FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

"Seguridad de la Información y la Gestión de Riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019"

TRABAJO DE INVESTIGACIÓN PARA OBTENER EL GRADO ACADÉMICO DE:
Bachiller en Ingeniería de Sistemas

AUTORES:

Ramirez Rodriguez, Jorge Luis (ORCID: 0000-0001-5322-628X)

Rodriguez Romero, Alejandro (ORCID: 0000-0003-3254-6465)

ASESOR:

Mg. Pérez Rojas, Even Deyser (ORCID: 0000-0002-5855-1767)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

CALLAO – PERÚ

2019

Dedicatoria

Este trabajo de investigación va dirigido a mis padres, por la confianza y el apoyo que constantemente me están brindando para ser mejor persona día a día.

A todas las personas que me acompañaron en este proceso de aprendizaje, tanto a profesores como a compañeros de aula.

Jorge Ramirez

El desarrollo de este trabajo de investigación lo dedico a mis padres y abuelo que me apoyan incondicionalmente en todo aspecto de mi vida, mis hermanas por los ánimos, energía y aliento que me dan al estar presentes y mis dos grandes amigas por escucharme y contribuir en el cumplimiento de mis metas.

Alejandro Rodriguez

Agradecimiento

Agradecer a los docentes de la Escuela de Pregrado de la Universidad César Vallejo, por brindarnos su conocimiento y experiencias vividas, lo cual nos ayudó a realizar la presente investigación.

Al Mgtr. Even Deyser Pérez Rojas docente del curso de Metodología de Investigación Científica, quien nos asesoró y corrigió en el transcurso de todas las sesiones a lo largo de la materia.

Jorge Ramirez

Agradecimiento a todos los docentes y amigos de la Escuela de Ingeniería de Sistemas de la Universidad César Vallejo por los consejos, recomendaciones para así ayudarnos a la creación del presente trabajo de investigación.

A nuestro asesor Mgtr. Even Deyser Pérez Rojas que se encargó de que realicemos un gran trabajo y estuvo pendiente de nuestro desarrollo cada semana a lo largo de todo el ciclo.

Alejandro Rodriguez

Página del jurado

Declaratoria de autenticidad

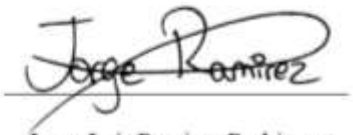
Declaratoria de Autenticidad

Nosotros: Jorge Luis Ramirez Rodriguez identificado con DNI N° 75200120 y Alejandro Rodriguez Romero identificado con DNI N° 70345671, estudiantes del programa de Ingeniería de Sistemas de la Escuela de Pregrado de la Universidad César Vallejo, con el trabajo de investigación titulado: "Seguridad de la Información y la Gestión de Riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019". Declaramos bajo juramento que:

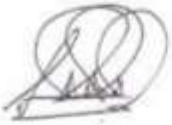
1. El trabajo de investigación es de nuestra autoría.
2. Hemos respetado las normas internacionales de citas y referencias para las fuentes consultadas. Por tanto, el trabajo de investigación no ha sido plagiado ni total ni parcialmente.
3. El trabajo de investigación no ha sido autoplagiado; es decir, no ha sido publicado ni presentado anteriormente para obtener algún grado académico previo o título profesional.
4. Los datos presentados en los resultados son reales, no han sido falseados, ni duplicados, ni copiados y por tanto los resultados que se presenten en el trabajo de investigación se constituirán en aportes a la realidad investigada.

De identificarse la presencia de fraude (datos falsos), plagio (información sin citar a autores), autoplagio (presentar como nuevo algún trabajo de investigación propio que ya ha sido publicado), piratería (uso ilegal de información ajena) o falsificación (representar falsamente las ideas de otras), asumimos las consecuencias y sanciones que de nuestras acciones deriven, sometiéndonos a la normativa vigente de la Universidad César Vallejo.

Callao, 08 de julio del 2019



Jorge Luis Ramirez Rodriguez



Alejandro Rodriguez Romero

Índice

Índice de tablas

Resumen

La presente investigación titulada: "Seguridad de la Información y la Gestión de Riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019", tiene como objetivo general: determinar la relación entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019; como objetivos específicos: (a) determinar la relación que existe entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo de recursos del cómputo de la Universidad Nacional del Callao, (b) determinar la relación que existe entre la seguridad de la información y el nivel de calidad de gastos de los recursos del centro de cómputo de la Universidad Nacional del Callao, (c) determinar la relación que existe entre la seguridad de la información y la tasa de usuarios capacitados de cultura informática del centro de cómputo de la Universidad Nacional del Callao.

Se ha desarrollado una investigación de tipo básica, con un diseño no experimental y de nivel correlacional, bajo un enfoque cualitativo. La muestra fue constituida por 13 estudiantes del centro de cómputo de la Universidad Nacional del Callao. Se aplicó la técnica de la encuesta y como instrumento de recolección de datos, dos cuestionarios (cada uno con 9 preguntas) para obtener información sobre las variables de estudio. Ambos instrumentos fueron validados por 3 expertos en la materia para garantizar la validez y confiabilidad de estos.

Se concluye que no existe relación significativa entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019. Según la correlación de Pearson de 0,055, representando este resultado como bajo con una significancia estadística de p=0,859 (p > 0,05). Por tanto, se acepta la hipótesis nula y se rechaza la hipótesis del investigador.

Palabras Claves: Seguridad de la información, gestión de riesgos, correlación de Pearson.

Abstract

This research entitled: "Information Security and Risk Management in the computing centers of the Universidad Nacional del Callao, 2019", has as its general objective: to determine the relationship between information security and risk management in the computing centers of the Universidad Nacional del Callao o, 2019; as specific objectives: (a) determine the relationship between the security of information and the average time of attention by resource monitoring agent of the computation of the Universidad Nacional del Callao, (b) determine the relationship that exists between security of the information and the level of quality of expenses of resources of the center of computation of the Universidad Nacional del Callao, (c) to determine the relation that exists between the security of the information and the rate of users trained of computer culture of the computer center of the Universidad Nacional del Callao.

A basic type of research has been developed, with a non-experimental and correlational level design, under a qualitative approach. The sample was constituted by 13 students of the computing center of the Universidad Nacional del Callao. The survey technique was applied and as a data collection instrument, two questionnaires (each with 9 questions) to obtain information about the study variables. Both instruments were validated by 3 experts in the field to guarantee the validity and reliability of these.

It is concluded that there is no significant relationship between information security and risk management in the computer centers of the Universidad Nacional del Callao, 2019. According to the Pearson correlation of 0.055, this result represents a low with a statistical significance of $p = 0.859$ ($p > 0.05$). Therefore, the null hypothesis is accepted and the researcher's hypothesis is rejected.

Keywords: Information security, risk management, Pearson correlation.

I. INTRODUCCIÓN

1.1. Realidad Problemática

Desde 1975 a la actualidad, las funciones principales de los seres humanos están relacionados con distintas operaciones con respecto a la información: adquisición, análisis, recreación y comunicación (Revista Sinéctica, 2013, p. 48).

Esto quiere decir que las tecnologías de la información cada día van abriéndose paso en la vida de las personas y evolucionando más y más. Como consecuencia del avance tenemos que hace algunos años pocas organizaciones digitalizaban su información, ya sea por miedo o por no contar con los recursos necesarios; hoy en día es difícil encontrar alguna empresa sea pequeña o grande, que trabaje de esa manera, debido a que es casi imprescindible hacer uso de estas tecnologías.

Entonces, en relación con lo citado inferimos que el mayor activo para cualquier organización, con o sin fines de lucro es su información. De esta forma nace la necesidad y deber de resguardar la data de las organizaciones, de sus usuarios; y también la de gestionar o administrar los posibles riesgos que amenacen la privacidad o atenten contra la estabilidad de este.

En algunos países (por ejemplo, España) existe leyes para la protección de datos, estas leyes van dirigidas a diferentes organizaciones, empresas e instituciones que almacenan y procesan todo tipo de información en sus sistemas (Ochoa, 2017, p. 16).

Se infiere entonces que los métodos de seguridad tomados para proteger la información de carácter personal no varían con relación al tipo de organización que pertenece; están las organizaciones comerciales, las ONG, las instituciones educativas (colegios, academias, universidades), etc. En esta situación, se evaluará a una universidad (Universidad Nacional del Callao) de la cual gran parte es de carácter personal.

Según la Srta. Cartolin estudiante de la Universidad Nacional del Callao y usuaria activa de uno de los centros de cómputo, afirma lo siguiente; para hacer uso de las

computadoras del centro es necesario solicitar el ingreso al encargado registrando tu ingreso, en caso de que alguna computadora presente algún desperfecto el encargado informa para así realizar la revisión para su posterior reparación, en el horario de descanso del encargado la sala queda cerrada imposibilitando el ingreso afectando la disponibilidad de la sala, finaliza mencionando lo paupérrimo que es la velocidad del internet. En base a lo mencionado se puede destacar; en primer lugar que la universidad desea mantener la disponibilidad del centro de cómputo al tener un encargado de supervisar su accesibilidad, sin embargo existen problemas como los son; el internet lento y la respuesta ante la ausencia del encargado, esto evidencia un vacío en el control del centro que puede llegar a ser cubierta con la adecuada implementación de un plan que permita gestionar riesgos, segundo, la existencia de registros de ingreso protege la integridad de la información, con relación a la confidencialidad se evidencio que gran parte del cuidado necesario es dependiente de la noción de seguridad de la información de cada usuario del laboratorio de cómputo, cabe recalcar que hace falta establecer objetivos de control en base a alguna normativa para realizar un análisis más profundo. (Ver Anexo d)

Se elaboró un supuesto caso en base a los mencionados por la Srta. Cartolin para que de esta manera sea posible comprender con mayor exactitud el nivel de seguridad que provee la universidad (UNAC) a los usuarios de los centros de cómputo. Como punto de partida se ideo a un usuario común y a un posible atacante (pirata informático). El planteamiento del caso inicio de la siguiente forma; el supuesto atacante instala software malicioso con la capacidad de capturar la información que ingresa por medio del teclado y enviarlo a un ordenador en una localidad distinta probablemente oculta, se concibió las siguientes preguntas, ¿es posible instalar software malicioso en los ordenadores?, ¿los ordenadores tienen antivirus?, cabe señalar que se brindó a la señorita Cartolin una definición de cada uno de los términos que se le menciono para evitar confusiones. Las respuestas obtenidas confirmaron lo evidenciado en las afirmaciones previas.

Para finalizar, todas las universidades tanto nacionales como particulares manejan una gran cantidad de información, con respecto a sus alumnos, catedráticos, personal administrativo, cursos, etcétera; por esta razón es necesario aplicar una gestión adecuada de riesgos, esto debido a las múltiples amenazas a las que se expone la

información de las organizaciones, pueden ser tanto internas (los propios usuarios a causa de la carencia de cultura de seguridad informática) como externas (piratas informáticos que pueden explotar la mínima seguridad de dichos centros). (Ver Anexo c)

1.2. Aporte para el contexto social

1.2.1. Antecedentes Internacionales

Ararat Muñoz, Johanna Carolina (2018) en su trabajo de investigación la cual lleva por título: "Diseño de un SGSI basado en la norma ISO 27001 para la empresa MA Peñarol Cía. S.A.S. sede principal Cúcuta", concebida en la Universidad Nacional Abierta y a Distancia; donde el objetivo principal es el de entregar un diseño que permita implementar un SGSI basándose en la norma ISO 27001 para la organización en estudio. Dicha investigación es de tipo aplicada, con una población y muestra de 54 y 10 empleados respectivamente. El autor llega a la conclusión que por el número de personas involucradas con el manejo de información es necesario poner en funcionamiento un SGSI, de esta manera asegurar la integridad de la data, y de igual manera la confidencialidad y disponibilidad de la información.

Nieves, Arlenys Carolina (2017) elaboró un trabajo de investigación: "Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2013", desarrollada en la casa de estudios Institución Universitaria Politécnico Grancolombiano; donde uno de los propósitos de la investigación es el concretar una metodología para poder conocer y calificar los activos de la información. Para dicha investigación se utilizó el cuestionario y entrevistas. El autor llego a la conclusión de que la valoración de los riesgos de los activos de la información permitió identificar que el desconocimiento del tema pone en peligro la disponibilidad, integridad y confidencialidad.

Maureira Sánchez, Daniel J. A. (2017) desarrollo una tesis de título "Norma ISO/IEC 27001 Aplicada A Una Carrea Universitaria" desarrollada en la Universidad Andrés Bello ubicada en Santiago de Chile. Dicha tesis tiene

como propósito general el proponer un diseño de SGSI para asegurar el cumplimiento de la auditabilidad, disponibilidad, confidencialidad e integridad de la data aplicando la norma ISO 27001. Para la investigación obtuvo sus datos del personal que se encuentra laborando en la Dirección de Servicios Telemáticos mediante entrevistas. Uno de los datos más relevantes que obtuvo el autor fue el de corroborar que solo se cumplen el 31% de los requisitos mínimos de la norma ISO/IEC 27001:2013. Llegando así a la conclusión general de que los sistemas de información aparte de ofrecer beneficios a una organización o institución conlleva riesgos que en su mayoría son desconocidos por la gerencia causando así la no inversión en mecanismos de protección.

Changoluisa Criollo, Wilson Fernando (2017), en su trabajo de titulación de nombre "Optimización Del Proceso De Alta Y Baja De Usuarios A Través De La Implementación De Gestión De Seguridad De La Información, Basado En La Norma ISO 27001:2013 En Una Empresa De Consultoría Para La Industria Petrolera" realizada en la Pontífice Universidad Católica del Ecuador-Matriz tiene como propósito general el de reducir el porcentaje de reprocesos que manifiesta la empresa. El trabajo obtuvo resultados positivos entre los que se puede destacar los siguientes; se redujo el valor promedio de reprocesos en un 76,84% lo que quiere decir que hubo una reducción de tiempos en los subprocesos que conforman el proceso de alta y baja de personas que interactúan con los ordenadores, y la alineación de los propósitos de control y controles aplicables según la Norma Internacional ISO 27001:2013.

Meneses Martinez, Alexander, Ramirez Camargo, Erney Alberto, Merchan Villalba, Maria Alejandra y Suarez de la Cruz, Yaditza, en su trabajo de grado para poder obtener el título de especialista en auditoría en sistemas nombrado "Diseño del Sistema de Gestión de Seguridad de la Información SGSI Basado en el Estándar ISO 27001, Para Los Procesos Soportados Por El Área De Sistemas En La Cámara De Comercio De Aguachica, Cesar" elaborada en la casa de estudios Universidad Francisco de Paula Santander Ocaña en Colombia teniendo como población y muestra el total del personal

administrativo resaltan la exigencia de implementar un marco de referencia que garantice la protección de la data en los procesos del área de sistemas de la Cámara de Comercio de Aguachica. El trabajo de grado establece en sus conclusiones que los riesgos a los que la empresa está expuesta, son principalmente a causa de la escasez de conocimiento de las costumbres adecuadas vinculadas a la seguridad básica para el cuidado de la información.

En términos generales basándonos en los resultados y conclusiones de los autores previamente mencionados podemos afirmar que una organización al realizar la implementación de un SGSI de forma adecuada puede reforzar los pilares de sus tan valiosos activos, su información, de esta manera se podrá realizar un mejor plan de gestión de riesgos antes posibles atentados para la información que se maneja.

1.2.2. Antecedentes Nacionales

Calderón Sánchez, Jorge Armando (2019) al realizar su investigación para obtener la Maestría en Ingeniería De Sistemas con reconocimiento en Tecnologías de la Información, que lleva por título: "Seguridad de la Información y la gestión de riesgos en los trabajos de la DIGERE del ministerio de educación, 2018", realizada en la Universidad Privada César Vallejo, donde el objetivo general es el de estatuir el vínculo que pueda existir entre las variables de estudio con respecto a los trabajadores de la organización mencionada. Dicho estudio aplicó el método hipotético–deductivo, con un enfoque cuantitativo, utilizo un diseño no experimental, de tipo básica, cuenta con una población y muestra de 106 y 83 trabajadores respectivamente. El autor finaliza su estudio con una conclusión positiva, si existe un vínculo directo entre ambas variables en los empleados de la DIGERE del MINEDU, debido a que se logró un valor de significancia igual a cero con un Rho de Spearman de (0.886).

Zacarias Villafranca Jean Carlo (2017) al realizar su tesis para obtener el Título Profesional de la carrera de Ingeniería de Sistemas e Informática: "Modelo de Seguridad de la Información basado en la ISO/IEC 27001:2013 para mitigar los riesgos de los activos de la información en la Central De

Operaciones Policiales de la Región Policial de Junín", realizada en la Universidad Continental, donde el objetivo principal es el de estatuir la influencia que tiene un modelo con respecto a la protección de la data fundamentada en la norma ISO/IEC 27001:2013 para poder contrarrestar los riesgos que atentan a los activos de la información. Es una investigación de tipo aplicada, donde la población son todos los efectivos policiales pertenecientes a la Central de Operaciones Policiales ubicada en la Región Junín, y la muestra es de 32 trabajadores. El autor llegó a la conclusión de que los conocimientos que tenían los efectivos policiales, con respecto al nivel de protección de la información han aumentado en 75% preliminar a la puesta en funcionamiento de un modelo que permita la protección de la data por parte de los trabajadores.

Vilca Mosquera, Ehytel Celestino (2017) presentó su tesis titulada: "Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de Lima", realizada a la Universidad de Huánuco; donde el objetivo general es el de estatuir que mejoras se obtienen al poner en funcionamiento un SGSI para la protección del área de RR.HH. de la organización Geosurvey S.A., la investigación cuenta con un enfoque cuantitativo, diseño pre experimental, como población se consideró a todos los integrantes del órgano administrativo de la organización y con una muestra de 33 personas. Los resultados y conclusiones obtenidos son positivos con relación a la situación que presentaba antes de poner en funcionamiento el SGSI, los resultados más destacados son; el 9,1% de la población carecía del conocimiento necesario para manejar las tecnologías de la información y comunicación de la organización, después de la implementación aumento al 90,0% esto gracias a las capacitaciones y la creación de un documento con la información requerida al que poder consultar, también se menciona que la empresa presentaba una cifra del 87,9% como el total de trabajadores que no aplicaban técnicas de cifrado como medida preventiva para la perdida de información, dicha porcentaje fue reducido a un 69,7%. Como conclusión general se

obtuvo que la implementación de un SGSI dio como resultado una mejora en todos los aspectos previstos.

Tarrillo Saldaña, Esther Marleni (2016) presento su tesis bajo el nombre: "Influencia de la Gestión de Riesgos en la seguridad de la información de la zona registral III sede Moyobamba, 2015", en la Universidad Privada César Vallejo, en el que se tiene como propósito, verificar la relación que guarda la Gestión de Riesgos en la protección de información del sector registral III sede Moyobamba. Para dicha investigación se trabajó con una muestra de 50 empleados mediante el muestreo no probabilístico por conveniencia de 150 trabajadores que conforman la población. Como conclusión general la investigación estableció el nivel de riesgo como "alto" en cada una de las dimensiones evaluadas en los activos de información.

Agurto Castillo, Manuel Armando (2017) realizó la tesis que lleva por título: "Diagnostico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001", en la que se define como objetivo principal proteger la información generada en el área de QHSE fundamentada en la norma ISO 27001. Para la investigación se realizaron reuniones, aplicaron cuestionarios, etcétera según la norma ISO 27001. La población y muestra de la investigación fue determinada en función del indicador a medir. Como conclusión general el autor determinó que existía muy poca entrega con respecto a la protección de la información dando como resultado una mejora en todos los aspectos evidenciados en la investigación.

Cruz Diaz, Miguel Angel y Fukusaki Infantas, Senyi (2017) en su tesis para obtener el título profesional de ingeniero de computación y sistemas de título "Diseño e Implementación De Un Sistema De Gestión De Seguridad De La Información Para Proteger Los Activos De Información De La Clínica MEDCAM PERU S.A.C." desarrollada en la Universidad Privada San Martin de Porres presenta como propósito general, mitigar los riesgos a la que la data de la clínica MEDCAM Perú S.A.C. se encuentra expuesta. Para la puesta en funcionamiento del SGSI se aplicó el ciclo de Deming o PHVA (P: Planificar,

H: Hacer, V: Verificar y A: Actuar). La tesis indica que finalizada la implementación, se pudieron concluir con los objetivos y metas trazadas llegando a una serie de conclusiones y recomendaciones de las cuales podemos resaltar la sensibilización del personal en aspectos de seguridad y ampliar el SGSI al resto de procesos de la clínica, respectivamente.

1.3. Marco Teórico

El presente estudio pretende estatuir cual es la relación que mantiene la seguridad de la información con la gestión de riesgos que posee la UNAC, esto con el fin de saber si cumple con los modelos de seguridad establecidos a nivel mundial.

Las empresas que posean una estructura jerárquica requieren de mecanismos que permitan realizar la gestión de posibles riesgos, garantizando la protección y las defensas de la data, y que se cumplan las etapas del PHVA (Vilca, 2018, p. 124). De lo mencionado, se puede inferir que en caso no exista una metodología de gestión para la protección de la información es posible que surjan amenazas y riegos que atenten contra la organización.

Por otra parte, Serrahima (2010, p. 18) indica que, "La tecnología informática avanza tan rápidamente que es imposible para una pyme dedicar recursos a estar permanentemente al día. Y peor aún. Mucho más rápido que la tecnología avanzan las amenazas y riesgos asociadas a la misma.". De lo citado, podemos obtener que mientras las tecnologías de la información están en crecimiento, proporcionalmente las amenazas y riesgos también elevan su porcentaje.

Entonces según los autores Vilca y Serrahima toda empresa u organización que maneje a un grupo de personas clasificadas de manera jerárquica está en la obligación e incluso la necesidad de poner en funcionamiento un SGSI, con el fin de administrar la vulnerabilidad de la información y así reducir las amenazas y riesgos al mínimo posible.

Kronisch afirma:

> El crecimiento acelerado de las redes sociales y el IoT, caracterizado por el aumento en el volumen y la velocidad de la información compartida públicamente, presenta consecuencias significativas para la seguridad de las operaciones más allá de los

> peligros más conocidos del robo de identidad u otros daños individuales causados por violaciones de datos personales. (2019, p. 9)

Lo mencionado por el autor refuerza la idea de optimizar el tratamiento que se le da a la protección con respecto a la información.

1.3.1 Seguridad de la Información

Para Cruz y Fukusaki (2017) la seguridad de la información engloba todo lo relacionado con políticas para la gestión de la seguridad de la información (p. 19).

Dicha variable es el eje central de este trabajo de investigación siendo el cimiento para el desarrollo del SGSI.

Dimensiones de la variable Seguridad de la Información

Dimensión confidencialidad

Según Meneses [et al.] (2012), la confidencialidad es el permitir acceder a la información a todo aquel que se encuentre autorizado sin ninguna excepción (p. 20).

Es una característica de difícil recuperación, que clasifica la información en pública y privada, pudiendo significar la infracción de leyes y compromisos con respecto a la protección datos (Zacarias, 2017, p. 29).

En términos generales se deduce de lo citado previamente que la confidencialidad es esencial tomarlo en cuenta por los beneficios que trae a la privacidad, de lo contrario puede llevar a un daño irremediable.

Indicador efectividad del control de acceso

Este indicador nos permite medir si los centros de cómputo de la Universidad Nacional del Callao restringen o permiten el acceso de un determinado usuario a una determinada área, previa validación de forma correcta.

> Cada persona que interactúa con el ordenador deberá de contar con un usuario y contraseña que le permita acceder al sistema, estos dos últimos deberán ser personales e intransferibles para que puedan hacer uso y manejo de las herramientas tecnológicas para la ejecución de sus deberes (Meneses, 2012, p. 193).

Dimensión integridad

Según Meneses et al. (2012) la integridad es la conservación de la información en su totalidad (p. 21).

Esto apoya la definición de Maureira (2017, p. 145) que afirma, "Permite que la información sea correcta y que no haya sido alterada por usuarios, entidades o procesos no autorizados".

Por lo tanto, mediante esta dimensión evaluamos los cambios que puedan llegar a tener los datos que almacena o gestiona la organización.

Indicador tasa de perdida de información

El mayor activo que puede poseer cualquier organización o empresa sea cual sea el rubro, es su información. Es por que uno de los principales problemas para las entidades, es perder su información (Mosquera, 2017, p. 59).

Se deduce de lo citado que un gran temor para las organizaciones es la perdida de información sensible, esto a causa de la inexistencia de un SGSI. El propósito de este indicador es obtener el porcentaje de información perdida mediante.

Dimensión disponibilidad

Disponibilidad hace referencia a la posibilidad de poder acceder a la información y sistemas cuando sea requerido (Mosquera, 2017, p.30).

En relación con lo mencionado, las posibles consecuencias de no cumplir con dicha dimensión los procesos de la organización se pueden ver ralentizados e incluso detener algo nada favorable para la organización.

Indicador gestión de contingencias

Rodríguez [et al.] (2007, p. 110) afirma lo siguiente: "El nivel de contingencia refleja los riesgos y la incertidumbre del proyecto y normalmente se reduce a medida que este avanza. Por este motivo, el plan de contingencias debe responder siempre a la valoración de los riesgos identificados.". De lo citado podemos inferir que siempre van a existir riesgos y amenazas, es responsabilidad de la organización realizar un plan de contingencias.

Para poder obtener el indicador, hay que saber si se está realizando correctamente la gestión de contingencias a través de pruebas de calidad.

1.3.2. Gestión de Riesgos

Kiesel (2001, p. 20) afirma que: "Es reducir la vulnerabilidad de la población, de la infraestructura y de las instituciones en zonas que puedan ser afectadas. Esta situación no incluye simplemente soluciones técnicas…".

Dimensiones de la variable Gestión de Riesgos

Dimensión Recursos

Tanto el hardware como el software están diseñados para poder interactuar uno con el otro, de no ser así, estos se volverían inservibles. Al no poder comunicarse, estos no podrán ser utilizados, por ende las empresas pierden herramientas informáticas muy valiosas, ya que los ordenadores son indispensables para cualquier negocio (Quispitupac y Mateo, 2014, p. 29).

De lo ya mencionado podemos deducir que los recursos siempre son importantes para las empresas, debido que le generan un valor agregado

a cada organización, estos pueden ser talento humano, infraestructura, hardware, software, etc.

Indicador Tiempo medio de atención

Muñoz (2009, p. 93) afirma lo siguiente: "Los principales componentes de la estrategia de las empresas que sustentan su éxito en el tiempo de respuesta las necesidades de los clientes, así como la importancia del tiempo de flujo, que es la medida de desempeño operacional más relacionada con el tiempo de respuesta".

De lo citado, se puede deducir que las empresas siempre buscan atender a la brevedad a los clientes, en este caso los clientes de la universidad vendrían a ser los estudiantes.

Indicador Nivel de Calidad de Gastos

Hace referencias a las actividades financieras por parte de las universidades, con las obligaciones de adquirir productos o pagar por la prestación de algún servicio (Gonzales, 2004, p. 76).

Este indicador busca evaluar los gastos realizados por parte de la Universidad Nacional del Callao; si fueron derivados a otras áreas, hardware, o software que en verdad sean necesarios.

Dimensión Cultura Informática

Esta dimensión hace referencia a la cultura que posee la población y comunidad de la Universidad Nacional del Callao, hacia sus instalaciones y equipos que conformas el centro de cómputo, el uso y cuidado de estos.

Indicador Tasa de usuarios capacitados

Como todo sistema, siempre va a tener usuarios, estas personas son las encargadas de relacionarse con los aplicativos, es por ello que se deben realizar campañas que permitan capacitar a los usuarios con respecto al uso del sistema (Kendall, 2005, p. 38).

El presente indicador tiene como propósito medir la capacidad de los usuarios, si están en las condiciones de hacer uso de los centros de cómputo de la Universidad Nacional del Callao.

1.4. Formulación del Problema

Problema general

¿Qué relación existe entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019?

Problemas específicos

PE1: ¿Qué relación existe entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo de recursos en los centros de cómputo de la Universidad Nacional del Callao, 2019?

PE2: ¿Qué relación existe entre la seguridad de la información y el nivel de calidad de gastos de los recursos en los centros de cómputo de la Universidad Nacional del Callao, 2019?

PE3: ¿Qué relación existe entre la seguridad de la información y la tasa de usuarios capacitados en cultura informática en los centros de cómputo de la Universidad Nacional del Callao, 2019?

1.5. Justificación de la Investigación

¿Cuál es el fin de este estudio?, ¿Por qué en una universidad?, ¿Por qué seguridad de la información?, ¿Por qué gestión de riesgos?, ¿cuáles son los beneficios de realizar la implementación de un plan de gestión de riesgos?, ¿por qué es conveniente el realizar el trabajo de investigación?, ¿cuál es la importancia de desarrollar la presente investigación?, son algunas de las interrogantes que nos planteamos al momento de realizar el presente trabajo de investigación.

El presente estudio tiene un alto grado de relevancia debido a que nos permite obtener un nuevo conocimiento acerca de la relación que mantiene la Seguridad de la Información y la Gestión de Riesgos; dicho conocimiento puede ser de gran

ayuda, tanto para autoridades del escenario de estudio (centros de cómputo de la UNAC), como para otras universidades.

Los motivos que nos llevaron a desarrollar el presente estudio es estatuir cual es la relación que mantiene la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, esto por la constante afluencia de alumnos y catedráticos.

Se realizará la investigación en una universidad por la importancia que representa en la sociedad, además de servir como modelo para futuras investigaciones vinculadas o relacionadas a la protección de la información en centros de estudio.

Los beneficios más notables de poner en funcionamiento un plan para gestionar y mitigar los riesgos vinculados a la protección de la data son; la capacidad de poder reaccionar ante cualquier incidente y evitar posibles gastos en reparación o subsanación por eventos que pueden ser evitados.

Al realizar la investigación se abre la posibilidad de realizar posteriormente la implementación de algún marco de referencia para así obtener alguna certificación como la norma ISO 2700,1 de esta forma el prestigio de la universidad incrementara logrando así un crecimiento de la cantidad de postulantes por ende ingresantes a su vez una mayor inyección de dinero para seguir mejorando.

Existen pautas para poder determinar los beneficios de un estudio propuesto, por lo general estas pautas son flexibles y no son completos. Muchas veces solo se cumplen una de estas pautas (Hernández, Fernández y Baptista, 2014, p. 40). Para el presente estudio se expondrá los siguientes criterios; justificación teórica, justificación tecnológica, justificación práctica, justificación social, justificación económica y justificación metodológica.

Justificación teórica

Desde la perspectiva teórica, esta investigación tiene como propósito, el de aportar al conocimiento existente sobre cómo funciona la seguridad de la información y la gestión de riesgos en las universidades, en este caso, específicamente en los centros de cómputo de la UNAC.

Justificación tecnológica

La recolección de datos de esta investigación permitirá brindar conocimiento a las autoridades de los centros de cómputo de la Universidad Nacional del Callao; si es necesario o no, realizar mejoras o correcciones con respecto al uso de su infraestructura tecnológica.

Justificación práctica

La presente investigación aspira recomendar una o varias medidas de solución al problema planteado anteriormente. Es decir, de qué manera se debe de gestionar la seguridad de la información, elaborando un plan que permita la gestión de riesgos.

Justificación económica

La recolección de datos de esta investigación permitirá brindar conocimiento a las autoridades de los centros de cómputo de la Universidad Nacional del Callao; con respecto a la calidad de gastos, invertidos en las instalaciones de la Universidad. Además, de realizarse la implementación de un plan de gestión de riesgos es posible ampliar implementación al resto de áreas de la universidad logrando así un ahorro en posibles incidencias o emergencias.

Justificación social

El implementar un marco de referencia para la seguridad de la información y la gestión de riesgos traería como consecuencia un aumento en la cultura informática consecuentemente menor información se verá en riesgo y se prevendrían problemas como la perdida de información personal (contraseñas, documentos privados, etc).

Justificación metodológica

De acuerdo con el aspecto metodológico, el presente producto de investigación busca poder estatuir la relación que pueda existir entre la Seguridad de la Información y la Gestión de Riesgos en los centros de cómputo de la Universidad Nacional del Callao, para poder gestionar de la mejor manera posible uno de los mayores activos de dicha organización, la información.

1.6. Hipótesis

Hipótesis general.

Existe relación significativa entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019.

Hipótesis específicas.

HE1: Existe relación significativa entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo de los recursos en los centros de cómputo de la Universidad Nacional del Callao, 2019.

HE2: Existe relación significativa entre la seguridad de la información y el nivel de calidad de gastos de los recursos en los centros de cómputo de la Universidad Nacional del Callao, 2019.

HE3: Existe relación significativa entre la seguridad de la información y la tasa de usuarios capacitados en cultura informática en los centros de cómputo de la Universidad Nacional del Callao, 2019.

1.7. Objetivo general y específico

Objetivo General.

Determinar la relación entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019.

Objetivos Específicos.

OE1: Determinar la relación que existe entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo de recursos en los centros cómputo de la Universidad Nacional del Callao.

OE2: Determinar la relación que existe entre la seguridad de la información y el nivel de calidad de gastos de los recursos en los centros de cómputo de la Universidad Nacional del Callao.

OE3: Determinar la relación que existe entre la seguridad de la información y la tasa de usuarios capacitados en cultura informática en los centros de cómputo de la Universidad Nacional del Callao.

II. MÉTODO

2.1. Tipo y Diseño de Investigación

2.1.1. Tipo de Estudio

El presente trabajo realiza una investigación de tipo básica; debido a que se busca obtener información acerca de las dos variables que la conforman (Seguridad de la Información y la Gestión de Riesgos), una vez recolectada toda la información posible, se elaborará recomendaciones. Al respecto, distintos autores afirmaron lo siguiente:

Según López et al. (2006, p. 38), "Su pretensión fundamental es incrementar el conocimiento en determinada área. Busca descubrir leyes o principios; en ella se apoyan quienes desean encontrar soluciones a problemas sociales y teóricos concretos". De lo anterior, se puede obtener que este tipo de investigación utiliza de una manera cuidadosa la técnica del muestreo, con el propósito de ampliar la visión de los resultados obtenidos.

2.1.2. Diseño de Investigación

El diseño de investigación propuesto a utilizar en el presente trabajo de investigación es no experimental transeccional correlacional-causal.

Para una investigación no experimental, se observan las situaciones de estudio que ya existen, no originadas intencionalmente en el estudio (Hernández, Fernández y Baptista, 2014, p. 152).

Con respecto a lo citado se infiere que, el tipo de diseño de investigación no experimental no necesita recrear un hecho para así obtener datos.

Con respecto a la investigación transeccional o transversal, su finalidad es detallar y estudiar variables, que relación y que incidencia pueden tener una con la otra (Hernández, Fernández y Baptista, 2014, p. 154).

De lo cual deducimos que al ser la investigación transversal se limita únicamente a un periodo de tiempo limitado.

Este diseño de investigación puede condicionarse a constituir relaciones entre las variables de estudio (Hernández, Fernández y Baptista, 2014, p. 157). Con relación a lo citado se puede inferir que el diseño de investigación correlacional-causal tiene como propósito el detallar las relaciones o vínculos con respecto a las variables de estudio.

En conclusión, según lo mencionado podemos manifestar que el diseño de la presente investigación es no experimental debido a que no se recrea ninguna situación de forma intencional, clasificada como transeccional o transversal por la delimitación temporal existente en la investigación y correlacional-causal debido a la situación actual de la UNAC y su relación con la seguridad de la información que mantiene en sus centros de cómputo.

2.1.3. Nivel de Investigación

El presente estudio utiliza un nivel de investigación correlacional; debido a que la investigación busca descubrir la relación o el vínculo que existe entre las dos variables de estudio para la obtención de información. Respecto a esto, anteriormente se mencionó lo siguiente:

Intenta ver de qué manera se relacionan distintos fenómenos de estudio, o en todo caso si no lo hicieran (Reguera, 2008, p. 46). Como bien menciona el autor, el propósito de este nivel de investigación es el de vincular dos variables; seguridad de la información y la gestión de riesgos.

2.1.4. Enfoque de Investigación

El enfoque de investigación a utilizar en el presente estudio es el cualitativo, esto debido a que utiliza un proceso inductivo. Emplea la recolección de

datos, y posteriormente su análisis para poder formular las interrogantes o presentar nuevas preguntas (Hernández, Fernández y Baptista, 2013, p. 7). Lo mencionado por el autor se ve reflejado en la elaboración de las encuestas para la obtención de información.

2.2. Escenario de Estudio

Se designó como escenario de estudio para la realización del presente estudio, los centros de cómputo de la UNAC, debido a que se considera que es un lugar donde se puede recolectar información importante para los propósitos de esta investigación.

2.3. Participantes

2.3.1. Población y muestra

Se designó como participantes para la realización del presente estudio, a los estudiantes que asisten a los centros de cómputo de la UNAC, debido a que ellos están haciendo uso continuo de dichos espacios. La población y muestra para la presente investigación son de 13 personas, ya que son el total de usuarios que se encontraban en el centro de cómputo de un total de 24 computadoras disponibles en la facultad de contabilidad en el momento de realizar las encuestas.

2.3.2. Muestreo

El tipo de muestreo a utilizar es el no probabilístico avalado según la afirmación de Hernández, Fernández y Baptista.

Este procedimiento no toma referencia de ningún tipo de fórmulas de probabilidades, por el contrario depende netamente del grupo de investigadores, por ende las muestras elegidas cumplen otros criterios de investigación. Si elegimos un muestreo probabilístico o no probabilístico va a depender de los problemas planteados en el estudio (Hernández, Fernández y Baptista, 2013, p. 176).

En base a lo mencionado por el autor se eligió el muestreo no probabilístico por el enfoque de la investigación, cualitativo, diseño de la investigación, correlacional y por el tipo de población del que se dispone.

2.4. Técnicas e Instrumentos de recolección de datos

Técnicas de recolección

Las técnicas componen las acciones y procedimientos que los investigadores emplean para la obtención de información. Se caracterizan por ser prácticas (Abril, 2008, p. 4).

La técnica empleada para la recolección de información que se empleó para el presente estudio es la encuesta.

Instrumentos de recolección

Herramienta que será empleada por el investigador o grupo de investigación para poder registrar todo tipo de información vinculada a las variables correspondientes al estudio planificado (Hernández, Fernández y Baptista, 2013, p. 199).

El instrumento que permitirá la recolección de datos que utilizará la presente investigación para obtener información será el cuestionario (Ver Anexo g).

Validez

Es el nivel en que el instrumento de recolección de datos evidencia información relevante para los propósitos de estudio (Landeau, 2007, p. 81).

De lo ya mencionado, se puede obtener que gracias a la validez se podrá saber si el instrumento es adecuado para la investigación.

Confiabilidad

Es el nivel con el cual el instrumento de recolección de datos demuestra su solidez y coherencia al aplicarlo al objeto en estudio (Landeau, 2007, p. 81).

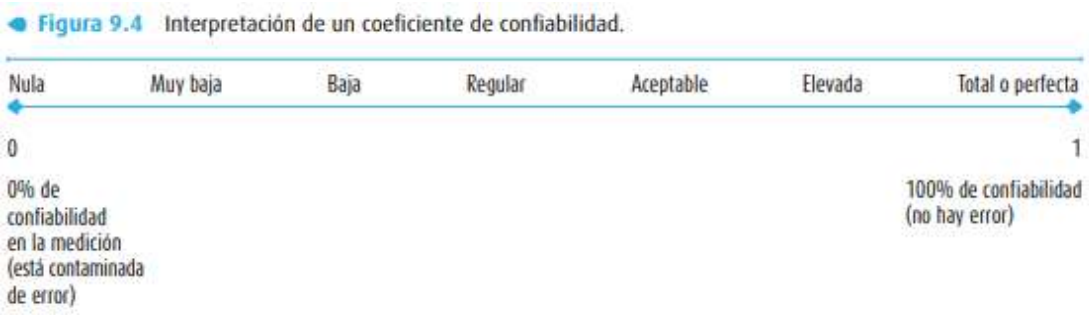
De lo citado, se puede obtener que la confiabilidad representa el nivel de coherencia que muestran los resultados obtenidos por medio del instrumento de recolección de datos.

Tabla 1: Juicio de expertos

		Seguridad de la Información			Gestión de Riesgos		
N.º	Expertos	Pertinencia	Relevancia	Claridad	Pertinencia	Relevancia	Claridad
1	Mg. Melquiades Efraín Melgarejo Graciano	✓	✓	✓	✓	✓	✓
2	Dr. Juan Brues Lee Chumpe Agesto	✓	✓	✓	✓	✓	✓
3	Mg. Bernardo Patricio Ávila López	✓	✓	✓	✓	✓	✓

Nota: La tabla muestra en forma resumida, el resultado obtenido de aplicar el análisis del juicio de expertos al presente estudio. Se manifiesta que el instrumento es aplicable en cada uno de los parámetros de evaluación de las variables en estudio.

Para que un instrumento de medición de datos llegue a ser confiable, puede ser especificado por distintas técnicas (Hernández, Fernández y Baptista, 2013, p. 200). El presente estudio opta por una técnica denominada "coeficiente alfa de Cronbach".



Fuente: Hernández, Fernández y Baptista (2013, p.207).

En base a lo expuesto por el autor obtenemos, lo siguiente:

Tabla 2: El resultado luego de aplicarse el análisis alfa de Cronbach a los resultados del cuestionario de la variable Seguridad de la Información

Variable	Alfa de Cronbach	N.º de ítems
Seguridad de la Información	0.734	9

Nota*:* La tabla muestra que el coeficiente del alfa de Cronbach aplicado a los resultados del cuestionario de la variable Seguridad de la Información es 0,734 el cual representa un nivel de confiabilidad aceptable.

Tabla 3: El resultado luego de aplicarse el análisis alfa de Cronbach a los resultados del cuestionario de la variable Gestión de Riesgos

Variable	Alfa de Cronbach	N.º de ítems
Gestión de Riesgos	0.729	9

Nota*:* La tabla muestra que el coeficiente del alfa de Cronbach aplicado a los resultados del cuestionario de la variable Gestión de Riesgos es 0,729 el cual representa un nivel de confiabilidad aceptable.

Tabla 4: El resultado luego de aplicarse el análisis alfa de Cronbach a los resultados del cuestionario de ambas variables

Variable	Alfa de Cronbach	N.º de ítems
Seguridad de la Información y Gestión de Riesgos	0.708	18

Nota*:* La tabla muestra que el coeficiente del alfa de Cronbach aplicado a los resultados del cuestionario de ambas variables es 0,729 el cual representa un nivel de confiabilidad aceptable.

2.5. Procedimiento

Mediante la información recolectada se procederá a ingresarla en el software SPSS para realizar las siguientes pruebas estadísticas; alfa de Cronbach, prueba de normalidad, y coeficiente de correlación según Pearson. De esta forma se obtendrá si existe o no una relación (o algún tipo de vínculo) significativa entre las variables de estudio.

Rho de Pearson

Prueba estadística que permite observar la relación y el vínculo que pueda existir entre dos variables. Los resultados de dicha prueba, no califican a una como

dependiente, ni a la otra como independiente, puesto a que no califica la casualidad (Hernández, Fernández y Baptista, 2013, p. 304).

Ya que las variables a evaluar en el presente trabajo no son dependiente ni independiente es posible aplicar dicha prueba e interpretarla. Hernández, Fernández y Baptista establecen una serie de indicaciones que sirve para interpretar los resultados.

En base a lo mencionado por los autores a través de una herramienta de pruebas estadísticas es posible obtener la información necesaria para su posterior evaluación.

2.6. Método de análisis de información

El presente estudio hará uso del software que emite reportes de datos estadísticos SPSS versión 25 para el análisis de datos. Mediante dio software se realizarán las pruebas de: alfa de Cronbach, correlación de Pearson. Una vez obtenido los resultados se procederá a la discusión y la formulación de hipótesis.

2.7. Aspectos éticos

El presente estudio no se encuentra excluido de los aspectos éticos, es por ello que se ejecutó una precisa y austera toma de información por medio de las encuestas realizadas a los estudiantes de los centros de cómputo de la UNAC con la finalidad de obtener datos totalmente verídicos y transparentes sin ningún tipo de manipulación de información.

Aportar al desarrollo regional y nacional, por consecuencia de ello se elevará el prestigio de la Universidad, todo ello gracias a la excelencia de los productos académicos. (Guía del Estudiante UCV, 2019, p. 23).

De lo citado anteriormente, la presente investigación busca poder aportar conocimientos por medio de realizar un trabajo transparente, como se detalla en la sección “Deberes del Estudiante”.

III. RESULTADOS Y DISCUSIÓN

RESULTADOS

Resultados descriptivos de la variable: Seguridad de la Información

Luego de aplicar la encuesta a los estudiantes de los centros de cómputo de la UNAC, para mayor precisión, en junio del 2019. Se obtuvieron los siguientes resultados: el 7,7% califica de nivel califica de nivel poco o nada a la Seguridad de la Información, el 61,5 % califica de nivel regular y el 30,8% califica de nivel aceptable.

Se concluye que la Seguridad de la Información posee una tendencia a ser regular en los centros de cómputo de la Universidad Nacional del Callao, 2019.

Tabla 5: Niveles de la variable Seguridad de la Información

		Frecuencia	Porcentaje
Válidos	Aceptable	4	30,8%
	Regular	8	61,5%
	Poco o nada	1	7,7%
	Total	13	100%

Nota: Información recopilada de los estudiantes del centro de cómputo de la Universidad Nacional del Callao, 2019.

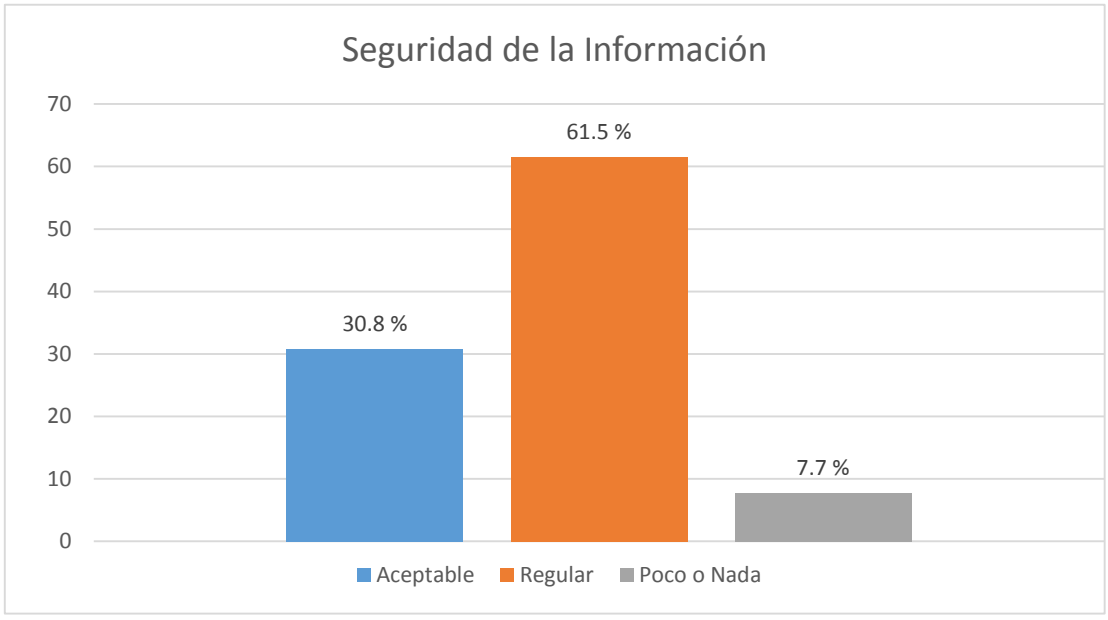


Figura 1: Niveles de la variable Seguridad de la Información

Resultados descriptivos de la variable: Gestión de Riesgos

Luego de aplicar la encuesta a los estudiantes de los centros de cómputo de la UNAC, para mayor precisión, en junio del 2019. Se obtuvieron los siguientes resultados: el 38,5% califica de nivel califica de nivel poco o nada a la Gestión de Riesgos, el 15,4 % califica de nivel regular y el 46,1% califica de nivel aceptable.

Se concluye que la Gestión de Riesgos posee una tendencia a ser aceptable en los centros de cómputo de la Universidad Nacional del Callao, 2019.

Tabla 6: Niveles de la variable Gestión de Riesgos

		Frecuencia	Porcentaje
Válidos	Aceptable	6	46,1%
	Regular	2	15,4%
	Poco o nada	5	38.5%
	Total	13	100%

Nota: Información recopilada de los estudiantes del centro de cómputo de la Universidad Nacional del Callao, 2019.

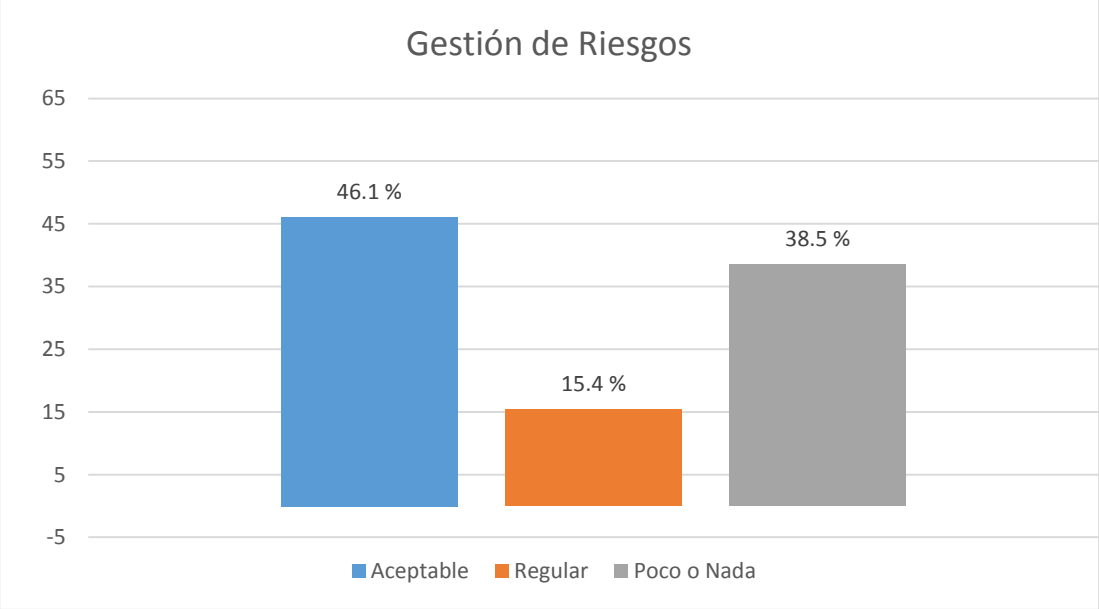


Figura 2: Niveles de la variable Gestión de Riesgos

Contrastación de hipótesis

Para el análisis de información, se empleó el siguiente sistema de hipótesis:

Ho = No existe relación significativa entre las variables

Ha = Existe una relación significativa entre las variables

95% nivel de confianza

0.05 α nivel de significancia

Prueba de Hipótesis general

Ho: No existe relación significativa entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019.

Ha: Existe relación significativa entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019.

Como se muestra en la siguiente tabla, la comprobación de hipótesis general, la seguridad de la información no está relacionado con la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019; según la correlación de Pearson de 0,055, con una significancia estadística de p = 0,859 (p > 0,05). Es por ello, que se acepta la hipótesis nula y se rechaza la hipótesis del investigador previamente planteada.

Como conclusión se obtiene que: No existe relación significativa entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019, con rho de Pearson de 0,055 y una significancia de 0,859.

Tabla 7: Prueba de hipótesis general

			Seguridad de la Información	Gestión de Riesgos
Rho de Pearson	Seguridad de la Información	Coeficiente de correlación	1	,055
		Sig. (bilateral)		,859
		N	13	13
	Gestión de Riesgos	Coeficiente de correlación	,055	1
		Sig. (bilateral)	,859	.
		N	13	13

Nota: No existe relación significativa entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019

Hipótesis específicas

Prueba de Hipótesis específica 1

Ho: No existe relación significativa entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo de los recursos del centro de cómputo de la Universidad Nacional del Callao, 2019

Ha: Existe relación significativa entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo de los recursos del centro de cómputo de la Universidad Nacional del Callao, 2019

Como se observa en la siguiente tabla (Tabla 8), la comprobación de la hipótesis específica 1, la seguridad de la información está relacionado de forma negativa con el tiempo medio de atención por agente de monitoreo de los recursos en los centros de cómputo de la Universidad Nacional del Callao, 2019; según la correlación de Pearson de -0,298, con una significancia estadística de p = 0,323 (p > 0,05). Por ende, se rechaza la hipótesis nula y se acepta la hipótesis del investigador adicionando que la relación existente es inversa.

Dada la información, se concluye que: Existe relación negativa débil entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo en los centros de cómputo de la Universidad Nacional del Callao, 2019, con rho de Pearson de -0,298 y un valor de significancia de 0,323.

Tabla 8: Prueba de hipótesis específica 1

			Seguridad de la Información	Tiempo medio de atención por agente de monitoreo de los recursos
Rho de Pearson	Seguridad de la Información	Coeficiente de correlación	1	-,298
		Sig. (bilateral)		,323
		N	13	13
	Tiempo medio de atención por agente de monitoreo de los recursos	Coeficiente de correlación	-,298	1
		Sig. (bilateral)	,323	.
		N	13	13

Nota: Existe relación negativa débil entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo de los recursos del centro de cómputo de la Universidad Nacional del Callao, 2019

Prueba de Hipótesis específica 2

Ho: No existe relación significativa entre la seguridad de la información y el nivel de calidad de gastos de los recursos del centro de cómputo de la Universidad Nacional del Callao, 2019

Ha: Existe relación significativa entre la seguridad de la información y el nivel de calidad de gastos de los recursos del centro de cómputo de la Universidad Nacional del Callao, 2019

Como se observa en la siguiente tabla, la prueba de la hipótesis específica 2, la seguridad de la información está relacionado o vinculada de forma positiva débil con el nivel de calidad de gastos de los recursos en los centros de cómputo de la Universidad Nacional del Callao, 2019; según la correlación de Pearson de 0,363, con una significancia estadística de p = 0,223 (p > 0,05). Es por ello, que se rechaza la hipótesis del investigador y se acepta la hipótesis nula.

Según los resultados obtenidos del instrumento de recolección de datos, se llega a la conclusión de que: Existe relación positiva débil entre la seguridad de la información y el nivel de calidad de gastos de los recursos del centro de cómputo de la Universidad Nacional del Callao, 2019, con rho de Pearson de 0,363 y un valor de significancia de 0,223.

Tabla 9: Prueba de hipótesis específica 2

			Seguridad de la Información	Nivel de calidad de gastos de los recursos
Rho de Pearson	Seguridad de la Información	Coeficiente de correlación	1	,363
		Sig. (bilateral)		,223
		N	13	13
	Nivel de calidad de gastos de los recursos	Coeficiente de correlación	,363	1
		Sig. (bilateral)	,223	.
		N	13	13

Nota: Existe relación positiva débil entre la seguridad de la información y el nivel de calidad de gastos de los recursos del centro de cómputo de la Universidad Nacional del Callao, 2019

Prueba de Hipótesis específica 3

Ho: No existe relación significativa entre la seguridad de la información y la tasa de usuarios capacitados en cultura informática del centro de cómputo de la Universidad Nacional del Callao, 2019

Ha: Existe relación significativa entre la seguridad de la información y la tasa de usuarios capacitados en cultura informática del centro de cómputo de la Universidad Nacional del Callao, 2019

Como se puede observar en la siguiente tabla, la prueba de la hipótesis específica 3, la seguridad de la información no está relacionado con la tasa de usuarios capacitados en cultura informática de los recursos en los centros de cómputo de la Universidad Nacional del Callao, 2019; según la correlación de Pearson de 0,051, con una significancia estadística de p = 0,869 (p > 0,05). Por ende, se rechaza la hipótesis del investigador y se acepta la hipótesis nula.

Dada la información, se llega a la conclusión de que: No existe relación significativa entre la seguridad de la información y la tasa de usuarios capacitados en cultura informática del centro de cómputo de la Universidad Nacional del Callao, 2019, con rho de Pearson de 0,051 y un valor de significancia de 0,869.

Tabla 10: Prueba de hipótesis específica 3

			Seguridad de la Información	Tasa de usuarios capacitados en cultura informática
Rho de Pearson	Seguridad de la Información	Coeficiente de correlación	1	,051
		Sig. (bilateral)		,869
		N	13	13
	Tasa de usuarios capacitados en cultura informática	Coeficiente de correlación	,051	1
		Sig. (bilateral)	,869	.
		N	13	13

Nota: No existe relación significativa entre la seguridad de la información y la tasa de usuarios capacitados en cultura informática del centro de cómputo de la Universidad Nacional del Callao, 2019

DISCUSIÓN

La presente investigación se desarrolló con el diseño no experimental, transversal correlacional, de tipo básica y con un enfoque cualitativo sobre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019. Después de un análisis, y su posterior interpretación de los resultados de la contrastación de la hipótesis, se manifiesta las siguientes afirmaciones:

Con respecto a la hipótesis general: se constató que la seguridad de la información no está relacionada con la gestión de riesgos en los laboratorios de cómputo de la Universidad Nacional del Callao, 2019; conforme la correlación de Pearson que es de 0,055, representado este resultado como bajo con un valor de significancia estadística de $p = 0,859$ ($p > 0,05$). A diferencia del autor Jorge Calderón como sustento en sus tesis previamente mencionada y referenciada, realizada en la casa de estudios Universidad César Vallejo, para optar por un grado de Maestría. La población fue de 106 trabajadores de la DIGERE del Ministerio de Educación a diferencia del presente estudio, donde la población fue de 13 estudiantes del centro de cómputo de la UNAC. Su instrumento de medición utilizado fue el cuestionario, de la misma manera que en la presente investigación; Calderón a diferencia de esta investigación, comprobó que existe relación altamente significativa entre la seguridad de la información y la gestión de riegos en la DIGERE del Ministerio de Educación, al alcanzar un valor de correlación rho Spearman de 0,886.

Conforme lo establecido en la introducción del presente estudio, se detalló que la protección de la información tiene un alto grado de relevancia para todas las organizaciones o empresas (sea cual sea el rubro), esto coincide con la tesis de Zacarias (2017) desarrollado en su trabajo: "Modelo de Seguridad de la Información basado en la ISO/IEC 27001:2013 para mitigar los riesgos de los activos de la información en la Central De Operaciones Policiales de la Región Policial de Junín", realizada en la Universidad Continental. Dicho autor utilizo una población de 32 trabajadores llegando a la conclusión de que la cultura organizacional con respecto a la seguridad de la información se incrementó en un 75%, siendo este último un saldo muy favorable en la organización de Junín.

A comparación de Vilca (2017) quien presento su tesis titulada: “Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de Lima”, la cual se desarrolló en la Universidad de Huánuco. Utilizó una muestra de 33 personas a comparación de la presente investigación, en la cual se utilizó a 20 estudiantes. Vilca llego a la conclusión de que el 9,1% de la población carecía del conocimiento óptimo para hacer uso de las tecnologías de la información, luego de implementar un SGSI dicho porcentaje aumento al 90%, esto debido a las capacitaciones y a la creación de un documento donde se detallaba toda la información posible respecto al manejo de este. Existe una similitud debido a que en la hipótesis específica tres del presente estudio, se puede observar la carencia de relación entre la protección de la información y la tasa de usuarios capacitados en cultura informática del centro de cómputo de la UNAC.

Esto conlleva a comprometernos todos a realizar el correcto manejo de las Tecnologías de la Información, esto porque nos serán de mucha ayuda tanto en nuestra vida ambiente laboral como en la vida profesional. Esto se puede contrastar con la investigación de Cruz y Fukusaki (2017): “Diseño e Implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica Medcam Perú SAC”, realizada en la Universidad Privada San Martín de Porres; llegan a una conclusión global de que consideran de gran importancia que los empleados de la clínica estén informados en la relevancia que conlleva la protección de la data privada de la empresa, frente a las posibles amenazas y riesgos.

IV. CONCLUSIONES

Primera: En conclusión, no existe ningún tipo de relación significativa entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019; conforme la correlación obtenida de Pearson de 0,055, con un valor de significancia estadística de p = 0,859.

Segunda: Del mismo modo, se confirma la existencia de una relación negativa débil entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo en los centros de cómputo de la Universidad Nacional del Callao, 2019, con rho de Pearson de -0,298 y un valor de significancia de 0,323.

Tercera: También se llega a la afirmación de que, está presente una relación positiva débil entre la seguridad de la información y el nivel de calidad de gastos de los recursos del centro de cómputo de la Universidad Nacional del Callao, 2019, con rho de Pearson de 0,363 y un valor de significancia de 0,223.

Cuarta: Seguidamente se concluye gracias a la presente investigación la carencia de relación significativa entre la seguridad de la información y la tasa de usuarios capacitados en cultura informática del centro de cómputo de la Universidad Nacional del Callao, 2019, con rho de Pearson de 0,051 y una significancia de 0,869.

Quinta: Del mismo modo, se concluye que la Seguridad de la Información posee una tendencia a ser regular en los laboratorios de cómputo de la Universidad Nacional del Callao, 2019; esto debido a los siguientes resultados: el 7,7% califica de nivel califica de nivel poco o nada a la Seguridad de la Información, el 61,5 % califica de nivel regular y el 30,8% califica de nivel aceptable.

Sexta: Una vez recolectado la información, se concluye que la Gestión de Riesgos posee una tendencia a ser aceptable en los centros o laboratorios de cómputo de la Universidad Nacional del Callao, 2019; obtenido de los siguientes resultados: el 38,5% califica de nivel califica de nivel poco o nada a la Gestión de Riesgos, el 15,4 % califica de nivel regular y el 46,1% califica de nivel aceptable

Séptima: Al realizar la entrevista y recopilar información mediante las encuestas se demostró el desconocimiento de las inversiones que realiza la universidad en el centro de cómputo, destacando que algunos de los encuestados manifiestan no conocer los medios necesarios para obtener dicha información siendo este de carácter público.

Octava: Se evidencio la carencia de conocimiento con respecto a la seguridad de la información en la mayoría de los encuestados incrementado el riesgo al que se encontraría expuesto una persona con nociones básicas de seguridad y de cómo actuar en caso de incidentes o emergencias.

V. RECOMENDACIONES

Primera: Organizar capacitaciones, talleres o seminarios que permitan ampliar el conocimiento con respecto al correcto manejo de las tecnologías de la información, tanto a estudiantes, encargados como a catedráticos de la casa de estudio de la Universidad Nacional del Callao.

Segunda: Adicionar avisos informando sobre el estado de la información de los usuarios de los centros de cómputo de la Universidad Nacional del Callao, sean los motivos por ejemplo: intento de acceso a su cuenta de intranet, actualización de datos u otras notificaciones.

Tercera: Buscar un medio de difusión más efectivo para la publicación del detalle de inversión con respectos a los centros de cómputo, ya sea página web, redes sociales, periódico institucional.

Cuarta: Invertir en infraestructura tecnológica, tanto en computadoras, dispositivos de red (router, switch, access point), para un mejor desarrollo de sesiones tanto de teoría como de prácticas en los ambientes del centro de cómputo de la UNAC.

Quinta: Buscar implementar un marco de referencia que tenga buenas prácticas con respecto a la Seguridad de la información para obtener una certificación, de esta manera se asegura el cumplimiento de las 3 dimensiones de la seguridad con respecto a la información (Disponibilidad, Integridad y Confidencialidad).

Sexta: La universidad debe dar a conocer los distintos medios por el que es posible informar, reportar cualquier tipo de incidencia, solicitud o queja así la universidad podría actuar de forma adecuada en su gestión.

Séptima: Buscar nuevas alternativas de solución para los distintos problemas encontrados para su posterior aplicación, de esta forma se crearía un ciclo de mejoras continuas que causaría el crecimiento a nivel de seguridad (Disponibilidad, Integridad y Confidencialidad) e incluso comodidad.

Octava: Para finalizar con las recomendaciones, se sugiere realizar nuevos estudios, utilizando también el cuestionario como medio para la obtención de información para

detectar cual fue la causa de la no existencia de relación entre seguridad de la información y la gestión de riesgos en los centros de cómputo de la UNAC, 2019.

REFERENCIAS

AGURTO, Manuel. Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C. Talara, basado en la norma ISO 27001. Tesis (Título Profesional de Ingeniero de Sistemas). Piura: Universidad César Vallejo, 2017.
Disponible en:
http://repositorio.ucv.edu.pe/bitstream/handle/UCV/11917/agurto_cm.pdf?sequence=1&isAllowed=y

ARARAT, Johanna. Diseño de un SGSI basado en la norma 27001 para la empresa MA Peñalosa Cía. S.A.S. sede principal Cúcuta. Tesis (Especialista en Seguridad Informática). San José de Cúcuta: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería, 2018.
Disponible en:
https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/21259/1/27604094.pdf

CHANGOLUISA, Wilson. Optimización del proceso de alta y baja de usuarios a través de la implementación de gestión de seguridad de la información, basado en la norma ISO 27001:2013 en una empresa de consultoría para la industria petrolera. Tesis (Título de Magister en Administración de empresas con mención en gerencia de la calidad y productividad). Quito: Pontifica Universidad Católica del Ecuador-Matriz, 2017.
Disponible en:
http://repositorio.puce.edu.ec/bitstream/handle/22000/13999/Proyecto%20Grado%20PUCE%20Wilson%20Changoluisa.pdf?sequence=1&isAllowed=y

CRUZ, Miguel y FUKUSAKI, Senyi. Diseño e Implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica Medcam Perú SAC. Tesis (Título Profesional de Ingeniero de Computación y Sistemas). Lima: Universidad de San Martín de Porres, Facultad de Ingeniería y Arquitectura, 2017.
Disponible en:
http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/3369/1/cruz_fukusaki.pdf

KIESEL, Carola. Guía para la gestión del riesgo en proyectos de desarrollo rural. San José: CEPREDENAC, 2001. [Consultado 30 de mayo de 2019].
ISBN: 9968-9918-8-0

MAURERIA, Daniel. Norma ISO/IEC 27001 aplicada a una carrera universitaria. Tesis (Título de Ingeniero Civil Informático). Santiago de Chile, Chile: Universidad Andrés Bello, 2017.
Disponible en:
http://repositorio.unab.cl/xmlui/bitstream/handle/ria/3720/a118929_Maureira_D_Norma_ISO_IEC_27001_aplicada_2017_Tesis.pdf?sequence=1&isAllowed=y

MENESES, Alexander, RAMIREZ, Erney, MERCHAN, Maria y SUAREZ, Yaditza. Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, para los procesos soportados por el área de sistemas en la cámara de comercio de Aguachica. Trabajo de Grado (Especialista en Auditoria de Sistemas). Ocaña: Universidad Francisco de Paula Santander Ocaña, 2016.
Disponible en:
http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/1434/1/29635.pdf

CALDERÓN, Jorge. Seguridad de la Información y la Gestión de Riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018. Tesis (Maestro en ingeniería de sistemas con mención en tecnologías de la información). Lima, Perú: Universidad Privada Cesar Vallejo, 2019
Disponible en:
http://repositorio.ucv.edu.pe/bitstream/handle/UCV/30014/Calder%C3%B3n_SJA.pdf?sequence=1&isAllowed=y

NIEVES, Arlenys. Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013. Trabajo de Grado (Especialista en Seguridad de la Información). Colombia: Institución Universitaria Politécnico Grancolombiano, Facultad de Ingeniería y Ciencias Básicas, 2017.
Disponible en:

http://repository.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y

OCHOA, Andrea. Sistema web de gestión de seguridad de la información asistida por computadora basada en el estándar ISO 27001 en la Universidad Nacional José María Arguedas. Tesis (Título Profesional de Ingeniero de Sistemas). Andahuaylas: Universidad Nacional José María Arguedas, Facultad de Ingeniería, 2017.
Disponible en:
http://repositorio.unajma.edu.pe/bitstream/handle/123456789/291/Andrea_Tesis_Bachiller_2017.pdf?sequence=1&isAllowed=y

TARRILLO, Esther. Influencia de la Gestión de Riesgo en la Seguridad de Activos de Información de la Zona Registral III Sede Moyobamba, 2015. Tesis (Maestría en Gestión Pública). Tarapoto, Perú: Universidad Privada Cesar Vallejo, 2016.
Disponible en:
http://repositorio.ucv.edu.pe/bitstream/handle/UCV/1286/tarrillo_se.pdf?sequence=1&isAllowed=y

VILCA, Ehytel. Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de la Lima. Tesis (Título Profesional de Ingeniero de Sistemas e Informática). Huánuco: Universidad de Huánuco, Facultad de Ingeniería, 2017.
Disponible en:
http://repositorio.udh.edu.pe/bitstream/handle/123456789/809/T_047_43087253_T.pdf?sequence=1&isAllowed=y

ZACARIAS, Jean. Modelo de seguridad de la información basado en la ISO/IEC 27001:2013 para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín. Tesis (Título Profesional de Ingeniero de Sistemas e Informática). Huancayo: Universidad Continental, Facultad de Ingeniería, 2017.

Disponible en:
https://repositorio.continental.edu.pe/bitstream/continental/4105/3/INV_FIN_103_TE_Zacarias_Villafranca_2017.pdf

Instituto Tecnológico y de Estudios Superiores de Occidente. La era digital. Nuevos desafíos educativos. *Revista Electrónica Sinéctica* [en línea]. Núm. 40, Enero-Junio, 2013. [Fecha de consulta: 21 de abril de 2019].
Disponible en: http://www.redalyc.org/articulo.oa?id=99827467010
ISSN: 1665-109X

REGUERA, Alejandra. Metodología de la Investigación lingüística. Córdova – Argentina: Editorial Brujas, 2008. [Consultado 14 de mayo de 2019].
ISBN: 978-987-591-117-8

ABRIL, Hugo. Técnicas e instrumentos de investigación. 2008. 19 pp. [Consultado 16 de junio de 2019]

HERNÁNDEZ, Roberto, FERNÁNDEZ, Carlos, BAPTISTA, Pilar. Metodología de la Investigación. 6ta. ed. México: McGraw-Hill, 2013. 565 pp.
ISBN: 978-1-4562-2396-0

LANDEAU, Rebeca. Elaboración de trabajos de investigación. Venezuela: Editorial Alfa, 2007. 187 pp. [Consultado 25 de junio de 2019]
ISBN: 980-354-214-1

LÓPEZ, Luisa, MONTENEGRO, María, TAPIA, Ruth. La investigación, eje fundamental en la enseñanza del derecho. Guía Práctica. Bogotá: Universidad Cooperativa de Colombia, 2006. [Consultado 14 de mayo de 2019].
ISBN: 958-8325-15-6

MUÑOZ, David. Administración de Operaciones, Enfoque de administración de procesos de negocios. México: CENCAGE Learning, 2009. 509. [Consultado 06 de junio de 2019]
ISBN: 978-970-830-074-2

SERRAHIMA, Joaquim. La amenaza digital. Barcelona: Editorial Profit, 2010. 148 pp. ISBN: 978-8492-9569-44

KRONISCH, Zach. Operational Security Erodes in Social Media Age. *National Defense Industrial Association*, Vol. 103 (787):9, Junio 2019.
ISSN: 0092-1491

QUISPITUPAC, Cynthia y MATEO, Silvia. Elaboración de una herramienta para la toma de decisiones en gestión del talento para líderes. Tesis (Magister en Administración de Empresas). Lima: UPC, 2014.

ANEXOS

Anexo a. Matriz de Consistencia

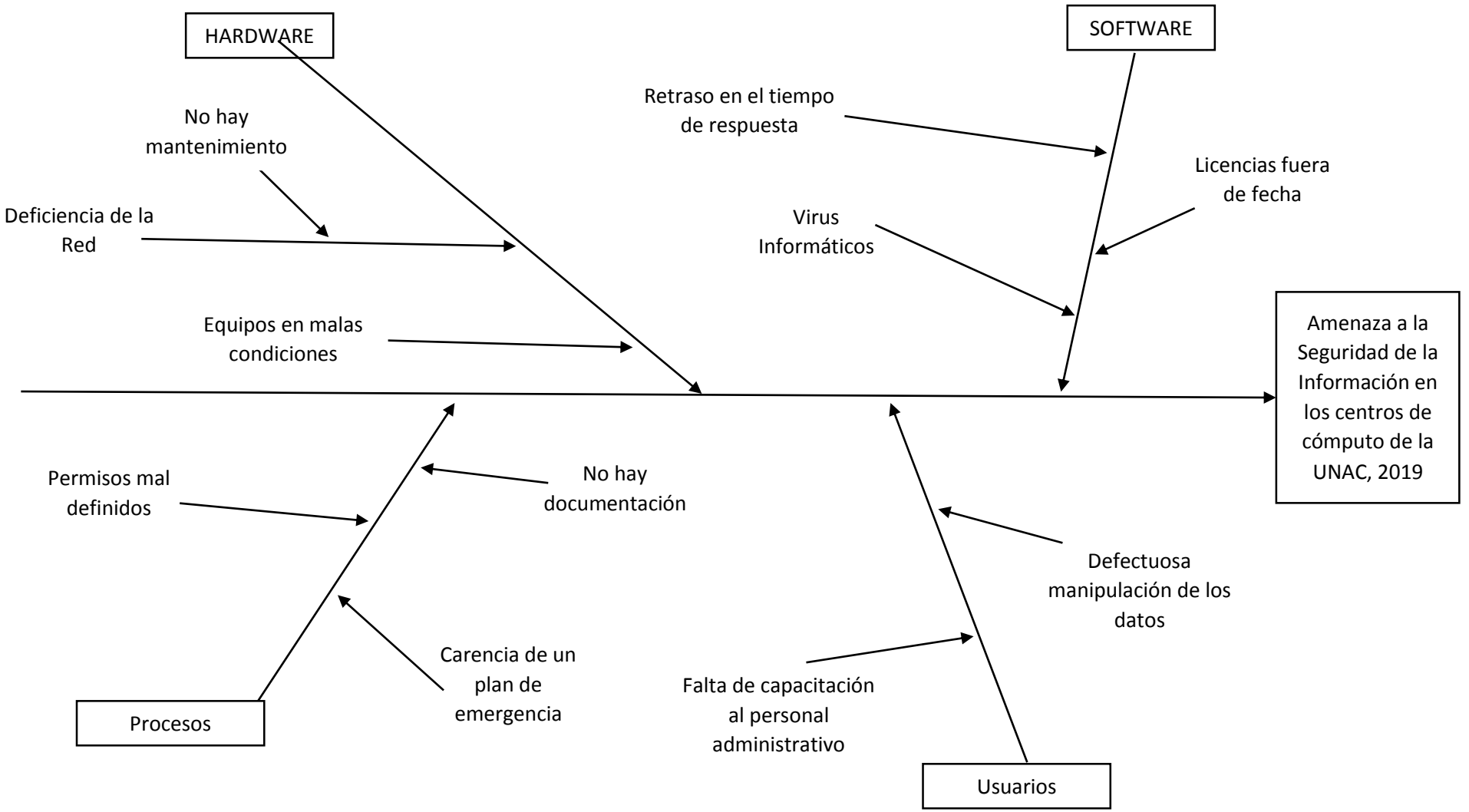
Título: La Seguridad de la Información y la Gestión de Riesgos en los centros de cómputo de la Universidad Nacional del Callao
Autor: Ramirez Rodriguez, Jorge Rodriguez Romero, Alejandro

Problema General	**Objetivo General**	**Hipótesis General**	**Variables**	**Dimensiones**	**Indicadores**	**Ítems**	**Método, de investigación**
¿Qué relación existe entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019?	Determinar la relación entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019.	Existe relación significativa entre la seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019.	V1: Seguridad de la Información	D1: Confidencialidad	I1: Efectividad del control de acceso	1 – 3	Tipo: Básica Diseño: No experimental Nivel: Correlacional Enfoque: Cualitativo
				D2: Integridad	I1: Tasa de perdida de información	4 – 6	
				D3: Disponibilidad	I1: Gestión de contingencias	7 – 9	
Problema Específico	**Objetivo Específico**	**Hipótesis Específico**	V2: Gestión de Riesgos	D1: Recursos	I1: Tiempo medio de atención por agente de monitoreo	10 – 12	
PE1: ¿Qué relación existe entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo de recursos en los centros de cómputo de la Universidad Nacional del Callao, 2019?	OE1: Determinar la relación que existe entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo de recursos del cómputo de la Universidad Nacional del Callao.	HE1: Existe relación significativa entre la seguridad de la información y el tiempo medio de atención por agente de monitoreo de los recursos del centro de cómputo de la Universidad Nacional del Callao, 2019.			I2: Nivel de calidad de gastos	13 – 15	
PE2: ¿Qué relación existe entre la seguridad de la información y el nivel de calidad de gastos de los recursos en los centros de cómputo de la Universidad Nacional del Callao, 2019?	OE2: Determinar la relación que existe entre la seguridad de la información y el nivel de calidad de gastos de los recursos del centro de cómputo de la Universidad Nacional del Callao.	HE2: Existe relación significativa entre la seguridad de la información y el nivel de calidad de gastos de los recursos del centro de cómputo de la Universidad Nacional del Callao, 2019.		D2: Cultura Informática	I1: Tasa de usuarios capacitados	16 – 18	**Población, muestra y muestreo** Población: 20 Muestra: 13 Muestreo: No probabilístico
PE3: ¿Qué relación existe entre la seguridad de la información y la tasa de usuarios capacitados en cultura informática en los centros de cómputo de la Universidad Nacional del Callao, 2019?	OE3: Determinar la relación que existe entre la seguridad de la información y la tasa de usuarios capacitados en cultura informática del centro de cómputo de la Universidad Nacional del Callao.	HE3: Existe relación significativa entre la seguridad de la información y la tasa de usuarios capacitados en cultura informática del centro de cómputo de la Universidad Nacional del Callao, 2019.					

Anexo b. Operacionalización de variables

Variables	**Descripción**	**Dimensiones**	**Descripción**	**Indicadores**	**Técnica**	**Instrumento**	**Escala**	**Ítems**
VI: Seguridad de la Información	"La seguridad de la información engloba todo lo relacionado con políticas para la gestión de la seguridad de la información" (Cruz y Fukusaki, 2017, p. 19)	D1: Confidencialidad	"Esta dimensión permitir acceder a la información a todo aquel que se encuentre autorizado sin ninguna excepción" (Meneses, 2012, p. 20)	I1: Efectividad del control de acceso	Encuesta	Cuestionario	1) Nunca 2) Casi Nunca 3) Algunas Veces 4) Casi siempre 5) Siempre	1 – 3
		D2: Integridad	"Permite que la información sea correcta y que no haya sido alterada por usuarios, entidades o procesos no autorizados" (Meneses, 2012, p. 21)	I1: Tasa de perdida de información				4 – 6
		D3: Disponibilidad	"Es la posibilidad de poder acceder a la información y sistemas cuando sea requerido" (Mosquera, 2017, p. 30)	I1: Gestión de contingencias				7 – 9
V2: Gestión de Riesgos	"Es el proceso de la identificación de las posibles amenazas, y elaborar un plan que implique controlar estos riesgos" (Kiesel, 2001, p. 20)	D1: Recursos	"Si no analizamos nuestro mercado como empresa, los cambios, las expectativas y la competencia, nuestro producto carecería de atractivo y perderíamos clientes y por tanto perderíamos mercado" (Quispitupac y Ramos, 2014, p.29)	I1: Tiempo medio de atención por agente de monitoreo				10 – 12
				I2: Nivel de calidad de gastos				13 – 15
		D2: Cultura informática	"Hace referencia a la cultura que posee la población y comunidad de la Universidad Nacional del Callao, hacia sus instalaciones y equipos que conformas el centro de cómputo, el uso y cuidado de estos" (Kendall, 2005, p. 38).	I1: Tasa de usuarios capacitados				16 – 18

Anexo c. Diagrama de Ishikawa



Anexo d. Constancia de asistencia a entrevista

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE ASISTENCIA A ENTREVISTA

Por medio de la presente se deja constancia de haber participado en la entrevista sobre los centros de cómputo de la Universidad Nacional del Callao.

Esta entrevista forma parte del trabajo de investigación para obtener el titulo de bachiller en Ingenieria de Sistemas de titulo "Seguridad De La Información Y La Gestión De Riesgos En El Centro De Cómputo De La Universidad Nacional Del Callao, 2019".

Entrevistada:
Allison Xiomara Cartolin Mendoza
DNI: 71727056

Entrevistador 1:
Jorge Luis Ramirez Rodriguez
DNI: 75200120

Entrevistador 2:
Alejandro Rodriguez Romero
DNI: 70345671

Anexo e. Matriz de Antecedentes

Antecedente	N°	Titulo	Año	País
INTERNACIONAL	**1**	Diseño de un SGSI basado en la norma 27001 para la empresa MA Peñalosa Cía. S.A.S. sede principal Cúcuta	2018	Colombia
	2	Optimización del proceso de alta y baja de usuarios a través de la implementación de gestión de seguridad de la información, basado en la norma ISO 27001:2013 en una empresa de consultoría para la industria petrolera	2017	Ecuador
	3	Norma ISO/IEC 27001 aplicada a una carrera universitaria	2017	Chile
	4	Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013	2017	Colombia
	5	Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001	2015	Ecuador

NACIONAL	**6**	Modelo de seguridad de la información basado en la ISO/IEC 27001:2013 para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín	2017	Perú
	7	Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de la Lima	2017	Perú
	8	Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C.	2017	Perú
	9	Diseño e Implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica Medcam Perú SAC.	2017	Perú
	10	Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015	2016	Perú

Anexo f. Formato de Validación

CERTIFICADO DE VALIDEZ DEL CONTENIDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DE RIESGOS EN EL CENTRO DE COMPUTO DE LA UNIVERSIDAD NACIONAL DEL CALLAO, 2019

VARIABLE: SEGURIDAD DE LA INFORMACIÓN

	Dimensiones	1.Pertinencia		2.Relevancia		3.Claridad		Sugerencias
Nº	**Confidencialidad**	SI	NO	SI	NO	SI	NO	
1	¿Han intentado acceder a su información de forma indebida?	X						
2	¿Le informa la universidad de accesos a su información sin su consentimiento?	X						
3	¿Alguna vez se ha divulgado información confidencial sobre usted o alguna persona conocida?	X						
Nº	**Integridad**	SI	NO	SI	NO	SI	NO	Sugerencias
4	¿Ha sufrido algún tipo de perdida de información?	X		X		X		
5	¿Realiza alguna copia de seguridad de su información?							Muy ambiguo mejorar
6	¿Alguna vez ha realizado el cambio de sus contraseñas?	X		X		X		

Nº	Disponibilidad	SI	NO	SI	NO	SI	NO	Sugerencias
7	¿Ante fallas en el centro de cómputo ha dejado de tener acceso a su información?	X		X		X		
8	¿Alguna vez has dejado de tener acceso al centro de cómputo por más de una hora?	X		X		X		
9	¿Has sido testigo de una acción tomada por un técnico ante un fallo?	X		X		X		

Observaciones (precisar si hay suficiencia) .....

Opinión de aplicabilidad: **Aplicable** (X) **Aplicable después de corregir** ( ) **No aplicable** ( )

Apellidos y nombres del juez validador. Dr/Mg: ..... B. Crumpa A.

Especialidad del validador: ..... Ing. Sistemas

1.Pertinencia: El ítem corresponde al concepto teórico formulado.
2.Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.
3.Claridad: No se encuentra dificultad alguna en el enunciado del ítem, es conciso, exacto y directo.

05 de 06 del 2015

.....
Firma del Experto Informante

CERTIFICADO DE VALIDEZ DEL CONTENIDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DE RIESGOS EN EL CENTRO DE COMPUTO DE LA UNIVERSIDAD NACIONAL DEL CALLAO, 2019

VARIABLE: GESTIÓN DE RIESGOS

	Dimensiones	1.Pertinencia		2.Relevancia		3.Claridad		Sugerencias
Nº	Recursos	SI	NO	SI	NO	SI	NO	
1	¿Existe algún monitoreo por parte de la UNAC hacia los equipos informáticos del centro de cómputo?	X		X		X		
2	¿Existe alguna respuesta inmediata ante alguna falla en el centro de cómputo?	X		X		X		
3	¿Has presenciado inconvenientes que no han tenido respuesta en un largo tiempo?	X		X		X		
4	¿Has sido testigo de alguna renovación en los equipos del centro de cómputo?	X		X		X		
5	¿Has sido testigo del manejo inadecuado de los recursos financieros de la UNAC para el centro de cómputo?	X		X		X		
6	¿Se detalla los gastos realizados por parte del área financiera de la UNAC para el centro de cómputo?	X		X		X		

Nº	Cultura Informática	SI	NO	SI	NO	SI	NO	Sugerencias
7	¿Cada cuánto tiempo se realizan campañas de capacitación?	X		X		X		
8	¿Alguna vez ha sufrido inconvenientes con el uso del software del centro de cómputo?							Mejorar
9	¿Alguna vez ha presenciado a algún catedrático con dificultades en el manejo de algún software (Intranet, Utilitarios, etc)?	X		X		X		

Observaciones (precisar si hay suficiencia) .....

Opinión de aplicabilidad: **Aplicable** (X) **Aplicable después de corregir ( )** **No aplicable ( )**

Apellidos y nombres del juez validador. Dr/Mg: Jim Lee Arango A.

Especialidad del validador: Ing. Sistemas

1.Pertinencia: El ítem corresponde al concepto teórico formulado.
2.Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.
3.Clarida: No se encuentra dificultad alguna en el enunciado del ítem, es conciso, exacto y directo.

..... de ..... del 20.....

.....
Firma del Experto Informante

CERTIFICADO DE VALIDEZ DEL CONTENIDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DE RIESGOS EN EL CENTRO DE COMPUTO DE LA UNIVERSIDAD NACIONAL DEL CALLAO, 2019

VARIABLE: SEGURIDAD DE LA INFORMACIÓN

	Dimensiones	1.Pertinencia		2.Relevancia		3.Claridad		Sugerencias
Nº	Confidencialidad	SI	NO	SI	NO	SI	NO	
1	¿Han intentado acceder a su información de forma indebida?	X		X		X		
2	¿Le informa la universidad de accesos a su información sin su consentimiento?	X		X		X		
3	¿Alguna vez se ha divulgado información confidencial sobre usted o alguna persona conocida?	X		X		X		
Nº	Integridad	SI	NO	SI	NO	SI	NO	Sugerencias
4	¿Ha sufrido algún tipo de perdida de información?	X		X		X		
5	¿Realiza alguna copia de seguridad de su información?	X		X		X		
6	¿Alguna vez ha realizado el cambio de sus contraseñas?	X		X		X		

Nº	Disponibilidad	SI	NO	SI	NO	SI	NO	Sugerencias
7	¿Ante fallas en el centro de cómputo ha dejado de tener acceso a su información?	X		X		X		
8	¿Alguna vez has dejado de tener acceso al centro de cómputo por más de una hora?	X		X		X		
9	¿Has sido testigo de una acción tomada por un técnico ante un fallo?	X		X		X		

Observaciones (precisar si hay suficiencia) ..... Si hay suficiencia .....

Opinión de aplicabilidad: **Aplicable (X)** **Aplicable después de corregir ( )** **No aplicable ( )**

Apellidos y nombres del juez validador. Dr/Mg: ..... Melgarejo Cavalieri Melquiades Efraín .....

Especialidad del validador: ..... Ing. Sistemas .....

1.Pertinencia: El ítem corresponde al concepto teórico formulado.
2.Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.
3.Claridad: No se encuentra dificultad alguna en el enunciado del ítem, es conciso, exacto y directo.

..... 05 de ..... 06 del 20..19...

.....

Firma del Experto Informante

CERTIFICADO DE VALIDEZ DEL CONTENIDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DE RIESGOS EN EL CENTRO DE COMPUTO DE LA UNIVERSIDAD NACIONAL DEL CALLAO, 2019

VARIABLE: GESTIÓN DE RIESGOS

	Dimensiones	1.Pertinencia		2.Relevancia		3.Claridad		Sugerencias
Nº	Recursos	SI	NO	SI	NO	SI	NO	
1	¿Existe algún monitoreo por parte de la UNAC hacia los equipos informáticos del centro de cómputo?	X		X		X		
2	¿Existe alguna respuesta inmediata ante alguna falla en el centro de cómputo?	X		X		X		
3	¿Has presenciado inconvenientes que no han tenido respuesta en un largo tiempo?	X		X		X		
4	¿Has sido testigo de alguna renovación en los equipos del centro de cómputo?	X		X		X		
5	¿Has sido testigo del manejo inadecuado de los recursos financieros de la UNAC para el centro de cómputo?	X		X		X		
6	¿Se detalla los gastos realizados por parte del área financiera de la UNAC para el centro de cómputo?	X		X		X		

Nº	Cultura Informática	SI	NO	SI	NO	SI	NO	Sugerencias
7	¿Cada cuánto tiempo se realizan campañas de capacitación?	X		X		X		
8	¿Alguna vez ha sufrido inconvenientes con el uso del software del centro de cómputo?	X		X		X		
9	¿Alguna vez ha presenciado a algún catedrático con dificultades en el manejo de algún software (Intranet, Utilitarios, etc)?	X		X		X		

Observaciones (precisar si hay suficiencia) ..... Si hay suficiencia .....

Opinión de aplicabilidad: **Aplicable (X)** **Aplicable después de corregir ( )** **No aplicable ( )**

Apellidos y nombres del juez validador. Dr/Mg: ..... Márquez Carrasco Alejandro Efraín .....

Especialidad del validador: ..... Ing. Sistemas .....

1.Pertinencia: El ítem corresponde al concepto teórico formulado.
2.Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.
3.Clarida: No se encuentra dificultad alguna en el enunciado del ítem, es conciso, exacto y directo.

05 de 06 del 20 21

Firma del Experto Informante

CERTIFICADO DE VALIDEZ DEL CONTENIDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DE RIESGOS EN EL CENTRO DE CÓMPUTO DE LA UNIVERSIDAD NACIONAL DEL CALLAO, 2019

VARIABLE: SEGURIDAD DE LA INFORMACIÓN

	Dimensiones	1.Pertinencia		2.Relevancia		3.Claridad		Sugerencias
Nº	Confidencialidad	SI	NO	SI	NO	SI	NO	
1	¿Alguna vez han intentado acceder a su información de forma indebida?	X		X		X		
2	¿Alguna vez la universidad le ha informado de accesos a su información sin su consentimiento?	X		X		X		
3	¿Alguna vez se ha divulgado información confidencial sobre usted o alguna persona conocida?	X		X		X		
Nº	Integridad	SI	NO	SI	NO	SI	NO	Sugerencias
4	¿Alguna vez ha sufrido algún tipo de perdida de información?	X		X		X		
5	¿Alguna vez ha realizado alguna copia de seguridad de su información?	X		X		X		

6	¿Alguna vez ha realizado el cambio de sus contraseñas?	X		X		X		
Nº	**Disponibilidad**	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	**Sugerencias**
7	¿Ante fallas en el centro de cómputo ha dejado de tener acceso a su información?	X		X		X		
8	¿Alguna vez ha dejado de tener acceso al centro de cómputo por más de una hora?	X		X		X		
9	¿Alguna vez ha sido testigo de una acción tomada por un técnico ante un fallo?	X		X		X		

Observaciones (precisar si hay suficiencia) ..Hay suficiencia.....

Opinión de aplicabilidad: **Aplicable (X)** **Aplicable después de corregir ( )** **No aplicable ( )**

Apellidos y nombres del juez validador. Dr/Mg: ..Avile López, Bernardo Patricio.....

Especialidad del validador: ..Mg. Administración Ingº de Sistemas.....

1.Pertinencia: El ítem corresponde al concepto teórico formulado.
2.Relevancia: El ítem es apropiado para representar al componente o dimensión especifica del constructo.
3.Clarida: No se encuentra dificultad alguna en el enunciado del ítem, es conciso, exacto y directo.

..... de ..... del 20.....

Firma del Experto Informante

CERTIFICADO DE VALIDEZ DEL CONTENIDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DE RIESGOS EN EL CENTRO DE CÓMPUTO DE LA UNIVERSIDAD NACIONAL DEL CALLAO, 2019

VARIABLE: GESTIÓN DE RIESGOS

	Dimensiones	1.Pertinencia		2.Relevancia		3.Claridad		Sugerencias
Nº	Recursos	SI	NO	SI	NO	SI	NO	
1	¿Existe algún monitoreo por parte de la UNAC hacia los equipos informáticos del centro de cómputo?	X		X		X		
2	¿Existe alguna respuesta inmediata ante alguna falla en el centro de cómputo?	X		X		X		
3	¿Ha presenciado inconvenientes que no han tenido respuesta en un largo tiempo?	X		X		X		
4	¿Ha sido testigo de alguna renovación en los equipos del centro de cómputo?	X		X		X		
5	¿Ha sido testigo del manejo inadecuado de los recursos financieros de la UNAC para el centro de cómputo?	X		X		X		
6	¿Se detalla los gastos realizados por parte del área financiera de la UNAC para el centro de cómputo?	X		X		X		

Nº	Cultura Informática	SI	NO	SI	NO	SI	NO	Sugerencias
7	¿Cada cuánto tiempo se realizan campañas de capacitación?	X		X		X		
8	¿Alguna vez ha sufrido inconvenientes con el uso del software del centro de cómputo?	X		X		X		
9	¿Alguna vez ha presenciado a algún catedrático con dificultades en el manejo de algún software (Intranet, Utilitarios, etc)?	X		X		X		

Observaciones (precisar si hay suficiencia) ...HAY SUFICIENCIA.....

Opinión de aplicabilidad: **Aplicable (x)** **Aplicable después de corregir ( )** **No aplicable ( )**

Apellidos y nombres del juez validador. Dr(Mg): AVILA LÓPEZ, BERNARDO PATRICIO

Especialidad del validador: ...ING. DE SISTEMAS, MG. ADMINISTRACIÓN.....

1.Pertinencia: El ítem corresponde al concepto teórico formulado.
2.Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.
3.Claridad: No se encuentra dificultad alguna en el enunciado del ítem, es conciso, exacto y directo.

..... de ..... del 20.....

Firma del Experto Informante

Anexo g. Matriz de datos

	V1. Seguridad de la Información								
	Confidencialidad			Integridad			Disponibilidad		
Nro.	P1	P2	P3	P4	P5	P6	P7	P8	P9
1	2	1	1	1	1	2	2	1	3
2	2	1	1	1	2	3	3	1	1
3	1	1	1	1	1	1	3	5	4
4	1	1	1	2	2	2	2	1	4
5	3	3	2	2	3	3	4	3	3
6	3	3	4	3	3	4	3	4	3
7	3	1	1	1	1	4	3	2	4
8	3	4	3	1	3	3	1	1	1
9	4	2	3	4	2	3	3	2	3
10	2	1	1	2	3	1	3	3	2
11	1	1	1	1	3	1	2	3	2
12	1	2	1	2	1	1	3	3	2
13	3	2	2	2	2	4	4	4	3

	V2. Gestión de Riesgos								
	Recursos						Cultura Informática		
Nro.	P10	P11	P12	P13	P14	P15	P16	P17	P18
1	3	4	3	1	1	1	3	2	2
2	3	3	2	1	2	2	2	2	3
3	3	4	1	1	1	1	3	3	1
4	5	5	5	3	3	3	1	3	2
5	3	4	3	3	4	1	1	3	2
6	2	2	2	2	2	2	2	2	2
7	4	5	3	4	3	2	2	4	2
8	4	3	2	4	3	2	4	4	3
9	3	2	3	3	3	3	3	4	3
10	3	4	2	1	2	3	3	2	3
11	2	3	2	2	2	2	3	2	2
12	4	3	2	4	3	2	4	4	3
13	3	3	3	3	3	3	3	4	3

Anexo h.

Instrumento de recolección de datos

ENCUESTA

Para medir la relación entre la Seguridad de la Información y la Gestión de Riesgos dirigida a los estudiantes del centro de cómputo de la Universidad Nacional del Callao.

DATOS GENERALES:

Edad: [ ]

Sexo: Femenino [ ] Masculino [ ]

Se ha diseñado el presente cuestionario con el objeto de tener un buen procedimiento de medición sobre la Seguridad de la Información, por lo que necesitamos de su colaboración. Marcar con una equis (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda:

1) Nunca

2) Casi Nunca

3) Algunas Veces

4) Casi siempre

5) Siempre

	DIMENSIONES	**ESCALA**				
		1	**2**	**3**	**4**	**5**
Ítem	**Confidencialidad**					
1	¿Alguna vez han intentado acceder a su información de forma indebida?					
2	¿Alguna vez la universidad le ha informado de accesos a su información sin su consentimiento?					

3	¿Alguna vez se ha divulgado información confidencial sobre usted o alguna persona conocida?					
	Integridad					
4	¿Alguna vez ha sufrido algún tipo de perdida de información?					
5	¿Alguna vez ha realizado alguna copia de seguridad de su información?					
6	¿Alguna vez ha realizado el cambio de sus contraseñas?					

	DIMENSIONES	**ESCALA**				
		1	**2**	**3**	**4**	**5**
Ítem	**Disponibilidad**					
7	¿Ante fallas en el centro de cómputo ha dejado de tener acceso a su información?					
8	¿Alguna vez ha dejado de tener acceso al centro de cómputo por más de una hora?					
9	¿Alguna vez ha sido testigo de una acción tomada por un técnico ante un fallo?					

Instrumento de recolección de datos

ENCUESTA

Para medir la relación entre la Seguridad de la Información y la Gestión de Riesgos dirigida a los estudiantes del centro de cómputo de la Universidad Nacional del Callao.

DATOS GENERALES:

Edad: [ ]

Sexo: Femenino [ ] Masculino [ ]

Se ha diseñado el presente cuestionario con el objeto de tener un buen procedimiento de medición sobre la Gestión de Riesgos, por lo que necesitamos de su colaboración. Marcar con una equis (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda:

1) Nunca

2) Casi Nunca

3) Algunas Veces

4) Casi siempre

5) Siempre

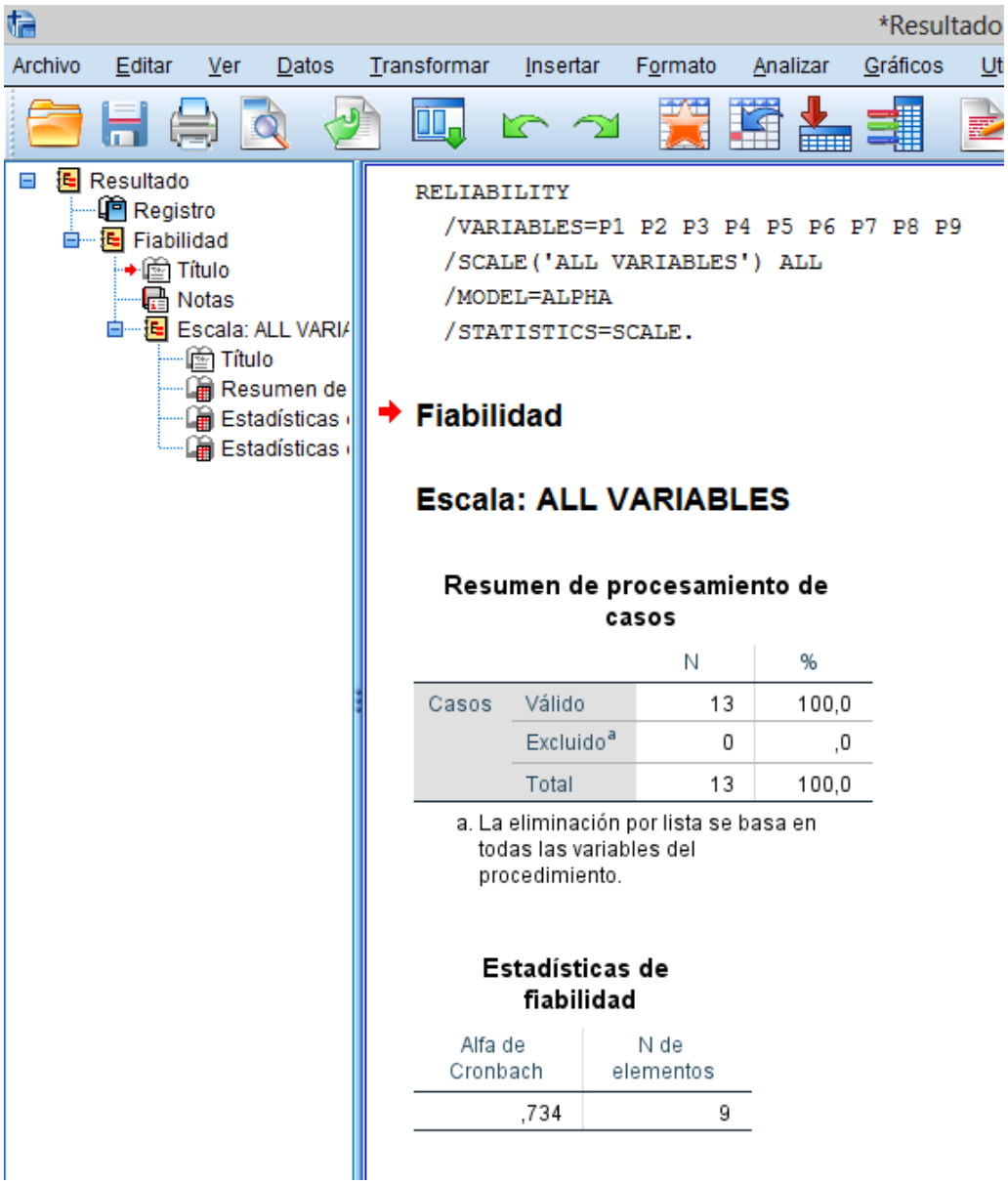
	DIMENSIONES	**ESCALA**				
		1	**2**	**3**	**4**	**5**
Ítem	**Recursos**					
10	¿Existe algún monitoreo por parte de la UNAC hacia los equipos informáticos del centro de cómputo?					
11	¿Existe alguna respuesta inmediata ante alguna falla en el centro de cómputo?					

12	¿Ha presenciado inconvenientes que no han tenido respuesta en un largo tiempo?					
13	¿Ha sido testigo de alguna renovación en los equipos del centro de cómputo?					
14	¿Ha sido testigo del manejo inadecuado de los recursos financieros de la UNAC para el centro de cómputo?					
15	¿Se detalla los gastos realizados por parte del área financiera de la UNAC para el centro de cómputo?					

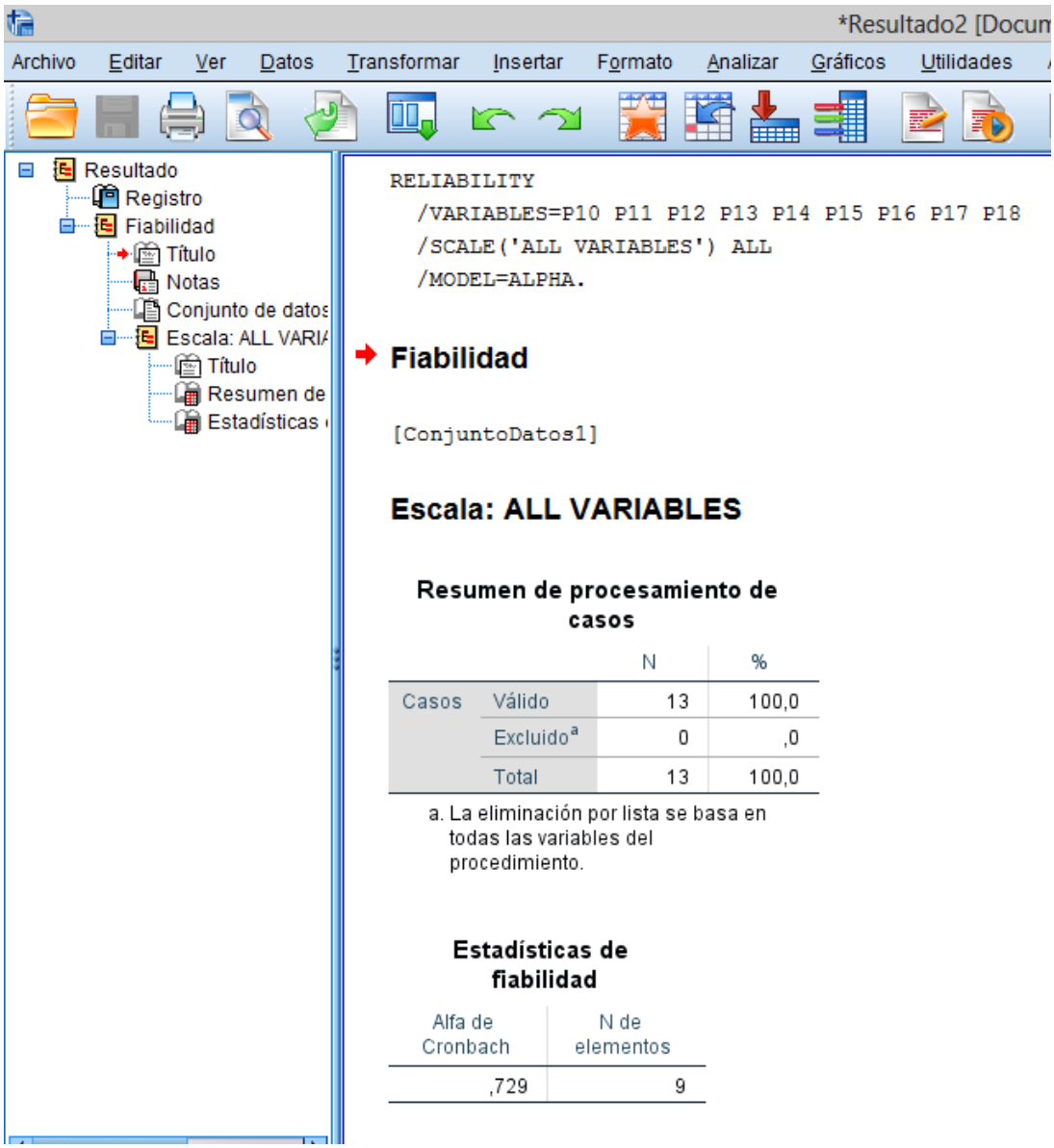
	DIMENSIONES	**ESCALA**				
		1	**2**	**3**	**4**	**5**
Ítem	**Cultura Informática**					
16	¿Cada cuánto tiempo se realizan campañas de capacitación?					
17	¿Alguna vez ha sufrido inconvenientes con el uso del software del centro de cómputo?					
18	¿Alguna vez ha presenciado a algún catedrático con dificultades en el manejo de algún software (Intranet, Utilitarios, etc)?					

Anexo i. Inprpant de resultados

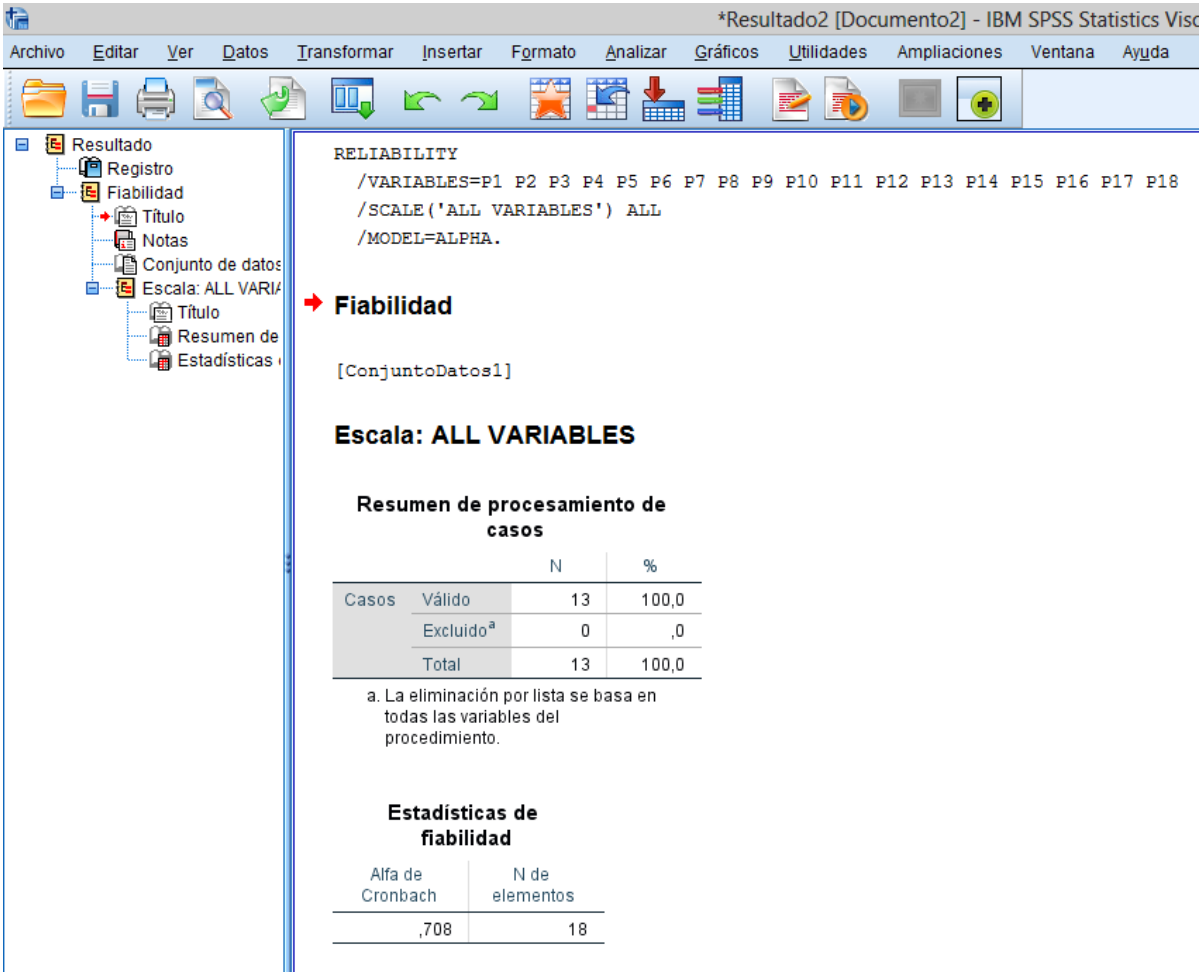
Análisis de Fiabilidad de la variable Seguridad de la Información



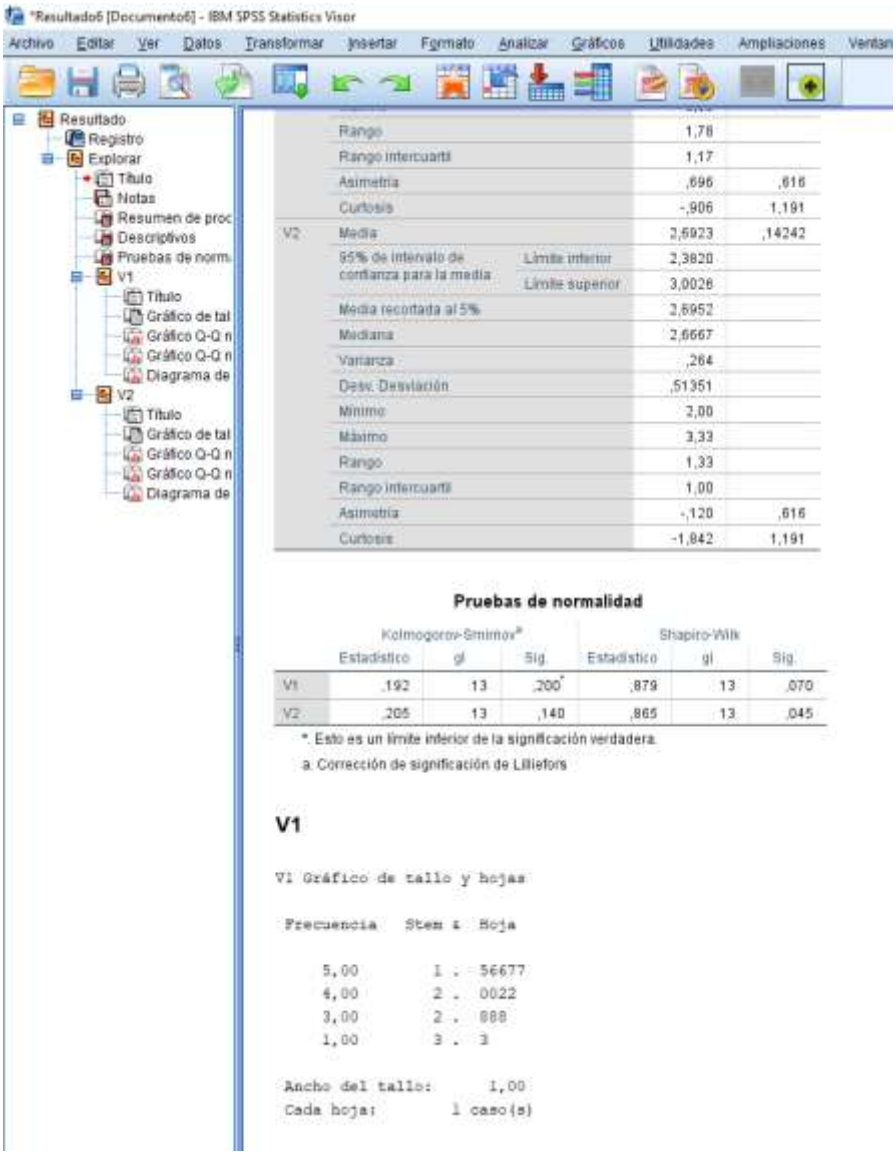
Análisis de Fiabilidad de la variable Gestión de Riesgos



Análisis de Fiabilidad de ambas variables



Pruebas de normalidad



	Rango		1,78	
	Rango intercuartil		1,17	
	Asimetría		,696	,616
	Curtosis		-,906	1,191
V2	Media		2,6923	,14242
	95% de intervalo de confianza para la media	Límite inferior	2,3820	
		Límite superior	3,0026	
	Media recortada al 5%		2,6952	
	Mediana		2,6667	
	Varianza		,264	
	Desv. Desviación		,51351	
	Mínimo		2,00	
	Máximo		3,33	
	Rango		1,33	
	Rango intercuartil		1,00	
	Asimetría		-,120	,616
	Curtosis		-1,842	1,191

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
V1	,192	13	,200*	,879	13	,070
V2	,205	13	,140	,865	13	,045

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

V1

```
V1 Gráfico de tallo y hojas

 Frecuencia    Stem &  Hoja

      5,00      1 .  56677
      4,00      2 .  0022
      3,00      2 .  888
      1,00      3 .  3

 Ancho del tallo:     1,00
 Cada hoja:        1 caso(s)
```

Correlación de Pearson