Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela de Ingeniería de Sistemas

Seguridad informática y toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025

Tesis

Para optar el Título Profesional de Ingeniero de Sistemas

Autor

Rodolfo Alberto Sanchez Espinoza

Asesor

Ing. Henry Marcial Arevalo Flores

HENRY MARCIAL AREVALO FLORES
INGENIERO INDUSTRIAL
Reg. CIP N° 108718

Huacho – Perú

2026

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 de Ingeniería de Sistemas

METADATOS

DATOS DEL AUTOR (ES):		
APELLIDOS Y NOMBRES	**DNI**	**FECHA DE SUSTENTACIÓN**
Rodolfo Alberto Sanchez Espinoza	09391723	30 de abril del 2026
DATOS DEL ASESOR:		
APELLIDOS Y NOMBRES	**DNI**	**CÓDIGO ORCID**
Henry Marcial Arevalo Flores	15723233	https://orcid.org/0000-0003-2958-9464
DATOS DE LOS MIEMBROS DE JURADOS – PREGRADO/POSGRADO-MAESTRÍA-DOCTORADO:		
APELLIDOS Y NOMBRES	**DNI**	**CÓDIGO ORCID**
Teodorico Jamanca Alberto	15604418	https://orcid.org/0000-0002-9739-6683
Carlos Enrique Bernal Valladares	15614554	https://orcid.org/0000-0002-7421-9537
Ronald Demetrio Flores Flores	15300224	https://orcid.org/0000-0003-4211-7285

Rodolfo Alberto Sanchez Espinoza

Seguridad informática y toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 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:::1:3536317975

Fecha de entrega
13 abr 2026, 1:26 p.m. GMT-5

Fecha de descarga
14 abr 2026, 8:12 a.m. GMT-5

Nombre del archivo
SANCHEZ.pdf

Tamaño del archivo
1.8 MB

75 páginas

13.706 palabras

85.580 caracteres

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

17% Fuentes de Internet
6% Publicaciones
10% 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

Dedico este trabajo de investigación a Dios, por brindarme fortaleza y sabiduría para superar cada desafío presentado durante mi formación profesional.

A mis padres Emilio y Florinda y a mi esposa Sandra é hijos Joan y Kevín de igual familia, por su apoyo incondicional, confianza y motivación constante. Gracias por acompañarme en cada etapa de este camino y ser el principal impulso para alcanzar esta importante meta académica y profesional.

AGRADECIMIENTO

A lo largo de este camino, comprendí que una tesis no se escribe en soledad, sino que se construye con la presencia, el apoyo y la paciencia de muchas personas que, de distintas formas, hicieron posible que este proyecto llegara a buen puerto por ello agradezco.

A Dios, por su infinita bondad y misericordia, por concederme la fortaleza, la sabiduría y la perseverancia necesarias para no rendirme ante las dificultades, y por permitirme alcanzar este sueño tan anhelado que hoy, gracias a Él, se hace realidad.

Dedico el presente trabajo de investigación, con el corazón lleno de amor y gratitud, a mis padres, Emilio Oswaldo Sánchez Salazar y Florinda Espinoza Becerra, quienes, aunque hoy no se encuentran físicamente a mi lado, viven en cada uno de mis pensamientos, decisiones y logros. Sus enseñanzas, principios y valores dejaron una huella imborrable en mi vida y continúan guiando mi caminar personal y profesional. Este título es, en esencia, reflejo de su ejemplo, de su sacrificio y del camino que con tanto amor me enseñaron a seguir.

A mi esposa, Sandra Patricia Díaz Mosquera, por su amor incondicional, su comprensión infinita y su paciencia constante a lo largo de este exigente proceso académico. Su fortaleza, apoyo silencioso y fe inquebrantable en mí fueron el sostén que me permitió avanzar incluso en los momentos más difíciles; este logro también le pertenece.

A mis hijos, Joan Alberto Sánchez Díaz y Kevín Adrián Sánchez Díaz, por ser la luz que ilumina mis días y la razón más profunda para seguir superándome. Su amor sincero y su alegría diaria dieron sentido a cada esfuerzo, a cada sacrificio y a cada paso dado para alcanzar este objetivo profesional.

De manera especial, a mi hermano, Mario Enrique Sánchez Espinoza, por su apoyo incondicional y consejos oportunos, fundamentales en momentos decisivos de este camino. Asimismo, expreso mi más sincero agradecimiento a la señora Enna Figueroa, por su constante motivación y sus palabras de aliento para culminar este objetivo profesional; un abrazo hasta el cielo, con eterna gratitud.

Finalmente, a mis familiares y amigos, quienes de una u otra manera contribuyeron para alcanzar mis objetivos profesionales.

Con profundo agradecimiento, dedico este logro a todos ellos, quienes forman parte esencial de esta historia y de este sueño cumplido.

ÍNDICE

RESUMEN

La presente investigación tuvo como objetivo determinar la relación entre la seguridad informática y la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima durante el año 2025. El estudio se desarrolló bajo un enfoque cuantitativo, de tipo básico, nivel correlacional y diseño no experimental de corte transversal. La población estuvo conformada por 380 trabajadores del Gobierno Regional de Lima y la muestra por 192 colaboradores, seleccionados mediante fórmula estadística. Para la recolección de datos se empleó la técnica de la encuesta y como instrumento un cuestionario estructurado con escala tipo Likert.

Los resultados evidenciaron que el 64.58% de los trabajadores perciben un nivel alto de seguridad informática, mientras que el 44.27% consideran que la toma de decisiones presenta un nivel alto. Asimismo, se identificó que la confidencialidad, integridad y disponibilidad de la información influyen significativamente en la calidad, oportunidad y confiabilidad de los datos utilizados en los procesos decisionales. El análisis estadístico mediante el coeficiente de correlación de Spearman permitió comprobar la existencia de una relación significativa entre las variables estudiadas.

Se concluye que una adecuada seguridad informática fortalece la calidad de la información y mejora la toma de decisiones dentro de los sistemas de gestión del Gobierno Regional de Lima. Por ello, resulta fundamental implementar políticas de seguridad, mecanismos de control y estrategias de protección de datos que contribuyan a optimizar la gestión pública y garantizar decisiones más eficientes, transparentes y confiables.

Palabras clave: seguridad informática, toma de decisiones, sistemas de gestión, información, gestión pública.

ABSTRACT

The objective of this research was to determine the relationship between information security and decision-making in the management systems of the Regional Government of Lima during 2025. The study was developed under a quantitative approach, basic type, correlational level, and non-experimental cross-sectional design. The population consisted of 380 workers from the Regional Government of Lima, and the sample included 192 employees selected through a statistical formula. Data collection was carried out using the survey technique and a structured questionnaire with a Likert-type scale as the instrument.

The results showed that 64.58% of the workers perceived a high level of information security, while 44.27% considered that decision-making was at a high level. Likewise, it was identified that the confidentiality, integrity, and availability of information significantly influence the quality, timeliness, and reliability of the data used in decision-making processes. Statistical analysis using Spearman's correlation coefficient confirmed the existence of a significant relationship between the studied variables.

It is concluded that adequate information security strengthens information quality and improves decision-making within the management systems of the Regional Government of Lima. Therefore, it is essential to implement security policies, control mechanisms, and data protection strategies that contribute to optimizing public management and ensuring more efficient, transparent, and reliable decisions.

Keywords: information security, decisión making, management systems, information, public management.

INTRODUCCIÓN

En el contexto contemporáneo de transformación digital, las organizaciones públicas enfrentan el desafío constante de integrar tecnologías de información en sus procesos administrativos y estratégicos, con el objetivo de optimizar la eficiencia, transparencia y calidad de los servicios ofrecidos a la ciudadanía. En este escenario, la seguridad informática emerge como un componente crítico que no solo garantiza la protección de los activos digitales, sino que también incide directamente en la confiabilidad de la información utilizada para la toma de decisiones. En el caso del Gobierno Regional de Lima, cuya estructura administrativa gestiona múltiples sistemas de información orientados a la planificación, ejecución y control de políticas públicas, resulta imprescindible analizar cómo las prácticas de seguridad informática influyen en la calidad y oportunidad de las decisiones institucionales durante el año 2025.

La creciente dependencia de los sistemas de gestión digitalizados ha generado una exposición significativa a riesgos tecnológicos, tales como accesos no autorizados, pérdida de información, ataques cibernéticos y vulnerabilidades en la infraestructura tecnológica. Estos riesgos no solo comprometen la integridad, confidencialidad y disponibilidad de los datos, sino que también afectan la capacidad de los directivos y funcionarios para tomar decisiones informadas y oportunas. En este sentido, la seguridad informática deja de ser un aspecto meramente técnico para convertirse en un factor estratégico que condiciona la gobernanza institucional y la gestión pública eficiente.

La toma de decisiones en el sector público se caracteriza por su complejidad, ya que involucra múltiples variables, actores y niveles de responsabilidad. En el Gobierno Regional de Lima, los sistemas de gestión constituyen la principal fuente de información para la formulación de políticas, asignación de recursos y evaluación de resultados. Por ello, la calidad de la información procesada en estos sistemas es determinante para asegurar decisiones acertadas. Sin embargo, cuando los mecanismos de seguridad informática son deficientes o insuficientes, se incrementa el riesgo de que la información sea alterada, incompleta o poco confiable, lo cual puede derivar en decisiones erróneas con impactos negativos en la gestión pública y en la ciudadanía.

Asimismo, es importante considerar que la implementación de políticas de seguridad informática no solo implica la adopción de herramientas tecnológicas, sino también el desarrollo de una cultura organizacional orientada a la protección de la información. Esto incluye la capacitación del personal, la definición de protocolos de acceso, la gestión de riesgos y la aplicación de normativas y estándares internacionales en materia de seguridad de la información. En el ámbito del Gobierno Regional de Lima, la madurez de estas prácticas puede influir significativamente en la forma en que los funcionarios perciben, procesan y utilizan la información disponible para la toma de decisiones.

Por otro lado, el entorno normativo peruano ha venido fortaleciendo progresivamente los lineamientos relacionados con la seguridad digital en las entidades públicas, promoviendo la adopción de marcos de referencia que permitan garantizar la protección de los sistemas de información. No obstante, la brecha entre la normativa y su implementación efectiva sigue siendo un desafío latente. En muchos casos, las entidades públicas enfrentan limitaciones presupuestales,

técnicas y humanas que dificultan la consolidación de sistemas de seguridad robustos. Esta situación genera un contexto de vulnerabilidad que puede afectar la calidad de la gestión institucional y la confianza de la ciudadanía en las decisiones adoptadas por sus autoridades.

En este marco, resulta pertinente abordar la relación entre la seguridad informática y la toma de decisiones desde una perspectiva integral que considere tanto los aspectos tecnológicos como organizacionales. La seguridad informática no solo debe entenderse como un mecanismo de protección, sino también como un habilitador de procesos decisionales eficientes. Cuando los sistemas de gestión cuentan con adecuados niveles de seguridad, se facilita el acceso a información confiable, se reduce la incertidumbre y se fortalece la capacidad analítica de los tomadores de decisiones. Por el contrario, la ausencia de controles adecuados puede generar desinformación, retrasos y errores que comprometen la efectividad de las acciones gubernamentales.

La relevancia de esta investigación radica en la necesidad de evidenciar cómo las condiciones de seguridad informática impactan en la calidad de la toma de decisiones en el Gobierno Regional de Lima, particularmente en un contexto de creciente digitalización y exposición a riesgos cibernéticos. El análisis de esta relación permitirá identificar brechas, debilidades y oportunidades de mejora en los sistemas de gestión institucional, contribuyendo al fortalecimiento de la gestión pública regional. Además, proporcionará insumos relevantes para la formulación de estrategias orientadas a mejorar la seguridad de la información y, por ende, la calidad de las decisiones adoptadas por los funcionarios públicos.

Cabe destacar que la toma de decisiones no es un proceso aislado, sino que se encuentra estrechamente vinculado con la disponibilidad y calidad de la información, así como con los mecanismos de control y seguridad que la respaldan. En este sentido, la seguridad informática actúa como un elemento transversal que influye en todas las etapas del proceso decisional, desde la recolección y almacenamiento de datos hasta su análisis y utilización en la formulación de políticas. Por ello, su adecuada gestión resulta fundamental para garantizar la coherencia, transparencia y efectividad de las decisiones en el ámbito público.

En el caso específico del Gobierno Regional de Lima, la diversidad de áreas funcionales y la complejidad de sus sistemas de gestión requieren un enfoque integral de seguridad informática que contemple tanto la protección de la infraestructura tecnológica como la gestión de los riesgos asociados al factor humano. La interacción entre estos elementos configura un entorno en el que la seguridad de la información se convierte en un determinante clave de la calidad institucional. En consecuencia, el estudio de esta problemática permitirá comprender mejor las dinámicas internas de la organización y su impacto en la toma de decisiones.

Finalmente, la presente investigación se justifica en la necesidad de generar conocimiento aplicado que contribuya al fortalecimiento de la gestión pública en el ámbito regional. Al analizar la relación entre la seguridad informática y la toma de decisiones, se busca no solo identificar problemáticas existentes, sino también proponer alternativas de solución que permitan mejorar la eficiencia, transparencia y confiabilidad de los sistemas de gestión del Gobierno Regional de Lima. En un contexto en el que la información se ha convertido en un activo estratégico, garantizar su

seguridad es un requisito indispensable para una adecuada toma de decisiones y, en última instancia, para el desarrollo sostenible de la región.

I. CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

En la actualidad, las organizaciones públicas enfrentan una creciente dependencia de los sistemas de información para la gestión eficiente de sus procesos, la planificación institucional y la toma de decisiones estratégicas. A nivel internacional, los gobiernos se han visto expuestos a un aumento significativo de ciberataques, accesos no autorizados y manipulación de información, los cuales afectan directamente la calidad y confiabilidad de los datos utilizados para la toma de decisiones. Según el Global Cybersecurity Outlook 2023 del World Economic Forum, más del 25% de los ataques reportados se dirigen a instituciones estatales, ocasionando interrupciones de servicios, pérdida de información crítica y decisiones administrativas basadas en información incompleta o alterada. Esta situación evidencia la necesidad de fortalecer la seguridad informática como pilar fundamental para asegurar que los datos utilizados en los procesos de análisis y toma de decisiones sean confiables, íntegros y oportunos.

En el contexto nacional, el Perú continúa experimentando un proceso acelerado de digitalización en las entidades del sector público. Sin embargo, diversas instituciones aún presentan vulnerabilidades en la protección de datos, deficiencias en la gestión de riesgos informáticos y limitaciones en la implementación de políticas efectivas de seguridad digital. Informes de la Contraloría General de la República (2022) advierten que muchas entidades públicas carecen de mecanismos adecuados para garantizar la integridad, disponibilidad y confidencialidad de la información utilizada en la toma de decisiones institucionales. Estos problemas generan riesgos como decisiones incorrectas basadas en datos alterados, retrasos en procesos administrativos y disminución de la confianza ciudadana en la gestión pública.

A nivel regional, el Gobierno Regional de Lima enfrenta desafíos similares. Sus sistemas de gestión administrativa, presupuestal, logística, de recursos humanos y de ejecución de proyectos dependen del flujo constante y seguro de información. Sin embargo, se han identificado brechas en la seguridad informática relacionadas con el control de accesos, la protección de datos sensibles, la integridad de la información almacenada en bases institucionales y la capacidad de prevenir o detectar modificaciones no autorizadas. Estas debilidades comprometen la calidad de los datos que utilizan los funcionarios y directivos para la toma de decisiones, afectando la eficiencia de la gestión pública, la priorización de recursos, la supervisión de obras y la planificación de intervenciones en beneficio de la ciudadanía.

Asimismo, la inexistencia o insuficiencia de protocolos formales de seguridad informática, la falta de monitoreo continuo de los sistemas de información, la debilidad en la gestión de riesgos tecnológicos y la limitada capacitación del personal en prácticas seguras incrementan la probabilidad de incidentes que puedan alterar la información institucional. Estas situaciones generan escenarios donde las decisiones administrativas se realizan con datos incompletos, desactualizados o vulnerados, afectando la transparencia, la eficiencia y la eficacia de la gestión regional.

En síntesis, la problemática central radica en que la seguridad informática insuficiente en el Gobierno Regional de Lima puede comprometer directamente la integridad, confiabilidad y disponibilidad de la información utilizada para la toma de decisiones en los sistemas de gestión. Ello podría derivar en decisiones erróneas, retrasos operativos, asignación inadecuada de recursos y afectación de los servicios ofrecidos a la población. Ante ello, es fundamental desarrollar un estudio que permita identificar las brechas existentes, evaluar la seguridad

informática actual y su incidencia en la toma de decisiones, y proponer estrategias que fortalezcan la gestión pública regional durante el año 2025.

1.2. Formulación del problema

Problema general

¿Qué relación existe entre la seguridad informática y la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025?

Problemas específicos

¿Cómo se relaciona la seguridad informática con la calidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025?

¿De qué manera la seguridad informática influye en la oportunidad y actualización de la información disponible para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025?

¿Qué relación existe entre la seguridad informática y la confiabilidad de los datos que sustentan la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025?

1.3. Objetivos de la investigación

Objetivo general

Determinar la relación entre la seguridad informática y la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

Objetivos específicos

Analizar cómo la seguridad informática se relaciona con la calidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

Evaluar de qué manera la seguridad informática influye en la oportunidad y actualización de la información disponible para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

Examinar la relación entre la seguridad informática y la confiabilidad de los datos utilizados en la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

1.4. Justificación de la investigación

La presente investigación se justifica por la creciente importancia que ha adquirido la seguridad informática en las entidades públicas, especialmente en lo referido al uso de información para la toma de decisiones. En un contexto donde los gobiernos dependen de sistemas digitales para gestionar recursos, administrar procesos y atender a la ciudadanía, asegurar la integridad, confidencialidad y disponibilidad de los datos se convierte en un factor crítico para garantizar decisiones oportunas, fundamentadas y efectivas.

Desde una perspectiva teórica, este estudio contribuye al fortalecimiento del conocimiento sobre la relación entre la seguridad informática y la toma de decisiones en instituciones gubernamentales. Explorar cómo los mecanismos de protección de datos, los protocolos de acceso, la gestión de riesgos informáticos y las políticas de seguridad inciden en la calidad, confiabilidad y oportunidad de la información permite generar evidencia que aporte al desarrollo de modelos de gestión digital más robustos. Asimismo, la investigación amplía el

marco conceptual existente al vincular dos variables estratégicas: la seguridad informática (como garante de la información) y la toma de decisiones (como proceso clave en la gestión pública).

En términos prácticos, el estudio permitirá identificar las brechas y vulnerabilidades existentes en los sistemas de gestión del Gobierno Regional de Lima, evaluando cómo estas limitaciones impactan en la obtención, procesamiento y análisis de datos utilizados por los funcionarios y directivos. Los resultados servirán para proponer mejoras concretas en la seguridad de la información, fortaleciendo la calidad de los datos que sustentan la toma de decisiones administrativas, presupuestales, logísticas y de planificación estratégica. Esto permitirá reducir errores, evitar decisiones basadas en información alterada o incompleta, y optimizar los procesos institucionales.

Desde un enfoque social, la relevancia de esta investigación radica en que decisiones adecuadas, informadas y oportunas impactan directamente en la calidad de los servicios públicos, la asignación de recursos, la supervisión de obras y la implementación de políticas regionales. La seguridad de la información no solo protege datos institucionales, sino también información sensible de la ciudadanía, promoviendo confianza, transparencia y eficiencia en la gestión pública.

Finalmente, en el marco institucional y nacional, el fortalecimiento de la seguridad informática y su integración con procesos de toma de decisiones se alinea con las recomendaciones de organismos nacionales e internacionales que promueven la gobernanza digital, la ciberseguridad y la toma de decisiones basadas en evidencia. En el Perú, diversas entidades han resaltado la necesidad de mejorar los sistemas de protección de datos y la gestión digital para garantizar una administración pública moderna, responsable y resiliente.

En conclusión, este estudio es pertinente, necesario y de alto impacto, ya que permitirá comprender y mejorar la relación entre seguridad informática y toma de decisiones en el Gobierno Regional de Lima, contribuyendo al fortalecimiento institucional y al buen uso de la información en beneficio de la ciudadanía.

1.5. Delimitación del estudio

Delimitación espacial:

La investigación se desarrollará en el Gobierno Regional de Lima, específicamente en las áreas y unidades que utilizan sistemas de gestión para la administración institucional, tales como las oficinas de logística, presupuesto, recursos humanos, planificación, tecnologías de la información y otras dependencias que intervienen en procesos de toma de decisiones basados en información digital.

Delimitación temporal:

El estudio se circunscribe al periodo correspondiente al año 2025, considerando la situación actual de la seguridad informática y los procesos de toma de decisiones implementados durante este periodo.

Delimitación conceptual:

La investigación aborda dos variables principales:

Seguridad informática, entendida como el conjunto de políticas, herramientas, medidas y protocolos destinados a garantizar la integridad, disponibilidad y confidencialidad de la información dentro de los sistemas de gestión institucionales. Incluye aspectos como gestión de accesos, protección de datos, control de riesgos, monitoreo, ciberseguridad y respaldo de información.

Toma de decisiones, definida como el proceso mediante el cual los funcionarios y responsables seleccionan alternativas, asignan recursos, priorizan acciones y establecen lineamientos basados en información proveniente de los sistemas de gestión. Se relaciona con la calidad, confiabilidad, oportunidad y precisión de los datos utilizados.

Delimitación metodológica:

La investigación será de enfoque cuantitativo, diseño no experimental, tipo correlacional y de corte transversal, puesto que se evaluará la relación entre las variables sin manipularlas y en un solo periodo de tiempo. Se aplicará un cuestionario estructurado a la población seleccionada, siguiendo las dimensiones establecidas para cada variable.

1.6. Viabilidad del Estudio

Viabilidad técnica:

La investigación es técnicamente viable porque el investigador cuenta con los recursos necesarios para la recolección, procesamiento y análisis de la información. Se dispone de computadoras, acceso a internet, software de ofimática, plataformas digitales para aplicar encuestas y herramientas estadísticas que permitirán analizar los datos obtenidos. Asimismo, el Gobierno Regional de Lima cuenta con sistemas de gestión activos y operativos, lo que facilita la identificación de los procesos vinculados a la seguridad informática y la toma de decisiones. Esto garantiza que la información requerida pueda ser obtenida sin dificultades técnicas.

Viabilidad económica:

El estudio no requiere de una inversión económica elevada, por lo que es totalmente accesible para el investigador. Los costos se limitan principalmente a la impresión de documentos, transporte ocasional, acceso a materiales bibliográficos y uso de herramientas digitales gratuitas

o de bajo costo. Además, la aplicación de encuestas puede realizarse mediante formularios virtuales, reduciendo gastos en materiales físicos. En conjunto, los costos estimados son mínimos y no representan una limitación para el desarrollo del estudio.

Viabilidad temporal:

La investigación es viable temporalmente, ya que el cronograma establecido permite realizar cada una de las etapas -revisión teórica, diseño metodológico, recolección de datos, análisis e interpretación de resultados- dentro del periodo académico previsto. El acceso al personal del Gobierno Regional de Lima puede coordinarse dentro de los tiempos regulares de atención institucional, lo que asegura que la aplicación de los instrumentos pueda ejecutarse sin contratiempos. El estudio se desarrollará durante el año 2025, periodo adecuado para cumplir todas las actividades planificadas.

Viabilidad social y administrativa:

La investigación es socialmente viable porque la temática aborda aspectos relevantes para la mejora de la gestión pública, especialmente en lo relacionado con la seguridad de la información y la calidad de las decisiones institucionales. Los resultados contribuirán a fortalecer los servicios que el Gobierno Regional de Lima brinda a la ciudadanía, lo cual genera aceptación social y pertinencia del estudio. Administrativamente, las autoridades y áreas vinculadas muestran disposición para colaborar en investigaciones académicas, facilitando el acceso al personal y permitiendo la ejecución de encuestas sin interferir en las actividades normales de la institución. Esto garantiza un entorno favorable para el desarrollo del estudio.

II. CAPITULO II: MARCO TEORICO

2.1. Antecedentes de la investigación

Investigaciones internacionales

1. (Hernández, 2021)

Título: *Seguridad informática y gestión de la información en instituciones públicas*. donde concluyeron que la falta de mecanismos de protección de datos afecta directamente la confiabilidad de la información utilizada por los funcionarios, generando decisiones basadas en datos incompletos o vulnerados. Los autores demostraron que la seguridad informática es un factor determinante para garantizar la integridad y disponibilidad de la información en la gestión pública. (pág. 34)

2. (Rojas & Javier, 2020)

Título: *Incidencia de la ciberseguridad en la toma de decisiones estratégicas en entidades gubernamentales*. El estudio evidenció que los niveles bajos de seguridad informática incrementan los riesgos operativos y reducen la eficacia en la toma de decisiones. Asimismo, determinaron que los organismos gubernamentales requieren políticas de seguridad digital más estrictas para proteger sus sistemas de información y mejorar los procesos administrativos. (pág. 64)

3. (Martínez, 2022)

Título: *Gestión de riesgos informáticos y su efecto en los procesos decisionales en instituciones públicas*. Los resultados mostraron que las decisiones administrativas dependen directamente de la integridad y actualización de los datos almacenados en sistemas digitales. Los

autores concluyeron que un adecuado sistema de seguridad informática reduce la incertidumbre y mejora la calidad de las decisiones institucionales. (pág. 36)

Investigaciones nacionales

1. (Chavez, 2022)

Título: *Seguridad de la información y gestión administrativa en entidades del sector público*. Sus principales conclusiones indican que los bajos niveles de seguridad informática generan fallas en los sistemas de registro, retrasos en los procesos y decisiones institucionales basadas en datos no verificados. Asimismo, identificó que las entidades públicas presentan brechas en el control de accesos, monitoreo de actividades digitales y capacitación del personal. (pág. 42)

2. (Salazar, 2021)

Título: *Seguridad digital y calidad de la información para la toma de decisiones en instituciones estatales*. El estudio determinó que la calidad de la información empleada en la toma de decisiones depende directamente del nivel de protección y actualización de los sistemas informáticos. Además, concluyó que la falta de políticas de seguridad informática afecta la confiabilidad de los datos utilizados por los funcionarios. (pág. 28)

3. (Lopez, 2020)

Título: *Ciberseguridad y eficiencia en la toma de decisiones en entidades públicas peruanas*. Los resultados evidenciaron que la insuficiencia de medidas de seguridad digital produce inconsistencias en la información, generando decisiones tardías o erróneas. El autor destaca la necesidad de implementar sistemas de seguridad robustos y capacitación permanente del personal. (pág. 18)

2.2. Bases teóricas

1. Seguridad Informática (Variable Independiente)

1. Introducción

La Seguridad Informática es el conjunto de políticas, procedimientos, herramientas y prácticas orientadas a proteger la información y los sistemas que la procesan. Su propósito fundamental es garantizar que los datos, recursos tecnológicos y servicios digitales se mantengan seguros frente a amenazas internas y externas. Según diversas definiciones académicas, la seguridad informática se enfoca en preservar la confidencialidad, integridad y disponibilidad de la información, conceptos que constituyen la base de cualquier sistema seguro.

En la actualidad, la seguridad informática ha adquirido un rol estratégico en instituciones públicas, privadas y gubernamentales, debido al incremento de ataques cibernéticos, pérdida de datos, fraudes electrónicos y espionaje digital. La creciente dependencia tecnológica en procesos administrativos, financieros, operativos y educativos ha convertido la seguridad informática en un componente esencial para la continuidad de las organizaciones.

De manera amplia, la Seguridad Informática no solo considera la protección de sistemas computacionales, sino también la seguridad humana, física y organizacional. Esto implica políticas de acceso, concientización del personal, control de redes, protección de infraestructuras críticas y monitoreo continuo de los sistemas.

2. Principios Fundamentales (Triada CIA)

Los principios fundamentales que sustentan la Seguridad Informática se conocen como la Triada CIA, por sus siglas en inglés: Confidentiality, Integrity y Availability. Estos tres pilares son la base para cualquier arquitectura de seguridad.

2.1 Confidencialidad

La confidencialidad garantiza que la información solo sea accesible por personas autorizadas. Este principio se basa en evitar que datos sensibles, estratégicos o personales sean divulgados sin permiso. Para ello se implementan mecanismos como contraseñas robustas, autenticación de múltiples factores, cifrado de datos y políticas de acceso. La confidencialidad es crucial en instituciones gubernamentales, de salud, educación y finanzas, donde la exposición de información puede generar graves consecuencias legales y económicas.

2.2 Integridad

La integridad asegura que la información no sea modificada de manera indebida o sin autorización. Implica que los datos deben mantenerse completos, consistentes y verídicos. El principio se aplica mediante controles de validación, firmas digitales, registros de auditoría y herramientas de detección de cambios. La pérdida de integridad puede afectar procesos críticos como registros académicos, datos financieros o documentos oficiales.

2.3 Disponibilidad

La disponibilidad establece que los sistemas, servicios y datos deben estar accesibles cuando los usuarios autorizados los necesiten. Este principio es esencial para la continuidad operativa. Para garantizarlo se emplean redundancias, respaldos, sistemas de recuperación ante desastres, protección contra ataques DDoS y planes de contingencia. La indisponibilidad de un sistema puede paralizar actividades empresariales, gubernamentales o educativas.

3. Activos de Información

Los activos de información son todos los recursos que poseen valor para una organización. Incluyen datos, documentos digitales, equipos, programas, redes y el personal que interactúa con ellos. La protección de estos activos es uno de los objetivos centrales de la seguridad informática.

Tipos de activos:

Activos físicos: servidores, computadoras, dispositivos de almacenamiento, infraestructura de red.

Activos lógicos: software, bases de datos, aplicaciones, sistemas operativos.

Activos de información: documentos, archivos, datos personales o corporativos.

Activos humanos: usuarios, administradores, especialistas.

Activos organizacionales: políticas, procesos, normas internas.

Cada activo debe ser clasificado según su nivel de criticidad, valor, sensibilidad y dependencia operativa. Esta clasificación permite priorizar la implementación de medidas de seguridad en aquellos recursos que son más vulnerables o esenciales.

4. Amenazas y Vulnerabilidades

En seguridad informática, una amenaza es cualquier evento, acción o circunstancia que pueda causar daño o afectar negativamente un sistema de información. Por otro lado, una vulnerabilidad es una debilidad o falla en el sistema que puede ser explotada por una amenaza para causar un incidente de seguridad.

Tipos de amenazas:

Amenazas humanas externas: hackers, ciberdelincuentes, grupos organizados.

Amenazas internas: empleados descontentos, errores humanos, negligencias.

Amenazas técnicas: fallas de hardware, errores de software, malware.

Amenazas naturales: incendios, sismos, inundaciones.

Vulnerabilidades comunes:

Contraseñas débiles.

Sistemas sin actualizaciones.

Falta de políticas de seguridad.

Puertos y servicios expuestos.

Equipos sin antivirus o firewall.

Redes Wi-Fi sin cifrado.

La gestión de amenazas y vulnerabilidades implica identificarlas, analizarlas y mitigarlas mediante controles preventivos y correctivos. Esto reduce el nivel de riesgo al que se expone una organización.

5. Delitos Informáticos

Los delitos informáticos son conductas ilícitas realizadas mediante el uso de tecnologías de información, redes digitales o sistemas informáticos. Estos delitos afectan a empresas,

instituciones públicas y ciudadanos, generando pérdidas económicas, robo de datos y afectación a la privacidad.

Entre los principales delitos informáticos se encuentran:

Acceso no autorizado: ingresar sin permiso a sistemas o redes.

Robo de información: apropiación de datos personales, financieros o confidenciales.

Fraude electrónico: estafas en línea, suplantación de identidad, phishing.

Sabotaje informático: destrucción o alteración de datos y sistemas.

Distribución de malware: creación de virus, ransomware y otros softwares maliciosos.

Intercepción de comunicaciones: espionaje digital o captura no autorizada de datos.

En el Perú, estos delitos están regulados por la Ley N.° 30096 – Ley de Delitos Informáticos, que establece sanciones penales para conductas relacionadas con la manipulación indebida de sistemas y datos.

6. Conclusiones

La seguridad informática constituye un elemento esencial en toda institución, especialmente en el sector público, donde la información y los sistemas son pilares para el adecuado funcionamiento de los servicios. (Altamirano de la borda, 2020)Proteger la confidencialidad, integridad y disponibilidad de los datos, así como gestionar adecuadamente los riesgos, no solo resguarda los recursos informacionales, sino que también garantiza la continuidad operativa y refuerza la confianza de la ciudadanía. La implementación de soluciones tecnológicas, la definición de políticas de seguridad efectivas y la capacitación permanente del

personal conforman los fundamentos necesarios para enfrentar los desafíos presentes y futuros en materia de ciberseguridad (pág. 32).

Dimensiones:

Confidencialidad de la Información:

1. Introducción

La confidencialidad es el principio que garantiza que la información solo sea accesible a personas, sistemas o procesos debidamente autorizados. Su propósito es evitar que datos sensibles sean divulgados, manipulados o utilizados sin permiso. Este principio es fundamental en instituciones públicas y privadas, donde el manejo de información personal, financiera o estratégica requiere altos niveles de protección para prevenir vulneraciones que afecten la privacidad o seguridad de los usuarios.

Dentro de la confidencialidad se desarrollan los siguientes subdimensiones:

a) Protección de accesos

La protección de accesos implica el establecimiento de mecanismos que controlan quién puede ingresar a sistemas, aplicaciones o bases de datos. Incluye el uso de contraseñas seguras, autenticación multifactor, tarjetas inteligentes, biometría y políticas de acceso basadas en roles. Su finalidad es bloquear intentos de acceso no autorizados y asegurar que solo personas acreditadas puedan consultar o modificar información.

b) Control de usuarios

El control de usuarios consiste en gestionar adecuadamente las cuentas, permisos y privilegios asignados a cada persona dentro de la organización. Esto implica crear, modificar o

eliminar usuarios según su función, aplicar el principio de mínimo privilegio y monitorear continuamente actividades sospechosas. Un control deficiente de usuarios puede permitir accesos indebidos, suplantación de identidad o uso malicioso del sistema.

c) Resguardo de información sensible

El resguardo de información sensible se enfoca en proteger datos estratégicos, confidenciales o personales mediante técnicas como el cifrado, la anonimización, la clasificación de la información y el almacenamiento seguro. Asegurar el resguardo previene filtraciones, pérdidas o divulgaciones que puedan generar daños institucionales, legales o reputacionales.

Integridad de los Sistemas:

1. Introducción

La integridad de la información garantiza que los datos se mantengan completos, exactos y sin alteraciones no autorizadas. (Avalos Mendoza, 2023)Este principio asegura que la información registrada y procesada en un sistema represente fielmente los hechos o transacciones reales. La integridad es fundamental para la toma de decisiones, la confianza institucional y la validez de documentos o procesos administrativos (pág. 64).

Sus subdimensiones son:

a) Exactitud de los datos

La exactitud se refiere a que la información registrada debe ser correcta, precisa y verificable. Para garantizarla se utilizan validaciones automáticas, reglas de negocio, auditorías internas y mecanismos de verificación. La falta de exactitud puede llevar a errores en reportes, decisiones equivocadas y pérdidas institucionales.

b) No alteración de registros

Esta subdimensión implica prevenir modificaciones no autorizadas, intencionales o accidentales en la información. Se basa en controles como firmas digitales, hash criptográficos, trazabilidad de cambios y registros de auditoría. Garantiza que los datos permanezcan intactos desde su creación hasta su uso final.

c) Consistencia de la información en los sistemas

La consistencia asegura que los datos mantengan coherencia en todos los sistemas donde se almacenan o replican. Esto es crucial cuando existen bases de datos interconectadas o múltiples puntos de acceso. La sincronización, el control de versiones y la integridad referencial son herramientas empleadas para evitar duplicidades, contradicciones o pérdidas de información.

Disponibilidad de los Sistemas:

1. Introducción

La disponibilidad garantiza que los sistemas, servicios y datos se encuentren accesibles y operativos cuando los usuarios autorizados los necesiten. (Guarneros, 2022)Es un elemento clave para la continuidad de las operaciones institucionales, especialmente en entidades públicas donde la interrupción de servicios puede generar impactos ciudadanos, administrativos y económicos. (pág. 41)

Sus subdimensiones son:

a) Acceso oportuno a los sistemas

El acceso oportuno asegura que los usuarios puedan ingresar sin retrasos o barreras a las plataformas y recursos informáticos necesarios para realizar sus actividades. Esto depende de

sistemas bien configurados, infraestructura adecuada y políticas de accesibilidad. Su objetivo es reducir tiempos de espera, congestión o bloqueos operativos.

b) Funcionamiento continuo

El funcionamiento continuo se refiere a mantener los servicios activos sin interrupciones, mediante la implementación de redundancia, alta disponibilidad, monitoreo constante y mantenimiento preventivo. Un sistema con funcionamiento continuo minimiza fallas, evita caídas inesperadas y garantiza que los usuarios puedan trabajar sin contratiempos.

c) Recuperación ante fallas y respaldo de información

Esta subdimensión se centra en la capacidad de recuperar los servicios y datos tras incidentes como fallas de hardware, errores humanos, ataques informáticos o desastres naturales. Incluye políticas de respaldo (backups), planes de recuperación ante desastres (DRP), planes de continuidad del negocio (BCP) y restauración rápida de sistemas. Sin mecanismos de recuperación, una organización podría enfrentar pérdida irrecuperable de información o interrupciones prolongadas.

2. Toma de Decisiones (Variable Dependiente)

1. Introducción

La toma de decisiones es un proceso esencial en toda organización, especialmente en entidades gubernamentales y de gestión pública, donde cada decisión influye directamente en la eficiencia, transparencia y calidad del servicio brindado. La toma de decisiones consiste en seleccionar la mejor alternativa disponible para resolver un problema, optimizar un proceso o cumplir un objetivo institucional.

Este proceso se sustenta en la disponibilidad, confiabilidad y calidad de la información. En entornos digitales, la toma de decisiones depende en gran medida de los datos generados por los sistemas informáticos, lo que refuerza la necesidad de que la información sea precisa, oportuna, completa y verificable. Una decisión basada en datos incorrectos o incompletos puede afectar la planificación, la gestión de recursos y la atención al ciudadano.

En el contexto de la administración pública, la toma de decisiones se relaciona directamente con la eficiencia institucional, la transparencia, el uso adecuado de los recursos y la satisfacción de la población. Por ello, su estudio requiere analizar las dimensiones que determinan la calidad de los datos utilizados por los responsables y gestores.

2. Desde un enfoque administrativo, la toma de decisiones se define como un procedimiento sistemático que incluye la identificación del problema, el análisis de información, la evaluación de alternativas y la selección de la opción más pertinente, considerando criterios como eficiencia, efectividad, impacto y disponibilidad de recursos. Chiavenato (2017) señala que decidir implica un acto de responsabilidad, ya que cada elección genera consecuencias organizacionales, tanto positivas como negativas.

En el ámbito organizacional moderno, la toma de decisiones está estrechamente vinculada con la gestión de la información, ya que los directivos necesitan datos oportunos, verificables y confiables para sustentar sus acciones. De esta manera, la decisión deja de basarse en la intuición para apoyarse en evidencias, indicadores y análisis objetivos. Por ello, la calidad de la información constituye un factor determinante para garantizar decisiones acertadas.

Asimismo, el proceso decisorio puede ser estructurado o no estructurado. Las decisiones estructuradas se apoyan en procedimientos claros y repetitivos, mientras que las decisiones no

estructuradas requieren análisis más complejos, creatividad y juicio profesional, lo cual es especialmente frecuente en instituciones públicas y sistemas de gestión gubernamental.

Por otra parte, la toma de decisiones puede clasificarse en programadas y no programadas. Las decisiones programadas se basan en políticas, normas y procedimientos formales; en cambio, las no programadas surgen frente a situaciones inéditas o emergencias que exigen respuestas rápidas y bien fundamentadas.

En contextos como los gobiernos regionales, la toma de decisiones adquiere una dimensión estratégica porque influye en la asignación de recursos, la administración de sistemas informáticos, la seguridad de los datos institucionales y la prestación de servicios a la ciudadanía. De esta manera, una decisión adecuada contribuye a la eficiencia operativa, la transparencia y el logro de metas institucionales.

En síntesis, la toma de decisiones es un proceso racional y sistemático que integra información confiable, análisis crítico y valoración de alternativas para seleccionar la opción más favorable en función de los objetivos institucionales. Su calidad depende tanto de la información disponible como de las capacidades del personal involucrado.

3. Dimensiones de la Toma de Decisiones

3.1 Calidad de la Información

La calidad de la información es el principal componente que influye en la toma de decisiones. Se refiere al grado en que los datos son útiles, pertinentes, exactos y confiables para cumplir una función específica dentro del proceso institucional. La calidad de la información permite reducir incertidumbre, respaldar análisis objetivos y mejorar la eficiencia administrativa.

Sus subdimensiones son:

a) Precisión de los datos

La precisión se refiere al nivel de exactitud con el que los datos representan la realidad. Información precisa reduce errores, evita desviaciones en los informes y permite que las decisiones se basen en hechos comprobables. En los sistemas institucionales, la precisión se garantiza mediante validaciones, controles automatizados y auditorías de datos.

b) Completitud

La completitud implica que los datos deben estar íntegros, es decir, contener toda la información necesaria para un análisis adecuado. Datos incompletos pueden conducir a interpretaciones erróneas, decisiones parciales o conclusiones inválidas. La completitud se fortalece mediante formatos estandarizados, registros obligatorios y sistemas que evitan campos vacíos.

c) Verificabilidad y actualización

La verificabilidad se refiere a la posibilidad de comprobar el origen, validez y consistencia de los datos. La actualización implica que la información debe encontrarse vigente y alineada con los procesos actuales. Si los datos no pueden verificarse o están desactualizados, las decisiones carecen de fundamento sólido. Las organizaciones garantizan este subdimensión mediante sistemas de trazabilidad, auditorías, indicadores y actualizaciones programadas.

3.2 Oportunidad de la Información

La oportunidad se relaciona con la disponibilidad de los datos en el momento preciso en que se necesitan, permitiendo que las decisiones puedan tomarse sin retrasos ni interrupciones.

La información tardía puede ser tan perjudicial como la información incorrecta, pues afecta procesos críticos, genera demoras y compromete la calidad del servicio público.

Sus subdimensiones son:

a) Acceso en el momento adecuado

Significa que los responsables de la toma de decisiones deben contar con la información justo cuando la requieren. Esto depende de sistemas accesibles, infraestructura tecnológica adecuada y plataformas confiables. El acceso oportuno evita la paralización de trámites o la postergación de decisiones institucionales.

b) Rapidez en la obtención de datos

La rapidez implica que los sistemas deben procesar, mostrar o generar reportes de datos sin demoras. Cuando la información se obtiene con agilidad, las decisiones pueden ejecutarse en tiempo real, favoreciendo la eficiencia administrativa. La lentitud en la recuperación de datos puede ocasionar retrasos en procesos clave.

c) Disponibilidad en procesos críticos

Se refiere a que la información debe estar accesible especialmente en situaciones o procesos clave, como emergencias, auditorías, planificación institucional o procedimientos administrativos sensibles. La falta de disponibilidad en estos momentos puede generar riesgos, errores o retrasos graves. Algunas instituciones emplean respaldos, redundancia y monitoreo para garantizar la disponibilidad continua.

3.3 Confiabilidad de los Datos

La confiabilidad es la certeza de que los datos son válidos, auténticos y provienen de fuentes seguras. Se basa en la consistencia interna de la información y en la garantía de que no ha sido alterada de manera indebida. La confiabilidad es indispensable para que las decisiones institucionales tengan legitimidad y exactitud.

Sus subdimensiones son:

a) Autenticidad

La autenticidad implica que los datos provienen de una fuente legítima y no han sido manipulados. Se garantiza mediante firmas digitales, certificados electrónicos, registros de auditoría y mecanismos criptográficos. La autenticidad permite asegurar la validez documental y la correcta identificación de los autores o responsables de los registros.

b) Procedencia segura

Se refiere a que toda información debe originarse en sistemas confiables, controlados, con protocolos de seguridad establecidos. La procedencia segura evita el ingreso de datos falsificados, manipulados o no verificados. Las instituciones deben controlar el acceso a los sistemas y registrar quién genera, edita o elimina información.

c) Coherencia con los procesos institucionales

La coherencia garantiza que la información esté alineada con las normas, procedimientos y flujos de trabajo de la organización. Datos incoherentes generan errores administrativos, retrasos o decisiones equivocadas. La coherencia se asegura mediante estándares, manuales de procesos y análisis de integridad interna en los registros.

2.3. Bases filosóficas

1. Paradigma de Investigación

La presente investigación se enmarca dentro del paradigma positivista, el cual sostiene que la realidad puede ser conocida, medida y explicada mediante métodos objetivos y sistemáticos. Este paradigma parte del supuesto de que los fenómenos observados -en este caso, la seguridad informática y la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima- existen independientemente de la percepción del investigador y pueden ser analizados mediante instrumentos cuantificables.

El paradigma positivista permite estudiar la relación entre ambas variables a partir de datos empíricos recogidos de los funcionarios y personal administrativo, lo que facilita identificar patrones y determinar el grado de asociación mediante técnicas estadísticas. Este enfoque privilegia la objetividad, validez, confiabilidad y replicabilidad de los resultados, fundamentos esenciales para investigaciones correlacionales.

2. Enfoque Filosófico Epistemológico

En el plano epistemológico, la investigación se fundamenta en el positivismo, corriente que sostiene que el conocimiento válido se obtiene a través de la observación, la medición y el análisis cuantitativo. Bajo este enfoque, la relación entre seguridad informática y toma de decisiones se estudia mediante instrumentos estructurados y análisis estadísticos que permiten identificar patrones, comportamientos y correlaciones objetivas.

Este enfoque considera que:

El conocimiento se construye a partir de datos empíricos recopilados del personal del Gobierno Regional.

La validez del estudio depende de la objetividad, evitando sesgos subjetivos.

Las conclusiones se obtienen mediante procesos sistemáticos de medición y análisis.

El positivismo respalda el uso del método científico para explicar la relación entre ambas variables.

3. Fundamento Ontológico

Desde el punto de vista ontológico, la investigación se sustenta en la concepción de que la realidad administrativa y tecnológica del Gobierno Regional de Lima es objetiva, observable y medible. La seguridad informática y la toma de decisiones se consideran fenómenos reales que existen independientemente de la percepción del investigador, y que pueden ser analizados mediante indicadores concretos: niveles de confidencialidad, integridad, disponibilidad de los sistemas, así como calidad, oportunidad y confiabilidad de la información.

4. Base Axiológica

Desde la perspectiva axiológica, esta investigación reconoce la importancia de los valores éticos en el uso, tratamiento y protección de la información dentro de las instituciones públicas. La seguridad informática está estrechamente vinculada con valores como la **confidencialidad, integridad, responsabilidad, transparencia y honestidad**.

5. Fundamentación Lógica y Racional

La fundamentación lógica y racional de la presente investigación se sustenta en la relación directa que existe entre la seguridad informática y la toma de decisiones dentro de los sistemas de gestión institucional. La lógica del estudio parte del principio de que la información

constituye un recurso esencial para la administración pública, y su calidad depende de los mecanismos que protegen su integridad, disponibilidad y confidencialidad.

Racionalmente, se establece que si la seguridad informática presenta brechas o debilidades, la información generada por los sistemas de gestión puede ser alterada, incompleta, inaccesible o poco confiable. En consecuencia, las decisiones administrativas basadas en dicha información podrían resultar erróneas, tardías o ineficaces. Por el contrario, cuando existe un adecuado nivel de seguridad informática, los datos que sustentan la toma de decisiones se mantienen íntegros, actualizados y verificables, fortaleciendo así la eficacia de la gestión institucional.

La relación entre ambas variables responde a un razonamiento causal:

Una mayor seguridad informática → genera información más confiable → y mejora la calidad de la toma de decisiones.

Este vínculo, claramente observable en el entorno administrativo del Gobierno Regional de Lima, justifica la pertinencia del estudio bajo un diseño correlacional.

Desde la racionalidad metodológica, la investigación adopta un enfoque cuantitativo que permite medir objetivamente las percepciones del personal respecto a los niveles de seguridad informática y cómo estos influyen en los procesos decisionales. La recolección de datos mediante un cuestionario estructurado proporciona evidencia empírica que respalda la relación planteada entre las variables y permite formular conclusiones lógicas basadas en resultados estadísticos.

Finalmente, la fundamentación racional se sustenta en la necesidad institucional de mejorar la gestión pública mediante sistemas seguros que garanticen información confiable. Esta

lógica respalda la importancia del estudio, dado que fortalece la transparencia, eficiencia y modernización del Gobierno Regional de Lima.

6. Relevancia Filosófica

La presente investigación posee una importante relevancia filosófica, en tanto se sustenta en principios que explican la naturaleza del conocimiento, la realidad administrativa y el valor ético de la información en las instituciones públicas. Su relevancia se articula desde tres perspectivas fundamentales: ontológica, epistemológica y axiológica.

Desde el punto de vista ontológico, la investigación considera que la seguridad informática y la toma de decisiones son fenómenos reales que existen independientemente del observador y que pueden medirse y analizarse de manera objetiva. Esto significa que la información, los sistemas digitales y los procesos de decisión constituyen entidades concretas que influyen directamente en la gestión institucional. Ontológicamente, la investigación reafirma la necesidad de comprender la información como un recurso esencial cuya protección determina la calidad de la realidad administrativa.

En el plano epistemológico, la relevancia filosófica radica en la aplicación del paradigma positivista para explicar la relación entre las variables. Bajo esta perspectiva, el conocimiento válido se construye mediante la observación sistemática, la medición y el empleo de métodos cuantitativos que permiten obtener conclusiones verificables. La investigación aporta al campo epistemológico al demostrar, mediante evidencia empírica, cómo la seguridad informática sostiene la validez del conocimiento utilizado en la toma de decisiones institucionales.

Asimismo, desde una perspectiva axiológica, la investigación resalta la importancia de los valores éticos en el tratamiento, protección y uso de la información en el Gobierno Regional

de Lima. La seguridad informática representa un compromiso ético con la transparencia, la integridad, la responsabilidad y la protección del bien común. La toma de decisiones basada en información confiable y segura contribuye directamente al cumplimiento de estos valores, fortaleciendo la confianza de la ciudadanía y promoviendo una administración pública justa y eficiente.

2.4. Definición de términos básicos

Seguridad informática

Conjunto de políticas, prácticas, normas y herramientas orientadas a proteger los sistemas de información frente a accesos no autorizados, alteraciones, pérdida o destrucción de datos. Garantiza la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad

Principio de seguridad que asegura que la información solo sea accesible a personas autorizadas. Incluye mecanismos de control de acceso, autenticación y encriptación.

Integridad

Condición en la que la información permanece completa, exacta y sin modificaciones no autorizadas. Implica la veracidad y coherencia de los datos almacenados en un sistema.

Disponibilidad

Capacidad de acceso oportuno a los sistemas y datos cuando son necesitados por los usuarios autorizados. Depende del funcionamiento continuo, respaldos y recuperación ante fallas.

Sistema de gestión

Plataforma informática que administra procesos institucionales, como trámites administrativos, recursos humanos, logística, presupuesto o planificación. Facilita el almacenamiento, registro y consulta de información relevante para la toma de decisiones.

Datos institucionales

Información generada, registrada o procesada por el Gobierno Regional de Lima en sus diferentes áreas. Incluye documentos, reportes, registros administrativos y bases de datos.

Toma de decisiones

Proceso mediante el cual un funcionario o unidad administrativa selecciona una alternativa o curso de acción basado en información disponible y análisis previo. Es esencial en la gestión pública para resolver problemas, asignar recursos o planificar actividades.

Calidad de la información

Grado en que los datos utilizados en los sistemas de gestión son precisos, completos, actualizados y verificables. Información de baja calidad afecta la eficacia de las decisiones institucionales.

Oportunidad de la información

Disponibilidad de los datos en el momento adecuado para su uso en procesos decisionales. Una información tardía puede afectar la eficacia de la gestión pública.

Confiabilidad de los datos

Nivel de autenticidad y veracidad de la información que se emplea para tomar decisiones. Depende de la protección de los sistemas y del adecuado registro y almacenamiento.

Ciberseguridad

Disciplina que comprende la protección frente a amenazas digitales, ataques externos o internos que buscan vulnerar la infraestructura tecnológica y los datos institucionales.

Incidente de seguridad

Cualquier evento que compromete la integridad, confidencialidad o disponibilidad de la información o de los sistemas informáticos. Incluye accesos indebidos, pérdida de datos o fallas del sistema.

Riesgo informático

Probabilidad de ocurrencia de un evento que afecte negativamente los sistemas de información. Se relaciona con vulnerabilidades, amenazas y la capacidad de respuesta institucional.

Usuario autorizado

Persona que tiene permisos para acceder, registrar o modificar información dentro de los sistemas de gestión institucional, según su rol o función.

Gestión pública

Conjunto de procesos y decisiones que realizan las entidades del Estado para administrar recursos, brindar servicios y ejecutar políticas orientadas al bienestar ciudadano.

2.5. Hipótesis de investigación

Hipótesis general

Existe una relación significativa entre la seguridad informática y la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

Hipótesis especificas

La confidencialidad de la información se relaciona significativamente con la calidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

La integridad de la información se relaciona significativamente con la oportunidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

La disponibilidad de la información se relaciona significativamente con la confiabilidad de los datos utilizados para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

2.6. Operacionalización de Variable e Indicadores

Tabla 1. Seguridad informática

Dimensiones	Indicadores	Ítems	Ninel/Rango
Confidencialidad de la información	• Control de accesos. • Protección de datos sensibles. • Cumplimiento de políticas de seguridad.	1,2,3	Escala de likert
Integridad	• Exactitud de los datos. • Veracidad de la información. • Consistencia en los sistemas de gestión.	4,5,6	
Disponibilidad	• Acceso oportuno a los sistemas. • Funcionalidad del sistema. • Respaldo y recuperación de datos.	7,8,9	

Tabla 2. Toma de Decisiones

Dimensiones	Indicadores	Ítems	Ninel/Rango
Calidad de la información	• Precisión de los datos. • Completitud de los registros. • Actualización de datos.	10,11,12	Escala de likert
Oportunidad de la información	• Acceso en el momento adecuado. • Rapidez en el procesamiento. • Pertinencia temporal.	13,14,15	
Confiabilidad de los datos	• Autenticidad de la información. • Coherencia en los registros. • Seguridad de la información utilizada.	16,17,18	

III. CAPITULO III: METODOLOGIA DE LA INVESTIGACION

3.1. Diseño metodológico

1. Enfoque de investigación

La investigación presenta un enfoque cuantitativo, debido a que se basa en la recolección y análisis de datos numéricos obtenidos mediante un cuestionario estructurado. Este enfoque permite medir las percepciones del personal respecto a las variables de estudio y establecer relaciones estadísticas objetivas entre ellas.

2. Tipo de investigación

El estudio es de tipo básico o sustantivo, ya que busca generar conocimientos orientados a comprender la relación entre la seguridad informática y la toma de decisiones, sin intervenir directamente en los procesos institucionales. Además, contribuye al desarrollo de fundamentos teóricos aplicables al ámbito de la gestión pública y la administración de sistemas de información.

3. Nivel de investigación

El estudio presenta un nivel correlacional, debido a que tiene como finalidad determinar la relación existente entre la Seguridad informática y toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima. Este nivel de investigación permite analizar la asociación entre las variables sin establecer relaciones de causalidad, aportando evidencia empírica sobre la interacción entre los factores estudiados.

4. Diseño de investigación

El diseño es no experimental, ya que no se manipulan intencionalmente las variables, sino que se observan tal como se presentan en su contexto natural dentro del Gobierno Regional de Lima. Asimismo, pertenece al diseño transeccional o transversal correlacional, debido a que la información se recolectará en un solo momento del tiempo con el fin de medir simultáneamente las variables y establecer su relación.

3.2. Población y muestra

Población

La población de la investigación está conformada por 380 trabajadores del Gobierno Regional de Lima, 2025.

Muestra

Para la muestra utilizaremos la siguiente formula.

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

Donde:

$$n = \frac{3.8416 * 0.25 * 380}{0.0025 * 379 + 3.8416 * 0.25}$$

Por lo cual nuestra muestra sería de 192 trabajadores del Gobierno Regional de Lima, 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 Seguridad Informática y toma de decisiones en los sistemas de Gestión del Gobierno Regional de Lima.

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 con las siguientes opciones:

- Siempre
- Casi siempre
- A veces
- Casi nunca
- Nunca

Esta metodología permitirá evaluar la percepción de los participantes respecto a los factores clave del estudio, asegurando la recopilación de datos cuantificables y comparables, que servirán para analizar el nivel de Seguridad Informática y toma de decisiones en los sistemas de Gestión del Gobierno Regional de Lima.

3.4. Técnicas para el procesamiento de la información

Los datos obtenidos a partir de las encuestas serán procesados y analizados utilizando el software SPSS (Statistical Package for the Social Sciences). Para ello, se aplicarán las siguientes técnicas:

Codificación y Tabulación de Datos: Se ingresarán los datos recolectados en una base de datos estructurada en SPSS, asignando valores numéricos a las respuestas del cuestionario, según la escala tipo Likert utilizada.

Análisis Descriptivo: Se generarán gráficos de barras y tablas de frecuencias con sus respectivos porcentajes, permitiendo visualizar la distribución de las respuestas y obtener un panorama general sobre la percepción de los participantes respecto a la Seguridad Informática y toma de decisiones en los sistemas de Gestión del Gobierno Regional de Lima.

Análisis de Correlación de Spearman: Para determinar la relación entre la Seguridad Informática y toma de decisiones en los sistemas de Gestión del Gobierno Regional de Lima, se aplicará el coeficiente de correlación de Spearman (ρ). Este método es adecuado cuando las variables son ordinales y no necesariamente cumplen con la normalidad, proporcionando una medida del grado de asociación entre ambas variables.

Este análisis permitirá verificar si existe una relación significativa entre la Seguridad Informática y toma de decisiones en los sistemas de Gestión del Gobierno Regional de Lima, lo que permitirá extraer conclusiones relevantes para la investigación.

IV. CAPITULO IV: RESULTADOS

4.1. Análisis de Resultados

Resultados de Seguridad Informática y sus dimensiones

Tabla 1 Seguridad Informática

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	3	1,6	1,6	1,6
	Medio	65	33,9	33,9	35,4
	Alto	124	64,6	64,6	100,0
	Total	192	100,0	100,0	

Fuente: Registros de Seguridad Informática que se obtuvo de los trabajadores del Gobierno Regional de Lima, 2025.

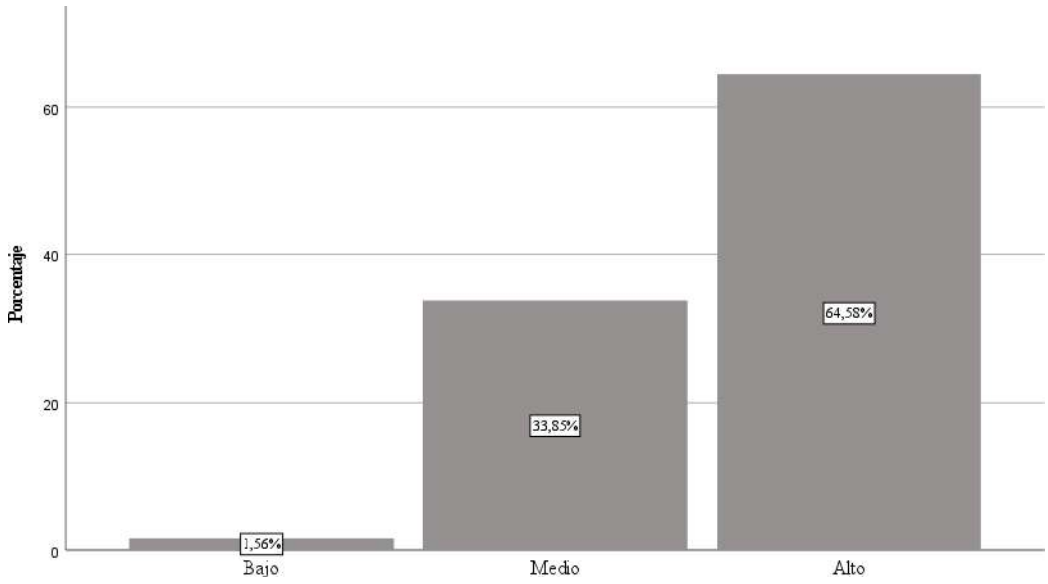

Gráfico 1 Seguridad Informática

En la fig. 1, el 64.58% de los trabajadores encuestados del Gobierno Regional de Lima perciben un nivel alto de seguridad informática, mientras que el 33.85% perciben un nivel medio y, por último, solo un 1.56% perciben que la seguridad informática se encuentra en un nivel bajo.

Tabla 2 Categoría Confidencialidad de la Información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	5	2,6	2,6	2,6
	Medio	65	33,9	33,9	36,5
	Alto	122	63,5	63,5	100,0
	Total	192	100,0	100,0	

Fuente: Registros de Confidencialidad de la Información que se obtuvo de los trabajadores del Gobierno Regional de Lima, 2025.

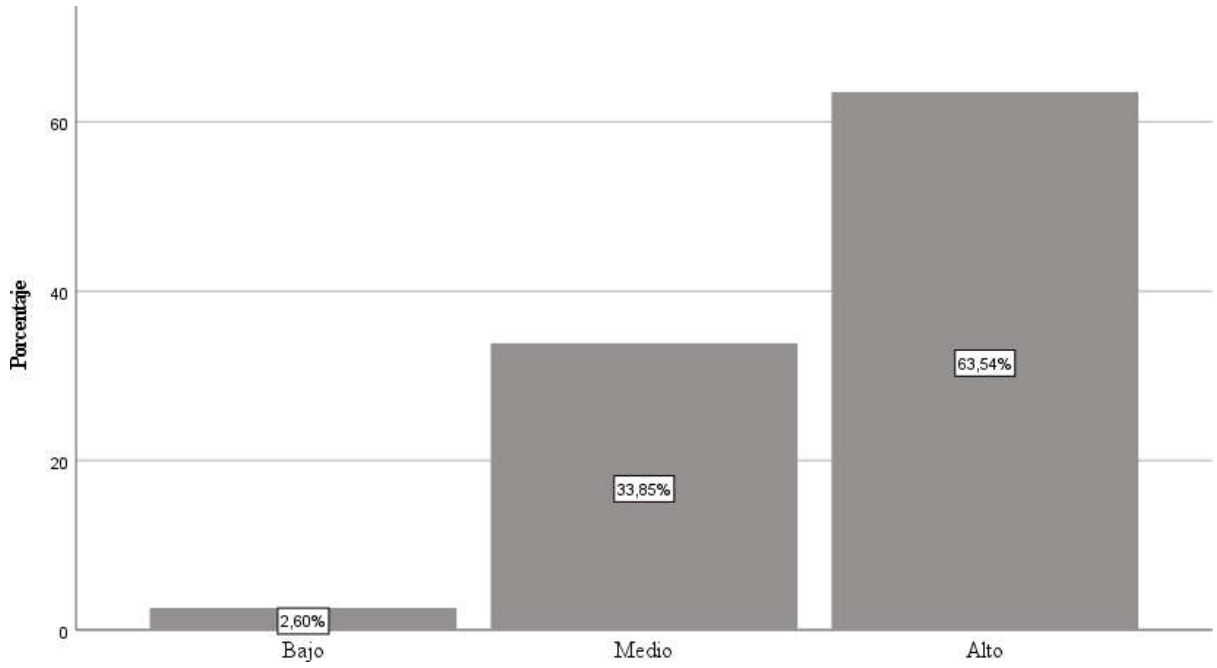

Gráfico 2 Categoría Confidencialidad de la Información

En la fig. 2, el 63.54% de los trabajadores encuestados del Gobierno Regional de Lima perciben un nivel alto de confidencialidad de la información, mientras que el 33.85% perciben un nivel medio y, por último, solo un 2.60% perciben que la confidencialidad de la información se encuentra en un nivel bajo.

Tabla 3 Categoría Integridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	6	3,1	3,1	3,1
	Medio	84	43,8	43,8	46,9
	Alto	102	53,1	53,1	100,0
	Total	192	100,0	100,0	

Fuente: Registros de Integridad que se obtuvo de los trabajadores del Gobierno Regional de Lima, 2025.

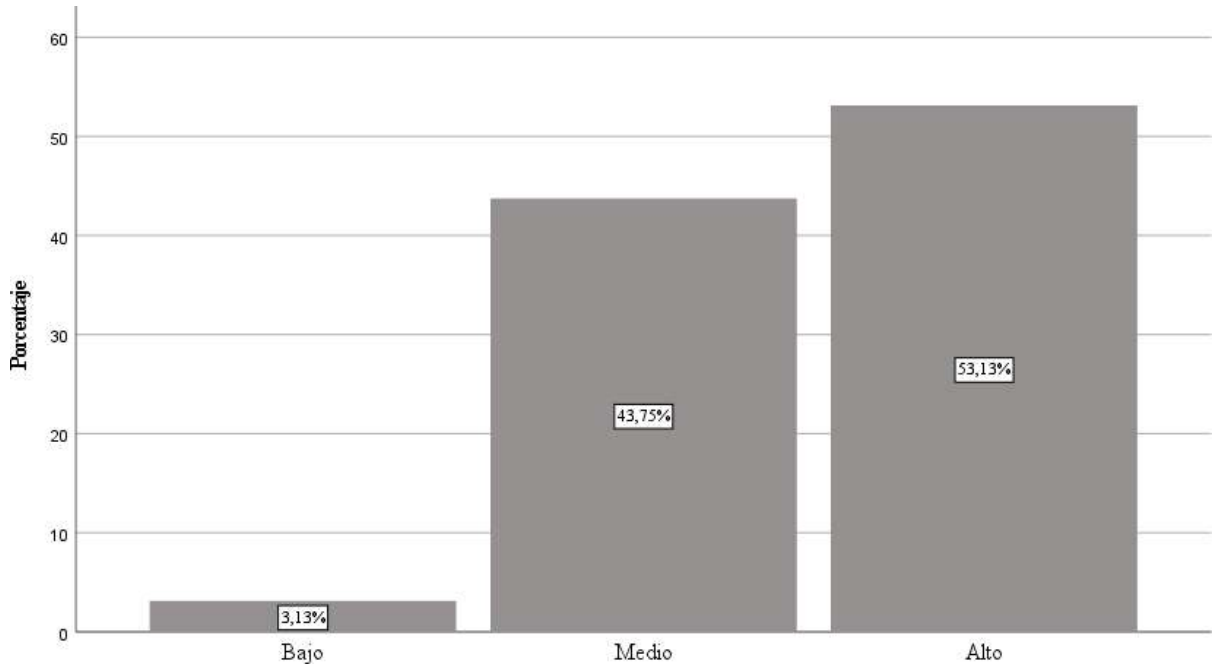

Gráfico 3 Categoría Integridad

En la fig. 3, el 53.13% de los trabajadores encuestados del Gobierno Regional de Lima perciben un nivel alto de integridad, mientras que el 43.75% perciben un nivel medio y, por último, solo un 3.13% perciben que la integridad se encuentra en un nivel bajo.

Tabla 4 Categoría Disponibilidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	3	1,6	1,6	1,6
	Medio	78	40,6	40,6	42,2
	Alto	111	57,8	57,8	100,0
	Total	192	100,0	100,0	

Fuente: Registros de Disponibilidad que se obtuvo de los trabajadores del Gobierno Regional de Lima, 2025.

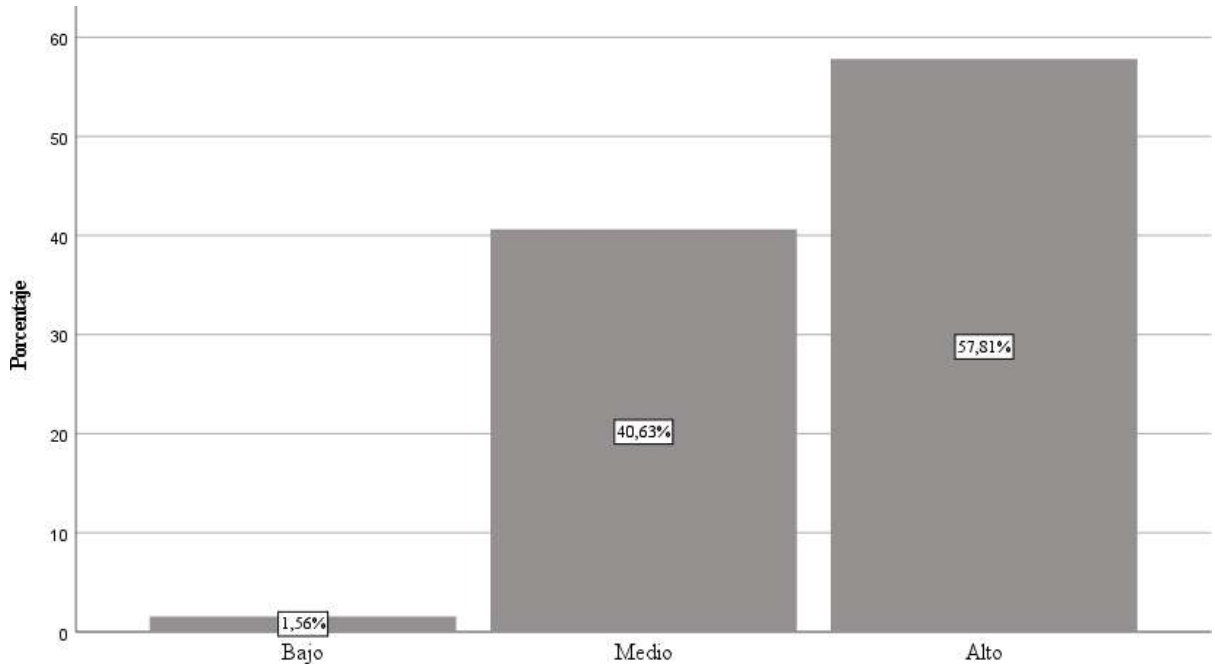

Gráfico 4 Categoría Disponibilidad

En la fig. 4, el 57.81% de los trabajadores encuestados del Gobierno Regional de Lima perciben un nivel alto de disponibilidad, mientras que el 40.63% perciben un nivel medio y, por último, solo un 1.56% perciben que la disponibilidad se encuentra en un nivel bajo.

Resultados de Toma de Decisiones y sus dimensiones

Tabla 5 Toma de Decisiones

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	6	3,1	3,1	3,1
	Medio	101	52,6	52,6	55,7
	Alto	85	44,3	44,3	100,0
	Total	192	100,0	100,0	

Fuente: Registros de Toma de Decisiones que se obtuvo de los trabajadores del Gobierno Regional de Lima, 2025.

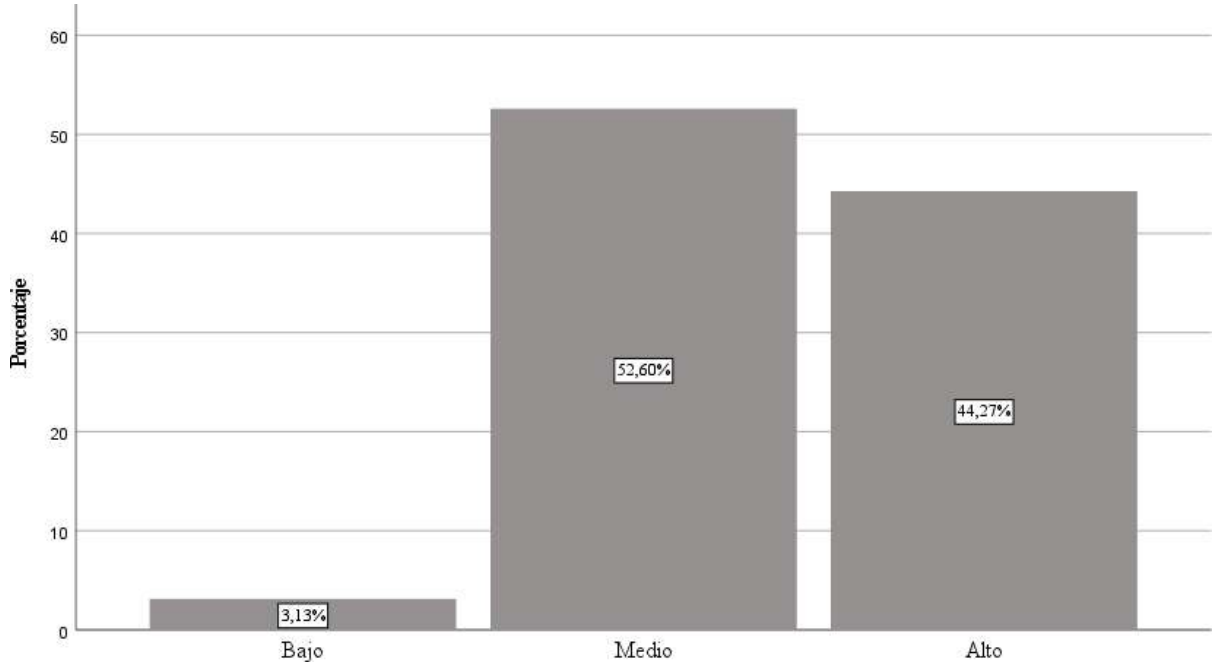

Gráfico 5 Toma de Decisiones

En la fig. 5, el 44.27% de los trabajadores encuestados del Gobierno Regional de Lima perciben un nivel alto de toma de decisiones, mientras que el 52.60% perciben un nivel medio y, por último, solo un 3.13% perciben que la toma de decisiones se encuentra en un nivel bajo.

Tabla 6 Categoría Calidad de la Información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	11	5,7	5,7	5,7
	Medio	118	61,5	61,5	67,2
	Alto	63	32,8	32,8	100,0
	Total	192	100,0	100,0	

Fuente: Registros de Calidad de la Información que se obtuvo de los trabajadores del Gobierno Regional de Lima, 2025.

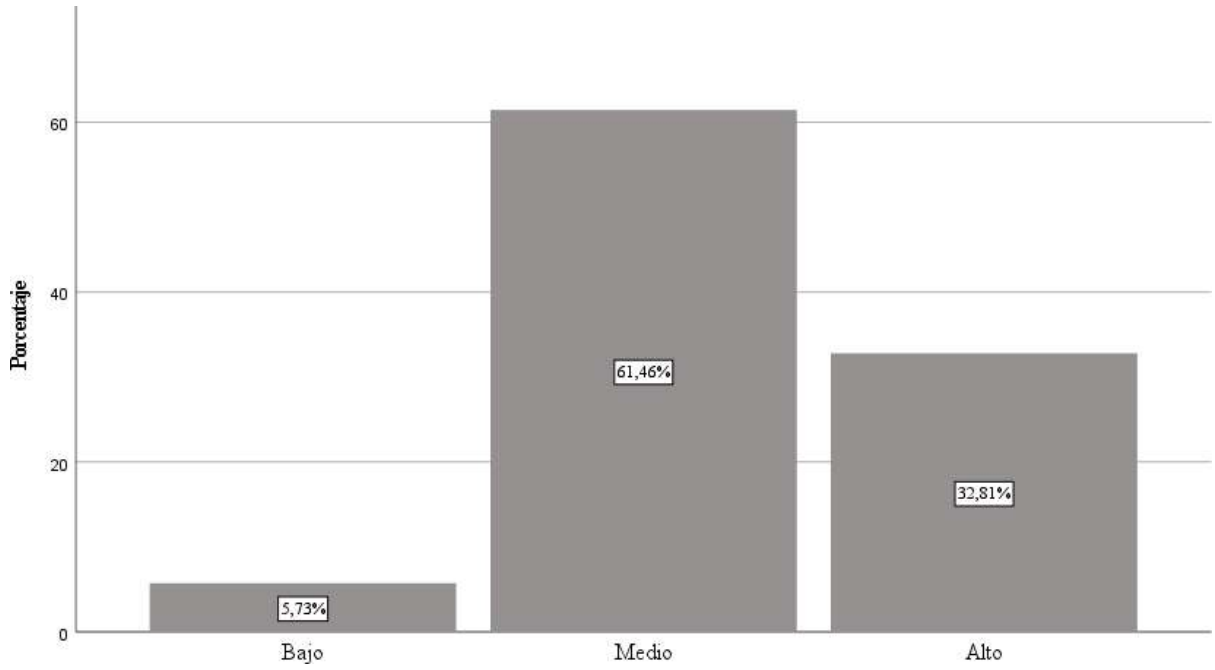

Gráfico 6 Categoría Calidad de la Información

En la fig. 6, el 61.46% de los trabajadores encuestados del Gobierno Regional de Lima perciben un nivel medio de calidad de la información, mientras que el 32.81% perciben un nivel alto y, por último, solo un 5.73% perciben que la calidad de la información se encuentra en un nivel bajo.

Tabla 7 Categoría Oportunidad de la Información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	18	9,4	9,4	9,4
	Medio	109	56,8	56,8	66,1
	Alto	65	33,9	33,9	100,0
	Total	192	100,0	100,0	

Fuente: Registros de Oportunidad de la Información que se obtuvo de los trabajadores del Gobierno Regional de Lima, 2025.

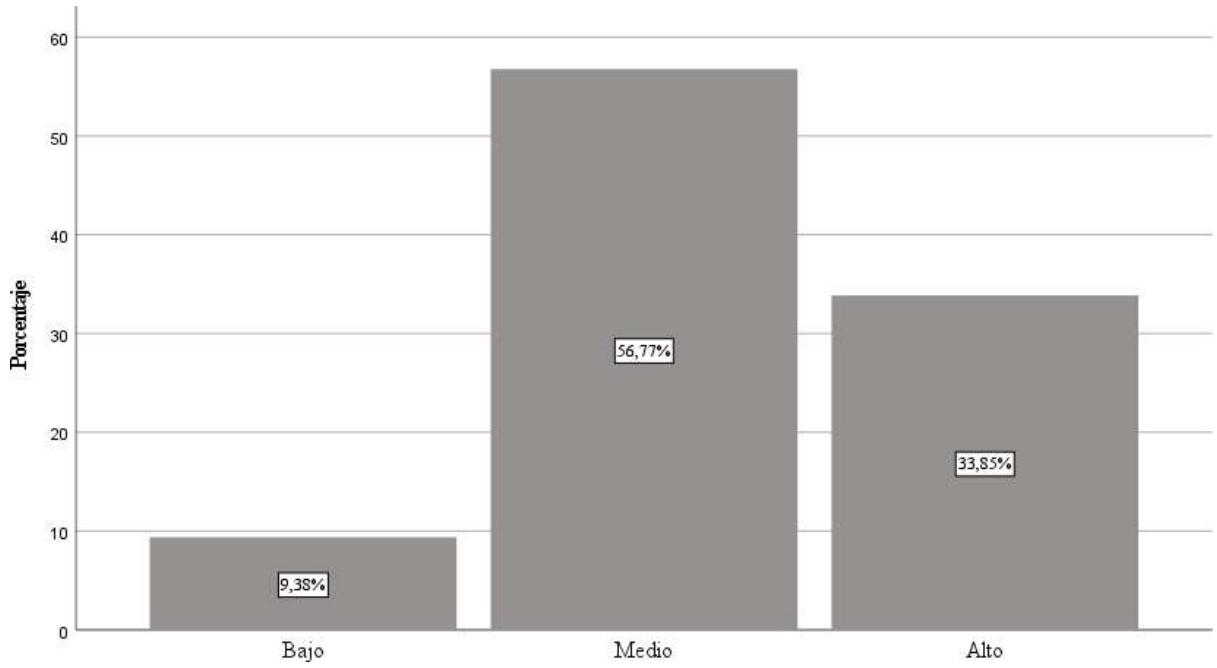

Gráfico 7 Categoría Oportunidad de la Información

En la fig. 7, el 56.77% de los trabajadores encuestados del Gobierno Regional de Lima perciben un nivel medio de oportunidad de la información, mientras que el 33.85% perciben un nivel alto y, por último, solo un 9.38% perciben que la oportunidad de la información se encuentra en un nivel bajo.

Tabla 8 Categoría Confiabilidad de los Datos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	8	4,2	4,2	4,2
	Medio	96	50,0	50,0	54,2
	Alto	88	45,8	45,8	100,0
	Total	192	100,0	100,0	

Fuente: Registros de Confiabilidad de los Datos que se obtuvo de los trabajadores del Gobierno Regional de Lima, 2025.

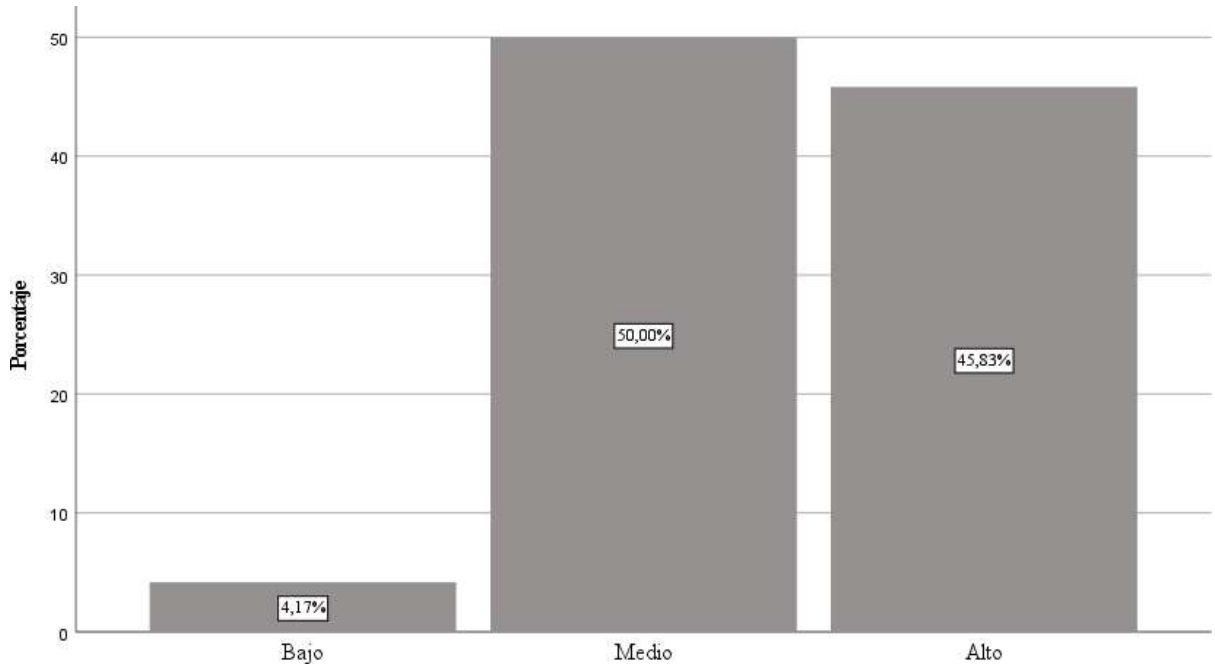

Gráfico 8 Categoría Calidad de la Información

En la fig. 8, el 50.00% de los trabajadores encuestados del Gobierno Regional de Lima perciben un nivel medio de confiabilidad de los datos, mientras que el 45.83% perciben un nivel alto y, por último, solo un 4.17% perciben que la confiabilidad de los datos se encuentra en un nivel bajo.

4.2. Contrastación de Hipótesis

Contrastación de Hipótesis General

a) Hipótesis General Nula (Ho)

La seguridad informática no se relaciona significativamente con la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

b) Hipótesis General Alternativa

La seguridad informática se relaciona significativamente con la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

c) Regla para Contrastar Hipótesis

Correlaciones: Seguridad Informática y Toma de Decisiones

		Seguridad Informática	Toma de Decisiones
Seguridad Informática	Correlación de Spearman	1,000	,895
	Sig. (bilateral)	.	,000
	N	192	192
Toma de Decisiones	Correlación de Spearman	,895	1,000
	Sig. (bilateral)	,000	.
	N	192	192

Interpretación

Se evidencia una correlación positiva fuerte (r = 0.895), lo que implica que, a mayor nivel de seguridad informática, más eficiente resulta la toma de decisiones, así mismo, el valor p < 0.001 confirma que el vínculo es estadísticamente altamente significativo.

Contrastación de Hipótesis Especifica 1

a) Hipótesis General Nula (Ho)

La confidencialidad de la información no se relaciona significativamente con la calidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

b) Hipótesis General Alternativa

La confidencialidad de la información se relaciona significativamente con la calidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

c) Regla para Contrastar Hipótesis

Correlaciones: Confidencialidad de la Información y Calidad de la Información

		Confidencialidad de la Información	Calidad de la Información
Confidencialidad de la Información	Correlación de Spearman	1,000	,706
	Sig. (bilateral)	.	,000
	N	192	192
Calidad de la Información	Correlación de Spearman	,706	1,000
	Sig. (bilateral)	,000	.
	N	192	192

Interpretación

Se evidencia una correlación positiva fuerte ($r = 0.706$), lo que implica que, a mayor nivel de confidencialidad de la información, mejor es la calidad de la información, así mismo, el valor $p < 0.001$ confirma que el vínculo es estadísticamente altamente significativo.

Contrastación de Hipótesis Especifica 2

a) Hipótesis General Nula (Ho)

La integridad de la información no se relaciona significativamente con la oportunidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

b) Hipótesis General Alternativa

La integridad de la información se relaciona significativamente con la oportunidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

c) Regla para Contrastar Hipótesis

Correlaciones: Integridad y Oportunidad de la Información

		Integridad	Oportunidad de la Información
Integridad	Correlación de Spearman	1,000	,773
	Sig. (bilateral)	.	,000
	N	192	192
Oportunidad de la Información	Correlación de Spearman	,773	1,000
	Sig. (bilateral)	,000	.
	N	192	192

Interpretación

Se evidencia una correlación positiva fuerte ($r = 0.773$), lo que implica que, a mayor integridad de la información, más oportuna resulta la información, así mismo, el valor $p < 0.001$ confirma que el vínculo es estadísticamente altamente significativo.

Contrastación de Hipótesis Especifica 3

a) Hipótesis General Nula (Ho)

La disponibilidad de la información no se relaciona significativamente con la confiabilidad de los datos utilizados para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

b) Hipótesis General Alternativa

La disponibilidad de la información se relaciona significativamente con la confiabilidad de los datos utilizados para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

c) Regla para Contrastar Hipótesis

Correlaciones: Disponibilidad y Confiabilidad de los Datos

		Disponibilidad	Confiabilidad de los Datos
Disponibilidad	Correlación de Spearman	1,000	,766
	Sig. (bilateral)	.	,000
	N	192	192
Confiabilidad de los Datos	Correlación de Spearman	,766	1,000
	Sig. (bilateral)	,000	.
	N	192	192

Interpretación

Se evidencia una correlación positiva fuerte ($r = 0.766$), lo que implica que, a mayor disponibilidad, más confiables resultan los datos, así mismo, el valor $p < 0.001$ confirma que el vínculo es estadísticamente altamente significativo.

V. CAPITULO V: DISCUSION

5.1. Discusión de Resultados

Se confirma una asociación positiva de carácter muy fuerte y altamente significativa entre las dos variables principales. La correlación obtenida (rho = 0.895) junto con un valor de significancia estadística ($p < 0.001$) evidencian que, cuando el Gobierno Regional de Lima implementa controles robustos de seguridad informática, se optimiza sustancialmente la eficiencia en la toma de decisiones. Este hallazgo sugiere que un entorno digital seguro reduce la incertidumbre y brinda a los directivos la confianza necesaria para actuar. Esto es coherente con los planteamientos de (Velásquez & Yujra, 2021) quienes afirman que la seguridad de la información no es solo un aspecto técnico, sino un activo estratégico que garantiza la gobernabilidad y el flujo correcto de los procesos administrativos. (pág. 45)

En lo correspondiente a las situaciones específicas, los datos muestran que cada una de las dimensiones evaluadas de la seguridad guarda un vínculo estrecho con los criterios de decisión. En el caso de la confidencialidad de la información, la correlación fuerte (rho = 0.706, $p < 0.001$) respecto a la calidad de la información sugiere que, al restringir el acceso únicamente a personal autorizado, se preserva la pureza y precisión de los datos. Esto evita manipulaciones indebidas que podrían degradar la calidad del insumo informativo, permitiendo a los gestores basar sus decisiones en reportes precisos y libres de sesgos.

En relación con la dimensión integridad, se obtuvo una correlación positiva fuerte (rho = 0.773, $p < 0.001$) con la oportunidad de la información. Al respecto, (Pérez Reséndiz & Martínez Bautista, 2021) sostienen que la exactitud y la limpieza de los datos no son meros atributos técnicos, sino requisitos previos fundamentales para evitar cuellos de botella en la

administración. Estos resultados indican que mantener los datos libres de errores y alteraciones no solo asegura su validez, sino que agiliza significativamente los tiempos de respuesta institucional, por lo que, cuando la información es íntegra, se eliminan los reprocesamientos y las verificaciones redundantes causadas por fallos técnicos, lo que permite que los informes lleguen a los decisores en el momento preciso, cumpliendo con la celeridad que demanda la gestión pública moderna.

Acerca de la disponibilidad, la investigación evidencia una calificación fuerte (rho = 0.766, $p < 0.001$) vinculada a la confiabilidad de los datos. Esto revela que la capacidad de acceder a los sistemas sin interrupciones es fundamental para generar confianza en los reportes extraídos. La continuidad operativa asegura que los datos analizados sean siempre los más actuales y no versiones obsoletas guardadas localmente ante caídas del sistema, garantizando así que la base para la toma de decisiones sea auténtica y verificable.

Los resultados del estudio reafirman el valor estratégico de la seguridad informática dentro del Gobierno Regional de Lima. Su implementación no debe verse solo como un cumplimiento normativo de protección, sino como un motor que impulsa la eficacia administrativa. Fortalecer estos sistemas permite cimentar una gestión basada en la evidencia, asegurando así una administración pública más transparente, ágil y orientada al servicio del ciudadano.

VI. CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

- La investigación ha logrado determinar, con un alto grado de certeza estadística (rho=0.895), que la seguridad informática constituye un pilar fundamental para la eficiencia en la toma de decisiones dentro del Gobierno Regional de Lima. Los hallazgos demuestran que la solidez de la infraestructura tecnológica y las políticas de protección no son meros requisitos técnicos, sino activos estratégicos; cuando el entorno digital es seguro, los funcionarios reducen la incertidumbre y agilizan los procesos administrativos, mejorando la gobernabilidad institucional.

- En lo referente a la confidencialidad, se ha comprobado que el control riguroso de accesos y la protección de datos sensibles elevan sustancialmente la calidad de la información (rho=0.706). Al garantizar que solo personal autorizado interactúe con los datos críticos, se minimiza el ruido informativo y la manipulación indebida, permitiendo que los directivos basen sus estrategias en reportes precisos, limpios y fieles a la realidad operativa de la región.

- La evidencia empírica confirma que la integridad de los datos actúa como un catalizador para la oportunidad de la información (rho=0.773). Mantener registros exactos y libres de errores sistémicos elimina la necesidad de reprocesos y verificaciones manuales redundantes, lo cual es decisivo para que la información llegue a los tomadores de decisiones en el tiempo exacto en que se requiere, superando así los habituales cuellos de botella burocráticos.

- Con respecto a la disponibilidad, se concluye que existe una vinculación directa y fuerte con la confiabilidad de los datos (rho=0.766). La capacidad de los sistemas para operar sin interrupciones ni caídas asegura que la información consultada esté siempre actualizada y disponible. Esto genera un clima de confianza en el usuario, quien tiene la certeza de que los datos en pantalla son auténticos y respaldan acciones administrativas válidas y auditables.

- Así mismo, el estudio revela que, aunque existe una percepción mayoritariamente positiva sobre la seguridad actual, aún persisten brechas en la percepción de los niveles medios de gestión. Esto subraya que la transformación digital en el Gobierno Regional no solo depende de adquirir tecnología, sino de consolidar una cultura de seguridad integral que garantice la sostenibilidad de las decisiones públicas a largo plazo.

6.2. Recomendaciones

- Se recomienda a la Oficina de Tecnologías de la Información institucionalizar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para elevar los estándares de protección de datos. Esto implica evolucionar de la aplicación de medidas de seguridad aisladas hacia una gobernanza de TI estructurada donde la clasificación de los activos de información sea la base para aplicar controles estrictos. De esta manera se garantizará que la data crítica para la gestión regional esté resguardada bajo estándares internacionales y brinde el soporte necesario para una administración eficiente.

- Es imperativo modernizar las políticas de control de accesos mediante la implementación de soluciones de Gestión de Identidades y Accesos que integren autenticación de

múltiples factores. Se debe aplicar rigurosamente la asignación de permisos según la función específica del usuario para asegurar que solo personal autorizado y validado interactúe con los sistemas sensibles. Al restringir los privilegios innecesarios se reduce drásticamente el riesgo de manipulación de datos y se asegura que los reportes gerenciales mantengan su calidad y precisión.

- Se sugiere la implementación masiva de mecanismos de validación de datos e integridad como el uso de firmas digitales y tecnología de encriptación en los flujos de trabajo administrativos. Estas herramientas garantizarán la inmutabilidad de los registros y la consistencia entre los diferentes sistemas de gestión utilizados en la entidad. Al tener la certeza técnica de que los datos no han sido alterados se eliminan los tiempos muertos por verificación manual y esto permite a los funcionarios tomar decisiones rápidas y oportunas en beneficio de la gestión pública.

- Para garantizar la disponibilidad de los servicios y la confiabilidad de los datos ante las amenazas técnicas o naturales se recomienda actualizar y probar periódicamente el Plan de Recuperación ante Desastres (DRP) junto con el Plan de Continuidad del Negocio. No basta con realizar copias de seguridad de la información, sino que la entidad debe ejecutar simulacros de restauración de servicios críticos para asegurar que el tiempo de recuperación sea mínimo. Esto asegura que la operatividad del Gobierno Regional se mantenga ante cualquier incidente y preserva la confianza en la capacidad de respuesta institucional.

- Se recomienda establecer un programa permanente de auditoría de vulnerabilidades técnicas y capacitación al personal sobre la higiene cibernética para mitigar los riesgos asociados al factor humano. Dado que las amenazas como la ingeniería social son

constantes es vital educar a los funcionarios sobre la identificación de riesgos para actuar como la primera línea de defensa. Un personal capacitado no solo protege los activos tecnológicos, sino que asegura que la información utilizada para la toma de decisiones estratégicas provenga de un entorno digital seguro y libre de compromisos.

VII. REFERENCIAS

7.1. Fuentes bibliográficas

Altamirano de la borda, k. (2020). *La seguridad de la informacion en la administración pública.* USA: Revista de Derecho Administrativo.

Avalos Mendoza, M. R. (2023). *Diseño de un modelo de gestión en seguridad digital.* Lima.

Chavez. (2022). *Seguridad de la información y gestión administrativa en entidades del sector público.* Perú.

Guarneros, J. (2022). *Implementación de procesos de seguridad informática bajo el* . USA.

Hernández, G. y. (2021). *Seguridad informática y gestión de la información en instituciones públicas.* mexico.

Lopez. (2020). *Ciberseguridad y eficiencia en la toma de decisiones en entidades públicas peruanas.* Perú.

Martínez, P. y. (2022). *Gestión de riesgos informáticos y su efecto en los procesos decisionales en instituciones públicas.* España.

Pérez Reséndiz, E., & Martínez Bautista, J. L. (2021). La calidad de la información como factor crítico en la eficiencia de la gestión administrativa pública. *Revista de Innovación y Gestión Pública*, 115.

Rojas, V., & Javier, J. (2020). *Incidencia de la ciberseguridad en la toma de decisiones estratégicas en entidades gubernamentales.* Colombia.

Salazar. (2021). *Seguridad digital y calidad de la información para la toma de decisiones en instituciones estatales.* Perú.

Velásquez, J. M., & Yujra, C. A. (2021). Gestión de seguridad de la información y toma de decisiones en entidades gubernamentales. *Gaceta Científica*, 45.

VIII. ANEXOS

8.1. MATRIZ DE CONSISTENCIA

Seguridad Informática y toma de decisiones en los sistemas de Gestión del Gobierno Regional de Lima, 2025.

<table>
<tr><th>PROBLEMAS</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th colspan="4">VARIABLES E INDICADORES</th></tr>
<tr><td rowspan="3"><u>Problema General</u>

¿Qué relación existe entre la seguridad informática y la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025?

<u>Problemas específicos</u>

¿Cómo se relaciona la seguridad informática con la calidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025?</td><td rowspan="3"><u>Objetivos General</u>

Determinar la relación entre la seguridad informática y la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

<u>Objetivos específicos</u>

• Analizar cómo la seguridad informática se relaciona con la calidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno</td><td rowspan="3"><u>Hipótesis General</u>

Existe una relación significativa entre la seguridad informática y la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.

<u>Hipótesis específicas</u>

• La confidencialidad de la información se relaciona significativamente con la calidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno</td><td colspan="4">VARIABLE INDEPENDIENTE (X): Seguridad informática</td></tr>
<tr><td>DIMENSIONES</td><td>INDICADORES</td><td>Ítem</td><td>Nivel/Rango</td></tr>
<tr><td>Confidencialidad de la información</td><td>• Control de accesos.
• Cumplimiento de políticas de seguridad.
• Protección de datos sensibles.</td><td>1,2,3,</td><td rowspan="2">Nunca

Casi nunca

A veces</td></tr>
<tr><td>Integridad</td><td>• Exactitud de los datos.
• Veracidad de la información.
• Consistencia en los sistemas de gestión.</td><td>4,5,6</td></tr>
</table>

<table>
<tr>
<td rowspan="11">¿De qué manera la seguridad informática influye en la oportunidad y actualización de la información disponible para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025?

¿Qué relación existe entre la seguridad informática y la confiabilidad de los datos que sustentan la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025?</td>
<td rowspan="11">Regional de Lima, 2025.
• Evaluar de qué manera la seguridad informática influye en la oportunidad y actualización de la información disponible para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.
• Examinar la relación entre la seguridad informática y la confiabilidad de los datos utilizados en la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.</td>
<td rowspan="11">Regional de Lima, 2025.
• La integridad de la información se relaciona significativamente con la oportunidad de la información utilizada para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.
• La disponibilidad de la información se relaciona significativamente con la confiabilidad de los datos utilizados para la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima, 2025.</td>
<td>Disponibilidad</td>
<td>• Funcionalidad des sistema.
• Respaldo y recuperación de datos.
• Acceso oportuno a la información.</td>
<td>7,8,9</td>
<td>Siempre

Casi Siempre</td>
</tr>
<tr>
<td colspan="4">VARIABLE DEPENDIENTE (Y): Toma de Decisiones</td>
</tr>
<tr>
<td colspan="4">DIMENSIONES</td>
</tr>
<tr>
<td>DIMENSIONES</td>
<td>INDICADORES</td>
<td colspan="2">Ítem
Nivel/Rango</td>
</tr>
<tr>
<td rowspan="3">Calidad de la Información</td>
<td rowspan="3">• Precisión de los datos.
• Completitud de los registros.
• Actualización de datos.</td>
<td rowspan="3">10,11,12</td>
<td rowspan="7">Nunca

Casi nunca

A veces

Siempre

Casi Siempre</td>
</tr>
<tr>
</tr>
<tr>
</tr>
<tr>
<td rowspan="3">Oportunidad de la Información</td>
<td rowspan="3">• Acceso en el momento adecuad
• Rapidez en el procesamiento.
• Pertinencia temporal.</td>
<td rowspan="3">13,14,15</td>
</tr>
<tr>
</tr>
<tr>
</tr>
<tr>
<td rowspan="3">Confiabilidad de los Datos</td>
<td rowspan="3">• Autenticidad de la información.
• Coherencia en los registros.
• Seguridad de la información utilizada.</td>
<td rowspan="3">16,17,18</td>
</tr>
<tr>
</tr>
<tr>
</tr>
</table>

8.2. CUESTIONARIO

Seguridad Informática y toma de decisiones en los sistemas de Gestión del Gobierno Regional de Lima, 2025

El objetivo de esta encuesta es recopilar información sobre la seguridad informática y la toma de decisiones en los sistemas de gestión del Gobierno Regional de Lima durante el año 2025. A través de este cuestionario, se pretende analizar cómo 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 impactan en la operación segura y continua de los sistemas de gestión institucional.

Los datos obtenidos permitirán evaluar el nivel de seguridad informática y la toma de decisiones, contribuyendo a identificar áreas de mejora y fortalecer la gestión tecnológica del Gobierno Regional de Lima.

La encuesta es completamente anónima y la información recopilada será utilizada exclusivamente con fines académicos, garantizando la confidencialidad de las respuestas. Agradecemos su tiempo y participación en este estudio.

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

a. Género

Masculino	
Femenino	

II. 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 SEGURIDAD INFORMÁTICA

DIMENSIÓN: Confidencialidad de la información

1. ¿En mi área se controla adecuadamente quién accede a los sistemas de información?

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

2. ¿Los datos sensibles manejados en los sistemas están protegidos contra accesos no autorizados?

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

3. ¿El personal cumple con las políticas de seguridad informática establecidas por la institución?

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

DIMENSIÓN: Integridad

4. ¿La información registrada en los sistemas es exacta y está libre de errores?

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

5. ¿Los datos ingresados a los sistemas son verificados para garantizar su veracidad?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

6. ¿La información se mantiene consistente entre los diferentes sistemas de gestión utilizados?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

DIMENSIÓN: Disponibilidad

7. ¿Los sistemas de información están disponibles cuando los necesito para realizar mis labores?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

8. ¿Los sistemas funcionan correctamente sin interrupciones frecuentes?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

9. ¿Existen mecanismos de respaldo y recuperación de datos para asegurar la continuidad del trabajo?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

NIVEL DE TOMA DE DESICIONES

DIMENSIÓN: Calidad de la Información

10. ¿La información disponible en los sistemas es precisa y representa adecuadamente la realidad institucional?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

11. ¿Los registros almacenados en los sistemas están completos y no presentan vacíos de información?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

12. ¿Los datos se encuentran actualizados y reflejan cambios recientes en los procesos del área?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

DIMENSIÓN: Oportunidad de la Información

13. ¿La información necesaria para la toma de decisiones está disponible en el momento adecuado?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

14. ¿Los sistemas procesan y entregan información con rapidez suficiente para decisiones oportunas?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

15. ¿Los datos proporcionados por los sistemas corresponden exactamente al periodo temporal que necesito analizar?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

DIMENSIÓN: Confiabilidad de los Datos

16. ¿La información utilizada para tomar decisiones es auténtica y proviene de fuentes verificadas?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

17. ¿Los registros presentan coherencia entre sistemas y no muestran contradicciones?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca

18. ¿Los datos empleados están protegidos y cuentan con mecanismos de seguridad que aseguran su confiabilidad?

a) Siempre b) Casi Siempre c) A veces

d) Casi Nunca e) Nunca