UNIVERSIDAD NACIONAL DEL CALLAO

FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

"SEGURIDAD DE LA INFORMACIÓN APLICANDO EL ISO 27001:2013 PARA LA OFICINA DE REGISTROS Y ARCHIVOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DEL CALLAO 2017"

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

PETER JONATHAN MONTALVO GARCÍA

Callao, Enero, 2018

PERÚ

DEDICATORIA

A mi madre, Gabriela García Beunza, y a mi abuelo, Hilario García Cruz. Por haberme apoyado en todo momento, por sus consejos, sus valores, motivación, deliciosas cenas y agradables sobremesas que me han permitido ser una persona de bien; pero más que nada, por su amor.

A mi hermano mayor, Rinaldo Montalvo García, por su ejemplo como profesional y por las pequeñas pero increíbles charlas camino a la universidad, que me han infundado siempre el valor de seguir adelante y ver más allá de lo evidente.

AGRADECIMIENTO

Un especial reconocimiento a mi alma mater: Universidad Nacional del Callao, a la plana docente de la Escuela Profesional de Ingeniería de Sistemas por sus sabias enseñanzas depositadas y darnos las herramientas con las cuales podemos forjar un futuro mejor.

A Luis Alberto Valdivia Sánchez, por su guía en mis primeros pasos en la Facultad de Ingeniería Industrial y de Sistemas.

A la Oficina de Registros y Archivos Académicos, por brindarnos la información necesaria para la elaboración de esta tesis.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

"SEGURIDAD DE LA INFORMACIÓN APLICANDO EL ISO 27001:2013 PARA LA OFICINA DE REGISTROS Y ARCHIVOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DEL CALLAO: 2017"

En la Oficina de Registros y Archivos Académicos, debido a escasez de recursos y tecnología se optó por aplicar, desarrollar, implementar recursos y capacitar al personal trabajador para que de una mejor manera se resguarde la información que se maneja dentro de este centro de información.

En el primer capítulo, se identificó el problema y se estableció los objetivos. En el segundo capítulo, se estableció el marco teórico, lo cual abarca antecedentes del estudio, marco conceptual, entre otros. En el tercer capítulo, se indicó las variables de estudio y la hipótesis planteada, mientras que en el cuarto capítulo se indicó la metodología de investigación. En el quinto y sexto capítulo se muestra los resultados obtenidos y la discusión de estos, respectivamente.

La implementación de la ISO 27001:2013 Seguridad de la información como propuesta de solución al nivel de seguridad en la Oficina de Registros y Archivos Académicos mejoró el nivel de confidencialidad, del 67% al 97%; disponibilidad, del 28% a 95%; e integridad, del 17% al 95%.

PALABRAS CLAVES: ISO 27001:2013, SISTEMAS DE INFORMACIÓN, CONFIDENCIALIDAD, DISPONIBILIDAD, INTEGRIDAD, UNAC.

ABSTRACT

"SECURITY OF INFORMATION APPLYING ISO 27001: 2013 FOR THE OFFICE OF RECORDS AND ACADEMIC ARCHIVES OF THE NATIONAL UNIVERSITY OF CALLAO: 2017"

In the Office of Academic Records and Archives, due to shortage of resources and technology, it was decided to apply, develop, implement resources and train the working personnel so that a better way to protect the information that is handled within this administrative center.

In the first chapter, the problem was identified and the objectives were established. In the second chapter, the theoretical framework was established, which includes the background of the study, conceptual framework, among others. In the third chapter, the study variables and the proposed hypothesis were indicated, while in the fourth chapter the research methodology was indicated. The results obtained and the discussion of these, respectively, are shown in the fifth and sixth chapters.

The implementation of ISO 27001: 2013 Information security as a solution proposal to the security level in the Office of Academic Records and File improved the level of confidentiality, from 67% to 97%; availability, from 28% to 95%; and integrity, from 17% to 95%.

KEYWORDS: ISO 27001:2013, INFORMATION SYSTEMS, CONFIDENTIALITY, AVAILABILITY, INTEGRITY, UNAC.

INTRODUCCIÓN

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

La Universidad Nacional del Callao cuenta con una oficina de registros y archivos académicos (ORAA); ORAA que se encarga de la administración y resguardo de la información de los alumnos y egresados. Es aquí donde parte nuestra investigación, preocupados por si cuentan con estándares de seguridad de la información.

Por ello se utilizará la ISO 27001; norma estándar que nos permite saber si la ORAA cuenta con los lineamientos básicos que le permitan el resguardo de la información del alumno.

Así también se podrá mejorar los lineamientos de seguridad y de prevención antes pérdida de información y ataques externos.

I. PLANTEAMIENTO DE LA INVESTIGACIÓN

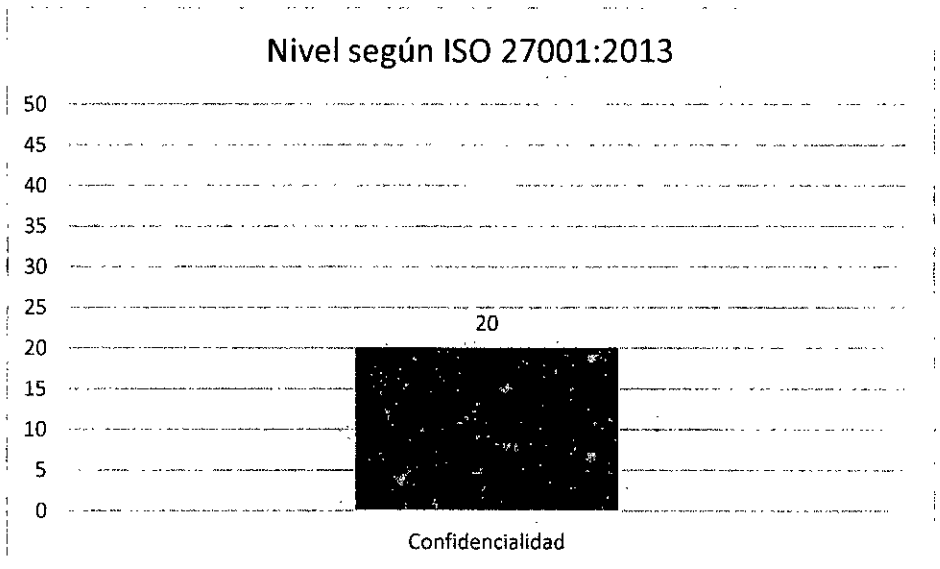
1.1. Identificación del problema

La Universidad Nacional del Callao tiene cargo la Unidad de Archivo General, tiene como misión, organizar, administrar y conservar el fondo documental de la UNAC, como un Sistema Institucional de Archivos de las 11 Facultades que conforman la Institución, siguiendo los actuales procedimientos técnicos-archivísticos que trabaja conjuntamente con la Oficina de Registros y Archivos Académicos y la Unidad de Archivo General de la Universidad Nacional del Callao, para cumplir su misión, dirigida a la comunidad universitaria, tiene la finalidad que se dedica al buen funcionamiento del fondo documental de Archivo General de la UNAC, lo cual muestra un reducido control de ello.

En este punto es donde radica el mayor problema de este caso, ya que con respecto a la seguridad de estos fondos documentales es inseguro, no encontramos las medidas preventivas y reactivas de la Oficina de Registros y Archivos Académicos y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la integridad y disponibilidad de datos y de la misma; ya que se ha evidenciado posibles atacantes que aprovechan para acceder al sistema y poder adulterar la información que maneja esta entidad.

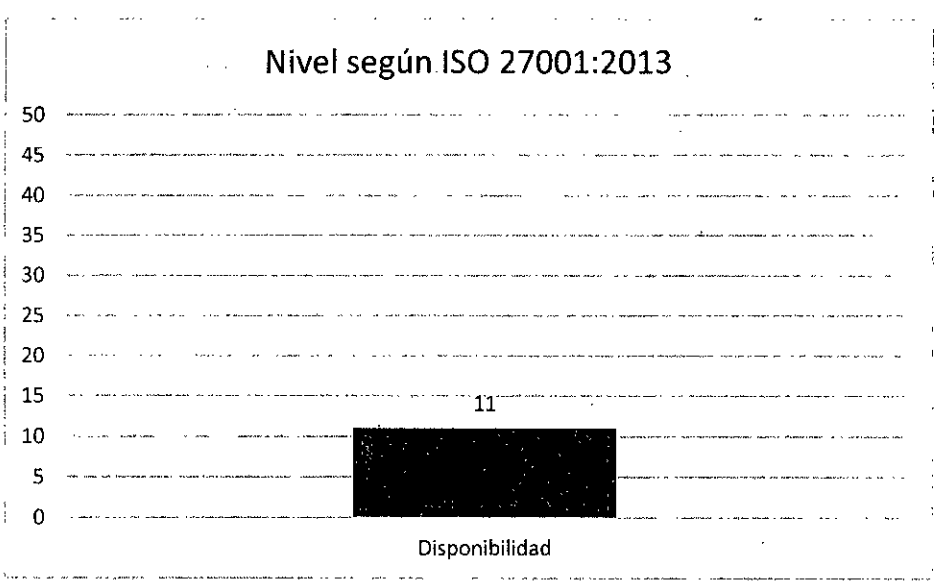
Se realizó la entrevista al director de ORAA en fecha 14 de Junio de 2017 y se evidenció mediante un cuestionario la problemática de la confidencialidad, integridad y disponibilidad.

FIGURA N° 1 Gráfico de Nivel de Confidencialidad de Información de ORAA.



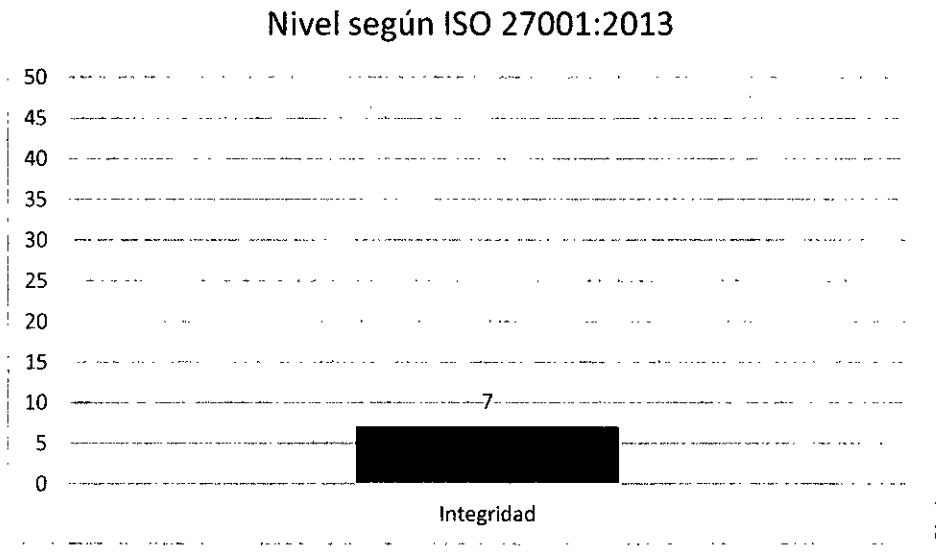
Fuente: Elaboración propia.

FIGURA N° 2 Gráfico de Nivel de Disponibilidad de Información de ORAA



Fuente: Elaboración propia.

FIGURA N° 3 Gráfico de Nivel de Integridad de Información de ORAA



Fuente: Elaboración propia.

1.2. Formulación de problemas

De lo anteriormente planteado, se obtiene los siguientes problemas:

1.2.1. Problema General

PG: ¿De qué manera mejora la seguridad de la información de la Oficina de Registros y Archivos Académicos aplicando la ISO 27001:2013?

1.2.2. Problemas específicos

P1: ¿De qué manera influye la confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos aplicando la ISO 27001:2013?

P2: ¿De qué manera mejora la disponibilidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos aplicando la ISO 27001:2013?

P3: ¿De qué manera se relaciona la integridad de la seguridad de la

información de la Oficina de Registros y Archivos Académicos aplicando la ISO 27001:2013?

1.3. Objetivos de la investigación

1.3.1. Objetivo General

OG: Conocer de qué manera se mejora la seguridad de la información de la Oficina de Registros y Archivos Académicos aplicando la ISO 27001:2013.

1.3.2. Objetivos Específicos

P1: Conocer de qué manera influye la confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos aplicando la ISO 27001:2013.

P2: Conocer de qué manera se mejora la disponibilidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos aplicando la ISO 27001:2013.

P3: Conocer de qué manera se relaciona la integridad de la seguridad de la información de la Oficina de Registros y Archivos Académicos aplicando la ISO 27001:2013.

1.4. Justificación

1.4.1. Justificación tecnológica

Según Kenneth (2004, p4), en la actualidad se reconoce ampliamente que el conocimiento de seguridad de información es esencial para los usuarios por que la mayoría de las organizaciones necesita información segura,

confiable y confidencial para sobrevivir y prosperar.

1.4.2. Justificación legal

De acuerdo al Decreto Supremo N°030-2002-PCM de Modernización de la Gestión Pública y a la Ley N°27658 Ley de Modernización de la Gestión del Estado, la modernización de la gestión pública comprende la seguridad de la información.

1.4.3. Justificación institucional

La visión de la UNAC es ser una universidad acreditada y con liderazgo a nivel nacional e internacional, con docentes altamente competitivos calificados con infraestructura moderna, que se desarrolla en alianzas estratégicas con instituciones públicas y privadas. Por ende, acorde a la visión de la Universidad Nacional del Callao, se debe modernizar, siendo la seguridad de la información de la Oficina de Registros y Archivos Académicos un objetivo fundamental para nuestra institución.

1.5. Limitaciones y Alcances

1.5.1. Limitaciones

Las limitaciones de esta investigación nos comprendieron las restricciones que se tuvo para ejecutarla:

- La presente investigación en el tiempo sólo alcanza o comprende, tantas años como las ISO 27001:2013 cambie a futuro a otras versiones.

- El presupuesto se limita a según el ambiente a analizar y a lo ausente en invertir.
- El personal se limita a una cantidad finita de 21 trabajadores en el área afectada.
- Los investigadores sólo pueden dedicar 10 horas a la semana a la investigación por temas laborales, académicos/profesionales, entre otros.
- Los investigadores sólo tienen acceso a la información web de 9:00am – 6:00pm (horario de oficina) a tal centros de información ORAA y solo se obtuvo acceso presencial por 2 horas por temas confidenciales y permisos de accesos de parte de jefatura de ORAA.
- Existen limitaciones como la infraestructura tecnológica y centro de equipo.

1.5.2. Alcances

- Se obtuvo la aprobación de parte del director de ORAA en cuestión de días lo cual hablando de una institución pública pudo demorar semanas.

II. MARCO TEÓRICO CONCEPTUAL

La elaboración de este marco teórico tiene como finalidad poder estructurar elementos e instrumentos que permitan orientar la investigación, la cual se emprende en busca de explicaciones e interpretaciones relacionadas con la seguridad de la información en Oficina de Registros y Archivos Académicos de la Universidad Nacional del Callao.

2.1. Antecedentes del estudio

A.- ANTECEDENTES NACIONALES

• En el año 2011, Ampuero Chang, Carlos Enrique, en la tesis titulada **"Diseño de un sistema de gestión de seguridad de información para una compañía de seguros"** para obtener el Título de Ingeniero Informático, sustentada y aprobada en la Pontificia Universidad Católica del Perú; incluyó implementar la norma ISO/IEC 27001:2005 que contiene los requisitos básicos que debe obtener todo sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma sobre la cual se certifican, por auditores externos, los SGSI de las organizaciones. A pesar de no ser obligatoria la implementación de todos los controles, se debe argumentar la no aplicabilidad de los controles no implementados. Recomienda el uso del Ciclo Plan - DO - Check - Act para el diseño de un SGSI.

• En el año 2005, Romero Echevarría, Luis Miguel, en la tesis **"Marco conceptual de los Delitos Informáticos"** para obtener el Grado Académico de Magíster en Computación e Informática, sustentada y aprobada en la Universidad Nacional Mayor de San Marcos del Perú; nos

dice que si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas. Y si a ello se agrega que existen Bancos de Datos, empresas o entidad dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a in Estado o particulares; se comprenderá que está en juego o podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

En su trabajo de investigación nos habla también que los Delitos Informáticos en el Perú están tipificados; pero que existen normas que indirectamente sancionan las conductas en las que se intervenga con hardware o software, como por ejemplo, la Ley de Derechos de Autor, regulada por el Decreto Legislativo N° 822, el que sanciona a los que copien, usen o adquieran un programa sin permiso del autor, sin mencionar en ningún momento que esto sería un Delito Informático; en segundo lugar tenemos la Resolución Ministerial N° 622-96MTC/15.17, con la que se aprueba la Directiva N° 002-96-MTC/15.17 referida a los Procedimiento de Inspección y requerimiento de información relacionados al Secreto de las Telecomunicaciones y Protección de Datos, ordenándose con ella a las empresas de telecomunicaciones a mantener en secreto la información de sus abonados o usuarios, sancionándose a la empresa si la información es entregada o la obtiene terceros mas no así a estos terceros.

• En el año 2011, Aliaga Flores, Luis Carlos, en la tesis titulada **"Diseño de un sistema de gestión de seguridad de información para un instituto educativo"** para obtener el Título de Ingeniero Informático, sustentada y aprobada en la Pontificia Universidad Católica del Perú;

Como resultado del incremento de la dependencia de las organizaciones respecto a la tecnología para el manejo de su información y del incremento de interconectividad en el ambiente comercial, la información cada vez está más expuesta a una variedad más amplia y sofisticada de amenazas y vulnerabilidades. Estas amenazas pueden ser internas, externas, premeditadas, accidentales, etc. En la mayoría de los casos mencionados, se generan diversas pérdidas dentro de la organización, siendo las reputacionales las más difíciles de contrarrestar. Por tanto, deberían aplicarse marcos y políticas de control implementadas dentro de una organización para minimizar los riesgos y asegurar la continuidad del negocio. En algunos sectores de la industria, existen entes reguladores que establecen normas obligatorias y recomendadas con respecto a dichos marcos y políticas de la seguridad de información. Sin embargo, en el sector educativo no existen leyes o normas establecidas por parte del Ministerio de Educación que regulen la seguridad de información dentro de las organizaciones bajo su jurisdicción. En consecuencia, se genera una falta de conocimiento e interés de dicho tema en las instituciones educativas En muchos casos, la razón por la cual estas instituciones educativas no han implementado estas políticas de seguridad de información es porque aún no han tenido algún incidente de seguridad relativamente grave, lo cual comprueba que las entidades peruanas siguen

siendo reaccionarias y no preventivas.

B.- ANTECEDENTES INTERNACIONALES

• En el año 2011, Guerra Valdivia, Alicia Rubí, en la tesis titulada **"Delitos Informáticos – Caso de Estudio"** para obtener el Grado Académico de Magister en Ingeniería en Seguridad y Tecnologías de la Información, sustentada y aprobada en el Instituto Politécnico Nacional de Ecuador; concluyó que los sistemas de información no deben ser descalificados, tampoco pretende demeritar las innumerables ventajas que su utilización puede conllevar para el beneficio social. Por lo contrario, se trata de centrar la mirada en aquellos sujetos que hacen mal uso de estos recursos, con la finalidad de obtener beneficios personales, a costa del bienestar particular o común de otros individuos.

• En el año 2010, Rosendo A. Mendoza Prado, en la tesis titulada **"Sistema De Gestión Para La Seguridad De La Información Caso: Centro De Tecnología De Información Y Comunicación Del Decanato De Ciencias Y Tecnología - Ucla"** para optar al grado de Magíster Scientiarum en Ciencias de la Computación, sustentada y aprobada en el Instituto Politécnico Nacional de Ecuador, El presente trabajo propone un Sistema de Gestión para la Seguridad de la Información (SGSI) en el Centro de Tecnología de Información y Comunicación (CTIC) del Decanato de Ciencias y Tecnología de acuerdo al estándar internacional ISO/IEC 27001:2005, debido a que las medidas actuales de control para satisfacer los requisitos mínimos en seguridad han sido efectivas sólo parcialmente.

Previamente se debió: (a) Diagnosticar la situación actual del CTIC en materia de seguridad de la información; y (b) Determinar la factibilidad de la propuesta presentada. Posteriormente se diseñó el SGSI, basado en la fase de planeación de la norma ISO/IEC 27001:2005 y en los controles de la norma ISO/IEC 27002:2005. Como metodología de Análisis de Gestión del Riesgo (AGR) se empleó MAGERIT versión 2.0, y la herramienta ISO27K de la ISO27001 Security Home. El estudio está enmarcado en la modalidad de "Proyecto Factible" apoyado en la investigación monográfica documental y de campo. En esta investigación científica se determinó que el Nivel de Madurez del SGSI actual del CTIC es del 42.69%, con la existencia de 22 amenazas importantes, de las cuales se estima reducir su riesgo hasta un nivel aceptable al implantar los controles que se proponen como correctivo. Vale destacar que la adopción de una metodología sólida para la gestión del riesgo permite descubrir los puntos vulnerables de un sistema de información lo que permite tomar los correctivos necesarios para su tratamiento.

2.2. Marco conceptual

2.2.1. Seguridad

La seguridad es una forma de gestión empresarial inteligente, para prevenir de las tres amenazas de la era digital: las responsabilidades, los pleitos y las pérdidas. En este mismo orden de ideas, la seguridad es un medio para conseguir un fin, y ese fin es la confianza, donde es una parte esencial de proposición de valor, como en la banca, la seguridad se convierte en un

factor facilitador crítico según lo expresado por MCCarthy, M., y Campbells., (2002).

Mientras que Cheswick, W., y Bellovin, S., (1994) señala que "Hablando ampliamente, la seg2uridad es evitar que alguien haga cosas que no quieres, que haga con o desde tu ordenador o alguno de sus periféricos" para estos expertos la seguridad es mantener el control.

Asimismo, Schneier, B., (2002) expresa que "La seguridad es un proceso, no un producto", es decir, la seguridad no es lo mismo que el conjunto de medidas de seguridad. La seguridad considerada en esta investigación, es la de crear medidas de control para protegerse de algunos riesgos que se expone las organizaciones, en este caso las universidades.

2.2.2. Seguridad de la información

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.

De igual manera, INFOSEC Glossary (2000) define la Seguridad Informática y mencionada por Aceituno, V., (2004) como "Las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los Sistemas de Información, incluyendo hardware, software,

firmware y aquella información que procesan, almacenan y comunican".

Asimismo, La seguridad de la información es un proceso en que involucra gran número de elementos, como: aspectos tecnológicos, de gestión organizacionales, de recursos humanos, de índole económica, de negocios, de tipo legal, de cumplimiento, etc.; abarcando no solo aspectos informáticos y telecomunicaciones sino también aspectos físicos, medioambientales, humanos, etc. (Areitio, 2008)

La Seguridad de la Información se logra con la implantación de un conjunto adecuado de controles y medidas, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles deberían establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la organización, minimizar los daños de esta, maximizar el entorno de las inversiones y las oportunidades de negocio. Para la presente investigación sería la Oficina de Registros y Archivos Académicos de la Universidad Nacional del Callao.

2.2.3. Seguridad Física

La seguridad física según Álvarez, G., y Pérez, P., (2004), se logra al impedir el acceso a las áreas críticas de personal no autorizado. Estas zonas habrán de estar delimitadas, pero no de forma visible sino de una manera formal, con un perímetro permanentemente controlado. Se pueden definir varios tipos de zonas seguras dependiendo del tipo Existe algún archivo de tipo Log donde guarde información Referida a las operaciones que realiza la Base de datosde sistema informático que contengan y de su grado de criticidad y, por lo tanto, las medidas de seguridad serán acordes

a dicho grado.

Este va ser uno de puntos esenciales en la seguridad de la información, porque permite crear medidas de prevención y controles ante posibles amenazas.

2.2.4. Seguridad Lógica

Según Carracedo, J., (2004), se refiere a:

La seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. La "seguridad lógica" involucra todas aquellas medidas establecidas por la administración -usuarios y administradores de recursos de tecnología de información- para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información. (pp.31)

En esta investigación la seguridad lógica permite al igual que la seguridad física a crear barreras y procedimientos para el acceso a la información a través de administración de cuentas de usuario, permisos, entre otros.

2.2.5. Controles

Con la finalidad de poder mitigar los efectos de las series de amenazas que enfrenta los sistemas como es desastres naturales, errores, las fallas en los sistemas y la seguridad, los delitos y fraudes por computadora, se hace necesario el diseño e implementación de políticas y procedimientos

adecuados.

Los controles según Laudon, K., y Laudon, J., (2002) "consisten en todos los métodos, políticas, y procedimientos para asegurar la protección de los archivos de la institución, la precisión y la confiabilidad de sus registros contables y la adherencia operativa a las normas de administración" pp.45. Asimismo, los citados autores dicen que los sistemas de información computarizados se deben controlar con una combinación de controles: generales y de aplicación.

Los controles de seguridad generales según Álvarez, G., y Pérez, P., (2004) van dirigidos al diseño y utilización del software, la seguridad de los archivos y la base de datos de la empresa. Además, de una combinación de software y procedimientos manuales; por tanto, son globales y se aplican en todas las áreas. Los controles generales incluyen los de proceso de implantación del sistema, para software, los físicos para el hardware, los de operaciones de cómputo, los de seguridad de datos y las disciplinas, normas y procedimientos administrativos.

Los controles de aplicación señalan Eterovic, J., y Pomar, P., (s.f) son específicos de cada sistema de información, programa o aplicación computarizada. Se aplican en procedimientos ya programados o en un área funcional específica de usuarios de un sistema en particular. Se enfocan en los objetivos de integridad del ingreso y la actualización, la validez y el mantenimiento. Estos controles incluyen los de entrada o acceso, de proceso o de procesamiento y de salida.

2.2.6. Amenazas

Las amenazas según Stallings, W., (2004), son "una posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio. Es decir, una amenaza es un peligro posible que podría explotar una vulnerabilidad".

En este mismo orden de ideas, MCCarthy, M., y Campbell S., (2002) dividen la amenaza en interna y externa. Las externas incluyen hackers aficionados, la competencia, extorsionadores y ladrones. Mientras que las amenazas internas, incluyen trabajadores descontentos, antiguos trabajadores que guardan algún tipo de rencor, empleados modelo que han contraído enormes deudas en el juego y empleados que planean dejar la empresa y trabajar para la competencia.

2.2.7. Ataques

Los ataques según Stallings, W., (2004), vienen dados por:
Un asalto a la seguridad del sistema derivado de una amenaza inteligente; es decir, un acto inteligente y deliberado (especialmente en el sentido de un método o técnica) para eludir los servicios de seguridad y violar la política de seguridad del sistema. (pp.56)

También el ataque según Eterovic, J., y Pomar, P., (s.f), es cualquier acción que comprometa la seguridad de la información de una organización. Por otra parte, señala MCCarthy, M., y Campbell S., (2002), que los ataques se

distinguen entre pasivos y activos: el ataque pasivo trata de saber o de usar la información del sistema, sin afectar los recursos del mismo. El ataque activo, en cambio, trata de cambiar los recursos del sistema o de afectar a su funcionamiento.

El modelo diseñado es una guía que contribuirá a reducir las amenazas y ataques que son desarrollados para las universidades de la región capital y concientizar a sus trabajadores de la importancia de respetar y resguardar los activos informáticos.

2.2.8. Riesgo

Según Gómez, L., Farías-Elinos, M., Mendoza, M., (2003) señalan que el riesgo "es la posibilidad de sufrir algún daño o pérdida". Asimismo, Carracedo, J., (2004) opina que los riesgos de la información son: pérdida, mal uso no intencional y deliberado, exposición o daño que sufre la información cuando esta resguardada en dispositivos tecnológicos.

Por lo anterior, es necesario que para estudiar y valorar los riesgos a los que está expuesta la información que se resguarda en las universidades, debe hacerse un análisis de las amenazas, vulnerabilidades y ataques de los activos informáticos.

2.2.9. Proceso de Capacitación

Se puede decir que la capacitación es un proceso continuo, porque aun cuando al personal de nuevo ingreso se le da la inducción en forma adecuada, con frecuencia es preciso entrenarlos o capacitarlos en las labores para las que fueron contratados y/o proporcionales nuevos

conocimientos necesarios para el desempeño de un puesto, al igual que los empleados con experiencia que son ubicados en nuevos puestos, pueden requerir capacitación para desempeñar adecuadamente su trabajo. Es posible que aún los candidatos internos no posean las habilidades o que también tengan hábitos incorrectos que requieran corregirse. También, siempre será necesario mantener un equilibrio entre las aptitudes y actitudes de los trabajadores y los requerimientos del puesto.

Los beneficios que aporta la capacitación son:

1) ayuda a mejorar las aptitudes y las actitudes.

2) eleva los conocimientos de los ocupantes de los puestos en todos los niveles organizacionales.

3) mejora la moral y la satisfacción de la fuerza de trabajo.

4) guía al personal a identificarse con los objetivos de la organización.

5) crea una mejor imagen tanto del personal como de la organización.

6) mejora las relaciones entre jefes y subordinados.

7) ayuda a sistematizar el trabajo.

8) fluyen mejor la toma de decisiones y la solución de problemas, 9) propicia el desarrollo y las promociones.

10) es la mejor herramienta para incrementar la productividad y la calidad.

11) contribuye a mantener bajos los costos de operación en muchas áreas.

12) contribuye positivamente en el manejo de conflictos y tensiones.

13) permite el establecimiento y logro de metas individuales. (werther jr, y davis 1998, p. 209).

2.3. Definiciones de términos básicos

2.3.1. ISO:

International Organization for Standardization. Fundada en 1946, es una federación internacional que unifica normas en unos cien países. Una de ellas es la norma OSI, modelo de referencia universal para protocolos de comunicación.

2.3.2. ISO/IEC/27001

Es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

2.3.3. SGSI

Un sistema de gestión de la seguridad de la información (SGSI) (en inglés: information security management system, ISMS) es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto.

2.3.4. PDCA

La ISO/IEC 27001 por lo tanto incorpora el típico Plan-Do-Check-Act (PDCA) que significa "Planificar-Hacer-Controlar-Actuar" siendo este un

enfoque de mejora continua:

Plan (planificar): es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.

Do (hacer): es una fase que envuelve la implantación y operación de los controles.

Check (controlar): es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

Act (actuar): en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

2.3.5. ISO/IEC 27002

(Anteriormente denominada ISO 17799) 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.

2.3.6. Confidencialidad

La confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

2.3.7. Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) Grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

2.3.8. Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

2.3.9. Backup

Copia de seguridad. Se hace para prevenir una posible pérdida de información.

2.3.10. UNAC

Es una universidad pública ubicada en el distrito de Bellavista, en la Provincia Constitucional del Callao, Perú. Fue creada mediante Ley N° 16225, el 2 de septiembre de 1966.

2.3.11. ORAA

La Oficina de Registros y Archivos Académicos y la Unidad de Archivo

General de la Universidad Nacional del Callao, para cumplir su misión, dirigida a la comunidad universitaria, tiene la finalidad que se dedica al buen funcionamiento del fondo documental de Archivo General de la UNAC.

2.3.12 Capacitación:

Es una actividad que debe ser sistémica, planeada, continua y permanente que tiene el objetivo de proporcionar el conocimiento necesario y desarrollar las habilidades (aptitudes y actitudes) necesarias para que las personas que ocupan un puesto en las organizaciones, puedan desarrollar sus funciones y cumplir con sus responsabilidades de manera eficiente y efectiva, esto es, en tiempo y en forma.

III. VARIABLES E HIPÓTESIS

3.1. Variables de la investigación

3.1.1. Variable independiente

ISO 27001:2013

3.1.2. Variable dependiente

Seguridad de la Información de la Oficina de Registros y Archivos Académicos.

3.2. Operacionalización de las variables

Tabla 1: Operacionalización de las variables

VARIABLES	DIMENSIONES	INDICADORES
VARIABLE INDEPENDIENTE: ISO 27001:2013	**Legal**	Porcentaje de conformidad de requisitos Legales
	Estratégica	Porcentaje de conformidad de políticas estratégicas
	Técnica	Promedio de implementación técnica
VARIABLE DEPENDIENTE: Seguridad de la Información de la Oficina de Registros y Archivos Académicos.	**Confidencialidad**	Promedio de información confidencial
	Disponibilidad	Tiempo de respuesta de continuidad
	Integridad	Porcentaje de información validada

3.3. Hipótesis General e Hipótesis Específicas

3.3.1. Hipótesis General

HG: La ISO 27001:2013 Mejora significativamente la Seguridad de la Información de la ORAA – UNAC

3.3.2. Hipótesis Específicas

P1: La ISO 27001:2013 influye significativamente en la confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

P2: La ISO 27001:2013 mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros y Archivos Académicos.

P3: La ISO 27001:2013 se relaciona significativamente con la integridad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

IV. METODOLOGÍA

4.1. Tipo de Investigación

El tipo de investigación de la presente tesis fue de tipo aplicada ya que pretendemos resolver la presente problemática que encontramos en este departamento acerca de los incidentes de seguridad que estén ocasionando la perdida, desorden y repetición de información aplicando la normativa internacional ISO 27001:2013 contribuyendo a que exista los requisitos de confiabilidad, disponibilidad e integridad de información en la Oficina de Registros y Archivos Académicos.

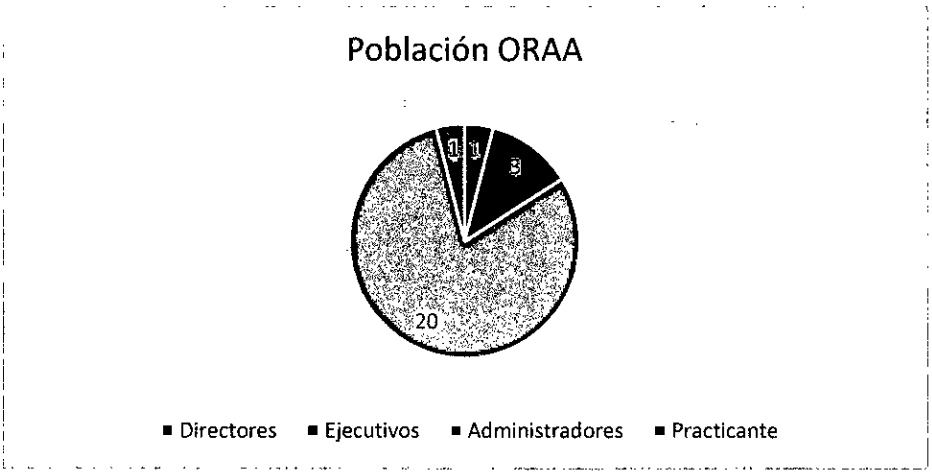
4.2. Población, muestra y muestreo

La presente investigación, fue pre-experimental porque se administra un estímulo o tratamiento a un grupo personas y un contexto después aplicamos una medición para observar sus efectos sobre la variable dependiente.

Debemos tener en cuenta que en este punto solo deberíamos hablar de solo población, y ya no de un posible muestreo y esto es debido a la cantidad reducida y exacta de personal especializado en la Oficina de Registros y Archivos Académicos.

Según nuestro estudio realizado mediante encuesta a la población en general de la Oficina de Registros y Archivos Académicos podemos encontrar desde la planta directiva hasta el practicante de área un total de 25 personas que laboran allí.

FIGURA N° 4 Gráfico de Población de ORAA



Fuente: Elaboración propia.

4.3. Instrumentos de recolección de datos

4.3.1. Técnicas de recolección de datos

- **Observación**

"La observación consiste en el registro sistemático, válido y confiable de comportamiento o conducta manifiesta. Puede utilizarse como instrumento de medición en diversas circunstancias." (Hernández 1998 p. 309)

Esta técnica que permite observar los fenómenos que se investiga, definida en los indicadores que se visualizan para conocer la realidad de la situación en la seguridad de la información de la Oficina de Registros y Archivos Académicos de la Universidad Nacional del Callao. Observando y analizando la confidencialidad, la disponibilidad y la integridad de la información.

- **Entrevista**

La entrevista es una forma oral de comunicación interpersonal, que tiene como finalidad obtener información en relación con un objetivo. Es por ello

que la comunicación debe ser propiciada a través de un adecuado manejo del juego existente entre causa y efecto en base al patrón de la conducta humana (Acevedo 1998, p. 10-11).

- **Revisión bibliográfica e internet**

Esta técnica que se utiliza en la búsqueda de información en la red de redes.

4.3.2. Instrumentos de recolección de datos

- **Fichas**

Instrumento para recolectar datos similares al análisis de contenido. De hecho, es una forma de observación del contenido de comunicaciones. (Hernández 1998, p. 310)

- **Cuestionarios**

Se presenta como un formulario, listando las preguntas sobre la seguridad de la información para realizar nuestra investigación y medir los indicadores de las variables con sus dimensiones.

Es el instrumento más utilizado para recolectar los datos es el cuestionario. Un cuestionario consiste en un conjunto de preguntas respecto a una o más variables a medir. (Hernández 1998, p. 276)

4.4 Procedimiento de recolección de datos

Para la presente investigación se utilizó la distribución normal Z, mediante la cual se realiza el análisis y contrastación de los datos que se realizó mediante la estadística inferencial, este es el caso de los indicadores

Promedio de información confidencial, Tiempo de respuesta de continuidad, Porcentaje de información validada. Se realizó los cálculos necesarios para realizar la Distribución Normal:

- **Validación de datos**

Se usó el coeficiente Alfa de Cronbach como modelo de consistencia interna, basado en el promedio de las correlaciones entre los ítems. Si el resultado del análisis se encuentra entre 0 y 1, es considerado con mayor validez del instrumento, es decir el instrumento es más confiable. Se tomó como valor crítico 0.8.

$$\propto = \frac{K}{K-1}\left(1 - \frac{\sum Vi}{\sum Vt}\right)$$

Donde:

$\propto$ = Alfa de Cronbach

K = Número de ítems (elementos para el cálculo de indicador)

Vi =Varianza de cada ítems

Vt = Varianza de la suma de cada ítems, (Varianza de suma total).

- **Test de Normalidad:**

Identificamos que los datos tengan o no una distribución normal, lo que nos permitió aplicar la prueba correcta.

Como nuestra población es menor a 50, se aplicó la prueba de normalidad de "método Shapiro Will", en este test se debe cumplir lo siguiente:

- ✓ sig 0.05 adopta una distribución no normal.
- ✓ sig 0.05 adopta una distribución normal.

En caso de que los datos tengan una distribución normal se puede aplicar para la contratación de hipótesis:

- ✓ Si la población es mayor a 30 Z
- ✓ Si la población es menor a 30 T

4.5. Plan de análisis estadístico de datos

4.5.1. Hipótesis general

La ISO 27001:2013 Mejora significativamente la Seguridad de la Información de la Oficina de Registros y Archivos Académicos de la Universidad Nacional del Callao.

Tabla 2: Relación entre la ISO 27001:2013 y la seguridad de la información de la oficina de registros y archivos académicos.

Modelo	R	R cuadrado
1	.832	0.692

Fuente: Elaboración propia.

Como se puede observar en la TABLA N° 2, el valor de r calculado (0.83) es positivo, entonces la relación entre la ISO 27001:2013 y la seguridad de la información de la oficina de registros y archivos académicos es directa, es decir, que cuando se implementa el ISO 27001:2013ISO 27001:2013, se mejora la entidad mencionada la oficina de registros y archivos académicos.

También, como el valor de r (0.89) se acerca al valor +1, significa que hay una relación muy estrecha entre la implementación del ISO 27001:2013 y el control de la entidad mencionada la oficina de registros y archivos académicos.

4.5.2. Hipótesis específica

- **Hipótesis específica 1:**

La ISO 27001:2013 influye significativamente en la confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

Variables:

I_{a1}: La confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos antes de la implementación de la ISO 27001:2013.

I_{d1}: La confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos después de la implementación de la ISO 27001:2013.

Hipótesis Nula (H_0): La ISO 27001:2013 no influye significativamente en la confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos

$$H_0: I_{a1} - I_{d1} \geq 0$$

Hipótesis Alternativa (H_a): La ISO 27001:2013 influye significativamente en la confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos

$$H_a: I_{a1} - I_{d1} < 0$$

- **Hipótesis específica 2:**

La ISO 27001:2013 mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros y Archivos Académicos.

Variables:

I_{a2}: la disponibilidad en la seguridad de la información de la Oficina de Registros y Archivos Académicos antes de la aplicación ISO 27001:2013.

I_{d2}: la disponibilidad en la seguridad de la información de la Oficina de Registros y Archivos Académicos después de la aplicación ISO 27001:2013.

Hipótesis Nula (H_0): La ISO 27001:2013 no mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros y Archivos Académicos.

$$H_0: I_{a2} - I_{d2} \geq 0$$

Hipótesis Alternativa (H_a): La ISO 27001:2013 mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros y Archivos Académicos.

$$H_1: I_{a2} - I_{d2} < 0$$

- **Hipótesis específica 3:**

La ISO 27001:2013 se relaciona significativamente con la integridad de la seguridad de la información de la Oficina de Registros y Archivos Académicos

Variables:

I_{a3}: la integridad en la seguridad de la información de la Oficina de Registros y Archivos Académicos antes de la aplicación ISO 27001:2013.

I_{d3}: la integridad en la seguridad de la información de la Oficina de Registros y Archivos Académicos después de la aplicación ISO 27001:2013.

Hipótesis Nula (H_0): La ISO 27001:2013 no se relaciona significativamente con la integridad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

$$H_0: I_{a2} - I_{d2} \geq 0$$

Hipótesis Alternativa (H_a): La ISO 27001:2013 se relaciona significativamente con la integridad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

$$H_1: I_{a2} - I_{d2} < 0$$

4.5.3. Nivel de significancia

Nivel de significancia (α):	0.05
Nivel de confianza (γ = 1-α):	0.95

4.5.4. Estadístico de prueba

Según Martínez (2005, p. 452), cuando se conoce la varianza muestral y el tamaño de la muestra fue menor que 30, la fórmula para calcular Z en la diferencia de medias, que es el caso del indicador disponibilidad, es:

$$Z = \frac{\overline{Tp} - \overline{Ta}}{\sqrt{\left(\frac{\sigma_a^2}{n_a} + \frac{\sigma_p^2}{n_p}\right)}}$$

Donde:

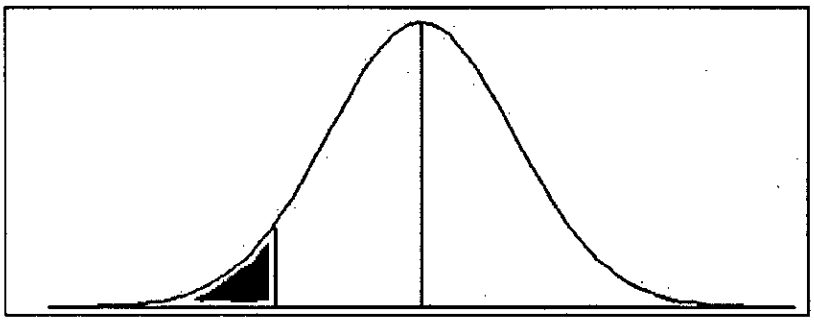
Ta: Indicador en el proceso actual.
Tp: Indicador con el sistema propuesto.
σa: Varianza con el proceso actual.
σp: Varianza con el sistema propuesto.
ηa: Muestra para el pre test.
np: Muestra para el post test.

4.5.5. Región del rechazo

Debido a que se ha establecido α = 0.05, entonces según la tabla de distribución normal Z, el punto crítico Z_x es 1.645. (Ortega, 2009, p182-184).

Tal como se aprecia en la FIGURA N°5, la región de rechazo (RR) será cuando el valor de Z_c calculado sea mayor que el valor de Z_x crítico que es 1.645.

FIGURA N° 5 Indicadores para contrastación de hipótesis. Distribución Normal.



Fuente: Elaboración propia.

La tabulación, análisis y la interpretación de los datos recopilados fueron realizados a través del programa SPSS para Windows.

V. RESULTADOS

5.1. Resultados parciales

En el presente capítulo se procedió a describir los resultados que se obtuvieron en la tesis en la fase de análisis de datos, haciendo uso de los indicadores se observó si la implementación de la ISO 27001:2013 Mejora significativamente la Seguridad de la Información de la ORAA – UNAC.

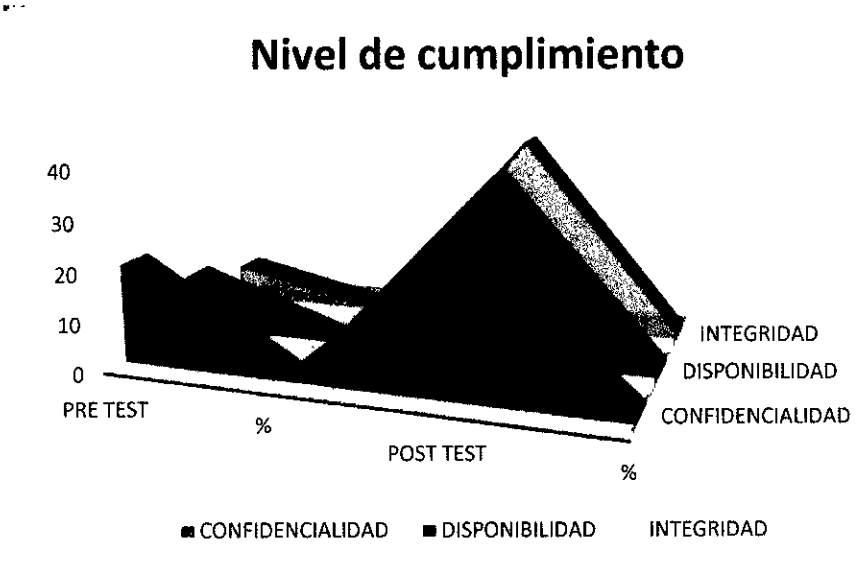
Dos meses después de la implementación de la ISO 27001:2013, se observó que el nivel de cumplimiento influía la confidencialidad, disponibilidad e integridad.

Tabla 3: Nivel de cumplimiento de la ISO 27001:2013

NIVEL DE CUMPLIMIENTO ISO 27001:2013				
INDICADORES DE SEGURIDAD DE LA INFORMACIÓN	PRE TEST	%	POST TEST	%
CONFIDENCIALIDAD	20	67%	29	97%
DISPONIBILIDAD	11	28%	37	95%
INTEGRIDAD	7	17%	40	95%

Fuente: Elaboración propia.

FIGURA N° 6 Nivel de cumplimiento



Fuente: Elaboración propia.

En dicha gráfica podemos apreciar que al implementar la ISO 27001:2013 influye significativamente en la confidencialidad; mejora significativamente en la disponibilidad y se relaciona significativamente con la integridad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

5.2. Resultados finales

En la TABLA N° 4, se puede apreciar la relación entre las variables:

ISO 27001 Y SEGURIDAD DE LA INFORMACION EN ORAA.

Tabla 4: Análisis de regresión

Estadísticas de la regresión	
Coeficiente de correlación múltiple	0.998046096
Coeficiente de determinación R^2	0.996096009
R^2 ajustado	0.992192019

Fuente: Elaboración propia.

Como el r calculado es r=0.99, es positivo nos indica que las variables son directamente proporcional.

A mayor cumplimiento de la ISO 27001:2013 mayor es la seguridad de la información.

Asimismo como el r calculado es r=0.99, se aproxima a 1, nos indica que la relación entre las variables, implementación de ISO 27001:2013 y la Seguridad de la información en ORAA, es estrecha o fuerte.

Finalmente como el coeficiente de determinación es 0.996, se indica que la variación de la seguridad de la información depende en 99.6% de la implementación de la ISO 27001:2013.

VI. DISCUSIÓN DE RESULTADOS

6.1. Contrastación de hipótesis con los resultados

6.1.1. Análisis de confiabilidad

Para realizar el análisis de confiabilidad de cada indicador se utilizó se utilizó método del Alfa de Cronbach, cuya fórmula es:

$$\alpha \text{ de Cronbach} = \frac{N}{N-1}\left(1 - \frac{\sum_i^n V_i}{VT}\right)$$

Donde:

N: N° de ítems.

Vi: Varianza de cada ítem.

VT: Varianza total

El Método de confiabilidad señalado indica 5 niveles de clasificación según los resultados que se obtengan al determinar el p - valor de contraste (sig.), como se muestra en la TABLA N° 5

Tabla 5: Nivel de confiabilidad de Cronbach

Escala	Nivel
0.00 < sig <0.20	Muy bajo
0.20 < sig <0.40	Bajo
0.40 < sig <0.60	Regular
0.60 < sig <0.80	Aceptable
0.80 < sig <1.00	Elevado

Fuente: Nivel de confiabilidad de Cronbach

Para esta investigación, se considera un valor óptimo si los resultados que se obtengan estén en la escala de 0.80 a 1.00, siendo este un nivel elevado de aceptación lo cual indica que el instrumento a medir es invariable y confiable.

Se realizaron las pruebas de confiabilidad con los 3 indicadores: Confidencialidad, Disponibilidad e Integridad.

6.1.1.1. Indicador: Disponibilidad

- **Disponibilidad (Pre-Test)**

A continuación, la TABLA N°6, muestra el análisis de confiabilidad realizado al indicador **Disponibilidad**, tomados sin la implementación del ISO 27001:2013.

Tabla 6: Disponibilidad (PRE-TEST)

Estadísticos de fiabilidad	
Alfa de Cronbach	N° de elementos
0.745	25

Fuente: Elaboración propia.

Se aprecia que el valor resultante de la prueba de confiabilidad aplicada a los datos del pre-test, para el indicador **Disponibilidad** es de 0.745, este valor es mayor a valor crítico planteado, por lo que se considera que el instrumento para este grupo de datos es confiable.

- **Disponibilidad (Post-Test)**

A continuación, la TABLA N°7, muestra el análisis de confiabilidad realizado al indicador de **Disponibilidad,** tomados con la implementación del ISO 27001:2013.

Tabla 7: Disponibilidad (POST-TEST)

Estadísticos de fiabilidad	
Alfa de Cronbach	N° de elementos
0.721	25

Fuente: Elaboración propia.

Se aprecia que el valor resultante de la prueba aplicada a los datos del post- test para el indicador **Disponibilidad** es de 0.721, este valor es mayor al valor crítico planteado, por lo que se considera que el instrumento para este grupo de datos es confiable.

6.1.1.2. Indicador: Confidencialidad

- **Confidencialidad (Pre-Test)**

A continuación la TABLA N°8, muestra el análisis de confiabilidad realizado al indicador **Confidencialidad,** tomados sin la implementación del ISO 27001:2013.

Tabla 8: Confidencialidad (PRE-TEST)

Estadísticos de fiabilidad	
Alfa de Cronbach	N° de elementos
0.715	25

Fuente: Elaboración propia.

Se aprecia que el valor resultante de la prueba de confiabilidad aplicada a los datos del pre-test, para el indicador **Confidencialidad** es de 0.715, este valor es mayor a valor crítico planteado, por lo que se considera que el instrumento para este grupo de datos es confiable.

- **Confidencialidad (Post-Test)**

A continuación, la TABLA N°9, muestra el análisis de confiabilidad realizado al indicador **Confidencialidad,** tomados con la implementación del ISO 27001:2013.

Tabla 9: Confidencialidad (POST-TEST)

Estadísticos de fiabilidad	
Alfa de Cronbach	N° de elementos
0.756	25

Fuente: Elaboración propia.

Se aprecia que el valor resultante de la prueba aplicada a los datos del post- test para el indicador **Confidencialidad**, es de 0.756, este valor es mayor al valor crítico planteado, por lo que se considera que el instrumento para este grupo de datos es confiable.

6.1.1.3. Indicador: Integridad

- **Integridad (Pre-Test)**

A continuación la TABLA N°10, muestra el análisis de confiabilidad realizado al indicador **Integridad,** tomados sin la implementación del ISO 27001:2013.

Tabla 10: Integridad (PRE-TEST)

Estadísticos de fiabilidad	
Alfa de Cronbach	N° de elementos
0.722	25

Fuente: Elaboración propia.

Se aprecia que el valor resultante de la prueba de confiabilidad aplicada a los datos del pre-test, para el indicador **Integridad** es de 0.715, este valor es mayor a valor crítico planteado, por lo que se considera que el instrumento para este grupo de datos es confiable.

- **Integridad (Post-Test)**

A continuación, la TABLA N°11, muestra el análisis de confiabilidad realizado al indicador **Integridad,** tomados con la implementación del ISO 27001:2013.

Tabla 11: Integridad (POST-TEST)

Estadísticos de fiabilidad	
Alfa de Cronbach	N° de elementos
0.781	25

Fuente: Elaboración propia.

Se aprecia que el valor resultante de la prueba aplicada a los datos del post- test para el indicador **Integridad**, es de 0.756, este valor es mayor al valor crítico planteado, por lo que se considera que el instrumento para este grupo de datos es confiable.

6.1.2. Pruebas de normalidad

Se realizó la prueba de normalidad para los indicadores a través del método Shapiro-Wilk, debido a que el tamaño de la muestra es menor a 50. Dicha prueba se realizó introduciendo los datos de cada indicador en el software estadístico SPSS 22.0, para un nivel de confiabilidad del 95%, bajo las siguientes condiciones:

Si: sig < 0.05 adopta una distribución no normal.

sig ≥ 0.05 adopta una distribución normal.

Dónde: sig. : P-valor o nivel crítico del contraste.

Los resultados fueron los siguientes:

6.1.2.1. Indicador: Disponibilidad

- **Disponibilidad (Pre-Test)**

A continuación la TABLA N° 12, muestra el resultado de la prueba de normalidad de datos del pre-test, para el indicador **Disponibilidad.**

Tabla 12: Prueba de SHAPIRO-WILK para el indicador Disponibilidad (PRE-TEST)

Shapiro-Wilk		
Estadístico	gl	Sig.
0.961	30	0.066

Fuente: Elaboración propia.

Se puede observar que el valor sig. es de 0.066 > 0.05, por lo tanto adopta una distribución normal.

- **Disponibilidad (Post-Test)**

A continuación en la TABLA N°13, se muestra el resultado de la prueba de normalidad aplicado a los datos del post test para el indicador **Disponibilidad.**

Tabla 13: Prueba de SHAPIRO-WILK para el indicador Disponibilidad (POST-TEST)

Shapiro-Wilk		
Estadístico	gl	Sig.
0.945	30	0.132

Fuente: Elaboración Propia.

Se puede apreciar que el valor del sig. es de 0.132 > 0.05, por lo tanto adopta una distribución normal.

6.1.2.2. Indicador: Confidencialidad

- **Confidencialidad (Pre-Test)**

En la TABLA N° 14, se muestra el resultado de la prueba de normalidad de datos del pre-test, para el indicador **Confidencialidad.**

Tabla 14: Prueba de SHAPIRO-WILK para el indicador Confidencialidad (PRE-TEST)

Shapiro-Wilk		
Estadístico	gl	Sig.
0.912	30	0.059

Fuente: Elaboración propia.

Se puede observar que el valor sig es de 0.059 > 0.05, por lo tanto adopta una distribución normal.

- **Confidencialidad (Post-Test)**

En la TABLA N°15, se muestra el resultado de la prueba de normalidad de datos del grupo experimental para el indicador **confidencialidad.**

Tabla 15: Prueba de SHAPIRO-WILK para el indicador Confidencialidad (POST-TEST)

Shapiro-Wilk		
Estadístico	gl	Sig.
0.912	30	0.109

Fuente: Elaboración Propia

Se puede apreciar que el valor del sig es de 0.109 > 0.05, por lo tanto adopta una distribución normal.

6.1.2.3. Indicador: Integridad

- **Integridad (Pre-Test)**

En la TABLA N° 16, se muestra el resultado de la prueba de normalidad de datos del pre-test, para el indicador **Integridad.**

Tabla 16: Prueba de SHAPIRO-WILK para el indicador Integridad (PRE-TEST)

Shapiro-Wilk		
Estadístico	gl	Sig.
0.891	30	0.071

Fuente: Elaboración propia.

Se puede observar que el valor sig es de 0.071 > 0.05, por lo tanto adopta una distribución normal.

- **Integridad (Post-Test)**

En la TABLA N°17, se muestra el resultado de la prueba de normalidad de datos del grupo experimental para el indicador **integridad.**

Tabla 17: Prueba de SHAPIRO-WILK para el indicador Integridad (POST-TEST)

Shapiro-Wilk		
Estadístico	gl	Sig.
0.813	30	0.091

Fuente: Elaboración Propia

Se puede apreciar que el valor del sig es de 0.09 > 0.05, por lo tanto adopta una distribución normal.

6.1.3. Pruebas de hipótesis

- **Prueba de Hipótesis (H1):**

La ISO 27001:2013 influye significativamente en la confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

- **Hipótesis Nula (H0):**

La ISO 27001:2013 no influye significativamente en la confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

$$H_0: I_{a1} - I_{d1} \geq 0$$

- **Hipótesis Alternativa (Ha):**

La ISO 27001:2013 influye significativamente en la confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

$$H_a: I_{a1} - I_{d1} < 0$$

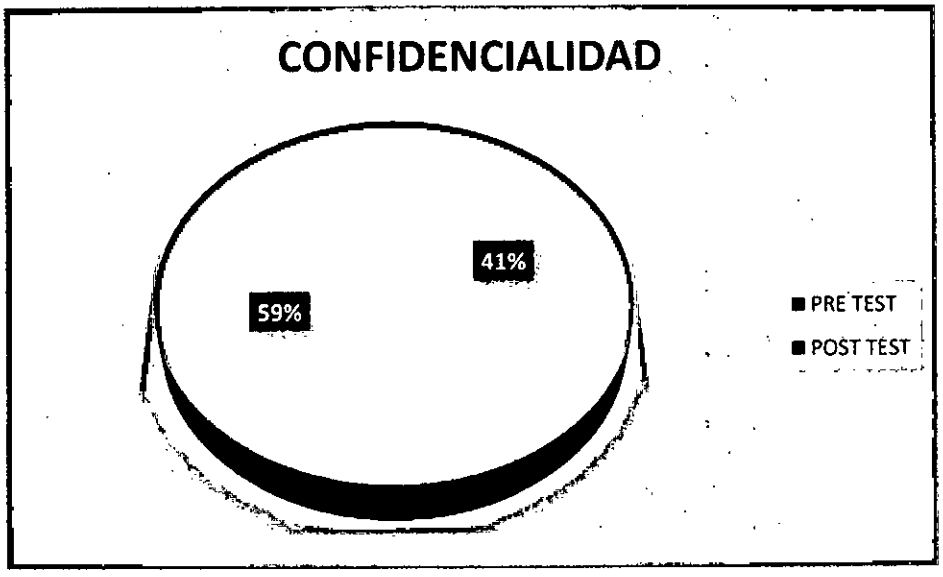
Donde:

Ia1: nivel confidencialidad antes de la implementación de un ISO 27001:2013

Id1: nivel de confidencialidad después de la implementación de un ISO 27001:2013

Como se puede observar en la FIGURA N°7, existe un aumento de la confidencialidad.

FIGURA N° 7 Confidencialidad



Fuente: Elaboración propia.

- **Prueba de Hipótesis (H2):**

La ISO 27001:2013 mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros y Archivos Académicos.

- **Hipótesis Nula (H0):**

La ISO 27001:2013 no mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros y Archivos Académicos.

$$H_0: I_{a2} - I_{d2} \geq 0$$

- **Hipótesis Alternativa (Ha):**

La ISO 27001:2013 mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros y Archivos Académicos.

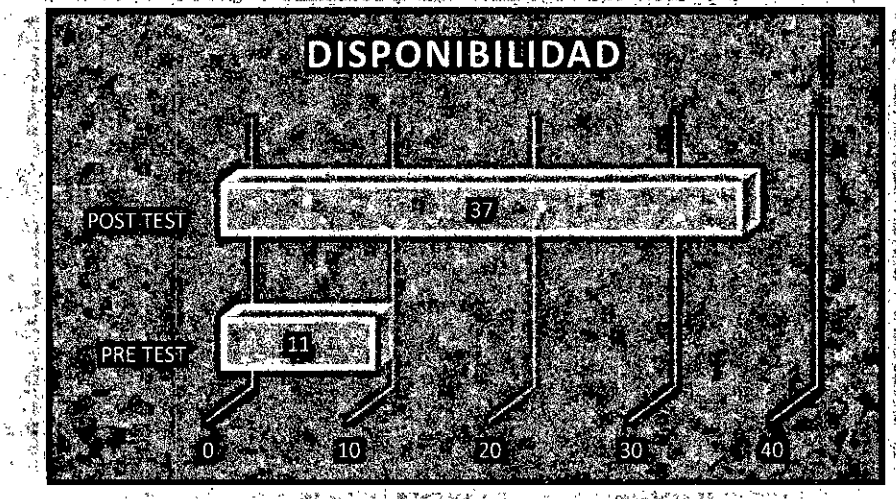
$$H_1: I_{a2} - I_{d2} < 0$$

Donde:

Ia2: nivel de disponibilidad antes de la aplicación de un ISO 27001:2013

Id2: nivel de disponibilidad después de la aplicación de un ISO 27001:2013

FIGURA N° 8 Disponibilidad



Fuente: Elaboración propia.

- **Prueba de Hipótesis (H3):**

La ISO 27001:2013 se relaciona significativamente con la integridad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

- **Hipótesis Nula (H0):**

La ISO 27001:2013 no se relaciona significativamente con la integridad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

$$H_0: I_{a2} - I_{d2} \geq 0$$

• **Hipótesis Alternativa (Ha):**

La ISO 27001:2013 se relaciona significativamente con la integridad de la seguridad de la información de la Oficina de Registros y Archivos Académicos.

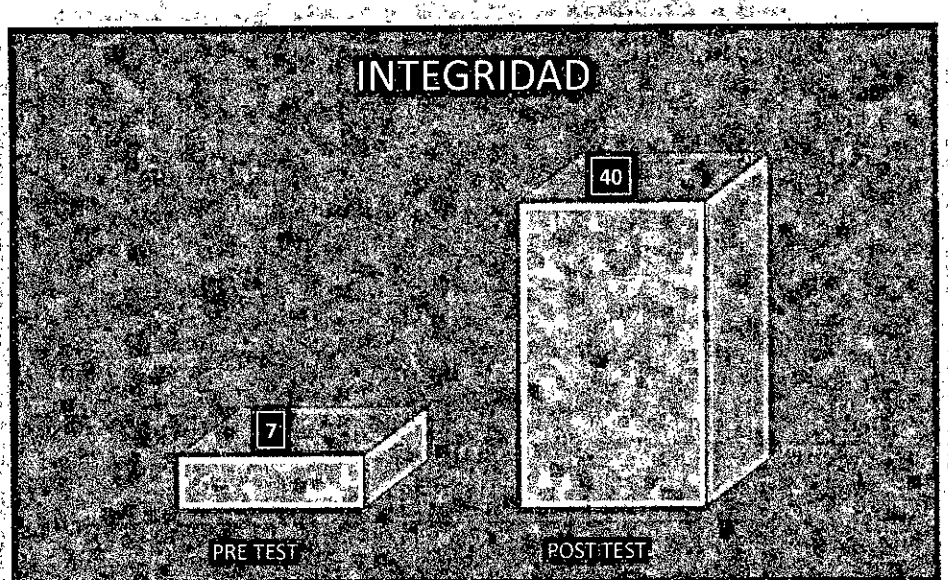
$$H_1: I_{a2} - I_{d2} < 0$$

Donde:

Ia2: nivel de integridad antes de la aplicación de un ISO 27001:2013.

Id2: nivel de integridad después de la aplicación de un ISO 27001:2013.

FIGURA N° 9 Integridad



Fuente: Elaboración propia.

6.1.4. Discusión

Tabla 18: Cruce de dimensiones de variables

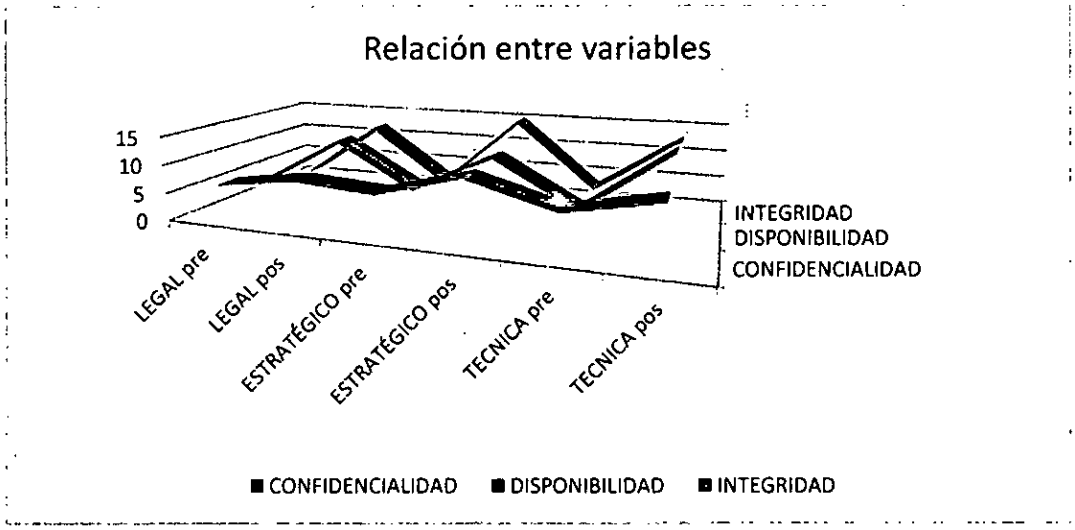
ISO/SEGURIDAD	LEGAL PRE	LEGAL POS	ESTRATEGICO PRE	ESTRATEGICO POS	TECNICA PRE	TECNICA POS
CONFIDENCIALIDAD	6	8	7	11	7	10
DISPONIBILIDAD	4	12	4	11	3	14
INTEGRIDAD	2	12	2	15	3	13

Fuente: Elaboración propia.

Se realizó el cruce de datos entre las dimensiones de ambas variables para entender mejor cuales son las relaciones.

Lo que nos indica en primer lugar es que la ORAA contaba con un nivel aceptable de confidencialidad, pero los niveles de los indicadores disponibilidad e integridad son muy bajos.

FIGURA N° 10 Relación entre variables.



Fuente: Elaboración propia.

6.2. Contrastación de resultados con otros estudios similares

En el año 2011, Ampuero Chang, Carlos Enrique; en la tesis titulada **"Diseño de un sistema de gestión de seguridad de información para una compañía de seguros",** A pesar de no ser obligatoria la implementación de todos los controles, se debe argumentar la no aplicabilidad de los controles no implementados. Recomienda el uso del Ciclo: Plan - Do - Check - Act para el diseño de un SGSI.

En el caso de nuestra investigación, si se implementó todos los controles utilizando el ISO 27001:2013.

En el año 2005, Romero Echevarría, Luis Miguel, en la tesis **"Marco conceptual de los Delitos Informáticos",** que le da énfasis al secreto de las Telecomunicaciones y Protección de Datos, ordenándose con ella a las empresas de telecomunicaciones a mantener en secreto la información de sus abonados o usuarios, sancionándose a la empresa si la información es entregada o la obtiene terceros mas no así a estos terceros.

En nuestro caso igualmente es necesario el secreto de la información de los registros académicos de los alumnos.

En el año 2011, Guerra Valdivia, Alicia Rubí, en la tesis titulada **"Delitos Informáticos – Caso de Estudio"**; concluyó que los sistemas de información no deben ser descalificados, tampoco pretende demeritar las innumerables ventajas que su utilización puede conllevar para el beneficio social. Por lo contrario, se trata de centrar la mirada en aquellos sujetos que hacen mal uso de estos recursos, con la finalidad de obtener beneficios

personales, a costa del bienestar particular o común de otros individuos.

Se realizó la capacitación al personal administrativo centrándonos también en el mal uso de los recursos informáticos, en contra de la UNAC.

VII. CONCLUSIONES

- La implementación del ISO 27001:2013 permitió determinar que existe relación directa entre ésta y la seguridad de información en ORAA.

- La implementación permitió determinar cómo un ISO 27001:2013 influye significativamente en la confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos, aumentando de 67% a 97%.

- La implementación permitió determinar cómo un ISO 27001:2013 mejora significativamente en la disponibilidad en la seguridad de la información de la Oficina de Registros y Archivos Académicos aumentando significativamente de 28% a 95%.

- La implementación permitió determinar cómo un ISO 27001:2013 se relaciona significativamente con la integridad de la seguridad de la información de la Oficina de Registros y Archivos Académicos aumentando considerablemente de 17 % a 95%.

VIII. RECOMENDACIONES

En relación a las conclusiones obtenidas, se recomienda las siguientes actividades:

- Mantener la frecuencia de actualización de la seguridad de la información.

- Luego de la implementación del ISO 27001:2013, seguir realizando un constante mantenimiento y actualización; incluyendo nuevos indicadores en las alertas, entre otros.

- Fomentar la utilización de medidas de seguridad, backups, passwords, niveles de usuario.

IX. REFERENCIAS BIBLIOGRÁFICAS

Aceituno, V. (2004). Definiciones de seguridad de la información y sus limitaciones. *Conferencias FIST.*

Alvarez, G., & Perez, P. (2004). Seguridad Informática para Empresas y Particulares. En G. Alvarez Marañon, & P. Perez Garcia, *Seguridad Informática para Empresas y Particulares* (págs. 83-88).

Campbell, S., McCarty, M., & Brownstein, R. (2002). *Seguridad Digital. Estrategias de defensa digital para proteger la reputación y la cuota de mercado de su compañía.* España: McGraw-Hill.

Carracedo Gallardo, J. (2004). *Seguridad en Redes Telemáticas. Universidad Politécnica de Madrid.* España: McGraw-Hill/Interamericana de España.

Cheswick, W., Bellovin, S., & Rubin, A. (1994). *Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley professional computing series.* Amazon.

Eterovic, J., & Pomar, P. (21 de Diciembre de 2007). *Introducción a la Seguridad Informática. Conceptos Básicos de Seguridad Informática en Números. Taller de Seguridad Informática.* Obtenido de Introducción a la Seguridad Informática. Conceptos Básicos de Seguridad Informática en Números. Taller de Seguridad Informática.: http://seginfo.tripod.com/files/17799a.pdf

Gómez, Á. (2006). *Enciclopedia de la Seguridad Informática. Ra-Ma*

Editorial. Madrid. Madrid: Ra-Ma.

Gómez, L., Farías-Elinos, M., & Mendoza, M. (10 de Enero de 2008). *Importancia del Análisis de Riesgo de Seguridad.* Obtenido de Importancia del Análisis de Riesgo de Seguridad.: http://seguridad.internet2.ulsa.mx/congresos/2003/cudi2/impariesgo.pdf

Laudon, J., & Laudon, K. (1991). *Business Information Systems, Ed. Dryden Press, Orlando.* Orlando: Prentice Hall.

Laudon, J., & Laudon, K. (2002). *Sistema de Información Gerencial.* Pearson Educación.

Schneier, B. (2002). *Secrets and Lies. Digital Security in a Networked World.* Amazon.

Stallings, W. (2004). *Fundamentos de Seguridad en Redes. Aplicaciones y Estándares.* España: Pearson.

Vicente, A. (2004). *Seguridad de la Información.* OLETVM.

ANEXOS

ANEXO "A": DESCRIPCIÓN DEL FORMATO DE ORDEN DE TRABAJO - CRONOLOGIA

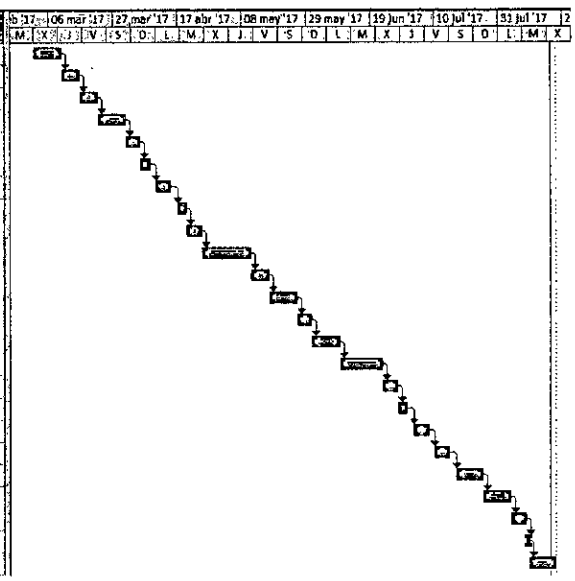
ANEXO "B": DESCRIPCIÓN DEL FORMATO DE SOLICITUD DE PERMISO PARA OBTENER INFORMACIÓN PARA PROYECTO DE INVESTIGACIÓN

ANEXO "C": DESCRIPCIÓN DEL FORMATO DE ENCUESTA DE LA ISO 27001:2013 APLICADAS A ORAA

ANEXO "D": "MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA OFICINA DE REGISTROS Y ARCHIVOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DEL CALLAO 2017"

ANEXO "A": DESCRIPCIÓN DEL FORMATO DE ORDEN DE TRABAJO - CRONOLOGIA

	Nombre de tarea	Duración	Comienzo	Fin
1	Identificación de la empresa o Institución a investigar.	7 días	mié 01/03/17	jue 09/03/17
2	Planteamiento del problema del proyecto de tesis.	4 días	vie 10/03/17	mié 15/03/17
3	Formulación del problema.	4 días	jue 16/03/17	mar 21/03/17
4	Establecer el problema general.	7 días	mié 22/03/17	jue 30/03/17
5	Establecer los problemas específicos.	3 días	vie 31/03/17	mar 04/04/17
6	Analizar los objetivos de la investigación.	3 días	mié 05/04/17	vie 07/04/17
7	Establecer el objetivo general.	5 días	lun 10/04/17	vie 14/04/17
8	Establecer los objetivos específicos.	3 días	lun 17/04/17	mié 19/04/17
9	Elaboración de la justificación.	3 días	jue 20/04/17	lun 24/04/17
10	Elaboración del marco teórico.	12 días	mar 25/04/17	mié 10/05/17
11	Definiciones de términos básicos.	4 días	jue 11/05/17	mar 16/05/17
12	Planteamineto de variables e hipotesis.	7 días	mié 17/05/17	jue 25/05/17
13	Operacionalización de las variables.	3 días	vie 26/05/17	mar 30/05/17
14	Elaboración de hipotesis.	7 días	mié 31/05/17	jue 08/06/17
15	Desarrollo de la metodología.	10 días	vie 09/06/17	jue 22/06/17
16	Establecer el tipo de investigación.	3 días	vie 23/06/17	mar 27/06/17
17	Diseño de la investigación.	3 días	mié 28/06/17	vie 30/06/17
18	Identificación de población y muestra.	5 días	lun 03/07/17	vie 07/07/17
19	Establecer técnicas e instrumentos de recolección de datos.	5 días	lun 10/07/17	vie 14/07/17
20	Planeamiento del analisis estadistico de datos.	7 días	lun 17/07/17	mar 25/07/17
21	Elaboración de la Matriz de Consistencia.	7 días	mié 26/07/17	jue 03/08/17
22	Esquema tentativo de proyecto de tesis.	3 días	vie 04/08/17	mar 08/08/17
23	Establecer Cronograma de actividades actualizado.	1 día	mié 09/08/17	mié 09/08/17
24	Absolución de las observaciones.	7 días	jue 10/08/17	vie 18/08/17



ANEXO "B": DESCRIPCIÓN DEL FORMATO DE SOLICITUD DE PERMISO PARA OBTENER INFORMACIÓN PARA PROYECTO DE INVESTIGACIÓN

SOLICITO: Permiso para obtener información para proyecto de investigación

DURAN HERRERA, VICTOR HUGO

DIRECTOR DE LA OFICINA DE REGISTROS Y ARCHIVOS ACADÉMICOS

UNIVERSIDAD NACIONAL DEL CALLAO
Oficina de Registros y Archivos Académicos
14 JUN. 2017
SECRETARIA - DIRECC

Yo, Casazola Cruz, Oswaldo Daniel, presento a los alumnos:

- Menacho Apolitano, Juan José
- Montalvo García, Peter Jonathan
- Valverde Reyes, José Irving

Con el tema "ISO 27001 para la seguridad de la información de ORAA UNAC – 2017" como proyecto de investigación.

Solicito a usted, brinde la facilidad del caso, con respecto a la información que soliciten para dicho proyecto.

Bellavista, 9 de Junio de 2017

Atentamente,

Casazola Cruz, Oswaldo Daniel

ANEXO "C": DESCRIPCIÓN DEL FORMATO DE ENCUESTA DE LA ISO 27001:2013 APLICADAS A ORAA

Encuestas de la ISO 27001:2013 aplicadas a ORAA

CONFIDENCIALIDAD		
PREGUNTAS	**SI**	**NO**
¿Existe algún archivo de tipo Log donde guarde información Referida a las operaciones que realiza la Base de datos?	1	
¿Existe algún usuario que no sea el DBA pero que tenga asignado el rol DBA del servidor?		1
¿Son gestionados los perfiles de estos usuarios por el administrador?	1	
¿Son gestionados los accesos a las instancias de la Base de Datos?	1	
¿Las instancias que contienen el repositorio, tienen acceso restringido?	1	
¿Se renuevan las claves de los usuarios de la Base de Datos?		1
¿Se obliga el cambio de la contraseña de forma automática?		1
¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?		1
¿Las copias de seguridad son encriptados?		1
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	1	
¿Existen logs que permitan tener pistas sobre las acciones realizadas sobre los objetos de las base de datos?	1	
¿Se tienen lugares de acceso restringido?		1
¿Se poseen mecanismos de seguridad para el acceso a estos lugares?		1
¿A este mecanismo de seguridad se le han detectado debilidades?		1
¿Tiene medidas implementadas ante la falla del sistema de seguridad?		1
¿Con cuanta frecuencia se actualizan las claves o credenciales de acceso?		1
¿Se tiene un registro de las personas que ingresan a las instalaciones?		1
¿Existen metodologías de respaldo de información?	1	
¿Se realizan respaldos de información periódicamente?	1	
¿Existe un administrador de sistemas que controle las cuentas de los usuarios?	1	
¿Existe algún estándar para la creación de contraseñas?		1
¿Se obliga, cada cierto tiempo a cambiar la contraseña?		1
¿La organización cuenta con un proceso para dar mantenimiento preventivo al software?	1	
¿La organización cuenta con un proceso para dar mantenimiento correctivo al software?	1	
¿Se tienen software antivirus instalados en los equipos de cómputo?	1	
¿Cuentan con antivirus actualizado?		1

¿Se tienen instalados anti malware en los equipos de cómputo?		1
¿Cuenta con licencias de software?		1
¿Existe un proceso para mantener las licencias actualizadas?		1
¿Existe un proceso para adquirir nuevas licencias?		1
¿Los usuarios de bajo nivel tienen restringido el acceso a las partes más delicadas de las aplicaciones?		1
¿Se realiza copias de seguridad (diariamente, semanalmente, Mensualmente, etc.)?	1	
¿Se encuentra un administrador de sistemas en la empresa que lleve un control de los usuarios?	1	
¿Las copias de seguridad son encriptados?		1
¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?	1	
¿Hay algún procedimiento para dar de alta a un usuario?		1
¿Hay algún procedimiento para dar de baja a un usuario?		1
¿La red cuenta con los equipos y aplicaciones (protección) necesarias para tener una mayor resguardo de intrusos activos (hackers)?		1
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?		1
¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?	1	
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?	1	
En caso de que el equipo principal sufra una avería, ¿existen equipos auxiliares?	1	
¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?	1	
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?	1	
¿Se documentan los cambios efectuados?		1
¿Es eliminada la cuenta del usuario en dicho procedimiento?		1
¿Existen lugares de acceso restringido?		1
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?		1
¿Los enlaces de la red se testean frecuentemente?		1
¿El equipo de cómputo cuenta con suficiente espacio en HD en función de los servicios que otorga?		1
TOTAL	**20**	**30**

DISPONIBILIDAD		
PREGUNTAS	**SI**	**NO**
¿Realizan mantenimiento preventivo a los equipo de cómputo?		1
¿Realizan mantenimiento correctivo al equipo de cómputo?		1
¿El equipo de cómputo cuenta con suficiente espacio en HD en función de los servicios que otorga?		1
¿El equipo de cómputo cuenta con suficiente memoria RAM en función de los servicios que otorga?	1	
¿La velocidad del procesador es el adecuado para los programas que son utilizados en los equipos?	1	
¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?	1	
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?	1	
En caso de que el equipo principal sufra una avería, ¿existen equipos auxiliares?	1	
¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?	1	
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?	1	
¿Se documentan los cambios efectuados?		1
¿Es eliminada la cuenta del usuario en dicho procedimiento?		1
¿El motor de Base de Datos soporta herramientas de auditoría?	1	
¿Se cuenta con un inventario de todos los equipos que integran el centro de cómputo?	1	
¿Se revisa el inventario con frecuencia semanal?	1	
¿Se posee de bitácoras de fallas detectadas en los equipos?		1
¿La bitácora es llenada por personal especializado?		1
¿Señala fecha de detección de la falla?		1
¿Señala fecha de corrección de la falla y revisión de que el equipo funcione correctamente?		1
¿Se poseen registros individuales de los equipos?		1
¿La bitácora hace referencia a hojas de servicio, en donde se detalla la falla, y las causas que la originaron, así como las refacciones utilizadas?		1
¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa, de mantenimiento?		1
¿Se cuenta con servicio de mantenimiento para todos los equipos?		1
¿Con cuanta frecuencia se realiza mantenimiento a los equipos?		1
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?		1
		1
¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?		1
¿Se cuenta con servicio de mantenimiento para todos los equipos?		1

¿Se realiza mantenimiento a los equipos con frecuencia?		1
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?		1
¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos a adquirir y así elegir el mejor?		1
¿El centro de cómputo tiene alguna sección con sistema de refrigeración?	1	
¿Con cuanta frecuencia se revisan y calibran los controles ambientales?		1
¿Se tiene contrato de mantenimiento para los equipos que proporcionan el control ambiental?		1
¿Se tienen instalados y se limpian regularmente los filtros de aire?		1
¿Con cuanta frecuencia se limpian los filtros de aire?		1
¿Se tiene plan de contingencia en caso de que fallen los controles ambientales?		1
¿Se cuenta con políticas claras y definidas al finalizar la vida útil de los elementos informáticos que se dan de baja?		1
¿Se cuenta con instalación con tierra física para todos los equipos?		1
¿La instalación eléctrica se realizó específicamente para el centro de cómputo?		1
¿Se cuenta con otra Instalación dentro el centro de cómputo, diferente de la que alimenta a los equipos de cómputo?		1
¿La acometida llega a un tablero de distribución?		1
¿El tablero de distribución está en la sala, visible y accesible?		1
¿El tablero considera espacio para futuras ampliaciones de hasta de un 30 % (Considerando que se dispone de espacio físico para la instalación de más equipos)?		1
¿La Instalación es independiente para el centro de cómputo?		1
¿La misma instalación con tierra física se ocupa en otras partes del edificio?		1
¿La iluminación está alimentada de la misma acometida que los equipos?		1
¿Las reactancias (balastros de las lámparas) están ubicadas dentro de la sala?		1
¿Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos a la planta de emergencia?		1
¿Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos al no-break?		1
TOTAL	**11**	**39**

INTEGRIDAD		
PREGUNTAS	**SI**	**NO**
¿Posee la base de datos un diseño físico y lógico?	1	
¿Posee el diccionario de datos un diseño físico y lógico?	1	
¿Los datos utilizados en el entorno de desarrollo, son reales?	1	
¿Las copias de seguridad se efectúan diariamente?	1	
¿Todos los nodos se encuentran bajo un mismo estándar de modo que no se reduzca la velocidad de transmisión?		1
¿Los enlaces de la red se testean frecuentemente?		1
¿La longitud de los tramos de cableado horizontal no excede de los 90 metros?	1	
¿El etiquetado implementado en la organización cuenta con un código de colores para facilitar su identificación?		1
¿Cuenta con un mapa arquitectónico para la verificación del sembrado de nodos?		1
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?	1	
¿Cuenta con dispositivo firewall físico para protección y aseguramiento de la red?		1
¿Las direcciones IP´S de los equipos son implementadas de forma fija?	1	
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?		1
¿Cuenta con dispositivos para la regulación del voltaje?		1
¿Se tiene implementado un sistema de control de acceso a los centros de cableado y dispositivos?		1
¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?		1
¿La red cuenta con los equipos y aplicaciones (protección) necesarias para tener una mayor resguardo de intrusos activos (hackers)?		1
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?		1
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?		1
¿Los datos que viajan por internet se encuentran cifrados?		1
En cuanto a las pruebas del cableado, ¿el departamento de TI, genera sus propios ataques para probar la solidez de la red y encontrar posibles fallas?		1
Cuentan con administración interna de la red es decir, ¿cuentan con VLAN's creadas en el servidor para tener una mayor administración en cada una de las oficinas que se dedican a diferentes actividades?		1
Para evitar vulnerabilidades en las WLAN ¿Usan protocolos de autenticación, como está establecido en el estándar IEEE 802.11?		1
¿La cantidad de dispositivos Access Point es la adecuada en función del número de usuarios que se conectan, como lo establece el estándar 802.11?		1

¿La red inalámbrica proporciona velocidades de transmisión de 54Mbps en distancias cortas?		1
¿Las instalaciones (aulas, cubículos y oficinas) fueron diseñadas o adaptadas específicamente para funcionar como un centro de cómputo?		1
¿Se tiene una distribución del espacio adecuada, de forma tal que facilite el trabajo y no existan distracciones?		1
¿Existe suficiente espacio dentro de las instalaciones de forma que permita una circulación fluida?		1
¿Existen lugares de acceso restringido?		1
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?		1
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de sensores?		1
¿Existen señalizaciones adecuadas en las salidas de emergencia y se tienen establecidas rutas de evacuación?		1
¿Se tienen medios adecuados para extinción de fuego en el centro de cómputo?		1
¿Se cuenta con iluminación adecuada y con iluminación de emergencia en casos de contingencia?		1
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?		1
¿Se tiene un lugar asignado para papelería y utensilios de trabajo?		1
¿Son funcionales los muebles instalados dentro del centro de cómputo: cinto teca, Discoteca, archiveros, mesas de trabajo, etc.?		1
¿Existen prohibiciones para fumar, consumir alimentos y bebidas?		1
¿Se cuenta con suficientes carteles en lugares visibles que recuerdan estas prohibiciones?		1
¿Con cuanta frecuencia se limpian las instalaciones?		1
¿Con cuanta frecuencia se limpian los ductos de aire y la cámara de aire que existe debajo del piso falso (si existe)?		1
¿Se cuenta con interruptores generales?		1
¿Se cuenta con interruptores de emergencia en serie al interruptor general?		1
¿Se cuenta con interruptores por secciones ó aulas?		1
¿Se tienen los interruptores rotulados adecuadamente?		1
¿Se tienen protecciones contra corto circuito?		1
¿Se tiene implementado algún tipo de equipo de energía auxiliar?		1
¿Se cuenta con Planta de emergencia?		1
¿Se tienen conectadas algunas lámparas del centro de cómputo a la planta de emergencia?		1
¿Se sanciona al integrante del departamento si instala software no permitido?		1
TOTAL	**7**	**43**

ANEXO "D": "MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA OFICINA DE REGISTROS Y ARCHIVOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DEL CALLAO 2017"

"Manual del Sistema de Gestión de Seguridad de la Información para la Oficina de Registros y Archivos Académicos de la Universidad Nacional del Callao 2017"

CONTENIDO

"MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA OFICINA DE REGISTROS Y ARCHIVOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DEL CALLAO 2017"

INTRODUCCIÓN

Para la Oficina de Registros y Archivos Académicos la seguridad de la información es un reto que se ha construido a través de un cuidadoso proceso que articula su misión, objetivos y valores corporativos. En el desarrollo de esta estrategia se ha revisado el enfoque basado en procesos de la organización y se han definido procedimientos documentados del sistema de gestión de la seguridad de la información.

En las siguientes secciones de este documento, se establecen el alcance del Sistema de Gestión de Seguridad de la Información para la Oficina de Registros y Archivos Académicos, así como los parámetros que orientan el plan de seguridad de la información y las acciones a seguir para prevenir la aparición o repetición de no conformidades en la compañía.

Este manual permite visualizar la organización como un sistema que interactúa en forma alineada y articulada con los objetivos de la organización, buscando agregar valor a los accionistas, funcionarios proveedores, a la comunidad, su entorno y especialmente a los clientes que han depositado en nosotros la confianza al elegirnos como compañía de financiamiento.

Alcance del manual

El Manual de Gestión de la Seguridad de la Oficina de Registros y Archivos Académicos, está basado en la norma internacional ISO 27001:2013 en esta norma se encuentran plasmadas las especificaciones para la creación de un sistema de gestión de la seguridad de la información (SGSI). El manual tiene por objeto recoger, analizar y definir los diferentes lineamientos que rigen al Sistema de Gestión de Seguridad de la Información de la Oficina de Registros y Archivos Académicos.

I. Control del manual

Es responsabilidad el Jefe de la Oficina de Registros y Archivos Académicos, lo concerniente a su elaboración, modificación, distribución y control.

1.1 Distribución del manual

Se estableció una única versión del manual para la Oficina de Registros y Archivos Académicos, para la fácil consulta de todos los funcionarios de esta.

1.2 Revisión del manual

Este documento será revisado como mínimo una vez al año para efectos de actualización, o por cualquier otro motivo que arroje resultados diferentes a los planeados por el Sistema de Gestión de Seguridad de la Información de la compañía.

II. Visión General del Sistema de Gestión de Seguridad de la Información

Debido a la creciente dependencia de la Oficina de Registros y Archivos Académicos sobre su tecnología y la información que maneja, se decide adoptar un Sistema de Gestión de Seguridad de la Información.

La adopción de un Sistema de Gestión de Seguridad de la Información (SGSI) es para la Oficina de Registros y Archivos Académicos, una decisión estratégica de negocio, que se ve influenciada por las necesidades, objetivos, requisitos de seguridad y los procesos de la organización. A continuación se presentan los lineamientos estratégicos por los cuales se rige la empresa y que ayudan a perfilar en una primera instancia al SGSI:

2.1 Alcance del Sistema de Gestión de Seguridad de la Información

El objeto del sistema de gestión planteado es incrementar la seguridad de la información mediante el mantenimiento de la integridad, disponibilidad y confidencialidad de la información manejada en el macro-proceso de colocación de operaciones administrativas, y de los sistemas informáticos donde esta es depositada y manejada.

2.2 Definición de la política de seguridad de la información

En el Documento "MG-06 Política de Seguridad de la Información" se encuentra definida la Política del Sistema de gestión de Seguridad de la Información de la Oficina de Registros y Archivos Académicos. La Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Oficina de Registros y Archivos Académicos. La Política aplica en todo el ámbito de la Oficina de Registros y Archivos Académicos, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros. Debe ser conocida y cumplida por toda la planta de personal de la Oficina de Registros y Archivos Académicos.

III. Planificación del Sistema de Gestión de Seguridad de la Información

Las etapas definidas para el desarrollo y la implementación del Sistema de Gestión de Seguridad de la Información son:

1. Documentar el sistema

2. Implementar el sistema

3. Evaluar el sistema a través de auditorías internas y externas

4. Mejorar continuamente la eficacia del sistema a través de del análisis de datos.

IV. ¿Qué es un SGSI?

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, entre otros.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

• **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

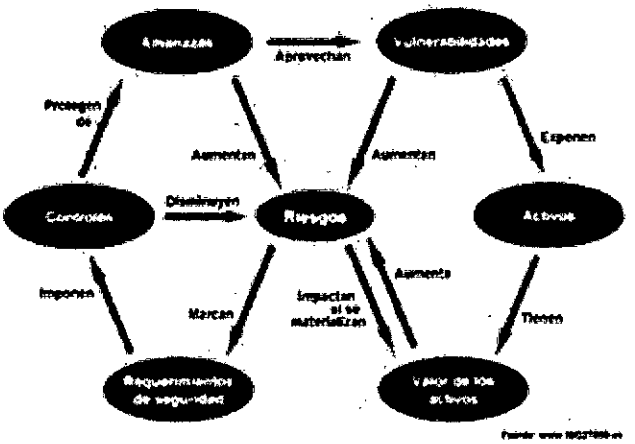
V. ¿Para qué sirve un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

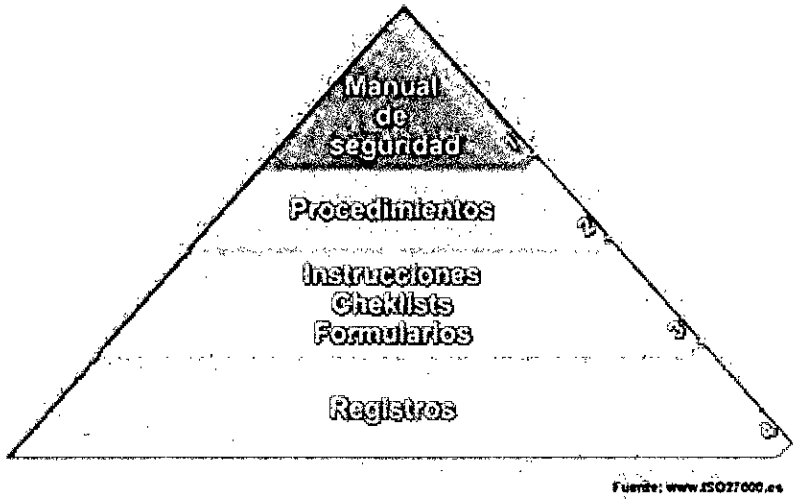


El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

VI. ¿Qué incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:



Documentos de Nivel 1
Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, entre otros, del SGSI.

Documentos de Nivel 2
Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Documentos de Nivel 3
Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4
Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

• **Alcance del SGSI:** Ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

• **Política y objetivos de seguridad:** Documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

• **Procedimientos y mecanismos de control que soportan al SGSI:** Son aquellos procedimientos que regulan el propio funcionamiento del SGSI.

• **Enfoque de evaluación de riesgos:** Descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables .

• **Informe de evaluación de riesgos:** Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

• **Plan de tratamiento de riesgos:** Documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

• **Procedimientos documentados:** Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

• **Registros:** Documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

• **Declaración de aplicabilidad:** (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Control de la documentación

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

• Aprobar documentos apropiados antes de su emisión.

• Revisar y actualizar documentos cuando sea necesario y renovar su validez.

• Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.

• Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.

• Garantizar que los documentos se mantienen legibles y fácilmente identificables.

• Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.

• Garantizar que los documentos procedentes del exterior están identificados.

• Garantizar que la distribución de documentos está controlada.

• Prevenir la utilización de documentos obsoletos.

• Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

VII. ¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

• Plan (planificar): establecer el SGSI.

• Do (hacer): implementar y utilizar el SGSI.

• Check (verificar): monitorizar y revisar el SGSI.

• Act (actuar): mantener y mejorar el SGSI.

VIII. Enfoque Organizacional para la valoración del riesgo

8.1 Metodología seleccionada para la valoración de riesgos

Para hacer la valoración de riesgos de seguridad de la información de la Oficina de Registros y Archivos Académicos se eligió metodología MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Se eligió esta metodología porque brinda una aproximación metódica con herramientas que no dejan lugar a la improvisación. A lo largo del desarrollo de la metodología se establece además un paralelo con la metodología de medición de riesgo operativo de la compañía para así poder comparar los riesgos de seguridad de la información con los demás riesgos operativos de la compañía.

8.2 Criterios de evaluación de riesgos

• La identificación de los riesgos se realizará conjuntamente con los funcionarios involucrados en cada proceso, el control y seguimiento se llevara a cabo de una manera dinámica para así mantener actualizados los factores de riesgo y poder mitigar su impacto oportunamente.

• El reconocimiento y reporte de los factores y eventos de riesgo es responsabilidad de cada área.

• Los Jefes de cada departamento serán los responsables de validar, documentar y firmar el registro de eventos o incidentes de seguridad de la

información, para luego ser enviado al Área de Riesgo Operativo. Los niveles de riesgo aceptables se encuentran plasmados en la siguiente tabla, adicionalmente en está tabla está relacionada la escala de riesgos de SARO con su respectivo nivel de aceptación:

Escala SARO	Riesgo de Seguridad de la Información	Tratamiento del Riesgo
Bajo	Despreciable	Los riesgos ubicados en este nivel se consideran "Altamente Aceptables" e insignificantes, los cuales se administraran con procesos rutinarios controlando que no suban a otro nivel.
	Bajo	
moderado	Medio	Los riesgos ubicados en este nivel se consideran "Aceptables", la responsabilidad de mejorar y monitorear los controles será de los dueños de procesos. Estos riesgos pueden ser objeto de estudio para su tratamiento.
Alto	Alto	
Extremo	Muy alto	Los riesgos ubicados en este nivel se consideran "Inaceptables", el tratamiento a estos riesgos debe ser inmediato, implementando planes de acción para que el nivel de riesgo baje, teniendo en cuenta las prioridades del negocio.
	Crítico	

Fuente: www.ISO27000.es

No todos los riesgos son susceptibles de ser tratados de manera inmediata. Esta decisión depende del nivel en que se encuentre dentro de la matriz o perfil de riesgo. Los riesgos de nivel muy alto y crítico son considerados como inaceptables y se dará prioridad de acción a estos riesgos.

IX. Declaración de aplicabilidad

La declaración de aplicabilidad proporciona un resumen de las decisiones concernientes al tratamiento de los riesgos. La justificación de las exclusiones permite validar que ningún control se omita involuntariamente.

X. Detección y respuesta a los incidentes de seguridad

La Oficina de Registros y Archivos Académicos establece y mantiene una metodología de gestión de incidentes de seguridad de la información. Allí se define la responsabilidad y autoridad con respecto al manejo e investigación de incidentes de seguridad de la información. Esta metodología se encuentra registrada en el documento: "IU-SOP-01-02 Gestión de Incidentes de Seguridad de la Información"

XI. Seguimiento y revisión del SGSI

La Oficina de Registros y Archivos Académicos establece y mantiene una metodología de gestión de incidentes de seguridad de la información. Allí se define la responsabilidad y autoridad con respecto al manejo e investigación de incidentes de seguridad de la información. Esta metodología se encuentra registrada en el documento: "IU-SOP-01-02 Gestión de Incidentes de Seguridad de la Información".

11.1 Auditorías internas del SGSI

La Oficina de Registros y Archivos Académicos establece una metodología de Auditorías Internas de Seguridad de la información. Allí se define la responsabilidad y autoridad en las auditorías de Seguridad de la Información. Esta metodología se encuentra registrada en el documento: "IU-SOP-03-01 Auditorías Internas de seguridad de la información".

MATRIZ DE CONSISTENCIA

Tabla 19: Matriz de Consistencia.

TITULO: "SEGURIDAD DE LA INFORMACIÓN APLICANDO EL ISO 27001:2013 PARA LA OFICINA DE REGISTROS Y ARCHIVOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DEL CALLAO 2017"									
LINEA DE INVESTIGACIÓN	EMPRESA	PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	ÍNDICES	METODOLOGÍA
GESTIÓ N DE TI		**Problema General** ¿De qué	**Objetivo General** Determinar de	**Hipótesis General** La ISO 27001:2013	**Variable 1 / Variable Independiente :** ISO	**ESTRATÉGICA** **TÉCNICA** **LEGAL**	CUMPLIMIENTO	$CUMPLIMIENTO = \frac{Puntj.\ Alcanzado}{Puntj.\ Esperado} \times 100$	

Fuente: Elaboración propia