

Universidad Nacional José Faustino Sánchez Carrión

Escuela de Posgrado

Seguridad de los sistemas de información y su relación con la continuidad operativa de los servicios informáticos de la Universidad Nacional José Faustino Sánchez Carrión, 2025

Tesis

Para optar el Grado Académico de Maestro en Ingeniería de Sistemas

Autor

Jhon Anderson Irigoin Campos

Asesor

Dr Edwin Ivan Farro Pacifico

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

Escuela de Posgrado

Maestría en Ingeniería de Sistemas

METADATOS

DATOS DEL AUTOR:		
NOMBRES Y APELLIDOS	DNI	FECHA DE SUSTENTACIÓN
Jhon Anderson Irigoin Campos	71585811	15-09-2026
DATOS DEL ASESOR:		
NOMBRES Y APELLIDOS	DNI	CÓDIGO ORCID
Dr. Edwin Ivan Farro Pacifico	15735619	https://orcid.org/0000-0002-8735-8851
DATOS DE LOS MIEMROS DE JURADOS-POSGRADO-MAESTRÍA		
NOMBRES Y APELLIDOS	DNI	CODIGO ORCID
Dr. Alfredo Edgar Lopez Jimenez	15605331	https://orcid.org/0000-0003-4859-1092
Mo Carlos Enrique Chinga Ramos	40801418	https://orcid.org/0000-0002-3847-9163
Mo Jose Antonio Galdos Felipe	15760821	https://orcid.org/0000-0003-4160-6925

JHON ANDERSON IRIGOIN CAMPOS (2026-052821)

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y SU RELACIÓN CON LA CONTINUIDAD OPERATIVA DE LOS SERV...

DGI-POSGRADO 2026

Dirección de Gestión de la Investigación-VRI 2026

DIRECCION DE GESTION DE LA INVESTIGACION

Detalles del documento

Identificador de la entrega
trn:oid:::1:3611370580

Fecha de entrega
14 jul 2026, 12:51 p.m. GMT-5

Fecha de descarga
14 jul 2026, 12:56 p.m. GMT-5

Nombre del archivo
Tesis_Irigoin_Jhon.pdf

Tamaño del archivo
1.1 MB

80 páginas

13.473 palabras

79.221 caracteres

20% Similitud general

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

Filtrado desde el informe

- Bibliografía
- Coincidencias menores (menos de 10 palabras)

Exclusiones

- N.º de fuentes excluidas
- N.º de coincidencias excluidas

Fuentes principales

17% Fuentes de Internet
5% Publicaciones
14% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

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

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

DEDICATORIA.

A mi padre, Wilder Irigoin, quien desde el cielo guía mis pasos y permanece como fuente constante de inspiración.

A mi madre, María Campos, por su fortaleza, su dedicación y su apoyo incondicional, así como por demostrar que la vida se construye con valentía.

Con profundo amor, respeto y gratitud, este logro les pertenece.

Jhon Anderson Irigoin Campos

AGRADECIMIENTO

Expreso mi más sincero agradecimiento a todas las per que contribuyeron al desarrollo y culminación de la presente investigación.

En primer lugar, a mis padres, por su apoyo incondicional, sus enseñanzas y por ser el pilar fundamental en mi formación personal y profesional. Su esfuerzo y confianza han sido clave para alcanzar este logro.

De manera especial, agradezco a mi asesor, por su orientación constante, sus valiosas observaciones y el acompañamiento brindado durante todo el proceso de investigación. Su experiencia y dedicación han sido fundamentales para el desarrollo de este trabajo.

Asimismo, agradezco a los docentes de la Escuela de Posgrado, quienes, a través de sus enseñanzas y exigencia académica, contribuyeron a fortalecer mis conocimientos y habilidades profesionales.

Finalmente, expreso mi gratitud al personal de la Oficina de Servicios Informáticos de la Universidad Nacional José Faustino Sánchez Carrión, por su disposición y colaboración en la recolección de información, lo cual hizo posible la realización de esta investigación.

Jhon Anderson Irigoin Campos

ÍNDICE

DEDICATORIA **4**

AGRADECIMIENTO **5**

INDICE **6**

RESUMEN **10**

ABSTRACT **11**

INTRODUCCION **13**

CAPITULO I. PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática 15

1.2. Formulación del problema 17

1.2.1. Problema general 17

1.2.2. Problemas específicos 17

1.3. Objetivos de la investigación 17

1.3.1. Objetivo general 18

1.3.2. Objetivos específicos 18

1.4. Justificación de la investigación 18

1.5.Delimitación del estudio 21

CAPITULO II. MARCO TEORICO

2.1. Antecedentes de la investigación 22

2.1.1 Investigaciones internacionales 22

2.1.2. Investigaciones nacionales 24

2.2. Bases teóricas 25

2.3. Bases filosóficas 27

2.4. Definición de términos básicos 30

2.5. Hipótesis de la investigación 33

2.5.1. Hipótesis general 33

2.5.2. Hipótesis específicas 33

2.6. Operacionalización de variables 34

CAPITULO III. METODOLOGIA

3.1. Diseño metodológico 35

3.2. Población y muestra 35

3.2.1. Población 35

3.2.2. Muestra 35

3.3. Técnicas de recolección de datos 36

3.4 Técnicas para el procesamiento de la información 36

CAPITULO IV. RESULTADOS

4.1. Análisis de resultados 37

4.2. Contrastación de hipótesis 55

CAPITULO V. DISCUSIÓN

5.1. Discusión de resultados 59

CAPITULO VI. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones 62

6.2. Recomendaciones 65

CAPITULO VII. REFERENCIAS

7.1. Fuentes bibliográficas 66

ÍNDICE DE TABLAS

Tabla 1. Cuadro de operacionalización 34

Tabla 2. En la oficina se aplican políticas formales de respaldo de información..... 37

Tabla 3. Las copias de seguridad se realizan con la frecuencia necesaria..... 38

Tabla 4. Los respaldos son almacenados en entornos seguros y protegidos 40

Tabla 5. El sistema exige contraseñas seguras y renovadas periódicamente 41

Tabla 6. Los accesos a los sistemas quedan registrados y son revisados regularmente 43

Tabla 7. Los roles y permisos de acceso se asignan correctamente según las funciones del personal..... 44

Tabla 8. Los incidentes de seguridad son detectados con rapidez..... 46

Tabla 9. La respuesta del personal técnico ante incidentes de seguridad es eficaz 47

Tabla 10. Después de un incidente, se implementan acciones correctivas para prevenir su repetición 49

Tabla 11. Los sistemas informáticos permanecen operativos la mayor parte del tiempo (alta disponibilidad). 50

Tabla 12. Los servicios presentan pocas interrupciones durante su funcionamiento 52

Tabla 13. El sistema se mantiene disponible durante los horarios de mayor demanda..... 53

ÍNDICE DE FIGURAS

Figura 1. En la oficina se aplican políticas forales de respaldo de información.....37

Figura 2, Las copias de seguridad se realizan con la frecuencia necesaria 39

Figura 3. Los respaldos son almacenados en entornos seguros y protegidos.....40

Figura 4. El sistema exige contraseñas seguras y renovadas periódicamente 42

Figura 5, Los accesos a los sistemas quedan registrados y son revisados regularmente 43

Figura 6. Los roles y permisos de acceso se asignan correctamente según las funciones del personal 45

Figura 7, Los incidentes de seguridad son detectados con rapidez 46

Figura 8. La respuesta del personal técnico ante incidentes de seguridad es eficaz 48

Figura 9. Después de un incidente, se implementan acciones correctivas para prevenir su repetición 49

Figura 10. Los sistemas informáticos permanecen operativos la mayor parte del tiempo (alta disponibilidad). 51

Figura 11. Los servicios presentan pocas interrupciones durante su funcionamiento.....52

Figura 12. El sistema se mantiene disponible durante los horarios de mayor demanda.....54

RESUMEN

La presente investigación tuvo como objetivo determinar la relación entre la seguridad de los sistemas de información y la continuidad operativa de los servicios informáticos en la Universidad Nacional José Faustino Sánchez Carrión, 2025. La problemática abordó las deficiencias en la protección de datos, control de accesos y gestión de incidentes, que pueden comprometer la disponibilidad y estabilidad de los servicios tecnológicos institucionales.

El estudio fue de tipo aplicado, enfoque cuantitativo, alcance correlacional y diseño no experimental de corte transeccional. La población y muestra censal estuvieron conformadas por 14 trabajadores de la Oficina de Servicios Informáticos. Se empleó la encuesta mediante un cuestionario Likert de 18 ítems, validado por juicio de expertos (93%) y con alta confiabilidad ($\alpha = 0.96$).

Los resultados evidenciaron una correlación positiva alta entre la seguridad de los sistemas de información y la continuidad operativa (Rho = 0.849; $p < 0.05$). Asimismo, se encontraron correlaciones positivas altas entre la protección de datos (Rho = 0.849) y la gestión de incidentes (Rho = 0.849) con la continuidad operativa, mientras que el control de accesos presentó una correlación positiva moderada (Rho = 0.548).

Se concluyó que existe una relación positiva significativa entre la seguridad de los sistemas de información y la continuidad operativa de los servicios informáticos. Sin embargo, las prácticas de seguridad requieren mayor fortalecimiento y estandarización para optimizar el desempeño institucional.

Palabras clave: Seguridad de la información, continuidad operativa, protección de datos, control de accesos, gestión de incidentes.

.

ABSTRACT

The present study aimed to determine the relationship between information systems security and the operational continuity of IT services at José Faustino Sánchez Carrión National University in 2025. The research addressed deficiencies in data protection, access control, and incident management, which may compromise the availability and stability of institutional IT services.

The study was applied in nature, with a quantitative approach, correlational scope, and a non-experimental, cross-sectional design. The population and census sample consisted of 14 employees from the Office of Information Technology Services. Data were collected through a survey using an 18-item Likert-scale questionnaire, validated through expert judgment (93%) and demonstrating high reliability ($\alpha = 0.96$).

The results revealed a strong positive correlation between information systems security and operational continuity (Spearman's rho = 0.849; $p < 0.05$). Similarly, strong positive correlations were found between data protection (rho = 0.849) and incident management (rho = 0.849) and operational continuity, while access control showed a moderate positive correlation (rho = 0.548).

It was concluded that a significant positive relationship exists between information systems security and the operational continuity of IT services. However, security practices require further strengthening and standardization to optimize institutional performance.

Keywords: Information security, operational continuity, data protection, access control, incident management.

INTRODUCIÓN

En la actualidad, el uso de tecnologías de la información se ha convertido en un elemento fundamental para el funcionamiento de las organizaciones, especialmente en instituciones educativas donde los sistemas informáticos soportan procesos académicos, administrativos y de gestión. En este contexto, la seguridad de los sistemas de información adquiere un rol estratégico, ya que permite proteger los datos institucionales y garantizar la disponibilidad, integridad y confidencialidad de la información, aspectos clave para el desarrollo eficiente de las actividades organizacionales.

A nivel internacional, el incremento de amenazas cibernéticas, ataques informáticos y fallas tecnológicas ha evidenciado la necesidad de fortalecer los mecanismos de seguridad en los sistemas de información. Diversos estudios han demostrado que una adecuada gestión de la seguridad informática no solo reduce riesgos, sino que también contribuye directamente a la continuidad operativa de los servicios, permitiendo que las organizaciones mantengan sus funciones incluso ante situaciones adversas. En este sentido, la seguridad de la información se consolida como un factor determinante para la resiliencia y sostenibilidad institucional.

En el contexto nacional, las instituciones públicas, particularmente las universidades, enfrentan importantes desafíos en la gestión de sus sistemas informáticos. La existencia de brechas en la protección de datos, debilidades en los controles de acceso y limitaciones en la gestión de incidentes evidencian la necesidad de fortalecer las estrategias de seguridad tecnológica. Estas deficiencias pueden generar interrupciones en los servicios, pérdida de información y afectación en los procesos académicos y administrativos, comprometiendo la calidad del servicio institucional.

En la Universidad Nacional José Faustino Sánchez Carrión, la Oficina de Servicios Informáticos presenta diversas dificultades relacionadas con la seguridad de los sistemas,

tales como fallas en los servidores, interrupciones en los servicios, debilidades en los mecanismos de respaldo y una limitada capacidad de respuesta ante incidentes. Estas condiciones afectan la disponibilidad de los sistemas y ponen en riesgo la continuidad operativa de los servicios informáticos, lo que justifica la necesidad de analizar la relación entre ambas variables.

En este marco, la presente investigación tiene como objetivo determinar de qué manera la seguridad de los sistemas de información se relaciona con la continuidad operativa de los servicios informáticos en la Universidad Nacional José Faustino Sánchez Carrión, considerando como dimensiones la protección de datos, el control de accesos y la gestión de incidentes. El estudio se desarrolla bajo un enfoque cuantitativo, de tipo aplicado, con alcance correlacional y diseño no experimental de corte transeccional, utilizando como instrumento un cuestionario tipo Likert aplicado al personal de la Oficina de Servicios Informáticos.

Finalmente, esta investigación busca aportar evidencia científica que permita comprender la importancia de la seguridad de los sistemas de información como un elemento clave para garantizar la continuidad operativa de los servicios informáticos. Asimismo, pretende servir como base para la toma de decisiones orientadas a fortalecer la gestión tecnológica institucional, mejorar la calidad de los servicios y asegurar un funcionamiento eficiente y confiable en beneficio de la comunidad universitaria.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

A nivel mundial, la seguridad de la información se ha consolidado como un pilar fundamental para el funcionamiento de organizaciones públicas y privadas, debido al incremento constante de ciberataques, brechas de datos y vulnerabilidades tecnológicas. Según Whitman y Mattord (2022), la seguridad de la información comprende la protección de los datos y de los sistemas que los procesan, almacenan y transmiten, mediante políticas, controles y mecanismos diseñados para garantizar su confidencialidad, integridad y disponibilidad, componentes esenciales en un entorno digital cada vez más complejo. La globalización tecnológica, la expansión del uso de servicios en la nube, el avance del Internet de las Cosas (IoT) y la sofisticación de las amenazas cibernéticas han hecho que las organizaciones deban adoptar estrategias más robustas y proactivas para mitigar riesgos y asegurar la continuidad de sus operaciones. Esto demuestra que, en el escenario internacional, la seguridad de la información ya no es una opción, sino un requisito indispensable para la sostenibilidad y competitividad institucional.

En el Perú, la seguridad de la información se ha convertido en un desafío prioritario para las instituciones públicas y privadas debido al incremento de ciberataques, incidentes de fuga de datos y vulnerabilidades en infraestructuras tecnológicas críticas. Según el informe elaborado por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual —INDECOPI— y el Centro Nacional de Seguridad Digital, muchas organizaciones del país aún presentan brechas significativas en la gestión de riesgos, control de accesos, protección de datos

y continuidad operativa, factores que incrementan la exposición frente a amenazas tecnológicas (Centro Nacional de Seguridad Digital, 2021). Esta situación coloca al país ante la necesidad urgente de fortalecer políticas de ciberseguridad, estandarizar procedimientos y promover una cultura organizacional orientada a la protección de activos digitales, garantizando así la estabilidad de los servicios institucionales.

En la actualidad, la Oficina de Servicios Informáticos de la Universidad Nacional José Faustino Sánchez Carrión enfrenta desafíos significativos en la gestión de la seguridad de los sistemas de información y en la continuidad operativa de sus servicios tecnológicos. Aunque la institución ha avanzado en la digitalización de numerosos procesos, la infraestructura tecnológica aún presenta limitaciones propias de equipos con años de uso, sistemas sin mantenimiento constante y recursos insuficientes para proteger adecuadamente los datos institucionales.

El análisis del centro de datos, según lo expuesto por el jefe del área en el video proporcionado, revela fallas recurrentes en los servidores, interrupciones inesperadas en los sistemas críticos, deficiencias en los mecanismos de respaldo y una alta dependencia de intervenciones manuales ante incidentes. Estas condiciones generan riesgos de pérdida de información, indisponibilidad de plataformas institucionales y demoras en los procesos administrativos y académicos que sustentan el funcionamiento universitario.

La carencia de un monitoreo robusto, controles de acceso actualizados y políticas de seguridad integrales incrementa la vulnerabilidad frente a incidentes informáticos, mientras que la limitada capacidad de recuperación ante fallos afecta directamente la continuidad de los servicios. Estas situaciones sugieren una posible relación entre el nivel de seguridad de los sistemas y la estabilidad operativa de los servicios informáticos, justificando la necesidad de desarrollar una investigación correlacional

que permita determinar cómo estos factores interactúan y en qué medida impactan en el desempeño tecnológico de la universidad.

1.1 Formulación del problema

1.2.1 Problema general

¿Cómo la seguridad de los sistemas de información se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025?

1.2.2. Problemas específicos

a) ¿Cómo la protección de datos se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025?
b) ¿Cómo los controles de accesos se relacionan con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025?
c) ¿Cómo la gestión de incidentes se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025?

1.3. Objetivos de la investigación

1.3.1 Objetivo general

Determinar de qué manera la seguridad de los sistemas de información se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

1.3.2 Objetivos específicos

a) Determinar de qué manera la protección de datos se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

b) Determinar de qué manera los controles de accesos se relacionan con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

c) Determinar de qué manera la gestión de incidentes se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

1.4. Justificación de la investigación

La presente investigación se justifica porque la Universidad Nacional José Faustino Sánchez Carrión atraviesa un momento clave en la gestión de su infraestructura tecnológica. En los últimos años, la universidad ha incrementado el uso de plataformas digitales para actividades académicas y administrativas, lo que ha vuelto indispensable contar con sistemas informáticos seguros, disponibles y preparados para responder ante incidentes. Sin embargo, como se ha evidenciado en diferentes situaciones ocurridas en la institución, los servicios tecnológicos aún presentan vulnerabilidades que pueden afectar el desarrollo normal de las labores universitarias, tanto para docentes, estudiantes como para el personal administrativo.

Los eventos recientes, como los problemas de acceso, interrupciones inesperadas y la vulnerabilidad de algunos sistemas institucionales, han demostrado que la seguridad de la información no solo es un requisito técnico, sino un componente esencial para

garantizar la continuidad de los procesos que sostienen la vida académica. Cuando un sistema falla o se ve comprometido, las actividades de la comunidad universitaria se detienen, se generan retrasos, se pierde información valiosa y se afecta la confianza en los servicios institucionales. Esta situación revela una necesidad urgente de comprender cómo la seguridad de los sistemas de información influye en su continuidad operativa.

El aporte de esta investigación es significativo porque permitirá identificar de manera objetiva la relación entre ambos factores, brindando evidencia científica que ayude a la universidad a tomar decisiones informadas para fortalecer sus servicios informáticos. Los resultados podrán orientar mejoras en políticas de seguridad, optimizar mecanismos de respaldo y recuperación, y promover prácticas que incrementen la resiliencia tecnológica ante fallas o amenazas externas. Asimismo, esta investigación puede servir como base para futuros proyectos de modernización tecnológica dentro de la institución.

Desde un enfoque académico, el estudio contribuye a la generación de nuevo conocimiento aplicado al contexto universitario peruano, donde aún existe limitada literatura sobre la relación entre seguridad informática y continuidad operativa en instituciones públicas de educación superior. Además, ofrece un valor práctico, ya que sus conclusiones permitirán implementar acciones que beneficien directamente a la comunidad universitaria, proporcionando servicios informáticos más confiables, estables y seguros.

En síntesis, esta investigación es necesaria porque aborda un problema real, actual y con impacto directo en el funcionamiento institucional. Busca comprender y mejorar la manera en que la universidad protege sus sistemas y garantiza su operatividad,

fortaleciendo así la calidad del servicio educativo y administrativo que brinda a la sociedad.

1.5. Delimitaciones del estudio

1.5.1. Delimitación espacial

La investigación se llevará a cabo en la oficina de servicios informáticos de la universidad nacional José Faustino Sánchez Carrión de la ciudad de Huacho.

1.5.2. Delimitación temporal

Se llevará a cabo entre 2025 - 2026

1.5.3. Delimitación social

Se tomó el personal de la oficina de servicios informáticos

1.6. Viabilidad del estudio

Es totalmentee viable porque cuenta con las condiciones técnicas, humanas e institucionales necesarias para su ejecución. En primer lugar, la Universidad Nacional José Faustino Sánchez Carrión, a través de la Oficina de Servicios Informáticos, brinda las facilidades de acceso a la información requerida, así como la disposición del personal especializado que forma parte de la población de estudio. Dado que el número de participantes es reducido y accesible, la aplicación del cuestionario y la recolección de datos pueden realizarse sin dificultades ni requerimientos logísticos complejos.

Desde el punto de vista técnico, la investigación no requiere equipamiento sofisticado ni recursos tecnológicos adicionales, ya que se trabajará con instrumentos accesibles como cuestionarios digitales o impresos, y el análisis estadístico se efectuará

mediante software disponible y conocido, como SPSS. Esto permite un procesamiento eficiente, rápido y seguro de la información, lo que facilita la obtención de resultados válidos y confiables.

Asimismo, la viabilidad económica está asegurada, dado que los costos asociados al desarrollo del estudio —como impresiones, movilidad, acceso a internet y materiales de trabajo— son asumibles por el investigador y no representan una limitación para el desarrollo del proyecto. Los recursos humanos también se encuentran garantizados, al contar con el acompañamiento del asesor y la disposición del personal de la oficina para participar en el proceso de investigación.

En términos institucionales, la universidad promueve y respalda investigaciones orientadas a mejorar sus procesos internos, especialmente aquellas relacionadas con la modernización tecnológica y la seguridad de la información. Por ello, existe un ambiente favorable y una actitud colaborativa que facilita la ejecución del estudio.

En conjunto, estas condiciones aseguran que la investigación pueda desarrollarse de manera ordenada, oportuna y con resultados útiles para la mejora continua de los servicios informáticos de la universidad.

CAPITULO II

MARCO TEORICO

1.1. Antecedentes de la investigación

2.1.1 Investigaciones internacionales

Autor(es): Jooda, T. O. (2025) Título del estudio: The impact of business continuity planning on cybersecurity risk management in financial institutions Tipo de documento: Artículo científico. Objetivo de la investigación: Evaluar el impacto de la planificación de continuidad de negocio (BCP) en la gestión de riesgos de ciberseguridad en instituciones financieras, midiendo su efecto en tiempos de respuesta, pérdidas financieras y tiempo de inactividad. Metodología: Enfoque mixto (cuantitativo y cualitativo), tipo convergent parall, el alcance exploratorio, diseño con regresión lineal múltiple, análisis de sensibilidad y estudios de caso; población de 50 instituciones financieras y 20 entrevistas con expertos. Conclusiones principales: La BCP reduce significativamente los riesgos cibernéticos (coeficiente -0.625), con instituciones de alta madurez BCP mostrando tiempos de respuesta 3.3 veces más rápidos y pérdidas 6 veces menores. La adopción de IA complementa, pero no sustituye la BCP. Se recomienda integrar BCP con monitoreo en tiempo real y entrenamiento para mejorar resiliencia. Los resultados validan empíricamente la correlación inversa entre BCP y disrupciones operativas.

Autor(es): Salam, M., Abu Bakar, K. A., & Mohd Aman, A. H. (2025) Título del estudio: Building cyber-resilient universities: A tailored maturity model for strengthening cybersecurity in higher education. Tipo de documento: Artículo científico. Objetivo de la investigación: Desarrollar y validar un modelo de madurez en ciberseguridad (CSMM) adaptado a instituciones de educación superior (HEIs) para evaluar y mejorar su resiliencia ante amenazas como ransomware y phishing. Metodología: Enfoque mixto exploratorio, tipo secuencial (cualitativo seguido de cuantitativo), alcance múltiple casos, diseño con entrevistas, encuestas y análisis temático; muestra de 400 profesionales de TI y expertos en HEIs. Conclusiones principales: El CSMM identifica 11 dominios clave (gobernanza, gestión de riesgos, etc.) para medir madurez, validado como práctico y confiable. Aborda brechas en HEIs como presupuestos limitados y sistemas abiertos. Mejora la preparación institucional contra interrupciones digitales. Se alinea con marcos como NIST e ISO 27001 para resiliencia operativa.

Alqahtani, H., & Kavakli-Thorne, M. (2024). Título del estudio: Fortifying organizational cyber resilience: An integrated framework for business continuity. Tipo de documento: Artículo científico. Objetivo de la investigación: Proponer marco integrado de políticas proactivas, pruebas de resiliencia y tecnologías emergentes para continuidad ante ciberamenazas. Metodología: Enfoque cualitativo, tipo literatura y desarrollo de framework, alcance conceptual, diseño analítico. Población o muestra: No aplica (estudio teórico-empírico). Conclusiones principales: Marco combina seguridad proactiva con colaboración para minimizar disrupciones. Identifica componentes clave como testing y IA para resiliencia

organizacional. Mejora continuidad operativa en entornos amenazados. Enfatiza adaptación dinámica a amenazas.

World Economic Forum (2025) Título del estudio: Global Cybersecurity Outlook 2025. Tipo de documento: Reporte académico. Objetivo de la investigación: Analizar tendencias globales en ciberseguridad y su impacto en resiliencia operativa de organizaciones. Metodología: Enfoque mixto, tipo descriptivo-analítico, alcance global, diseño con encuestas y casos. Población o muestra: Líderes empresariales y expertos en ciberseguridad internacionales. Conclusiones principales: Brechas en resiliencia cibernética amenazan continuidad operativa; urge inversión en capacidades predictivas. Correlación fuerte entre madurez de seguridad y recuperación rápida. Recomienda colaboración público-privada. Enfatiza rol de IA en gestión de riesgos

2.1.2. Investigaciones nacionales

Sanchez Estupiñan, E. G. (2023) Título: Seguridad de la información y su relación con la calidad de servicio en la Universidad Nacional José Faustino Sánchez Carrión. Tipo de documento: Tesis. Objetivo del estudio: Determinar la correlación entre seguridad de la información y calidad de servicio en servicios TI universitarios. Metodología: Enfoque cuantitativo correlacional, tipo no experimental, alcance descriptivo, diseño transversal; población de personal universitario. Conclusiones principales: Alta correlación (0.881) entre seguridad de la información y calidad de servicio, enfatizando integridad, disponibilidad y confidencialidad. Evidencia relación directa con continuidad operativa. Recomienda fortalecer políticas para minimizar interrupciones.

Atalaya Urrutia, C. W. (2023) Título: Modelo de ciberseguridad en universidades privadas en el Perú. Tipo de documento: Tesis doctoral. Objetivo del estudio: Implemetar un modelo de ciberseguridad basado en ISO/IEC 27032 y NIST para universidades privadas peruanas. Metodología: Enfoque mixto, tipo aplicado, alcance propositivo, diseño con revisión literaria y propuesta de modelo; población universidades privadas. Conclusiones principales: Reduce exposición a amenazas mediante evaluación de riesgos, políticas y monitoreo. Mejora protección de activos digitales y resiliencia. Aplicable a entidades públicas similares.

Avalos Mendoza, M. R. (2023) Título: Diseño de un modelo de gestión en seguridad digital para entidades del sector público peruano. Tipo de documento: Tesis de maestría. Objetivo del estudio: Proponer modelo integrable con marcos como NIST para prevención y respuesta en seguridad digital pública. Metodología: Enfoque cualitativo-propositivo, tipo diseño de modelo, alcance sectorial, diseño basado en buenas prácticas. Población o muestra: Entidades públicas peruanas. Conclusiones principales: Fortalece capacidades preventivas y de respuesta cibernética. Integra NIST/ISO para resiliencia operativa. Reduce vulnerabilidades en servicios TI públicos. Evidencia necesidad de adopción inmediata.

2.2. Bases teóricas

Seguridad de la informacion

ISO/IEC JTC 1/SC 27. (2022) Seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además de la protección contra la divulgación, modificación, destrucción no autorizada o interrupción del acceso o uso.

National Institute of Standards and Technology (NIST) 2020. Seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de información, y protección contra divulgación no autorizada, disrupción, modificación o destrucción de información y sistemas de información

ISACA (2022). Seguridad de la información son prácticas para salvaguardar la información contra acceso, divulgación, disrupción, modificación o eliminación no autorizados, incluyendo prevención, detección y respuesta a incidentes.

IBM Corporation (2023). Seguridad de la información (InfoSec) es la protección de la información contra acceso, divulgación, uso, alteración o interrupción no autorizados, abarcando seguridad de TI física, endpoints, cifrado y redes.

García Mayor, A. (2023) Seguridad de la información en sistemas es la gestión de riesgos mediante SGSI (ISO 27001) y ENS, protegiendo confidencialidad, integridad y disponibilidad en entornos con IA y tecnologías emergentes.

Continuidad operativa de servicios informáticos

ISO (2019) Continuidad operativa es la capacidad organizacional para entregar productos/servicios a un nivel aceptable durante interrupciones, integrando resiliencia, recuperación y contingencia para disponibilidad TI.

NIST (2020). Contingencia TI es el desarrollo de planes para recuperación continua de sistemas TI críticos, asegurando disponibilidad, integridad y operaciones post-interrupción.

AXELOS (2020) La Gestión de continuidad TI, asegura operatividad de servicios TI durante/tras interrupciones, mediante resiliencia, recuperación de desastres y contingencia alineada con ITIL.

ISACA (2022). Continuidad operativa es la gobernanza para mantener servicios TI críticos ante disrupciones, integrando planes de contingencia y resiliencia en COBIT.

NIST (2024) Resiliencia TI es la capacidad de anticipar, resistir, absorber, adaptarse a y recuperarse de disrupciones adversas, manteniendo operaciones esenciales.

2.3. Bases filosóficas

Tiene diversos enfoques filosóficos que orientan la manera en que se concibe el fenómeno estudiado, así como la forma en que se interpreta la relación entre la seguridad de los sistemas de información y la continuidad operativa de los servicios informáticos en la Universidad Nacional José Faustino Sánchez Carrión. Estas bases permiten comprender no solo el aspecto técnico del problema, sino también su dimensión humana, institucional y social.

a) Enfoque ontológico

Desde la perspectiva ontológica, esta investigación parte del reconocimiento de que la seguridad de los sistemas de información es una condición real, objetiva y medible dentro del entorno tecnológico de la universidad. La continuidad operativa, por su parte, también se concibe como un fenómeno concreto que puede observarse en el funcionamiento diario de los sistemas informáticos, en la estabilidad de los servicios y en la capacidad institucional para recuperarse ante incidentes.

Así, se asume que ambas variables existen independientemente del investigador y pueden ser analizadas mediante indicadores claros, como la protección de datos, los controles de acceso, la gestión de incidentes, la disponibilidad, la recuperación y la resiliencia operativa. Esta comprensión ontológica permite estudiar la relación entre ambas variables de manera objetiva y verificable.

b) Enfoque epistemológico

En el plano epistemológico, el trabajo se sustenta en el enfoque cuantitativo, el cual considera que el conocimiento válido surge del análisis sistemático de datos obtenidos de la realidad. Esto implica que los fenómenos estudiados, como los niveles de seguridad informática y la continuidad operativa, pueden ser medidos, comparados y correlacionados mediante instrumentos y técnicas estadísticas confiables, lo que permite establecer patrones y relaciones significativas.

Este enfoque reconoce que el conocimiento se construye a partir de evidencias empíricas, por lo que el uso de encuestas, análisis de frecuencia y pruebas estadísticas como chi-cuadrado es fundamental para comprender de manera rigurosa cómo la seguridad tecnológica incide en la continuidad de los servicios informáticos.

c) Enfoque axiológico

En el aspecto axiológico, la investigación reconoce la importancia de los valores éticos asociados al manejo de la información, tales como la responsabilidad, la transparencia, la protección de datos y el respeto a la privacidad institucional. La seguridad de los sistemas de información no es solo un requisito técnico, sino un compromiso moral con la comunidad universitaria, ya que su adecuada gestión garantiza servicios confiables, protege la integridad de la información y promueve la seguridad de los usuarios.

Asimismo, la continuidad operativa adquiere un valor fundamental porque asegura que los procesos administrativos y académicos no se vean afectados ante fallas o incidentes,

evitando perjuicios a estudiantes, docentes y personal administrativo. En este sentido, la investigación reconoce que mejorar la seguridad y la continuidad no solo es una decisión técnica, sino también un acto ético orientado al bienestar institucional.

d) Enfoque teleológico

Desde la perspectiva teleológica, el estudio se orienta hacia un fin claro: contribuir al fortalecimiento de los servicios informáticos de la universidad mediante el análisis de la relación entre la seguridad de la información y la continuidad operativa. La finalidad última es generar evidencia que permita mejorar políticas, procesos y prácticas institucionales, favoreciendo la modernización tecnológica y el funcionamiento eficiente de la universidad.

El propósito de la investigación no se limita a describir un problema, sino que busca ofrecer resultados que permiten tomar mejores decisiones, asegurando que la institución pueda anticipar, resistir y recuperarse de incidentes informáticos de manera efectiva.

e) Enfoque humanista

Finalmente, esta investigación se sustenta en una mirada humanista al reconocer que detrás de cada sistema informático existe una comunidad de personas que depende de su correcto funcionamiento. La seguridad tecnológica y la continuidad operativa no solo garantizan que los sistemas funcionen correctamente, sino que permiten que estudiantes, docentes y trabajadores desarrollen sus actividades sin interrupciones ni riesgos.

Este enfoque recuerda que la tecnología debe estar al servicio de las personas y que toda mejora en la gestión de seguridad y continuidad impacta directamente en la calidad de vida académica y administrativa de quienes forman parte de la institución.

2.4. Definiciones conceptuales

- Seguridad de los sistemas de información: Es el conjunto de prácticas, políticas, controles y mecanismos destinados a proteger los datos y los sistemas tecnológicos que utiliza una organización. Involucra acciones preventivas y reactivas que buscan garantizar la confidencialidad, integridad y disponibilidad de la información, evitando accesos no autorizados, pérdida de datos o interrupciones en los servicios institucionales.
- Protección de datos: Hace referencia a todas las medidas implementadas para resguardar la información institucional frente a pérdidas, alteraciones o accesos indebidos. Incluye actividades como realizar copias de seguridad, aplicar políticas de respaldo y almacenar los datos en entornos seguros. Este término expresa el compromiso de la institución por preservar el valor y la confiabilidad de su información.
- *Políticas de respaldo:* Son lineamientos establecidos para definir cómo, cuándo y con qué frecuencia se deben realizar copias de seguridad de la información. Su propósito es garantizar que los datos puedan recuperarse en caso de fallos o incidentes.
- *Frecuencia de copias de seguridad:* Se refiere a la periodicidad con la que la institución realiza respaldos de su información. Una frecuencia adecuada disminuye el riesgo de pérdida de datos importantes.
- *Almacenamiento seguro de la información:* Implica guardar los respaldos en lugares protegidos, tanto física como digitalmente, de modo que no puedan ser alterados, dañados o robados.
- Control de accesos: Es el proceso mediante el cual se regula quién puede ingresar a los sistemas informáticos de la institución y qué acciones puede realizar cada

usuario. Su objetivo es evitar accesos no autorizados, reducir riesgos y mantener la seguridad de la infraestructura tecnológica.

- *Contraseñas seguras:* Son claves creadas bajo criterios de complejidad y seguridad que reducen la posibilidad de ser vulneradas. Su correcto uso ayuda a prevenir intrusiones en los sistemas.
- *Registros de accesos:* Son archivos o bitácoras que almacenan información sobre quién ingresó al sistema, cuándo lo hizo y qué acciones realizó. Estos registros ayudan a identificar incidentes y fortalecer la seguridad.
- *Gestión de permisos y roles:* Consiste en asignar a cada usuario los niveles de acceso que corresponden a sus funciones. Una adecuada gestión evita que personas sin autorización accedan a información sensible.
- Gestión de incidentes: Es el conjunto de procedimientos y acciones que se aplican para detectar, analizar y responder a eventos que afectan la seguridad o el funcionamiento de los sistemas informáticos. Incluye tanto la identificación temprana de amenazas como la puesta en marcha de medidas correctivas que permitan minimizar daños y evitar que incidentes similares vuelvan a ocurrir.
- *Tiempo de detección de ataques:* Mide la rapidez con la que la institución identifica un incidente de seguridad. Detectar a tiempo permite reducir la magnitud del daño.
- *Respuesta ante incidentes:* Hace referencia a la capacidad de la institución para actuar oportunamente cuando se presenta un problema de seguridad, restaurar los servicios afectados y proteger los datos.
- *Acciones correctivas:* Son las medidas implementadas después de un incidente para evitar que vuelva a repetirse. Representan el aprendizaje institucional frente a eventos adversos.

- Continuidad operativa de los servicios informáticos: Es la capacidad de la institución para mantener activos sus servicios tecnológicos aun cuando se presenten fallos, interrupciones o incidentes de seguridad. Incluye los mecanismos de disponibilidad, recuperación y resiliencia, todos orientados a asegurar que los procesos administrativos y académicos no se detengan ante una eventualidad.
- Disponibilidad: Indica el grado en que los servicios informáticos están activos, accesibles y funcionando correctamente cuando los usuarios los necesitan. La disponibilidad es un factor crítico, pues su interrupción afecta directamente el desarrollo de actividades institucionales.
- *Tiempo de funcionamiento (uptime):* Mide la proporción del tiempo en que los sistemas permanecen operativos sin fallas.
- *Frecuencia de interrupciones:* Se refiere a cuántas veces los servicios dejan de funcionar en un periodo determinado.
- *Disponibilidad en horas de mayor demanda:* Evalúa si los sistemas se mantienen operativos en aquellos momentos en los que más se necesitan, como días de matrícula, entrega de notas o sesiones virtuales.
- Recuperación: Es el proceso mediante el cual la institución restaura sus servicios informáticos después de un fallo, ataque o interrupción. Una recuperación rápida y completa contribuye a reducir impactos negativos en la comunidad universitaria.
- *Tiempo de restauración:* Mide qué tan pronto los sistemas vuelven a estar operativos tras un incidente.
- *Aplicación del plan de contingencia:* Indica si la institución cuenta con procedimientos previamente establecidos para actuar ante emergencias y si dichos procedimientos se ejecutan adecuadamente.

- *Recuperación total de datos y servicios:* Evalúa si, después del incidente, la institución logra restaurar la totalidad de la información y funcionalidades afectadas.
- Resiliencia operativa: Es la capacidad de los sistemas informáticos para resistir, adaptarse y continuar funcionando cuando enfrentan incidentes, fallos o cambios en el entorno. Una infraestructura resiliente no solo responde a los problemas, sino que también aprende de ellos para fortalecerse a futuro.
- *Resistencia ante ataques o fallos:* Indica si el sistema puede mantener un nivel mínimo de servicio aun cuando ocurre un incidente.
- *Adaptación frente a amenazas o cambios:* Evalúa la capacidad del sistema para ajustarse de forma dinámica ante situaciones imprevistas.
- *Mejoras preventivas posteriores a incidentes:* Refleja si la institución implementa ajustes y aprendizajes para evitar que eventos similares se repitan.

2.5. Formulación de la hipótesis

2.5.1. Hipótesis general

La seguridad de los sistemas de información se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

2.5.2. Hipótesis específicas

a) La protección de datos se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

b) Los controles de accesos se relacionan con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

c) La gestión de incidentes se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

2.6.Operacionalización de variables

Tabla 1. Cuadro de operacionalización

Variables	Definición conceptual	Definición operacional	Dimensiones	Indicadores
Seguridad de los sistemas de información	La seguridad de los sistemas de información se refiere al conjunto de políticas, procedimientos, controles técnicos y administrativos implementados para garantizar la confidencialidad, integridad y disponibilidad de los datos y servicios informáticos. Su objetivo es prevenir accesos no autorizados, evitar la alteración o pérdidade información y asegurar que los sistemas permanezcan operativos ante incidentes o amenazas internas y externas.	Para efectos de la presente investigación, la seguridad de los sistemas de información se medirá mediante una encuesta tipo Likert aplicada al personal de la Oficina de Servicios Informáticos. Esta variable se evaluará a través de las dimensiones protección de datos, control de accesos y gestión de incidentes, considerando indicadores como: aplicación de políticas de respaldo, uso adecuado de mecanismos de autenticación, registro de accesos, tiempo de detección de incidentes y capacidadde respuesta ante ataques	Protección de datos	Políticas de respaldo implementadas Frecuencia de copias de seguridad Almacenamiento seguro de la información
			Control de accesos	Uso de contraseñas seguras Registros de accesos Gestión de permisos y roles de usuario
			Gestión de incidentes	Tiempo de detección de ataques Respuesta ante incidentes Implementación de acciones correctivas
Continuidad operativa	Conjunto de mecanismos destinados a resguardar la información institucional mediante políticas de respaldo, almacenamiento seguro y procedimientos que garantizan que los datos no se pierdan ni sean alterados	Será medida mediante ítems que evalúan la frecuencia de copias de seguridad, existencia de políticas de respaldo y aplicación de estrategias de protección de información crítica.	Disponibilidad	Tiempo de funcionamiento (uptime) Frecuencia de interrupciones Disponibilidad durante horas de mayor demanda.
			Recuperación	Tiempo de restauración tras incidentes Aplicación del plan de contingencia Recuperación total de datos y servicios afectados.
			Resiliencia Operativa	Capacidad del sistema para resistir ataques o fallos. Adaptación del sistema frente a cambios o amenazas. Implementación de mejoras preventivas luego de incidentes.

CAPITULO III

METODOLOGIA

3.1. Diseño metodológico

3.1.1. Tipo de investigación

Tipo aplicada

3.1.2. Enfoque

Investigación de enfoque cuantitativo

3.1.3. Alcance

Investigación con alcance correlacional

3.1.4. Diseño

Es no experimental y transeccional

3.2. Población y muestra

3.2.1 Población

La población está conformada por 14 personas de la dependencia de servicios inforáticos.

3.2.2 Muestra

La muestra es la totalidad de la población

3.3. Técnicas e instrumentos de recolección de datos

3.3.1. Técnicas a emplear

Técnica principal empleada para la recolección de datos es la encuesta. Para garantizar la validez del instrumento, este se sometió a un juicio de expertos, mientras que su consistencia interna se determinó mediante el cálculo del coeficiente de confiabilidad.

3.3.2. Descripción del instrumento

Nuestro estudio empleará un cuestionario estructurado siendo un instrumento de recolección de datos, el cual será aplicado a una muestra representativa de la población de interés. Dicho instrumento estará compuesto por preguntas cerradas, de opción múltiple y reactivos bajo la escala de Likert. El proceso de levantamiento de información se ejecutará en un lapso de tiempo predeterminado, asegurando en todo momento el anonimato, la confidencialidad y los principios éticos de la participación.

3.4. Técnicas para el procesamiento de la información

Se realizará mediante estadística descriptiva, específicamente a través de distribuciones de frecuencias, y estadística inferencial mediante la prueba de chi-cuadrado. El análisis automatizado se efectuará con el software IBM SPSS Statistics, y los hallazgos cuantitativos se organizarán y expondrán mediante tablas y gráficos estadísticos para su posterior interpretación.

CAPITULO IV

RESULTADOS

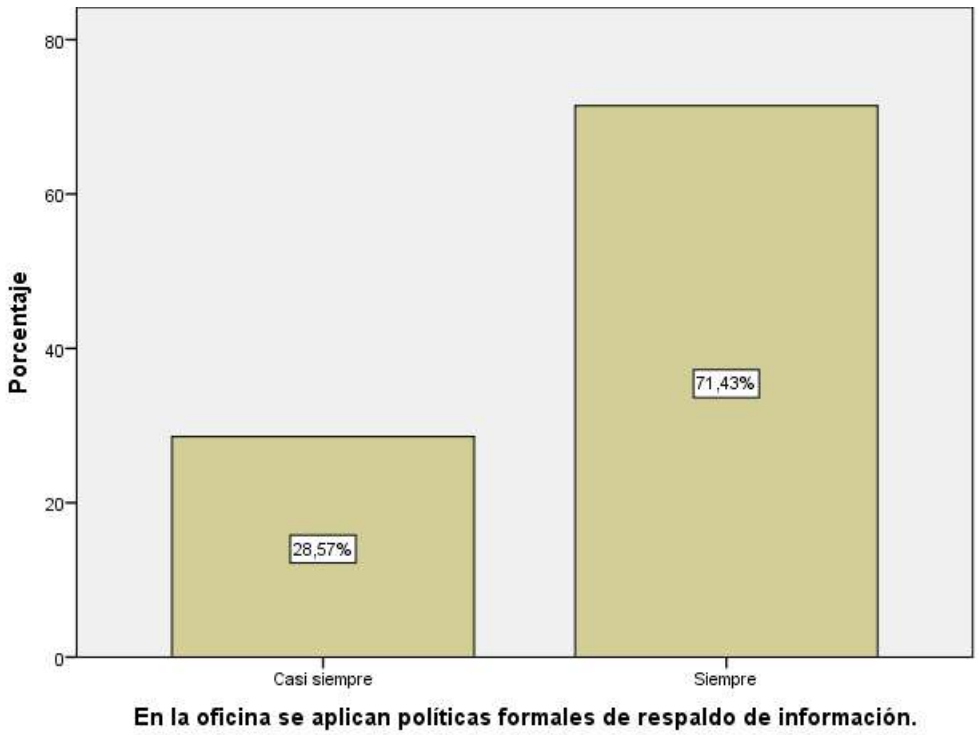
4.1. Análisis de resultados

4.1.1. Análisis de indicadores

Tabla 2. En la oficina se aplican políticas formales de respaldo de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	4	28,6	28,6	28,6
	Siempre	10	71,4	71,4	100,0
	Total	14	100,0	100,0	

Figura 1. En la oficina se aplican políticas formales de respaldo de información



De acuerdo con los resultados obtenidos, el 71.4% de los encuestados manifestó que siempre se aplican políticas formales de respaldo de información en la oficina de servicios informáticos, mientras que el 28.6% indicó que casi siempre se aplican dichas políticas.

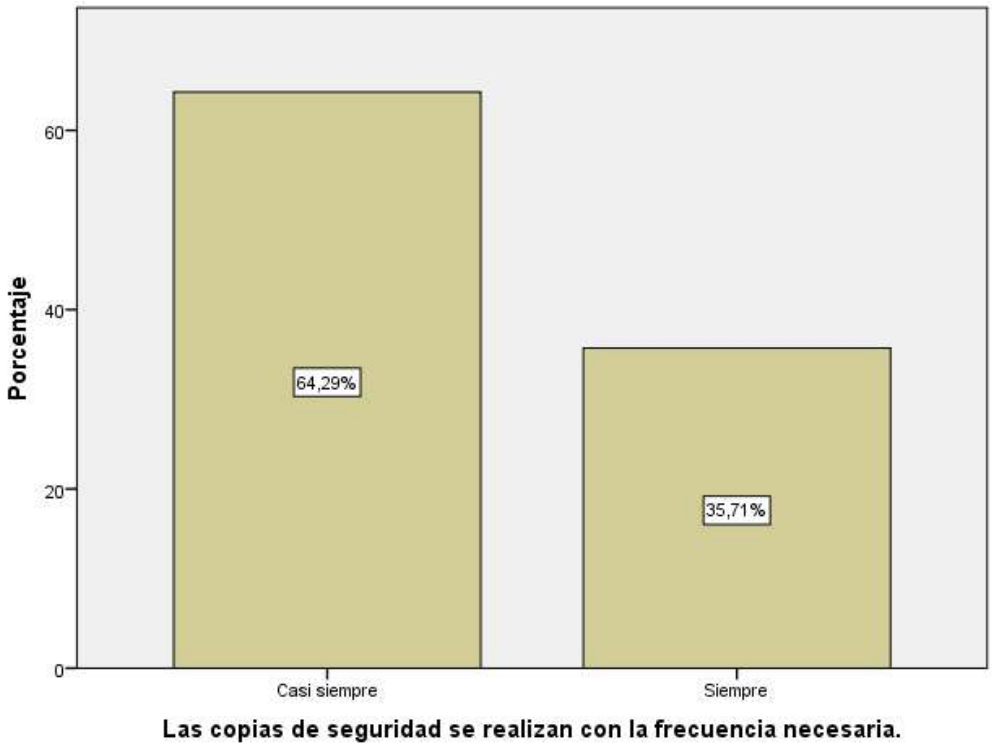
Estos resultados evidencian que la implementación de políticas de respaldo de información es una práctica consolidada dentro de la institución, lo que contribuye significativamente a la protección de los datos y a la prevención de pérdidas de información ante posibles fallos o incidentes.

En este sentido, la alta frecuencia en la aplicación de estas políticas refleja un adecuado nivel de gestión en la protección de datos, lo cual favorece la continuidad operativa de los servicios informáticos

Tabla 3. Las copias de seguridad se realizan con la frecuencia necesaria

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	9	64,3	64,3	64,3
	Siempre	5	35,7	35,7	100,0
	Total	14	100,0	100,0	

Figura 2, Las copias de seguridad se realizan con la frecuencia necesaria



De acuerdo con los resultados obtenidos, el 64.3% de los encuestados indicó que casi siempre se realizan copias de seguridad con la frecuencia necesaria, mientras que el 35.7% manifestó que siempre se llevan a cabo dichas actividades.

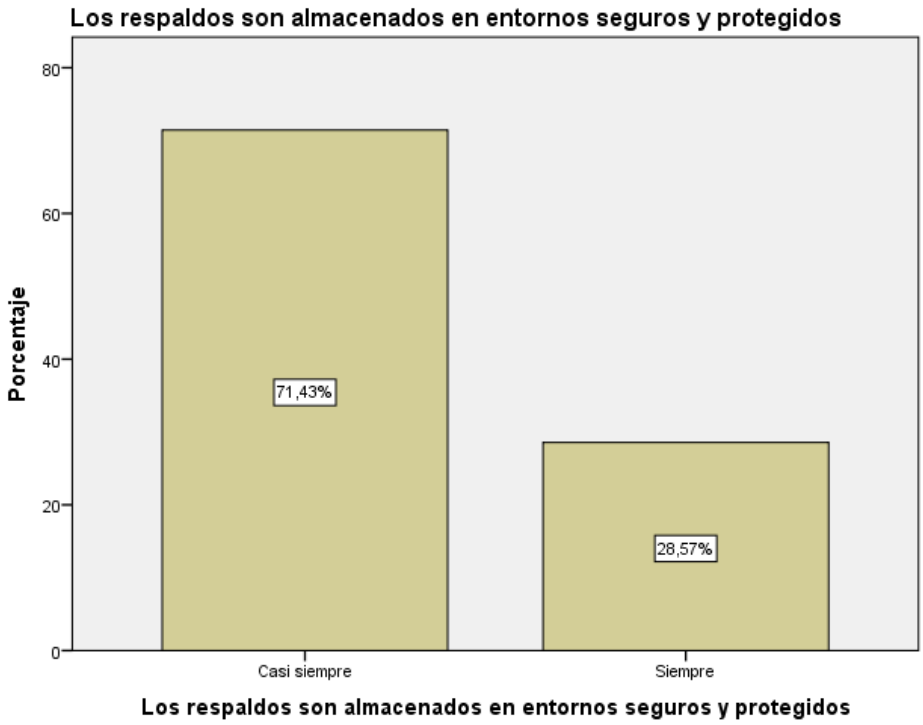
Estos resultados evidencian que, si bien existe una práctica frecuente en la realización de copias de seguridad dentro de la oficina de servicios informáticos, esta no se ejecuta de manera totalmente constante en todos los casos.

En este sentido, se observa que la institución mantiene un nivel adecuado en la gestión de respaldos de información; sin embargo, aún existen oportunidades de mejora para garantizar que esta actividad se realice siempre con la periodicidad requerida, fortaleciendo así la protección de los datos y la continuidad operativa de los servicios informáticos.

Tabla 4. Los respaldos son almacenados en entornos seguros y protegidos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	10	71,4	71,4	71,4
	Siempre	4	28,6	28,6	100,0
	Total	14	100,0	100,0	

Figura 3. Los respaldos son almacenados en entornos seguros y protegidos



De acuerdo con los resultados obtenidos, el 71.4% de los encuestados indicó que casi siempre los respaldos son almacenados en entornos seguros y protegidos, mientras que el 28.6% manifestó que siempre se realiza esta práctica.

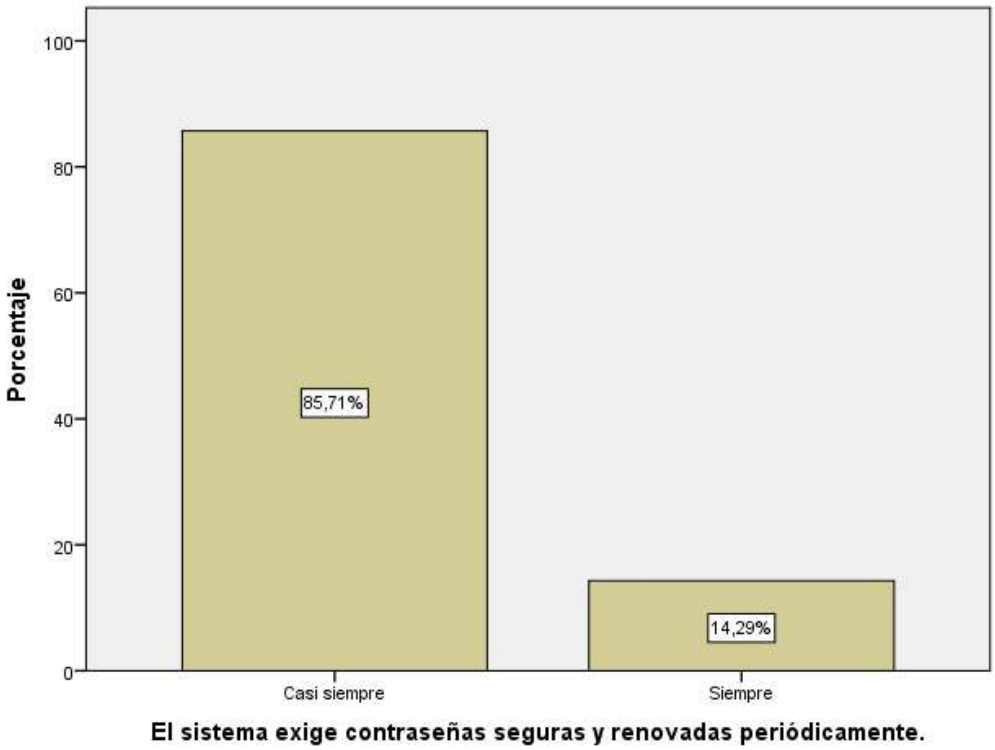
Estos resultados evidencian que el almacenamiento seguro de la información es una práctica frecuente dentro de la oficina de servicios informáticos; sin embargo, no se ejecuta de manera completamente constante en todos los casos.

En este sentido, se observa que la institución cuenta con mecanismos adecuados para la protección de los respaldos de información, aunque aún existen oportunidades de mejora para garantizar que esta práctica se realice siempre bajo condiciones óptimas de seguridad, lo cual es fundamental para asegurar la integridad de los datos y la continuidad operativa de los servicios informáticos.

Tabla 5. El sistema exige contraseñas seguras y renovadas periódicamente

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	12	85,7	85,7	85,7
	Siempre	2	14,3	14,3	100,0
	Total	14	100,0	100,0	

Figura 4. El sistema exige contraseñas seguras y renovadas periódicamente



De acuerdo con los resultados obtenidos, el 85.7% de los encuestados indicó que casi siempre el sistema exige contraseñas seguras y renovadas periódicamente, mientras que el 14.3% manifestó que siempre se cumple con esta exigencia.

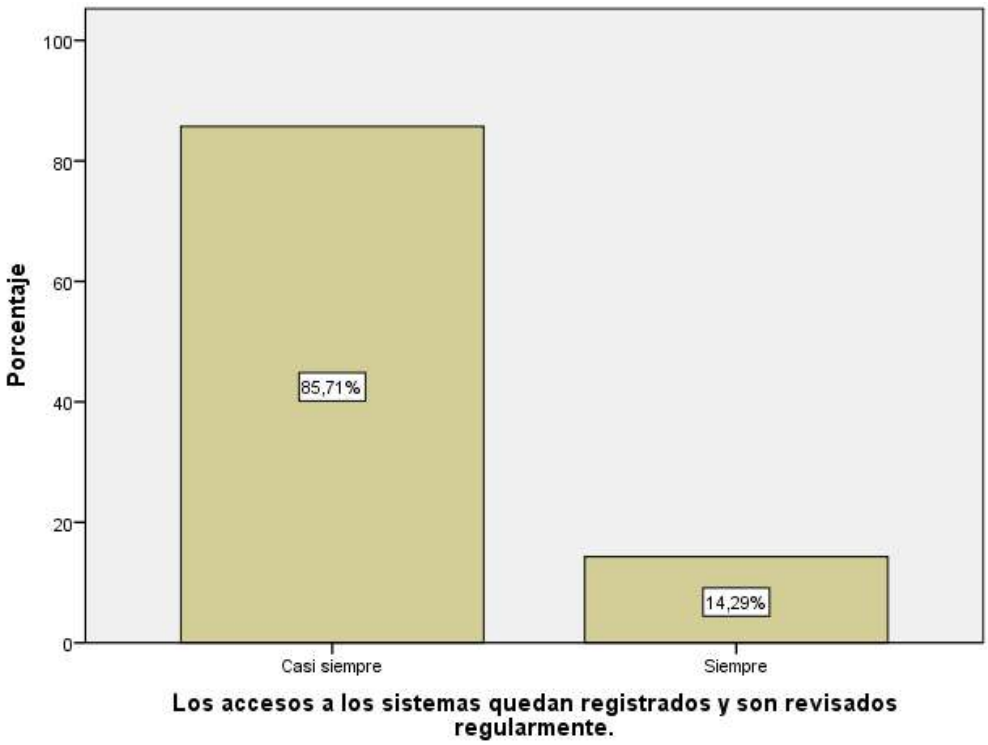
Estos resultados evidencian que el uso de contraseñas seguras y su actualización periódica es una práctica frecuente dentro de la oficina de servicios informáticos; sin embargo, no se aplica de manera totalmente constante en todos los casos.

En este sentido, se observa que la institución mantiene un nivel adecuado en la implementación de mecanismos de autenticación segura, lo cual contribuye a la protección de los sistemas y a la reducción de riesgos de accesos no autorizados. No obstante, es necesario fortalecer esta práctica para garantizar su cumplimiento permanente y así mejorar la seguridad de la información y la continuidad operativa de los servicios informáticos.

Tabla 6. Los accesos a los sistemas quedan registrados y son revisados regularmente

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	12	85,7	85,7	85,7
	Siempre	2	14,3	14,3	100,0
	Total	14	100,0	100,0	

Figura 5, Los accesos a los sistemas quedan registrados y son revisados regularmente



De acuerdo con los resultados obtenidos, el 85.7% de los encuestados indicó que casi siempre los accesos a los sistemas quedan registrados y son revisados regularmente, mientras que el 14.3% manifestó que siempre se realiza esta práctica.

Estos resultados evidencian que el registro y revisión de accesos es una actividad frecuente dentro de la oficina de servicios informáticos; sin embargo, no se ejecuta de manera totalmente constante en todos los casos.

En este sentido, se observa que la institución cuenta con mecanismos adecuados de monitoreo y control de accesos, lo cual contribuye a la identificación de actividades inusuales y al fortalecimiento de la seguridad de los sistemas. No obstante, es necesario reforzar esta práctica para garantizar su aplicación permanente, lo que permitirá mejorar la prevención de incidentes y asegurar la continuidad operativa de los servicios informáticos.

Tabla 7. Los roles y permisos de acceso se asignan correctamente según las funciones del personal

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	8	57,1	57,1	57,1
	Siempre	6	42,9	42,9	100,0
	Total	14	100,0	100,0	

Figura 6. Los roles y permisos de acceso se asignan correctamente según las funciones del personal



De acuerdo con los resultados obtenidos, el 57.1% de los encuestados indicó que casi siempre los roles y permisos de acceso se asignan correctamente según las funciones del personal, mientras que el 42.9% manifestó que siempre se realiza esta práctica.

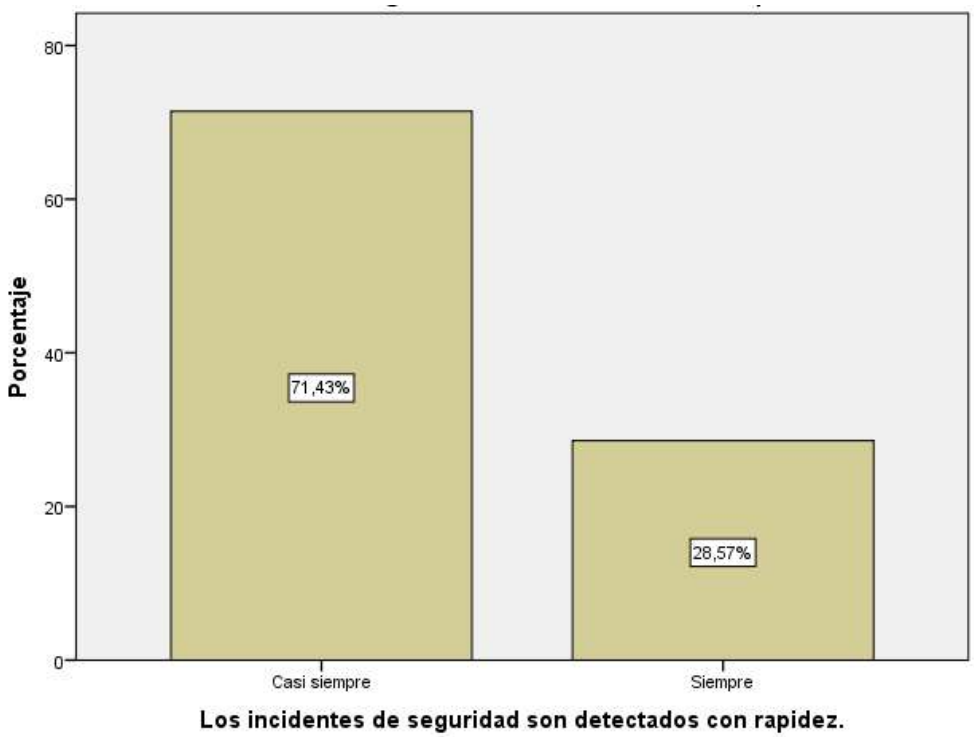
Estos resultados evidencian que la asignación de roles y permisos es una práctica frecuente y relativamente consolidada dentro de la oficina de servicios informáticos. Sin embargo, el hecho de que una proporción importante de encuestados indique "casi siempre" sugiere que aún existen situaciones en las que esta asignación no se realiza de manera totalmente adecuada.

En este sentido, se observa que la institución mantiene un nivel adecuado en la gestión de accesos, lo cual contribuye a la seguridad de los sistemas y a la prevención de accesos no autorizados. No obstante, es necesario fortalecer esta práctica para garantizar una asignación precisa y constante de permisos, lo que permitirá mejorar la protección de la información y la continuidad operativa de los servicios informáticos.

Tabla 8. Los incidentes de seguridad son detectados con rapidez

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	10	71,4	71,4	71,4
	Siempre	4	28,6	28,6	100,0
	Total	14	100,0	100,0	

Figura 7, Los incidentes de seguridad son detectados con rapidez



De acuerdo con los resultados obtenidos, el 71.4% de los encuestados indicó que casi siempre los incidentes de seguridad son detectados con rapidez, mientras que el 28.6% manifestó que siempre se realiza esta detección de manera oportuna.

Estos resultados evidencian que la detección de incidentes de seguridad es una práctica frecuente dentro de la oficina de servicios informáticos; sin embargo, no se ejecuta de forma completamente constante en todos los casos.

En este sentido, se observa que la institución cuenta con mecanismos adecuados para la identificación de incidentes, lo cual contribuye a reducir riesgos y minimizar impactos negativos en los sistemas. No obstante, es necesario fortalecer esta capacidad para garantizar una detección inmediata y permanente, lo que permitirá mejorar la seguridad de la información y la continuidad operativa de los servicios informáticos.

Tabla 9. La respuesta del personal técnico ante incidentes de seguridad es eficaz

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	10	71,4	71,4	71,4
	Siempre	4	28,6	28,6	100,0
	Total	14	100,0	100,0	

Figura 8. La respuesta del personal técnico ante incidentes de seguridad es eficaz



De acuerdo con los resultados obtenidos, el 71.4% de los encuestados indicó que casi siempre la respuesta del personal técnico ante incidentes de seguridad es eficaz, mientras que el 28.6% manifestó que siempre se brinda una respuesta efectiva.

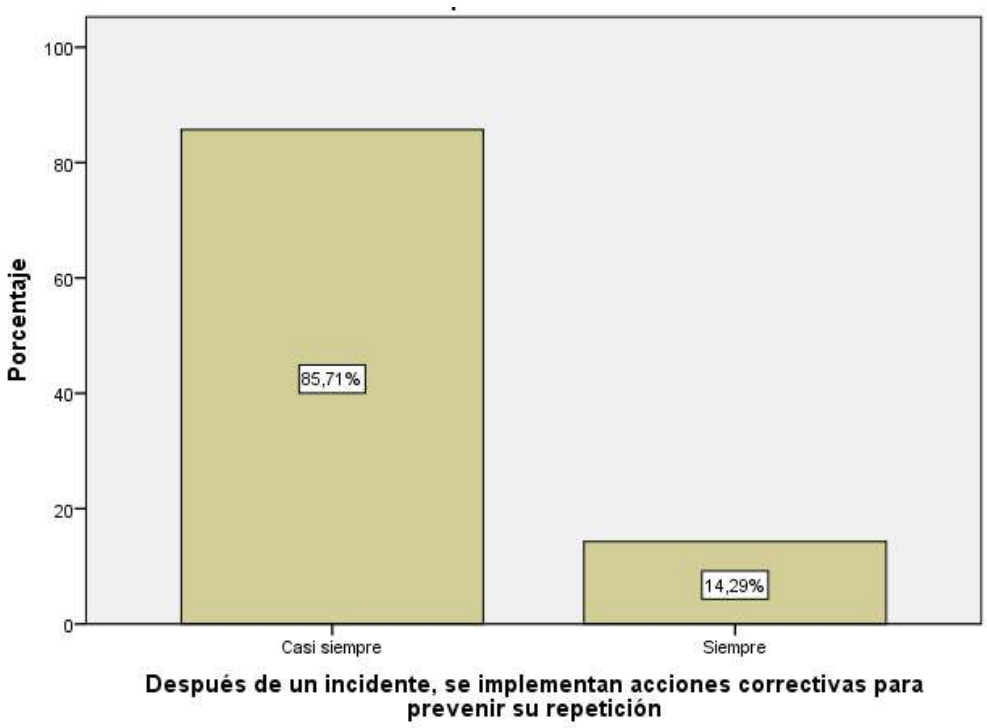
Estos resultados evidencian que la capacidad de respuesta del personal técnico es una práctica frecuente dentro de la oficina de servicios informáticos; sin embargo, no se ejecuta de manera completamente constante en todos los casos.

En este sentido, se observa que la institución cuenta con un nivel adecuado de preparación para atender incidentes de seguridad, lo cual contribuye a minimizar impactos y restablecer los servicios de manera oportuna. No obstante, es necesario fortalecer esta capacidad para garantizar respuestas rápidas y eficaces en todos los escenarios, mejorando así la seguridad de la información y la continuidad operativa de los servicios informáticos.

Tabla 10. Después de un incidente, se implementan acciones correctivas para prevenir su repetición

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	12	85,7	85,7	85,7
	Siempre	2	14,3	14,3	100,0
	Total	14	100,0	100,0	

Figura 9. Después de un incidente, se implementan acciones correctivas para prevenir su repetición



De acuerdo con los resultados obtenidos, el 85.7% de los encuestados indicó que casi siempre se implementan acciones correctivas después de un incidente para prevenir su repetición, mientras que el 14.3% manifestó que siempre se realizan dichas acciones.

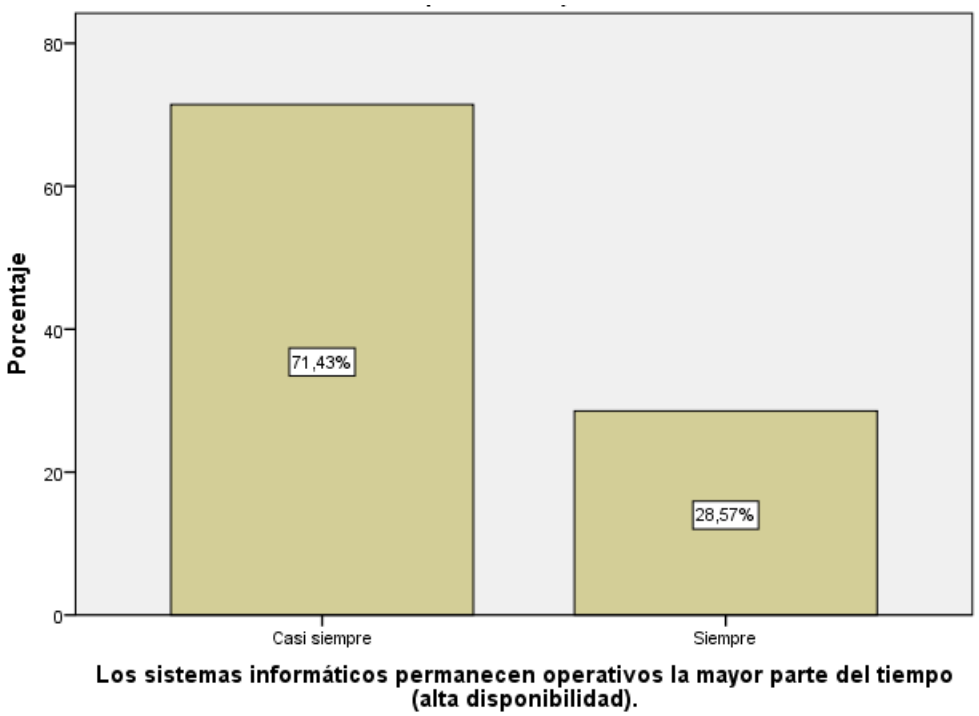
Estos resultados evidencian que la implementación de acciones correctivas es una práctica frecuente dentro de la oficina de servicios informáticos; sin embargo, no se ejecuta de manera totalmente constante en todos los casos.

En este sentido, se observa que la institución cuenta con una adecuada cultura de mejora continua frente a incidentes de seguridad, lo cual contribuye a reducir la probabilidad de recurrencia de fallos y fortalece la seguridad de los sistemas. No obstante, es necesario reforzar esta práctica para garantizar su aplicación permanente, lo que permitirá mejorar la gestión de incidentes y asegurar la continuidad operativa de los servicios informáticos.

Tabla 11. Los sistemas informáticos permanecen operativos la mayor parte del tiempo (alta disponibilidad).

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	10	71,4	71,4	71,4
	Siempre	4	28,6	28,6	100,0
	Total	14	100,0	100,0	

Figura 10. Los sistemas informáticos permanecen operativos la mayor parte del tiempo (alta disponibilidad).



De acuerdo con los resultados obtenidos, el 71.4% de los encuestados indicó que casi siempre los sistemas informáticos permanecen operativos la mayor parte del tiempo, mientras que el 28.6% manifestó que siempre se mantiene dicha operatividad.

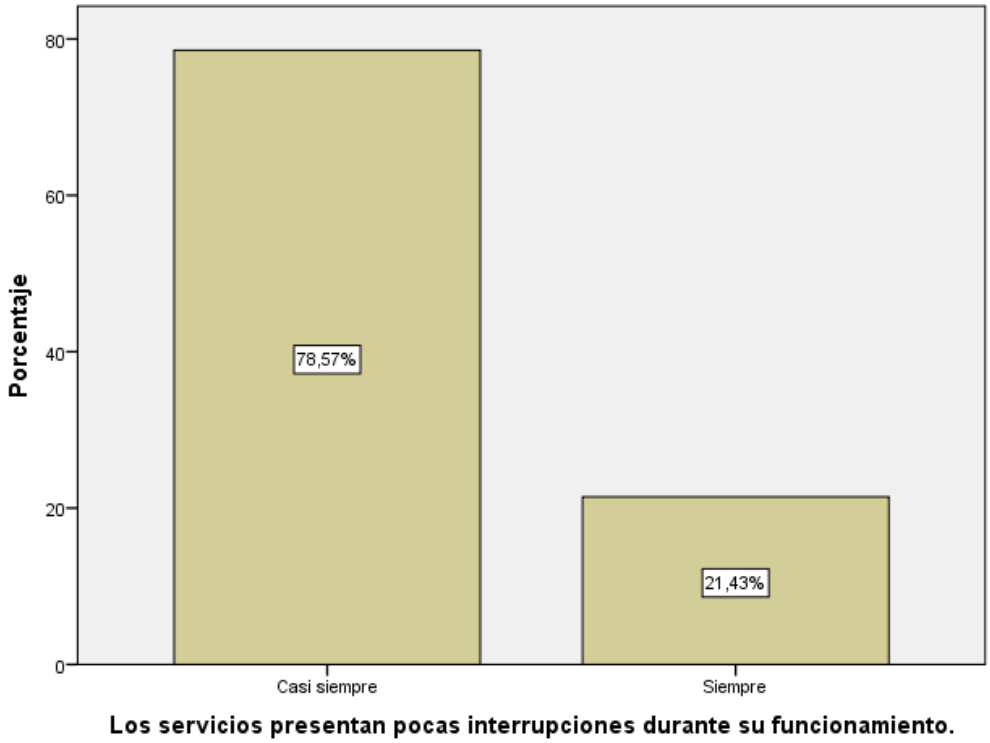
Estos resultados evidencian que la disponibilidad de los sistemas informáticos es una condición frecuente dentro de la oficina de servicios informáticos; sin embargo, no se garantiza de manera completamente constante en todos los casos.

En este sentido, se observa que la institución cuenta con un nivel adecuado de disponibilidad de sus sistemas, lo cual permite el desarrollo continuo de las actividades académicas y administrativas. No obstante, es necesario fortalecer los mecanismos de monitoreo, mantenimiento y prevención de fallas para asegurar una operatividad permanente, lo que contribuirá significativamente a la continuidad de los servicios informáticos.

Tabla 12. Los servicios presentan pocas interrupciones durante su funcionamiento

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	11	78,6	78,6	78,6
	Siempre	3	21,4	21,4	100,0
	Total	14	100,0	100,0	

Figura 11. Los servicios presentan pocas interrupciones durante su funcionamiento



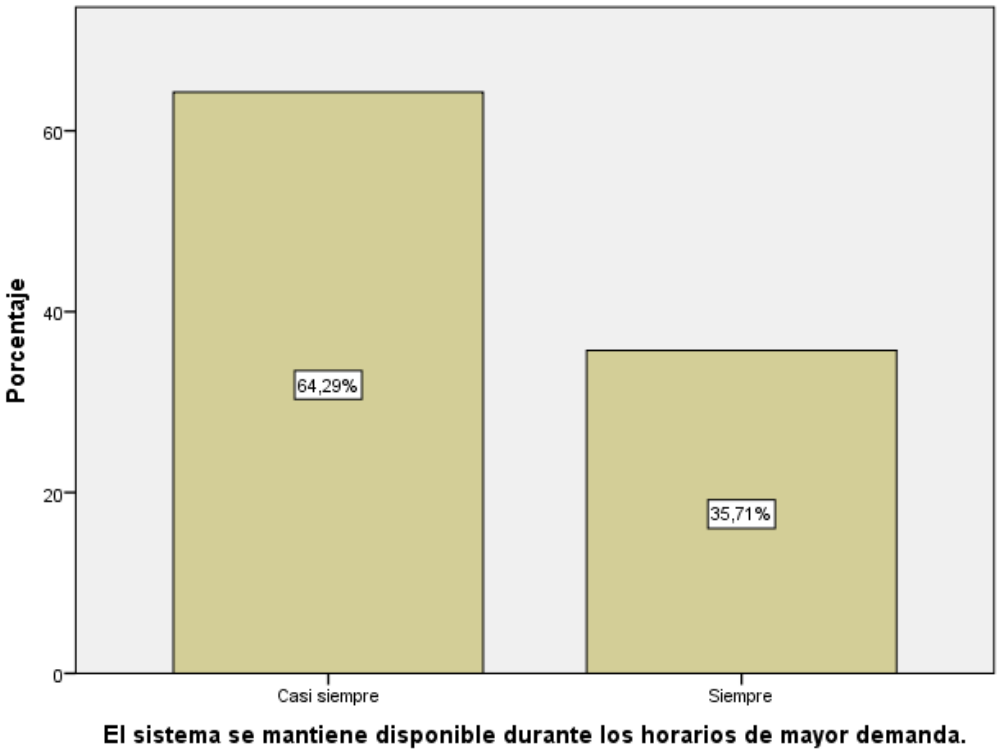
De acuerdo con los resultados obtenidos, el 78.6% de los encuestados indicó que casi siempre los servicios presentan pocas interrupciones durante su funcionamiento, mientras que el 21.4% manifestó que siempre se cumple esta condición.

Estos resultados evidencian que los servicios informáticos operan con un bajo nivel de interrupciones en la mayoría de los casos, lo cual refleja un adecuado desempeño en la gestión de la continuidad operativa. Sin embargo, el predominio de la opción "casi siempre" indica que aún se presentan interrupciones ocasionales que afectan la estabilidad del servicio. En este sentido, se observa que la institución mantiene un nivel aceptable de continuidad en sus servicios informáticos; no obstante, es necesario fortalecer los mecanismos de prevención y control de fallas para garantizar una operatividad constante y sin interrupciones, lo cual contribuirá a mejorar la disponibilidad y confiabilidad de los sistemas.

Tabla 13. El sistema se mantiene disponible durante los horarios de mayor demanda

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	9	64,3	64,3	64,3
	Siempre	5	35,7	35,7	100,0
	Total	14	100,0	100,0	

Figura 12. El sistema se mantiene disponible durante los horarios de mayor demanda



De acuerdo con los resultados obtenidos, el 64.3% de los encuestados indicó que casi siempre el sistema se mantiene disponible durante los horarios de mayor demanda, mientras que el 35.7% manifestó que siempre se garantiza dicha disponibilidad.

Estos resultados evidencian que, en la mayoría de los casos, los sistemas informáticos logran mantenerse operativos en momentos críticos de uso; sin embargo, no se asegura una disponibilidad total y constante en todos los escenarios.

En este sentido, se observa que la institución presenta un nivel adecuado de disponibilidad en horarios de alta demanda, lo cual permite el desarrollo de actividades académicas y administrativas. No obstante, es necesario fortalecer la capacidad de los sistemas para responder de manera eficiente en estos periodos críticos, mediante mejoras en infraestructura, monitoreo y gestión de recursos, con el fin de garantizar una continuidad operativa óptima.

4.2. Contrastación de hipótesis

Contrastación de la hipótesis específica 1

H_0: La protección de datos no se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

H_a: La protección de datos se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

			Protección de datos	Continuidad operativa
Rho de Spearman	Protección de datos	Coeficiente de correlación	1,000	,849**
		Sig. (bilateral)	.	,000
		N	14	14
	Continuidad operativa	Coeficiente de correlación	,849**	1,000
		Sig. (bilateral)	,000	.
		N	14	14

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

De acuerdo con los resultados obtenidos mediante el coeficiente de correlación de Spearman, se evidencia un valor de Rho = 0.849, lo que indica la existencia de una correlación positiva alta entre la protección de datos y la continuidad operativa de los servicios informáticos en la Universidad Nacional José Faustino Sánchez Carrión.

Asimismo, el nivel de significancia obtenido (p = 0.000) es menor al nivel de significancia establecido ($\alpha = 0.05$), lo que demuestra que la relación encontrada es estadísticamente significativa.

En consecuencia, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alternativa (H1), concluyendo que la protección de datos se relaciona significativamente con la continuidad operativa de los servicios informáticos.

Contrastación de la hipótesis específica 2

H_0: Los controles de accesos no se relacionan con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

Ha: Los controles de accesos se relacionan con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.

			Control de accesos	Continuidad operativa
Rho de Spearman	Control de accesos	Coeficiente de correlación	1,000	,548*
		Sig. (bilateral)	.	,043
		N	14	14
	Continuidad operativa	Coeficiente de correlación	,548*	1,000
		Sig. (bilateral)	,043	.
		N	14	14

*. La correlación es significativa en el nivel 0,05 (bilateral).

De acuerdo con los resultados obtenidos mediante el coeficiente de correlación de Spearman, se observa un valor de Rho = 0.548, lo que indica la existencia de una correlación positiva de nivel moderado entre el control de accesos y la continuidad operativa de los servicios informáticos en la Universidad Nacional José Faustino Sánchez Carrión.

Asimismo, el nivel de significancia obtenido (p = 0.043) es menor al nivel de significancia establecido (α = 0.05), lo que demuestra que la relación encontrada es estadísticamente significativa.

En consecuencia, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alternativa (H1), concluyendo que el control de accesos se relaciona significativamente con la continuidad operativa de los servicios informáticos.

Contrastación de la hipótesis específica 3

H_0: La gestión de incidentes no se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025

Ha: La gestión de incidentes se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025

			Gestión de incidentes	Continuidad operativa
Rho de Spearman	Gestión de incidentes	Coeficiente de correlación	1,000	,849**
		Sig. (bilateral)	.	,000
		N	14	14
	Continuidad operativa	Coeficiente de correlación	,849**	1,000
		Sig. (bilateral)	,000	.
		N	14	14

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

De acuerdo con los resultados obtenidos mediante el coeficiente de correlación de Spearman, se evidencia un valor de Rho = 0.849, lo que indica la existencia de una correlación positiva alta entre la gestión de incidentes y la continuidad operativa de los servicios informáticos en la Universidad Nacional José Faustino Sánchez Carrión.

Asimismo, el nivel de significancia obtenido (p = 0.000) es menor al nivel de significancia establecido (α = 0.05), lo que demuestra que la relación encontrada es estadísticamente significativa.

En consecuencia, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alternativa (H1), concluyendo que la gestión de incidentes se relaciona significativamente con la continuidad operativa de los servicios informáticos.

Contrastación de la hipótesis general

H_0: La seguridad de los sistemas de información no se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025

Ha: La seguridad de los sistemas de información se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025

			Seguridad de los sistemas de información	Continuidad operativa
Rho de Spearman	Seguridad de los sistemas de información	Coeficiente de correlación	1,000	,849**
		Sig. (bilateral)	.	,000
		N	14	14
	Continuidad operativa	Coeficiente de correlación	,849**	1,000
		Sig. (bilateral)	,000	.
		N	14	14

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

De acuerdo con los resultados obtenidos mediante el coeficiente de correlación de Spearman, se evidencia un valor de Rho = 0.849, lo que indica la existencia de una correlación positiva alta entre la seguridad de los sistemas de información y la continuidad operativa de los servicios informáticos en la Universidad Nacional José Faustino Sánchez Carrión.

Asimismo, el nivel de significancia obtenido (p = 0.000) es menor al nivel de significancia establecido (α = 0.05), lo que demuestra que la relación encontrada es estadísticamente significativa.

En consecuencia, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alternativa (H1), concluyendo que la seguridad de los sistemas de información se relaciona significativamente con la continuidad operativa de los servicios informáticos.

CAPITULO V
DISCUSION

5.1. Discusión de resultados

Los resultados obtenidos en la presente investigación evidencian la existencia de una relación significativa entre la seguridad de los sistemas de información y la continuidad operativa de los servicios informáticos en la Universidad Nacional José Faustino Sánchez Carrión, lo cual coincide con el objetivo general planteado en el estudio .

En primer lugar, respecto a la hipótesis general, se encontró una correlación positiva alta (Rho = 0.849; p = 0.000), lo que demuestra que a mayor nivel de seguridad en los sistemas de información, mayor es la continuidad operativa de los servicios informáticos. Este resultado es coherente con lo planteado por el World Economic Forum (2025), donde se señala que existe una relación directa entre la madurez en ciberseguridad y la capacidad de recuperación y continuidad de las operaciones. Asimismo, coincide con lo señalado por Sanchez Estupiñan (2023), quien encontró una alta correlación entre la seguridad de la información y la calidad del servicio en entornos universitarios.

En relación con la hipótesis específica 1, los resultados evidenciaron una correlación positiva alta entre la protección de datos y la continuidad operativa (Rho = 0.849; p = 0.000). Este hallazgo indica que prácticas como la implementación de políticas de respaldo, la frecuencia de copias de seguridad y el almacenamiento seguro de la información contribuyen significativamente a la estabilidad de los servicios informáticos. Estos resultados son consistentes con lo señalado por Whitman y Mattord (2022), quienes destacan que la protección de la información es un componente esencial para garantizar la disponibilidad de los sistemas. Asimismo, se

relaciona con lo propuesto por Alqahtani y Kavakli-Thorne (2024), quienes enfatizan que la prevención y protección de datos reducen significativamente las interrupciones operativas.

Respecto a la hipótesis específica 2, se obtuvo una correlación positiva moderada (Rho = 0.548; p = 0.043) entre el control de accesos y la continuidad operativa. Este resultado sugiere que, aunque los mecanismos de autenticación, registro de accesos y gestión de permisos influyen en la continuidad de los servicios, su impacto es menor en comparación con otras dimensiones como la protección de datos o la gestión de incidentes. Esto puede explicarse porque el control de accesos actúa principalmente como una medida preventiva, cuyo efecto en la continuidad operativa es indirecto. Sin embargo, estos resultados coinciden con lo planteado por ISACA (2022), donde se indica que una adecuada gestión de accesos reduce riesgos de intrusión y contribuye a la estabilidad de los sistemas.

En cuanto a la hipótesis específica 3, se identificó una correlación positiva alta (Rho = 0.849; p = 0.000) entre la gestión de incidentes y la continuidad operativa. Este resultado demuestra que la capacidad de detectar, responder y aplicar acciones correctivas frente a incidentes tiene un impacto directo en la continuidad de los servicios informáticos. Este hallazgo es consistente con lo señalado por NIST (2024), quien destaca que la resiliencia organizacional depende en gran medida de la capacidad de respuesta ante eventos adversos. Asimismo, coincide con Jooda (2025), quien evidenció que las organizaciones con mejores prácticas de gestión de incidentes presentan tiempos de recuperación más rápidos y menores interrupciones.

Desde el análisis descriptivo, se observó que la mayoría de los indicadores presentan una tendencia predominante en la categoría “casi siempre”, lo que evidencia que las prácticas de seguridad y continuidad operativa son frecuentes, pero no

completamente consolidadas. Este comportamiento sugiere que la institución cuenta con una base adecuada en la gestión de seguridad, pero aún existen oportunidades de mejora para alcanzar un nivel óptimo de desempeño.

Por ejemplo, en la dimensión protección de datos, si bien se aplican políticas de respaldo de manera constante, la frecuencia de copias de seguridad y el almacenamiento seguro aún presentan variabilidad. En la dimensión control de accesos, aunque existen mecanismos de autenticación y monitoreo, su aplicación no es totalmente uniforme. Asimismo, en la dimensión gestión de incidentes, la detección y respuesta son adecuadas, pero requieren mayor estandarización para garantizar su eficacia en todos los casos.

En cuanto a la variable dependiente, los resultados muestran que la continuidad operativa presenta un nivel adecuado, evidenciado en la alta disponibilidad de los sistemas, la baja frecuencia de interrupciones y la capacidad de funcionamiento en horarios críticos. Sin embargo, la predominancia de respuestas en “casi siempre” indica que aún existen fallas ocasionales que afectan la estabilidad del servicio.

En síntesis, los resultados confirman que la seguridad de los sistemas de información es un factor determinante para la continuidad operativa de los servicios informáticos. No obstante, también evidencian que la institución se encuentra en un nivel intermedio de madurez, donde las prácticas existen y funcionan, pero requieren ser fortalecidas, estandarizadas y optimizadas para garantizar un desempeño continuo, seguro y confiable.

CAPITULO VI
CONCLUSIONES Y ECOMENDACIONES

6.1. Conclusiones

Los resultados obtenidos en la presente investigación evidencian la existencia de una relación significativa entre la seguridad de los sistemas de información y la continuidad operativa de los servicios informáticos en la Universidad Nacional José Faustino Sánchez Carrión, lo cual coincide con el objetivo general planteado en el estudio .

En primer lugar, respecto a la hipótesis general, se encontró una correlación positiva alta (Rho = 0.849; p = 0.000), lo que demuestra que a mayor nivel de seguridad en los sistemas de información, mayor es la continuidad operativa de los servicios informáticos. Este resultado es coherente con lo planteado por el World Economic Forum (2025), donde se señala que existe una relación directa entre la madurez en ciberseguridad y la capacidad de recuperación y continuidad de las operaciones. Asimismo, coincide con lo señalado por Sanchez Estupiñan (2023), quien encontró una alta correlación entre la seguridad de la información y la calidad del servicio en entornos universitarios.

En relación con la hipótesis específica 1, los resultados evidenciaron una correlación positiva alta entre la protección de datos y la continuidad operativa (Rho = 0.849; p = 0.000). Este hallazgo indica que prácticas como la implementación de políticas de respaldo, la frecuencia de copias de seguridad y el almacenamiento seguro de la información contribuyen significativamente a la estabilidad de los servicios informáticos. Estos resultados son consistentes con lo señalado por Whitman y Mattord (2022), quienes destacan que la protección de la información es un componente esencial para garantizar la disponibilidad de los sistemas. Asimismo, se

relaciona con lo propuesto por Alqahtani y Kavakli-Thorne (2024), quienes enfatizan que la prevención y protección de datos reducen significativamente las interrupciones operativas.

Respecto a la hipótesis específica 2, se obtuvo una correlación positiva moderada (Rho = 0.548; p = 0.043) entre el control de accesos y la continuidad operativa. Este resultado sugiere que, aunque los mecanismos de autenticación, registro de accesos y gestión de permisos influyen en la continuidad de los servicios, su impacto es menor en comparación con otras dimensiones como la protección de datos o la gestión de incidentes. Esto puede explicarse porque el control de accesos actúa principalmente como una medida preventiva, cuyo efecto en la continuidad operativa es indirecto. Sin embargo, estos resultados coinciden con lo planteado por ISACA (2022), donde se indica que una adecuada gestión de accesos reduce riesgos de intrusión y contribuye a la estabilidad de los sistemas.

En cuanto a la hipótesis específica 3, se identificó una correlación positiva alta (Rho = 0.849; p = 0.000) entre la gestión de incidentes y la continuidad operativa. Este resultado demuestra que la capacidad de detectar, responder y aplicar acciones correctivas frente a incidentes tiene un impacto directo en la continuidad de los servicios informáticos. Este hallazgo es consistente con lo señalado por NIST (2024), quien destaca que la resiliencia organizacional depende en gran medida de la capacidad de respuesta ante eventos adversos. Asimismo, coincide con Jooda (2025), quien evidenció que las organizaciones con mejores prácticas de gestión de incidentes presentan tiempos de recuperación más rápidos y menores interrupciones.

Desde el análisis descriptivo, se observó que la mayoría de los indicadores presentan una tendencia predominante en la categoría “casi siempre”, lo que evidencia que las prácticas de seguridad y continuidad operativa son frecuentes, pero no

completamente consolidadas. Este comportamiento sugiere que la institución cuenta con una base adecuada en la gestión de seguridad, pero aún existen oportunidades de mejora para alcanzar un nivel óptimo de desempeño.

Por ejemplo, en la dimensión protección de datos, si bien se aplican políticas de respaldo de manera constante, la frecuencia de copias de seguridad y el almacenamiento seguro aún presentan variabilidad. En la dimensión control de accesos, aunque existen mecanismos de autenticación y monitoreo, su aplicación no es totalmente uniforme. Asimismo, en la dimensión gestión de incidentes, la detección y respuesta son adecuadas, pero requieren mayor estandarización para garantizar su eficacia en todos los casos.

En cuanto a la variable dependiente, los resultados muestran que la continuidad operativa presenta un nivel adecuado, evidenciado en la alta disponibilidad de los sistemas, la baja frecuencia de interrupciones y la capacidad de funcionamiento en horarios críticos. Sin embargo, la predominancia de respuestas en “casi siempre” indica que aún existen fallas ocasionales que afectan la estabilidad del servicio.

En síntesis, los resultados confirman que la seguridad de los sistemas de información es un factor determinante para la continuidad operativa de los servicios informáticos. No obstante, también evidencian que la institución se encuentra en un nivel intermedio de madurez, donde las prácticas existen y funcionan, pero requieren ser fortalecidas, estandarizadas y optimizadas para garantizar un desempeño continuo, seguro y confiable

6.2. Recomendaciones

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que integre políticas, procedimientos y controles de seguridad, con el fin de fortalecer de manera integral la seguridad de los sistemas de información y garantizar la continuidad operativa de los servicios informáticos.

Fortalecer la protección de datos mediante la automatización de copias de seguridad, el establecimiento de políticas obligatorias de respaldo y el uso de entornos de almacenamiento seguros, asegurando la disponibilidad y recuperación de la información ante posibles incidentes.

Optimizar el control de accesos implementando políticas más estrictas de autenticación, como el uso de contraseñas robustas, autenticación multifactor (MFA) y auditorías periódicas de accesos, con el propósito de reducir vulnerabilidades y mejorar la seguridad de los sistemas.

Implementar un plan formal de gestión de incidentes de seguridad, que incluya protocolos de detección, respuesta y acciones correctivas, así como capacitaciones continuas al personal técnico, con el fin de mejorar la capacidad de respuesta y asegurar la continuidad operativa de los servicios informáticos.

CAPITULO VII
REFERENCIAS

Espinoza, H. (2023). *Implementación de un sistema web para el proceso de ventas de la empresa Via Data Consulting.* Universidad Nacional José Faustino Sánchez Carrión, Huacho.

Galdós, F. (2020). *Propuesta d implementación de un sistema de caja para mejorar la administración de la información en la oficina de tesorería del gobierno regional de Lima.* Universidad Nacional José Faustino Sánchez Carrión, Huacho.

Gallardo, J. (2020). *Propuesta de implementación de un sistema de registro de visitas para mejorar el control de ingreso de las personas que realzian trámites en las sedes del gobierno regional de LIma.* Universidad Nacional José Faustino Sánchez Carrión, Huachi.

Institute, P. M. (2021). Guía de los fundamentos para la dirección de proyectos. Newtown Square, Pennsylvania, , Estados Unidos: Project Management Institute.

Lledó, P., & Rivarola, G. (2007). Gestión de proyectos. México, México: Pearson Educación.

Maldonado, J. (2018). Gestión de proyectos. Málaga, España: Universidad de Málaga.

Mateus, C. (2004). *Desarrollo de aplicaciones web.* Catalunya: Fundació per a la Universitat Oberta de Catalunya.

Meza, A. (2024). Metodología ágil Scrum y su incidencia en la gestión de proyectos de edificación en empresas constructoras - Lima, 2024. Lima, Perú: Universidad Cesar Vallejo.

Moreno, N., Sánchez, L., & Velosa, J. (2018). Introducción a la gerencia de proyectos. Bogotá, Colombia: Ediciones EAN.

Palomino, E. (2024). Metodología scrum en la gestión de proyectos de tecnologías de información en una entidad financiera Lima 2024. Lima, Perú: Universidad Cesar Vallejo.

Ríos, M. (2019). *Propuesta de un sistema de control de gestión para la universidad de la Serena area de pregrado.* Universidad de Chile, Santiago.

Riquelme, D., Galaz, E., & Aros, M. (2004). *Guía para desarrollo de sitios web.* Santiago-Chile: ADROS impresores.

Rojas, V. (2020). FAF: Marco de trabajo ágil y formal, para el desarrollo de software en el colegio de México. México, México: Infotec centro de investigación e innovación en tecnologías de la información y comunicación.

Untuña, L. (2021). *Implementación de la metodología PACIE en la plataforma Moodle de la policía metropolitana de Quita.* Universidad Israel, Quito-Ecuador.

Wallace, W. (2014). Gestión de proyectos. Edimburgo, Reino Unido: Edinburgh Business School, Heriot-Watt University.

Yáñez, A. (2021). *Sistema web con Framework libre para la optimización de procesos de información en florícolas.* Universidad Técnica de CotopaXI, Latacunga-Euador.

ANEXO 01

MATRIZ DE CONSISTENCIA

Seguridad de los sistemas de información y su relación con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES – INDICAD.	METODOLOGIA
Problema Principal: ¿Cómo la seguridad de los sistemas de información se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025?	Objetivo General: Determinar de qué manera la seguridad de los sistemas de información se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.	Hipótesis Central: La seguridad de los sistemas de información se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.	Variable 1: Seguridad de los sistemas de información Dimensiones Protección de datos • Políticas de respaldo implementadas • Frecuencia de copias de seguridad • Almacenamiento seguro de la información Control de accesos • Uso de contraseñas seguras • Registros de accesos • Gestión de permisos y roles de usuario Gestión de incidentes • Tiempo de detección de ataques • Respuesta ante incidentes • Implementación de acciones correctivas Variable 2: Continuidad operativa Dimensiones Disponibilidad • Tiempo de funcionamiento (uptime) • Frecuencia de interrupciones • Disponibilidad durante horas críticas Recuperación • Tiempo de restauración tras incidentes • Aplicación del plan de contingencia • Recuperación total de datos y servicios afectados Resiliencia operativa • Capacidad del sistema para resistir ataques o fallos. • Adaptación del sistema frente a cambios o amenazas • Implementación de mejoras preventivas luego de incidentes	Población: 14 personas Muestra: 14 personas Metodología de investigación Diseño: No experimental de carácter transeccional. Tipo de investigación: Aplicada Nivel: Correccional Enfoque: Cuantitativo Instrumento: Mediante encuesta. Cuestionario de encuesta tipo Likert de 12 preguntas.
Problemas Específicos: a) ¿Cómo la protección de datos se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025? b) ¿Cómo los controles de accesos se relacionan con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025? c) ¿Cómo la gestión de incidentes se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025?	Objetivos Específicos: a) Determinar de qué manera la protección de datos se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025. b) Determinar de qué manera los controles de accesos se relacionan con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025. c) Determinar de qué manera la gestión de incidentes se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.	Hipótesis Específicos: a) La protección de datos se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025. b) Los controles de accesos se relacionan con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025. c) La gestión de incidentes se relaciona con la continuidad operativa de los servicios informáticos de la universidad nacional José Faustino Sánchez Carrión, 2025.		

ANEXO 02

CUESTIONARIO

CUESTIONARIO

"Seguridad de los sistemas de información y su relación con la continuidad operativa de los servicios informáticos de la Universidad Nacional José Faustino Sánchez Carrión"

Instrucciones:
Marque con una "X" la alternativa que mejor represente su opinión.

1 = Nunca, 2 = Casi nunca, 3 = A veces, 4 = Casi siempre, 5 = Siempre

Nro	Enunciado	1	2	3	4	5
	Dimensión: Protección de datos					
01	En la oficina se aplican políticas formales de respaldo de información.					
02	Las copias de seguridad se realizan con la frecuencia necesaria.					
03	Los respaldos son almacenados en entornos seguros y protegidos					
	Dimensión: Control de accesos					
04	El sistema exige contraseñas seguras y renovadas periódicamente.					
05	Los accesos a los sistemas quedan registrados y son revisados regularmente.					
06	Los roles y permisos de acceso se asignan correctamente según las funciones del personal					
	Dimensión: Gestión de incidentes					
07	Los incidentes de seguridad son detectados con rapidez.					
08	La respuesta del personal técnico ante incidentes de seguridad es eficaz.					
09	Después de un incidente, se implementan acciones correctivas para prevenir su repetición					
	Dimensión: Disponibilidad					
10	Los sistemas informáticos permanecen operativos la mayor parte del tiempo (alta disponibilidad).					
11	Los servicios presentan pocas interrupciones durante su funcionamiento.					
12	El sistema se mantiene disponible durante los horarios de mayor demanda.					
	Dimensión: Recuperación					

13	Los servicios informáticos se restauran en tiempos adecuados después de un incidente.					
14	El plan de contingencia se activa correctamente ante fallas o ataques.					
15	La recuperación de datos y servicios después de un incidente es completa y confiable					
	Dimensión: Resiliencia operativa					
16	Los sistemas mantienen un funcionamiento básico aun cuando ocurre un incidente.					
17	El sistema se adapta adecuadamente frente a fallas para continuar operando.					
18	Después de incidentes pasados, se aplican mejoras que fortalecen el sistema					

ANEXO 03

VALIDACION DE JUICIO DE EXPERTOS

VALIDACIÓN DEL INSTRUMENTO

Universidad Nacional
José Faustino Sánchez Carrión

VALIDACIÓN CON JUICIO DE EXPERTO: ENCUESTA GENERAL.

TEMA: SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y SU RELACIÓN CON LA CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS DE LA UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN, 2025

OPINIÓN Ó JUICIO DE EXPERTO:

1. La opinión que Ud. nos brinde es Personal, Sincera y Anónima.
2. Marque con un aspa " **X** " dentro del cuadrado de Valoración, solo una vez por cada criterio, el que Ud. Considere su opinión.

1 = Muy Malo **2 = Malo** **3 = Regular** **4 = Bueno** **5 = Muy Bueno**

CRITERIOS	VALORACIÓN				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.					X
Objetividad: Esta expresado en conductas observables.					X
Actualidad: Adecuado al avance de la ciencia y la tecnología.					X
Organización: Existe una organización lógica.				X	
Suficiencia: Comprende los aspectos de cantidad y calidad.				X	
Intencionalidad: Adecuado para conocer las opiniones de las encuestadas.					X
Consistencia: Basados en aspectos teóricos científicos de organización.					X
Coherencia: Establece coherencia entre las variables y los indicadores.					X
Metodología: La estrategia responde a los propósitos del estudio.					X
Pertinencia: El instrumento es adecuado al tipo de investigación.					X

Muchas Gracias por su Respuesta.

Mo CRISTINA PILAR DAMIAN ESPINOZA

VALIDACIÓN DEL INSTRUMENTO

Universidad Nacional
José Faustino Sánchez Carrión

VALIDACIÓN CON JUICIO DE EXPERTO: ENCUESTA GENERAL.

TEMA: SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y SU RELACIÓN CON LA CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS DE LA UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN, 2025

OPINIÓN Ó JUICIO DE EXPERTO:

1. La opinión que Ud. nos brinde es Personal, Sincera y Anónima.
2. Marque con un aspa "**X**" dentro del cuadrado de Valoración, solo una vez por cada criterio, el que Ud. Considere su opinión.

1 = Muy Malo 2 = Malo 3 = Regular 4 = Bueno 5 = Muy Bueno

CRITERIOS	VALORACIÓN				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.					X
Objetividad: Esta expresado en conductas observables.				X	
Actualidad: Adecuado al avance de la ciencia y la tecnología.				X	
Organización: Existe una organización lógica.					X
Suficiencia: Comprende los aspectos de cantidad y calidad.				X	
Intencionalidad: Adecuado para conocer las opiniones de las encuestadas.				X	
Consistencia: Basados en aspectos teóricos científicos de organización.					X
Coherencia: Establece coherencia entre las variables y los indicadores.					X
Metodología: La estrategia responde a los propósitos del estudio.					X
Pertinencia: El instrumento es adecuado al tipo de investigación.					X

Muchas Gracias por su Respuesta.

Mo. JORGE ANTONIO SANCHEZ GUZMAN

VALIDACIÓN DEL INSTRUMENTO

Universidad Nacional
José Faustino Sánchez Carrión

VALIDACIÓN CON JUICIO DE EXPERTO: ENCUESTA GENERAL.

TEMA: SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y SU RELACIÓN CON LA CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS DE LA UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN, 2025;

OPINIÓN Ó JUICIO DE EXPERTO:

1. La opinión que Ud. nos brinde es Personal, Sincera y Anónima.
2. Marque con un aspa " **X** " dentro del cuadrado de Valoración, solo una vez por cada criterio, el que Ud. Considere su opinión.

1 = Muy Malo **2 = Malo** **3 = Regular** **4 = Bueno** **5 = Muy Bueno**

CRITERIOS	VALORACIÓN				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.				X	
Objetividad: Esta expresado en conductas observables.					X
Actualidad: Adecuado al avance de la ciencia y la tecnología.					X
Organización: Existe una organización lógica.					X
Suficiencia: Comprende los aspectos de cantidad y calidad.					X
Intencionalidad: Adecuado para conocer las opiniones de las encuestadas.				X	
Consistencia: Basados en aspectos teóricos científicos de organización.					X
Coherencia: Establece coherencia entre las variables y los indicadores.				X	
Metodología: La estrategia responde a los propósitos del estudio.				X	
Pertinencia: El instrumento es adecuado al tipo de investigación.					X

Muchas Gracias por su Respuesta.

Mo RONALD DEMETRIO FLORES FLORES

CALCULO DE COEFICIENTE DE VALIDEZ

CRITERIOS	JUECES			TOTAL
	J1	J2	J3	
CLARIDAD	5	5	4	14
OBJETIVIDAD	5	4	5	14
ACTUALIDAD	5	4	5	14
ORGANIZACIÓN	4	5	5	14
SUFICIENCIA	4	4	5	13
INTENCIONALIDAD	5	4	4	13
CONSISTENCIA	5	5	5	15
COHERENCIA	5	5	4	15
METODOLOGIA	5	5	4	14
PRTINENCIA	5	5	5	15
TOTAL OPINION	48	46	46	140

$$\text{Validez} = \frac{\text{Total de Opinión}}{\text{Total Máximo}}$$

Total Máximo = (Nº criterios) x (Nº de Jueces) x (Puntaje Máximo de Respuesta).

TOTAL DE OPINION	140
TOTAL MAXINO	150
COEFICIENTE DE VALIDEZ	**93%**

ANEXO 04

COEFICIENTE DE CONFIABILIDAD

Persona	ITEMS (PREGUNTAS)																		Total
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	
1	5	4	4	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	85
2	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	73
3	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	73
4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	73
5	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	73
6	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	73
7	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	73
8	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	73
9	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	73
10	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	90
11	4	5	4	4	4	5	4	4	4	4	4	5	4	4	5	5	5	4	78
12	4	5	5	4	4	5	4	4	4	5	4	5	5	5	5	5	5	4	82
13	4	5	5	4	4	5	5	5	4	5	5	5	5	5	5	5	5	5	86
14	4	5	5	4	4	5	5	5	4	5	5	5	5	5	5	5	5	5	86
Varianza–j	0,22	0,25	0,22	0,13	0,13	0,26	0,22	0,22	0,13	0,22	0,18	0,25	0,25	0,25	0,26	0,26	0,26	0,22	**41.3**
Total=	**3.93**																		

$$\alpha = \frac{n}{n-1} \times \frac{S^2 - \sum Si^2}{S^2}$$

Donde:

- α = Coeficiente de Confiabilidad.
- n = Número de Items (preguntas).
- S^2 = Varianza del Total de prueba.
- $\sum Si^2$ = Suma de Varianzas de Items.

Si (suma varianzas items) = 3.93

S (varianza del total de filas) = 41.3

n (número de Items) = 18

Alpha de Cronbach = 0.96