencialidad, la integridad y otras características de seguridad de la información. Sin embargo, no solo se requiere la aplicación de instrumentos tecnológicos para una administración eficaz de la seguridad informática; también son necesarios procedimientos de control apropiados, políticas institucionales bien definidas, programas de capacitación continuos y un enfoque cultural organizacional que proteja la información. Además, exige que los directores y todos los empleados se comprometan a asegurar que se cumplan las medidas de seguridad dispuestas. El reforzamiento de la seguridad en el ámbito informático ayuda a disminuir los peligros, evitar sucesos imprevistos, salvaguardar los activos de información, garantizar que se cumplan las normativas vigentes y asegurar que las operaciones institucionales continúen. Así, se favorecen la estabilidad, la confiabilidad y la sostenibilidad de los sistemas informáticos, características imprescindibles para que las actividades de las organizaciones se desarrollen con eficacia y para que los servicios sean de buena calidad.

2.3. Definición de términos básicos

Protección de datos

Se refiere al conjunto de políticas, procedimientos, medidas y principios técnicos y organizativos que tienen como objetivo proteger la información contra amenazas que puedan poner en peligro su seguridad, confidencialidad, integridad o disponibilidad. Su objetivo es asegurar que los datos sean manejados de forma apropiada, segura y responsable en todas las fases de su ciclo de vida, desde su recogida y almacenamiento hasta el empleo, la transferencia y la eliminación. La protección de información cobra especial importancia cuando se refiere a datos personales o información delicada, ya que su objetivo es proteger la privacidad de los individuos y garantizar el respeto a sus derechos. Con este fin, se establecen procedimientos de control que impiden la divulgación no autorizada, la modificación, el extravío u otras formas de uso que podrían causar daños a los titulares de la información o a la entidad responsable de su gestión. Así, la protección de los datos ayuda a incrementar la confianza en el manejo institucional, fomentar el acatamiento de las normativas legales actuales y asegurar un tratamiento responsable de los recursos informativos.

Seguridad informática

Es el grupo de procesos, controles y medidas de naturaleza técnica, administrativa y humana que tienen como objetivo salvaguardar los sistemas informáticos y los recursos tecnológicos de una entidad frente a amenazas, vulnerabilidades y riesgos provenientes del interior o exterior. Su propósito es proteger la información mientras se almacena, procesa, transmite y utiliza, asegurando que solo las personas autorizadas tengan acceso a ella, que permanezca íntegra y que esté disponible cuando se necesite para llevar a cabo las actividades de

la institución. El aseguramiento de los sistemas de información implica la puesta en marcha de políticas, normas y procedimientos de seguridad enfocados en evitar accesos no autorizados, interrupciones del servicio, alteraciones no permitidas, pérdida de datos y cualquier otro incidente que pueda perjudicar el rendimiento de los sistemas. Además, ayuda a mantener la continuidad operacional de la organización, aumentar la fiabilidad de los datos institucionales y garantizar que las metas y procedimientos organizativos se cumplan correctamente en un ambiente cada vez más dependiente de las tecnologías de información.

Sistemas de gestión

Son plataformas tecnológicas integradas que posibilitan la recolección, el registro, el procesamiento, el almacenamiento y la gestión de los datos relacionados con los procedimientos administrativos, financieros, operativos y de gestión que una municipalidad realiza. Estos sistemas son instrumentos esenciales para gestionar y controlar la información institucional, lo que permite el acceso a datos fiables de manera oportuna para poder llevar a cabo las funciones y competencias de la entidad. Además, ayudan a que los procedimientos se automaticen, los recursos se optimicen y la eficiencia en la administración pública local aumente. Los sistemas de información, en el contexto municipal, respaldan el planeamiento, la implementación y la supervisión de tareas vinculadas con la provisión de servicios públicos, el manejo tributario, el control del presupuesto, la gestión de recursos humanos y otros deberes inherentes al gobierno local. Asimismo, brindan datos significativos para la toma de decisiones, robustecen los métodos de transparencia y rendición de cuentas, y promueven una atención más eficaz de las necesidades ciudadanas a través de una administración fundamentada en información actualizada y ordenada.

Confidencialidad

Se define como el principio de la seguridad de la información que garantiza que los datos, documentos y recursos informativos sean accesibles únicamente para las personas que cuentan con la autorización correspondiente. Su finalidad es proteger la información frente al acceso, uso, divulgación, copia o distribución no autorizada, especialmente cuando se trata de información sensible, reservada o de carácter personal. La confidencialidad busca preservar la privacidad de los datos y evitar que terceros obtengan conocimiento de información que podría generar perjuicios a la organización o a las personas involucradas. Para ello, se establecen controles de acceso, niveles de autorización y otras medidas de protección que limitan el acceso a la información según las funciones y responsabilidades de cada usuario. De esta manera, se asegura que la información sea conocida únicamente por quienes tienen una necesidad legítima de acceder a ella en el ejercicio de sus actividades.

Integridad de la información

Se refiere a la propiedad que asegura que la información conserve su integridad, exactitud y coherencia en todas las etapas de su ciclo de vida, desde la creación y el almacenamiento hasta el procesamiento, uso y transmisión. Este principio tiene como objetivo garantizar la inalterabilidad de los datos, evitando que sean manipulados, modificados o eliminados sin autorización y preservando su contenido original y su fiabilidad. La integridad de los datos posibilita que los documentos, registros y bases de datos representen con fidelidad la realidad que reflejan, impidiendo modificaciones inapropiadas, errores o incongruencias que pueden influir en el desarrollo de las actividades institucionales y en la toma de decisiones. Para esto, se implementan controles y procedimientos de protección que buscan mantener la precisión y validez de los datos, asegurándose de que cualquier cambio sea autorizado, documentado y

verificable. Así, la información mantiene su calidad, utilidad y valía como un recurso esencial para la organización.

Disponibilidad

Es la base esencial de la seguridad de la información que asegura que los sistemas, aplicaciones, servicios tecnológicos y datos institucionales estén disponibles, sean utilizables y funcionen cuando sean solicitados por los usuarios con autorización. Su objetivo es garantizar la continuidad de las actividades organizativas a través del suministro fiable y puntual de la información requerida para llevar a cabo los procesos institucionales. La disponibilidad supone la aplicación de acciones de infraestructura, técnicas y administrativas que tienen como objetivo evitar interrupciones, disminuciones en el servicio o pérdidas de acceso causadas por fallos tecnológicos, desastres naturales, ataques cibernéticos, errores humanos u otros sucesos que puedan perturbar la operación normal de los sistemas de información. Igualmente, este principio incluye la implementación de procedimientos de redundancia, respaldo, supervisión constante y planes de continuidad operativa que posibiliten conservar los servicios informáticos activos o restablecerlos en el tiempo más corto posible. Así, la disponibilidad ayuda a asegurar la satisfacción de los usuarios, la protección de los activos de información ante circunstancias que puedan amenazar su acceso continuo y oportuno y la eficacia de las operaciones institucionales.

Control de accesos

Se refiere al conjunto de procedimientos, políticas, mecanismos tecnológicos y medidas de seguridad que supervisan, controlan y limitan el acceso a los sistemas de información dentro de una organización. Su objetivo es asegurar que solo las personas con autorización adecuada tengan acceso a los servicios, datos y recursos informáticos de la institución, en función de los

niveles de privilegio, responsabilidades y funciones asignadas dentro del ente. Para ello, se definen procedimientos de autorización, autenticación e identificación que posibilitan comprobar la identidad del usuario y especificar el rango de las acciones que puede llevar a cabo con respecto a la información. El control de acceso también ayuda a salvaguardar la confidencialidad, integridad y disponibilidad de los datos institucionales, al disminuir las posibilidades de accesos indebidos, cambios no permitidos, pérdida de información, fraude informático y otros peligros que pueden poner en riesgo la seguridad de los activos informativos de la entidad. Asimismo, facilita la trazabilidad de las acciones ejecutadas por los usuarios a través del registro y seguimiento de accesos, lo que robustece los procedimientos de cumplimiento normativo y control interno.

Gestión de riesgos

Se refiere al procedimiento continuo, sistemático y organizado a través del cual una entidad reconoce, investiga, valora, establece prioridades y gestiona los riesgos vinculados con la utilización de activos de información y tecnologías de la información. El propósito de este procedimiento es prever, regular y disminuir la posibilidad de que sucedan sucesos que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de los datos institucionales. Para esto, se evalúan las amenazas posibles, las vulnerabilidades que hay y el grado de exposición al riesgo en bases de datos, redes, sistemas, aplicaciones e infraestructura tecnológica. Con base en la evaluación mencionada, se crean y aplican medidas de control con el objetivo de prevenir incidentes de seguridad, mitigar sus consecuencias o permitir una respuesta apropiada cuando ocurren. Además, la administración de riesgos facilita mejorar el proceso de tomar decisiones relacionadas con la seguridad informativa, hacer más robusta la capacidad de una organización para resistir amenazas internas y externas, asegurar que las operaciones continúen funcionando y

ayudar a cumplir con los estándares y normas pertinentes en cuanto a protección informativa y seguridad informática.

Copias de seguridad (backup)

Son procesos técnicos y administrativos a través de los cuales se lleva a cabo la copia, el almacenamiento y la preservación de la información que se encuentra en las bases de datos, sistemas de gestión, servidores y otros recursos tecnológicos de una entidad. Su objetivo es asegurar que los datos estén disponibles y puedan recuperarse a tiempo ante acontecimientos que puedan poner en riesgo su accesibilidad o integridad, como errores de software y hardware, ataques cibernéticos, desastres naturales, pérdida accidental de información o fallos humanos. Estos procedimientos abarcan la planificación, implementación, comprobación y actualización regular de las copias de seguridad; además, involucran el establecimiento de mecanismos para restaurar que posibiliten la recuperación eficaz de la información en los plazos solicitados por la entidad. Además, el soporte y la recuperación de datos son una parte fundamental de los planes de continuidad del negocio y de la gestión de la seguridad informativa. Esto se debe a que ayudan a disminuir las pérdidas de información, acortar los períodos en que los servicios están interrumpidos y garantizar el mantenimiento de las actividades institucionales en circunstancias adversas.

Incidentes de seguridad informática

Son eventos, situaciones o actividades que comprometen, afectan o representan una amenaza para la confidencialidad, integridad y disponibilidad de la información, así como para el funcionamiento seguro de los sistemas, redes e infraestructuras tecnológicas de una organización. Estos incidentes pueden originarse por causas internas o externas e incluyen, entre

otros, accesos no autorizados, robo o divulgación indebida de información, ataques cibernéticos, infecciones por software malicioso, alteración o destrucción de datos, fallas de seguridad en aplicaciones, interrupciones de los servicios informáticos y vulneraciones a las políticas de seguridad establecidas. La ocurrencia de un incidente puede generar consecuencias operativas, económicas, legales y reputacionales para la organización, afectando la continuidad de sus procesos y la confianza de los usuarios. Por ello, resulta fundamental contar con mecanismos de detección, reporte, análisis, respuesta y recuperación que permitan gestionar oportunamente estos eventos, minimizar sus impactos y fortalecer las medidas de protección frente a futuras amenazas.

2.4. Hipótesis de investigación

2.4.1. Hipótesis general

Existe una relación significativa entre la protección de datos y la seguridad informática en los sistemas de gestión de la Municipalidad de Carquin, 2025.

2.4.2. Hipótesis específicas

Existe una relación significativa entre la protección de datos y la confidencialidad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025.

Existe una relación significativa entre la protección de datos y la integridad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025.

Existe una relación significativa entre la protección de datos y la disponibilidad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025.

2.5. Operacionalización de Variable e Indicadores

Tabla 1. Protección de datos

Dimensiones	Indicadores	Ítems	Nivel/Rango
Políticas de protección de datos	- Existencia de normas internas. - Cumplimiento de políticas.	1,2,	Nunca (1)
Control de acceso a la información	- Autenticación de usuarios. - Restricción según funciones.	3,4,	Casi nunca (2) A veces (3)
Manejo y tratamiento de datos	- Uso responsable de la información. - Confidencialidad de datos.	5,6,	Casi siempre (4) Siempre (5)

Tabla 2. Seguridad informática

Dimensiones	Indicadores	Ítems	Nivel/Rango
Confidencialidad	- Protección contra accesos no autorizados. - Gestión de permisos.	7,8,	Nunca (1) Casi nunca (2)
Integridad	- Protección contra alteraciones. - Confiabilidad de la información.	9,10,	A veces (3) Casi siempre (4)
Disponibilidad	- Acceso oportuno a sistemas. - Recuperación de información.	11,12,	Siempre (5)

III. CAPITULO III: METODOLOGIA DE LA INVESTIGACION

3.1. Diseño metodológico

1. Enfoque de investigación

La investigación se lleva a cabo con un enfoque cuantitativo porque busca la recopilación y el análisis de datos numéricos para medir las variables de estudio y contrastar las hipótesis formuladas. Este método posibilita caracterizar los fenómenos de forma objetiva, utilizando procedimientos estadísticos que ayudan a determinar relaciones, tendencias y niveles entre las variables estudiadas. En la investigación actual, se utiliza un cuestionario estructurado con una escala tipo Likert para recopilar datos, lo que hace posible convertir los puntos de vista y las percepciones de los participantes en información cuantificable. Luego, estos datos se procesan usando métodos de estadística descriptiva e inferencial, lo que hace posible determinar cómo se comportan las variables y si hay relaciones significativas entre ellas. Así, el enfoque cuantitativo ofrece resultados que se pueden medir y verificar, lo que ayuda a una interpretación objetiva del fenómeno investigado.

2. Tipo de investigación

La investigación actual es fundamental o básica, ya que tiene como objetivo aumentar y robustecer el saber científico acerca de la conexión entre la protección de datos y la seguridad informática en el entorno organizacional. Su objetivo esencial no es aplicar soluciones al instante ni participar directamente en los procedimientos institucionales, sino entender, describir y examinar las propiedades y conductas de las variables investigadas con base en fundamentos teóricos y evidencia empírica. Además, los resultados alcanzados contribuyen al progreso

teórico de estos campos de estudio, produciendo información que podría ser utilizada como fundamento para investigaciones futuras y para el diseño de tácticas enfocadas en robustecer la administración de seguridad y protección de datos en las organizaciones.

3. Nivel de investigación

Esta investigación es de tipo correlacional, ya que su objetivo es descubrir y establecer el nivel de relación entre la seguridad informática y la protección de datos en los sistemas de gestión del municipio distrital de Carquín. Este grado de estudio se enfoca en examinar la manera en que las variables interactúan y determinar si hay una conexión entre ellas dentro del contexto estudiado, sin necesidad de establecer una relación de causa-efecto. Con el fin de determinar la dirección y la magnitud de la relación entre dos variables, se emplean métodos de análisis estadístico. Esto posibilita comprobar si las alteraciones en una variable están relacionadas con cambios en la otra. Así, el estudio brinda evidencia empírica acerca del nivel de relación que hay entre los factores analizados, lo cual ayuda a comprender mejor el fenómeno y produce información valiosa para futuras investigaciones y procesos de toma de decisiones institucionales.

4. Diseño de investigación

Como las variables de estudio no serán manipuladas o controladas intencionalmente por el investigador, sino que se observarán y analizarán tal como ocurren en su contexto real, la investigación emplea un diseño no experimental. Este diseño posibilita analizar las propiedades y la conexión entre la seguridad informática y la protección de datos en los sistemas de gestión de la Municipalidad Distrital de Carquín, sin interferir con el comportamiento de las variables o

modificar las condiciones bajo las cuales ocurren los sucesos observados. Además, el estudio es de tipo transversal, ya que la recolección de datos se llevará a cabo en un solo punto en el tiempo, lo que posibilitará una perspectiva concreta de la situación durante el periodo analizado. Este diseño tiene como objetivo describir y examinar el estado actual de las variables estudiadas, además de establecer la relación entre ellas utilizando los datos obtenidos en un contexto y tiempo específicos. Se busca así aportar información objetiva acerca de la realidad institucional analizada.

3.2. Población y muestra

3.2.1. Población

La población de la investigación está conformada por 120 trabajadores de la Municipalidad de Carquin, 2025.

3.2.2. Muestra

Para la muestra utilizaremos la siguiente formula.

$$n = \frac{Z^2 \cdot p \cdot q \cdot N}{E^2(N - 1) + Z^2 \cdot p \cdot q}$$

Donde:

N es 120 el Tamaño total de la Población.

Z es 1.96 Para un nivel de confianza del 95%.

p es 0.5 Proporción esperada, cuando no se tiene un dato exacto.

q es 1-p que es 0.5

E es 0.05 Margen de error del 5%.

Reemplazando es

$$n = \frac{3.8416 * 0.25 * 120}{0.0025 * 119 + 3.8416 * 0.25}$$

Lo cual nuestra muestra sería de 92 trabajadores de la Municipalidad de Carquin, 2025.

Según Otzen y Manterola (2017), la muestra es un subconjunto de la población que permite, de manera representativa, realizar inferencias sobre el total de la población.

3.3. Técnicas de recolección de datos

Para la recopilación de datos, se empleará la técnica de la encuesta, utilizando un cuestionario estructurado como instrumento de medición. Este cuestionario permitirá obtener información sobre la Protección de Datos y Seguridad Informática en los sistemas de gestión de la Municipalidad de Carquin, 2025.

El cuestionario estará compuesto por una serie de afirmaciones relacionadas con las dimensiones de cada variable, y las respuestas serán valoradas mediante una escala ordinal tipo Likert.

Los valores obtenidos en la correlación de Spearman serán analizados según los siguientes criterios:

$\rho \approx 1$ o $-1 \rightarrow$ Correlación fuerte

$\rho \approx 0.5$ o $-0.5 \rightarrow$ Correlación moderada

$\rho \approx 0 \rightarrow$ Correlación débil o inexistente

Este análisis permitirá verificar si existe una relación significativa entre la Protección de Datos y la Seguridad Informática en los sistemas de gestión de la Municipalidad de Carquin, lo que permitirá extraer conclusiones relevantes para la investigación.

IV. CAPITULO IV: RESULTADOS

4.1. Análisis de Resultados

4.1.1. Resultados de Protección de Datos y sus dimensiones

Tabla 1 Protección de Datos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	10	10,9	10,9	10,9
	Medio	60	65,2	65,2	76,1
	Alto	22	23,9	23,9	100,0
	Total	92	100,0	100,0	

Fuente: Información recopilada de Protección de Datos proveniente de los trabajadores de la Municipalidad de Carquin, 2025.

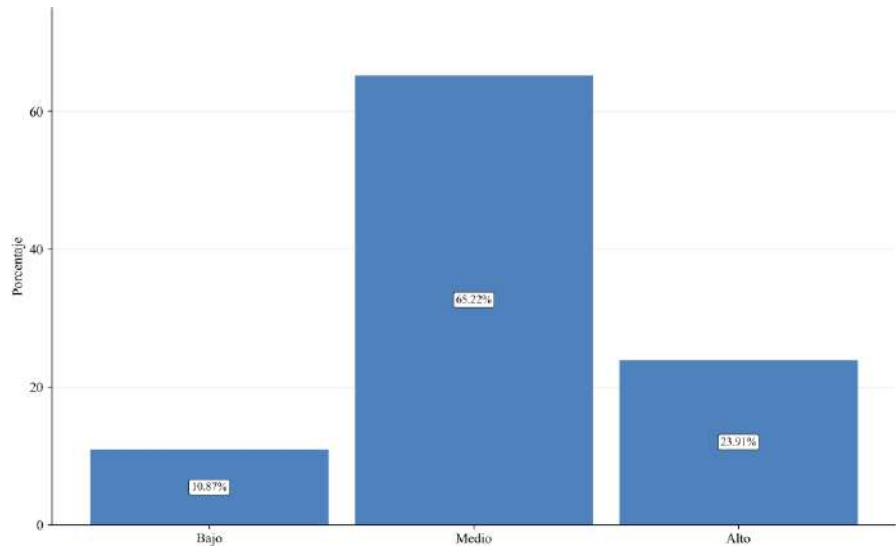


Gráfico 1 Protección de Datos

La gráfica 1 muestra que el 65.2% de los empleados de la Municipalidad Distrital de Carquín considera que la protección de datos está en un nivel promedio, lo cual demuestra que las acciones implementadas son vistas como adecuadas, aunque todavía tienen elementos que

pueden ser mejorados. De igual modo, el 23,9 % de los encuestados cree que la protección de datos es alta, lo que muestra una valoración positiva sobre los procedimientos y mecanismos implementados para salvaguardar la información institucional. Por otra parte, el 10,9% indica que la protección de datos está a un nivel bajo, lo cual evidencia que hay ciertas carencias o restricciones en los métodos de salvaguarda de la información. Los resultados en general señalan que existe una percepción de nivel medio acerca de la protección de datos en la entidad, lo que indica que es necesario robustecer las políticas, controles y acciones enfocadas en asegurar una gestión más segura de la información.

Tabla 2 Categoría Políticas de Protección de Datos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	23	25,0	25,0	25,0
	Medio	61	66,3	66,3	91,3
	Alto	8	8,7	8,7	100,0
	Total	92	100,0	100,0	

Fuente: Información recopilada de Políticas de Protección de Datos proveniente de los trabajadores de la Municipalidad de Carquin, 2025.

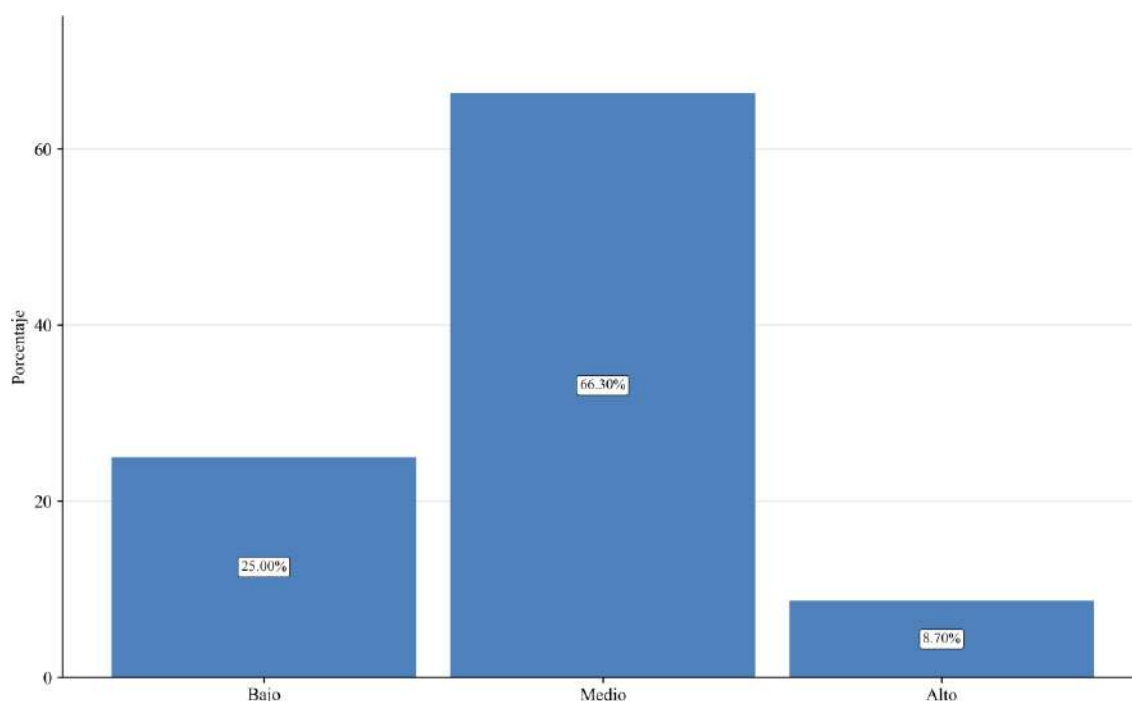


Gráfico 2 *Políticas de Protección de Datos*

El 66,3 % de los empleados de la Municipalidad Distrital de Carquín cree que las políticas de protección de datos están en un nivel medio, según se observa en la Figura 2; esto sugiere que, desde el punto de vista del grueso de los encuestados, hay pautas y disposiciones orientadas a proteger la información. Sin embargo, es necesario fortalecerlas para lograr una eficacia más elevada. El 25,0 % de los participantes también indica que dichas políticas se encuentran a un nivel bajo, lo que muestra la percepción de restricciones en su ejecución, divulgación o cumplimiento dentro de la entidad. En contraste, solo el 8,7 % opina que las políticas de protección de datos son de calidad elevada, lo que refleja una apreciación positiva por parte de un pequeño conjunto de empleados. En términos generales, los hallazgos indican que prevalece una percepción de nivel medio en relación con las políticas de protección de datos.

Esto indica la necesidad de fortalecer su implementación y establecer una cultura institucional enfocada en proteger la información.

Tabla 3 Categoría Control de Acceso a la Información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	3	3,3	3,3	3,3
	Medio	34	37,0	37,0	40,2
	Alto	55	59,8	59,8	100,0
	Total	92	100,0	100,0	

Fuente: Información recopilada de Control de Acceso a la Información proveniente de los trabajadores de la Municipalidad de Carquin, 2025.

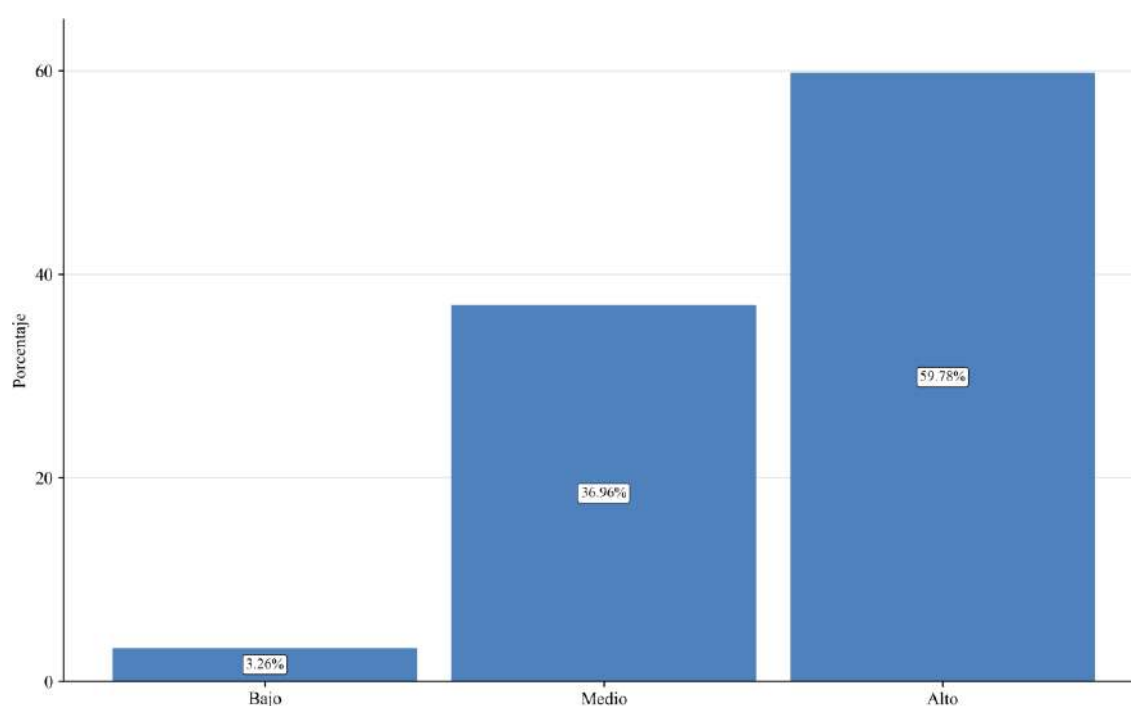


Gráfico 3 Control de Acceso a la Información

La Figura 3 muestra que el 59,8 % de los empleados del municipio distrital de Carquín opina que el control de acceso a la información tiene un nivel elevado, lo cual indica una

valoración positiva sobre los procedimientos puestos en práctica para limitar y controlar el acceso a la información institucional. Además, el 37.0% de los encuestados indica que este aspecto está a un nivel medio, lo que sugiere que, aunque hay controles establecidos, todavía es posible reforzar ciertos procedimientos para optimizar la seguridad de la información. El 3,3 % de los encuestados, por su parte, piensa que el control de acceso está en un nivel bajo; esto demuestra que una pequeña proporción de empleados percibe fallas importantes en este aspecto. En general, los resultados indican que se da una valoración positiva del control de acceso a la información. Esto sugiere que la entidad dispone de mecanismos adecuadamente configurados para administrar los permisos y salvaguardar el acceso a los recursos informativos.

Tabla 4 Categoría Manejo y Tratamiento de Datos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	9	9,8	9,8	9,8
	Medio	58	63,0	63,0	72,8
	Alto	25	27,2	27,2	100,0
	Total	92	100,0	100,0	

Fuente: Información recopilada de Manejo y Tratamiento de Datos proveniente de los trabajadores de la Municipalidad de Carquin, 2025.

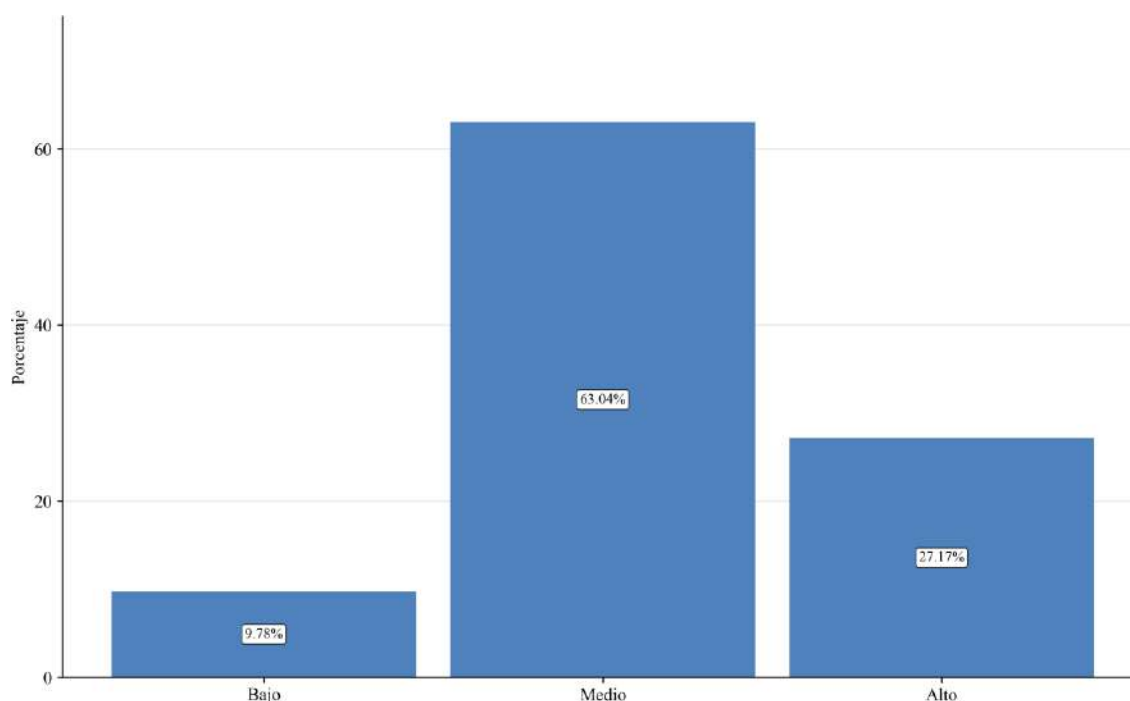


Gráfico 4 Manejo y Tratamiento de Datos

De acuerdo con la Figura 4, el 63.0 % de los empleados de la Municipalidad Distrital de Carquín piensa que la gestión y tratamiento de datos están en un nivel medio, lo que muestra que la mayor parte considera que las prácticas vinculadas a la recolección, almacenamiento, uso y administración de información se llevan a cabo suficientemente bien, aunque aún hay áreas que pueden ser mejoradas. Además, el 27,2% de los que participaron en la encuesta indica que esta dimensión es elevada, lo que muestra una evaluación positiva de las prácticas puestas en marcha para el manejo de datos dentro de la institución. Por otra parte, un 9,8% sostiene que la gestión y el tratamiento de datos están en un nivel bajo, lo cual señala que perciben algunas falencias o limitaciones en los métodos utilizados. En términos generales, los resultados indican que el nivel medio es predominante, lo que sugiere la necesidad de seguir reforzando las prácticas y procedimientos relacionados con el manejo correcto de la información para llegar a niveles más altos de protección y control de datos.

Resultados de Seguridad Informática y sus dimensiones

Tabla 5 Seguridad Informática

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	16	17,4	17,4	17,4
	Medio	55	59,8	59,8	77,2
	Alto	21	22,8	22,8	100,0
	Total	92	100,0	100,0	

Fuente: Información recopilada de Seguridad Informática proveniente de los trabajadores de la Municipalidad de Carquin, 2025.

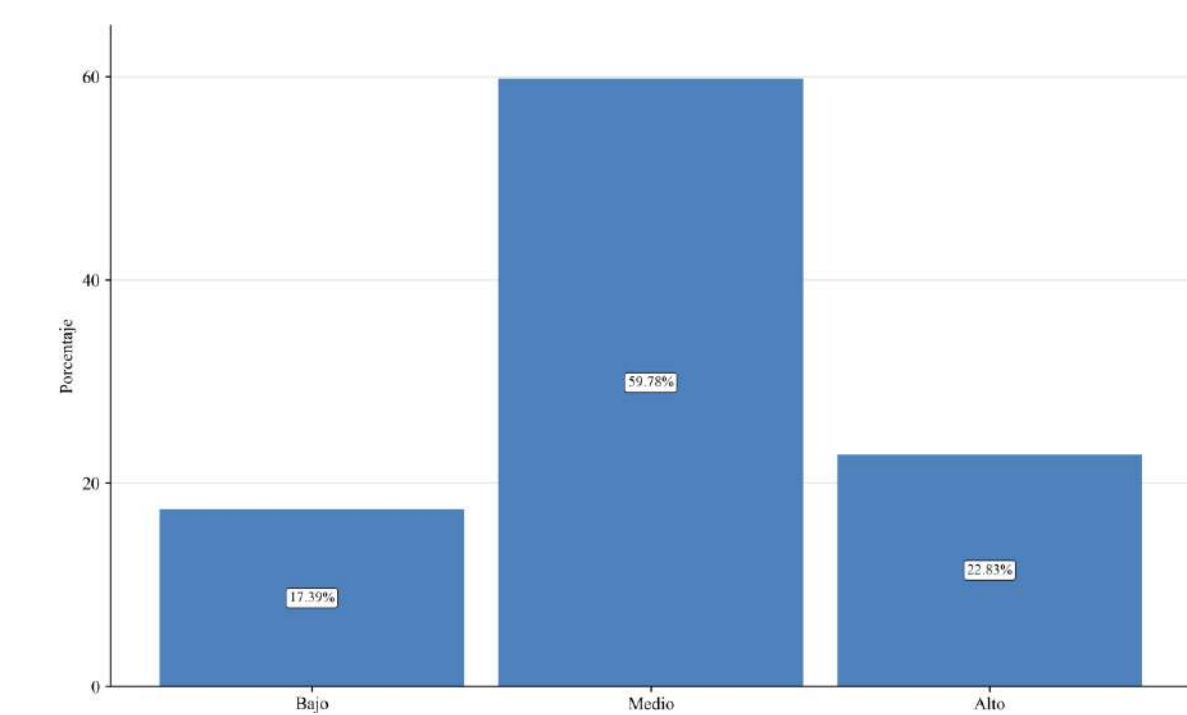


Gráfico 5 Seguridad Informática

La mayoría de los empleados de la Municipalidad Distrital de Carquín (59,8 %) considera que la seguridad informática es promedio, lo cual sugiere que las medidas de protección implementadas en los sistemas y en los recursos tecnológicos son aceptables, aunque todavía hay oportunidades para mejorar y robustecer la seguridad institucional. De igual manera, el 22,8% de

los participantes en la encuesta indica que la seguridad informática se encuentra en un nivel alto, lo cual demuestra una opinión positiva sobre los mecanismos y controles empleados para salvaguardar la información y los sistemas informáticos. Por otra parte, el 17,4 % opina que esta variable se encuentra en un nivel bajo, lo cual demuestra la percepción de algunas falencias o carencias en las acciones de seguridad implementadas por la entidad. Los resultados en general indican que el nivel medio es predominante, lo que indica que se deben seguir reforzando las políticas, controles y estrategias de seguridad informática con el fin de aumentar la protección de los activos informáticos y disminuir los peligros relacionados con amenazas tecnológicas potenciales.

Tabla 6 Categoría Confidencialidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	4	4,3	4,3	4,3
	Medio	48	52,2	52,2	56,5
	Alto	40	43,5	43,5	100,0
	Total	92	100,0	100,0	

Fuente: Información recopilada de Confidencialidad proveniente de los trabajadores de la Municipalidad de Carquin, 2025.

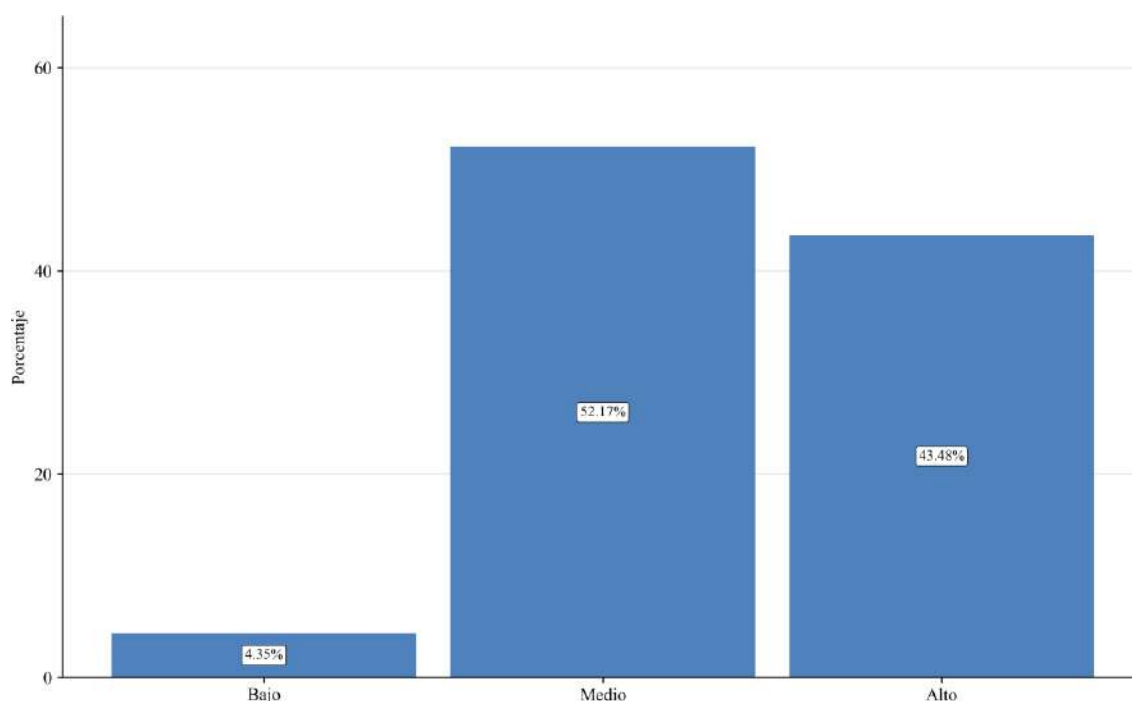


Gráfico 6 Confidencialidad

La Figura 6 muestra que el 52,2 % de los empleados de la Municipalidad Distrital de Carquín opina que la confidencialidad está en un nivel intermedio. Esto indica que la mayoría cree que las acciones tomadas para resguardar la información contra accesos o revelaciones no autorizadas son medianamente eficaces. También, el 43,5 % de los encuestados indica que este aspecto tiene un nivel alto, lo que muestra una evaluación positiva sobre los procedimientos puestos en marcha para asegurar que la información solo sea accesible para las personas autorizadas. Por otra parte, solo el 4.3 % de los empleados cree que la confidencialidad está en un nivel bajo, lo cual sugiere que una pequeña parte de ellos nota carencias importantes en cuanto a la protección de la información. En líneas generales, los resultados indican una inclinación positiva hacia niveles medio y alto de confidencialidad, lo que apunta a que la entidad ha adoptado medidas para proteger correctamente la información. Sin embargo, todavía

hay posibilidades de reforzar las regulaciones y establecer una cultura más robusta en términos de seguridad de la información.

Tabla 7 Categoría Integridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	30	32,6	32,6	32,6
	Medio	53	57,6	57,6	90,2
	Alto	9	9,8	9,8	100,0
	Total	92	100,0	100,0	

Fuente: Información recopilada de Integridad proveniente de los trabajadores de la Municipalidad de Carquin, 2025.

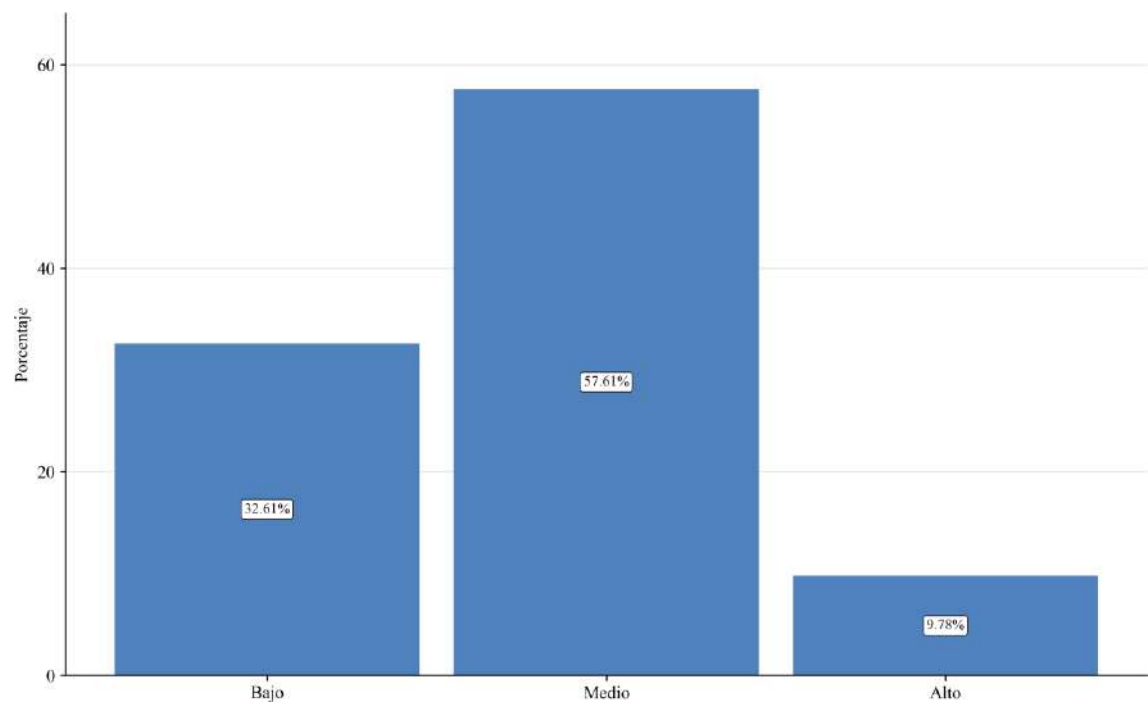


Gráfico 7 Integridad

La mayoría de los trabajadores de la Municipalidad Distrital de Carquín (57,6 %) considera que la integridad de la información está en un nivel medio, según lo muestra la Figura 7. Esto sugiere que los empleados creen que los datos tienen un grado aceptable de protección

ante alteraciones no autorizadas, así como también una consistencia y exactitud razonables, aunque todavía hay elementos que necesitan ser mejorados. Además, el 32,6% de los encuestados indica que esta dimensión está en un nivel bajo, lo cual demuestra que una porción significativa de empleados nota faltas en los procedimientos destinados a asegurar la veracidad y confiabilidad de la información institucional. En contraste, únicamente el 9,8 % cree que la integridad se encuentra en un nivel elevado, lo que muestra una apreciación positiva de un grupo pequeño de participantes. En términos generales, los resultados reflejan que, aunque el nivel medio es predominante, hay un porcentaje importante que considera que existen limitaciones en este aspecto. Esto indica la necesidad de reforzar los controles de validación, las medidas de protección y los mecanismos de auditoría destinados a mantener la precisión y consistencia de la información en los sistemas administrativos de la entidad.

Tabla 8 Categoría Disponibilidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	15	16,3	16,3	16,3
	Medio	47	51,1	51,1	67,4
	Alto	30	32,6	32,6	100,0
	Total	92	100,0	100,0	

Fuente: Información recopilada de Disponibilidad proveniente de los trabajadores de la Municipalidad de Carquin, 2025.

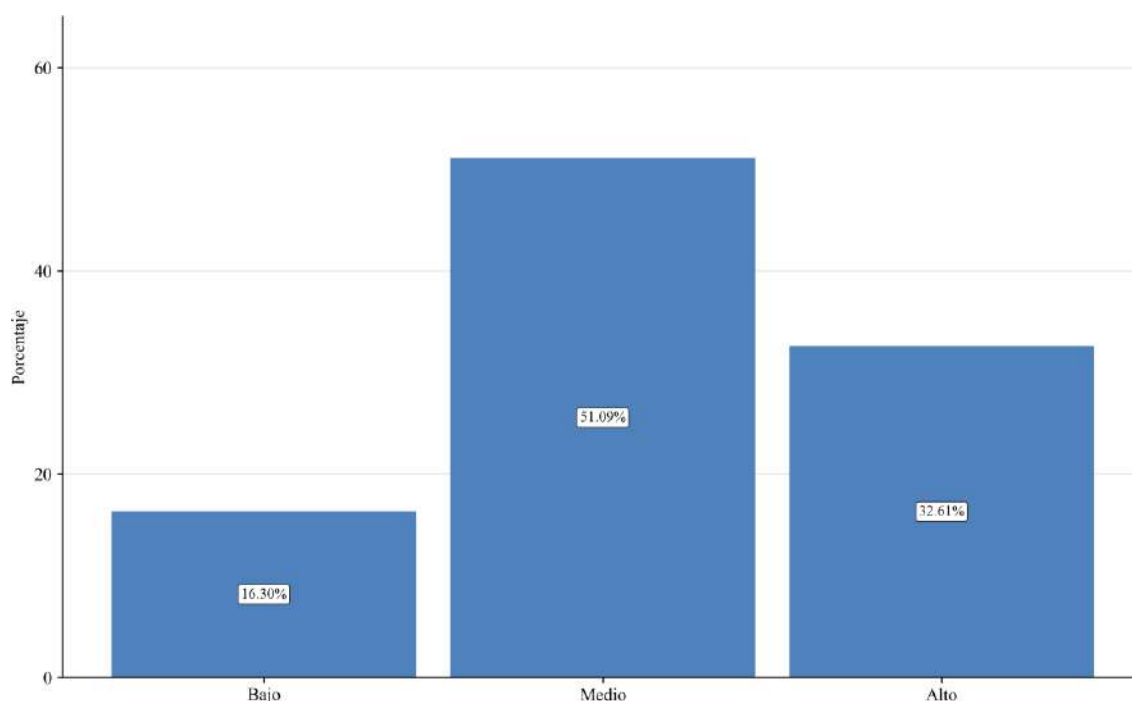


Gráfico 8 Disponibilidad

De acuerdo con la figura 8, el 51,1 % de los empleados de la Municipalidad Distrital de Carquín piensa que la disponibilidad de información está en un nivel medio. Esto sugiere que la mayoría considera que cuando se necesita, se pueden acceder a los datos y sistemas institucionales, pero aún hay elementos que podrían mejorarse para asegurar una continuidad más prolongada en los servicios. Igualmente, el 32,6% de los encuestados indica que este aspecto tiene un nivel elevado, lo cual demuestra una apreciación positiva con respecto a la habilidad de los sistemas para brindar acceso oportuno a la información y conservar la operatividad en los procedimientos institucionales. Por otro lado, un 16,3 % opina que la disponibilidad es baja, lo cual demuestra la percepción de algunas limitaciones relacionadas con el acceso a la información o con la continuidad de los servicios informáticos. Los resultados indican, en líneas generales, que el nivel medio es predominante y que existe una proporción significativa de valoraciones altas, lo cual sugiere que la entidad tiene condiciones adecuadas de disponibilidad. No obstante,

para optimizar el acceso continuo a la información y minimizar posibles interrupciones en los sistemas de gestión, es recomendable afianzar las medidas de respaldo, recuperación y continuidad operativa.

4.2. Contrastación de Hipótesis

4.2.1. Contrastación de Hipótesis General

a) Hipótesis General Nula (H_0)

La protección de datos no se relaciona significativamente con la seguridad informática en los sistemas de gestión de la Municipalidad de Carquin, 2025.

b) Hipótesis General Alternativa

La protección de datos se relaciona significativamente con la seguridad informática en los sistemas de gestión de la Municipalidad de Carquin, 2025.

c) Regla para Contrastar Hipótesis

Si se encontrase el valor de $p > 0,05$ se acepta H_0 . Si se encontrase el valor de $p < 0,05$ se rechaza H_0 .

Correlaciones: Protección de Datos y Seguridad Informática

		Protección de Datos	Seguridad Informática
Protección de Datos	Correlación de Spearman	1,000	,612
	Sig. (bilateral)	.	,000
	N	92	92
Seguridad Informática	Correlación de Spearman	,612	1,000
	Sig. (bilateral)	,000	.
	N	92	92

Interpretación

Los hallazgos muestran que hay una correlación positiva moderada entre la seguridad informática y la protección de datos ($r = 0,612$), lo cual señala que ambas variables tienen una relación directa: a medida que aumentan los grados de protección de datos en la organización, también se espera una mejora en los niveles de seguridad informática. La asociación es de intensidad moderada, según lo indica la magnitud del coeficiente de correlación; esto sugiere que el reforzamiento de los mecanismos, prácticas y políticas dirigidos a proteger los datos ayuda a aumentar la seguridad de los sistemas de información. Además, el valor de significación ($p < 0,001$) obtenida muestra que la relación observada tiene una alta significación estadística, lo que hace improbable que dicha asociación sea el resultado del azar. Por lo tanto, hay pruebas suficientes para sostener que la seguridad informática en los sistemas de gestión de la Municipalidad Distrital de Carquín está estrechamente vinculada a la protección de datos.

4.2.2. *Contrastación de Hipótesis Especifica 1*

a) Hipótesis General Nula (H_0)

La protección de datos no se relaciona significativamente con la confidencialidad en los sistemas de gestión de la Municipalidad de Carquin, 2025.

b) Hipótesis General Alternativa

La protección de datos se relaciona significativamente con la confidencialidad en los sistemas de gestión de la Municipalidad de Carquin, 2025.

c) Regla para Contrastar Hipótesis

Si se encontrase el valor de $p > 0,05$ se acepta H_0 . Si se encontrase el valor de $p < 0,05$ se rechaza H_0 .

Correlaciones: Protección de Datos y Confidencialidad

		Protección de Datos	Confidencialidad
Protección de Datos	Correlación de Spearman	1,000	,592
	Sig. (bilateral)	.	,000
	N	92	92
Confidencialidad	Correlación de Spearman	,592	1,000
	Sig. (bilateral)	,000	.
	N	92	92

Interpretación

Los hallazgos indican que hay una correlación positiva moderada entre la confidencialidad y la protección de datos ($r = 0,592$), lo que sugiere que ambas variables están directamente relacionadas. En esta línea, la confidencialidad de la información dentro de la organización tiende a aumentar a medida que las políticas, procedimientos y medidas para proteger los datos se van robusteciendo. El coeficiente de correlación tiene un tamaño moderado, lo que muestra que una gestión apropiada de la protección de datos ayuda a controlar el acceso a la información y disminuye el peligro de divulgaciones no autorizadas. De igual manera, el nivel de significancia obtenido ($p < 0,001$) ratifica que la relación observada tiene una alta significación estadística, lo cual posibilita descartar que los resultados sean producto de la casualidad. Por lo tanto, hay pruebas suficientes que demuestran que la protección de datos está relacionada de manera relevante con la confidencialidad en los sistemas de gestión de la Municipalidad Distrital de Carquín.

4.2.3. Contrastación de Hipótesis Específica 2

a) Hipótesis General Nula (H_0)

La protección de datos no se relaciona significativamente con la integridad en los sistemas de gestión de la Municipalidad de Carquin, 2025.

b) Hipótesis General Alternativa

La protección de datos se relaciona significativamente con la integridad en los sistemas de gestión de la Municipalidad de Carquin, 2025.

c) Regla para Contrastar Hipótesis

Si se encontrase el valor de $p > 0,05$ se acepta H_0 . Si se encontrase el valor de $p < 0,05$ se rechaza H_0 .

Correlaciones: Protección de Datos e Integridad

		Protección de Datos	Integridad
Protección de Datos	Correlación de Spearman	1,000	,543
	Sig. (bilateral)	.	,000
	N	92	92
Integridad	Correlación de Spearman	,543	1,000
	Sig. (bilateral)	,000	.
	N	92	92

Interpretación

Los resultados muestran una correlación positiva moderada entre la protección de datos y la integridad de la información ($r = 0,543$), lo cual señala que existe una conexión directa entre las dos variables. Esto quiere decir que, conforme se vuelven más robustas las políticas, los procesos y los mecanismos enfocados en la protección de datos, tienden a incrementarse también los niveles de integridad de la información. De esta manera, se asegura que los datos permanezcan sin alteraciones no autorizadas, completos y precisos. El coeficiente de correlación tiene una magnitud que muestra una asociación moderada, lo cual indica que proteger los datos de manera adecuada ayuda a mantener la consistencia y fiabilidad de la información institucional. Además, el valor de significancia obtenido ($p < 0,001$) corrobora que la relación observada tiene una alta relevancia estadística, lo que permite descartar que los resultados sean

producto del azar. Por lo tanto, hay suficiente evidencia para sostener que la integridad de la información en los sistemas de gestión de la Municipalidad Distrital de Carquín está estrechamente relacionada con la protección de datos.

4.2.4. *Contrastación de Hipótesis Específica 3*

a) Hipótesis General Nula (H_0)

La protección de datos no se relaciona significativamente con la disponibilidad en los sistemas de gestión de la Municipalidad de Carquin, 2025.

b) Hipótesis General Alternativa

La protección de datos se relaciona significativamente con la disponibilidad en los sistemas de gestión de la Municipalidad de Carquin, 2025.

c) Regla para Contrastar Hipótesis

Si se encontrase el valor de $p > 0,05$ se acepta H_0 . Si se encontrase el valor de $p < 0,05$ se rechaza H_0 .

Correlaciones: Protección de Datos y Disponibilidad

		Protección de Datos	Disponibilidad
Protección de Datos	Correlación de Spearman	1,000	,424
	Sig. (bilateral)	.	,000
	N	92	92
Disponibilidad	Correlación de Spearman	,424	1,000
	Sig. (bilateral)	,000	.
	N	92	92

Interpretación

Los hallazgos muestran una correlación positiva débil entre la protección de datos y la disponibilidad de información ($r = 0,424$). Esto señala que hay un vínculo directo entre las dos

variables, aunque es menos intenso en comparación con otras dimensiones estudiadas. Esto quiere decir que, conforme se van robusteciendo las medidas de protección de datos, la disponibilidad de los sistemas y la información tiende a aumentar, lo cual promueve que los usuarios autorizados puedan acceder a los recursos informáticos de manera oportuna. No obstante, la magnitud del coeficiente de correlación indica que otros elementos, como los planes de contingencia, la gestión de continuidad operativa, la infraestructura tecnológica y los mecanismos de respaldo, también podrían tener un impacto en la disponibilidad. Además, el valor de significancia obtenido ($p < 0,001$) confirma que la relación observada es muy significativa desde un punto de vista estadístico, lo que permite descartar que dicha asociación sea fortuita. Por lo tanto, hay pruebas suficientes para sostener que la disponibilidad de información en los sistemas de gestión tiene una relación importante con la protección de datos.

V. CAPITULO V: DISCUSIÓN

5.1. Discusión de Resultados

La asociación positiva entre las dos variables principales del estudio es moderada y altamente significativa. Un coeficiente de correlación de $\rho = 0.612$ y un valor p de $p < 0.001$ sugieren que, en la Municipalidad de Carquín, la protección de los sistemas de gestión de datos tiene un impacto directo en la seguridad de los sistemas. Esto enfatiza que las medidas legales y técnicas para la protección de la información procesada no son simplemente un requisito que aborda brechas y debilidades existentes en una subestructura; en cambio, representan las medidas de protección y el fortalecimiento de la resiliencia de dicha subestructura. Esto refuerza un entorno en el que existen medidas para la protección de la privacidad de la información; los sistemas de gestión operan dentro de un marco de confianza y control establecidos dentro de la institución.

Al considerar la protección de la privacidad de la información, los datos indican que la confidencialidad y la protección de los datos ($\rho = 0.592$, $p < 0.001$) están relacionadas. Esto significa que se mantiene la implementación de medidas de protección que aseguren que la información sea accesible solo para el personal autorizado, que se haga cumplir el control y que la información sensible de los ciudadanos no se exponga a usuarios externos. Este control garantiza el flujo de información dentro de la Administración Pública de la localidad, minimizando el riesgo de exposición que pondría en peligro la integridad y seguridad de la Administración Pública local.

En términos de integridad, hubo una correlación positiva moderada ($\rho = 0.543$, $p < 0.001$). Esto indica que la protección de los datos es importante en la gestión de los sistemas, de modo que la información no se altere, ni haya errores en el procesamiento de la información. En la gestión de los sistemas, la protección de los datos es importante en la indicación de que existe el procesamiento de la información y la protección de los datos en los sistemas y en la gestión de los sistemas, porque no hay errores en el procesamiento de los datos. Estos resultados muestran que la precisión de los datos protege la gestión municipal contra errores tanto en interrupciones accidentales como intencionales.

Finalmente, en relación con la disponibilidad, la investigación muestra una correlación positiva débil ($\rho = 0.424$, $p < 0.001$). Aunque esta correlación es la más débil entre las dimensiones, sigue siendo significativa. La protección de los datos asegura que la información esté accesible cuando sea necesaria, sin embargo, hay varias otras variables técnicas u operativas que influyen en la funcionalidad del sistema. Sin embargo, la provisión de datos, sin interrupciones, es el componente principal de la efectividad operativa. Esto asegura que los servidores municipales puedan proporcionar servicios ininterrumpidos y consistentes al personal y a los ciudadanos, evitando una parálisis en la prestación de servicios causada por interrupciones o bloqueos en los datos.

Una vez más, los resultados del estudio reafirman que la protección de los datos y la protección de los datos mediante ciberseguridad para la Municipalidad de Carquín, 2025, son de carácter interdependiente y estratégico. El fortalecimiento de ambos sistemas en conjunto no debe considerarse simplemente como un sistema técnico y defensivo, sino que proporciona la garantía de los sistemas modernos de administración pública, tanto continuos como transparentes, presentando un sistema más confiable y robusto.

VI. CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

La investigación utilizando la correlación de Spearman analizó los datos para el año 2025 y encontró una relación positiva moderada y altamente significativa de $\rho = 0.612$ para las variables de protección de datos y seguridad de la información para el Municipio de Carquín. Se encuentra que la gestión legal y técnica de los datos personales no es una actividad separada. Más bien, es una actividad clave que integra y fortalece las demás actividades del municipio. La correcta gestión de los mecanismos de protección de la privacidad ayuda a disminuir las oportunidades de riesgo y permite que la infraestructura tecnológica del municipio gestione sus operaciones con un mayor nivel de confianza y acompañamiento institucional.

En cuanto a la protección de la privacidad, se ha demostrado que la protección adecuada de los datos sensibles y la implementación estricta del control de acceso tienen una relación positiva directa y significativa con la seguridad global de los sistemas con un valor de $\rho = 0.592$. Se asegura que los datos de los ciudadanos y los archivos internos del municipio estén en manos del personal autorizado, para lo cual existen las salvaguardas adecuadas, y se mantiene el control de la información del Portal de Transparencia. Esta gestión de la privacidad es primordial para evitar la exposición de datos sensibles de carácter personal que, en el marco de la transparencia, están protegidos cuando el municipio implementa sus servicios digitalmente.

La investigación recopilada fundamenta que la integridad de los datos es un factor importante para la confiabilidad de los sistemas de gestión administrativa como el SIAF y el SIGA ($\rho=0.543$). Mantener datos registrados con precisión y sin alteraciones de finanzas y logística es sumamente crítico para evitar errores en la ejecución de presupuestos y en la

adquisición de bienes y servicios. Se deduce que a través de la protección rigurosa de la integridad de los datos, se eliminan discrepancias técnicas, y toda la gestión municipal de suministros y tesorería se basa en datos confiables, lo cual es un elemento importante para una rendición de cuentas transparente frente a las agencias de control correspondientes.

En el área de disponibilidad, se indica que hay una relación positiva, aunque débil ($\rho=0.424$), con la operatividad de los servicios municipales. Aunque la protección de datos genera una garantía del funcionamiento de los servicios, la disponibilidad depende de varios otros factores técnicos, como el estado de la red y el soporte ante incidentes de servicio. Sin embargo, la protección de los servicios para evitar interrupciones y garantizar un servicio eficiente en el Distrito de Carquín son de extrema importancia y los servicios operativos del sistema para los usuarios autorizados son, por tanto, de máxima prioridad.

La última conclusión que muestra el estudio es que los empleados califican la protección de datos y la seguridad de la información en un nivel "medio" (más del 60% en varias escalas). Esto demuestra que hay espacio para mejorar para el horizonte de 2025, cuando enfrentaremos ataques de ransomware y phishing más sofisticados. Se puede afirmar que el municipio debe pasar de un enfoque fragmentado de protección de datos a un enfoque integrado de protección y seguridad de datos que sea digitalmente resistente a los desafíos del compromiso constructivo y positivo con los ciudadanos, quienes son más digitalmente sofisticados.

6.2. Recomendaciones

Se recomienda que la alta dirección del Municipio de Carquín establezca formalmente un Sistema de Gestión de Seguridad de la Información que cumpla con la norma ISO/IEC 27001, conforme a las indicaciones de la Oficina de la Secretaría de Gobierno y Transformación Digital, en conjunto con la Unidad de TI. El objetivo principal es proteger el sistema SIAF-RP y el sistema SIGA-MEF para facilitar la transición de una gestión de TI ad hoc a una gestión de Gobierno de TI más proactiva y estructurada. En este contexto, la clasificación de los activos de información permitiría el uso de medidas de gestión de TI y organización apropiadas y proporcionales al nivel de riesgo, asegurando que existan medidas de gestión adecuadas para la administración presupuestaria frente a las amenazas existentes en el entorno digital.

Es necesario actualizar las políticas de control de acceso institucional a un marco de "Cero Confianza" y crear un sistema de Gestión de Identidad y Acceso (IAM) más integral. En este contexto, se deben implementar medidas de control más estrictas, como la Autenticación Multifactor (MFA), para todo el personal que tenga acceso a bases de datos sensibles y/o interactúe con el Portal de Transparencia. Se debe implementar un proceso automático para oscurecer los datos personales publicados en un documento oficial, para garantizar la integridad de los datos públicos y la privacidad del ciudadano. Esto debe hacerse en sentido estricto para cumplir con la Ley de Protección de Datos Personales.

Para mejorar la confiabilidad de sus flujos de trabajo administrativos, recomiendan el uso completo de firmas digitales y canales encriptados para la interoperabilidad entre SIGA y SIAF. Siempre que el municipio utilice encriptación y certificados digitales emitidos por la plataforma nacional "Firma Perú," el municipio podrá mantener la integridad de documentos clave (por ejemplo, órdenes de compra y documentos de tesorería). Esto ayudará a reducir la amenaza de

manipulación (ya sea interna o externa) y disminuirá la necesidad de controles manuales.

También aumentará la velocidad de ejecución de los gastos públicos con un mayor nivel de garantía de transparencia.

Para enfrentar los desafíos de continuidad operativa ante el aumento previsto de ataques de ransomware en 2025, se recomienda una actualización completa del Plan de Recuperación ante Desastres (DRP), acompañada de un cronograma para simulacros planificados. El municipio debe invertir en sistemas de respaldo de datos con protección contra modificaciones (inmutables) y almacenamiento en air-gapped (offline). Esto asegura que la capacidad de restaurar los sistemas del municipio que proporciona el servicio de recaudación de impuestos y el servicio de atención a ciudadanos en sus solicitudes esté inmediatamente funcional, incluso en caso de un ataque que exija rescate de datos. Se debe enfatizar que el uso de sistemas de respaldo en la nube es una medida inadecuada. Se requiere un enfoque integral para minimizar la interrupción de los servicios.

La recomendación siete sugiere establecer un programa de capacitación institucional permanente para todos los funcionarios sobre “Higiene Cibernética” y los riesgos que puede conllevar la Inteligencia Artificial ofensiva. Los ataques de phishing personalizados y el robo de identidad facilitados por tecnología deepfake son desafíos urgentes y los empleados deben ser capacitados en la primera línea de defensa. Para complementar esta estrategia, se formalizará el nombramiento de un Oficial de Seguridad Digital (OSD) que supervise el fortalecimiento de la cultura de seguridad mediante una orden del alcalde. Esto asegurará que la transformación digital de Carquín sea sostenible, ética y confiable para la comunidad.

VII. REFERENCIAS

7.1. Fuentes bibliográficas

Autoridad Nacional de Protección de Datos. (2021). Guía para el tratamiento de datos personales. (ANPD), 17.

Ávila-Coello, A. A. (2024). *Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano*. Guayaquil: Journal of Economic and Social Science Research.

Delgado Ramos, D. (2022). *La protección de datos personales en la era digital*. Lima: PUCP.

Díaz Sandoval, M. E. (2024). *Análisis del nivel de seguridad de la información de la oficina de informática y telecomunicaciones de la Municipalidad Distrital de San Juan Bautista – 2023*. Lima: Universidad Científica del Perú.

Gómez Vieites, Á. (2021). *Seguridad de la información: amenazas, riesgos y contramedidas*. Madrid: RA-MA.

Mata García, A. E. (2025). *Ciberseguridad para todos. Aprende, protege y responde. Ediciones de la U / Ra-Ma Editorial*. Paracuellos de Jarama: Ra-Ma S.A. Editorial y Publicaciones.

Melgarejo Solórzano, J. M. (2023). *Las medidas de seguridad y la interceptación de datos informáticos en la regulación peruana 2021-2022*. Trujillo: Universidad Privada del Norte (UPN).

Rodríguez, J. L. (2021). *Protección de datos personales y derecho a la privacidad*. Madrid: Dykinson.

Sevillano Jaén, F. &. (2022). *Dirección de seguridad y gestión del ciberriesgo*. Bogota: Ediciones de la U.

Stallings, W. (2021). *Criptografía y seguridad de redes: principios y práctica*. Madrid: Pearson Educación.

T Montano, R. E. (2025). *Gobierno digital y protección de datos personales en la administración pública*. Lima: Sapere.

Torres Montano, R. E. (2025). *Gobierno digital y protección de datos personales en la administración pública peruana*. Lima: Sapere.

Vasco Delgado, J. C. (2025). *Ciberseguridad y protección de datos personales: desafíos y perspectivas. Fundación GADE / GADE: Revista Científica (revista semestral en acceso abierto)*, 5.

Whitman, M. E. (2020). *Principios de seguridad de la información*. México: Cengage Learning.

VIII. ANEXOS

8.1. MATRIZ DE CONSISTENCIA

Protección de Datos y Seguridad Informática en los sistemas de Gestión de la Municipalidad de Carquin, 2025.

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
<u>Problema General</u> ¿Qué relación existe entre la protección de datos y la seguridad informática en los sistemas de gestión de la Municipalidad de Carquin, 2025? <u>Problemas específicos</u> ¿Cómo se relaciona la protección de datos con la confidencialidad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025? ¿De qué manera la protección de datos se	<u>Objetivos General</u> Determinar la relación entre la protección de datos y la seguridad informática en los sistemas de gestión de la Municipalidad de Carquin, 2025. <u>Objetivos específicos</u> Analizar la relación entre la protección de datos y la confidencialidad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025.	<u>Hipótesis General</u> Existe una relación significativa entre la protección de datos y la seguridad informática en los sistemas de gestión de la Municipalidad de Carquin, 2025. <u>Hipótesis específicas</u> Existe una relación significativa entre la protección de datos y la confidencialidad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025.	VARIABLE INDEPENDIENTE (X): Protección de Datos			
			DIMENSIONES	INDICADORES	Ítem	Nivel/Rango
			Políticas de protección de datos	- Existencia de normas internas. - Cumplimiento de políticas.	1,2,	Nunca
			Control de acceso a la información	- Autenticación de usuarios. - Restricción según funciones.	3,4	Casi nunca A veces

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
relaciona con la integridad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025? ¿Qué relación existe entre la protección de datos y la disponibilidad de los sistemas de gestión de la Municipalidad de Carquin, 2025?	- Evaluar la relación entre la protección de datos y la integridad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025. - Examinar la relación entre la protección de datos y la disponibilidad de los sistemas de gestión de la Municipalidad de Carquin, 2025.	- Existe una relación significativa entre la protección de datos y la integridad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025. - Existe una relación significativa entre la protección de datos y la disponibilidad de la información en los sistemas de gestión de la Municipalidad de Carquin, 2025.	Manejo y tratamiento de datos	- Uso responsable de la información. - Confidencialidad de datos.	5,6	Siempre Casi Siempre
			VARIABLE DEPENDIENTE (Y): Seguridad Informática			
			DIMENSIONES			
			DIMENSIONES	INDICADORES	Ítem Nivel/Rango	
			Confidencialidad	- Protección contra accesos no autorizados. - Gestión de permisos.	7,8	Nunca Casi nunca
			Integridad	- Protección contra alteraciones. - Confiabilidad de la información.	9,10	A veces Siempre

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
			Disponibilidad	• Acceso oportuno a sistemas. • Recuperación de información.	11,12	Casi Siempre

8.2. CUESTIONARIO

El objetivo de esta encuesta es recopilar información sobre la Protección de Datos y Seguridad Informática en los sistemas de gestión de la Municipalidad de Carquin, 2025. A través de este cuestionario se busca analizar cómo la protección de datos y la seguridad informática influyen en los sistemas de gestión de la Municipalidad de Carquin, considerando aspectos como la protección de la información, la gestión de riesgos tecnológicos, la implementación de políticas de seguridad, los planes de contingencia, la capacitación del personal y la infraestructura tecnológica. Los datos obtenidos permitirán evaluar el nivel de seguridad informática existente en los sistemas de gestión municipal, contribuyendo a identificar áreas de mejora y fortalecer la toma de decisiones orientadas a una gestión institucional más segura, eficiente y confiable. La encuesta es completamente anónima y la información recopilada será utilizada exclusivamente con fines académicos, garantizando en todo momento la confidencialidad de las respuestas. Agradecemos su valiosa participación en este estudio.

Por favor marque con una equis (X) en el espacio correspondiente:

a. Género

Masculino	
Femenino	

I. Instrucciones

En el esquema marcar con una tacha o encierra tu respuesta según considere usted su correspondencia teniendo en cuenta la escala de calificación que aparece.

CUESTIONARIO

NIVEL DE PROTECCIÓN DE DATOS

DIMENSIÓN: Políticas de protección de datos

1. ¿La Municipalidad de Carquin cuenta con normas internas claramente establecidas para la protección de los datos institucionales?

- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca

2. ¿Las políticas internas sobre protección de datos se cumplen adecuadamente en las actividades diarias?

- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca

DIMENSIÓN: Control de acceso a la información

3. ¿El acceso a los sistemas de gestión se realiza mediante mecanismos de autenticación personal (usuario y contraseña)?

- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca

4. ¿El acceso a la información está restringido de acuerdo con las funciones y responsabilidades del personal?

- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca

DIMENSIÓN: Manejo y tratamiento de datos

5. ¿ La información institucional se utiliza de manera responsable y únicamente para fines laborales?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

6. ¿ Los datos sensibles y confidenciales están adecuadamente protegidos dentro de los sistemas de gestión?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

NIVEL DE SEGURIDAD INFORMÁTICA**DIMENSIÓN: Confidencialidad**

7. ¿ Los sistemas de gestión cuentan con mecanismos que evitan accesos no autorizados a la información?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

8. ¿ La asignación de permisos de acceso a los sistemas es adecuada según el rol del usuario?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

DIMENSIÓN: Integridad

9. ¿ Los sistemas de gestión protegen la información contra modificaciones no autorizadas?

- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca

10. ¿ La información almacenada en los sistemas de gestión es confiable y precisa?

- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca

DIMENSIÓN: Disponibilidad

11. ¿ Los sistemas de gestión están disponibles cuando se requieren para el desarrollo de las actividades laborales?

- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca

12. ¿ Existen mecanismos que permiten recuperar la información ante fallas o incidentes informáticos?

- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca