



Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

Seguridad informática y continuidad operativa en los sistemas de gestión
del Gobierno Regional de Lima, - 2025

Tesis

Para optar el Título Profesional de Ingeniero de Sistemas.

Autor

Leonardo Anthony Amet Cristobal Laos

Asesor

Ing. Carlos Manuel Cruz Castañeda



Huacho – Perú

2026



Reconocimiento - No Comercial – Sin Derivadas - Sin restricciones adicionales

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

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



UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

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

FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

INFORMACIÓN

DATOS DEL AUTOR (ES):		
NOMBRES Y APELLIDOS	DNI	FECHA DE SUSTENTACIÓN
Cristobal Laos Leonardo Anthony Amet	45047031	18 de junio del 2026
DATOS DEL ASESOR:		
NOMBRES Y APELLIDOS	DNI	CÓDIGO ORCID
Carlos Manuel Cruz Castañeda	80593441	https://orcid.org/0000-0003-3311-8251
DATOS DE LOS MIEMBROS DE JURADOS – PREGRADO/POSGRADO-MAESTRÍA-DOCTORADO:		
NOMBRES Y APELLIDOS	DNI	CÓDIGO ORCID
Alfredo Edgar Lopez Jimenez	15605331	https://orcid.org/0000-0003-4859-1092
Julio Enrique Guerrero Hurtado	15580855	https://orcid.org/0000-0001-5717-3648
Ronald Demetrio Flores Flores	15300224	https://orcid.org/0000-0003-4211-7285

Leonardo Anthony Amet Cristobal Laos

Seguridad informática y continuidad operativa 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::1:3509750465

Fecha de entrega

17 mar 2026, 11:37 a.m. GMT-5

Fecha de descarga

17 mar 2026, 11:40 a.m. GMT-5

Nombre del archivo

os_sistemas_de_gesti_n_del_Gobierno_Regional_de_Lima,-_2025.pdf

Tamaño del archivo

2.4 MB

102 páginas

16.637 palabras

107.845 caracteres



Página 1 de 110 - Portada

Identificador de la entrega trn:oid::1:3509750465



Página 2 de 110 - Descripción general de integridad

Identificador de la entrega trn:oid::1:3509750465

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
- 5% Publicaciones
- 13% 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 con gratitud a **mi familia**, por su apoyo incondicional, paciencia y amor en cada etapa de mi formación. A ellos, que son mi motivación y fortaleza para alcanzar cada meta propuesta.

AGRADECIMIENTO

Agradezco sinceramente a **Dios**, por brindarme sabiduría y fortaleza durante todo este proceso.

A mis **docentes y asesores**, por su guía y dedicación en el desarrollo de esta investigación.

Y a mi **familia**, por su constante apoyo, comprensión y aliento, que hicieron posible la culminación de este logro académico.

ÍNDICE

DEDICATORIA.....	II
AGRADECIMIENTO	III
INDICE.....	IV
RESUMEN	VIII
ABSTRACT.....	IX
INTRODUCCION.....	X
I. CAPITULO I: PLANTEAMIENTO DEL PROBLEMA	12
1.1. Descripción de la realidad problemática	12
1.2. Formulación del problema.....	14
1.2.1. Problema general	14
1.2.2. Problemas específicos.....	14
1.3. Objetivos de la investigación.....	15
1.3.1. Objetivo general	15
1.3.2. Objetivos específicos	15
1.4. Justificación de la investigación	16
1.5. Delimitación del estudio	17
1.6. Viabilidad del Estudio.....	19
II. CAPITULO II: MARCO TEORICO	22
2.1. Antecedentes de la investigación.....	22
2.1.1. Investigaciones internacionales	22
2.1.2. Investigaciones nacionales	24
2.2. Bases teóricas	26
2.3. Bases filosóficas	58
2.4. Definición de términos básicos.....	61
2.5. Hipótesis de investigación.....	63
2.5.1. Hipótesis general	63
2.5.2. Hipótesis específicas.....	63
2.6. Operacionalización de Variable e Indicadores	63
III. CAPITULO III: METODOLOGIA DE LA INVESTIGACION.....	65
3.1. Diseño metodológico	65

3.2.	Población y muestra.....	66
3.2.1.	Población.....	66
3.2.2.	Muestra	66
3.3.	Técnicas de recolección de datos.....	66
3.4.	Técnicas para el procesamiento de la información.....	67
IV.	CAPITULO IV: RESULTADOS.....	68
4.1.	Análisis de Resultados	68
4.1.1.	Resultados de Seguridad Informática y sus dimensiones.....	68
4.1.2.	Resultados de Continuidad operativa y sus dimensiones.....	73
4.2.	Contrastación de Hipótesis.....	78
4.2.1.	Contrastación de Hipótesis General.....	78
4.2.2.	Contrastación de Hipótesis Especifica 1	79
4.2.3.	Contrastación de Hipótesis Especifica 2.....	80
4.2.4.	Contrastación de Hipótesis Especifica 3.....	81
4.2.5.	Contrastación de Hipótesis Especifica 4.....	82
V.	CAPITULO V: DISCUSIÓN.....	83
5.1.	Discusión de Resultados	83
VI.	CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES.....	86
6.1.	Conclusiones.....	86
6.2.	Recomendaciones	88
VII.	REFERENCIAS.....	90
6.3.	Fuentes bibliográficas	90
VIII.	ANEXOS.....	93
8.1.	MATRIZ DE CONSISTENCIA.....	93
8.2.	CUESTIONARIO.....	95

INDICE DE TABLAS

Tabla 1	Niveles de Seguridad Informática	68
Tabla 2	Niveles de Confidencialidad de la información	69
Tabla 3	Niveles de Integridad de los sistemas	70
Tabla 4	Niveles de Disponibilidad de los sistemas	71
Tabla 5	Niveles de Gestión de riesgos y políticas de seguridad	72
Tabla 6	Niveles de Continuidad operativa	73
Tabla 7	Niveles de Planes de continuidad del negocio	74
Tabla 8	Niveles de Recuperación ante desastres	75
Tabla 9	Niveles de Resiliencia de los sistemas	76
Tabla 10	Niveles de Monitoreo y mantenimiento de operaciones críticas	77

INDICE DE FIGURAS

Figura 1	Niveles de Seguridad Informática.....	68
Figura 2	Niveles de Confidencialidad de la información.....	69
Figura 3	Niveles de Integridad de los sistemas	70
Figura 4	Niveles de Disponibilidad de los sistemas	71
Figura 5	Niveles de Gestión de riesgos y políticas de seguridad	72
Figura 6	Niveles de Continuidad operativa.....	73
Figura 7	Niveles de Planes de continuidad del negocio.....	74
Figura 8	Niveles de Recuperación ante desastres.....	75
Figura 9	Niveles de Resiliencia de los sistemas	76
Figura 10	Niveles de Monitoreo y mantenimiento de operaciones críticas	77

RESUMEN

La investigación titulada “**Seguridad Informática y Continuidad Operativa en los Sistemas de Gestión del Gobierno Regional de Lima, 2025**” tuvo como objetivo principal analizar la relación existente entre la seguridad informática y la continuidad operativa dentro de los sistemas institucionales. El estudio adoptó un **enfoque cuantitativo**, con un **diseño no experimental, correlacional y transversal**, aplicándose un cuestionario estructurado a **210 trabajadores** del Gobierno Regional de Lima. Los resultados obtenidos mediante la prueba de correlación de Spearman revelaron una **relación positiva moderada y estadísticamente significativa** ($r = 0.528$; $p = 0.010$) entre ambas variables, lo que evidencia que el fortalecimiento de la seguridad informática favorece la estabilidad, disponibilidad y funcionamiento continuo de los sistemas de gestión. Asimismo, las dimensiones analizadas planes de continuidad del negocio, recuperación ante desastres, resiliencia de los sistemas y monitoreo de operaciones críticas mostraron correlaciones significativas con la variable principal. En conjunto, los hallazgos destacan que una adecuada gestión de la seguridad informática contribuye de manera directa a la **eficiencia operativa, la sostenibilidad tecnológica y la capacidad institucional de respuesta** frente a incidentes o contingencias.

Palabras clave: seguridad informática, continuidad operativa, resiliencia, recuperación ante desastres, gestión institucional.

ABSTRACT

The research entitled “**Information Security and Operational Continuity in the Management Systems of the Regional Government of Lima, 2025**” aimed to analyze the relationship between information security and operational continuity within the institution’s management systems. The study followed a **quantitative approach** with a **non-experimental, correlational, and cross-sectional design**, applying a structured questionnaire to **210 employees** of the Regional Government of Lima. The results obtained through the Spearman correlation test revealed a **moderate and statistically significant positive relationship** ($r = 0.528$; $p = 0.010$) between the two variables, indicating that strengthening information security enhances the stability, availability, and continuous operation of management systems. Likewise, the analyzed dimensions business continuity planning, disaster recovery, system resilience, and monitoring of critical operations showed significant correlations with the main variable. Overall, the findings demonstrate that an adequate information security management contributes directly to **operational efficiency, technological sustainability, and the institutional capacity to respond effectively to incidents or contingencies**.

Keywords: information security, operational continuity, resilience, disaster recovery, institutional management.

INTRODUCCION

En la actualidad, la **seguridad informática** se ha convertido en un elemento esencial para el funcionamiento eficiente de las instituciones públicas y privadas, especialmente en un contexto en el que la información constituye uno de los recursos más valiosos. Las organizaciones, particularmente las entidades gubernamentales, dependen de sistemas digitales para gestionar sus procesos, almacenar datos y brindar servicios a la ciudadanía. Por ello, la protección de la información y la garantía de la **continuidad operativa** resultan factores determinantes para mantener la confianza institucional y asegurar la calidad en la gestión pública.

En el caso del **Gobierno Regional de Lima**, los sistemas de gestión desempeñan un papel fundamental en la administración de recursos, la toma de decisiones y la prestación de servicios. Sin embargo, dichos sistemas están expuestos a múltiples riesgos, como fallas técnicas, ciberataques, errores humanos o desastres naturales, los cuales pueden comprometer la disponibilidad y confiabilidad de la información. Ante esta realidad, se vuelve indispensable contar con políticas, procedimientos y tecnologías orientadas a prevenir incidentes y garantizar la recuperación oportuna de los sistemas afectados, asegurando así la **continuidad de las operaciones institucionales**.

La **seguridad informática** no solo implica la protección de datos, sino también la implementación de estrategias que fortalezcan la **resiliencia de los sistemas**, la **recuperación ante desastres** y la **planificación de la continuidad del negocio**. Estas acciones permiten que la entidad mantenga sus actividades esenciales aun frente a situaciones adversas, reduciendo el impacto de las interrupciones y optimizando los tiempos de respuesta. En ese sentido, la seguridad informática se convierte en un componente clave dentro de la gestión pública

moderna, garantizando que los servicios digitales permanezcan disponibles y confiables para los usuarios.

En los últimos años, el incremento de amenazas cibernéticas y la creciente dependencia tecnológica han evidenciado la necesidad de reforzar la seguridad digital en las instituciones estatales. Las vulnerabilidades informáticas no solo afectan el flujo de trabajo interno, sino que también pueden comprometer la transparencia y la confianza ciudadana. Por esta razón, analizar la relación entre la seguridad informática y la continuidad operativa en los sistemas de gestión del Gobierno Regional de Lima es fundamental para identificar las fortalezas y debilidades del entorno tecnológico, así como proponer medidas que contribuyan a mejorar la eficiencia y sostenibilidad institucional.

La presente investigación tiene como propósito **determinar la relación entre la seguridad informática y la continuidad operativa en los sistemas de gestión del Gobierno Regional de Lima, 2025**, considerando dimensiones clave como los **planes de continuidad del negocio, la recuperación ante desastres, la resiliencia de los sistemas y el monitoreo de operaciones críticas**. A través de este estudio se busca aportar información valiosa que oriente la toma de decisiones y promueva el fortalecimiento de la infraestructura tecnológica, garantizando la continuidad de los servicios públicos y la protección integral de los activos digitales de la institución.

I. CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

En la actualidad, los gobiernos y organizaciones de todo el mundo dependen cada vez más de los sistemas de información para la gestión eficiente de sus operaciones y la prestación de servicios a la ciudadanía. A nivel internacional, se observa un aumento constante de ciberataques y amenazas informáticas que comprometen la seguridad de los datos y la continuidad de los servicios. Según el **Informe de Seguridad Cibernética Global 2023**, los ataques a instituciones públicas representan más del 25% de los incidentes reportados, generando pérdidas económicas y afectando la confianza de la población en la administración pública (World Economic Forum., 2023). Esta situación evidencia la necesidad de fortalecer la seguridad informática y los planes de continuidad operativa en los sistemas de gestión gubernamentales, para garantizar que los servicios esenciales permanezcan operativos ante incidentes tecnológicos o cibernéticos.

En el contexto nacional, Perú enfrenta desafíos similares. La creciente digitalización de los servicios públicos y la implementación de sistemas electrónicos de gestión, como la administración tributaria, salud y educación, han expuesto vulnerabilidades en la infraestructura tecnológica de las instituciones. Estudios recientes destacan que la falta de políticas claras de seguridad informática, la carencia de personal capacitado en ciberseguridad y la insuficiente implementación de planes de continuidad operativa generan riesgos de interrupciones en los servicios públicos (Contraloría General de la República., 2022)). Estos problemas no solo afectan la eficiencia administrativa, sino también la confianza de los ciudadanos y la integridad de la información manejada por las instituciones públicas.

A nivel local, en el Gobierno Regional de Lima, la situación refleja estas problemáticas. La dependencia de sistemas electrónicos para la gestión de procesos administrativos y de servicios a la población exige que la infraestructura tecnológica esté protegida frente a ataques cibernéticos, fallas técnicas y desastres que puedan interrumpir la operación. Sin embargo, se han identificado deficiencias en la implementación de políticas de seguridad informática y en los protocolos de continuidad operativa, lo que pone en riesgo la prestación eficiente de servicios críticos a la ciudadanía. La ausencia de mecanismos adecuados para la recuperación de información, la falta de pruebas de los planes de contingencia y la limitada capacitación del personal son factores que vulneran la operatividad de los sistemas y, por ende, afectan la gestión pública local (Ministerio de Transportes y Comunicaciones del Per, 2023).

En síntesis, la problemática se centra en que la seguridad informática insuficiente y la ausencia de estrategias robustas de continuidad operativa en el Gobierno Regional de Lima podrían derivar en interrupciones de los servicios, pérdida de información crítica y disminución de la confianza de la población en la administración pública. Esta situación justifica la necesidad de realizar un estudio que permita identificar los factores de riesgo, evaluar la seguridad de los sistemas de gestión y proponer mejoras para garantizar una operación estable y segura en el contexto regional, contribuyendo así al fortalecimiento institucional y a la protección de los intereses de la ciudadanía.

1.2. Formulación del problema

1.2.1. Problema general

¿Qué relaciona seguridad informática y continuidad operativa de los trabajadores del Gobierno Regional de Lima, 2025?

1.2.2. Problemas específicos

¿Cómo se relaciona seguridad informática y planes de continuidad del negocio de los trabajadores del Gobierno Regional de Lima, 2025?

¿De qué manera seguridad informática se relaciona con recuperación ante desastres (Disaster Recovery) de los trabajadores del Gobierno Regional de Lima, 2025?

¿Qué relación hay en seguridad informática y resiliencia de los sistemas de los trabajadores del Gobierno Regional de Lima, 2025?

¿Cómo se relaciona seguridad informática en la capacitación y monitoreo y mantenimiento de operaciones críticas de los trabajadores del Gobierno Regional de Lima, 2025?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Determinar relación a seguridad informática y continuidad operativa de los trabajadores del Gobierno Regional de Lima, 2025.

1.3.2. Objetivos específicos

Analizar cómo seguridad informática se relaciona en planes de continuidad del negocio de los trabajadores del Gobierno Regional de Lima, 2025.

Evaluar de qué manera seguridad informática se relacionan con Recuperación ante desastres (Disaster Recovery) de los trabajadores del Gobierno Regional de Lima, 2025.

Examinar la relación de seguridad informática y Resiliencia de los sistemas de los trabajadores del Gobierno Regional de Lima, 2025.

Investigar cómo seguridad informática se relaciona en Monitoreo y mantenimiento de operaciones críticas de los trabajadores del Gobierno Regional de Lima, 2025.

1.4. Justificación de la investigación

La presente investigación se fundamenta en la necesidad de garantizar la seguridad y continuidad operativa de los sistemas de gestión del Gobierno Regional de Lima, considerando que la dependencia de tecnologías de la información se ha incrementado significativamente en la administración pública. La seguridad informática no solo protege la confidencialidad, integridad y disponibilidad de la información, sino que también asegura que los procesos administrativos y servicios esenciales puedan mantenerse activos ante incidentes, fallas técnicas o ataques cibernéticos. Por tanto, estudiar esta relación resulta crucial para evitar interrupciones que afecten la eficiencia institucional y la confianza de la ciudadanía.

Desde un **enfoque teórico**, esta investigación contribuye a la consolidación del conocimiento sobre la interrelación entre seguridad informática y continuidad operativa en el contexto de los gobiernos regionales. Analizar cómo las políticas, protocolos y estrategias de seguridad impactan la resiliencia de los sistemas de gestión permite generar evidencia empírica que fortalezca los modelos de gestión tecnológica en la administración pública, aportando lineamientos aplicables en otros niveles de gobierno o instituciones similares.

En términos **prácticos**, el estudio permitirá identificar las vulnerabilidades existentes en los sistemas de información del Gobierno Regional de Lima y evaluar la efectividad de las medidas de seguridad y planes de continuidad operativa. Con estos hallazgos, se podrán proponer mejoras concretas que fortalezcan la protección de los datos, optimicen los procesos administrativos y aseguren la continuidad de los servicios esenciales, reduciendo los riesgos de pérdidas de información, interrupciones operativas y afectaciones a la población.

En un **contexto social y local**, la investigación tiene un impacto directo en la ciudadanía, ya que la operatividad confiable de los sistemas de gestión regional asegura la prestación oportuna y eficiente de servicios públicos. Esto no solo incrementa la confianza de los ciudadanos en las instituciones, sino que también contribuye a una administración más transparente y responsable, promoviendo el desarrollo institucional y la seguridad de la información pública.

Finalmente, la relevancia de este estudio también se refleja en el **marco nacional e internacional**, donde la seguridad informática y la continuidad operativa se han convertido en prioridades estratégicas para la gestión pública moderna. Organismos internacionales recomiendan la implementación de políticas robustas de seguridad y planes de continuidad ante la creciente incidencia de ciberataques, mientras que en Perú se evidencia una necesidad urgente de fortalecer la protección de los sistemas tecnológicos en entidades públicas para asegurar la eficiencia, transparencia y sostenibilidad de los servicios (World Economic Forum, 2023; Contraloría General de la República, 2022).

En conclusión, esta investigación se justifica por su aporte a la mejora de la gestión tecnológica y la protección de la información en el Gobierno Regional de Lima, brindando beneficios teóricos, prácticos y sociales, al tiempo que fortalece la resiliencia institucional y la confianza de la ciudadanía en los servicios públicos.

1.5. Delimitación del estudio

Delimitación espacial:

La investigación se realizará en el **Gobierno Regional de Lima**, considerando específicamente los sistemas de gestión que se utilizan para la administración de procesos internos y la prestación

de servicios a la ciudadanía. La elección de este espacio se debe a la relevancia institucional que tiene como ente rector de la región, siendo responsable de coordinar y supervisar la ejecución de políticas públicas y la atención a la población en distintas áreas como salud, educación, transporte y desarrollo social. Se considerará la infraestructura tecnológica, los recursos informáticos disponibles y el personal encargado de la administración de los sistemas, con el fin de evaluar la seguridad informática y la continuidad operativa en un contexto real y representativo.

Delimitación temporal:

El estudio se centrará en el **año 2025**, considerando los sistemas de gestión y las políticas de seguridad informática implementadas durante este período. Este marco temporal permite analizar la situación actual de la gestión tecnológica y los riesgos asociados, considerando los avances recientes en digitalización de la administración pública y la implementación de nuevas herramientas tecnológicas que puedan impactar la seguridad y continuidad de los sistemas.

Delimitación teórica:

La investigación se enfocará en dos variables principales: **seguridad informática** (como variable independiente) y **continuidad operativa** (como variable dependiente). La seguridad informática se analizará a través de sus dimensiones de confidencialidad, integridad, disponibilidad y gestión de riesgos/políticas de seguridad, mientras que la continuidad operativa se estudiará mediante los planes de continuidad del negocio, recuperación ante desastres, resiliencia de los sistemas y monitoreo de operaciones críticas. Se considerarán únicamente los elementos relacionados con la protección de los sistemas de información y la capacidad de mantener la operación de los servicios esenciales, dejando fuera otros factores de gestión

administrativa que no estén directamente vinculados con la seguridad tecnológica y la continuidad operativa.

Delimitación metodológica:

El estudio adoptará un **enfoque cuantitativo**, con diseño **descriptivo correlacional**, ya que busca medir la relación entre la seguridad informática y la continuidad operativa en los sistemas de gestión del Gobierno Regional de Lima. La población estará constituida por los **responsables de la administración de los sistemas y personal técnico relacionado con la gestión de tecnología de la información** en la institución. La técnica de recolección de datos será la **encuesta**, mediante un cuestionario estructurado que permita evaluar las dimensiones de ambas variables. El análisis estadístico se realizará utilizando correlación de Spearman u otros métodos adecuados para determinar la relación entre las variables.

En resumen, la delimitación del estudio establece un marco **claro y específico** que permite centrarse en los aspectos tecnológicos y de gestión relacionados con la seguridad informática y la continuidad operativa, garantizando que los resultados obtenidos sean aplicables y relevantes para la mejora de los sistemas de gestión del Gobierno Regional de Lima durante el año 2025.

1.6. Viabilidad del Estudio

Viabilidad técnica:

El estudio es técnicamente viable, ya que el Gobierno Regional de Lima cuenta con infraestructura tecnológica accesible y sistemas de gestión digitalizados que permiten recopilar información sobre seguridad informática y continuidad operativa. Además, el acceso a los responsables de la administración de los sistemas y personal técnico especializado facilita la

aplicación de encuestas y entrevistas, garantizando la obtención de datos confiables y representativos. Las herramientas tecnológicas actuales, como software de análisis estadístico y plataformas de recopilación de información digital, permiten procesar y analizar los datos de manera eficiente y precisa.

Viabilidad económica:

El estudio requiere recursos limitados, ya que se centrará en la recolección de información mediante cuestionarios estructurados y entrevistas con el personal clave del Gobierno Regional. No se necesitan grandes inversiones en infraestructura adicional ni en equipamiento tecnológico, pues se aprovechará la infraestructura existente en la institución. Los costos asociados se concentran en la impresión de cuestionarios, transporte para acceder a las oficinas y la implementación de software estadístico, los cuales son mínimos y accesibles dentro de un presupuesto de investigación académico.

Viabilidad temporal:

El estudio puede realizarse en un periodo razonable, considerando que se abordará únicamente el año 2025 y los sistemas de gestión correspondientes. La recolección de datos se puede llevar a cabo en pocas semanas debido al tamaño manejable de la población objetivo (personal encargado de los sistemas), y el análisis estadístico y redacción de resultados puede completarse dentro del marco temporal de la tesis. Esto asegura que los objetivos del estudio se cumplan oportunamente sin retrasos significativos.

Viabilidad social y administrativa:

El estudio es socialmente relevante, ya que sus resultados permitirán al Gobierno Regional de Lima fortalecer la seguridad informática y garantizar la continuidad operativa de sus sistemas de gestión, beneficiando directamente a los ciudadanos mediante la mejora en la prestación de

servicios públicos. Administrativamente, la institución tiene interés en optimizar sus procesos tecnológicos y minimizar riesgos, lo que facilita la colaboración y el acceso a la información necesaria para la investigación. La disposición del personal para participar y la relevancia institucional del tema refuerzan la viabilidad del estudio.

En conclusión, la investigación es **totalmente factible**, considerando que cuenta con el soporte técnico, económico, temporal y social necesario. Además, los resultados esperados aportarán recomendaciones prácticas y estratégicas que contribuirán al fortalecimiento de la seguridad y la operatividad de los sistemas de gestión del Gobierno Regional de Lima, asegurando la eficiencia y confiabilidad en la prestación de servicios a la ciudadanía.

II. CAPITULO II: MARCO TEORICO

2.1. Antecedentes de la investigación

2.1.1. Investigaciones internacionales

1. (Ávila-Coello, A. A., 2025).

Título: *Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano.* Esta investigación analiza la necesidad creciente de fortalecer las estrategias de seguridad de la información en las instituciones públicas de Ecuador. A través de una revisión sistemática de la literatura, se examinan las prácticas actuales de seguridad, la madurez en ciberseguridad, los programas de formación y la adopción de tecnologías emergentes. El estudio destaca la importancia de optimizar las estrategias de seguridad, considerando las particularidades del contexto ecuatoriano, para mejorar la protección de datos y la gestión de la información en el sector público. (pág. 25)

2. (Zamora, L. , 2023).

Título: *Propuesta de creación de un CSIRT para el sector gubernamental.* Esta tesis propone la creación de un Centro de Respuesta a Incidentes Cibernéticos (CSIRT) en el sector gubernamental de Nicaragua, ante las vulnerabilidades y pérdidas económicas que sufren los gobiernos por amenazas cibernéticas. A través de un estudio de caso, se determina la viabilidad de implementar un CSIRT, analizando la infraestructura existente, los procedimientos de ciberseguridad y los planes de recuperación ante desastres. El estudio destaca la importancia de contar con un equipo especializado para gestionar incidentes cibernéticos y garantizar la continuidad operativa de los servicios públicos. (pág. 84)

3. (Muñoz, J. J., 2023).

Título: *Modelo de gestión de riesgos basado en AMFE para el GAD Municipal de Flavio Alfaro.* Ante la vulnerabilidad tecnológica del Gobierno Autónomo Descentralizado (GAD) Municipal de Flavio Alfaro, caracterizada por infraestructura obsoleta y ausencia de planes de contingencia, esta investigación diseña un modelo de gestión de riesgos utilizando la metodología AMFE (Análisis Modal de Fallos y Efectos). El estudio identifica, evalúa y mitiga riesgos potenciales que podrían afectar la continuidad operativa de la institución, proponiendo medidas correctivas y preventivas para mejorar la seguridad informática y garantizar la prestación continua de servicios a la ciudadanía. (pág. 66)

4. (Altamirano de la Borda, K. J., 2020).

Título: *La seguridad de la información en la administración pública.* Este estudio aborda la importancia de la seguridad de la información en las instituciones públicas, enfocándose en la protección de datos sensibles y la garantía de la continuidad operativa. Se analizan las políticas y normativas existentes, así como los desafíos enfrentados por las entidades gubernamentales en la implementación de medidas de seguridad. El trabajo destaca la necesidad de adoptar enfoques integrales que incluyan formación del personal, actualización tecnológica y establecimiento de protocolos claros para la gestión de la seguridad de la información.

2.1.2. Investigaciones nacionales

1. (Del Maestro Chamberg, M. G., 2025).

Título: *Ciberseguridad y su incidencia en la seguridad informática del área de sistemas en una entidad pública, Lima-2024.* Esta investigación analiza cómo la ciberseguridad influye en la seguridad informática del área de sistemas en una entidad pública de Lima. Se evalúan las dimensiones de detección, protección y respuesta ante incidentes cibernéticos, destacando la importancia de establecer un sistema de seguridad bien definido en la institución para garantizar su funcionamiento eficiente en la etapa post-COVID-19. (pág. 71)

2. (Olarte Quispe, P. B., 2023).

Título: *Seguridad informática y la vulnerabilidad del sistema de gestión de información en la Municipalidad de Lambayeque.* Esta tesis aborda la situación actual de la seguridad de la información en la Municipalidad Distrital de Lambayeque, identificando vulnerabilidades en su sistema de gestión de información. Se propone una metodología para implementar un Sistema de Gestión de Seguridad de la Información basado en la Norma Técnica Peruana NTP 17799:2008, con el objetivo de mejorar la protección de los datos y garantizar la continuidad operativa de los servicios municipales. (pág. 61)

3. (Avalos Mendoza, M. R., 2023).

Título: *Diseño de un modelo de gestión en seguridad digital para la administración pública peruana.* Esta investigación propone el diseño de un modelo de Gestión de Seguridad Digital aplicable a las entidades del sector público peruano. El modelo integra marcos de referencia y buenas prácticas reconocidas a nivel mundial, como COBIT 2019, con el objetivo de fortalecer las capacidades de prevención y respuesta en materia de seguridad digital,

garantizando la continuidad operativa y la protección de la información en las instituciones públicas. (pág. 89)

4. (Sánchez, N. G. M., 2023).

Título: *El E-Gobierno y la transformación de la administración pública en el Perú.* Este estudio analiza el impacto del E-Gobierno en la transformación de la administración pública en el Perú, enfocándose en la implementación de tecnologías digitales para mejorar la eficiencia y transparencia en la gestión pública. Se discuten los desafíos y beneficios de la digitalización en el sector público, incluyendo aspectos relacionados con la seguridad informática y la continuidad operativa de los servicios gubernamentales. (pág. 53)

5. (Rodríguez, N. J., 2023).

Título: *Continuidad técnica operativa en la infraestructura de red de una entidad pública peruana*

Resumen:

Esta investigación aborda los desafíos y estrategias para garantizar la continuidad técnica operativa dentro de la infraestructura de red de una entidad pública peruana. Se analizan aspectos relacionados con la heterogeneidad de los activos de TI, como hardware y software, y se proponen soluciones para asegurar la disponibilidad y fiabilidad de los servicios digitales ofrecidos por la institución. (pág. 64)

2.2. Bases teóricas

1. Seguridad Informática (Variable Independiente)

1. Introducción

La seguridad informática se ha convertido en un pilar fundamental para la gestión eficiente de las organizaciones modernas, especialmente en el sector público. Con el aumento de la digitalización de los procesos administrativos y la interconexión de sistemas, la información se ha vuelto uno de los activos más valiosos de las instituciones. La protección de estos datos frente a accesos no autorizados, alteraciones o destrucción es esencial para garantizar la continuidad operativa, la confiabilidad de los servicios y la confianza de la ciudadanía (Ávila-Coello, A. A., 2024).

El presente estudio busca analizar los elementos fundamentales de la seguridad informática, sus dimensiones, herramientas, normativas y retos en el contexto institucional, considerando cómo su adecuada implementación contribuye a la eficiencia y resiliencia de los sistemas de información.

2. Concepto de Seguridad Informática

La seguridad informática se define como el conjunto de medidas, políticas y prácticas orientadas a proteger los sistemas de información contra amenazas internas y externas, asegurando la confidencialidad, integridad y disponibilidad de los datos (Guarneros, J., 2022). En el ámbito gubernamental, esta disciplina no solo protege la información sensible de la administración y de los ciudadanos, sino que también garantiza la continuidad de los servicios esenciales, minimizando riesgos de interrupción y pérdidas de datos.

2.1 Confidencialidad

La confidencialidad consiste en asegurar que la información sea accesible únicamente a personas autorizadas. En instituciones públicas, esto implica proteger bases de datos de ciudadanos, expedientes administrativos y reportes internos, evitando filtraciones o usos indebidos. Las técnicas comunes incluyen cifrado de datos, control de accesos y autenticación multifactorial (Ávila-Coello, A. A., seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano., 2024)

2.2 Integridad

La integridad se refiere a la protección de la información y los sistemas frente a modificaciones no autorizadas o accidentales. Mantener la integridad garantiza que los datos reflejen con exactitud la realidad, permitiendo decisiones administrativas basadas en información confiable. Se utilizan mecanismos como firmas digitales, auditorías de registro y controles de versiones de datos (Guarneros, J., 2022).

2.3 Disponibilidad

La disponibilidad asegura que los sistemas y servicios estén accesibles cuando se necesiten. La indisponibilidad de sistemas puede paralizar operaciones críticas y afectar la prestación de servicios a la ciudadanía. Estrategias para garantizar la disponibilidad incluyen redundancia de sistemas, copias de seguridad, mantenimiento preventivo y monitoreo continuo (Torres Quevedo, L. A., 2023).

2.4 Gestión de riesgos y políticas de seguridad

Una correcta gestión de riesgos permite identificar, evaluar y mitigar amenazas que puedan comprometer los sistemas. Las políticas de seguridad institucional formalizan normas y procedimientos, definiendo responsabilidades, protocolos de respuesta y medidas preventivas. Esto incluye planes de contingencia, formación del personal y cumplimiento de estándares internacionales, como ISO 27001 (Collantes Collantes, R. A., 2025).

3. Importancia de la Seguridad Informática

La seguridad informática es crucial por varias razones:

Protección de activos críticos: Garantiza la integridad de los sistemas y datos estratégicos de la institución.

Cumplimiento normativo: Permite cumplir regulaciones nacionales e internacionales sobre manejo de información.

Confianza ciudadana: La seguridad de los sistemas aumenta la credibilidad de la institución ante la población.

Prevención de pérdidas económicas: Reduce riesgos de fraude, ataques cibernéticos o fallas que puedan generar costos altos.

En el sector público peruano, la falta de seguridad informática puede afectar la eficiencia de la gestión, la transparencia y la continuidad de los servicios, especialmente en gobiernos regionales donde los sistemas administrativos dependen cada vez más de la tecnología (Torres Quevedo, L. A., 2023) (Collantes Collantes, R. A., 2025).

4. Herramientas y Tecnologías de Seguridad Informática

Entre las principales herramientas y tecnologías destacan:

Cifrado de datos: Protege la información mediante algoritmos que la hacen ilegible para usuarios no autorizados.

Firewalls y antivirus: Previenen accesos no deseados y detectan programas maliciosos.

Sistemas de control de acceso: Permiten definir quién puede acceder a qué información.

Monitoreo y auditoría de sistemas: Detectan anomalías y posibles ataques en tiempo real.

La implementación adecuada de estas herramientas requiere capacitación constante del personal y actualización tecnológica frente a nuevas amenazas cibernéticas.

5. Retos y desafíos

Entre los principales desafíos de la seguridad informática se encuentran:

Ciberataques cada vez más sofisticados: Phishing, ransomware y ataques dirigidos a instituciones públicas.

Limitaciones presupuestales: Falta de recursos para actualizar sistemas y contratar personal especializado.

Capacitación insuficiente del personal: La seguridad depende tanto de la tecnología como de la formación de los usuarios.

Gestión de la continuidad operativa: Garantizar que los sistemas sigan funcionando ante fallas técnicas o desastres naturales.

6. Conclusiones

La seguridad informática es un componente crítico para cualquier organización, especialmente en el ámbito público, donde los datos y sistemas son fundamentales para la prestación de servicios. Garantizar la confidencialidad, integridad, disponibilidad y una adecuada gestión de riesgos no solo protege la información, sino que asegura la continuidad de las operaciones y fortalece la confianza ciudadana. La integración de herramientas tecnológicas, políticas de seguridad claras y capacitación constante del personal constituyen la base para enfrentar los retos actuales y futuros de la ciberseguridad.

Dimensiones:

Confidencialidad de la Información:

1. Introducción

La confidencialidad de la información es un principio fundamental dentro de la seguridad informática, que asegura que los datos sean accesibles únicamente a las personas autorizadas. En un contexto gubernamental, proteger la información sensible de ciudadanos y del Estado es crucial para mantener la confianza pública, garantizar la privacidad y prevenir el uso indebido de datos críticos. La digitalización de los procesos administrativos ha incrementado la necesidad de implementar medidas que aseguren la confidencialidad, especialmente ante amenazas cibernéticas cada vez más sofisticadas (Ávila-Coello, A. A., 2024).

2. Concepto de Confidencialidad de la Información

La confidencialidad de la información se define como la propiedad de la información que asegura que únicamente personas autorizadas puedan acceder a ella, evitando su divulgación a individuos, entidades o procesos no permitidos (ISO/IEC 27002, 2022). En términos prácticos, implica proteger datos sensibles, registros administrativos, información financiera y expedientes personales de ciudadanos, evitando filtraciones que puedan generar perjuicios legales, económicos o sociales.

Según (Guarneros, J., 2022), la confidencialidad no solo protege los datos, sino que también fortalece la confianza en los sistemas de información y en las instituciones que los administran.

3. Principios y Mecanismos de Confidencialidad

3.1 Principios básicos

Acceso limitado: Solo usuarios autorizados pueden consultar, modificar o transmitir la información.

Necesidad de saber: Cada persona tiene acceso únicamente a la información necesaria para cumplir sus funciones.

Protección legal y normativa: El cumplimiento de leyes y normativas sobre protección de datos refuerza la confidencialidad (Ley N° 29733, Ley de Protección de Datos Personales, Perú).

3.2 Mecanismos y herramientas

Cifrado de datos: Transformación de la información en códigos ilegibles para personas no autorizadas.

Control de accesos: Sistemas que asignan permisos según roles y niveles jerárquicos.

Autenticación multifactor: Verificación mediante combinaciones de contraseñas, biometría o tokens de seguridad.

Políticas y protocolos internos: Normas que establecen responsabilidades, sanciones y procedimientos para proteger la información (Ávila-Coello, A. A., seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano., 2024).

4. Importancia de la Confidencialidad en el Ámbito Gubernamental

Protección de datos ciudadanos: Los gobiernos manejan información sensible como datos de salud, registros civiles y financieros, cuya filtración puede afectar derechos fundamentales.

Prevención de fraudes y delitos cibernéticos: La confidencialidad ayuda a mitigar riesgos de robo de identidad, corrupción y espionaje digital.

Garantía de confianza institucional: Los ciudadanos confían en las instituciones que aseguran la privacidad de su información personal.

Cumplimiento legal: Las normativas locales e internacionales obligan a proteger la información para evitar sanciones legales.

5. Retos y Desafíos

La implementación de la confidencialidad enfrenta varios desafíos, especialmente en instituciones públicas:

Amenazas cibernéticas crecientes: Malware, phishing y ataques dirigidos pueden comprometer la información sensible.

Falta de capacitación del personal: Los errores humanos representan uno de los mayores riesgos para la confidencialidad.

Recursos limitados: La inversión en tecnología y herramientas de seguridad a menudo es insuficiente.

Integración con sistemas existentes: Garantizar confidencialidad en sistemas heredados o antiguos requiere actualizaciones y protocolos específicos (Torres Quevedo, L. A., 2023).

6. Conclusiones

La confidencialidad de la información es un componente esencial de la seguridad informática y un requisito indispensable en la gestión pública moderna. Proteger los datos frente a accesos no autorizados fortalece la confianza ciudadana, asegura la continuidad de los servicios y minimiza riesgos legales y económicos. La implementación efectiva de políticas, herramientas tecnológicas y formación del personal son factores clave para garantizar que la información sensible permanezca protegida frente a amenazas internas y externas.

En conclusión, la confidencialidad no solo es un principio técnico, sino también un compromiso institucional que sustenta la eficiencia, transparencia y confiabilidad de las organizaciones.

Integridad de los Sistemas:

1. Introducción

La integridad de los sistemas es un principio esencial dentro de la seguridad informática que garantiza que la información y los procesos permanezcan completos, precisos y libres de alteraciones no autorizadas. En el ámbito gubernamental, asegurar la integridad de los sistemas es crucial para mantener la confianza en los servicios digitales ofrecidos a los ciudadanos y para proteger la veracidad de la información administrativa, financiera y legal. Las fallas en la integridad pueden derivar en decisiones erróneas, pérdida de credibilidad institucional y vulnerabilidades frente a ataques cibernéticos (Guarneros, J., 2022)

El propósito de esta monografía es analizar la importancia de la integridad de los sistemas, sus mecanismos de protección, retos y su relevancia en la gestión pública moderna.

2. Concepto de Integridad de los Sistemas

La integridad de los sistemas se define como la propiedad que asegura que la información almacenada y procesada por los sistemas se mantenga completa, exacta y confiable durante todo su ciclo de vida, evitando modificaciones no autorizadas o accidentales (ISO/IEC 27002, 2022). Esto abarca tanto la información digital como los procesos automatizados y manuales asociados a la gestión de los datos.

Según (Ávila-Coello, A. A., seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano., 2024), la integridad es clave para generar confianza en los sistemas de información y garantizar que las decisiones tomadas por la administración pública se basen en datos correctos y verificados.

3. Principios y Mecanismos de Integridad

3.1 Principios básicos

Exactitud: La información debe reflejar correctamente la realidad que representa.

Compleitud: Ningún dato relevante debe ser omitido o alterado sin autorización.

Consistencia: Los datos deben mantener coherencia interna y entre sistemas relacionados.

3.2 Mecanismos y herramientas

Firmas digitales: Garantizan que los documentos y transacciones no hayan sido alterados desde su emisión.

Control de versiones y auditorías: Permiten rastrear cambios en archivos, bases de datos y sistemas, asegurando transparencia y trazabilidad.

Checksums y hashes criptográficos: Detectan cualquier modificación no autorizada de archivos o bases de datos.

Políticas de control de acceso: Limita las acciones que cada usuario puede realizar sobre la información, reduciendo riesgos de alteración accidental o maliciosa (Collantes Collantes, 2025).

4. Importancia de la Integridad en el Ámbito Gubernamental

Toma de decisiones confiable: Los sistemas gubernamentales dependen de información precisa para gestionar recursos, servicios y políticas públicas.

Protección contra fraudes y manipulaciones: La integridad ayuda a prevenir modificaciones maliciosas que puedan afectar resultados electorales, financieros o administrativos.

Confianza ciudadana: Garantiza que la información proporcionada por las instituciones públicas sea veraz y verificable.

Cumplimiento normativo: Responde a regulaciones y estándares nacionales e internacionales que exigen manejo seguro y confiable de datos.

5. Retos y Desafíos

Ataques internos y externos: Empleados deshonestos o hackers pueden alterar datos críticos.

Errores humanos: Cambios accidentales pueden comprometer la integridad de la información.

Compatibilidad entre sistemas: Mantener consistencia y exactitud entre múltiples plataformas requiere procedimientos y herramientas avanzadas.

Gestión de grandes volúmenes de datos: La cantidad de información que manejan los gobiernos hace que el monitoreo y control sean complejos (Ávila-Coello, A. A., 2024).

6. Conclusiones

La integridad de los sistemas es un principio esencial para garantizar la precisión, completitud y confiabilidad de la información en las instituciones públicas. Su implementación efectiva protege contra fraudes, errores y ataques cibernéticos, asegurando que los servicios digitales sean confiables y que las decisiones se basen en datos verificados. Los mecanismos

tecnológicos, junto con políticas claras de control y auditoría, son fundamentales para mantener la integridad, fortaleciendo así la confianza ciudadana y la eficiencia administrativa.

En síntesis, la integridad no solo es un requisito técnico, sino también un pilar ético y operativo que sustenta la transparencia y efectividad de la administración pública.

Disponibilidad de los Sistemas:

1. Introducción

La disponibilidad de los sistemas es un principio esencial dentro de la seguridad informática que asegura que los servicios y sistemas tecnológicos estén accesibles y operativos cuando se necesiten. En el ámbito gubernamental, mantener la disponibilidad es crucial para garantizar la continuidad de los procesos administrativos, la prestación de servicios a los ciudadanos y la confiabilidad de la gestión pública. La indisponibilidad de sistemas puede afectar la eficiencia institucional, generar pérdidas económicas y comprometer la confianza de la ciudadanía (Torres Quevedo, L. A., 2023).

Esta monografía analiza la importancia de la disponibilidad de los sistemas, los mecanismos para garantizarla, los retos en su implementación y su relevancia para la administración pública.

2. Concepto de Disponibilidad de los Sistemas

La disponibilidad se refiere a la capacidad de un sistema de información para estar operativo y accesible cuando sea necesario, minimizando el tiempo de inactividad y asegurando la continuidad de los procesos críticos (ISO/IEC 27002, 2022).

Según (Guarneros, J., 2022), la disponibilidad no solo implica que los sistemas funcionen, sino también que los servicios digitales asociados sean confiables y se mantengan activos incluso ante fallas técnicas o incidentes externos.

3. Principios y Mecanismos de Disponibilidad

3.1 Principios básicos

Acceso continuo: Los usuarios autorizados deben poder acceder a la información y sistemas sin interrupciones.

Redundancia: Sistemas críticos deben tener respaldo para evitar fallos totales.

Mantenimiento proactivo: Revisión y actualización constante de hardware, software y redes para evitar interrupciones.

3.2 Mecanismos y herramientas

Servidores redundantes: Permiten que, ante la falla de un servidor, otro asuma la operación sin afectar los servicios.

Sistemas de respaldo y recuperación: Copias de seguridad periódicas que aseguran restauración rápida ante fallos.

Monitoreo en tiempo real: Supervisión constante de sistemas para detectar y solucionar problemas antes de que afecten a los usuarios.

Planes de contingencia: Procedimientos claros para garantizar la continuidad de los servicios ante interrupciones imprevistas (Collantes Collantes, R. A., 2025).

4. Importancia de la Disponibilidad en el Ámbito Gubernamental

Garantiza continuidad operativa: Mantiene los procesos administrativos y servicios esenciales funcionando incluso en situaciones adversas.

Evita pérdidas económicas y sociales: La indisponibilidad de sistemas puede generar retrasos en pagos, trámites y atención al público.

Fortalece la confianza ciudadana: Los ciudadanos confían en los servicios públicos cuando estos son accesibles y eficientes.

Cumplimiento de normativas: Asegura que las entidades públicas cumplan con regulaciones sobre continuidad de operaciones y servicio a la ciudadanía (Ávila-Coello, A. A., 2024).

5. Retos y Desafíos

Fallos técnicos inesperados: Problemas de hardware, software o red que pueden interrumpir el acceso a los sistemas.

Ataques cibernéticos: Ransomware y ataques de denegación de servicio (DoS) afectan la disponibilidad.

Falta de recursos tecnológicos: Algunas instituciones públicas no cuentan con sistemas redundantes o herramientas de monitoreo avanzado.

Gestión de grandes volúmenes de datos: La alta demanda de acceso simultáneo puede comprometer la disponibilidad si no hay infraestructura adecuada (Guarneros, 2022).

6. Conclusiones

La disponibilidad de los sistemas es un componente crítico de la seguridad informática y de la gestión pública eficiente. Garantizar que los servicios y sistemas estén accesibles en todo momento asegura la continuidad operativa, protege la confianza de los ciudadanos y minimiza riesgos económicos y administrativos. La implementación de mecanismos tecnológicos, políticas de mantenimiento y planes de contingencia son esenciales para mantener la disponibilidad y resiliencia de los sistemas gubernamentales.

En conclusión, la disponibilidad no solo es un requisito técnico, sino también un compromiso institucional que sustenta la eficiencia, transparencia y confiabilidad de los servicios públicos.

Gestión de Riesgos y Políticas de Seguridad:

1. Introducción

La gestión de riesgos y la implementación de políticas de seguridad son componentes esenciales de la seguridad informática, especialmente en instituciones públicas. Estas prácticas permiten identificar, evaluar y mitigar riesgos asociados a los sistemas de información, asegurando que la operación de los servicios críticos se mantenga frente a posibles amenazas. La adopción de políticas y protocolos claros fortalece la prevención de incidentes y garantiza la continuidad operativa en un entorno cada vez más digitalizado (Ávila-Coello, A. A., 2024).

Esta monografía analiza los conceptos, mecanismos, importancia, retos y beneficios de la gestión de riesgos y políticas de seguridad, con énfasis en su aplicación en entornos gubernamentales.

2. Concepto de Gestión de Riesgos y Políticas de Seguridad

La gestión de riesgos en seguridad informática es el proceso sistemático de identificar amenazas potenciales, evaluar su impacto y probabilidad, y aplicar medidas para reducir los riesgos a niveles aceptables. Por su parte, las políticas de seguridad son normas, protocolos y directrices que regulan la protección de los sistemas de información y definen responsabilidades del personal (ISO/IEC 27005, 2022).

Según (Guarneros, J., 2022), la combinación de gestión de riesgos y políticas de seguridad permite prevenir incidentes de seguridad, mejorar la resiliencia de los sistemas y garantizar la confianza en la información y los servicios ofrecidos por las instituciones públicas.

3. Principios y Mecanismos

3.1 Principios básicos

Identificación de riesgos: Reconocer amenazas internas y externas que puedan afectar la seguridad de los sistemas.

Evaluación de riesgos: Analizar la probabilidad e impacto de cada amenaza para priorizar acciones.

Mitigación: Aplicar controles, herramientas y procedimientos para reducir la exposición a riesgos.

Documentación y actualización: Mantener registros de riesgos, incidentes y medidas adoptadas, revisándolos periódicamente.

3.2 Mecanismos y herramientas

Análisis de vulnerabilidades: Escaneo y monitoreo constante de los sistemas para detectar debilidades.

Plan de contingencia: Estrategias para responder rápidamente ante incidentes de seguridad.

Normas y estándares de seguridad: Cumplimiento de ISO 27001, NIST y otras regulaciones que establecen buenas prácticas.

Capacitación del personal: Programas de formación para que los empleados conozcan los riesgos y protocolos de seguridad (Collantes Collantes, R. A., 2025).

4. Importancia de la Gestión de Riesgos y Políticas de Seguridad

Prevención de incidentes: La identificación y mitigación de riesgos reduce la probabilidad de ataques y fallas.

Protección de activos críticos: Los datos, sistemas y procesos estratégicos se mantienen seguros frente a amenazas.

Continuidad operativa: Minimiza interrupciones y asegura que los servicios públicos sigan funcionando ante incidentes.

Cumplimiento legal y normativo: Evita sanciones y asegura el respeto a regulaciones nacionales e internacionales sobre seguridad de la información (Torres Quevedo, 2023; Ávila-Coello, 2024).

5. Retos y Desafíos

Evolución constante de amenazas: Nuevos tipos de ataques requieren actualización continua de políticas y medidas de seguridad.

Falta de cultura organizacional: Sin compromiso del personal, los protocolos y políticas pueden ser ignorados o mal aplicados.

Recursos limitados: Instituciones públicas pueden carecer de presupuesto para implementar todas las medidas de seguridad necesarias.

Integración de sistemas heterogéneos: Garantizar la seguridad de sistemas antiguos y modernos simultáneamente puede ser complejo (Guarneros, 2022).

6. Conclusiones

La gestión de riesgos y políticas de seguridad es un componente esencial para proteger la información y los sistemas de cualquier organización, especialmente en el sector público. Identificar amenazas, evaluar su impacto, aplicar medidas de mitigación y establecer políticas claras permite prevenir incidentes, mantener la continuidad operativa y asegurar la confianza ciudadana. La combinación de herramientas tecnológicas, normas internacionales y capacitación del personal constituye la base para una gestión de riesgos eficaz.

En síntesis, esta dimensión no solo protege los activos de información, sino que fortalece la resiliencia institucional y la capacidad de respuesta frente a amenazas internas y externas, asegurando una administración pública confiable y eficiente.

Autores Relevantes:

(Ávila-Coello, A. A., 2024): En su estudio sobre la seguridad de la información en instituciones públicas, destaca la importancia de fortalecer las estrategias de seguridad, la madurez en ciberseguridad, los programas de formación y la adopción de tecnologías emergentes.

(Guarneros, J., 2022): Propone la implementación de procesos de seguridad informática bajo el estándar ISO 27001 para garantizar la continuidad de las operaciones en instituciones educativas.

2. Continuidad Operativa (Variable Dependiente)**1. Introducción**

La continuidad operativa es un principio fundamental en la gestión organizacional que busca garantizar que las funciones críticas de una institución puedan mantenerse frente a cualquier incidente o interrupción, ya sea de origen natural, técnico o humano. En el ámbito gubernamental, la continuidad operativa adquiere especial relevancia porque asegura la prestación ininterrumpida de servicios públicos esenciales, protege los datos de los ciudadanos y garantiza la eficiencia administrativa (Ávila-Coello, 2024).

La digitalización de los procesos y la dependencia de sistemas tecnológicos han incrementado la necesidad de establecer planes de continuidad operativa, con protocolos claros que permitan reaccionar y adaptarse rápidamente ante eventos inesperados. Esta monografía analiza el concepto, dimensiones, mecanismos, importancia y desafíos de la continuidad operativa en instituciones públicas.

2. Concepto de Continuidad Operativa

La continuidad operativa se define como la capacidad de una organización para mantener sus procesos críticos y funciones esenciales durante y después de un incidente disruptivo, minimizando la interrupción de servicios y el impacto negativo en la institución (ISO 22301, 2022).

Según Guarneros (2022), la continuidad operativa no solo depende de la infraestructura tecnológica, sino también de la planificación estratégica, los recursos humanos capacitados y la implementación de protocolos de respuesta ante contingencias. En el contexto gubernamental, la continuidad operativa asegura que los ciudadanos puedan acceder a servicios vitales como atención médica, registros civiles y pagos de servicios sin interrupciones prolongadas.

3. Principios y Mecanismos de la Continuidad Operativa

3.1 Principios básicos

Identificación de procesos críticos: Reconocer las funciones esenciales que no deben interrumpirse.

Planificación y preparación: Establecer procedimientos y recursos necesarios para mantener operaciones en situaciones adversas.

Capacidad de recuperación rápida: Minimizar el tiempo de inactividad mediante estrategias y herramientas adecuadas.

Evaluación y mejora continua: Revisar y actualizar regularmente los planes de continuidad según cambios en la organización y nuevas amenazas.

3.2 Mecanismos y herramientas

Planes de continuidad del negocio (BCP): Estrategias documentadas que definen cómo mantener los procesos críticos ante interrupciones.

Recuperación ante desastres (Disaster Recovery): Procedimientos y sistemas para restaurar operaciones y datos tras incidentes como fallas técnicas o desastres naturales.

Sistemas redundantes: Infraestructura tecnológica duplicada que asegura la disponibilidad de servicios críticos.

Monitoreo y mantenimiento de operaciones críticas: Supervisión constante para detectar problemas y garantizar que los procesos esenciales funcionen de manera continua (Collantes Collantes, 2025).

4. Importancia de la Continuidad Operativa en el Ámbito Gubernamental

Garantiza la prestación continua de servicios públicos: Minimiza interrupciones que afectan a la ciudadanía.

Protege los datos de los ciudadanos: Evita pérdidas o daños de información crítica durante incidentes.

Fortalece la resiliencia institucional: Permite que la organización se recupere rápidamente y continúe operando con eficiencia.

Cumplimiento de normativas y estándares internacionales: Asegura que la institución cumpla con regulaciones sobre gestión de riesgos y continuidad de servicios (Torres Quevedo, 2023; Ávila-Coello, 2024).

5. Retos y Desafíos

Amenazas externas e internas: Desastres naturales, ataques cibernéticos y errores humanos pueden afectar la continuidad.

Recursos limitados: La implementación de planes y sistemas de respaldo requiere inversión tecnológica y capacitación especializada.

Integración de sistemas: Garantizar continuidad en sistemas antiguos y modernos simultáneamente puede ser complejo.

Pruebas y actualizaciones constantes: Los planes deben revisarse periódicamente para asegurar su eficacia frente a nuevos riesgos (Guarneros, 2022).

6. Conclusiones

La continuidad operativa es un elemento estratégico indispensable para cualquier institución, especialmente en el sector público, donde la interrupción de servicios puede afectar directamente a la población y comprometer la confianza ciudadana. Su implementación efectiva requiere planificación, sistemas redundantes, procedimientos de recuperación ante desastres y supervisión constante.

En síntesis, garantizar la continuidad operativa no solo protege los activos y datos de la organización, sino que también fortalece su resiliencia, eficiencia y capacidad de respuesta frente a incidentes, asegurando que los servicios esenciales se mantengan siempre disponibles para los ciudadanos.

Dimensiones:**Planes de Continuidad del Negocio:****1. Introducción**

Los Planes de Continuidad del Negocio (Business Continuity Plan, BCP) son herramientas estratégicas fundamentales que permiten a las organizaciones mantener sus operaciones críticas durante situaciones de crisis, desastres o interrupciones imprevistas. En el ámbito gubernamental, estos planes son esenciales para asegurar que los servicios públicos, la atención ciudadana y la protección de información sensible se mantengan operativos frente a eventos disruptivos (Ávila-Coello, 2024).

El BCP proporciona un marco estructurado que identifica funciones críticas, establece procedimientos alternativos y asigna recursos necesarios para garantizar la continuidad de la operación institucional.

2. Concepto de Planes de Continuidad del Negocio

Un Plan de Continuidad del Negocio es un conjunto documentado de estrategias, políticas y procedimientos que permite a una organización continuar con sus funciones esenciales en caso de incidentes que interrumpan la operación normal (ISO 22301, 2022). Estos planes no solo buscan la recuperación tras un evento adverso, sino que también permiten mitigar riesgos y mantener la confianza de los ciudadanos y stakeholders en la institución.

Según Guarneros (2022), el BCP es un instrumento preventivo y estratégico que asegura que los procesos críticos de una organización se mantengan activos y que los impactos de interrupciones se reduzcan al mínimo posible.

3. Principios y Componentes

3.1 Principios básicos

Identificación de funciones críticas: Determinar cuáles procesos y servicios son esenciales para la operación institucional.

Evaluación de riesgos: Analizar las amenazas potenciales y el impacto que tendrían sobre las operaciones críticas.

Planificación de recursos alternativos: Asignar personal, tecnología y procedimientos de respaldo para garantizar continuidad.

Pruebas y mantenimiento: Evaluar periódicamente la efectividad del plan y actualizarlo según cambios internos o externos.

3.2 Componentes del BCP

Análisis de impacto al negocio (BIA): Estudio de las funciones críticas y el efecto de su interrupción.

Estrategias de recuperación: Procedimientos alternativos para mantener operaciones esenciales.

Plan de comunicación: Definición de canales y responsables para informar al personal y ciudadanos durante una crisis.

Documentación y capacitación: Registro detallado de procedimientos y entrenamiento del personal para su correcta ejecución (Collantes Collantes, 2025).

4. Importancia de los Planes de Continuidad del Negocio

Garantiza la prestación de servicios esenciales: Minimiza la interrupción de trámites, pagos y servicios al ciudadano.

Protege la información crítica: Evita la pérdida o corrupción de datos esenciales durante emergencias.

Fortalece la resiliencia institucional: Permite que la organización se recupere rápidamente y continúe operando eficientemente.

Cumplimiento normativo: Responde a estándares internacionales y leyes locales sobre gestión de riesgos y continuidad operativa (Torres Quevedo, 2023; Ávila-Coello, 2024).

5. Retos y Desafíos

Desconocimiento o falta de cultura organizacional: Personal no capacitado puede dificultar la ejecución efectiva del plan.

Limitaciones de recursos: Implementar BCP requiere inversión en infraestructura, tecnología y formación.

Adaptación a cambios tecnológicos: Los sistemas digitales en constante evolución requieren actualización constante de los planes.

Pruebas y simulaciones insuficientes: La ausencia de pruebas periódicas puede hacer que los planes no funcionen adecuadamente durante una crisis (Guarneros, 2022).

6. Conclusiones

Los Planes de Continuidad del Negocio (BCP) son una herramienta estratégica indispensable para cualquier institución, especialmente en el sector público, donde la interrupción de servicios puede afectar directamente a la ciudadanía. Su implementación garantiza la identificación de funciones críticas, la planificación de recursos alternativos y la capacidad de respuesta ante incidentes, fortaleciendo la resiliencia institucional y asegurando la prestación ininterrumpida de servicios esenciales.

En síntesis, los BCP no solo protegen la operación y los datos de la institución, sino que también refuerzan la confianza ciudadana y la eficiencia de la gestión pública.

Recuperación ante Desastres (Disaster Recovery):

1. Introducción

La **recuperación ante desastres** o *Disaster Recovery (DR)* es un componente esencial de la continuidad operativa y de la seguridad informática, enfocado en restaurar los sistemas, aplicaciones y servicios críticos después de un fallo, ataque cibernético o desastre natural. En el ámbito gubernamental, este proceso es vital para garantizar que los servicios públicos continúen operando y que los datos de los ciudadanos se mantengan protegidos y disponibles (Ávila-Coello, 2024).

El objetivo principal de la recuperación ante desastres es minimizar el tiempo de inactividad, reducir el impacto negativo sobre la organización y asegurar que las operaciones puedan reanudarse de manera efectiva y segura.

2. Concepto de Recuperación ante Desastres

La **recuperación ante desastres** se define como el conjunto de políticas, procedimientos y herramientas que permiten restaurar los sistemas, aplicaciones y datos críticos después de un evento disruptivo, garantizando que la institución pueda continuar con sus operaciones esenciales en el menor tiempo posible (ISO 22301, 2022).

Según Guarneros (2022), el *Disaster Recovery* no solo se centra en la recuperación tecnológica, sino que también implica planificación estratégica, asignación de recursos y entrenamiento del personal para garantizar una respuesta efectiva ante cualquier contingencia.

3. Principios y Mecanismos

3.1 Principios básicos

Tiempo de recuperación mínimo (RTO): Definir el tiempo máximo permitido para restaurar operaciones críticas.

Pérdida de datos aceptable (RPO): Determinar la cantidad máxima de datos que se pueden perder sin afectar la continuidad del negocio.

Redundancia y respaldo: Contar con sistemas, datos y aplicaciones duplicadas para garantizar disponibilidad.

Pruebas periódicas: Evaluar la efectividad del plan mediante simulaciones y ajustes constantes.

3.2 Mecanismos y herramientas

Copias de seguridad (Backups): Almacenamiento seguro de datos críticos en medios físicos, virtuales o en la nube.

Centros de recuperación alternativos: Instalaciones secundarias que pueden asumir la operación en caso de fallo del centro principal.

Software de recuperación automatizada: Herramientas que aceleran la restauración de sistemas y datos.

Protocolos de comunicación y coordinación: Procedimientos claros para informar al personal y ciudadanos durante la recuperación (Collantes Collantes, 2025).

4. Importancia de la Recuperación ante Desastres en el Ámbito Gubernamental

Minimiza interrupciones en servicios públicos: Permite que los ciudadanos continúen accediendo a trámites y servicios esenciales.

Protege la información sensible: Evita la pérdida de datos críticos y garantiza la integridad de la información gubernamental.

Fortalece la resiliencia institucional: Asegura que la organización pueda recuperarse rápida y eficazmente tras incidentes.

Cumple normativas y estándares internacionales: Responde a requerimientos de gestión de riesgos, continuidad operativa y seguridad de la información (Torres Quevedo, 2023; Ávila-Coello, 2024).

5. Retos y Desafíos

Ataques cibernéticos sofisticados: Ransomware y malware pueden comprometer la recuperación de datos.

Falta de infraestructura adecuada: Instituciones públicas pueden carecer de centros de respaldo o software especializado.

Capacitación insuficiente: Personal no entrenado puede retrasar o complicar la recuperación.

Actualización constante: Los planes de recuperación deben adaptarse a cambios tecnológicos y a la evolución de amenazas (Guarneros, 2022).

6. Conclusiones

La **recuperación ante desastres** es un pilar crítico dentro de la continuidad operativa, asegurando que los sistemas, aplicaciones y datos esenciales se restauren de manera rápida y efectiva tras cualquier incidente. Su implementación requiere planificación estratégica, herramientas tecnológicas, infraestructura de respaldo y personal capacitado.

En síntesis, un plan de recuperación ante desastres eficiente no solo protege la operación institucional y la información crítica, sino que también fortalece la confianza ciudadana y la capacidad de respuesta del gobierno frente a situaciones adversas, garantizando la continuidad de los servicios públicos.

Resiliencia de los Sistemas:

1. Introducción

La **resiliencia de los sistemas** es un principio clave dentro de la continuidad operativa y la seguridad informática, que se centra en la capacidad de los sistemas para adaptarse, resistir y recuperarse rápidamente ante interrupciones o incidentes. En el contexto gubernamental, la resiliencia es fundamental para garantizar la prestación ininterrumpida de servicios públicos y proteger los datos de los ciudadanos frente a fallas técnicas, ataques cibernéticos o desastres naturales (Ávila-Coello, 2024).

Esta monografía analiza la importancia de la resiliencia, los mecanismos para fortalecerla, su relación con la continuidad operativa y los desafíos que enfrentan las instituciones públicas en su implementación.

2. Concepto de Resiliencia de los Sistemas

La **resiliencia de los sistemas** se define como la capacidad de una infraestructura tecnológica para mantener su funcionamiento esencial, adaptarse a condiciones adversas y recuperarse rápidamente después de una interrupción (ISO 22301, 2022).

Según Guarneros (2022), la resiliencia no solo depende de la redundancia de hardware y software, sino también de la preparación del personal, los protocolos de respuesta y la planificación estratégica de la institución. En entornos gubernamentales, la resiliencia asegura que los servicios esenciales continúen operando ante cualquier eventualidad, minimizando impactos negativos en la ciudadanía.

3. Principios y Mecanismos

3.1 Principios básicos

Redundancia de sistemas: Implementación de componentes duplicados para garantizar la disponibilidad ante fallas.

Capacidad de adaptación: Ajuste de los sistemas y procesos según la naturaleza y magnitud del incidente.

Recuperación rápida: Minimización del tiempo de inactividad y restauración eficiente de los servicios críticos.

Evaluación y mejora continua: Revisión periódica de la resiliencia de los sistemas y actualización de estrategias ante nuevas amenazas.

3.2 Mecanismos y herramientas

Infraestructura redundante: Servidores, redes y bases de datos duplicadas para mantener la operación continua.

Automatización de procesos críticos: Sistemas que permiten recuperación y respuesta rápida sin intervención manual completa.

Protocolos de respuesta ante incidentes: Procedimientos claros que guían al personal ante fallas o ataques.

Simulaciones y pruebas de estrés: Evaluación de la capacidad de los sistemas para resistir y recuperarse de situaciones críticas (Collantes Collantes, 2025).

4. Importancia de la Resiliencia en el Ámbito Gubernamental

Garantiza la continuidad de servicios públicos: Permite que los ciudadanos accedan a servicios esenciales sin interrupciones prolongadas.

Minimiza impactos negativos: Reduce pérdidas de información, retrasos administrativos y daños en la infraestructura tecnológica.

Fortalece la confianza ciudadana: Los usuarios confían en instituciones que mantienen sus servicios operativos aun frente a incidentes.

Cumple con estándares de seguridad y continuidad: Contribuye al cumplimiento de normas internacionales y políticas de gobierno relacionadas con la gestión de riesgos (Torres Quevedo, 2023; Ávila-Coello, 2024).

5. Retos y Desafíos

- **Ataques cibernéticos avanzados:** Malware y ataques de denegación de servicio pueden comprometer la resiliencia si no hay sistemas preparados.
- **Limitaciones de recursos:** Implementar infraestructura redundante y automatización requiere inversión tecnológica y capacitación.
- **Integración de sistemas heterogéneos:** Mantener resiliencia en sistemas antiguos y modernos simultáneamente puede ser complejo.
- **Mantenimiento constante:** Los sistemas y protocolos deben actualizarse regularmente para asegurar efectividad frente a nuevas amenazas (Guarneros, 2022).

6. Conclusiones

La **resiliencia de los sistemas** es un elemento crítico para garantizar la continuidad operativa en instituciones públicas. A través de la redundancia, la capacidad de adaptación y la rápida recuperación, las organizaciones pueden minimizar interrupciones, proteger la información y mantener la prestación de servicios esenciales.

En síntesis, fortalecer la resiliencia de los sistemas no solo asegura la operación continua de los servicios gubernamentales, sino que también aumenta la confiabilidad, eficiencia y capacidad de respuesta de las instituciones frente a cualquier eventualidad, consolidando la confianza de la ciudadanía.

Autores Relevantes:

(Torres Quevedo, L. A., 2023): En su tesis sobre la gestión operativa del Gobierno Regional de Lima, aborda la importancia de implementar estrategias de continuidad operativa para mejorar la eficiencia en la prestación de servicios públicos.

(Collantes Collantes, R. A., 2025): Analiza las estrategias de gestión y su impacto en la eficiencia operativa del Gobierno Regional de Lima, destacando la necesidad de fortalecer la continuidad operativa en el sector público.

2.3. Bases filosóficas

1. Paradigma de Investigación

El presente estudio se enmarca dentro del paradigma positivista, ya que busca analizar la relación entre variables concretas y observables: la *seguridad informática* (variable independiente) y la *continuidad operativa* (variable dependiente). Este enfoque se centra en la recolección de datos cuantificables, el establecimiento de relaciones causales y el uso de métodos estadísticos para validar hipótesis, garantizando objetividad, precisión y replicabilidad en los resultados (Hernández, R., Fernández, C., & Baptista, P., 2014).

El paradigma positivista permite que la investigación adopte un enfoque cuantitativo, caracterizado por medición numérica de variables, análisis estadístico de datos y conclusiones basadas en evidencia empírica. Este enfoque es fundamental en el contexto gubernamental, donde las decisiones sobre seguridad y continuidad operativa deben sustentarse en resultados concretos y verificables.

2. Enfoque Filosófico Epistemológico

Desde la perspectiva epistemológica, la investigación se fundamenta en el conocimiento empírico-científico, que sostiene que la realidad puede ser observada, medida y comprendida a través de métodos sistemáticos. La seguridad informática y la continuidad operativa son fenómenos que, si bien implican procesos tecnológicos complejos, pueden evaluarse mediante indicadores objetivos como confidencialidad, integridad, disponibilidad, resiliencia y planes de recuperación (Kerlinger, F. N., & Lee, H. B., 2022).

Este enfoque epistemológico asegura que los hallazgos del estudio no dependan de interpretaciones subjetivas, sino de evidencia concreta que permita generar recomendaciones aplicables a la gestión del Gobierno Regional de Lima.

3. Fundamento Ontológico

Desde la ontología, se asume que la realidad organizacional y tecnológica es objetiva y estructurada. La infraestructura tecnológica, los sistemas de información, los protocolos de seguridad y los planes de continuidad existen de manera independiente de la percepción del investigador, pero son susceptibles de análisis y optimización (Guba, E. G., & Lincoln, Y. S., 1994).

Este enfoque ontológico justifica la evaluación sistemática de variables y dimensiones, permitiendo identificar problemas, medir riesgos y proponer estrategias para mejorar la seguridad y la continuidad operativa de los sistemas gubernamentales.

4. Base Axiológica

La investigación también posee una dimensión axiológica, ya que se rige por valores éticos y de responsabilidad social. En el ámbito de la administración pública, garantizar la seguridad de la información y la continuidad de los servicios no solo es una cuestión técnica, sino también ética, pues protege datos sensibles de los ciudadanos, asegura el funcionamiento eficiente de los servicios y contribuye a la confianza de la población en las instituciones (Torres Quevedo, 2023).

Los principios axiomáticos incluyen:

Transparencia: Publicar resultados y recomendaciones de manera clara y verificable.

Responsabilidad: Garantizar que las estrategias propuestas sean aplicables y beneficien al ciudadano.

Equidad y justicia: Asegurar que todos los usuarios tengan acceso continuo a servicios públicos críticos, sin discriminación.

Seguridad y confianza: Proteger la información y los sistemas de posibles vulneraciones que comprometan a la ciudadanía.

5. Fundamentación Lógica y Racional

El estudio se sustenta en una base lógica y racional, dado que busca relaciones causales verificables entre la seguridad informática y la continuidad operativa. La investigación emplea un diseño correlacional para determinar cómo los niveles de seguridad informática influyen en la capacidad de los sistemas de mantener operaciones críticas sin interrupciones.

El razonamiento lógico permite identificar patrones, evaluar riesgos y generar estrategias de mejora basadas en evidencia cuantitativa, lo que fortalece la validez de las conclusiones y garantiza su aplicabilidad en la administración pública.

6. Relevancia Filosófica

Desde un punto de vista filosófico, la investigación contribuye al desarrollo del conocimiento aplicado, al vincular la teoría de la seguridad informática con la práctica de la continuidad operativa. Además, promueve una cultura organizacional orientada a la prevención, resiliencia y eficiencia, principios esenciales para la modernización de la gestión pública y la protección de los derechos de los ciudadanos en un entorno digitalizado.

2.4. Definición de términos básicos

Seguridad Informática:

Es el conjunto de medidas para proteger los sistemas de información.

Busca evitar accesos no autorizados, pérdidas o alteraciones de datos.

Garantiza que la información del gobierno y de los ciudadanos se mantenga segura.

Continuidad Operativa:

Es la capacidad de mantener los servicios del gobierno funcionando durante emergencias o fallos.

Incluye planes para restaurar sistemas, datos y operaciones rápidamente.

Garantiza que los servicios públicos no se interrumpan y que los procesos esenciales sigan operativos.

- **Confidencialidad de la información:** Protege los datos frente a accesos no autorizados, asegurando que solo las personas autorizadas puedan verlos.
- **Integridad de los sistemas:** Garantiza que la información y los procesos no sean modificados de manera indebida.
- **Disponibilidad de los sistemas:** Asegura que los sistemas y servicios estén operativos cuando se necesiten.
- **Gestión de riesgos y políticas de seguridad:** Incluye normas, protocolos y análisis de riesgos para prevenir incidentes y proteger los sistemas.
- **Planes de continuidad del negocio:** Estrategias y procedimientos que permiten mantener operaciones críticas ante emergencias.
- **Recuperación ante desastres (Disaster Recovery):** Capacidad de restaurar sistemas, datos y operaciones rápidamente después de un fallo o ataque.
- **Resiliencia de los sistemas:** Habilidad de adaptarse y recuperarse rápidamente de interrupciones, garantizando la estabilidad de los servicios.
- **Monitoreo y mantenimiento de operaciones críticas:** Supervisión constante y mantenimiento de los procesos esenciales para asegurar su funcionamiento continuo.

2.5. Hipótesis de investigación

2.5.1. Hipótesis general

Seguridad informática tiene una relación positiva en Continuidad operativa de los trabajadores del Gobierno Regional de Lima, 2025.

2.5.2. Hipótesis específicas

a. Seguridad informática tiene una relación positiva en Planes de continuidad del negocio de los trabajadores del Gobierno Regional de Lima, 2025.

b. Seguridad informática tiene una relación positiva en Recuperación ante desastres (Disaster Recovery) de los trabajadores del Gobierno Regional de Lima, 2025.

c. Seguridad informática tiene una relación positiva en Resiliencia de los sistemas de los trabajadores del Gobierno Regional de Lima, 2025.

d. Seguridad informática tiene una relación positiva en Monitoreo y mantenimiento de operaciones críticas de los trabajadores del Gobierno Regional de Lima, 2025.

2.6. Operacionalización de Variable e Indicadores

Tabla 1. Seguridad informática

Dimensiones	Indicadores	Ítems	Nivel/Rango
Confidencialidad de la información	- Control de accesos a los sistemas. - Uso de contraseñas seguras y autenticación. - Protección de datos sensibles.	1,2,3	
Integridad de los sistemas	- Prevención de modificaciones no autorizadas. - Registro de cambios en la información. - Validación de datos antes de su uso.	4,5,6	Nunca (1)
Disponibilidad de los sistemas	- Funcionamiento continuo de los sistemas críticos. - Minimización de tiempos de inactividad. - Acceso oportuno a la información.	7,8,9	Casi nunca (2) A veces (3) Casi siempre (4)
Gestión de riesgos y políticas de seguridad	- Existencia de políticas de seguridad formalizadas. - Evaluación periódica de riesgos informáticos. - Capacitación del personal en seguridad.	10,11,12	Siempre (5)

Tabla 2. Continuidad operativa

Dimensiones	Indicadores	Ítems	Nivel/Rango
Planes de continuidad del negocio	- Documentación de procedimientos de emergencia. - Identificación de procesos críticos. - Actualización periódica de los planes.	13,14,15	
Recuperación ante desastres	- Disponibilidad de respaldos de información. - Pruebas periódicas de recuperación. - Tiempo de recuperación ante fallas.	16,17,18	Nunca (1) Casi nunca (2)
Resiliencia de los sistemas	- Capacidad de adaptación ante incidentes. - Redundancia de sistemas críticos. - Respuesta rápida a interrupciones.	19,20,21	A veces (3) Casi siempre (4)
Monitoreo y mantenimiento de operaciones críticas	- Supervisión constante de sistemas esenciales. - Mantenimiento preventivo de equipos. - Detección temprana de fallas.	22,23,24	Siempre (5)

III. CAPITULO III: METODOLOGIA DE LA INVESTIGACION

3.1. Diseño metodológico

1. Enfoque de investigación

El presente estudio adopta un enfoque cuantitativo, ya que busca medir la relación entre la Seguridad Informática (variable independiente) y la Continuidad Operativa (variable dependiente) en los sistemas de gestión del Gobierno Regional de Lima a través de datos numéricos y análisis estadísticos. Según Hernández, Fernández y Baptista (2014), el enfoque cuantitativo permite obtener resultados objetivos, confiables y generalizables mediante el uso de instrumentos estructurados como encuestas o cuestionarios.

2. Tipo de investigación

La investigación es de tipo aplicada, puesto que busca aportar soluciones prácticas para mejorar la seguridad informática y la continuidad operativa en los sistemas de gestión del Gobierno Regional de Lima, optimizando la protección de la información y la prestación de servicios a los ciudadanos.

3. Nivel de investigación

El nivel de la investigación es correlacional, dado que pretende determinar la relación existente entre los niveles de seguridad informática implementados y la efectividad de la continuidad operativa en los sistemas gubernamentales.

4. Diseño de investigación

El diseño de investigación es no experimental y transversal.

3.2. Población y muestra

3.2.1. Población

La población de la investigación está conformada por 460 trabajadores del Gobierno Regional de Lima, 2025.

3.2.2. Muestra

Lo cual nuestra muestra sería de 210 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 la Continuidad Operativa 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.

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 la efectividad de la continuidad operativa 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 la continuidad operativa en los sistemas de gestión.

Análisis de Correlación de Spearman: Para determinar la relación entre la Seguridad Informática y la Continuidad Operativa, 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 la continuidad operativa 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

4.1.1. Resultados de Seguridad Informática y sus dimensiones

Tabla 1 Niveles de Seguridad Informática

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BAJO	36	17,1	17,1	17,1
	MEDIO	70	33,3	33,3	50,5
	ALTO	104	49,5	49,5	100,0
	Total	210	100,0	100,0	

Fuente: Registros de Seguridad Informática que se desarrolló a trabajadores del

Gobierno Regional de Lima, 2025.

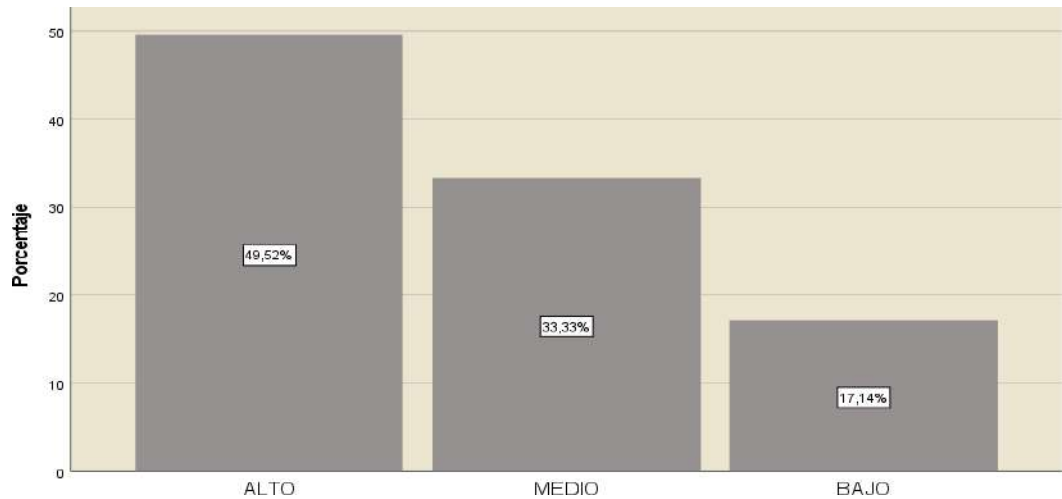


Figura 1 Niveles de Seguridad Informática

En la fig. 1 el 33,33% trabajadores del Gobierno Regional de Lima, 2025, llegaron a un nivel medio de Seguridad Informática, el 49,52% logro el nivel alto, finalmente un 17,14% mostro un nivel bajo para Seguridad Informática.

Tabla 2 Niveles de Confidencialidad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BAJO	36	17,1	17,1	17,1
	MEDIO	94	44,8	44,8	61,9
	ALTO	80	38,1	38,1	100,0
	Total	210	100,0	100,0	

Fuente: Registros de Confidencialidad de la información que se desarrolló a trabajadores del Gobierno Regional de Lima, 2025.

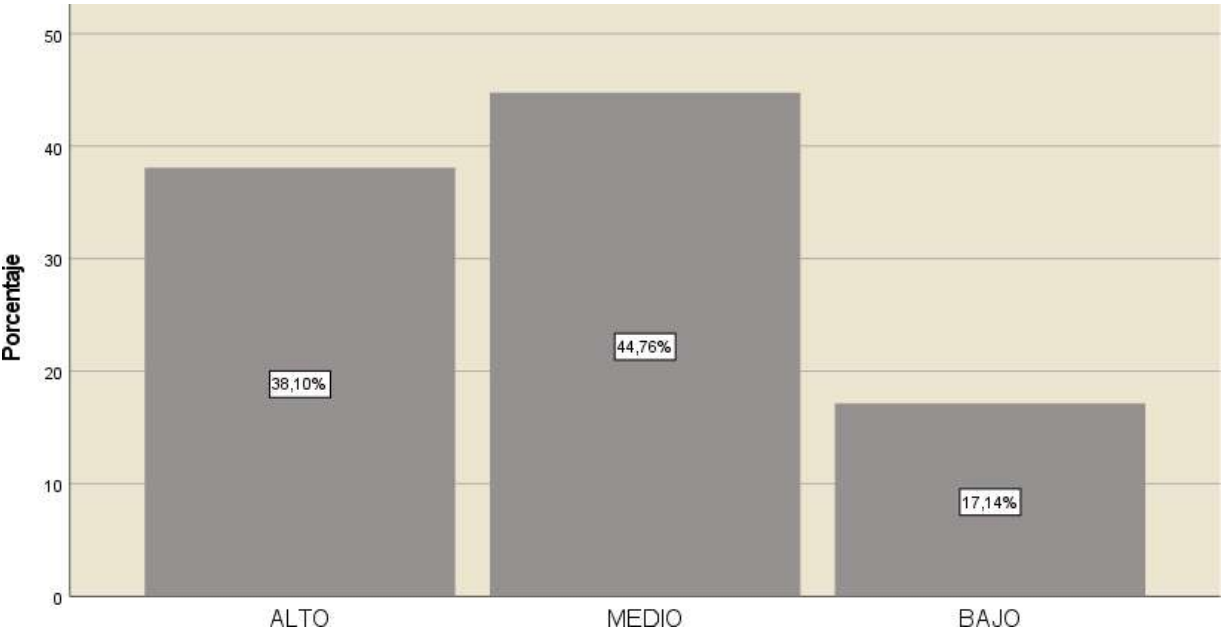


Figura 2 Niveles de Confidencialidad de la información

En la fig. 2 el 44,76% de trabajadores del Gobierno Regional de Lima, 2025, llegaron a un nivel medio de Confidencialidad de la información, el 38,10% logro el nivel alto, finalmente un 17,14% mostro un nivel bajo para Confidencialidad de la información.

Tabla 3 Niveles de Integridad de los sistemas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BAJO	32	15,2	15,2	15,2
	MEDIO	35	16,7	16,7	31,9
	ALTO	143	68,1	68,1	100,0
	Total	210	100,0	100,0	

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

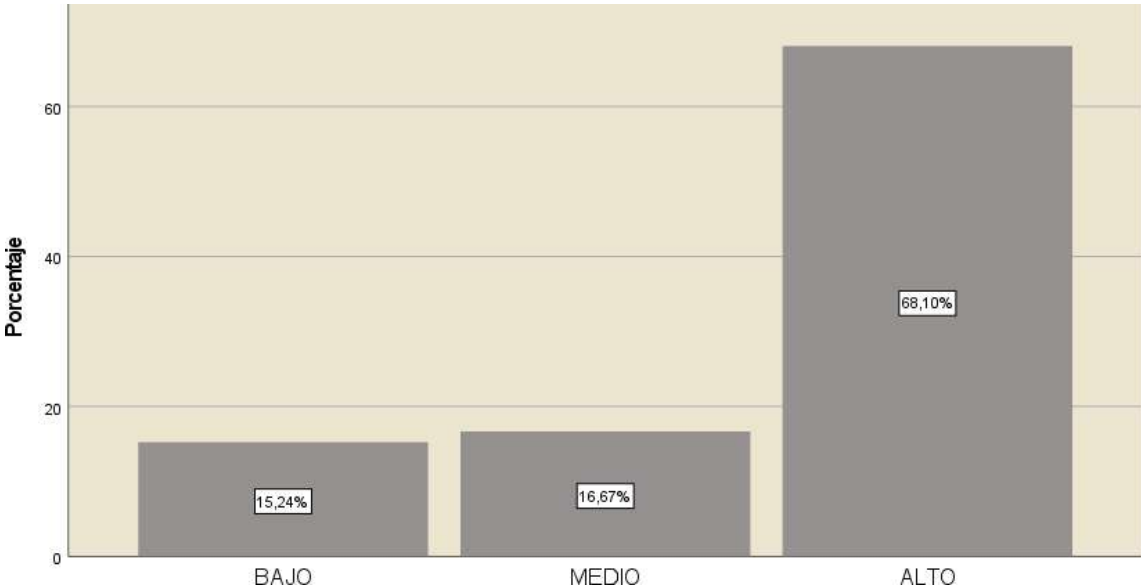


Figura 3 Niveles de Integridad de los sistemas

En la fig. 3 el 16,67% de trabajadores del Gobierno Regional de Lima, 2025, llegaron a un nivel medio de Integridad de los sistemas, el 68,10% logro el nivel alto, finalmente un 15,24% mostro un nivel bajo para Integridad de los sistemas.

Tabla 4 Niveles de Disponibilidad de los sistemas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BAJO	25	11,9	11,9	11,9
	MEDIO	116	55,2	55,2	67,1
	ALTO	69	32,9	32,9	100,0
	Total	210	100,0	100,0	

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

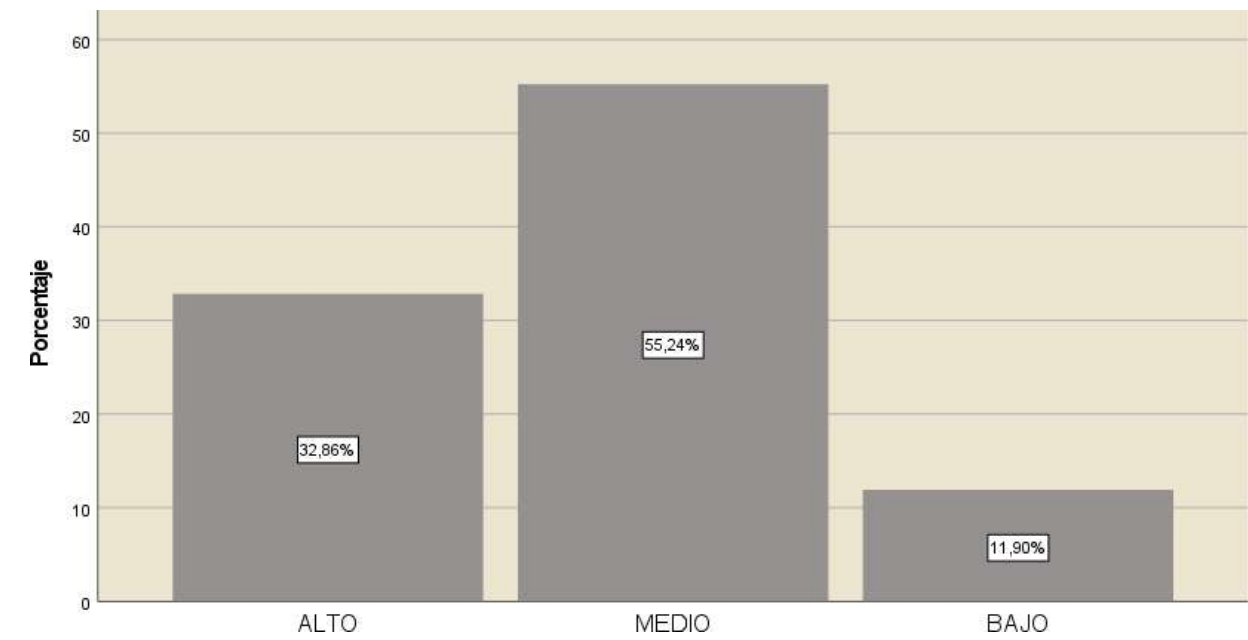


Figura 4 Niveles de Disponibilidad de los sistemas

En la fig. 4 el 55,24% de trabajadores del Gobierno Regional de Lima, 2025, llegaron a un nivel medio de Disponibilidad de los sistemas, el 32,86% logro el nivel alto, finalmente un 11,90% mostro un nivel bajo para Disponibilidad de los sistemas.

Tabla 5 Niveles de Gestión de riesgos y políticas de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BAJO	39	18,6	18,6	18,6
	MEDIO	73	34,8	34,8	53,3
	ALTO	98	46,7	46,7	100,0
	Total	210	100,0	100,0	

Fuente: Registros de Gestión de riesgos y políticas de seguridad que se desarrolló a trabajadores del Gobierno Regional de Lima, 2025.

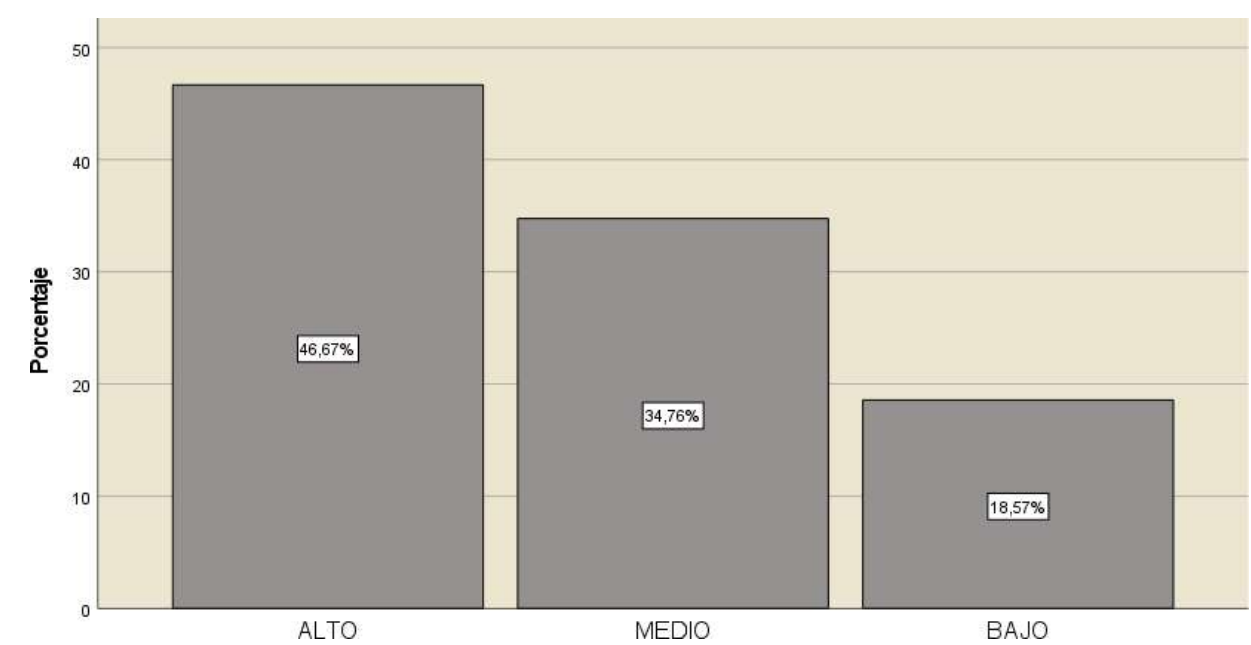


Figura 5 Niveles de Gestión de riesgos y políticas de seguridad

En la fig. 5 el 34,76% de trabajadores del Gobierno Regional de Lima, 2025, llegaron a un nivel medio de Gestión de riesgos y políticas de seguridad, el 46,67% logro el nivel alto, finalmente un 18,57% mostro un nivel bajo para Gestión de riesgos y políticas de seguridad.

4.1.2. Resultados de Continuidad operativa y sus dimensiones

Tabla 6 Niveles de Continuidad operativa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BAJO	23	11,0	11,0	11,0
	MEDIO	81	38,6	38,6	49,5
	ALTO	106	50,5	50,5	100,0
	Total	210	100,0	100,0	

Fuente: Registros de Continuidad operativa que se desarrolló a trabajadores del

Gobierno Regional de Lima, 2025.

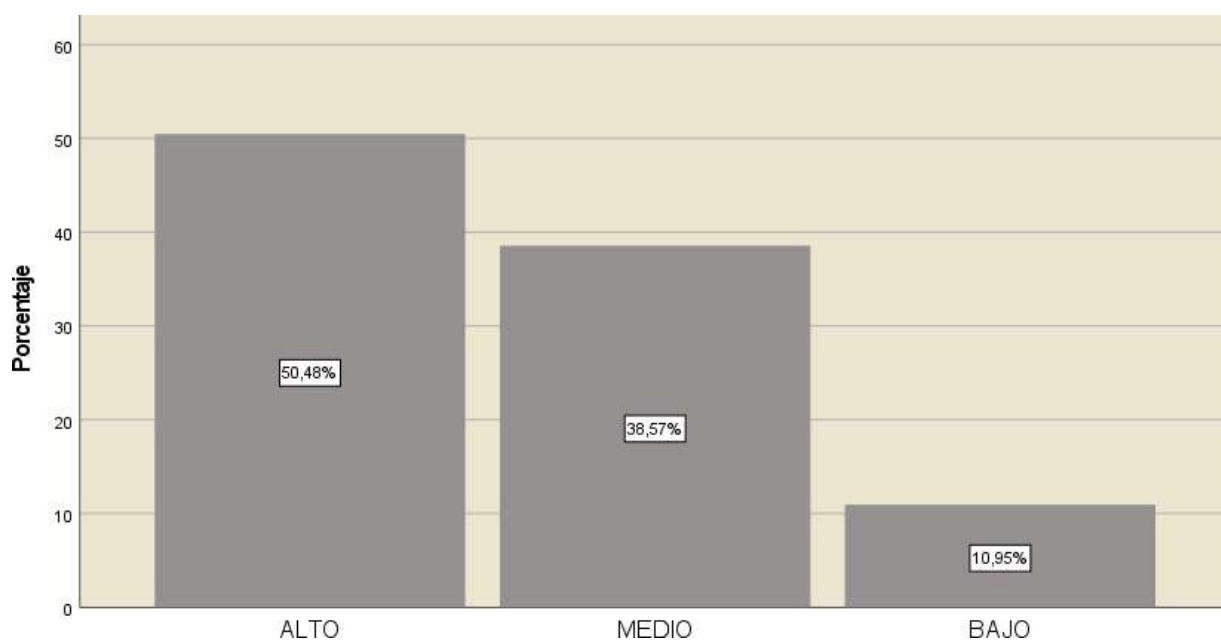


Figura 6 Niveles de Continuidad operativa

En la fig. 6 el 38,57% de trabajadores del Gobierno Regional de Lima, 2025, llegaron a un nivel medio de Continuidad operativa, el 50,48% logro el nivel alto, finalmente un 10,95% mostro un nivel bajo para Continuidad operativa.

Tabla 7 Niveles de Planes de continuidad del negocio

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BAJO	35	16,7	16,7	16,7
	MEDIO	25	11,9	11,9	28,6
	ALTO	150	71,4	71,4	100,0
	Total	210	100,0	100,0	

Fuente: Registros de Planes de continuidad del negocio que se desarrolló a trabajadores del Gobierno Regional de Lima, 2025.

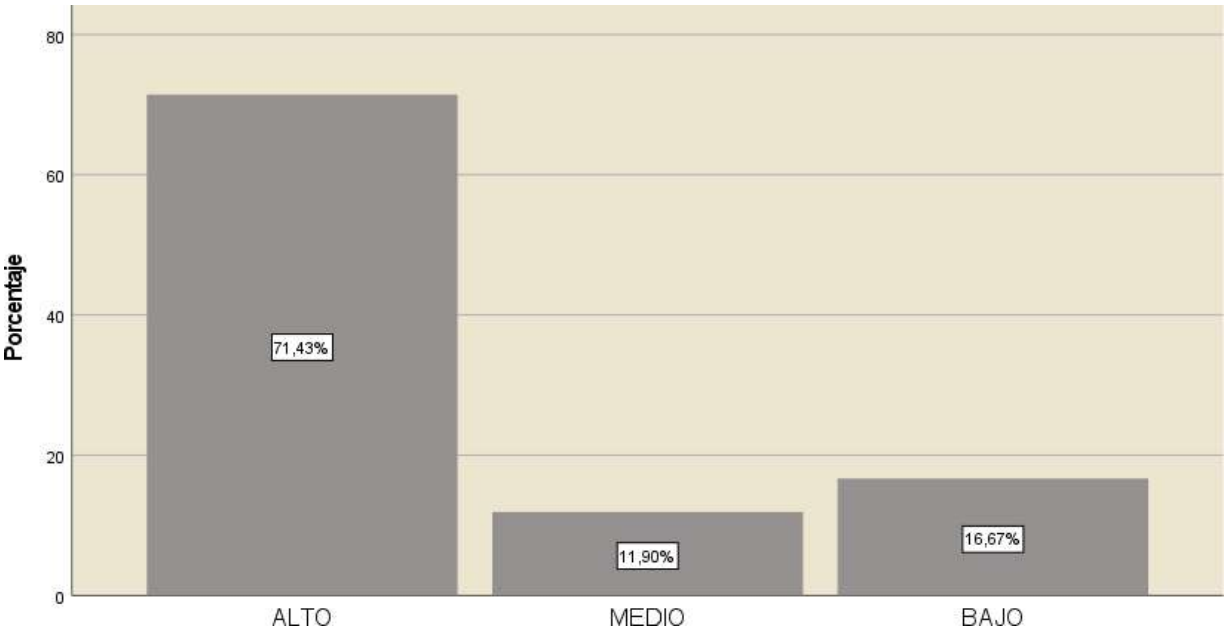


Figura 7 Niveles de Planes de continuidad del negocio

En la fig. 7 el 11,90% de trabajadores del Gobierno Regional de Lima, 2025, llegaron a un nivel medio de Planes de continuidad del negocio, el 71,43% logro el nivel alto, finalmente un 16,67% mostro un nivel bajo para Planes de continuidad del negocio.

Tabla 8 Niveles de Recuperación ante desastres

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BAJO	26	12,4	12,4	12,4
	MEDIO	38	18,1	18,1	30,5
	ALTO	146	69,5	69,5	100,0
	Total	210	100,0	100,0	

Fuente: Registros de Recuperación ante desastres que se desarrolló a trabajadores del Gobierno Regional de Lima, 2025.

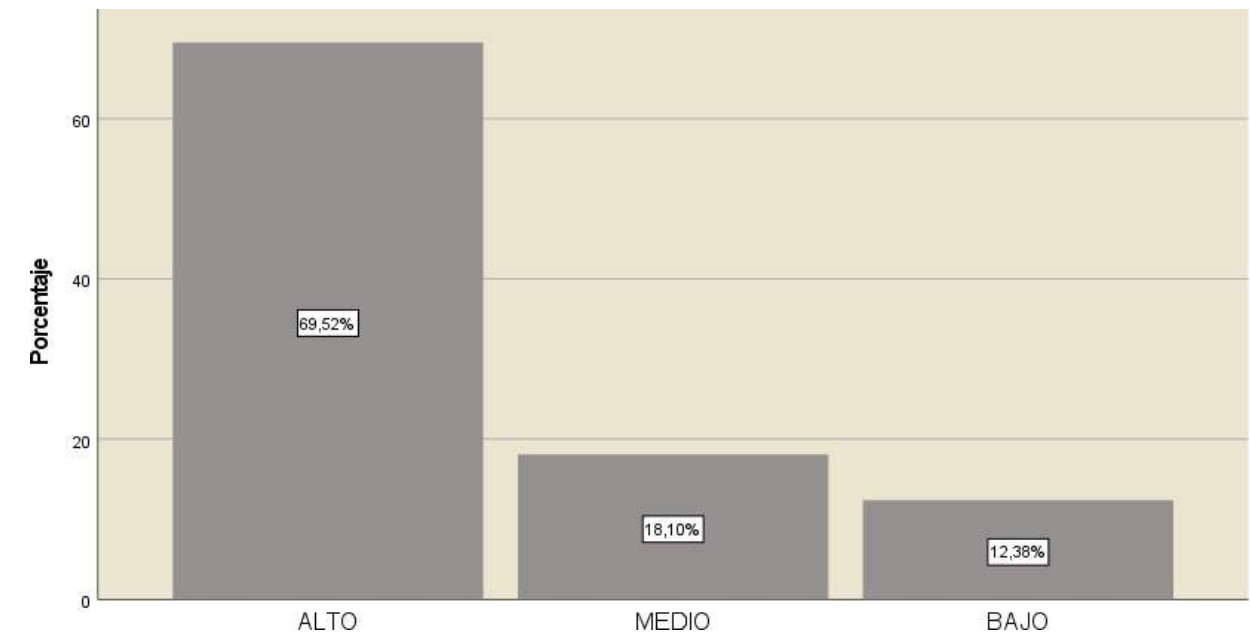


Figura 8 Niveles de Recuperación ante desastres

En la fig. 8 el 18,10% de trabajadores del Gobierno Regional de Lima, 2025, llegaron a un nivel medio de Recuperación ante desastres, el 69,52% logro el nivel alto, finalmente un 12,38% mostro un nivel bajo para Recuperación ante desastres.

Tabla 9 Niveles de Resiliencia de los sistemas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BAJO	38	18,1	18,1	18,1
	MEDIO	85	40,5	40,5	58,6
	ALTO	87	41,4	41,4	100,0
	Total	210	100,0	100,0	

Fuente: Registros de Resiliencia de los sistemas que se desarrolló a trabajadores del Gobierno Regional de Lima, 2025.

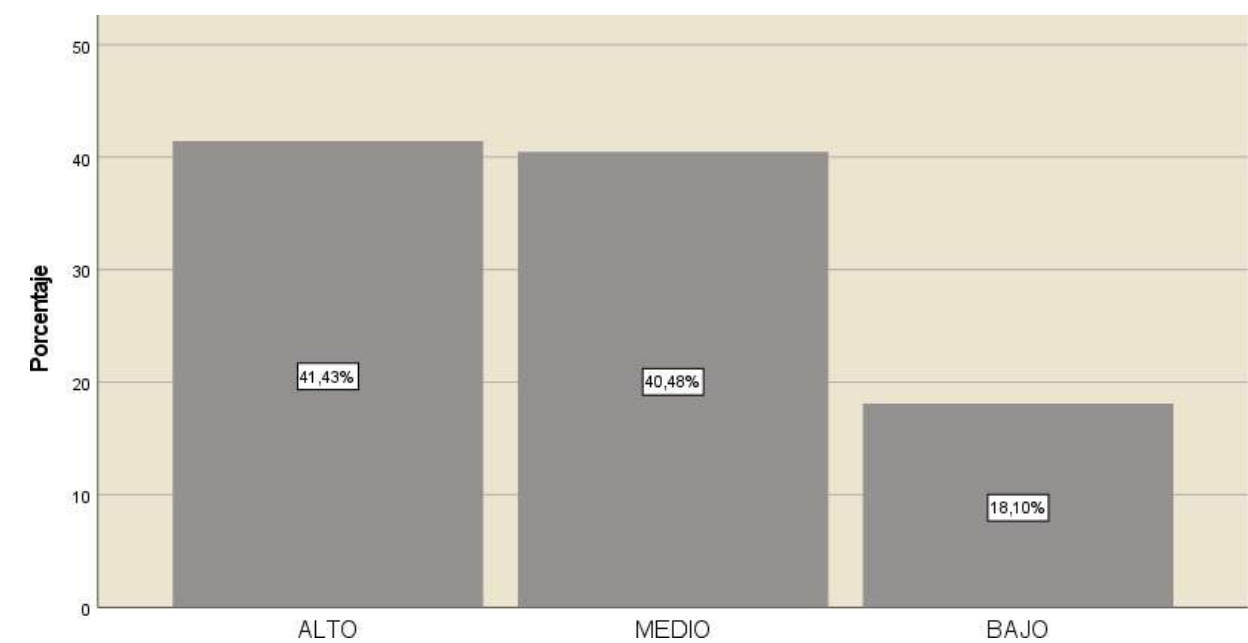


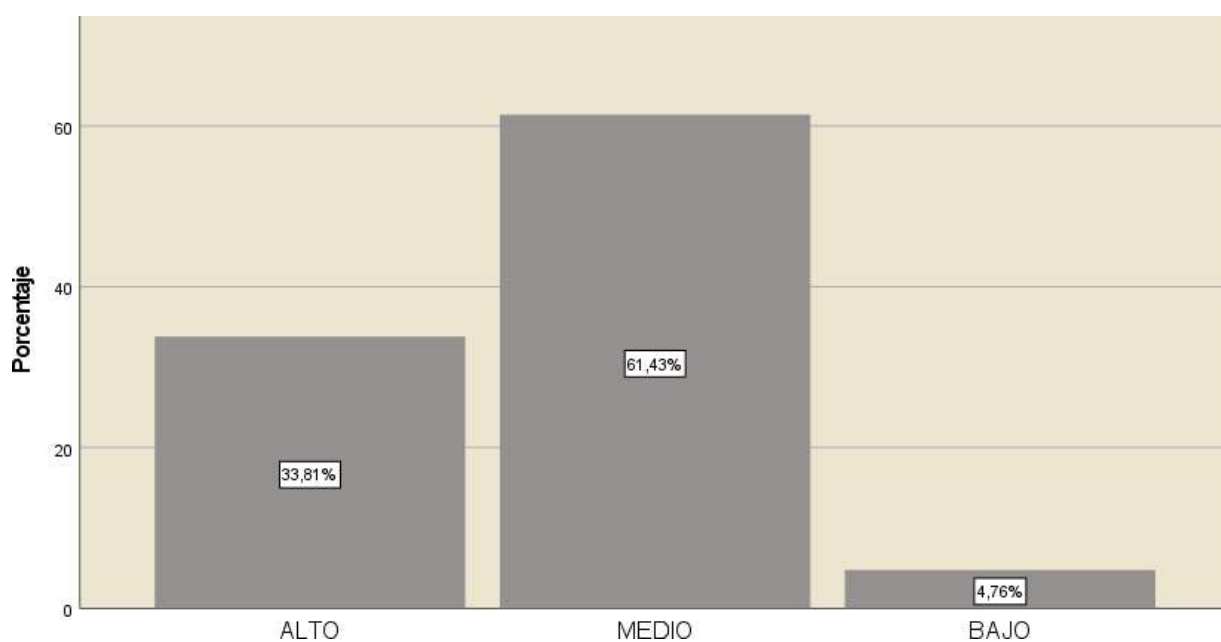
Figura 9 Niveles de Resiliencia de los sistemas

En la fig. 9 el 40,48% de trabajadores del Gobierno Regional de Lima, 2025, llegaron a un nivel medio de Resiliencia de los sistemas, el 41,43% logro el nivel alto, finalmente un 18,10% mostro un nivel bajo para Resiliencia de los sistemas.

Tabla 10 Niveles de Monitoreo y mantenimiento de operaciones críticas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BAJO	10	4,8	4,8	4,8
	MEDIO	129	61,4	61,4	66,2
	ALTO	71	33,8	33,8	100,0
	Total	210	100,0	100,0	

Fuente: Registros de Monitoreo y mantenimiento de operaciones críticas que se desarrolló a trabajadores del Gobierno Regional de Lima, 2025.

**Figura 10 Niveles de Monitoreo y mantenimiento de operaciones críticas**

En la fig. 10 el 61,43% trabajadores del Gobierno Regional de Lima, 2025, llegaron a un nivel medio de Monitoreo y mantenimiento de operaciones críticas, el 33,81% logro el nivel alto, finalmente un 4,76% mostro un nivel bajo para Monitoreo y mantenimiento de operaciones críticas.

4.2. Contrastación de Hipótesis

4.2.1. Contrastación de Hipótesis General

a) Hipótesis General Nula.

Seguridad Informática no se relaciona con Continuidad operativa de los trabajadores del Gobierno Regional de Lima, 2025.

b) Hipótesis General Alternativa.

Seguridad Informática se relaciona con Continuidad operativa de los trabajadores del Gobierno Regional de Lima, 2025.

Correlaciones: Seguridad Informática y Continuidad operativa

		Seguridad Informática	Continuidad operativa
Seguridad Informática	Correlación de Spearman	1	,528
	Sig. (bilateral)		,010
	N	210	210
Continuidad operativa	Correlación de Spearman	,528	1
	Sig. (bilateral)	,570	
	N	210	210

INTERPRETACION

El coeficiente de Spearman de **0.528** y una significancia de **0.010** muestran una **relación positiva moderada y significativa** entre la **seguridad informática** y la **continuidad operativa**, lo que implica que mejorar la seguridad favorece la estabilidad y funcionamiento constante de las operaciones.

4.2.2. *Contrastación de Hipótesis Específica 1*

a) Hipótesis General Nula.

Seguridad Informática no se relaciona con Planes de continuidad del negocio de los trabajadores del Gobierno Regional de Lima, 2025.

b) Hipótesis General Alternativa.

Seguridad Informática se relaciona con Planes de continuidad del negocio de los trabajadores del Gobierno Regional de Lima, 2025.

Correlaciones:

		Seguridad Informática	Planes de continuidad del negocio
Seguridad Informática	Correlación de Spearman	1	,686
	Sig. (bilateral)		,003
	N	210	210
Planes de continuidad del negocio	Correlación de Spearman	,686	1
	Sig. (bilateral)	,003	
	N	210	210

INTERPRETACION

El coeficiente de Spearman de **0.686** con una significancia de **0.003** revela una **correlación positiva moderada y significativa** entre la **seguridad informática** y los **planes de continuidad del negocio**. Esto indica que un mayor nivel de seguridad informática contribuye al fortalecimiento y eficacia de los planes destinados a mantener las operaciones durante situaciones adversas.

4.2.3. *Contrastación de Hipótesis Específica 2*

a) Hipótesis General Nula.

Seguridad Informática no se relaciona con Recuperación ante desastres de los trabajadores del Gobierno Regional de Lima, 2025.

b) Hipótesis General Alternativa.

Seguridad Informática se relaciona con Recuperación ante desastres de los trabajadores del Gobierno Regional de Lima, 2025.

Correlaciones:

		Seguridad Informática	Recuperación ante desastres
Seguridad Informática	Correlación de Spearman	1	,661
	Sig. (bilateral)		,001
	N	210	210
Recuperación ante desastres	Correlación de Spearman	,661	1
	Sig. (bilateral)	,001	
	N	210	210

INTERPRETACION

El coeficiente de Spearman de **0.661** con una significancia de **0.001** evidencia una **correlación positiva moderada y estadísticamente significativa** entre la **seguridad informática** y la **recuperación ante desastres**. Esto significa que al mejorar las prácticas de seguridad informática, aumenta la capacidad de la organización para recuperarse eficazmente frente a incidentes o desastres.

4.2.4. *Contrastación de Hipótesis Específica 3*

a) Hipótesis General Nula.

Seguridad Informática no se relaciona con Resiliencia de los sistemas de los trabajadores del Gobierno Regional de Lima, 2025.

b) Hipótesis General Alternativa.

Seguridad Informática se relaciona con Resiliencia de los sistemas de los trabajadores del Gobierno Regional de Lima, 2025.

Correlaciones:

		Seguridad Informática	Resiliencia de los sistemas
Seguridad Informática	Correlación de Spearman	1	,704
	Sig. (bilateral)		,002
	N	210	210
Resiliencia de los sistemas	Correlación de Spearman	,704	1
	Sig. (bilateral)	,002	
	N	210	210

INTERPRETACION

El coeficiente de Spearman de **0.704** con una significancia de **0.002** muestra una **correlación positiva moderadamente alta y significativa** entre la **seguridad informática** y la **resiliencia de los sistemas**. Esto indica que cuando se fortalecen las medidas de seguridad informática, los sistemas tienden a ser más resilientes ante fallos o ataques.

4.2.5. *Contrastación de Hipótesis Específica 4*

a) Hipótesis General Nula.

Seguridad Informática no se relaciona con Monitoreo y mantenimiento de operaciones críticas de los trabajadores del Gobierno Regional de Lima, 2025.

b) Hipótesis General Alternativa.

Seguridad Informática se relaciona con Monitoreo y mantenimiento de operaciones críticas de los trabajadores del Gobierno Regional de Lima, 2025.

Correlaciones:

		Seguridad Informática	Monitoreo y mantenimiento de operaciones críticas
Seguridad Informática	Correlación de Spearman	1	,826
	Sig. (bilateral)		,001
	N	210	210
Monitoreo y mantenimiento de operaciones críticas	Correlación de Spearman	,826	1
	Sig. (bilateral)	,001	
	N	210	210

INTERPRETACION

El coeficiente de Spearman de **0.826** con una significancia de **0.001** indica una **relación positiva alta y significativa** entre la **seguridad informática** y el **monitoreo y mantenimiento de operaciones críticas**. Esto significa que, al mejorar la seguridad informática, también se fortalecen las operaciones críticas, evidenciando una conexión real y no casual entre ambas variables.

V. CAPITULO V: DISCUSIÓN

5.1. Discusión de Resultados

Los resultados obtenidos en la presente investigación demuestran que existe una relación significativa entre la **seguridad informática** y la **continuidad operativa** en los trabajadores del Gobierno Regional de Lima, año 2025. En términos generales, el análisis de correlación de Spearman reveló un coeficiente de **0.528** con una significancia de **0.010**, lo cual indica una **correlación positiva moderada y estadísticamente significativa**. Este hallazgo sugiere que a medida que se fortalecen las medidas de seguridad informática dentro de la institución, la capacidad de mantener las operaciones de forma continua y estable también mejora. En consecuencia, se puede afirmar que la seguridad informática no solo protege los datos y sistemas, sino que también se convierte en un factor clave para garantizar la operatividad institucional ante posibles interrupciones.

Estos resultados coinciden con estudios previos en el ámbito de la gestión tecnológica, los cuales sostienen que la implementación de políticas de seguridad digital eficaces contribuye directamente a la **sostenibilidad operativa** de las organizaciones públicas y privadas. En el caso específico del Gobierno Regional de Lima, este vínculo refuerza la importancia de adoptar protocolos sólidos de ciberseguridad, capacitación del personal y mantenimiento preventivo de los sistemas informáticos, factores que en conjunto aseguran la continuidad de los procesos institucionales y reducen los riesgos de paralización frente a incidentes tecnológicos o cibernéticos.

Asimismo, la primera hipótesis específica, que evalúa la relación entre la **seguridad informática** y los **planes de continuidad del negocio**, arrojó un coeficiente de **0.686** y una

significancia de **0.003**, lo que evidencia una **correlación positiva moderada y significativa**.

Este resultado pone en manifiesto que el fortalecimiento de la seguridad informática incide de manera directa en la eficacia de los planes diseñados para mantener las operaciones ante contingencias. La existencia de políticas de respaldo, sistemas redundantes y procedimientos claros para enfrentar crisis tecnológicas o desastres digitales permiten que la organización responda con rapidez, minimizando pérdidas y manteniendo la confianza de los usuarios internos y externos.

En relación con la segunda hipótesis específica, correspondiente a la **recuperación ante desastres**, el coeficiente de **0.661** con una significancia de **0.001** confirma una **relación positiva moderada y significativa**. Este resultado refuerza la idea de que la seguridad informática juega un papel esencial en la **capacidad de respuesta post-incidente**, ya que las medidas de protección, respaldo de información y protocolos de restauración aseguran una recuperación eficiente del sistema tras una falla o ataque. En el contexto del Gobierno Regional, esto se traduce en una gestión más resiliente ante eventos que puedan comprometer la integridad o disponibilidad de la información institucional.

Por su parte, la tercera hipótesis específica, que analiza la **resiliencia de los sistemas**, presentó un coeficiente de **0.704** y una significancia de **0.002**, demostrando una **correlación positiva moderadamente alta y significativa**. Este hallazgo indica que los sistemas informáticos de la entidad son más resistentes y capaces de adaptarse ante fallos o ciberataques en la medida en que se implementan mecanismos de seguridad adecuados. La resiliencia tecnológica no solo depende del hardware o software, sino también de la cultura de seguridad instaurada en la organización, el monitoreo constante y la actualización continua de las medidas de protección frente a nuevas amenazas digitales.

Finalmente, la cuarta hipótesis específica, correspondiente al **monitoreo y mantenimiento de operaciones críticas**, mostró el coeficiente más alto, **0.826**, con una significancia de **0.001**, lo que refleja una **relación positiva alta y significativa**. Este resultado evidencia que el monitoreo constante, el mantenimiento preventivo y la supervisión de procesos esenciales se ven ampliamente fortalecidos cuando existe una adecuada gestión de seguridad informática. Esto sugiere que la institución puede anticiparse a fallas o incidentes mediante un control permanente de los sistemas, asegurando la operatividad continua de los servicios críticos que brinda a la población.

En conjunto, los resultados confirman que la **seguridad informática es un elemento determinante para la continuidad y estabilidad operativa** del Gobierno Regional de Lima. Cada una de las dimensiones evaluadas planes de continuidad del negocio, recuperación ante desastres, resiliencia de los sistemas y monitoreo de operaciones críticas mantiene una correlación significativa con la variable principal, lo que demuestra que la seguridad tecnológica no debe ser considerada un aspecto secundario, sino un pilar fundamental de la gestión pública moderna.

En términos prácticos, estos hallazgos sugieren que fortalecer las políticas de seguridad informática contribuye no solo a proteger la información, sino también a **optimizar la eficiencia institucional**, garantizar la **prestación ininterrumpida de servicios** y aumentar la **confianza de los ciudadanos** en la administración pública. Asimismo, los resultados respaldan la necesidad de invertir en capacitación del personal, infraestructura tecnológica y estrategias de prevención, con el fin de consolidar una cultura organizacional orientada a la seguridad, la resiliencia y la mejora continua en los procesos tecnológicos del Gobierno Regional de Lima.

VI. CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

- Los resultados obtenidos confirman que existe una **relación positiva moderada y significativa entre la seguridad informática y la continuidad operativa** de los trabajadores del Gobierno Regional de Lima, 2025. Esto demuestra que el fortalecimiento de las medidas de seguridad informática contribuye directamente a garantizar la estabilidad y funcionamiento constante de las operaciones institucionales.
- Se determinó que la **seguridad informática influye de manera significativa en los planes de continuidad del negocio**, evidenciado por un coeficiente de correlación de 0.686 y un valor p de 0.003. Esto indica que la implementación de protocolos y estrategias de seguridad adecuados permite mantener la operatividad de los servicios frente a contingencias o interrupciones.
- La investigación también evidenció que existe una **relación positiva moderada entre la seguridad informática y la recuperación ante desastres**, con un coeficiente de 0.661 y una significancia de 0.001. Esto resalta la importancia de contar con sistemas de respaldo y procedimientos claros que aseguren una recuperación rápida y eficiente ante incidentes tecnológicos.
- En cuanto a la **resiliencia de los sistemas**, se observó una correlación de 0.704 con una significancia de 0.002, lo que demuestra que el fortalecimiento de la seguridad informática incrementa la capacidad de los sistemas para resistir, adaptarse y recuperarse ante posibles ataques o fallos, asegurando así la continuidad de los procesos institucionales.

- La dimensión con mayor nivel de relación fue el **monitoreo y mantenimiento de operaciones críticas**, con un coeficiente de 0.826 y una significancia de 0.001. Este resultado evidencia que una adecuada gestión de la seguridad informática favorece la supervisión constante y el mantenimiento oportuno de los sistemas, previniendo fallas que puedan afectar las operaciones esenciales del Gobierno Regional.

- En síntesis, se concluye que la **seguridad informática es un componente estratégico para la gestión pública**, ya que permite proteger la información, mantener la continuidad de los servicios y fortalecer la confianza institucional. Su adecuada implementación garantiza la eficiencia operativa, la prevención de incidentes y la sostenibilidad tecnológica en el tiempo.

6.2. Recomendaciones

- **Fortalecer las políticas institucionales de seguridad informática** en el Gobierno Regional de Lima mediante la implementación de normas, protocolos y procedimientos actualizados que garanticen la protección integral de la información, asegurando la continuidad operativa frente a eventuales amenazas o incidentes tecnológicos.
- **Diseñar y actualizar los planes de continuidad del negocio** considerando distintos escenarios de riesgo, como fallas en los sistemas, ataques cibernéticos o desastres naturales. Estos planes deben incluir estrategias de respaldo de datos, comunicación de crisis y procedimientos de recuperación que aseguren la operatividad de los servicios públicos sin interrupciones prolongadas.
- **Fortalecer las estrategias de recuperación ante desastres** mediante la creación de copias de seguridad periódicas, la implementación de servidores alternos y la evaluación constante de los tiempos de respuesta ante emergencias. De esta manera, se garantiza la rápida restauración de la información y la reanudación eficiente de las actividades institucionales.
- **Promover la resiliencia tecnológica de los sistemas informáticos**, asegurando su mantenimiento continuo, la actualización de software y la detección temprana de vulnerabilidades. Se recomienda además la integración de soluciones tecnológicas que permitan a la institución adaptarse de manera ágil frente a nuevas amenazas digitales.
- **Implementar programas permanentes de monitoreo y mantenimiento de operaciones críticas**, a fin de supervisar el rendimiento de los sistemas y prevenir posibles fallos. Este proceso debe estar acompañado de la capacitación del personal técnico y de la asignación de recursos suficientes para la gestión eficiente de la infraestructura tecnológica.

- **Capacitar de forma continua al personal administrativo y técnico** en temas de seguridad informática, buenas prácticas digitales, manejo responsable de la información y respuesta ante incidentes. La formación constante contribuye a crear una cultura organizacional orientada a la prevención y protección de los activos digitales.

- Finalmente, se recomienda que el **Gobierno Regional de Lima adopte un enfoque estratégico en la gestión de la seguridad informática**, integrándola como parte esencial de la planificación institucional. Esto permitirá no solo garantizar la protección de la información, sino también mejorar la eficiencia, la confianza ciudadana y la sostenibilidad tecnológica en el largo plazo.

VII. REFERENCIAS

7.1.Referencias bibliográficas

Altamirano de la Borda, K. J. (2020). *La seguridad de la información en la administración pública*. USA: Revista de Derecho Administrativo.

Avalos Mendoza, M. R. (2023). *Diseño de un modelo de gestión en seguridad digital para la administración pública peruana*. LIMA: Recuperado de <https://repositorio.esan.edu.pe/items/b111397c-5702-4dd8-8ea1-018635e9f28b>.

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

Ávila-Coello, A. A. (2025). *Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano*. ECUADOR: Revista GAEA.

Collantes Collantes, R. A. (2025). *Estrategias de gestión y su impacto en la eficiencia operativa del Gobierno Regional de Lima*. HUACHO: Tesis de Maestría, Universidad Nacional José Faustino Sánchez Carrión. Recuperado de <https://repositorio.unjfsc.edu.pe/bitstream/handle/20.500.14067/11450/TESIS.pdf>.

Contraloría General de la República. (2022). *Informe sobre seguridad informática en entidades públicas peruanas*. PERU: Contraloría General de la República.

Del Maestro Chambergo, M. G. (2025). *Ciberseguridad y su incidencia en la seguridad informática del área de sistemas en una entidad pública, Lima-2024*. LIMA: Recuperado de

https://alicia.concytec.gob.pe/vufind/Record/UCVV_6115a033c131d0bd29ca07bd47745418/Details.

Guarneros, J. (2022). *Implementación de procesos de seguridad informática bajo el estándar ISO 27001 en instituciones educativas*. USA: Recuperado de <https://rinacional.tecnm.mx/bitstream/TecNM/6163/1/Guarneros.pdf>.

Guba, E. G., & Lincoln, Y. S. (1994). *Competing paradigms in qualitative research*. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (pp. 105–117). USA: Sage.

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6ª ed.). usa: McGraw-Hill.

Kerlinger, F. N., & Lee, H. B. (2022). *Foundations of behavioral research* (4th ed.). USA: Wadsworth.

Ministerio de Transportes y Comunicaciones del Per. (2023). *Evaluación de la infraestructura tecnológica en gobiernos regionales*. PERU: Ministerio de Transportes y Comunicaciones del Perú.

Muñoz, J. J. (2023). *Modelo de gestión de riesgos basado en AMFE para el GAD Municipal de Flavio Alfaro*. ALFARO: Revista de Gestión Pública.

Olarte Quispe, P. B. (2023). *Seguridad informática y la vulnerabilidad del sistema de gestión de información en la Municipalidad de Lambayeque*. LAMBAYEQUE: Recuperado de https://repositorio.ulp.edu.pe/bitstream/handle/ULP/49/T142_73185092_B_PAUL%20OLARTE.pdf.

Rodríguez, N. J. (2023). *Continuidad técnica operativa en la infraestructura de red de una entidad pública peruana*. LIMA: Recuperado de https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/660151/Rodriguez_NJ.pdf.

Sánchez, N. G. M. (2023). *El E-Gobierno y la transformación de la administración pública en el Perú*. PERU: Recuperado de <https://ciencialatina.org/index.php/cienciala/article/view/7876>.

Torres Quevedo, L. A. (2023). *Gestión operativa del Gobierno Regional de Lima: Estrategias para mejorar la eficiencia en la prestación de servicios públicos*. PERU: tesis de Maestría, Universidad Nacional José Faustino Sánchez Carrión.

World Economic Forum. (2023). *Global Cybersecurity Report 2023*. USA: Global Cybersecurity Report 2023.

Zamora, L. . (2023). *Propuesta de creación de un CSIRT para el sector gubernamental*. NICARAGUA: Revista de Ingeniería y Tecnología.

VIII. ANEXOS

8.1. MATRIZ DE CONSISTENCIA

Seguridad informática y continuidad operativa en los sistemas de gestión del Gobierno Regional de Lima, 2025.

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
<u>Problema General</u>	<u>Objetivos General</u>	<u>Hipótesis General</u>	VARIABLE INDEPENDIENTE (X): Seguridad informática			
			DIMENSIONES	INDICADORES	Ítem	Nivel/Rango
¿Qué relaciona seguridad informática y continuidad operativa de los trabajadores del Gobierno Regional de Lima, 2025? <u>Problemas específicos</u>	Determinar relación a seguridad informática y continuidad operativa de los trabajadores del Gobierno Regional de Lima, 2025. <u>Objetivos específicos</u> - Analizar cómo seguridad informática se relaciona en planes de continuidad del negocio de los trabajadores del Gobierno Regional de Lima, 2025. - Evaluar de qué manera seguridad informática se relacionan con recuperación ante desastres (Disaster Recovery) de los trabajadores del Gobierno Regional de Lima, 2025.	Seguridad informática tiene una relación positiva en Continuidad operativa de los trabajadores del Gobierno Regional de Lima, 2025. <u>Hipótesis específicas</u> a. Seguridad informática tiene una relación positiva en Planes de continuidad del negocio de los trabajadores del Gobierno Regional de Lima, 2025. b. Seguridad informática tiene una relación positiva en Recuperación ante desastres (Disaster Recovery) de los trabajadores del Gobierno Regional de Lima, 2025. c. Seguridad informática tiene una	Confidencialidad de la información	- Control de accesos a los sistemas. - Uso de contraseñas seguras y autenticación. - Protección de datos sensibles.	1,2,3,	Nunca
			Integridad de los sistemas	- Prevención de modificaciones no autorizadas. - Registro de cambios en la información. - Validación de datos antes de su uso.	4,5,6	
¿De qué manera seguridad informática se relaciona con recuperación ante desastres (Disaster Recovery) de los trabajadores del Gobierno Regional de Lima, 2025? ¿Qué relación hay en seguridad informática y resiliencia de los sistemas de los trabajadores del			Disponibilidad de los sistemas	- Funcionamiento continuo de los sistemas críticos. - Minimización de tiempos de inactividad. - Acceso oportuno a la información.	7,8,9	A veces
			Gestión de riesgos y políticas de seguridad	- Existencia de políticas de seguridad formalizadas. - Evaluación periódica de riesgos informáticos. - Capacitación del personal en seguridad.	10,11,12	Siempre

Gobierno Regional de Lima, 2025?	- Examinar la relación de seguridad informática y Resiliencia de los sistemas de los trabajadores del Gobierno Regional de Lima, 2025. - Investigar cómo seguridad informática se relaciona en Monitoreo y mantenimiento de operaciones críticas de los trabajadores del Gobierno Regional de Lima, 2025.	relación positiva en Resiliencia de los sistemas de los trabajadores del Gobierno Regional de Lima, 2025. d. Seguridad informática tiene una relación positiva en Monitoreo y mantenimiento de operaciones críticas de los trabajadores del Gobierno Regional de Lima, 2025.			
VARIABLE DEPENDIENTE (Y): Continuidad operativa					
DIMENSIONES					
DIMENSIONES	INDICADORES	Ítem Nivel/Rango			
Planes de continuidad del negocio	- Documentación de procedimientos de emergencia. - Identificación de procesos críticos. - Actualización periódica de los planes.	13,14,15	Nunca		
Recuperación ante desastres	- Disponibilidad de respaldos de información. - Pruebas periódicas de recuperación. - Tiempo de recuperación ante fallas.	16,17,18	A veces		
Resiliencia de los sistemas	- Capacidad de adaptación ante incidentes. - Redundancia de sistemas críticos. - Respuesta rápida a interrupciones.	19,20,21	Siempre		
Monitoreo y mantenimiento de operaciones críticas	- Supervisión constante de sistemas esenciales. - Mantenimiento preventivo de equipos. - Detección temprana de fallas.	22,23,24	Casi Siempre		

8.2. CUESTIONARIO

Seguridad Informática y Continuidad Operativa 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 continuidad operativa 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 efectividad de las estrategias de continuidad operativa, 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. ¿Los sistemas del Gobierno Regional de Lima cuentan con controles adecuados de acceso para proteger la información?

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

2. ¿Se utilizan contraseñas seguras y métodos de autenticación confiables para el acceso a los sistemas?

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

3. ¿La información sensible se protege adecuadamente frente a accesos no autorizados?

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

DIMENSIÓN: Integridad de los sistemas

4. ¿Se previenen modificaciones no autorizadas en los sistemas y la información?
- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca
5. ¿Los cambios realizados en los sistemas se registran y controlan correctamente?
- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca
6. ¿La información es validada antes de su uso para evitar errores o inconsistencias?
- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca

DIMENSIÓN: Disponibilidad de los sistemas

7. ¿Los sistemas críticos funcionan de manera continua, sin interrupciones significativas?
- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca
8. ¿Se minimizan los tiempos de inactividad de los sistemas importantes?
- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca
9. ¿La información necesaria está disponible de manera oportuna cuando se requiere?
- a) Siempre b) Casi Siempre c) A veces
d) Casi Nunca e) Nunca

DIMENSIÓN: Gestión de riesgos y políticas de seguridad

10. ¿Existen políticas de seguridad formalmente establecidas y conocidas por el personal?

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

11. ¿Se realizan evaluaciones periódicas de riesgos informáticos en los sistemas?

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

12. ¿El personal recibe capacitación continua en seguridad informática?

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

NIVEL DE CONTINUIDAD OPERATIVA**DIMENSIÓN: Planes de continuidad del negocio**

13. ¿Los procedimientos de emergencia están documentados y actualizados regularmente?

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

14. ¿Se identifican claramente los procesos críticos para la operación del Gobierno Regional?

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

15. ¿Los planes de continuidad se revisan y actualizan periódicamente para mantener su efectividad?

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

DIMENSIÓN: Recuperación ante desastres

16. ¿Se realizan respaldos de información de manera regular y confiable?

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

17. ¿Se efectúan pruebas periódicas para asegurar la recuperación ante fallas?

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

18. ¿El tiempo de recuperación ante incidentes o fallas es adecuado y eficiente?

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

DIMENSIÓN: Resiliencia de los sistemas

19. ¿Los sistemas cuentan con mecanismos que permiten adaptarse rápidamente ante incidentes?

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

20. ¿Existe redundancia en los sistemas críticos para garantizar su funcionamiento continuo?

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

21. ¿Se responde de manera rápida y efectiva ante interrupciones o problemas técnicos?

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

DIMENSIÓN: Monitoreo y mantenimiento de operaciones críticas

22. ¿Los sistemas esenciales se supervisan de manera constante para prevenir fallas?

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

23. ¿Se realiza mantenimiento preventivo de los equipos y sistemas críticos regularmente?

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

24. ¿Se detectan de manera temprana los posibles problemas o fallas en los sistemas?

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