

# **UNIVERSIDAD NACIONAL DEL CALLAO**

**FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**



**“SEGURIDAD DE LA INFORMACIÓN APLICANDO EL ISO  
27001:2013 PARA LA UNIDAD DE REGISTROS Y ARCHIVOS  
ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DEL CALLAO  
- 2023”**

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE  
INGENIERO DE SISTEMAS**

**AUTORES:**

**MUÑOZ LIÑÁN, AUGUSTO JESÚS**

**ROLDAN ALBINAGORTA, BRUNO RODRIGO**

**KOLEVIC AGUAYO, ALEXANDER GUILLERMO**

**ASESOR: DR. TORRE CAMONES ANIVAL ALFREDO**

**LÍNEA DE INVESTIGACIÓN: SISTEMAS DE INFORMACIÓN**

**Callao, 2024**

**PERÚ**

# 3A, MUÑOZ LIÑAN, ROLDAN ALBINAGORTA, KOLEVIC AGUAYO-TESIS PREGRADO-2024

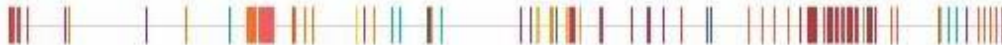


Nombre del documento: 3A, MUÑOZ LIÑAN, ROLDAN ALBINAGORTA, KOLEVIC AGUAYO-TESIS PREGRADO-2024.docx  
 ID del documento: 07a3b75947c58230659953a79b60857633bd85f  
 Tamaño del documento original: 6.5125 kB

Depositante: FIS PREGRADO UNIDAD DE INVESTIGACION  
 Fecha de depósito: 22/5/2024  
 Tipo de carga: interface  
 fecha de fin de análisis: 22/5/2024

Número de palabras: 3758  
 Número de caracteres: 65.877

Ubicación de las similitudes en el documento



## Fuentes de similitudes

### Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	<b>1A, NUÑEZ ZEGARRA, VILLEGAS PACHCO, FLORES HUANCA-TESIS PREGRADO-2024.docx</b> El documento proviene de mi biblioteca de referencias. 27 fuentes similares	3%		Palabras idénticas: 36 (317 palabras)
2	<b>repositorio.usac.edu.pe</b> <a href="http://repositorio.usac.edu.pe/bitstream/20.500.12952/127/1/Valverde%20Reyes,%20TITULO%20SISTEMAS%20de%20Gesti...">http://repositorio.usac.edu.pe/bitstream/20.500.12952/127/1/Valverde Reyes, TITULO SISTEMAS de Gesti...</a> 88 fuentes similares	3%		Palabras idénticas: 36 (378 palabras)
3	<b>www.rndalyc.org</b> <a href="https://www.rndalyc.org/bit/1/1614831006.pdf">https://www.rndalyc.org/bit/1/1614831006.pdf</a> 1 fuente similar	2%		Palabras idénticas: 24 (185 palabras)
4	<b>Documento de otro usuario</b> El documento proviene de otro grupo. 3 fuentes similares	1%		Palabras idénticas: 14 (128 palabras)
5	<b>www.acefio.org.mx</b>   <a href="https://www.acefio.org.mx/informacion-de-nuestros-y-nuestras-paises-federaciones-de-los-estados-unidos-mexico">información de nuestros y nuestras países federaciones de los estados unidos mexico</a> <a href="https://www.acefio.org.mx/informacion-de-nuestros-y-nuestras-paises-federaciones-de-los-estados-unidos-mexico">https://www.acefio.org.mx/informacion-de-nuestros-y-nuestras-paises-federaciones-de-los-estados-unidos-mexico</a> 1 fuente similar	1%		Palabras idénticas: 14 (174 palabras)

### Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	<b>Documento de otro usuario</b> El documento proviene de otro grupo.	< 1%		Palabras idénticas: 4 (140 palabras)
2	<b>repositorio.ufdech.edu.pe</b> <a href="https://repositorio.ufdech.edu.pe/bitstream/20.500.13032/2796/1/COMUNICACION%20GESTION%20DE%20SERVICIOS%20AL%20USUARIO%20EN%20UNIVERSIDADES%20PUBLICAS%20DE%20PERU.pdf">https://repositorio.ufdech.edu.pe/bitstream/20.500.13032/2796/1/COMUNICACION_GESTION_...</a>	< 1%		Palabras idénticas: 4 (142 palabras)
3	<b>1A, VARGAS VALENZUELA, SALAS MENDOZA-TESIS PREGRADO-2024.docx</b> El documento proviene de mi biblioteca de referencias.	< 1%		Palabras idénticas: 4 (123 palabras)
4	<b>Documento de otro usuario</b> El documento proviene de otro grupo.	< 1%		Palabras idénticas: 4 (124 palabras)
5	<b>repositorio.ufdech.edu.pe</b> <a href="http://repositorio.ufdech.edu.pe/bitstream/20.500.13032/2796/1/COMUNICACION%20GESTION%20DE%20SERVICIOS%20AL%20USUARIO%20EN%20UNIVERSIDADES%20PUBLICAS%20DE%20PERU.pdf">http://repositorio.ufdech.edu.pe/bitstream/20.500.13032/2796/1/COMUNICACION_GESTION_...</a>	< 1%		Palabras idénticas: 4 (124 palabras)

## **INFORMACIÓN BÁSICA**

FACULTAD: FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS

UNIDAD DE INVESTIGACIÓN DE FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS

TÍTULO: "SEGURIDAD DE LA INFORMACIÓN APLICANDO EL ISO 27001:2013 PARA LA OFICINA DE REGISTROS Y ARCHIVOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DEL CALLAO"

### **AUTORES:**

Muñoz Liñán, Augusto Jesús DNI 74026341 ORCID 0009-0005-2628-7147

Roldan Albinagorta, Bruno Rodrigo DNI 72734137ORCID 0009-0006-1243-5636

Kolevic Aguayo, Alexander Guillermo DNI 74284686 ORCID 0009-0003-0119-9648

### **ASESOR:**

Torre Camones Anival Alfredo DNI 06607141 ORCID 0000-0002-7392-8884

LUGAR DE EJECUCIÓN: OFICINA DE REGISTROS Y ARCHIVOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DEL CALLAO

UNIDAD DE ANÁLISIS: 25 participantes de la URA

TIPO DE INVESTIGACIÓN: INVESTIGACIÓN APLICADA

ENFOQUE DE INVESTIGACIÓN: INVESTIGACIÓN CUANTITATIVA

DISEÑO DE INVESTIGACIÓN: INVESTIGACIÓN EXPERIMENTAL

TIPO OCDE: SISTEMAS DE INFORMACIÓN

## HOJA DE REFERENCIA Y APROBACIÓN DEL JURADO



# ACTA DE SUSTENTACIÓN



LIBRO 001 FOLIO N° 41 ACTA DE SUSTENTACIÓN DE TESIS  
N° 026-UIFIS-UNAC DEL 14.06.2024  
ACTA DE SUSTENTACION POR LA MODALIDAD: SIN CICLO TALLER DE TESIS  
PARA LA OBTENCIÓN DEL TÍTULO PROFESIONAL DE  
INGENIERO DE SISTEMAS


Siendo las 13:30 horas del día Viernes 14 de junio del año 2024, reunidos en el auditorio de la Facultad de Ingeniería Industrial y de Sistemas; el **JURADO DE SUSTENTACIÓN** de la tesis titulada: "**SEGURIDAD DE LA INFORMACIÓN APLICANDO EL ISO 27001:2013 PARA LA UNIDAD DE REGISTROS Y ARCHIVOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DEL CALLAO-2023**", presentada por los Bachilleres **MUÑOZ LIÑÁN AUGUSTO JESÚS, ROLDAN ALBINAGORTA BRUNO RODRIGO** y **KOLEVIC AGUAYO ALEXANDER GUILLERMO**; para la obtención del título profesional de **INGENIERO DE SISTEMAS** en la Facultad de **INGENIERÍA INDUSTRIAL Y DE SISTEMAS DE LA UNIVERSIDAD NACIONAL DEL CALLAO**; en concordancia a la Resolución Decanal N° 184-2024-D-FIIS de fecha 30 de mayo del 2024, el Jurado de Sustentación está conformado por los siguientes Docentes Ordinarios de la Universidad Nacional del Callao:


<b>PRÉSIDENTE</b>	Dr. VILCAPUMA MALPICA HERNAN MARIO
<b>SECRETARIO</b>	Mg. GRADOS ESPINOZA HERBERT JUNIOR
<b>VOCAL</b>	Mg. CASAZOLA CRUZ OSWALDO DANIEL
<b>SUPLENTE</b>	Mg. RAMOS CHOQUEHUANCA ANGELINO ABAD
<b>ASESOR</b>	Dr. TORRE CAMONES ANIVAL ALFREDO

Con el quórum reglamentario de ley y de conformidad con lo establecido por el Reglamento de Grados y Títulos vigente según resolución de consejo universitario N°150-2023-CU de fecha 15 de junio del 2023, se dio inicio al acto de sustentación de los bachilleres quienes han cumplido con los requisitos para optar el Título Profesional de **INGENIERO DE SISTEMAS**. Sustentaron la tesis titulada: "**SEGURIDAD DE LA INFORMACIÓN APLICANDO EL ISO 27001:2013 PARA LA UNIDAD DE REGISTROS Y ARCHIVOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DEL CALLAO-2023**". Cumpliendo con la sustentación en Acto Público, de manera presencial en el Auditorio de la Facultad de Ingeniería Industrial y de Sistemas.

Luego de la exposición, y la absolución de las preguntas formuladas por el jurado y efectuadas las deliberaciones pertinentes, el **JURADO DE SUSTENTACIÓN** acordó: Dar por **APROBADO** con la escala de calificación cualitativa **BUENA** y calificación cuantitativa **15** la presente tesis, conforme a lo dispuesto en el Art. 27 del Reglamento de Grados y Títulos de la UNAC, aprobado por Resolución de Consejo Universitario N° 150-2023-CU del 15 de junio del 2023.

Se dio por concluida la Sesión a las **14:30** horas del día 14 de junio del 2024.

  
Dr. VILCAPUMA MALPICA HERNAN MARIO  
Presidente

  
Mg. GRADOS ESPINOZA HERBERT JUNIOR  
Secretario

  
Mg. CASAZOLA CRUZ OSWALDO DANIEL  
Vocal

## **DEDICATORIA**

A nuestros padres que han sabido formarnos con buenos hábitos, sentimientos y valores; los cuales nos ayudan a seguir adelante en cada objetivo que nos planteamos y a todos los profesores que nos brindaron el camino del conocimiento, gracias a nuestros asesores y compañeros que nos apoyaron.

## **AGRADECIMIENTO**

Agradecer a Dios, por las bendiciones que nos sigue brindando, y por las veces que quisimos parar y nos mantuvo firme para lograr nuestras metas, también a nuestras familias que gracias a su apoyo constante siempre pudimos completar los objetivos en nuestros estudios.

## ÍNDICE

<b>RESUMEN</b>	6
<b>ABSTRACT</b>	7
<b>I. PLANTEAMIENTO DEL PROBLEMA</b>	8
1.1 Descripción de la realidad problemática	8
1.2 Formulación del problema	11
1.3 Objetivos	11
1.4 Justificación	12
1.5 Delimitantes	12
<b>II. MARCO TEÓRICO</b>	14
2.1 Antecedentes	14
2.2 Bases Teóricas	12
2.2 Marco Conceptual	20
2.3 Definiciones de términos básicos	46
<b>III. VARIABLES E HIPÓTESIS</b>	49
3.1 Hipótesis	49
3.2 Operacionalización de variable	49
<b>IV. METODOLOGÍA</b>	51
4.1 Diseño metodológico	51
4.2 Método de investigación	51
4.3 Población y muestra	52
4.4 Lugar de estudio y periodo de desarrollo	52
4.5 Técnicas e instrumentos de recolección de la información	53
4.6 Análisis y procesamiento de datos	54
4.7 Aspectos éticos en la investigación	54
<b>V. RESULTADOS</b>	58
5.1 Resultados Descriptivos	59
5.2 Resultados Inferenciales	63
5.3 Otro tipo de resultado	52
<b>VI. DISCUSIÓN DE RESULTADOS</b>	88
6.1 Contrastación y demostración de la hipótesis con los resultados	52
6.2 Contrastación de los resultados con otros estudios similares	52
6.3 Responsabilidad ética de acuerdo a los reglamentos vigentes	52
<b>VII. CONCLUSIONES</b>	91
<b>VIII. RECOMENDACIONES</b>	92
<b>IX. REFERENCIAS BIBLIOGRÁFICAS</b>	93
<b>ANEXOS</b>	96

· <b>Matriz de consistencia</b>	96
· <b>Instrumentos validados</b>	96
· <b>Consentimiento informado en caso de ser necesario</b>	96
· <b>Base de datos</b>	96



## INTRODUCCIÓN

La seguridad de los datos es un aspecto fundamental en la gestión de datos y registros en todas las organizaciones, especialmente en instituciones educativas como la Universidad Nacional del Callao. La protección de datos académicos y administrativos es esencial para garantizar la confidencialidad, integridad y disponibilidad de los datos y para cumplir con los requisitos de las leyes y regulaciones aplicables.

En este contexto, la norma ISO 27001:2013 se presenta como una referencia internacional un marco para crear, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI) en una organización. La implementación de este estándar en los archivos académicos y archivos de la Universidad Nacional del Callao puede fortalecer significativamente la seguridad de la información y reducir los riesgos asociados a posibles amenazas y vulnerabilidades.

El propósito de este estudio es desarrollar la seguridad de la información. plan basado en la norma ISO 27001:2013 de Registros Académicos de la Universidad Nacional de Calais. Para ello se realiza un análisis de la situación actual de seguridad de la información de la oficina, en el que se identifican los activos de información, las amenazas y vulnerabilidades, así como los requisitos legales y reglamentarios aplicables.

A continuación un SGSI conforme a ISO 27001: 2013, incluida la definición de seguridad. políticas y procedimientos, realizando análisis de riesgos, implementando medidas de control de seguridad y realizando auditorías

internas y externas para garantizar el cumplimiento de los requisitos establecidos. .

## RESUMEN

Las ciencias aplicadas permite que los procesos mejoren, y por ello las universidades pueden enfrentar desafíos en la modernización de sus infraestructuras tecnológicas, lo que puede dejarlas más vulnerables a ataques, la falta de regulaciones específicas o estándares de seguridad puede dejar a las instituciones académicas más susceptibles a riesgos de seguridad de la información, en la investigación aplicada pretendió conocer cómo mejora la seguridad de la información de la Unidad de Registros Académicos aplicando la ISO 27001:2013, se trabajó con una población de 25 personas, logrando los siguientes resultados que la seguridad de la información mejora significativamente en 42.4% gracias a la ISO 27001:2013, concluyendo que la ISO 27001:2013 mejora significativamente la Seguridad de la Información, además influye significativamente en la integridad, confidencialidad, disponibilidad de la seguridad de la información de la Unidad de Registros Académicos de la Universidad Nacional del Callao.

## ABSTRACT

Applied sciences allow processes to improve, and therefore universities can face challenges in modernizing their technological infrastructures, which can leave them more vulnerable to attacks, the lack of specific regulations or security standards can leave academic institutions more susceptible to information security risks, in the applied research titled Information Security applying ISO 27001:2013 for the academic records and archives office of the National University of Callao, the objective was to know how security is improved of the information from the Academic Records and Archive Office applying ISO 27001:2013, we worked with a population of 25 people, achieving the following results that information security improves significantly by 42.4% thanks to ISO 27001:2013, concluding that ISO 27001:2013 significantly improves Information Security, and also significantly influences the confidentiality, availability and integrity of the information security of the Academic Records Office of the National University of Callao.

## I. PLANTEAMIENTO DEL PROBLEMA

### 1.1. Determinación del problema

La seguridad de la información en los registros académicos universitarios es un tema crucial en la era digital, ya que la información personal y educativa de los estudiantes, profesores y personal administrativo está en riesgo debido a diversas amenazas cibernéticas. **A nivel mundial**, cada vez más, las universidades enfrentan ataques de hackers y ciberdelincuentes que intentan acceder a información confidencial, como datos personales, calificaciones, y registros financieros, la falta de medidas de seguridad adecuadas ha llevado a brechas de seguridad en universidades de renombre, exponiendo información sensible y comprometiendo la confianza de los estudiantes y profesores, muchas instituciones académicas utilizan sistemas de gestión de registros antiguos y desactualizados que pueden presentar vulnerabilidades de seguridad.(1)

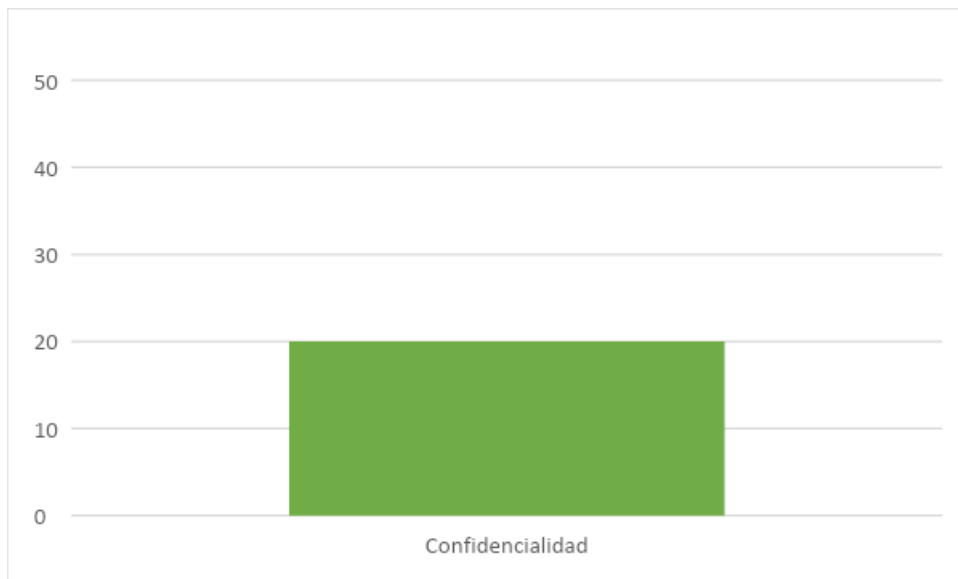
En algunos países **de América Latina**, las universidades pueden enfrentar desafíos en la modernización de sus infraestructuras tecnológicas, lo que puede dejarlas más vulnerables a ataques, la falta de regulaciones específicas o estándares de seguridad puede dejar a las instituciones académicas más susceptibles a riesgos de seguridad de la información, aunque hay esfuerzos por mejorar la seguridad de la información, las regulaciones en el ámbito de la protección de datos pueden estar aún en desarrollo, lo que podría dejar lagunas en la protección de la información en registros académicos.(2)

**En nuestro país**, existe una necesidad de crear mayor conciencia sobre la importancia de la seguridad de la información en las universidades peruanas, tanto a nivel de gestión como entre los usuarios finales.(3)

La Universidad Nacional del Callao tiene a su cargo la Unidad de Archivo General, la cual tiene la tarea de organizar, administrar y preservar el acervo documental de la UNAC como un sistema de archivo institucional, conformado por 11 facultades que conforman la institución siguiendo los actuales procedimientos técnicos-archivísticos; que trabaja conjuntamente con la Unidad de Registros Académicos; La Universidad Nacional del Callao se encuentra abocada al buen funcionamiento del fondo documental del Archivo General de la UNAC lo que demuestra que es limitado. No encontramos medidas preventivas, medidas de respuesta y sistemas técnicos que permitan seguridad y protección en la Oficina del Archivo Académico debido a la incertidumbre sobre la seguridad de los fondos documentales. Hay evidencia de posibles atacantes que pudieron acceder al sistema y robar datos de esta unidad. Durante la entrevista realizada en la URA se comprobaron cuestiones de confidencialidad, integridad y disponibilidad.

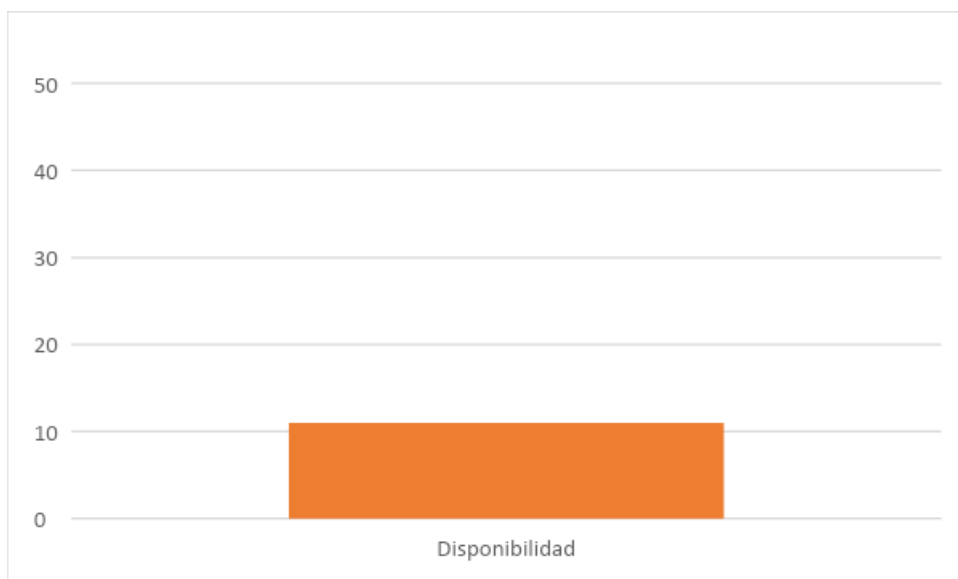
Para ello se trabajó un cuestionario que permita conocer la problemática de la inseguridad de información en el ámbito de su gestión para determinar las posibles incidencias en esta investigación

Figura 1. Evidencia de Confidencialidad de información URA



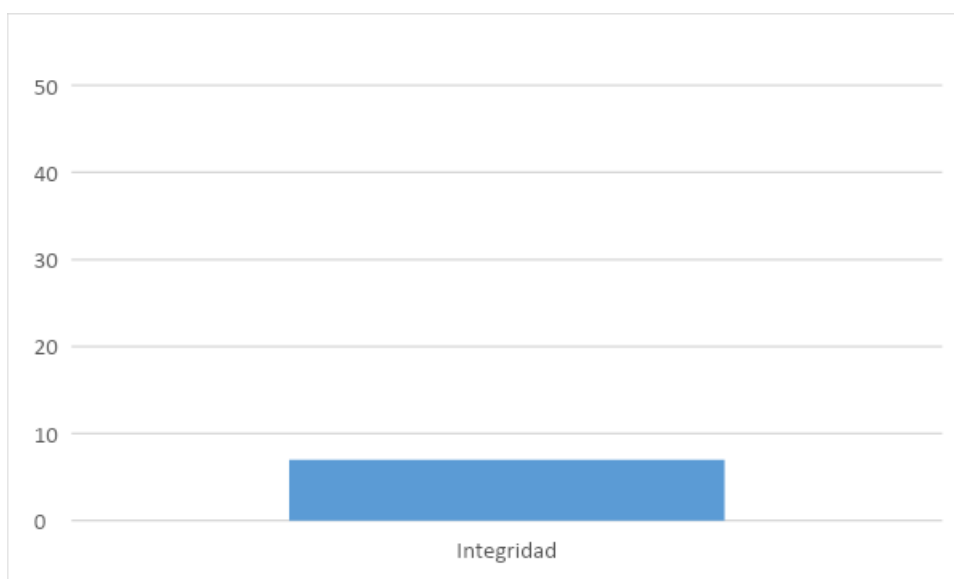
Fuente propia.

Figura 2. Evidencia de Disponibilidad de información -URA



Fuente propia.

Figura 3. Evidencia de Integridad de Información URA



Fuente propia.

## 1.2. Formulación del problema

### Problema general

PG: ¿Aplicando la ISO 27001:2013 cómo la Unidad de Registros Académicos mejora la seguridad de la información de la Unidad de Registros Académicos?

### Problemas específicos

PE1 ¿La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión confidencialidad de la seguridad de la información?

PE2 ¿La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión disponibilidad de la seguridad de la información?



PE3 ¿La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión integridad de la seguridad de la información?

### **1.3. Objetivos de la investigación**

#### **Objetivo general**

**OG:** Mejorar la seguridad de la información de la Unidad de Registros Académicos aplicando la ISO 27001:2013

#### **Objetivos específicos**

OE1 Relacionar la ISO 27001:2013 con la Unidad de Registros Académicos en la dimensión confidencialidad de la seguridad de la información

OE2: Relacionar la ISO 27001:2013 con la Unidad de Registros Académicos en la dimensión disponibilidad de la seguridad de la información

OE3: Relacionar la ISO 27001:2013 con la Unidad de Registros Académicos en la dimensión integridad de la seguridad de la información

### **1.4. Justificación**

#### **Justificación Tecnológica:**

La oficina de expedientes y archivos académicos de la UNAC implementará basada en la norma ISO 27001:2013 sistema de gestión de seguridad de la información. La confidencialidad, integridad y disponibilidad de la información estará asegurada por el conjunto de

controles y prácticas recomendadas que establece la norma ISO 27001:2013

**Justificación Legal:**

La Universidad Nacional del Callao podrá cumplir con las leyes y regulaciones aplicables en materia de protección de datos y seguridad de la información como resultado de la implementación de un SGSI. Existen leyes y regulaciones que exigen que las organizaciones protejan adecuadamente la información personal y sensible en muchos países, y la aplicación de la norma ISO 27001:2013 es una medida eficaz para cumplir con estos requisitos.

**Justificación Teórica:**

La oficina de expedientes y archivos académicos de la UNAC se basa en principios de buenas prácticas de seguridad de la información aceptados internacionalmente. El estándar se basa en el ciclo de mejora continua Planificar-Hacer-Verificar-Actuar (PDCA), que garantiza que el SGSI se mantenga actualizado y se ajuste a los cambios en el entorno de seguridad de la información.

**Justificación Institucional:**

La Universidad Nacional del Callao se dedica a proteger la información académica y administrativa. Este compromiso institucional y el hecho de que la universidad se toma en serio la seguridad de la información quedan demostrados con la

implementación de un SGSI. La reputación y la imagen de la universidad se pueden mejorar mediante la implementación de la norma ISO 27001: 2013, que resulta beneficiosa para atraer y retener a estudiantes y personal talentosos.

## **1.5 Delimitantes de la investigación**

### **Delimitante teórica**

De acuerdo a la investigación que se realizará tenemos limitantes en cuanto a la búsqueda de información específica en bibliotecas especializadas por contar con escasos recursos que permitan mayor información.

### **Delimitante espacial**

Se establecerá dentro del espacio de trabajo de la unidad de registros académicos que nos permitirá seguir con los procedimientos de la investigación.

### **Delimitante temporal**

Se trabajó un cronograma de actividades de 05 meses para la elaboración de la investigación en su totalidad.

## II. MARCO TEÓRICO

### 2.1. Antecedentes del estudio

Smith, J. (2019). En su tesis titulada *Implementation of ISO 27001:2013 in Small and Medium Enterprises*. University of Oxford; tuvo como Objetivo General: Evaluar la efectividad de la implementación de ISO 27001:2013 en pequeñas y medianas empresas (PYMEs), contando con una población: 50 PYMEs en el Reino Unido; con un tipo de Investigación: Estudio de caso cualitativo. Presentado los resultados: La implementación mejoró significativamente la gestión de riesgos y la conciencia sobre la seguridad de la información, con las siguientes conclusiones: La adopción de ISO 27001:2013 es viable y beneficiosa para las PYMEs, aumentando la confianza de los clientes y la seguridad interna.

Wang, L. (2020). En su tesis titulada *Assessing the Impact of ISO 27001:2013 on Organizational Performance*. Tsinghua University; tuvo como Objetivo General: Investigar el impacto de la certificación ISO 27001:2013 en el rendimiento organizacional, contando con una población: 100 empresas tecnológicas en China; con un tipo de Investigación: Cuantitativa, mediante encuestas. Presentado los resultados: Las empresas certificadas mostraron una mejora del 25% en la eficiencia operativa, con las siguientes conclusiones: La certificación no solo fortalece la seguridad de la información, sino que también mejora el rendimiento general de la organización.

Garcia, M. (2021). En su tesis titulada Challenges in Implementing ISO 27001:2013 in Public Sector Organizations. University of Sao Paulo; tuvo como Objetivo General: Identificar los desafíos en la implementación de ISO 27001:2013 en el sector público, contando con una población: 30 agencias gubernamentales en Brasil; con un tipo de Investigación: Estudio cualitativo. Presentado los resultados: Los principales desafíos incluyen la resistencia al cambio y la falta de recursos, con las siguientes conclusiones: La formación y el apoyo gubernamental son esenciales para una implementación exitosa.

Rahman, A. (2019). En su tesis titulada The Role of ISO 27001:2013 in Enhancing Cybersecurity in Financial Institutions. National University of Singapore; tuvo como Objetivo General: Evaluar cómo ISO 27001:2013 mejora la ciberseguridad en instituciones financieras, contando con una población: 20 bancos en Singapur; con un tipo de Investigación: Mixta, cualitativa y cuantitativa. Presentado los resultados: Reducción del 30% en incidentes de seguridad tras la implementación, con las siguientes conclusiones: La norma es altamente efectiva en fortalecer las defensas cibernéticas de los bancos.

Brown, D. (2020). En su tesis titulada ISO 27001:2013 and its Impact on Information Security Culture. Stanford University; tuvo como Objetivo General: Investigar el impacto de ISO 27001:2013 en la cultura de seguridad de la información, contando con una población: 15

multinacionales en Estados Unidos; con un tipo de Investigación: Estudio de caso. Presentado los resultados: Mejora notable en la cultura de seguridad y la participación de los empleados, con las siguientes conclusiones: La norma no solo mejora los procesos, sino también la mentalidad de seguridad en las organizaciones.

Kim, S. (2021). En su tesis titulada Effectiveness of ISO 27001:2013 in Preventing Data Breaches. Korea University; tuvo como Objetivo General: Analizar la efectividad de ISO 27001:2013 en la prevención de brechas de datos, contando con una población: 25 empresas de TI en Corea del Sur; con un tipo de Investigación: Cuantitativa. Presentado los resultados: Reducción significativa en el número de brechas de datos reportadas, con las siguientes conclusiones: La certificación es crucial para minimizar riesgos de seguridad de datos.

Ali, H. (2019). En su tesis titulada Implementing ISO 27001:2013 in Healthcare Organizations. University of Melbourne; tuvo como Objetivo General: Evaluar la implementación de ISO 27001:2013 en organizaciones de salud, contando con una población: 10 hospitales en Australia; con un tipo de Investigación: Cualitativa. Presentado los resultados: Mejoras en la protección de datos de pacientes y cumplimiento normativo, con las siguientes conclusiones: La norma es vital para la protección de información sensible en el sector salud.

Gonzalez, R. (2020). En su tesis titulada ISO 27001:2013 and Risk Management in Telecommunications. University of Madrid; tuvo como Objetivo General: Explorar el impacto de ISO 27001:2013 en la gestión de riesgos en telecomunicaciones, contando con una población: 15 empresas de telecomunicaciones en España; con un tipo de Investigación: Mixta. Presentado los resultados: Mejoras en la identificación y mitigación de riesgos, con las siguientes conclusiones: La norma fortalece significativamente la gestión de riesgos en el sector.

Kumar, P. (2021). En su tesis titulada Cost-Benefit Analysis of ISO 27001:2013 Implementation. Indian Institute of Technology; tuvo como Objetivo General: Realizar un análisis costo-beneficio de la implementación de ISO 27001:2013, contando con una población: 20 empresas de TI en India; con un tipo de Investigación: Cuantitativa. Presentado los resultados: Beneficios superan los costos a largo plazo, con las siguientes conclusiones: La inversión en la certificación es rentable y beneficiosa para la seguridad de la información.

Nguyen, T. (2022). En su tesis titulada ISO 27001:2013 in the Context of Cloud Computing. Vietnam National University; tuvo como Objetivo General: Evaluar la implementación de ISO 27001:2013 en servicios de computación en la nube, contando con una población: 10 proveedores de servicios en la nube en Vietnam; con un tipo de Investigación: Estudio de caso. Presentado los resultados: Mejora en la seguridad de los datos

almacenados en la nube, con las siguientes conclusiones: La norma es efectiva para garantizar la seguridad de la información en entornos de computación en la nube.

Tesis Nacionales sobre Seguridad de la Información Aplicando ISO 27001:2013

Ramírez, J. (2019). En su tesis titulada Implementación de ISO 27001:2013 en Instituciones Financieras Peruanas. Universidad Nacional Mayor de San Marcos; tuvo como Objetivo General: Evaluar la implementación de ISO 27001:2013 en instituciones financieras peruanas, contando con una población: 5 bancos en Lima; con un tipo de Investigación: Cuantitativa. Presentado los resultados: Reducción de incidentes de seguridad en un 40%, con las siguientes conclusiones: La norma mejora la seguridad y genera confianza entre los clientes.

Fernández, L. (2020). En su tesis titulada ISO 27001:2013 en el Sector Salud en el Perú. Universidad Peruana Cayetano Heredia; tuvo como Objetivo General: Analizar la implementación de ISO 27001:2013 en el sector salud, contando con una población: 7 hospitales en Lima; con un tipo de Investigación: Cualitativa. Presentado los resultados: Mejoras en la protección de datos de pacientes, con las siguientes conclusiones: La norma es crucial para la seguridad de la información en el sector salud.

Pérez, M. (2021). En su tesis titulada Eficacia de ISO 27001:2013 en Empresas de Telecomunicaciones. Pontificia Universidad Católica del



Perú; tuvo como Objetivo General: Evaluar la eficacia de ISO 27001:2013 en empresas de telecomunicaciones, contando con una población: 10 empresas en Lima; con un tipo de Investigación: Mixta. Presentado los resultados: Reducción del 30% en riesgos de seguridad, con las siguientes conclusiones: La norma es altamente efectiva en la gestión de riesgos.

Torres, S. (2019). En su tesis titulada ISO 27001:2013 en Pequeñas Empresas Peruanas. Universidad de Lima; tuvo como Objetivo General: Evaluar la implementación de ISO 27001:2013 en pequeñas empresas, contando con una población: 20 PYMEs en Lima; con un tipo de Investigación: Estudio de caso. Presentado los resultados: Mejoras en la gestión de seguridad y satisfacción del cliente, con las siguientes conclusiones: La norma es viable y beneficiosa para las PYMEs.

García, A. (2020). En su tesis titulada Impacto de ISO 27001:2013 en Universidades Peruanas. Universidad Nacional de Ingeniería; tuvo como Objetivo General: Evaluar el impacto de ISO 27001:2013 en universidades, contando con una población: 5 universidades en Lima; con un tipo de Investigación: Cuantitativa. Presentado los resultados: Mejoras en la protección de datos académicos, con las siguientes conclusiones: La norma es esencial para la seguridad de la información en el ámbito académico.

Vargas, E. (2021). En su tesis titulada ISO 27001:2013 y su Aplicación en Gobiernos Locales. Universidad Nacional del Callao; tuvo como Objetivo

General: Analizar la aplicación de ISO 27001:2013 en gobiernos locales, contando con una población: 10 municipios en Lima; con un tipo de Investigación: Cualitativa. Presentado los resultados: Mejoras en la gestión de la seguridad de la información, con las siguientes conclusiones: La norma es fundamental para la seguridad en el sector público.

López, C. (2022). En su tesis titulada Evaluación de ISO 27001:2013 en el Sector Energético. Universidad Nacional Agraria La Molina; tuvo como Objetivo General: Evaluar la implementación de ISO 27001:2013 en el sector energético, contando con una población: 5 empresas energéticas en Lima; con un tipo de Investigación: Mixta. Presentado los resultados: Reducción de riesgos de seguridad en un 35%, con las siguientes conclusiones: La norma es altamente efectiva para la seguridad en el sector energético.

Martínez, D. (2019). En su tesis titulada ISO 27001:2013 en Empresas de Tecnología. Universidad Peruana de Ciencias Aplicadas; tuvo como Objetivo General: Evaluar la implementación de ISO 27001:2013 en empresas de tecnología, contando con una población: 10 empresas en Lima; con un tipo de Investigación: Cuantitativa. Presentado los resultados: Mejoras en la gestión de riesgos y seguridad, con las siguientes conclusiones: La norma es crucial para la protección de datos en el sector tecnológico.

Rojas, F. (2020). En su tesis titulada ISO 27001:2013 y la Gestión de Riesgos en Bancos. Universidad Ricardo Palma; tuvo como Objetivo General: Analizar la gestión de riesgos en bancos con ISO 27001:2013, contando con una población: 5 bancos en Lima; con un tipo de Investigación: Estudio de caso. Presentado los resultados: Reducción significativa de incidentes de seguridad, con las siguientes conclusiones: La norma es esencial para la seguridad de la información en bancos.

Sánchez, H. (2021). En su tesis titulada Implementación de ISO 27001:2013 en Instituciones Educativas. Universidad Nacional Federico Villarreal; tuvo como Objetivo General: Evaluar la implementación de ISO 27001:2013 en instituciones educativas, contando con una población: 10 colegios en Lima; con un tipo de Investigación: Cuantitativa. Presentado los resultados: Mejoras en la protección de datos estudiantiles, con las siguientes conclusiones: La norma es fundamental para la seguridad de la información en el sector educativo

## **2.2. Bases Teóricas**

### **2.2.1. Seguridad**

La seguridad de los datos es una forma de gestión empresarial inteligente que previene los tres peligros de la era digital: deudas, demandas y pérdidas. Del mismo modo, la seguridad es un medio para lograr un fin y la confianza es parte integral de la propuesta de valor, del mismo modo que en la banca la seguridad se convierte en un habilitador fundamental.(16)

"En general, el objetivo de la seguridad es evitar que alguien haga cosas que usted no desea hacer con su computadora o sus periféricos." "La seguridad es un proceso, no un producto", es decir. Seguridad no es lo mismo que un conjunto de medidas de seguridad. (17).

El objetivo de la seguridad discutido en este estudio es crear controles que protejan contra algunos de los riesgos que enfrentan las organizaciones, en este caso las universidades. (18)

### **2.2.2. Seguridad de la información**

La seguridad de la información se define como el conjunto de medidas y procedimientos diseñados para proteger la confidencialidad, integridad y disponibilidad de la información. ( 19).

La Seguridad Informática y mencionada por Aceituno,V.,( 2004) como " Las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los aspectos tecnológicos, sino también los procesos, políticas y prácticas de gestión relacionadas con la protección de la información"( 20).

De igual forma, la seguridad de la información es un proceso que incluye diversos elementos como: B. Aspectos técnicos, gestión organizativa, recursos humanos, economía, negocios, asuntos legales, cumplimiento, etc. Incluye no sólo aspectos informáticos y de telecomunicaciones, sino también aspectos físicos, ambientales, humanos, etc. ( 21)

La seguridad de la información se logra mediante la implementación de controles y medidas apropiadas, incluidas políticas, prácticas, procedimientos, estructuras organizativas y características del software. Estos controles deben establecerse para garantizar que se cumplan los objetivos de seguridad específicos de una organización, minimizar los daños a la seguridad y maximizar el clima de inversión y las oportunidades comerciales. ( 22)

### **2.2.3. Seguridad Física**

La seguridad física según Álvarez,G., y Pérez,P.,( 2004), se refiere a la protección de los activos físicos de una organización, como servidores, equipos de red y documentos impresos. Incluye medidas como la seguridad de las instalaciones, el control de acceso físico, la protección contra incendios y la seguridad ambiental.

**Protección de Instalaciones:** Implica asegurar las instalaciones físicas donde se almacena o procesa la información. Esto puede incluir el uso de cerraduras, sistemas de alarma, cámaras de seguridad y controles de acceso.

**Control de Acceso Físico:** Se refiere a los mecanismos utilizados para regular quién puede ingresar a las instalaciones. Esto puede incluir sistemas de tarjetas de acceso, reconocimiento biométrico o guardias de seguridad.

**Protección contra Desastres:** Involucra la implementación de medidas para prevenir o mitigar los efectos de desastres naturales o provocados por el hombre, como incendios, inundaciones, terremotos o sabotaje.

Seguridad Ambiental: Se refiere a mantener condiciones ambientales óptimas para los equipos de tecnología de la información, como temperatura, humedad y suministro eléctrico estable. ( 23)

#### **2.2.4. Seguridad Lógica**

La seguridad lógica se centra en la protección de los activos digitales de una organización, como datos, sistemas y redes.

Incluye medidas como la autenticación de usuarios, el control de acceso lógico, la encriptación de datos y la detección de intrusiones.

**Autenticación de Usuarios:** Consiste en verificar la identidad de los usuarios antes de permitirles el acceso a los sistemas o datos. Esto puede incluir contraseñas, tarjetas inteligentes, biometría o métodos multifactoriales.

**Control de Acceso Lógico:** Se refiere a los mecanismos utilizados para regular qué recursos digitales pueden ser accedidos por usuarios autorizados. Esto incluye listas de control de acceso (ACL), roles y permisos ( 24)

**Encriptación de Datos:** Implica codificar la información para que solo las partes autorizadas puedan acceder y comprender los datos. Esto protege la confidencialidad de la información, especialmente durante la transmisión o el almacenamiento.

**Detección de Intrusiones:** Involucra la monitorización activa de la red y los sistemas para identificar y responder a actividades sospechosas o intentos de acceso no autorizado ( 25)

#### **2.2.5. Controles**

Los controles de seguridad son medidas específicas implementadas para mitigar riesgos y proteger los activos de la organización.

Pueden clasificarse en controles físicos, técnicos y administrativos, y pueden incluir políticas, procedimientos, tecnologías y prácticas de gestión. ( 26).

Controles Físicos: Incluyen medidas como cercas, puertas con cerradura, sistemas de alarma, cámaras de vigilancia y controles de acceso biométricos. ( 27).

Controles Técnicos: Implican el uso de tecnología para proteger la información, como firewalls, antivirus, sistemas de detección de intrusiones (IDS), sistemas de prevención de pérdida de datos (DLP) y software de encriptación. (28).

Controles Administrativos: Se refieren a políticas, procedimientos y prácticas de gestión diseñadas para promover la seguridad de la información. Esto puede incluir políticas de seguridad, entrenamiento de empleados, evaluaciones de riesgos y programas de concientización sobre seguridad (29).

#### **2.2.6. Amenazas**

Las amenazas son eventos potenciales que pueden causar daño a los activos de información. Los ataques son acciones deliberadas llevadas a cabo por personas u entidades con el objetivo de explotar vulnerabilidades y comprometer la seguridad de la información.

Amenazas Internas: Proviene de personas dentro de la organización, como empleados descontentos, ex empleados, o errores humanos involuntarios. ( 30).

Amenazas Externas: Proviene de fuentes externas a la organización, como hackers, malware, competidores o desastres naturales. ( 31).

### **2.2.7. Ataques**

Ataques Cibernéticos: Incluyen una amplia gama de acciones maliciosas, como ataques de denegación de servicio (DDoS), phishing, ransomware, robo de datos y ataques de ingeniería social.( 32)

Entre ellos se encuentran ISO 27001, NIST SP 800-53, GDPR, HIPAA, entre otros, que proporcionan directrices y requisitos específicos para la gestión de la seguridad de la información ( 33).

Existen numerosas normativas y estándares relacionados con la seguridad de la información, que pueden ser obligatorios o voluntarios dependiendo del contexto y la industria.( 34)

### **2.2.8. Riesgo**

Carracedo,J.,( 2004) opina que la gestión de riesgos es un proceso sistemático para identificar, evaluar y mitigar los riesgos de seguridad de la información. Incluye actividades como la realización de evaluaciones de riesgos, la implementación de controles de seguridad y la monitorización continua del entorno de seguridad.

Los riesgos son la probabilidad de que una amenaza se materialice y cause un impacto negativo en la organización.



Riesgos de Cumplimiento: Relacionados con el incumplimiento de leyes, regulaciones o estándares de seguridad de la información, lo que puede resultar en sanciones legales o daños a la reputación de la organización.

## **NORMA ISO 27001:2013**

### **Gestión de la Seguridad de la Información (GSI):**

En el centro de la ISO 27001 se encuentra el concepto de que la seguridad de la información debe ser gestionada de manera proactiva y sistemática en toda la organización. Esto implica la implementación de un enfoque basado en procesos para identificar, evaluar y tratar los riesgos de seguridad de la información de manera continua y efectiva. La gestión de la seguridad de la información se basa en la comprensión de que la seguridad no es un estado estático, sino un proceso dinámico que requiere atención constante y mejora continua.

### **Enfoque Basado en Procesos:**

La ISO 27001 adopta un enfoque basado en procesos para la gestión de la seguridad de la información. Esto significa que se deben establecer, implementar, mantener y mejorar procesos documentados para lograr los objetivos de seguridad de la información de la organización. Estos procesos deben ser coherentes, repetibles y medibles, y deben abarcar todas las áreas relevantes de la organización, desde la alta dirección hasta el personal operativo. Este enfoque garantiza que la seguridad de la información se integre de

manera efectiva en las operaciones diarias de la organización y se considere como parte integral de su cultura organizativa.

#### **Ciclo de Mejora Continua:**

La norma ISO 27001 se basa en el ciclo de mejora continua conocido como Planificar, Hacer, Verificar, Actuar (PHVA), también conocido como ciclo de Deming o ciclo de PDCA. Este enfoque iterativo permite a las organizaciones identificar áreas de mejora en su sistema de gestión de la seguridad de la información y tomar medidas correctivas y preventivas según sea necesario. El ciclo PHVA se aplica en todas las etapas del proceso de gestión de la seguridad de la información, desde la identificación de riesgos hasta la implementación de controles y la revisión del desempeño del sistema.

#### **Enfoque Basado en el Riesgo:**

La ISO 27001 se basa en un enfoque basado en el riesgo para la gestión de la seguridad de la información. Esto implica identificar y evaluar los riesgos de seguridad de la información que enfrenta la organización, y luego implementar controles para mitigar estos riesgos de manera proporcionada al impacto potencial en la organización. El enfoque basado en el riesgo permite a las organizaciones priorizar sus esfuerzos de seguridad en función de la magnitud y la probabilidad de los riesgos identificados, lo que

garantiza una asignación eficiente de recursos y un enfoque centrado en los aspectos críticos de la seguridad de la información.

## **2.3. Marco Conceptual**

Norma ISO

La ISO 27001:2013 requiere que las organizaciones establezcan una política de seguridad de la información que establezca el marco general y los objetivos de seguridad de la información de la organización. Esta política debe ser aprobada por la dirección y comunicada a todas las partes interesadas relevantes.

### **Alcance del Sistema de Gestión de la Seguridad de la Información (SGSI):**

La norma establece los requisitos para determinar el alcance del SGSI de una organización, es decir, qué activos de información y procesos están cubiertos por el sistema de gestión de la seguridad de la información.

### **Identificación de Riesgos y Evaluación de Riesgos:**

La ISO 27001:2013 requiere que las organizaciones identifiquen los riesgos de seguridad de la información que enfrentan y evalúen la probabilidad y el impacto de estos riesgos en la

organización. Esto se hace utilizando un enfoque basado en el riesgo para priorizar la implementación de controles de seguridad.

### **Selección de Controles de Seguridad:**

Una vez que se han identificado y evaluado los riesgos de seguridad de la información, la norma requiere que las organizaciones seleccionen y apliquen controles de seguridad adecuados para mitigar estos riesgos. Estos controles pueden incluir medidas técnicas, organizativas y físicas.

### **Implementación y Operación: La ISO 27001:2013**

establece requisitos detallados para la implementación y operación efectiva del SGSI de una organización. Esto incluye la documentación de políticas, procedimientos y controles de seguridad, la asignación de responsabilidades y recursos, y la realización de actividades de concientización y formación en seguridad.

### **Supervisión y Revisión:**

La norma requiere que las organizaciones supervisen y revisen regularmente el desempeño de su SGSI para garantizar su eficacia continua. Esto incluye la realización de auditorías internas, revisiones de la dirección y la evaluación del cumplimiento de los requisitos de la norma.

## **Mejora Continua: La ISO 27001:2013**

promueve la mejora continua del SGSI de una organización mediante la identificación de áreas de mejora y la toma de medidas correctivas y preventivas según sea necesario. Esto se logra utilizando el ciclo PHVA para planificar, implementar, controlar y mejorar el sistema de gestión de la seguridad de la información. (36)

## **Seguridad de la Información**

Confidencialidad:

La confidencialidad se refiere a la protección de la información contra el acceso no autorizado. Se logra mediante la implementación de controles de acceso, como contraseñas, cifrado de datos y restricciones de acceso físico.

Integridad:

La integridad asegura que la información sea precisa, completa y no haya sido modificada de manera no autorizada. Se pueden implementar controles de integridad, como firmas digitales y registros de cambios, para garantizar la exactitud y la integridad de los datos.

Disponibilidad:

La disponibilidad garantiza que la información esté disponible y accesible cuando sea necesario por aquellos autorizados. Se pueden implementar medidas de redundancia y respaldo para garantizar la disponibilidad continua de los datos, incluso en caso de fallas o ataques. (37)

Autenticación:

La autenticación verifica la identidad de los usuarios para garantizar que solo los usuarios autorizados tengan acceso a la información. Esto puede incluir el uso de contraseñas, biometría y tokens de seguridad.

Autorización:

La autorización determina qué recursos o información pueden acceder los usuarios autorizados y en qué medida. Se basa en los derechos y privilegios asignados a cada usuario dentro del sistema de información.

Criptografía:

La criptografía es una técnica utilizada para proteger la confidencialidad e integridad de la información mediante el cifrado y descifrado de datos. Se utiliza ampliamente en la protección de datos sensibles durante su almacenamiento y transmisión.

Auditoría y Monitoreo:

La auditoría y el monitoreo son procesos para supervisar y registrar actividades relacionadas con la seguridad de la información. Esto incluye la revisión de registros de eventos, la detección de anomalías y la respuesta a incidentes de seguridad en tiempo real.

(38)

## 2.4 Definiciones de términos básicos

**Seguridad de la Información:** Conjunto de medidas y procedimientos diseñados para proteger la confidencialidad, integridad y disponibilidad de la información.

**Activo de Información:** Cualquier elemento de información o recurso relacionado con la información que sea valioso para la organización, como datos, sistemas, hardware, software o documentación.

**Riesgo de Seguridad de la Información:** Probabilidad de que una amenaza explote una vulnerabilidad y cause un daño a un activo de información.

**Amenaza:** Circunstancia, evento o proceso que tiene el potencial de causar daño a un activo de información al explotar una vulnerabilidad.

**Vulnerabilidad:** Debilidad o fallo en un sistema, proceso o control que podría ser explotado por una amenaza para causar daño a un activo de información.

**Control de Seguridad:** Medida o salvaguarda implementada para reducir el riesgo de seguridad de la información, mitigar amenazas y proteger los activos de información.

**Política de Seguridad de la Información:** Declaración formal de los objetivos, principios y responsabilidades de una organización en relación con la seguridad de la información.

**Gestión de Riesgos:** Proceso sistemático para identificar, evaluar y tratar los riesgos de seguridad de la información de una organización.

**Plan de Tratamiento de Riesgos:** Documento que describe cómo una organización responderá a los riesgos de seguridad de la información

identificados, incluyendo la implementación de controles de seguridad y la asignación de responsabilidades.

**Auditoría de Seguridad de la Información:** Proceso de evaluación independiente y sistemática de los controles de seguridad de la información de una organización para garantizar su eficacia y cumplimiento.

**Incidente de Seguridad de la Información:** Evento que compromete la confidencialidad, integridad o disponibilidad de la información y que requiere una respuesta adecuada.

**Contingencia:** Planes y procedimientos establecidos para responder a incidentes de seguridad de la información y minimizar su impacto en la organización.

**Concienciación en Seguridad de la Información:** Programas educativos y de sensibilización diseñados para informar y educar a los empleados sobre las mejores prácticas de seguridad de la información y sus responsabilidades.

**Análisis de Impacto en el Negocio (BIA):** Evaluación de los efectos potenciales de la interrupción de los procesos de negocio y la pérdida de activos de información para la organización.

**Mejora Continua:** Proceso de revisión y actualización periódica de los controles de seguridad de la información y los procesos de gestión de riesgos para garantizar su eficacia y adaptabilidad a los cambios en el entorno operativo.



### **III. HIPÓTESIS Y VARIABLES**

#### **3.1. Hipótesis**

##### **Hipótesis general**

HG: Aplicando la ISO 27001:2013o la Unidad de Registros

Académicos mejora la seguridad de la información

##### **Hipótesis específicas**

HE1 La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión confidencialidad de la seguridad de la información

HE2 La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión disponibilidad de la seguridad de la información

HE3 La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión integridad de la seguridad de la información

Variables de la investigación

##### **Variable independiente**

ISO 27001:2013

##### **Variable dependiente**

Seguridad de la Información de la Oficina de Registro Académico y Archivo.

### 3.1.1 Operacionalización de las variables

VARIABLES	Definición conceptual	Definición operacional	Dimensión	Indicadores	Índices	Metodología
<b>VARIABLE INDEPENDIENTE</b> ISO 27001:2013	Es un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013. (ISO 27001)	La norma ISO, permite que la información fluya por la organización, usando una estrategia de políticas, normatividad legal y con una técnica de seguridad para toda la información.	Legal  Estratégica  Técnica	Porcentaje de conformidad de requisitos Legales  Porcentaje de conformidad de políticas estratégicas  Promedio de implementación técnica	1-10	Diseño pre-experimental  tipo de investigación aplicada  método inductivo
<b>VARIABLE DEPENDIENTE:</b>  Seguridad de la Información de la Oficina de Registro Académico y Archivo.	Gómez, A., (2006) define la seguridad de la información como una medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios al sistema.	La seguridad de la información se define como el buen uso de la información a través de la integridad, suministrando confidencialidad y disponibilidad.	Confidencialidad  Disponibilidad  Integridad	Promedio de información confidencial  Tiempo de respuesta de continuidad  Porcentaje de información validada	11-20	Población 25 personas

## **IV. METODOLOGÍA**

### **4.1. Diseño metodológico**

La presente investigación, fue pre-experimental porque se dan estímulos y tratamientos a grupos de personas y situaciones. Luego, apliqué la medición y observé su efecto sobre la variable dependiente. Este tipo de investigación es correlacional porque se encontró la relación que permite solucionar los problemas actuales que se encuentran en este sector respecto a incidentes de seguridad que provocan pérdida, confusión y repetición de información, utilizando la norma internacional ISO aplicación 270012013, mejorando así la situación de la sociedad. Esto se debe a que el propósito es contribuir al desarrollo. Requisitos Fiabilidad, disponibilidad e integridad de la información proporcionada por el Unidad de Registro Académico UNAC. (39).

### **4.2. Método de investigación**

La presente investigación, tuvo el método inductivo para deducir las observaciones de los efectos sobre la variable dependiente con el fin de resolver la problemática que encontramos acerca de los ocurrencias de seguridad que estén produciendo repetición de datos, pérdida de data y desorden de información en la Unidad de Registro Académico UNAC(40).

### 4.3. Población y Muestra

Para la investigación se trabajó con un total de 25 personas que laboran en la Unidad de registros académicos .



Figura 4. Gráfico de Población de ORAA.

Fuente propia.

### 4.4. Lugar de estudios y periodo desarrollado

Para la presente investigación se desarrollo en la Unidad de registros académicos de la Universidad Nacional del Callao desde Setiembre del 2023 hasta Enero del 2024

### 4.5. Técnicas e instrumentos de recolección de datos

#### Técnicas de recolección de datos

**Entrevista.-** Es una técnica de recolección de datos mediante el uso de cuestionarios aplicados a un grupo representativo para detectar tendencias de comportamiento y otros objetivos.

**Observación.-** Es una técnica que se usa para estudiar la muestra en sus propias actividades de grupo. Permite conocer: qué, quién, cómo, cuándo, cuánto, dónde, porqué, etc.

### **Instrumentos de recolección de datos**

**Checklist.-** Es un instrumento de comprobación que sirve para utilizar de guía y recordar los puntos que deben ser inspeccionados en función de los conocimientos que se tienen sobre las características y riesgos de las instalaciones. Viene a ser un cuestionario de preguntas en el que se responderá SI o NO, concretamente es una lista de comprobación de determinadas condiciones de trabajo compuesta por varios ítems que pueden contener una o varias preguntas según sea el caso.

**Cuestionario de la ISO 27001:2013.-** Es un instrumento de recolección de datos cualitativos o cuantitativos mediante el uso de un conjunto de preguntas diseñadas para conocer o evaluar a una o más personas acerca de la Organización internacional de Normalización para la seguridad de la información ISO 27001.

Validez. Se realizó la validez se refiere al grado en que un instrumento realmente mide la variable que pretende medir (38)". Para la recolección de datos se utilizaron estos dos cuestionarios fueron validado a través del alfa de ha sido utilizado en diversos estudios, mostrando una sensibilidad del 0.841 para el instrumento

## Instrumento

Estadísticas de fiabilidad		
Alfa de Cronbach	AC en elementos estandarizados	N de elementos
,841	,811	20

### 4.6. Plan de análisis estadísticos de datos

Los datos recolectados de la investigación encuestas serán procesados mediante software estadístico SPSS 25.

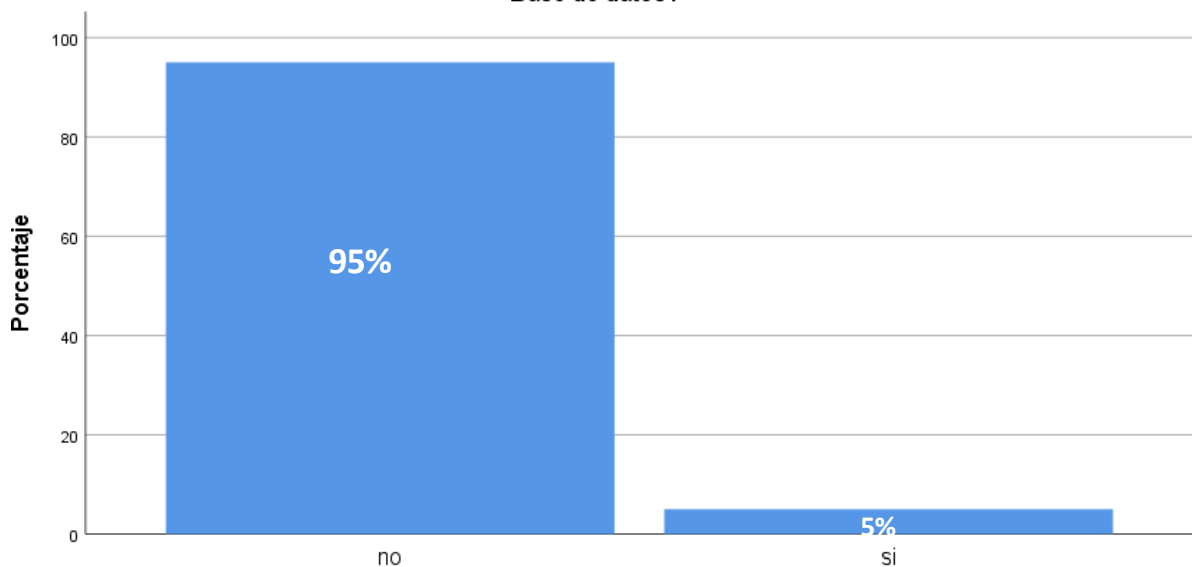
## CAPITULO V RESULTADOS

### Resultados Descriptivos

#### ¿Existe archivo Log?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	38	95,0	95,0	95,0
	si	2	5,0	5,0	100,0
Total		40	100,0	100,0	

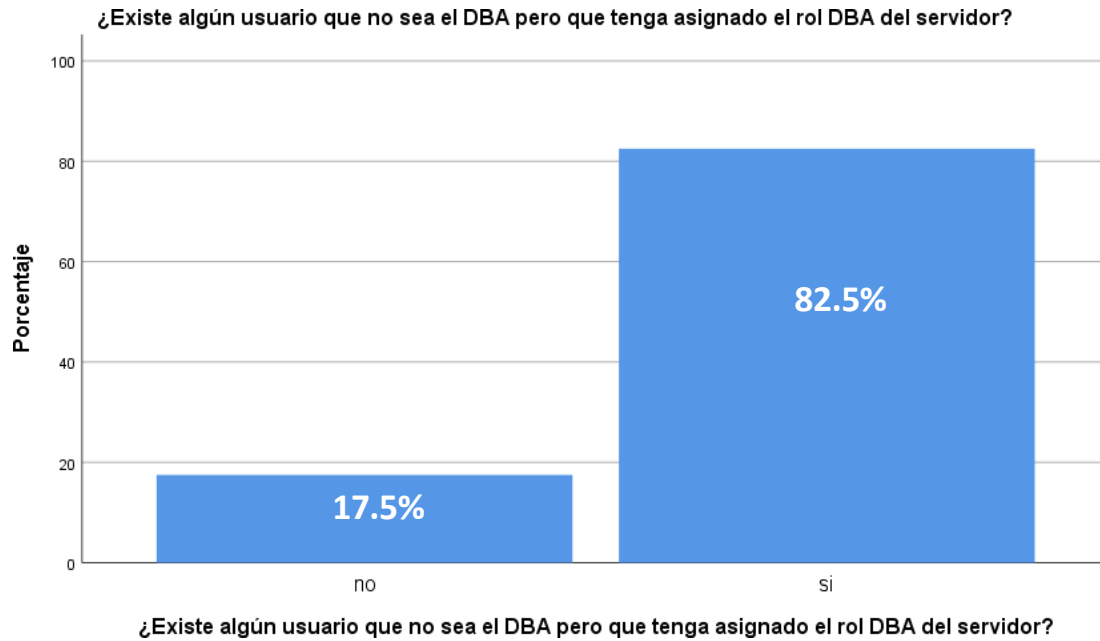
¿Existe algún archivo de tipo Log donde guarde información Referida a las operaciones que realiza la Base de datos?



¿Existe algún archivo de tipo Log donde guarde información Referida a las operaciones que realiza la Base de datos?

### ¿Diferentes usuarios asignado el rol DBA del servidor?

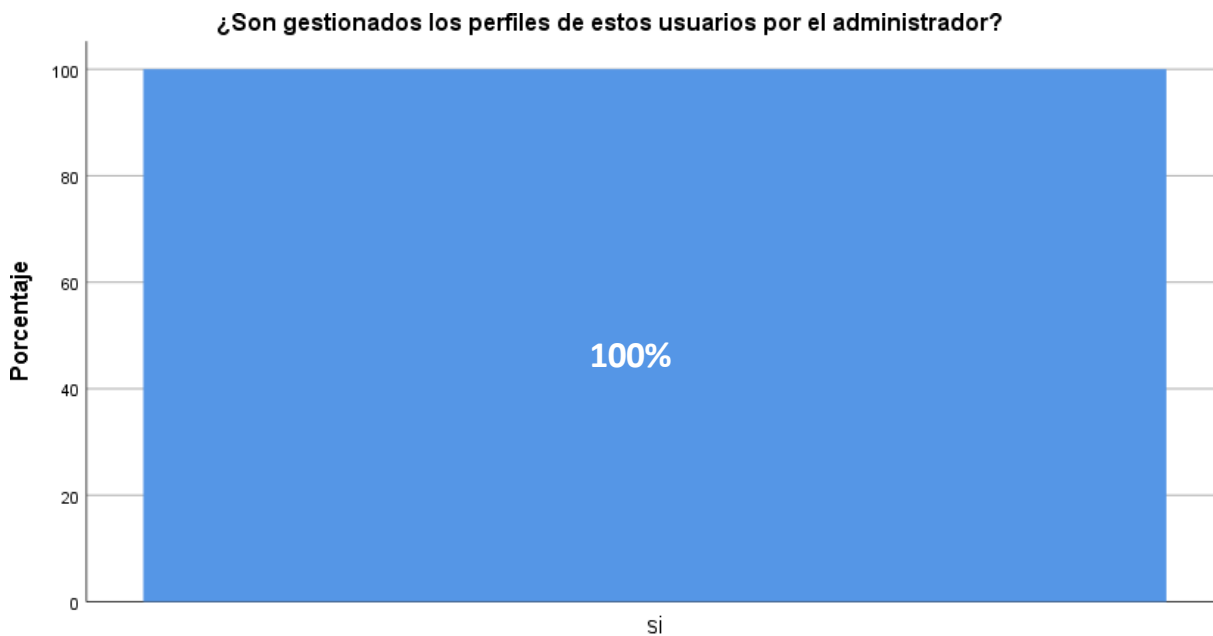
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	7	17,5	17,5	17,5
	si	33	82,5	82,5	100,0
	Total	40	100,0	100,0	





### ¿El administrador gestiona usuarios?

Válido	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
si	40	100,0	100,0	100,0

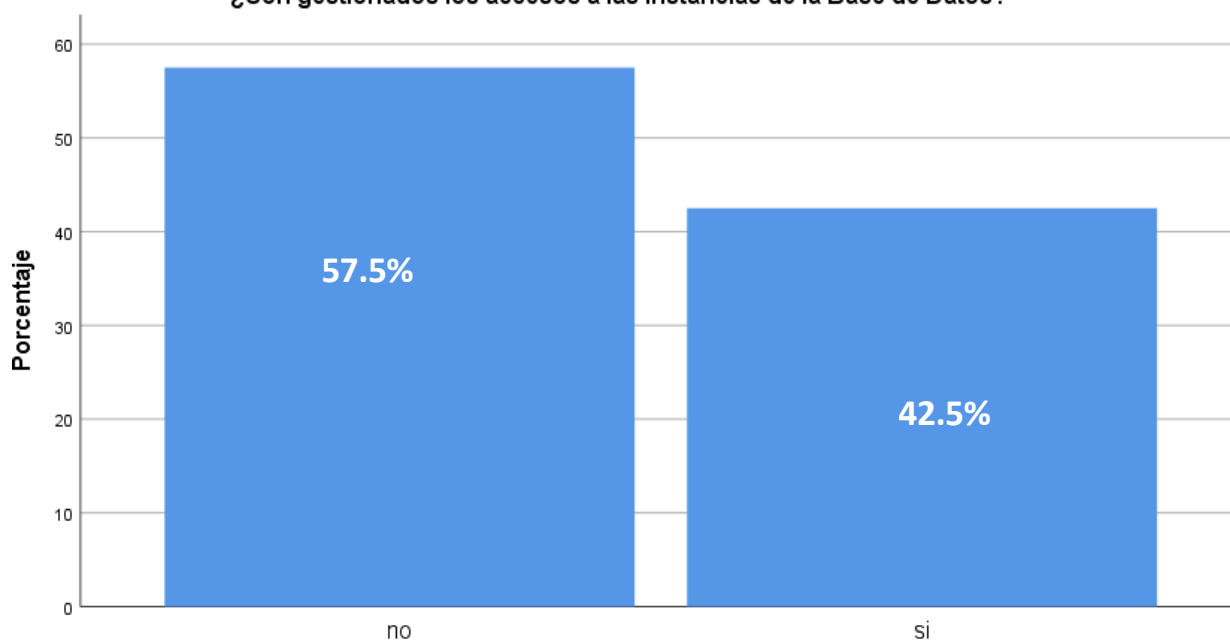


¿Son gestionados los perfiles de estos usuarios por el administrador?

### ¿Base de Datos gestionada?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	23	57,5	57,5	57,5
	si	17	42,5	42,5	100,0
	Total	40	100,0	100,0	

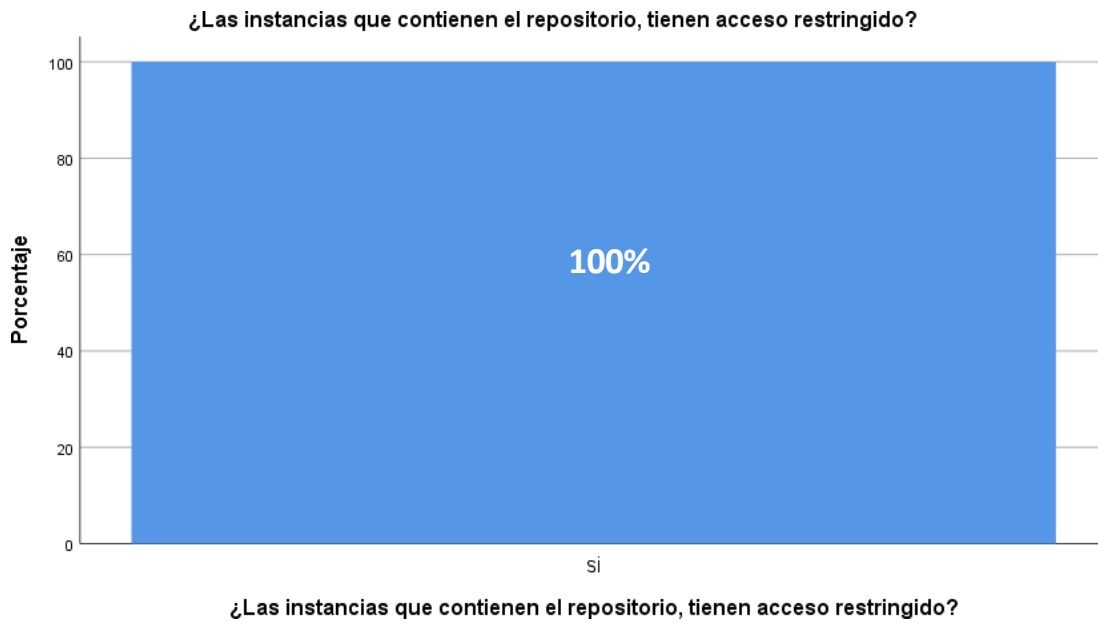
### ¿Son gestionados los accesos a las instancias de la Base de Datos?



### ¿Son gestionados los accesos a las instancias de la Base de Datos?

**¿Las instancias que contienen el repositorio, tienen acceso restringido?**

Válido	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
si	40	100,0	100,0	100,0



## 5.2 RESULTADOS INFERENCIALES

Suponiendo que su hipótesis señala que:

### HIPOTESIS GENERAL

Aplicando la ISO 27001:2013, la Unidad de Registros Académicos mejora la seguridad de la información

Usamos r de Pearson para hallar el grado de relación entre las variables.

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,651 <sup>a</sup>	,424	,400	3,112

a. Predictores: (Constante), POSTEST (USANDO APLICATIVO)

### INTERPRETACIÓN

Como el r de Pearson 0.651 es positivo se interpreta que las variables son directamente proporcional, ósea, mejora significativamente la Seguridad de la Información de la URA aplicando si la ISO 27001:2013.

Como el r de Pearson calculado 0.651 se aproxima a 1 quiere decir que la relación entre las variables es fuerte.

Finalmente se observa en la tabla que la seguridad de la información en URA UNAC mejora significativamente en 42.4% gracias a la implementación de la ISO 27001:2013

## HIPOTESIS ESPECÍFICA

**HE1:** La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión confidencialidad de la seguridad de la información

### Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,744 <sup>a</sup>	,553	,540	2,26880

a. Predictores: (Constante), DORSAL\_POSTEST

## INTERPRETACIÓN

Como el r de Pearson 0.744 es positivo se interpreta que las variables son directamente proporcional, ósea, mejora significativamente la Seguridad de la Información en la dimensión confidencialidad de la URA aplicando si la ISO 27001:2013.

Como el r de Pearson calculado 0.744 se aproxima a 1 quiere decir que la relación entre las variables es fuerte.

Finalmente se observa en la tabla que la seguridad de la información en la dimensión confidencialidad en URA UNAC mejora significativamente en 55.3% gracias a la implementación de la ISO 27001:2013

**HE2:** La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión disponibilidad de la seguridad de la información

### Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,754 <sup>a</sup>	,568	,556	2,21935

a. Predictores: (Constante), PECTORAL\_POSTEST

### INTERPRETACIÓN

Como el r de Pearson 0.754 es positivo se interpreta que las variables son directamente proporcional, ósea, mejora significativamente la Seguridad de la Información en la dimensión disponibilidad de la URA aplicando si la ISO 27001:2013.

Como el r de Pearson calculado 0.754 se aproxima a 1 quiere decir que la relación entre las variables es fuerte.

Finalmente se observa en la tabla que la seguridad de la información en la dimensión disponibilidad en URA UNAC mejora significativamente en 56.8% gracias a la implementación de la ISO 27001:2013

**HE3:** La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión integridad de la seguridad de la información

#### Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,711 <sup>a</sup>	,505	,500	2,11844

a. Predictores: (Constante), PECTORAL\_POSTEST

### INTERPRETACIÓN

Como el r de Pearson 0.711 es positivo se interpreta que las variables son directamente proporcional, ósea, mejora significativamente la Seguridad de la Información en la dimensión integridad de la URA aplicando si la ISO 27001:2013.

Como el r de Pearson calculado 0.711 se aproxima a 1 quiere decir que la relación entre las variables es fuerte.

Finalmente se observa en la tabla que la seguridad de la información en la dimensión integridad en URA UNAC mejora significativamente en 51% gracias a la implementación de la ISO 27001:2013

## CAPÍTULO VI: DISCUSIÓN DE RESULTADOS

### 6.1 CONTRASTACIÓN Y DEMOSTRACIÓN DE LA HIPÓTESIS CON LOS RESULTADOS

#### HIPOTESIS GENERAL

Aplicando la ISO 27001:2013 la Unidad de Registros Académicos mejora la seguridad de la información

**Ha:** Hipótesis alterna, **Ho:** Hipótesis nula.

**Ha:** Aplicando la ISO 27001:2013 la Unidad de Registros Académicos mejora la seguridad de la información

**Ho:** Aplicando la ISO 27001:2013 la Unidad de Registros Académicos no mejora la seguridad de la información

E= 0.05 (nivel de significancia SIG) 5% (por usar muestra)

#### ENTONCES

Estadísticamente vamos a hallar el p (nivel de significancia o SIG)

Si  $p < 0.05$ , se rechaza la hipótesis nula, se acepte la hipótesis alterna

Si  $p > 0.05$  se acepta la hipótesis nula, se rechaza la hipótesis alterna

		Prueba de muestras emparejadas					t	gl	Sig. (bilateral)
		Diferencias emparejadas							
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	PRETEST - POSTEST	45,55 5	6,67809	1,11301	-47,81509	-43,29602	- 40,93 0	35	,000

Como  $p < 0.05$ , se rechaza la hipótesis nula, se acepte la hipótesis alterna

**Ha:** Aplicando la ISO 27001:2013 la Unidad de Registros Académicos mejora la seguridad de la información



## HIPOTESIS ESPECIFICA 1

**HE1:** La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión confidencialidad de la seguridad de la información

**Ha:** Hipótesis alterna, **Ho:** Hipótesis nula

**Ha:** La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión confidencialidad de la seguridad de la información

**Ho:** La ISO 27001:2013 no se relaciona con la Unidad de Registros Académicos en la dimensión confidencialidad de la seguridad de la información

E= 0.05 (nivel de significancia SIG) 5% (por usar muestra)

## ENTONCES

Estadísticamente vamos a hallar el p (nivel de significancia o SIG)

Si  $p < 0.05$ , se rechaza la hipótesis nula, se acepte la hipótesis alterna

Si  $p > 0.05$  se acepta la hipótesis nula, se rechaza la hipótesis alterna

		Prueba de muestras emparejadas					t	g l	Sig. (bilateral)
		Diferencias emparejadas							
		Me dia	Desv. Desviaci ón	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	DORSAL_PRETEST	-	2,29907	,38318	-21,27789	-19,72211	-	3 5	,000
	DORSAL_POSTEST	20, 500							

Como  $p < 0.05$ , se rechaza la hipótesis nula, se acepte la hipótesis alterna

**Ha:** la ISO 27001:2013 influye significativamente en la confidencialidad de la seguridad de la información de la Oficina de Registros Académicos

## HIPOTESIS ESPECIFICA 2

**HE2:** La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión disponibilidad de la seguridad de la información

**Ha:** Hipótesis alterna, **Ho:** Hipótesis nula

**Ha:** La ISO 27001:2013 mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros Académicos

**Ho:** La ISO 27001:2013 no mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros Académicos

$E = 0.05$  (nivel de significancia SIG) 5% (por usar muestra)

## ENTONCES

Estadísticamente vamos a hallar el p (nivel de significancia o SIG)

Si  $p < 0.05$ , se rechaza la hipótesis nula, se acepta la hipótesis alterna

Si  $p > 0.05$  se acepta la hipótesis nula, se rechaza la hipótesis alterna

Prueba de muestras emparejadas									
		Diferencias emparejadas							
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia		t	gl	Sig. (bilateral)
					Inferior	Superior			
Par 1	PECTORAL_PRETES T - PECTORAL_POSTES T	20,44444	2,20965	,36827	-21,19208	-19,69681	55,514	35	,000

Como  $p < 0.05$ , se rechaza la hipótesis nula, se acepta la hipótesis alterna

**Ha:** La ISO 27001:2013 mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros Académicos

### HIPOTESIS ESPECIFICA 3

**HE3:** La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión integridad de la seguridad de la información

**Ha:** Hipótesis alterna, **Ho:** Hipótesis nula

**Ha:** La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión integridad de la seguridad de la información

**Ho:** La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión integridad de la seguridad de la información Académicos

E= 0.05 (nivel de significancia SIG) 5% (por usar muestra)

### ENTONCES

Estadísticamente vamos a hallar el p (nivel de significancia o SIG)

Si  $p < 0.05$ , se rechaza la hipótesis nula, se acepta la hipótesis alterna

Si  $p > 0.05$  se acepta la hipótesis nula, se rechaza la hipótesis alterna

Prueba de muestras emparejadas									
		Diferencias emparejadas							
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia		t	gl	Sig. (bilateral)
					Inferior	Superior			
Par 1	PECTORAL_PRETES T - PECTORAL_POSTES T	20,444	2,20965	,36827	-21,19208	-19,69681	55,514	35	,000

Como  $p < 0.05$ , se rechaza la hipótesis nula, se acepta la hipótesis alterna

**Ha:** La ISO 27001:2013 se relaciona con la Unidad de Registros Académicos en la dimensión integridad de la seguridad de la información

## 6.2 CONTRASTACIÓN DE LOS RESULTADOS CON ESTUDIOS SIMILARES

Huang, Han, Yang, & Ren en el 2019, (5) esta investigación generó un proceso metodológico para implementación exitosa del SGSI, similar a la investigación presentada ya que por el proceso se implementó la seguridad de la información.

En la misma línea de investigación, Bravo Ramos, M. J. (2018) como resultado que las mejoras planteadas le permiten al SGSI, alcanzar niveles de madures más altos y en el futuro tener la posibilidad de obtener la certificación del mismo, mediante la norma ISO/IEC 27001:2013. (6), a diferencia de est investigación solo se puede señalar la compatibilidad de los seis pasos de Margerit V.3, Octave V.2 y Nist 800-30, con la norma ISO/IEC 27001:2013.

De igual forma Nieves, Y. en el 2018, se desarrolló una investigación que tuvo como resultados de la encuesta realizada a estos profesionistas arrojan que se considera la aplicación de normas como un proceso necesario, en el caso de esta investigación la encuesta arrojó mejoras en la aplicación de las normas.

Así mismo, Montilla, L. y Pérez, G. en el 2016, en la investigación presentaron los resultados donde indican que 25 de los 32 factores de riesgo analizados se pueden relacionar con el elemento de fuentes de información, de la misma manera 12 de los 32 con el elemento talento humano, 12 de los 32 con el elemento usuario, 12 de los 32 con el elemento edificación y 10 de los 32 con el elemento equipos, similar a nuestra investigación.

En este mismo orden de ideas, Sandoval Vargas en el 2016 su trabajo se desarrolló teniendo en cuenta la necesidad de que la seguridad en la empresa cumpla cabalmente con los parámetros internacionales establecidos, contribuyendo así al mejoramiento y al propósito de obtener su certificación, al contrario de la presente investigación no fue la necesidad de la universidad pero se desarrolló las propuestas.

Torres en el año 2018, realizó su investigación donde tuvo como resultado que todos los elementos anteriores se logran creando métodos específicos de

gestión de la información de seguridad basados en las mejores prácticas del mercado e implementándolos como se define en este documento (10) dentro del alcance definido en el presente trabajo.

Santos en el 2017, realizó su investigación donde como resultado permite que el sistema funcione según los principios de mejora continua, beneficiando a la organización permanentemente en el largo plazo y promoviendo una adecuada y regular gestión de la seguridad de la información. (11); en nuestro caso solamente se recomienda la implementación del SGSI.

Castillo en el año 2018, en su tesis tuvo como resultados de la encuesta entre los empleados, se confirmó que no tienen conocimientos ni medidas suficientes para proteger los recursos de información. En la Calificación Global para la evaluación de madurez, el 93% evalúa la información de que esta actividad en el municipio se encuentra en un nivel que no existe según el nivel de madurez ISO/IEC 27001:2013; Evaluación de datos para actividades de seguimiento. 7% Proceso normal de recolección y evaluación no determinado. Como resultado, esta evaluación permite a la empresa tomar acciones preventivas y correctivas en actividades que deben realizarse de manera inmediata a nivel de seguridad para que sean efectivas (12), similarmente a la investigación presentada sobre el conocimiento de seguridad de la información.

Vegas en el 2019, realizó su tesis que tuvo como resultados de este estudio indican que las políticas y controles se han implementado de forma limitada, evidenciando traumáticamente que siendo una universidad, estos no se encuentran documentados o evidenciados, bajo porcentaje de cumplimiento de seguridad de datos y altas críticas a datos y activos en procesos académicos. Por lo anterior, se diseñó basados en la norma NTP ISO/IEC 27001 el sistema de gestión de seguridad de la información con los elementos de control propuestos. (13). A diferencia de nuestra investigación no se diseñó el Sistema de Gestión de Seguridad de la Información, solo se revisó los controles propuestos basado en la NTP ISO/IEC 27001.

Lara en el 2018, desarrollo su investigación que tuvo como resultados: En el Nivel 01: Estado actual; El 61% de los colaboradores entrevistados cree que actualmente existe una inadecuada gestión de las actividades clínicas de

Simedic Diagnóstica S.A.C, mientras que el 39% está de acuerdo con la situación clínica. Y en el nivel 02: seguridad de la información; Se determinó que el 68% de los colaboradores que participaron en la encuesta consideró que aceptaba la oferta de seguridad informática en la clínica Simedic Diagnóstica S.A.C, mientras que el 32% no aceptó la oferta de seguridad de la información. Simedic Diagnóstica S.A. En la clínica se ha finalizado una propuesta de seguridad informática basada en la norma ISO/IEC 27001. C - Piura; 2018, porque la seguridad de los datos está totalmente certificada para garantizar la máxima seguridad para clínicas, empleados y clientes. (14), similarmente de nuestra investigación los trabajadores encuestados opinaron que, Si están de acuerdo con la que se debería realizar la propuesta para la seguridad informática

Albán en el año 2016, realizó la encuesta donde reveló que el 92.00% de los encuestados no está satisfecho con la situación actual, por lo que el 100% de los encuestados expresó la necesidad de implementar una gestión de seguridad de la información; para resolver cualquier problema relacionado con la ejecución de cualquier proceso o solicitud. (15) , similarmente de la investigación presentada existe un gran porcentaje del personal no satisfecho con la situación actual.

### **6.3 RESPONSABILIDAD ÉTICA DE ACUERDO A LOS REGLAMENTOS VIGENTES**

Esta investigación fue elaborada de acuerdo a los lineamientos y reglamentos de la Universidad Nacional del Callao.

Los datos mostrados en esta investigación fueron recogidos y procesados de una manera adecuada sin distorsionar ni adulterar, los datos están fundamentados en el instrumento aplicado al Pre-Test y Post-Test de estudio.

Se respetó a los integrantes que participaron en el estudio, no se hizo ninguna discriminación, de sexo, raza o religión.

Para ello se solicitó autorización de la documentación a utilizar a las personas correspondientes e involucradas en esta investigación.

## CONCLUSIONES

### Conclusión 1:

Se concluye que la seguridad de la información en URA UNAC mejora significativamente en 42.4% gracias a la implementación de la ISO 27001:2013

#### Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,651 <sup>a</sup>	,424	,400	3,112

a. Predictores: (Constante), POSTEST (USANDO APLICATIVO)

### Conclusión 2:

Se concluye que la seguridad de la información en la dimensión confidencialidad en URA UNAC mejora significativamente en 55.3% gracias a la implementación de la ISO 27001:2013

#### Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,744 <sup>a</sup>	,553	,540	2,26880

a. Predictores: (Constante), DORSAL\_POSTEST

### Conclusión 3:

Se concluye que la seguridad de la información en la dimensión disponibilidad en URA UNAC mejora significativamente en 56.8% gracias a la implementación de la ISO 27001:2013



### Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,754 <sup>a</sup>	,568	,556	2,21935

a. Predictores: (Constante), PECTORAL\_POSTEST

#### Conclusión 4:

Se concluye que la seguridad de la información en la dimensión disponibilidad en URA UNAC mejora significativamente en 51% gracias a la implementación de la ISO 27001:2013

### Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,711 <sup>a</sup>	,505	,500	2,11844

a. Predictores: (Constante), PECTORAL\_POSTEST

## RECOMENDACIONES

### Recomendación 1:

Se recomienda que la Seguridad de la Información de la Unidad de Registros Académicos de la Universidad Nacional del Callao sea siempre prioridad en el plan operativo de la institución.

### Recomendación 2:

Se recomienda que los niveles de seguridad sean fuertes para mejorar la confidencialidad de la seguridad de la información de la Unidad de Registros Académicos de la Universidad Nacional del Callao

### Recomendación 3:

Se recomienda que existan copias de seguridad que permitan la disponibilidad en la seguridad de la información de la Unidad de Registros Académicos de la Universidad Nacional del Callao

### Recomendación 4:

Se recomienda que se incluyan servicios de ethikal hacking para que sustenten la integridad de la seguridad de la información de la Unidad de Registros Académicos de la Universidad Nacional del Callao

## REFERENCIA BIBLIOGRÁFICA

1. Smith, J. Implementation of ISO 27001:2013 in Small and Medium Enterprises. University of Oxford. (2019).
2. Wang, L. Assessing the Impact of ISO 27001:2013 on Organizational Performance. Tsinghua University. (2020).
3. Garcia, M. Challenges in Implementing ISO 27001:2013 in Public Sector Organizations. University of Sao Paulo.(2021).
4. Rahman, A. The Role of ISO 27001:2013 in Enhancing Cybersecurity in Financial Institutions. National University of Singapore. (2019).
5. Brown, D. ISO 27001:2013 and its Impact on Information Security Culture. Stanford University.(2020).
6. Kim, S. Effectiveness of ISO 27001:2013 in Preventing Data Breaches. Korea University. (2021).
7. Ali, H. Implementing ISO 27001:2013 in Healthcare Organizations. University of Melbourne. (2019).
8. Gonzalez, R. ISO 27001:2013 and Risk Management in Telecommunications. University of Madrid. (2020).
9. Kumar, P. Cost-Benefit Analysis of ISO 27001:2013 Implementation. Indian Institute of Technology. (2021).
10. Nguyen, T. ISO 27001:2013 in the Context of Cloud Computing. Vietnam National University. (2022).
11. Ramírez, J. Implementación de ISO 27001:2013 en Instituciones Financieras Peruanas. Universidad Nacional Mayor de San Marcos. (2019).
12. Fernández, L. ISO 27001:2013 en el Sector Salud en el Perú. Universidad Peruana Cayetano Heredia. (2020).
13. Pérez, M. Eficacia de ISO 27001:2013 en Empresas de Telecomunicaciones. Pontificia Universidad Católica del Perú. (2021).
14. Torres, S. ISO 27001:2013 en Pequeñas Empresas Peruanas. Universidad de Lima. (2019).
15. García, A. Impacto de ISO 27001:2013 en Universidades Peruanas. Universidad Nacional de Ingeniería. (2020).

16. Vargas, E. ISO 27001:2013 y su Aplicación en Gobiernos Locales. Universidad Nacional del Callao. (2021).
17. López, C. Evaluación de ISO 27001:2013 en el Sector Energético. Universidad Nacional Agraria La Molina. (2022).
18. Martínez, D. ISO 27001:2013 en Empresas de Tecnología. Universidad Peruana de Ciencias Aplicadas. (2019).
19. Rojas, F. ISO 27001:2013 y la Gestión de Riesgos en Bancos. Universidad Ricardo Palma.
20. Sánchez, H. Implementación de ISO 27001:2013 en Instituciones Educativas. Universidad Nacional Federico Villarreal. (2021).
21. Santos D. Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de Consultoría de Software. Tesis de pregrado. Lima - Perú: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería; 2016.
22. Castillo R. Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Pira aplicando la norma ISO/IEC 27001:2013. Tesis de pregrado. Huaraz - Ancash: Universidad Católica los Ángeles de Chimbote, Ingeniería de Sistemas; 2016.
23. Vegas I. Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001. Tesis de pregrado. Piura: Universidad Nacional de Piura, Facultad de Ingeniería Industrial - Escuela Profesional de Ingeniería Informática; 2019.
24. Lara. Propuesta para la seguridad informática basado en la norma ISO /IEC 27001 en la clínica Simedic diagnóstica S.A.C – Piura; 2018. Tesis de pregrado. Piura: Universidad Católica los Ángeles de Chimbote, Ingeniería de Sistemas; 2018.
25. Albán E. Gestión de seguridad de información basado en la norma ISO/IEC 27000 en la Municipalidad Provincial de Talara año 2016. Tesis Magíster. Piura: Universidad Católica los Ángeles de Chimbote, Ingeniería de Sistemas; 2017.

26. Vasconcelos Santillan J. Tecnología de la Información. Segunda ed. Patria GE, editor.  
Mexico: Patria; 2015.
27. Gutiérrez González. Introducción a la Ingeniería. Primera ed. Marcombo , editor. Madrid: Alfaomega; 2016.
28. Cubillos Ospina D. Tecnología De La Información Y Comunicación - Yopal. [Online].; 2012 [cited 2018 Nobiembre 11. Available from:  
<https://sites.google.com/site/ticsyopal5/assignments/homeworkforweekofoctober18th>.
29. Arturo Betancourt S. Origen y evolución de las TIC y aportes a la educación. [Online].; 2012 [cited 2018 Abril 1. Available from:  
<https://www.sutori.com/story/origen-yevolucion-de-las-tic-y-aportes-a-la-educacion>.
30. Villafuerte Quiroga D. solucionespracticas. [Online]. Lima; 2009 [cited 2018 marzo 1.  
Available from: <https://solucionespracticas.org.pe/Descargar/398/3726>.
31. Instituto Nacional de Calidad. INACAL. [Online].; 2016 [cited 2018 Octubre 30. Available from: <https://www.inacal.gob.pe/principal/categoria/ntp>.
32. Garre Gui S, Tortajada Gallego , Segovia Henares , Cruz Allende. Sistema de gestión de la seguridad de la información. Primera ed. España: Editorial UOC; 2018.
33. Vidalina De Freitas FN. Sistema de Gestion de Seguridad de La Informacion. Primera ed. Venezuela: Eae; 2012.
34. sbqconsultores. Consultora de Sistemas de Gestión y Normas ISO. [Online].; 2015 [cited 2018 Enero 27. Available from:  
<https://www.s bqconsultores.es/el-ciclo-dedeming-o-circulo-pdca/>.
35. Daltabuit Godas , Hernandez Audelo. La seguridad de la información. Primera ed. México: Limusa; 2007.
36. Harold F. Tipton MK. Information security management handbook. Sexto ed. Tipton HF, editor. Nueva york: Auerbach; 2008.
37. Miguel Pérez C. Protección de datos y seguridad de la información. Cuarta ed. España:  
Ra-Ma ; 2015.

38. ISO. ISO. [Online]. [Online]. [cited 2017 agosto 01. Available from: Available from: <http://www.iso.org/>.
39. iso27000. Portal de ISO 27001 en español. [Online].; 2017 [cited 2017 Marzo 27. Available from: <http://www.iso27000.es/iso27000.html>.
40. Núñez Ponce J. JULIO NUNEZ DERECHO INFORMATICO. [Online].; 2016 [cited 2016 Marzo 1. Available from: <http://julionunezderechoinformatico.blogspot.com/2016/01/>.
41. elperuano. aprueban el uso obligatorio de la norma tecnica peruana NTP resolucion ministerial n° 004 2016 pcm. [Online].; 2016 [cited 2016 Enero 8. Available from: <https://busquedas.elperuano.pe/normaslegales/aprueban-el-uso-obligatorio-de-lanorma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/>.
42. Rubio JA. isaca. [Online].; 2013 [cited 2013 Noviembre 11. Available from: <http://www.isaca.org/chapters7/Madrid/Events/Documents/Principales%20Novedades%20de%20la%20ISO27001ISO%2027002%20-%20Paloma%20Garcia.pdf>.

## ANEXO

## MATRIZ DE CONSISTENCIA

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPOTESIS GENERAL	VARIABLES	DIMENSIONES
¿De qué manera mejora la seguridad de la información de la Oficina de Registros Académicos y Archivo aplicando la ISO 27001:2013?	Conocer de qué manera se mejora la seguridad de la información de la Oficina de Registros Académicos y Archivo aplicando la ISO 27001:2013	La ISO 27001:2013 Mejora significativamente la Seguridad de la Información de la ORAA – UNAC	ISO 27001:2013	Legal
<b>PROBLEMAS ESPECIFICOS</b>	<b>OBJETIVOS ESPECIFICOS</b>	<b>HIPOTESIS ESPECIFICAS</b>		Estratégica
¿De qué manera influye la confidencialidad de la seguridad de la información de la Oficina de Registros Académicos y Archivo aplicando la ISO 27001:2013?	Conocer de qué manera influye la confidencialidad de la seguridad de la información de la Oficina de Registros Académicos y Archivo aplicando la ISO 27001:2013	La ISO 27001:2013 influye significativamente en la confidencialidad de la seguridad de la información de la Oficina de Registros Académicos	Seguridad de la Información	Técnica
¿De qué manera mejora la disponibilidad de la seguridad de la información de la Oficina de Registros Académicos y Archivo aplicando la ISO 27001:2013?	Conocer de qué manera se mejora la disponibilidad de la seguridad de la información de la Oficina de Registros Académicos y Archivo aplicando la ISO 27001:2013	La ISO 27001:2013 mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros Académicos		Confidencialidad
¿De qué manera se relaciona la integridad de la seguridad de la información de la Oficina de Registros Académicos y Archivo aplicando la ISO 27001:2013?	Conocer de qué manera se relaciona la integridad de la seguridad de la información de la Oficina de Registros Académicos y Archivo aplicando la ISO 27001:2013	La ISO 27001:2013 se relaciona significativamente con la integridad de la seguridad de la información de la Oficina de Registros Académicos		Disponibilidad
				Integridad



# BASE DE DATOS

VAR0000 1	VAR0000 2	VAR0000 3	VAR0000 4	VAR0000 5	VAR0000 6	VAR0000 7	VAR0000 8	VAR0000 9	VAR0000 0	VAR0001 1	pre	VAR0001 3	VAR0001 4	VAR0001 5	VAR0001 6	VAR0001 7
5.00	5.00	1.00	5.00	5.00	5.00	5.00	5.00	4.00	4.00	1.00	45.00	5.00	3.00	5.00	3.00	3.00
4.00	3.00	1.00	3.00	3.00	3.00	5.00	5.00	5.00	4.00	1.00	37.00	5.00	3.00	5.00	3.00	3.00
4.00	4.00	1.00	4.00	4.00	4.00	4.00	4.00	4.00	5.00	1.00	39.00	5.00	4.00	5.00	5.00	4.00
5.00	3.00	1.00	4.00	2.00	3.00	5.00	5.00	5.00	5.00	1.00	39.00	4.00	3.00	4.00	5.00	3.00
5.00	5.00	2.00	5.00	5.00	5.00	5.00	5.00	4.00	4.00	2.00	47.00	4.00	3.00	4.00	5.00	3.00
4.00	3.00	2.00	2.00	3.00	2.00	5.00	5.00	5.00	2.00	2.00	35.00	4.00	2.00	4.00	4.00	3.00
5.00	5.00	2.00	2.00	5.00	2.00	5.00	5.00	4.00	2.00	2.00	39.00	4.00	5.00	4.00	4.00	5.00
4.00	3.00	2.00	2.00	3.00	2.00	5.00	5.00	5.00	2.00	2.00	35.00	4.00	3.00	4.00	4.00	3.00
4.00	4.00	1.00	1.00	4.00	1.00	4.00	4.00	4.00	1.00	1.00	29.00	4.00	4.00	4.00	4.00	2.00
5.00	3.00	2.00	2.00	5.00	2.00	5.00	5.00	5.00	2.00	2.00	38.00	5.00	3.00	5.00	4.00	2.00
5.00	3.00	1.00	1.00	5.00	1.00	3.00	3.00	4.00	1.00	1.00	28.00	5.00	3.00	5.00	4.00	3.00
4.00	4.00	1.00	1.00	5.00	1.00	4.00	4.00	4.00	1.00	1.00	30.00	5.00	2.00	5.00	5.00	2.00
5.00	5.00	1.00	1.00	5.00	1.00	5.00	5.00	4.00	1.00	1.00	34.00	5.00	2.00	5.00	5.00	3.00
4.00	4.00	1.00	1.00	3.00	1.00	5.00	5.00	5.00	1.00	1.00	31.00	5.00	2.00	5.00	5.00	3.00
4.00	4.00	1.00	1.00	4.00	1.00	4.00	4.00	4.00	1.00	1.00	29.00	5.00	4.00	5.00	5.00	2.00
5.00	3.00	1.00	1.00	2.00	1.00	5.00	5.00	5.00	1.00	1.00	30.00	4.00	3.00	4.00	5.00	3.00
5.00	5.00	1.00	1.00	5.00	1.00	5.00	5.00	4.00	1.00	1.00	34.00	4.00	3.00	4.00	5.00	3.00
4.00	3.00	1.00	1.00	3.00	1.00	5.00	5.00	5.00	1.00	1.00	30.00	4.00	3.00	4.00	4.00	3.00
5.00	5.00	1.00	1.00	5.00	1.00	5.00	5.00	4.00	1.00	1.00	34.00	4.00	4.00	4.00	4.00	4.00
4.00	3.00	2.00	2.00	3.00	2.00	5.00	5.00	5.00	2.00	2.00	35.00	4.00	3.00	4.00	4.00	3.00
5.00	5.00	2.00	2.00	5.00	2.00	5.00	5.00	4.00	2.00	2.00	39.00	4.00	3.00	4.00	4.00	3.00
4.00	4.00	2.00	2.00	4.00	2.00	5.00	5.00	5.00	2.00	2.00	37.00	5.00	2.00	5.00	4.00	3.00
4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	44.00	5.00	5.00	5.00	4.00	5.00
5.00	3.00	1.00	1.00	4.00	1.00	5.00	5.00	5.00	1.00	1.00	32.00	5.00	3.00	5.00	5.00	3.00
5.00	5.00	1.00	1.00	4.00	1.00	5.00	5.00	4.00	1.00	1.00	33.00	4.00	4.00	4.00	5.00	4.00
4.00	3.00	1.00	1.00	4.00	1.00	5.00	5.00	5.00	1.00	1.00	31.00	5.00	3.00	5.00	5.00	2.00

**¿Se renuevan las claves de los usuarios de la Base de Datos?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	28	70,0	70,0	70,0
	si	12	30,0	30,0	100,0
	Total	40	100,0	100,0	

**¿Se obliga el cambio de la contraseña de forma automática?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	2	5,0	5,0	5,0
	si	38	95,0	95,0	100,0
	Total	40	100,0	100,0	

**¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	1	2,5	2,5	2,5
	si	39	97,5	97,5	100,0
	Total	40	100,0	100,0	

**¿Las copias de seguridad son encriptados?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	13	32,5	32,5	32,5
	si	27	67,5	67,5	100,0
	Total	40	100,0	100,0	

**¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	1	2,5	2,5	2,5
	si	39	97,5	97,5	100,0
	Total	40	100,0	100,0	

**¿Existen logs que permitan tener pistas sobre las acciones realizadas sobre los objetos de las base de datos?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	1	2,5	2,5	2,5
	si	39	97,5	97,5	100,0
	Total	40	100,0	100,0	

**¿Se tienen lugares de acceso restringido?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	2	5,0	5,0	5,0
	si	38	95,0	95,0	100,0
	Total	40	100,0	100,0	

**¿Se poseen mecanismos de seguridad para el acceso a estos lugares?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	24	60,0	60,0	60,0
	si	16	40,0	40,0	100,0
	Total	40	100,0	100,0	

**¿A este mecanismo de seguridad se le han detectado debilidades?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	5	12,5	12,5	12,5
	si	35	87,5	87,5	100,0
	Total	40	100,0	100,0	

**¿Tiene medidas implementadas ante la falla del sistema de seguridad?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	16	40,0	40,0	40,0
	si	24	60,0	60,0	100,0
	Total	40	100,0	100,0	

**¿Con cuanta frecuencia se actualizan las claves o credenciales de acceso?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	23	57,5	57,5	57,5
	si	17	42,5	42,5	100,0
	Total	40	100,0	100,0	

**¿Se tiene un registro de las personas que ingresan a las instalaciones?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	17	42,5	42,5	42,5
	si	23	57,5	57,5	100,0
	Total	40	100,0	100,0	

**¿Existen metodologías de respaldo de información?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	22	55,0	55,0	55,0
	si	18	45,0	45,0	100,0
	Total	40	100,0	100,0	

**¿Se realizan respaldos de información periódicamente?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	30	75,0	75,0	75,0
	si	10	25,0	25,0	100,0
	Total	40	100,0	100,0	

**¿Existe un administrador de sistemas que controle las cuentas de los usuarios?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	21	52,5	52,5	52,5
	si	19	47,5	47,5	100,0
	Total	40	100,0	100,0	

**¿Existe algún estándar para la creación de contraseñas?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	30	75,0	75,0	75,0
	si	10	25,0	25,0	100,0
	Total	40	100,0	100,0	

**¿Se obliga, cada cierto tiempo a cambiar la contraseña?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	39	97,5	97,5	97,5
	si	1	2,5	2,5	100,0
	Total	40	100,0	100,0	

**¿La organización cuenta con un proceso para dar mantenimiento preventivo al software?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	38	95,0	95,0	95,0
	si	2	5,0	5,0	100,0
	Total	40	100,0	100,0	

**¿La organización cuenta con un proceso para dar mantenimiento correctivo al software?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	5	12,5	12,5	12,5
	si	35	87,5	87,5	100,0
	Total	40	100,0	100,0	

**¿Se tienen software antivirus instalados en los equipos de cómputo?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	2	5,0	5,0	5,0
	si	38	95,0	95,0	100,0
	Total	40	100,0	100,0	

**¿Cuentan con antivirus actualizado?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	1	2,5	2,5	2,5
	si	39	97,5	97,5	100,0
	Total	40	100,0	100,0	

**¿Se tienen instalados anti malware en los equipos de cómputo?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	si	40	100,0	100,0	100,0

**¿Cuenta con licencias de software?**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	39	97,5	97,5	97,5
	si	1	2,5	2,5	100,0
	Total	40	100,0	100,0	

**¿Existe un proceso para mantener las licencias actualizadas?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Existe un proceso para adquirir nuevas licencias?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Los usuarios de bajo nivel tienen restringido el acceso a las partes más delicadas de las aplicaciones?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Se realiza copias de seguridad (diariamente, semanalmente, Mensualmente, etc.)?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Se encuentra un administrador de sistemas en la empresa que lleve un control de los usuarios?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Las copias de seguridad son encriptados?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Hay algún procedimiento para dar de alta a un usuario?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Hay algún procedimiento para dar de baja a un usuario?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿La red cuenta con los equipos y aplicaciones (protección) necesarias para tener una mayor resguardo de intrusos activos (hackers)?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa ?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**En caso de que el equipo principal sufra una avería, ¿existen equipos auxiliares?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Cuando se necesita restablecer la base de datos, se le comunica al administrador?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Se documentan los cambios efectuados?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Es eliminada la cuenta del usuario en dicho procedimiento?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Existen lugares de acceso restringido?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?**

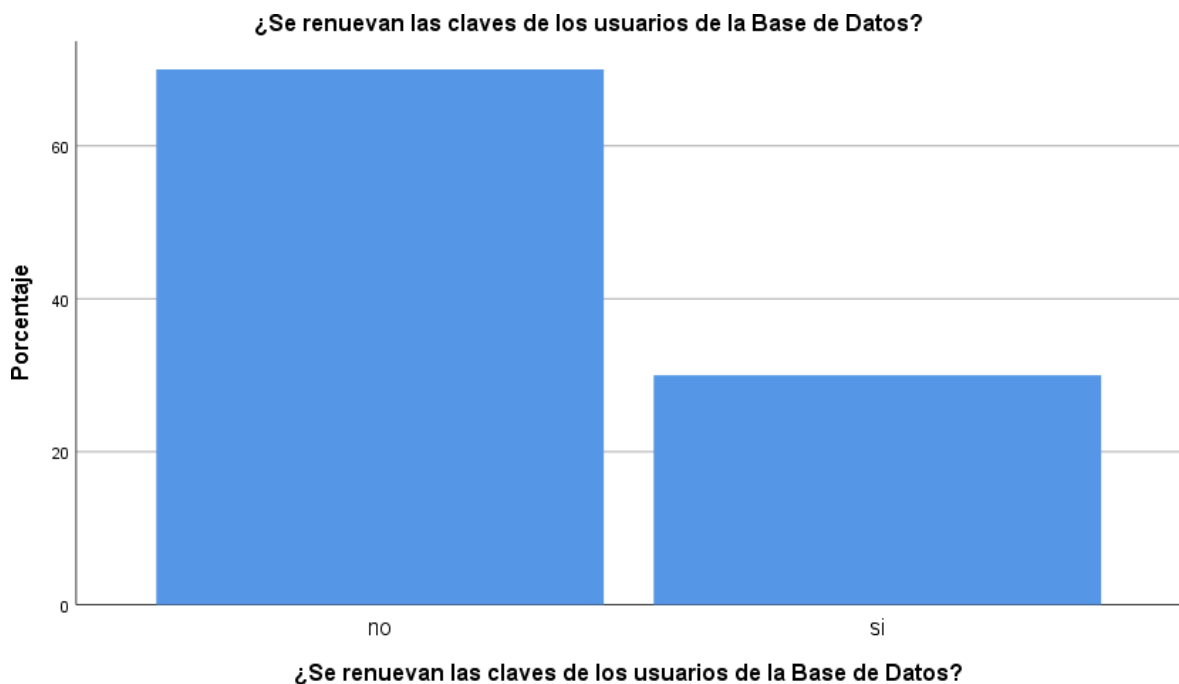
		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

**¿Los enlaces de la red se testean frecuentemente?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0

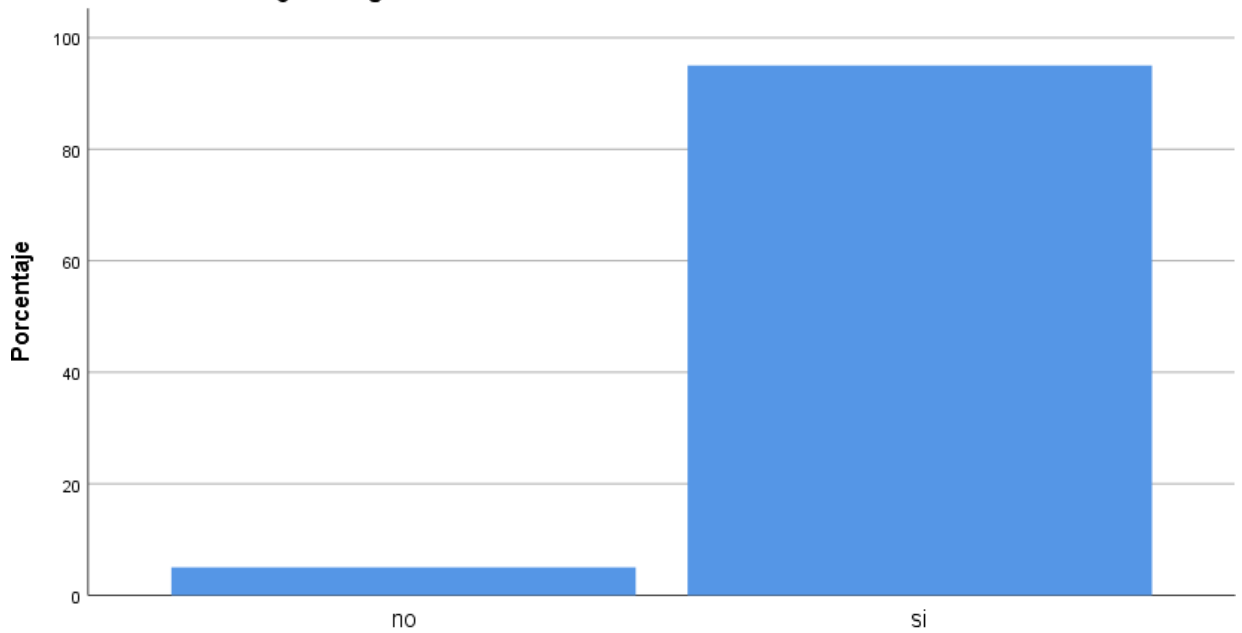
**¿El equipo de cómputo cuenta con suficiente espacio en HD en función de los servicios que otorga?**

		Frecuencia	Porcentaje
Perdidos	Sistema	40	100,0



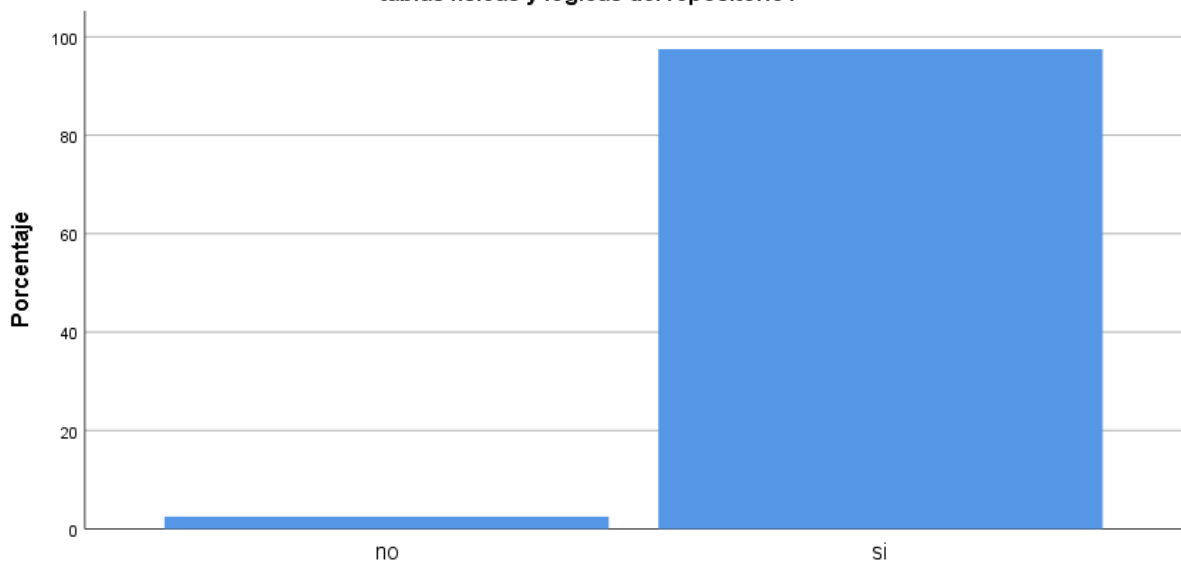


**¿Se obliga el cambio de la contraseña de forma automática?**

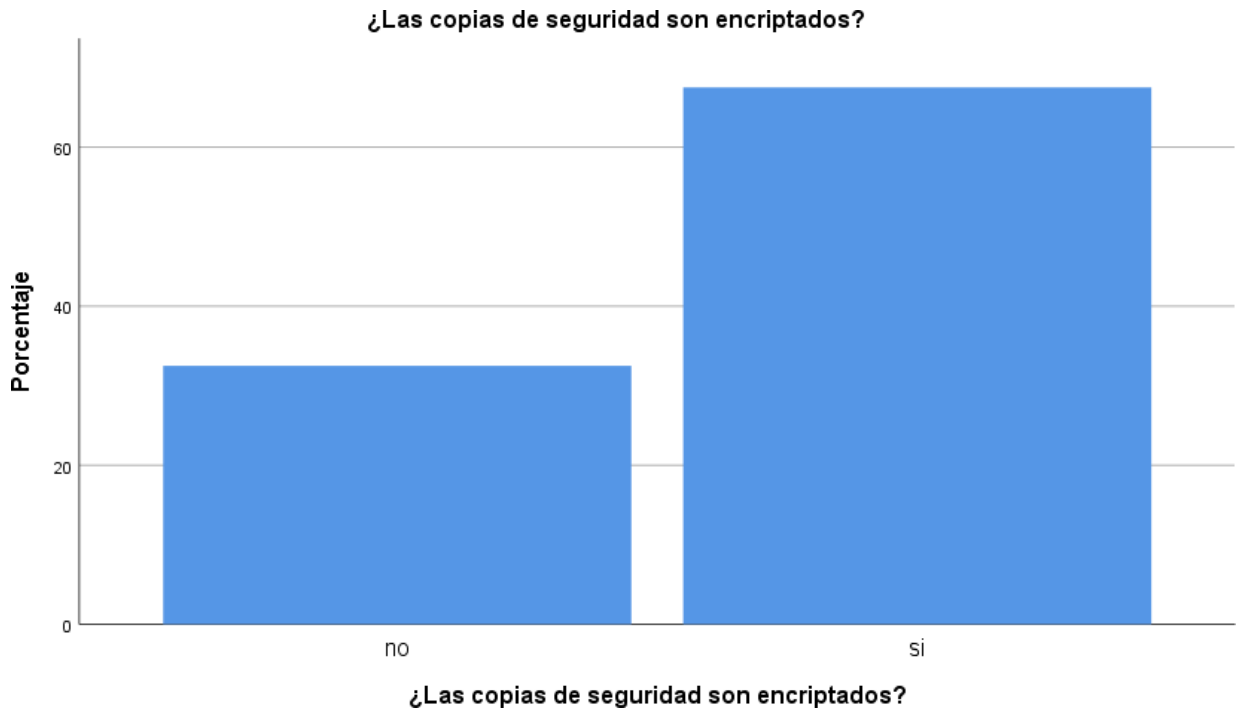


**¿Se obliga el cambio de la contraseña de forma automática?**

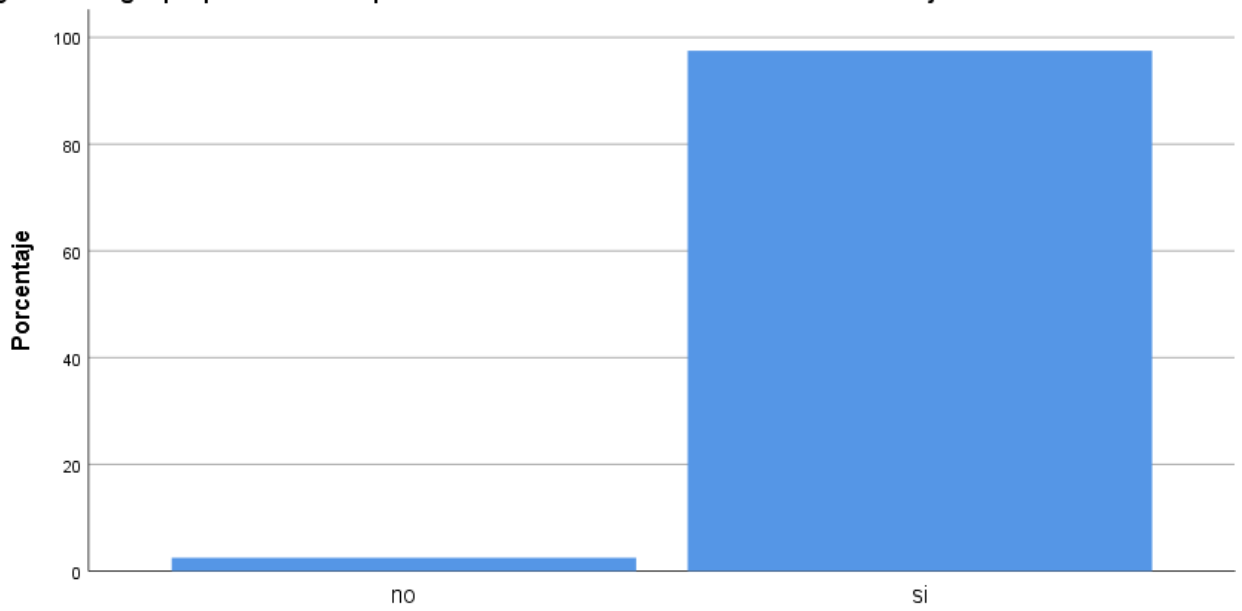
**¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?**



**¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?**

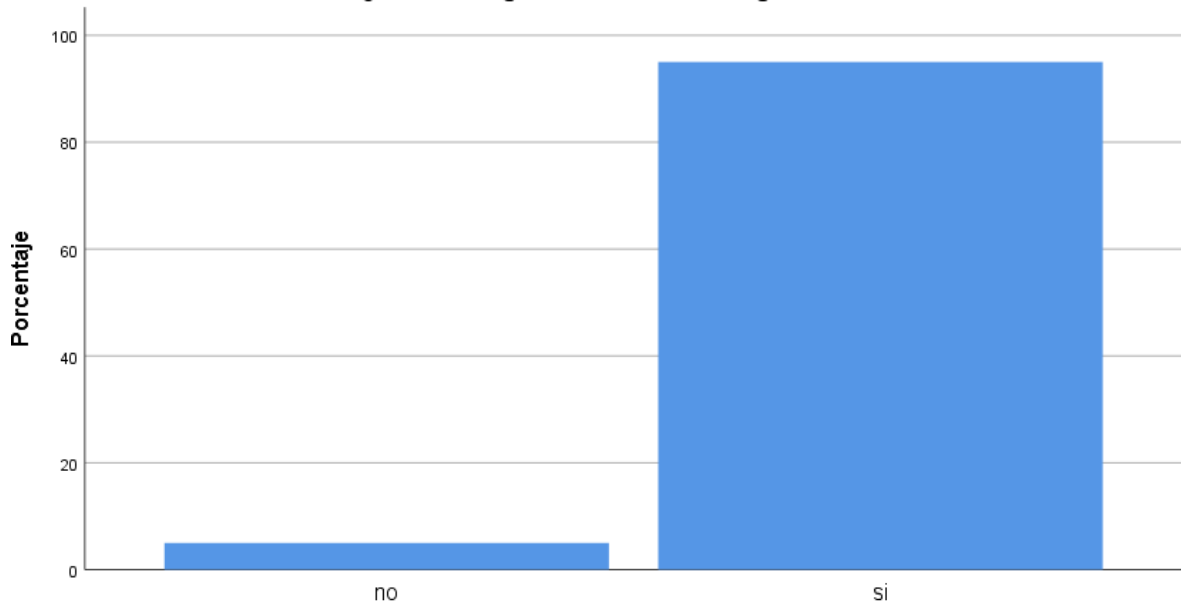


¿Existen logs que permitan tener pistas sobre las acciones realizadas sobre los objetos de las base de datos?

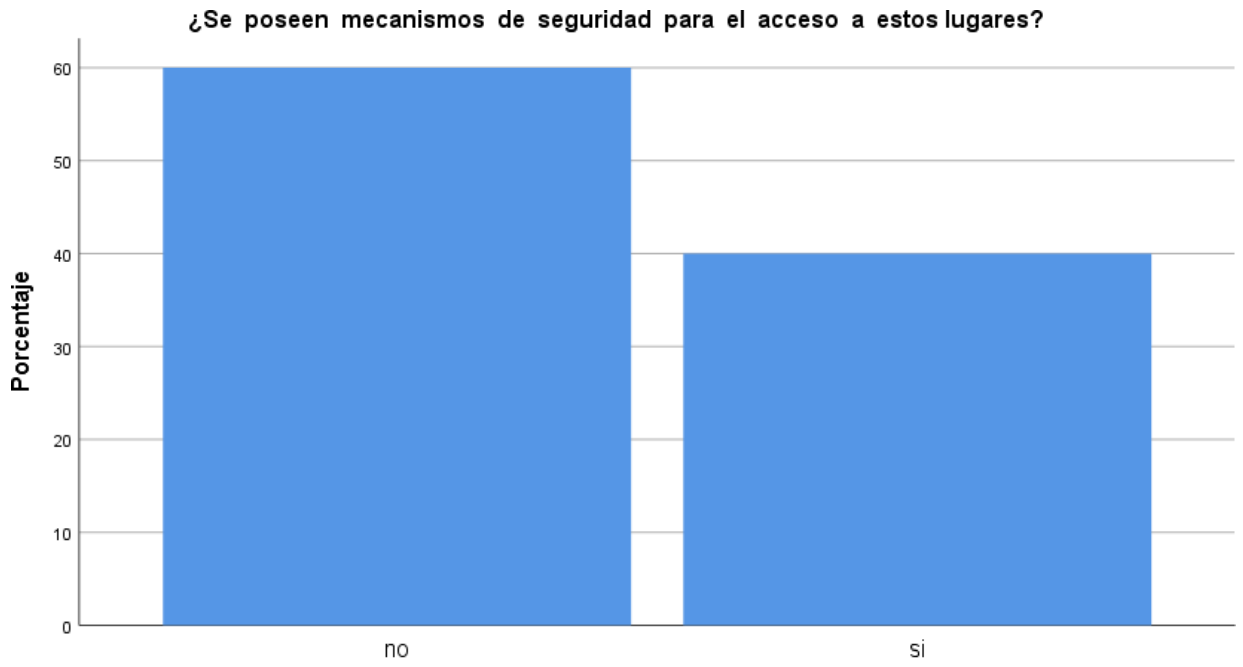


¿Existen logs que permitan tener pistas sobre las acciones realizadas sobre los objetos de las base de datos?

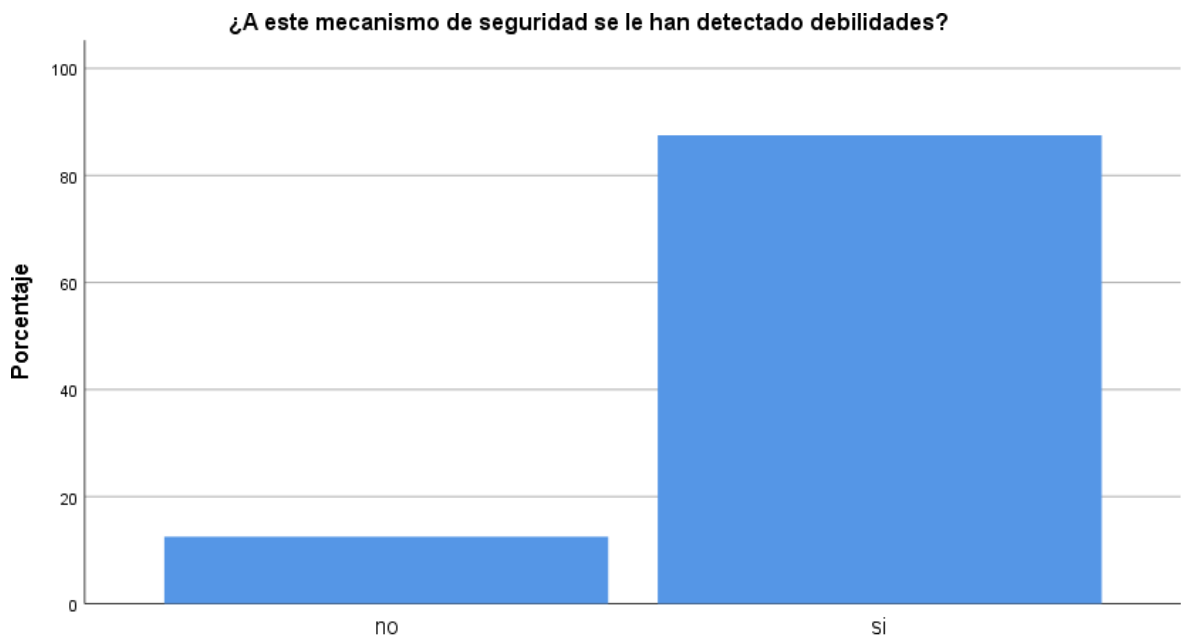
¿Se tienen lugares de acceso restringido?



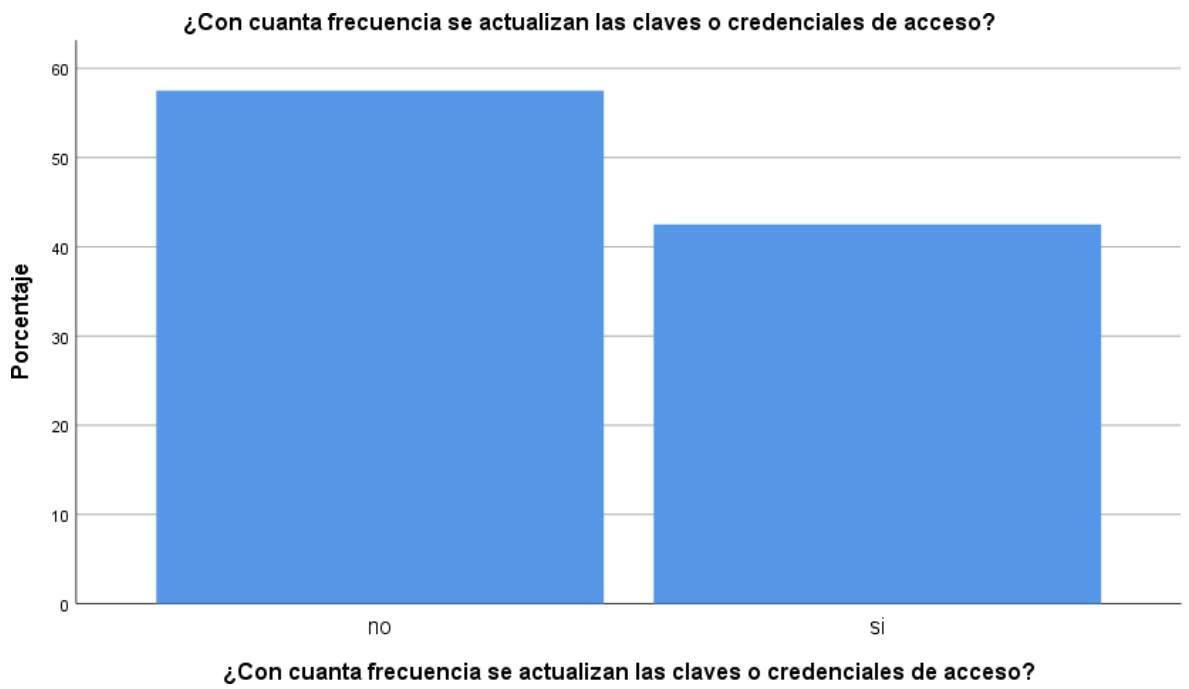
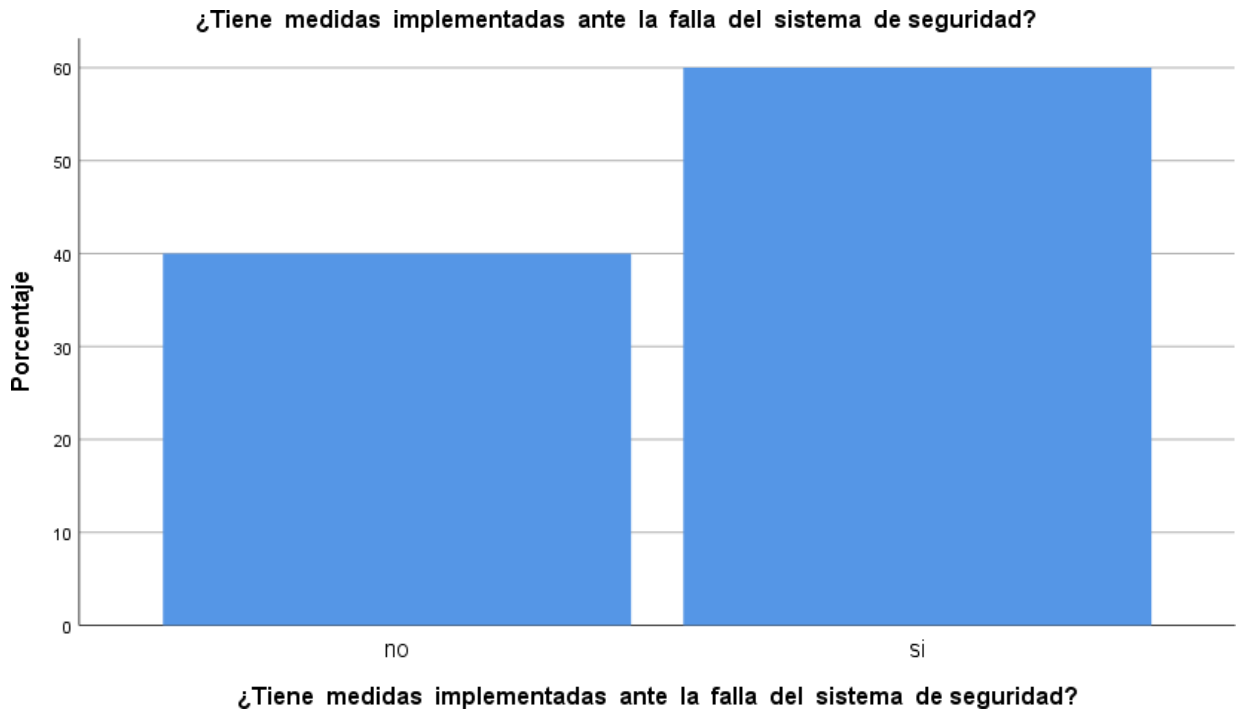
¿Se tienen lugares de acceso restringido?



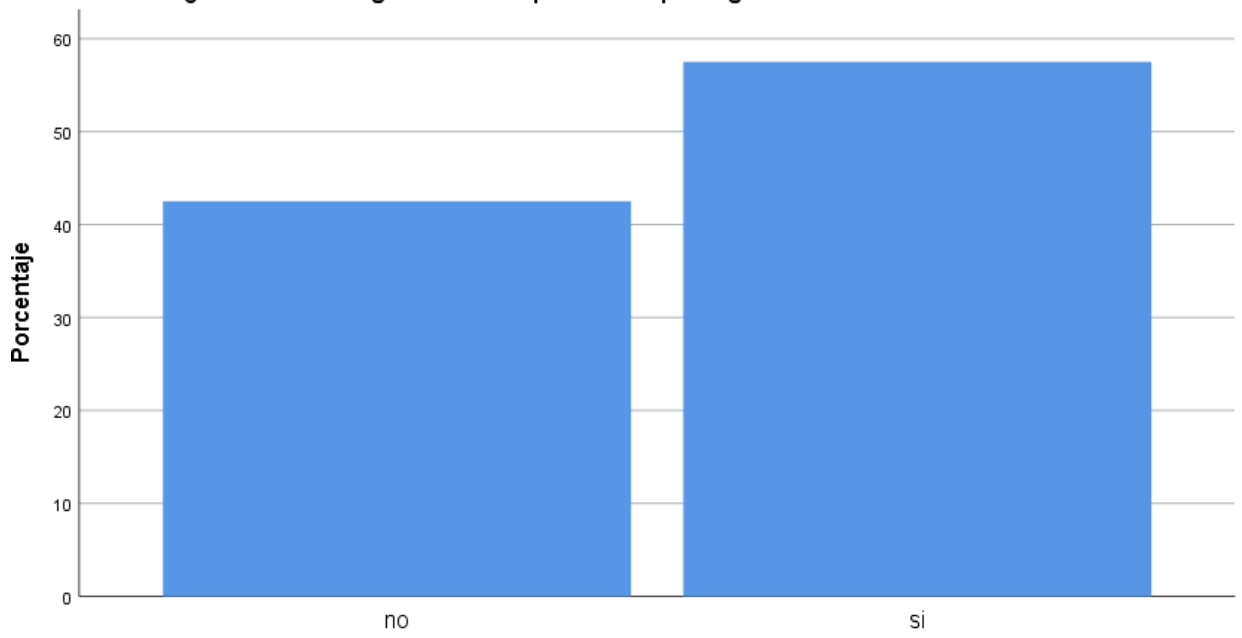
**¿Se poseen mecanismos de seguridad para el acceso a estos lugares?**



**¿A este mecanismo de seguridad se le han detectado debilidades?**

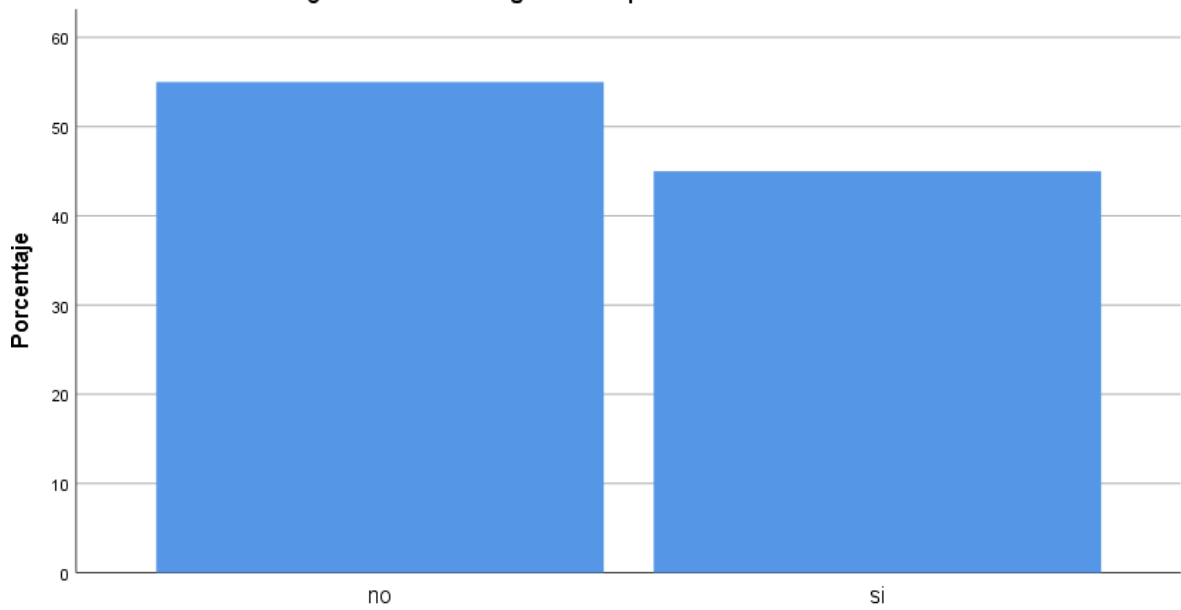


¿Se tiene un registro de las personas que ingresan a las instalaciones?

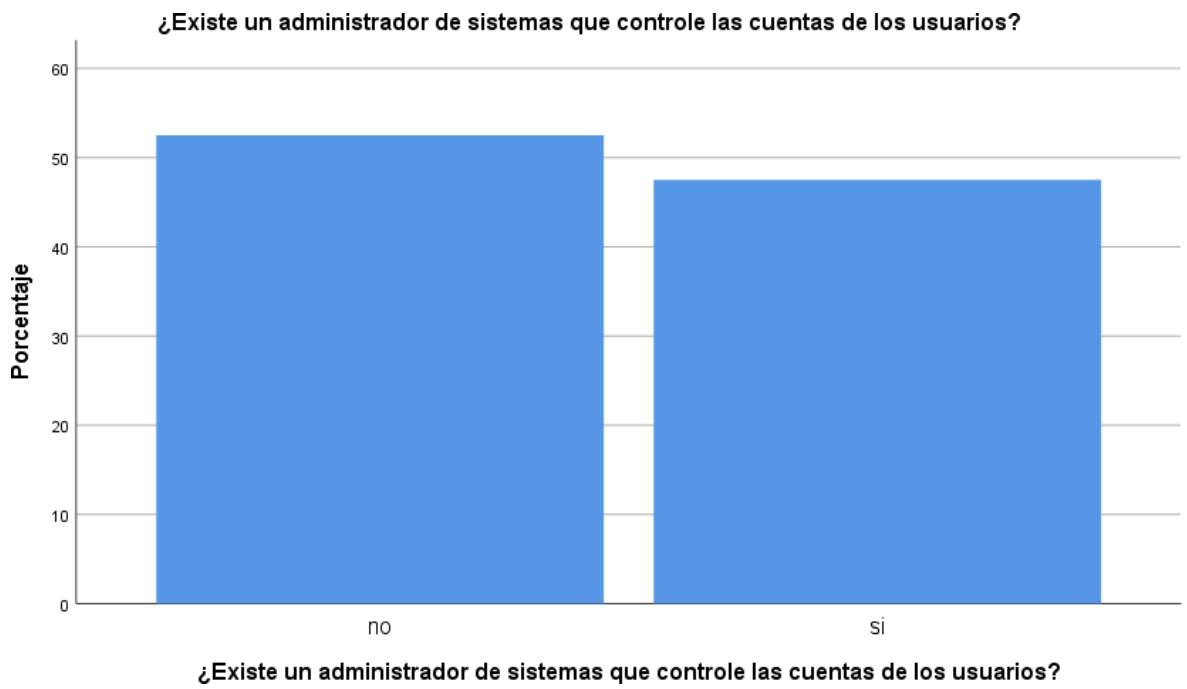
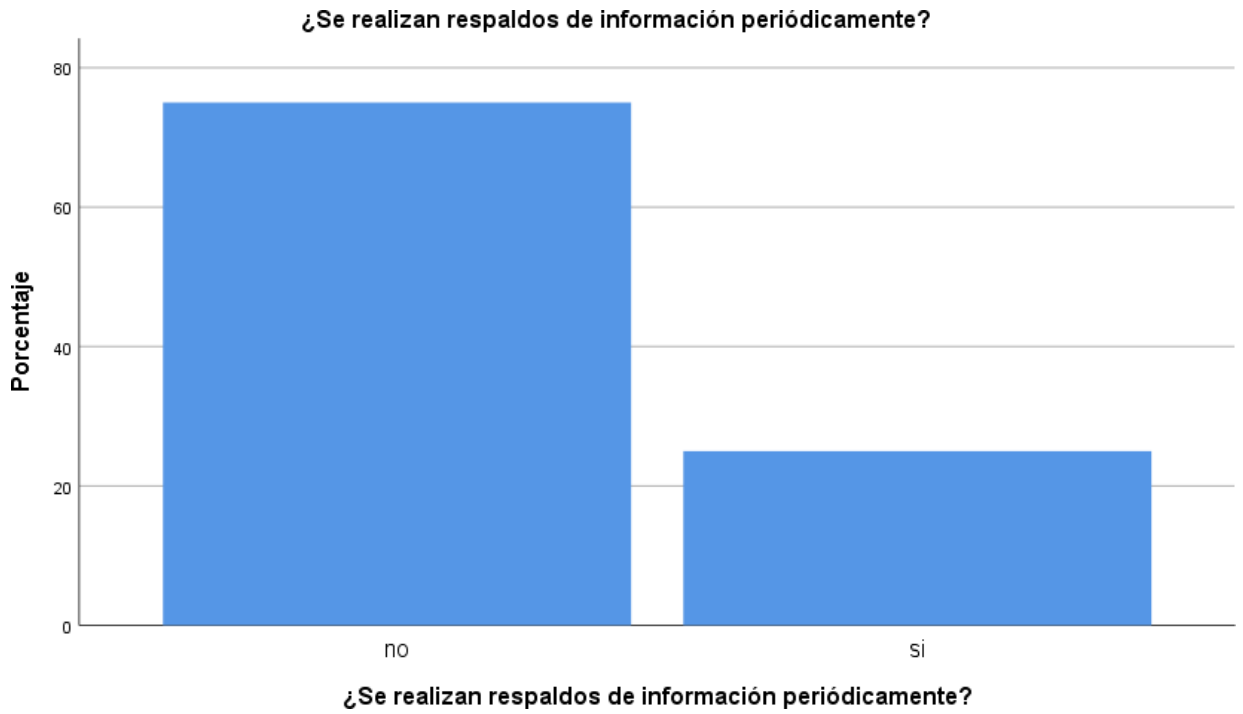


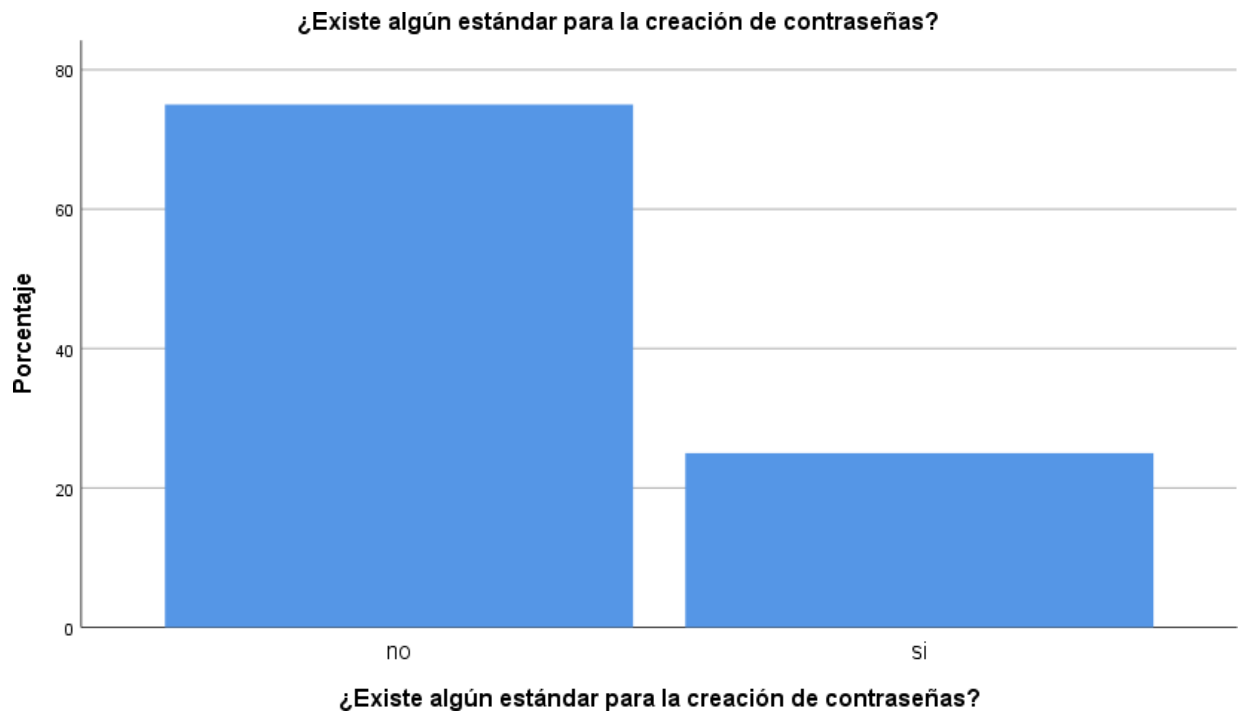
¿Se tiene un registro de las personas que ingresan a las instalaciones?

¿Existen metodologías de respaldo de información?



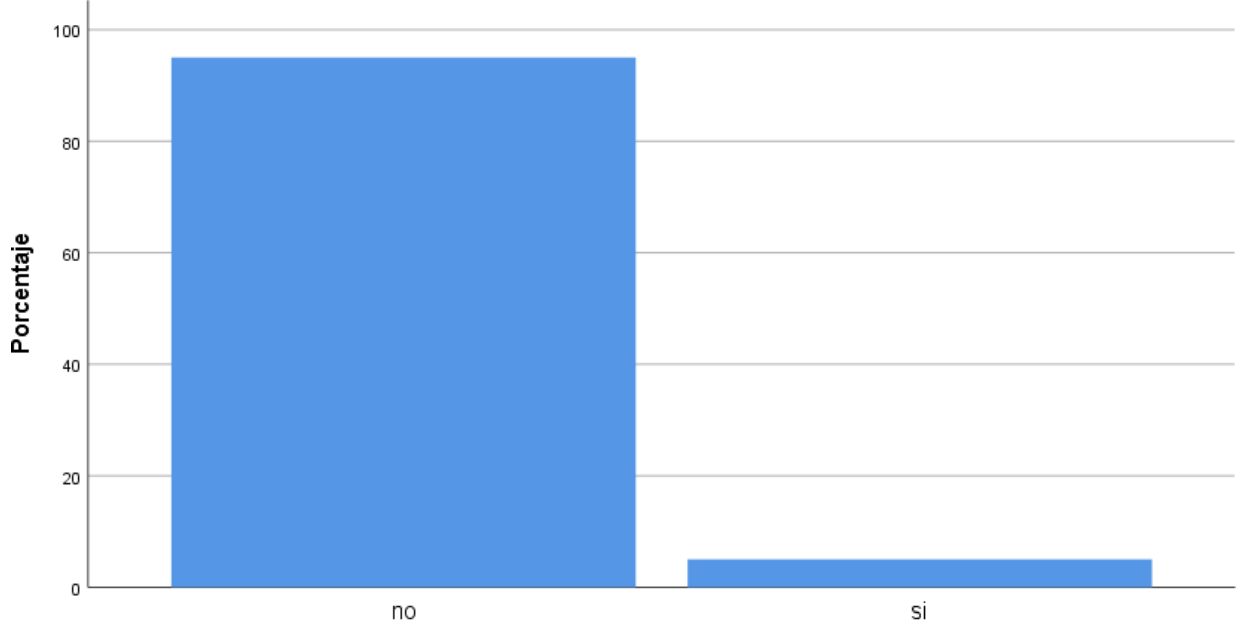
¿Existen metodologías de respaldo de información?





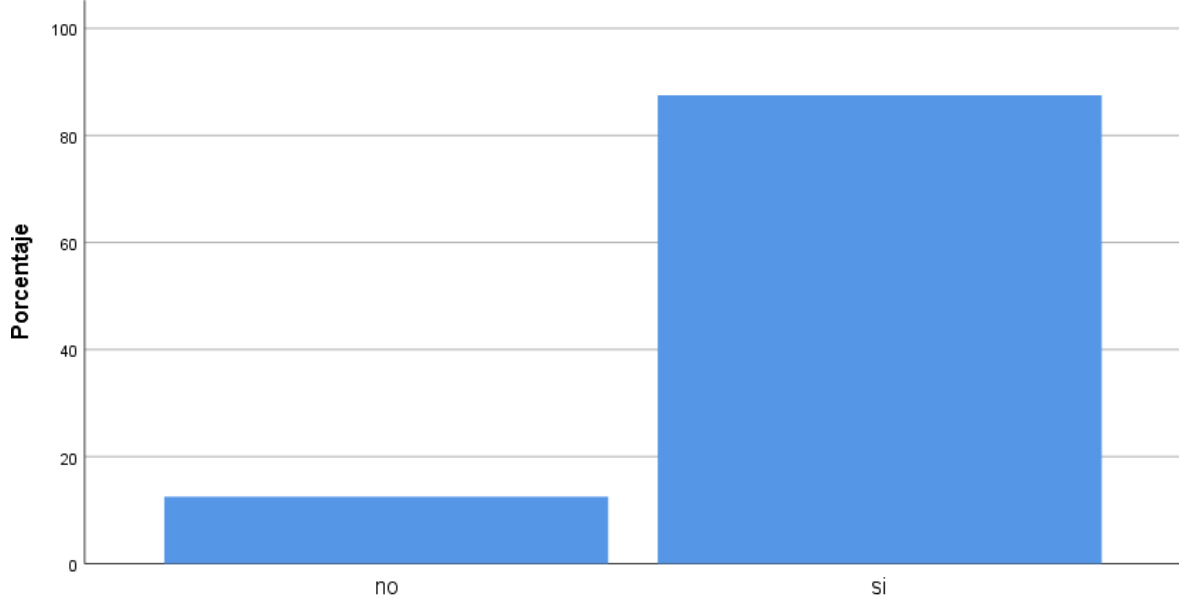


¿La organización cuenta con un proceso para dar mantenimiento preventivo al software?



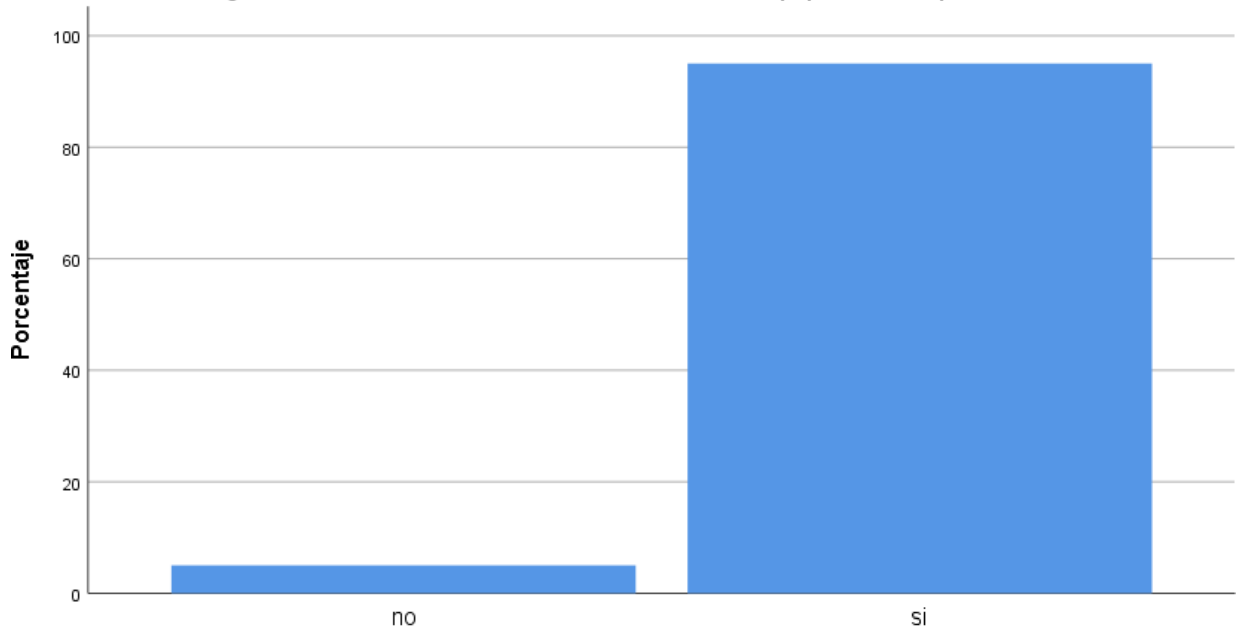
¿La organización cuenta con un proceso para dar mantenimiento preventivo al software?

¿La organización cuenta con un proceso para dar mantenimiento correctivo al software?



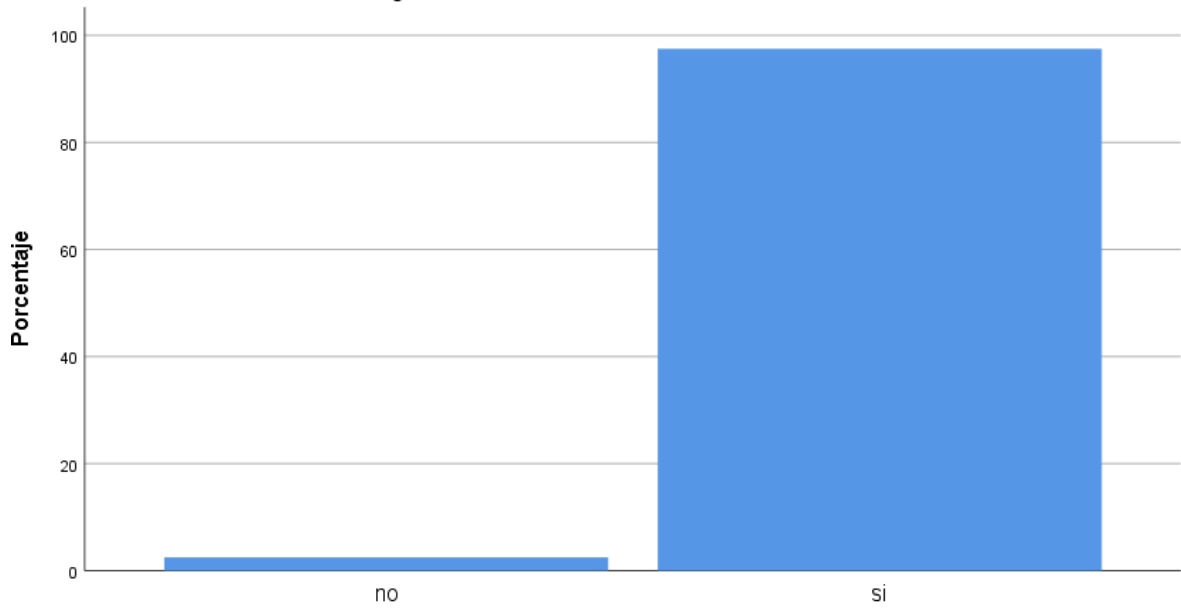
¿La organización cuenta con un proceso para dar mantenimiento correctivo al software?

¿Se tienen software antivirus instalados en los equipos de cómputo?



¿Se tienen software antivirus instalados en los equipos de cómputo?

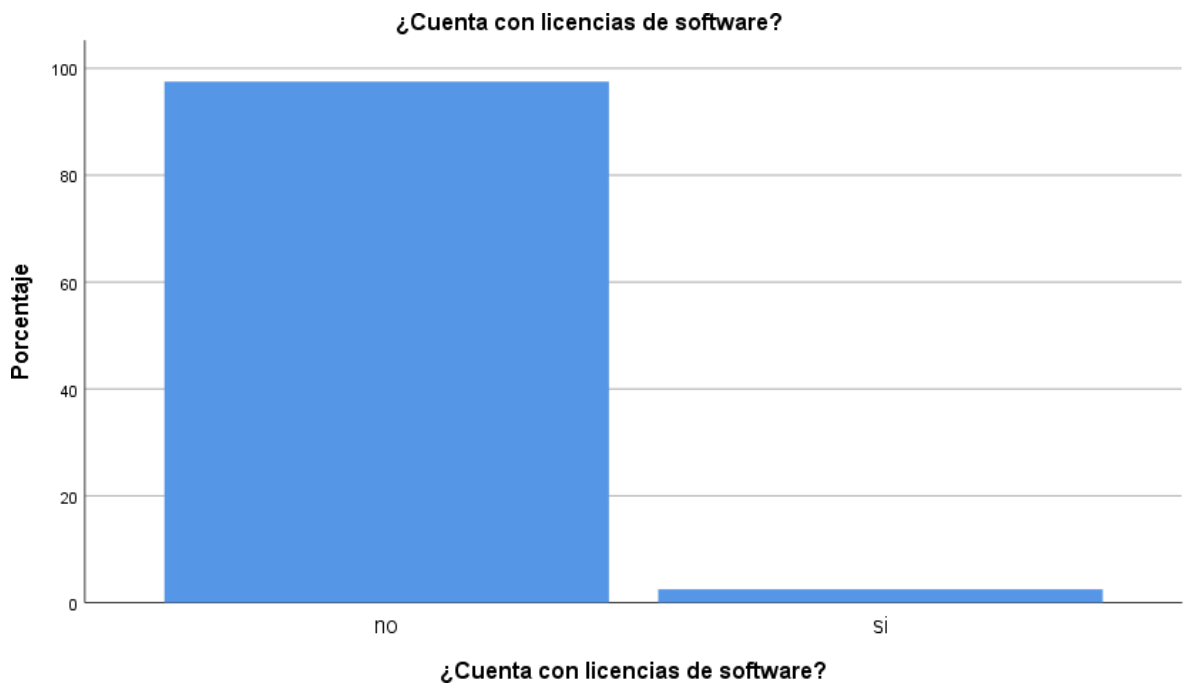
¿Cuentan con antivirus actualizado?



¿Cuentan con antivirus actualizado?



¿Se tienen instalados anti malware en los equipos de cómputo?



¿Cuenta con licencias de software?