FACULTAD DE INGENIERÍA DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍIA DE SISTEMAS

INFORME DE TESIS

"Seguridad de información basada en la norma ISO/IEC 27001:2013 y nivel de seguridad en el centro de capacitaciones SENCICO – Ucayali 2018"

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

AUTOR:

BACH. ERICK MARTIN VELA RIOS

ASESOR:

MG. JUAN CARLOS LAZARO GUILLERMO

LINEA DE INVESTIGACION:

SISTEMA DE GESTION DE INFORMACION Y CONOCIMIENTO

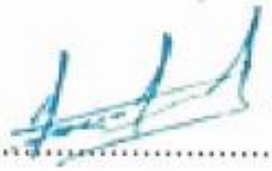
SUB LINEA:

ANALISIS DE PROCESO

UCAYALI – PERU

2021

Jurado Evaluador



.....

Mg. David Alfonso Ponce López

Presidente

.....

Mg. Adrian Marcelo Sifuentes Rosales

Secretario

.....

Dr. Jaime Augusto Rojas Elescano

Vocal

Mg. Juan Carlos Lázaro Guillermo

Asesor

Dedicatoria

A mis padres que me han dado la existencia; y en ella la capacidad por superarme y desear lo mejor en cada paso por este camino difícil y arduo de la vida. Gracias por ser como son, porque su presencia y su persona han ayudado a construir y forjar la persona que soy hoy.

Agradecimiento

El amor recibido, la dedicación y la paciencia con la que cada día se preocupan mis padres por mi avance y desarrollo de esta tesis, es simplemente único y se refleja en la vida de un hijo.

Gracias a mis padres por ser los principales promotores de mis sueños, gracias a ellos por cada día confiar y creer en mí y n mis expectativas, gracias a mi madre por estar acompañándome cada larga y agotadora noche de estudios; gracias a mi padre por siempre desear y anhelar siempre lo mejor para mi vida, gracias a los dos por los consejos, las reñidas y sobre todo gracias por estar a mi lado en este largo camino.

Constancia de Originalidad

Yo, ERICK MARTIN VELA RIOS, identificado con DNI Nº 71055617; egresado de la Escuela Profesional de Ingeniería de Sistemas de la Facultad de Ingeniería de Sistemas, de la Universidad Privada de Pucallpa.

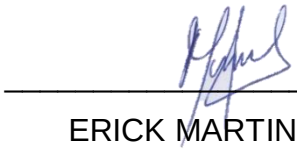
Declaro bajo juramento que:

Soy autor de la tesis titulada: “Seguridad de información basada en la norma ISO/IEC 27001:2013 y nivel de seguridad en el centro de capacitaciones SENCICO – Ucayali 2018”

1) La cual presento para optar el título profesional de Ingeniero de Sistemas.
2) He respetado las normas internacionales de citas y referencias para las fuentes consultadas. Por tanto, la tesis no ha sido plagiada ni total ni parcialmente.
3) La tesis no ha sido autoplagiada; es decir, no ha sido publicada ni presentada 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 la tesis se constituirán en aportes a la realidad investigada.

De identificarse 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 otros), asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad Privada de Pucallpa.

Pucallpa, 11 de enero del 2021



ERICK MARTIN VELA RIOS
DNI N° 71055617

UPP
Universidad Privada de Pucallpa

COORDINACIÓN DE INVESTIGACIÓN DE LA FACULTAD DE ADMINISTRACIÓN Y CIENCIAS CONTABLES

Constancia de Originalidad de trabajos de Investigación

Pucallpa, 30 de diciembre del 2020

Yo, JAIME AUGUSTO ROJAS ELESCANO, informo a la decanatura y a quien corresponda que se presentó a mi despacho la tesis titulada: "SEGURIDAD DE INFORMACION BASADA EN LA NORMA ISO/IEC 27001:2013 Y NIVEL DE SEGURIDAD EN EL CENTRO DE CAPACITACION SENCICO – UCAYALI 2018" perteneciente al bachiller, ERICK MARTIN VELA RIOS.

Habiendo realizado la verificación de coincidencia con el Software Antiplagio PlagScan, los resultados de similitud fueron de: 24.5 %. El cual está en los parámetros aceptados por las normas de la Universidad Privada de Pucallpa, que es máximo el 30%, por consiguiente, esta Coordinación da su aprobación de conformidad de la aplicación de la prueba de similitud y se autoriza al egresado a continuar con el trámite administrativo correspondiente.

Es todo por informar a su despacho señora Decana.

Jaime Augusto Rojas Elescano
Coordinadora de Investigación de la FCC y A-D

Resumen

El objetivo del trabajo de investigación fue; determinar la relación entre la seguridad de información, basada en la “Norma ISO/IEC 27001:2013” y el Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali 2018; para hacer la medición de la variable se dividieron en sub dimensiones como, Organización de seguridad de la información, Cubrimiento del SGSI en activos de información, identificación de riegos y estimación de riesgos.

La investigación, por su tipo de estudio fue sin intervención, prospectivo, transversal y analítico; por su nivel de investigación es relacional y por su finalidad cuantitativa y de modo específico el método descriptivo y por su diseño de investigación fue, correlacional de dos variables; para la muestra se tomó a 30 participantes. Se utilizó la técnica de la encuesta y el instrumento fue el cuestionario, sobre las variables seguridades de información, basada en la Norma ISO/IEC 27001:2013 y el Nivel de seguridad en los sistemas de información. Los datos se contrastaron mediante prueba no paramétrica Rho de Spearman con un nivel de significación de 0.01 y su coeficiente de correlación por presentar variables categórico ordinal.

La conclusión general a la que se arribó la investigación fue; una existencia de asociación entre Seguridad de información, bajo la Norma ISO/IEC 27001:2013 y Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018. En efecto cada vez que aumenta la puntuación Seguridad de información aumenta en forma positiva o directa de moderada a muy buena, puntuación de Nivel de seguridad en los sistemas de información siempre, porque así arrojó los datos. Es decir, el coeficiente de Rho de Spearman fue 0.819.

Palabras claves: seguridad de información y nivel de seguridad

Abstract

The objective of the research work was; determine the relationship between information security, based on the “ISO / IEC 27001: 2013 standard” and the security level in the information systems of the SENCICO training center in Ucayali 2018; for the measurement of the variable they were divided into sub dimensions such as, Organization of information security, Coverage of the ISMS in information assets, Compliance tasks and Security incidents.

The research, by its type of study was without intervention, prospective, transversal and analytical; due to its level of research it is relational and for its quantitative purpose and in a specific way the descriptive method and for its research design was correlational of two variables; 30 participants were taken for the sample. The survey technique was used and the instrument was the questionnaire, on the information assurance variables, based on ISO / IEC 27001: 2013 and the Security level in information systems. The data were contrasted by Spearman's nonparametric Rho test with a significance level of 0.01 and its correlation coefficient for presenting ordinal categorical variables.

The general conclusion reached in the investigation was; There is an association between Information Security, under the ISO / IEC 27001: 2013 Standard and Security level in the information systems of the SENCICO training center in Ucayali, 2018. Indeed Every time the score increases Information security increases in a positive way or direct from moderate to very good, security level score in the information systems provided, because that is how the data was sent. In other words, Spearman's Rho coefficient was 0.819.

Keywords: information security and security level

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

Introducción

El presente trabajo de tesis tuvo como objetivo general determinar la relación entre la seguridad de información, basada en la “Norma ISO/IEC 27001:2013” y el Nivel de seguridad de información en el centro de capacitación SENCICO de Ucayali 2018; y aportar así a la investigación científica datos importantes que permitan conocer fortalecer la seguridad de información y nivel de seguridad en el centro de capacitación SENCICO de Ucayali. Los datos se contrastaron mediante prueba no paramétrica estadístico Rho de Spearman con un nivel de significación de 0.01 por presentar variables categórico ordinal y su coeficiente de correlación para ver el grado de intensidad de correlación de las variables, Se utilizó para la descripción de resultados tablas y graficas estadísticos y sus interpretaciones respectivas, además, para la inferencia estadística la contratación de las hipótesis, con programa SPSS versión 22. Los resultados fueron, si existe le relación porque la significación fue de 0.000, valor inferior al nivel de significación propuesto (α = 0.01). Además, el coeficiente de Rho de Spearman que muestra el grado de relación entre estas dos variables fue 0.819, esto significa grado de relación positiva o directa de moderada a muy buena.

El presente trabajo cuenta con los siguientes capítulos:

En el capítulo I se presente el problema de la investigación, planteamiento del problema, formulación del problema, formulación de objetivos, justificación de la investigación, delimitación del estudio y viabilidad del estudio.

En el capítulo II se presenta el marco teórico, antecedente del problema, bases teóricas, definición de términos básicos, formulación de hipótesis y variable.

En el capítulo III se presenta metodología, diseño de la metodología, población y muestra, técnicas e instrumentos de recolección de datos, validez y confiabilidad del instrumento, técnicas para el procesamiento de la información.

En el capítulo IV se presente resultados y discusiones.

En el capítulo V se presenta las conclusiones y recomendaciones del resultado final de la tesis.

CAPITULO I: EL PROBLEMA DE LA INVESTIGACIÓN

1.1. Planteamiento del problema

El uso de las tecnologías de la información en las organizaciones ha ido aumentando rápidamente porque nos ayudan a optimizar y mejorar las actividades de cada proceso convirtiéndose en una herramienta valiosa. Así la continua evolución de la tecnología indudablemente representa una fuente de posibles riesgos para las organizaciones.

Con el uso de la tecnología, con el fin de almacenar, mantener, transmitir y recuperar información, se ha logrado que la variedad de amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información, los cuales provocan graves afectaciones ya sean de tipo financiero, operacional y de reputación en las organizaciones.

Actualmente un activo muy importante que poseen las organizaciones es la información, sin embargo, en muchas ocasiones éstas no cuentan con políticas adecuadas para protegerla, generando vulnerabilidades que pueden ser aprovechadas por las amenazas existentes en el entorno y dar como resultado riesgos y el comportamiento observado en las organizaciones ante esta situación mayormente es reactivo, es decir actúan luego de que el incidente de seguridad ha ocurrido.

1.2. Formulación del Problema

1.2.1. Problema General

¿Qué relación existe entre la seguridad de información, basada en la "Norma ISO/IEC 27001:2013" y el Nivel de seguridad de información del centro de capacitación SENCICO de Ucayali, 2018?

1.2.2. Problemas específicos

¿Cuál es la relación que existe entre la seguridad de información, basado en la "Norma ISO/IEC 27001:2013" y la identificación de riesgos para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018?

¿Cuál es la relación que existe entre la seguridad de información, basado en la "Norma ISO/IEC 27001:2013" y la estimación de riesgos para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018?

1.3. Formulación de objetivos

1.3.1. Objetivo General

Determinar la relación entre la seguridad de información, basada en la "Norma ISO/IEC 27001:2013" y el Nivel de seguridad de información del centro de capacitación SENCICO de Ucayali, 2018.

1.3.2. Objetivos específicos

Establecer la relación que existe entre la seguridad de información, basado en la "Norma ISO/IEC 27001:2013" y la identificación de riegos para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018.

Establecer la relación que existe entre la seguridad de información, basado en la "Norma ISO/IEC 27001:2013" y la estimación de riesgos para apoyar la seguridad de información del centro de capacitación

SENCICO de Ucayali, 2018.

1.4. Justificación de la investigación

El presente estudio se justifica en la necesidad de saber si cuentan con un sistema de gestión en la seguridad de información, basado en la "Norma ISO 27001: 2013" para asegurar la confidencialidad, integridad y sobre todo disponibilidad de información que maneja el centro de capacitación SENCICO de Ucayali; En consecuencia, tiene sustento en las siguientes justificaciones:

Justificación Teórica. - Es relevante desde el punto de vista teórico porque se encarga de estudiar cómo funciona la implementación del sistema de seguridad de información basada en ISO 27001: 2013 en el centro de capacitación SENCICO de Ucayali,2018.

Justificación Metodológica. –

El método a utilizar fue la investigación descriptiva – aplicativo gracias a la información que se requiera y proporcione los trabajadores y estudiantes de SENCICO.

Los lineamientos del proceso de investigación científica se seguirán en el presente proyecto, se incluirá además del planteamiento de los problemas, objetivos e hipótesis, con la finalidad de establecer un conocimiento acerca del sistema de gestión teniendo como resultado la mejora de ésta. Los procedimientos, técnicas y métodos e instrumentos que se empleen en la investigación y cuando sean demostrado su validez y confiabilidad podrán ser utilizados en otros trabajos de investigación (Carrasco, 2006, p. 401).

Justificación Práctica. - Existe la necesidad de encontrar la solución al problema planteado para esta investigación a través de la relación de las variables

Justificación Normativa. - La presente investigación servirá como base para fortalecer las metodologías a emplear en la "Implementación de Sistema de Gestión de Seguridad de Información" ya que es necesario modernizar nuestro sistema de protección de activos de información.

1.5. Delimitación del estudio

1.5.1. Delimitación Espacial

La investigación se llevará a cabo en el centro de capacitación Sencico de Ucayali. Está localizada en la región oriental del Perú, ostenta una amplia región amazónica del país; por la característica geográfica que presenta su territorio, existe cierta dificultad para trasladarse a la capital de la república.

1.5.2. Delimitación Temporal

El tiempo propuesto para el desarrollo del estudio es de 4 meses (marzo a junio del 2018).

1.5.3. Delimitación Social

El grupo social que serán sujetos de análisis será el total de trabajadores del centro de capacitación SENCICO de Ucayali.

1.5.4. Delimitación Conceptual

Las variables en estudio son:

“Sistema de Gestión de la seguridad de información”.

“Protección de información”.

1.6. Viabilidad del estudio

1.6.1. Viabilidad Técnica

El proyecto hará uso de programa de manejo de texto y cálculos (Word y Excel, SPSS) por lo que se cuenta con dicha tecnología.

1.6.2. Viabilidad Operativa

El presente proyecto permitirá el manejo adecuado de la norma ISO 27001: 2013.

1.6.3. Viabilidad Económica

El proyecto será financiado en su totalidad por el proyectista por lo que se cuenta con el financiamiento.

CAPITULO II: MARCO TEÓRICO

2.1. Antecedentes del problema

Las empresas que se dedican a brindar servicios como capacitaciones, investigaciones e innovaciones como es el caso de SENCICO, maneja información de cada uno de sus estudiantes y por lo tanto es de mucha importancia tener protegida dicha información.

2.1.1. Antecedentes internacionales

Según Andrade y Chávez (2018). En sus tesis *"Generación de un plan para la gestión integral de seguridad de la información basado en el marco de la norma ISO 27001 y las mejores prácticas de seguridad de la norma ISO 27002 para la compañía International Gym ECUAINTERGYM S.A*". de la ciudad de Guayaquil. Tuvo como objetivo es generar un plan de mejoras en la obtención, manipulación y conservación de la información en la empresa INTERNATIONAL GYM ECUAINTERGYM S.A. basado en la norma ISO 27001 y las buenas prácticas definidas en la norma ISO 27002. Se concluyó:

Por medio de la determinación de los activos críticos de información de la empresa International Gym Ecuaintergym S.A. se concluye que posee una serie de factores que ponen en riesgo la integridad de los activos de la información, siendo estos la falta de controles en el acceso a los equipos y servicios, la manipulación

Incorrecta de los activos, el ingreso de personas sin autorización a áreas de procesamiento de datos sensibles de la compañía y teniendo un nivel de perjuicio alto en las operaciones en caso de materializar alguna vulnerabilidad, adicional a eso la falta de condiciones físicas adecuadas producen daños permanentes en los equipos, no existe una correcta identificación de los activos de la información lo cual produce pérdida de tiempo en la búsqueda de datos.

Con el análisis de las buenas prácticas de seguridad de la información para solventar los puntos débiles de seguridad se determinó cuáles de ellas son aplicables a la propuesta presentada con el objetivo de que la empresa International Gym Ecuaintergym S.A. mantenga un nivel de seguridad optimo previniendo estimacion de riesgos de la información.

Por medio de la propuesta de los procesos de gestión de riesgos de seguridad se identificó que controles son necesarios para reducir el riesgo detectado, reconociendo cada una de las posibles amenazas que perjudiquen los activos de la información. Determinando la estrategia para mitigar los riesgos por medio del establecimiento de medidas de seguridad.

Al elaborar el plan de mejoras para la empresa International Gym se podrá contar con políticas que aseguren la disponibilidad, accesibilidad e integridad de la información, estableciendo formalmente responsabilidades y procedimientos sobre los diversos activos de la información para la correcta ejecución de las buenas prácticas de seguridad de la información.

Con la elaboración del plan de capacitación sobre las buenas prácticas de seguridad se podría informar y concienciar a los empleados de la compañía International Gym Ecuaintergym S.A. sobre la correcta ejecución de las normas y procedimientos que se encuentren establecidos en el plan de mejoras para así evitar incidentes por falta de información.

Según Tola (2015) en su tesis titulada *"Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001*", de pregrado, Ecuador. Tuvo como objetivo general es lograr la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001:2005 para preservar la confidencialidad, integridad y disponibilidad de la información que maneja la empresa A&CGroup S.A. Se concluyó:

Debido a que en las organizaciones es primordial la optimización de recursos, el establecimiento del alcance del sistema de gestión de seguridad de la información se convierte en una actividad muy importante ya que delimita el campo de acción y el uso de recursos.

Es importante establecer los objetivos y políticas del sistema de gestión de seguridad de la información, ya que estos van delineando el camino hacia donde la organización desea dirigirse para preservar la confidencialidad, integridad y disponibilidad de la información y por lo tanto es relevante la participación de la alta gerencia.

La adopción de la metodología MAGERIT para el análisis de riesgos, permitirá identificar de manera oportuna la probabilidad y el impacto de que se materialicen los riesgos y de esta manera poder establecer controles que nos ayuden a prevenirlos.

Los sistemas de Gestión de Seguridad de Información bajo la norma ISO 27001, se basan en la prevención, por lo tanto, es muy importante identificar los riesgos a los que están expuestos los activos para así evitar pérdidas económicas u operacionales.

Una vez identificados los riesgos a los que están expuestos los activos de información, es necesario implementar controles o salvaguardas, con la finalidad de proteger estos activos y lograr minimizar la probabilidad de que se materialicen los riesgos o el impacto que pueden tener sobre la organización. Es importante considerar que al momento de seleccionar los controles se debe

realizar un análisis de costo beneficio ya que el costo de la implementación de un control no debe exceder la posible pérdida económica de no tener implementado el control.

Dentro del ciclo de un Sistema de Gestión de Seguridad de la Información, basado en ISO 27001, se encuentra la mejora continua lo cual hace que sea muy importante que la organización se asegure de crear procedimientos para el monitoreo y revisión del sistema, los mismos que deben cubrir estimacion de riesgos, auditorías internas y revisiones gerenciales. Estos elementos aportan retroalimentación al Sistema posibilitando conocer el estado del mismo y aplicar acciones correctivas, si fuera el caso, que permitan el cumplimiento de los planes y objetivos

2.1.2. Antecedentes nacionales

Según Santos (2016). En su tesis *"Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software*", de pregrado. Tuvo como objetivo de desarrollar un Sistema de Gestión de Seguridad de Información (SGSI) para una empresa de consultoría en desarrollo y calidad de software, tomando como marco normativo el estándar ISO/IEC 27001:2013. Se concluyó:

Para elaborar adecuadamente los componentes que permitan cumplir los requisitos del estándar 27001 deben considerarse aquellos estándares que, aunque no son referenciados, forman parte del dominio de algunos de los requisitos del SGSI.

Como resultado de las exigencias del proyecto y sus interesados, se han podido elaborar propuestas innovadoras asociadas a: la metodología de gestión de riesgos, la normalización de los planes del sistema y realizar la verificación integral de cumplimiento de los componentes requeridos como requisitos por la ISO/IEC 27001:2013.

2.2. Bases teóricas

2.2.1. Variable 1 - Seguridad de la información, bajo la “Norma ISO/IEC 27001:2013”.

Según ADVISERA (2019) es “Norma internacional que ayuda a gestionar la información de una empresa pública o privada”.

Según ADVISERA (2019) el ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

Finalmente, el ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento; aquí se puede ver la cantidad de certificados en los últimos años.

A continuación, se considera algunos fundamentos y normas técnicas referentes a la Variable 1:

“NTP ISO/IEC 27001:2014 Tecnología de Información, Técnicas de Seguridad y Sistemas de Gestión de Seguridad de Información. Requerimientos”.

“Norma técnica peruana de requisitos para implementar un SGSI. Es

una traducción del estándar ISO/IEC 27001:2013, razón por la cual cambia mucho respecto a la versión precedente (2008), actualmente se encuentra vigente y es de cumplimiento obligatorio para las entidades del estado peruano, por resolución aprobada por la Presidencia del Consejo de Ministros (PCM). Las entidades privadas pueden tomarlo como marco referencial." **(Horna, 2014),**

NTP ISO/IEC 17799:2007 Tecnología de Información, Técnicas de Seguridad y Código de prácticas para controles de seguridad de información"

"Norma técnica peruana de controles de seguridad de información. Es una traducción de la ISO/IEC 17799:2005. Si bien ya existe una nueva versión del estándar (ISO/IEC 27002:2013), aún no se ha realizado su traducción como norma técnica peruana, por lo que la presentación de los grupos de controles contenidos en esta norma técnica se puede considerar desfasado".**(ESAN, 2016),**

OCTAVE – Allegro

"Es el acrónimo de evaluación de las amenazas, activos y vulnerabilidades operacionalmente críticas (OCTAVE, por sus siglas en inglés). Contiene una metodología de análisis de riesgo desarrollada por Computer Emergency Response Team (CERT), enfocada en el estudio de riesgos para organizaciones pequeñas (versión Allegro). La evaluación parte de la identificación de activos relacionados con la información, para identificar amenazas y vulnerabilidades, a partir de los cuales se pueden determinar riesgos de seguridad de información. A partir de estos resultados se plantean estrategias y planes, para mitigar los riesgos identificados. **(Fernández, 2016),**

NIST SP 800 - 100 Manual de Seguridad de Información: Guía para gestores

"La SP 800-100 es la guía de gobierno de la seguridad de información del National Institute of Standards and Technology (NIST);

incluye los roles de gobierno, el ciclo de vida para la gestión de la seguridad, la capacitación, gestión de recursos, indicadores, gestión de riesgos, manejo de incidentes, entre otros aspectos de la administración de la seguridad de información en organizaciones" (***Laudon K.C. y Laudon J.P., 2012).***

NIST SP 800 - 39 Gestionar Riesgos de Seguridad de Información

"La SP 800-39 es la guía para la gestión de riesgos de seguridad de información del National Institute of Standards and Technology (NIST); comprende: el Enmarcado del Riesgos, estableciendo un contexto; la Evaluación del Riesgo, identificando, priorizando y estimando el riesgo; la Respuesta al Riesgo, definiendo las opciones de curso de acción frente al riesgo; y el Monitoreo del Riesgo, para evaluar la situación final de los riesgos". ***(Laudon K.C, y Laudon J.P., 2012).***

NIST SP 800 – 53 Controles de Seguridad y Privacidad para Sistemas de Información Federales y Organizaciones – Revisión 4

"La SP 800-53 es un marco referencial de controles de seguridad de información del National Institute of Standards and Technology (NIST). El fin de esta propuesta de controles es servir de referente para la selección de aquellos que sean necesarios para la organización. Los presenta en grupos de controles organizados en 18 dominios. La versión vigente de este documento es la revisión 4 (2013)". ***(Laudon K.C, y Laudon J.P., 2012).***

2.2.1.1 Dimensiones de la Variable 1

Organización de seguridad de la información

Si se desee implantar un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001 deberá llevar a cabo una evaluación de los riesgos de la seguridad de la información para poder establecer controles que aseguren un entorno invariable bajo los criterios de disponibilidad, confidencialidad e integridad. (ISOTools, 2019).

Cubrimiento del SGSI en activos de información

En un enfoque tradicional de proteger los activos de la información existido en la seguridad física durante muchos años. Tiene un activo físico y luego construye un perímetro de seguridad alrededor de él (ISOTools, 2019).

2.2.1.2 Indicadores

Evaluación de desempeño

En una organización que esté modernizada y a la vanguardia de las últimas corrientes la aplica. Lo mejor es que la empresa no se quede atrás y aproveche los continuos adelantos y mejoras que se producen en Recursos Humanos, que a su vez logran que una organización sea más competitiva y eficaz (ISOTools, 2019).

Nivel de programas de capacitación

La capacitación o desarrollo de personal, es una actividad realizada en una organización que responde a sus necesidades y busca la mejorar actitud, conocimiento, habilidades o conductas de su personal. (ISOTools, 2019).

Activos críticos de información

En la gestión es una tarea de las gerencias de seguridad o de gestión de la información que involucra el diseño, establecimiento e implementación de un proceso que permita la identificación, valoración, clasificación y tratamiento de los activos de información más importantes del negocio (NovaSec, 2021).

Un activo de información en el contexto de la norma ISO/IEC 27001 es: “algo que una organización valora y por lo tanto debe proteger”. (NovaSec, 2021).

Inventario de activos

Se define como una lista de todos aquellos recursos (físicos, software, documentos, servicios, personas, instalaciones, etc.) que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. **(**ISOTools, **2019).**

2.2.2. Nivel de seguridad

Se detalla algunas fuentes referentes al nivel de seguridad y finalmente sus definiciones.

MAGERIT VERSIÓN 3

"Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, desarrollada por el gobierno español. Propone un esquema de gestión de riesgos basado en identificar activos, amenazas, impactos, controles (salvaguardas) y estado del riesgo; posteriormente, con esta información se realiza la **evaluación del riesgo y la subsecuente aceptación** / tratamiento del riesgo".**(Magerit Versión 3, 2012).**

Directiva de Seguridad (Ley de Protección de Datos Personales 29733)

"Marco de recomendaciones en seguridad de información, relacionadas al adecuado tratamiento y custodia de la información de carácter personal. Documento emitido por la Autoridad Nacional de Datos Personales como marco complementario para la implementación de la Ley. En base a la categoría de los bancos de datos personales administrados por las organizaciones, esta directiva **define niveles de requisitos a manejarse**. A mayor volumen y complejidad de los datos, mayor **el nivel de exigencia**. En el nivel más alto se recomienda implementar un SGSI".

"Es una guía profesional que parte del modelo, conceptos, artefactos y principios de COBIT 5. Se basa en el modelo BMIS (Modelo de

Negocio para la Seguridad de Información) bajo un enfoque específico de seguridad de información sobre las tecnologías de información. Integra componentes y controles desarrollados por otros estándares, en un esquema único que permite que la organización interesada **pueda seleccionar los más adecuados**. Desarrolla un marco de: Políticas y principios, los cinco grupos de procesos de COBIT aplicados a la seguridad de información, el marco organizacional y cultural, los controles para el manejo de la información, los servicios, infraestructura y aplicaciones, personas, gobierno y riesgos. Para el desarrollo de un marco de gestión de riesgos que le permita operar, se apoya en la propuesta metodológica de RISK IT. **(Franco, 2012).**

Marco Risk IT para la Gestión de TI relacionada a Riesgos del Negocio

"Es el marco de gestión de riesgos TI de ISACA, relacionado a su vez al marco de riesgos empresariales que aplican sobre la organización. Cuenta con una serie de principios propios, similares a los de COBIT, a partir de los cuales despliega tres dominios para poner en práctica el marco: el Gobierno del Riesgo, donde se establece el enfoque de riesgos, la integración a los riesgos empresariales y la toma de decisiones; la **Evaluación de Riesgos**, donde se obtienen datos, se analiza y mantienen los riesgos; y la Respuesta a los Riesgos, donde se reacciona a los riesgos". **(Espinoza, 2013).**

De las cuatro (04) referencias anteriores sobre el concepto de Nivel de seguridad se asemejan y consideran con otra terminología siempre buscando minimizar los riesgos. Según Arévalo (2020) considera como ventaja de implementar las Normas ISO 27001 la siguiente: Permite crear metodologías que contribuyan a la mitigación de los riesgos y a **incrementar el nivel de seguridad** en la información que se tiene.

La información documentada que debe tener un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 es el Plan de Tratamiento de riesgos. **El nivel se**

seguridad se define como los niveles aceptables de seguridad de la información en la organización garantizado por la implementación del plan de tratamiento de riesgos, aprobado por la alta dirección con los recursos asignados para tal fin, y el mantenimiento de los controles existentes. Todo ello se fundamenta en la implementación de un Sistema de Gestión de Seguridad de la Información en la Fase 5: Diseñar el SGSI (Humphreys, 2020).

Según ISOTools (2019) el nivel de seguridad es: “Conjunto de medidas preventivas y reactivas, que permiten proteger y resguardar la información, manteniendo la confiabilidad e integridad de los datos”.

Las dimensiones V2 son subniveles del Análisis del Anexo A – ISO 27001-2013 y análisis de controles.

2.2.2.1 Dimensiones V2

Identificación de riesgo

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación. Los activos de información se clasifican en dos tipos (Humphreys, 2020).

Estimación de riesgo

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos (Humphreys, 2020).

2.2.2.2 Indicadores V2

Primario

Según Humphreys (2020) implica 3 bases y son:

- Procesos o subprocesos y actividades del Negocio:

procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

- Información: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.
- Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

Soporte

Según Humphreys (2020) implica 5 bases y son:

- Hardware: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
- Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
- Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de

acceso, etc.)

- Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- Sitio: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
- Estructura organizativa: responsables, áreas, contratistas, etc.

Probabilidad

La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse (Humphreys, 2020).

Impacto

Hace referencia a las consecuencias que puede ocasionar a la Universidad la materialización del riesgo; se refiere a la magnitud de sus efectos (Humphreys, 2020).

2.3. Definición de términos básico

- **Activo de Información**: Es un elemento intangible, físico o tecnológico que genera, procesa o almacena alguna información que tiene valor para la organización como programas, archivos, bases de datos, manuales y la imagen de la empresa. La información puede existir de muchas formas:
  - Impresas
  - Almacenadas electrónicamente
  - Transmitida con medios electrónicos
  - Mostrada en videos
  - Conocimiento de las personas. (Robin. J y Salcedo. B., 2014).
- **Amenazas**: Eventos en las cuales se originan pérdidas por riesgos en la seguridad de información. (Belmonte. A, 2017).

- **Análisis de Riesgos**: Estudio y evaluación del riesgo de la difusión de información necesaria para formular recomendaciones orientadas a adoptar medidas en respuesta a un peligro determinado (Belmonte. A, 2017).
- **Audiovisuales**: Conformada por discos duros, cintas, usb, videos y CD - ROM. (Belmonte. A, 2017).
- **Auditoría**: Proceso para obtener evidencias que al evaluarse de manera objetiva permiten determinar que se cumplen los criterios definidos para la auditoría interna. (Belmonte. A, 2017).
- **Clasificación de la Información**: Es ejercicio por el cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la organización. El cual tiene como objetivo asegurar que la información recibida tenga el nivel de protección adecuado. (Belmonte. A, 2017).
- **Conformidad**: cumplimiento de un requisito. (Belmonte. A, 2017).
- **Control**: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía. Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en una estructura organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal. (Belmonte. A, 2017).
- **Custodio**: Es una parte designada de la entidad, un cargo, proceso, o un grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. (Belmonte. A, 2017).
- **Declaración de aplicabilidad**: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la compañía. (Belmonte. A, 2017).
- **Disponibilidad**: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en

pérdidas financieras, de imagen y/o credibilidad ante nuestros clientes. (Belmonte. A, 2017).

- **Efectividad**: Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles. (Belmonte. A, 2017).
- **Eficacia**: Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados. (Belmonte. A, 2017).
- **Eficiencia**: Relación entre el resultado alcanzado y los recursos utilizados. (Belmonte. A, 2017).
- **Impacto**: Se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos del negocio. (Belmonte. A, 2017).
- **Incidente de seguridad de la información**: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (Belmonte. A, 2017).
- **Información**: Datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio. (Belmonte. A, 2017).
- **Integridad**: La información de SENCICO debe ser clara y completa y solo podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la información puede exponer a la Empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas financieras. (Robin. J y Salcedo. B., 2014).
- **La Dirección**: Es la encargada de combinar los recursos humanos y técnicos lo mejor posible para conseguir los objetivos de la empresa; está conformada por la presidencia y directivos, quienes se encargarán de desarrollar los planes a largo plazo de la empresa. (Robin. J y Salcedo. B., 2014).
- **No conformidad**: El no cumplimiento de un requisito especificado. También puede denominarse no conformidad real. (Robin. J y Salcedo. B., 2014).

- **No conformidad mayor**: El no cumplimiento de un requisito debido a la falta frecuente o deliberada de cumplimiento de un requisito documentado en el sistema, incumplimiento de requisitos legales o reglamentarios, múltiples no conformidades menores dentro del mismo requisito de la Norma o la falta deliberada en corregir No Conformidades. (Robin. J y Salcedo. B., 2014).
- **No conformidad menor**: El no cumplimiento de un requisito sin que exista una amenaza relevante o significativa para el Sistema de Gestión de Calidad o cuando sea una instancia aislada de incumplimiento. (Robin. J y Salcedo. B., 2014).
- **No conformidad potencial**: Evento en el cual no hubo No Conformidad, pero en caso de repetirse pudiera serlo, por la existencia de un riesgo. Una acción preventiva pudiera ser tomada para evitar su ocurrencia. (Robin. J y Salcedo. B., 2014).
- **Observación**: Apartado del informe de auditoría en el que el auditor deja constancia de las oportunidades de mejora, de los riesgos para la calidad o de cualquier otro detalle que haya observado y le parece relevante registrar. (Robin. J y Salcedo. B., 2014).
- **Observador**: Integrante del equipo auditor que se encuentra en proceso de entrenamiento y su objetivo es adquirir competencia mediante la observación. Algunas veces apoya al equipo auditor tomando notas de los hallazgos de la auditoría en las listas de chequeo. (Robin. J y Salcedo. B., 2014).

2.4. Formulación de hipótesis

2.4.1. Hipótesis General

H1: Existe relación entre la seguridad de información, basada en la "Norma ISO/IEC 27001:2013" y el Nivel de seguridad de información del centro de capacitación SENCICO de Ucayali, 2018.

H0: No existe relación entre la seguridad de información, basada en la "Norma ISO/IEC 27001:2013" y el Nivel de seguridad de información del centro de capacitación SENCICO de Ucayali, 2018,

2.4.2. Hipótesis específicas

Establecer la relación que existe entre la seguridad de información, basado en la "Norma ISO/IEC 27001:2013" y la identificación de riegos para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018.

Establecer la relación que existe entre la seguridad de información, basado en la "Norma ISO/IEC 27001:2013" y la estimación de riesgos para apoyar la seguridad de información del centro de capacitación SENCICO de Ucayali, 2018.

2.4.3. Definición conceptual de la variable

Variable Asociado.

V1: Seguridad de la información, bajo la "Norma ISO/IEC 27001:2013".

"Norma internacional que ayuda a gestionar la información de una empresa pública o privada". ADVISERA (2019).

Variable de supervisión.

V2: Nivel de seguridad.

Conjunto de medidas preventivas y reactivas, que permiten proteger y resguardar la información, manteniendo la confiabilidad e integridad de los datos". ISOTools (2019)

2.4.4. Definición operacional de la variable

Dimensiones V1

- Organización de seguridad de la información
- Cubrimiento del SGSI en activos de información.

Indicadores V1

- Evaluación de desempeño.
- Nivel de programas de capacitación.
- Activos críticos de información.
- Inventario de activos.

Dimensiones V2

- Identificación de riegos
- Estimación de riesgos

.

Indicadores V2

- Primarios
- Soporte
- Probabilidad
- impacto.

2.4.5. **Matriz de Operacionalización de las variables.**

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSION	INDICADOR	ESCALA DE MEDICION
Seguridad de información, bajo la Norma ISO/IEC 27001:2013.	"Noma internacional que ayuda a gestionar la información de una empresa pública o privada". ADVISERA (2019)	Organización de seguridad de la información	Evaluación de desempeño.	Muy buena Buena Regular Mala
			Nivel de programas de capacitación.	
		Cubrimiento del SGSI en activos de información	Activos críticos de información.	
			Inventario de activos.	
Nivel de seguridad	"Conjunto de medidas preventivas y reactivas, que permiten proteger y resguardar la información, manteniendo la confiabilidad e integridad de los datos". ISOTools (2019)	Identificación de riesgos	Primario	
			Soporte	
		Estimación de riesgos	Probabilidad	
			Impacto	

Fuente: Elaboración propia

CAPÍTULO III: METODOLOGÍA.

3.1. Diseño de la investigación

3.1.1. Tipo de la investigación

La investigación de tipo Aplicada tiene como propósito dar solución a situaciones o problemas concretos e identificables (Bunge, 1971).

La investigación será de tipo aplicada, porque se aplicará la Norma ISO/IEC 27001:2013 en el Nivel de seguridad de los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018

3.1.2. Nivel de investigación

El nivel de investigación: Este se refiere al grado de profundidad con que se aborda un fenómeno u objeto de estudio. Así, en función de su nivel el tipo de investigación es Descriptivo Correlacional

Según Sampieri (1998) los estudios descriptivos permiten detallar situaciones y eventos, es decir cómo es y cómo se manifiesta determinado fenómeno y busca especificar propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis. Esta tesis considera usar la Norma ISO/IEC 27001:2013 para establecer, implementar, utilizar, monitorear, revisar,

mantener y mejorar el Nivel de Seguridad del centro de capacitación SENCICO de Ucayali, 2018. La Correlaciona busca establecer la relación entre la variable V1 la variable V2.

3.1.3. Diseño de investigación

Para esta investigación se usó como diseño de investigación lo propuesto por (Hernández, 2014) el Diseño No Experimental, en ello el investigador observa los fenómenos tal y como ocurren naturalmente, sin manipular a la variable.

Esquema de Investigación

Se puede representar mediante la siguiente simbología: M1, G1, O1 y X

M1: G1 X O1

Donde

G1: Seguridad de la información, bajo la Norma ISO/IEC 27001:2013

O2: Nivel de Seguridad

3.2. Población y muestra.

La población de la presente investigación lo constituirá los 30 trabajadores del Centro de capacitación SENCICO compuesto de la siguiente manera:

Docentes	= 18
Secretaria	= 2
Director	= 1
Soporte técnico	= 9
Total	= 30

Según Hernández et al (1998): Debido a que la población es muy pequeña (n<=30) se tomarán a los 30 trabajadores de la Entidad mencionada. La selección de la muestra será en base a un muestreo no probabilístico, de tipo

intencional o por conveniencia; que para el caso la muestra será el total de la población.

3.3. Técnicas e Instrumentos de recolección de datos

3.3.1. Técnicas

La encuesta.

Se aplicará a los usuarios con la finalidad de recoger evidencias sobre el conocimiento, interés y necesidades de parte de cada uno de ellos con respecto a la existe relación entre la seguridad de información, basada en la “Norma ISO/IEC 27001:2013” y el Nivel de seguridad en los sistemas de información.

3.3.2. Instrumentos

El instrumento utilizado fue Cuestionario, cuya estructura consta La estructura del instrumento consta de 8 items que corresponde a

Variable categórica y con escala de medición ordinal Muy Buena, Buena, Regular, Mala, según lo establecido por escalamiento Likert el valor de (1) es asignado a (Malo) y el máximo valor (4) a (Muy Bueno).

3.4. Validez y confiabilidad del instrumento

La **validación de Instrumento**, se utilizará el juicio de expertos el cual ayudará validar el instrumento. En la investigación se aplicó validez de contenido, específicamente Validez de juicio de experto y se midió el dominio específico de contenido de lo que se mide Validez de juicio de experto, ellos dieron su apreciación cualitativa a través de una ficha que se adjunta como anexo de esta manera tuvo 03 expertos (un metodólogo, uno de especialidad y un estadístico).

Para la **confiabilidad**, el instrumento producirá resultados consistentes y coherentes. Es decir, en que su aplicación al mismo sujeto u objeto debe

producir resultados iguales, Kerlinger (2002). En la investigación se aplicó Medidas de consistencia interna específicamente el Coeficiente del Alfa de Cronbach, cuya fórmula es:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum S^2 i}{\sum S^2 t}\right]$$

Variable: Seguridad de la Información bajo la Norma ISO/IEC 27001:2013

Nombre de la prueba de confiabilidad	
Alfa de Cronbach	**Ítems**
0,917	4

Fuente: Propia, aplicando el programa SPSS V22.0

Interpretación: El Estadístico de fiabilidad de Alfa de Cronbach aplicada al instrumento de investigación arrojo 0,917, por ende, el instrumento es altamente confiable para la investigación por el resultado que arrojó.

Variable: Nivel de Seguridad

Nombre de la prueba de confiabilidad	
Alfa de Cronbach	**Ítems**
0,917	4

Fuente: Propia, aplicando el programa SPSS V22.0

Interpretación: El Estadístico de fiabilidad de Alfa de Cronbach aplicada al instrumento de investigación arrojo 0,917, por ende, el instrumento es altamente confiable para la investigación por el resultado que arrojó.

3.5. Técnicas para el procesamiento de la información

Como lo menciona Hernández (2003) debe decidir qué tipo de análisis de los datos se llevará a cabo: cuantitativo, cualitativo o mixto. Por lo que el análisis elegido es cuantitativo, para poder pre diseñar o coreografiar el esquema de análisis de los datos. Se utilizó para la descripción de resultados

tablas y graficas estadísticos y sus interpretaciones respectivas, mientras para para la inferencia la contratación de las hipótesis, con programa SPSS versión 22.

CAPITULO IV: RESULTADOS Y DISCUSIÓN

4.1. Presentación de resultados

La característica de la población de estudio después de la realización de la toma de datos, la información presentó de 30 unidades de estudio en total, mayor cantidad de docentes y técnicos (en una relación de 60.0% a 30.0%) y el 10% corresponde entre Secretarias y Director.

RESULTADOS DESCRIPTIVOS DE LAS VARIABLES Y DIMENSIONES.

Variable Asociado V1

Seguridad de la información, bajo la Norma ISO/IEC 27001:2013; Esta variable tiene 02 dimensiones: la primera dimensión: Organización de seguridad de la información y su indicador (Evaluación de desempeño, Nivel de programas de capacitación), y la segunda dimensión: Cubrimiento del SGSI en activos de información, y su indicador (Número de activos críticos de información e Inventario de activos); así mismo corresponde a variable categórico y con nivel de medición ordinal donde su escala de medición es: (Muy buena, Buena, Regular y Mala).

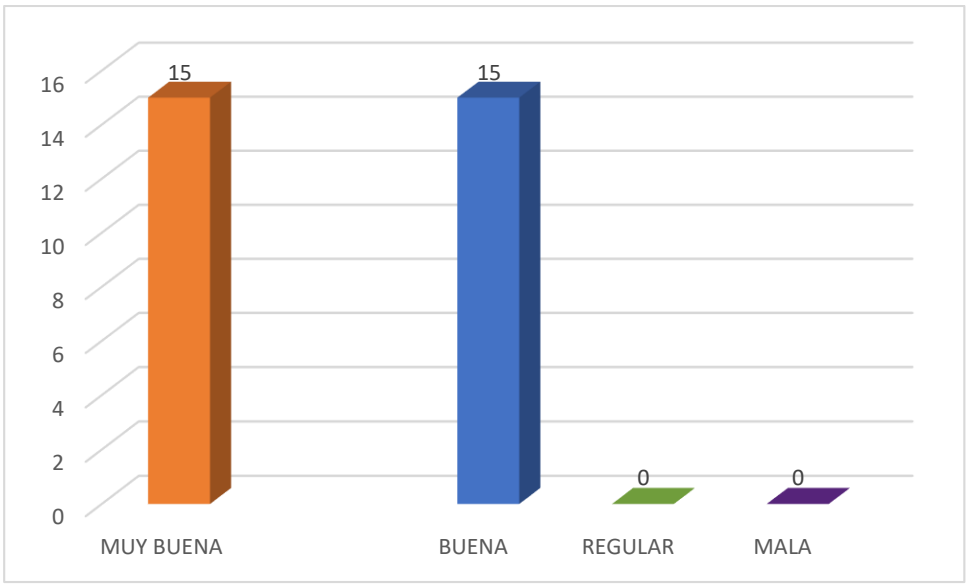
Tabla 1. Distribución de frecuencias sobre Opinión de seguridad de información bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	MUY BUENA	15	50,0%	50,0%
	BUENA	15	50,0%	100,0%
	REGULAR	0	0,0%	100,0%
	MALA	0	0,0%	100,0%
	Total	30	100,0%	

Fuente: Datos obtenidos en la investigación al personal de SENCICO.

Como se observó en la Tabla 01, los participantes en igual proporción opinaron solo Muy buena y Buena cada uno 50% respectivamente, mientras ningún participante opinó Mala y Regular, esta información demostró que la seguridad de información bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO se encuentran en óptimas condiciones.

Figura 1. Descripción de los participantes que respondieron referente a la variable seguridad de información bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO



Fuente: Datos obtenidos en la investigación al personal de SENCICO.

Según la figura 01, se observó de los 30 participantes opinaron que la seguridad de información bajo la norma ISO se encontró en igual proporción, ellos evaluaron que su desempeño es Buena y Muy buena, es decir sus desempeños no están en absoluto entre Regular y Mala. En consecuencia, el desempeño del personal de seguridad de SENCICO se encuentra en óptimas condiciones por ello se refleja sus opiniones entre buena a muy buena.

Variable de Supervisión V2

Nivel de Seguridad; Esta variable también comprende 02 dimensiones primera dimensión: Identificación de riesgos con sus indicadores (Primario y soporte) y la segunda dimensión: Estimación de riesgos con sus indicadores (Probabilidad e Impacto), corresponde a variable categórico y con nivel de medición ordinal donde su escala de medición es: (Muy buena, Buena, Regular y Mala).

Tabla 2. Distribución de frecuencias sobre Opinión Nivel de seguridad de información bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO

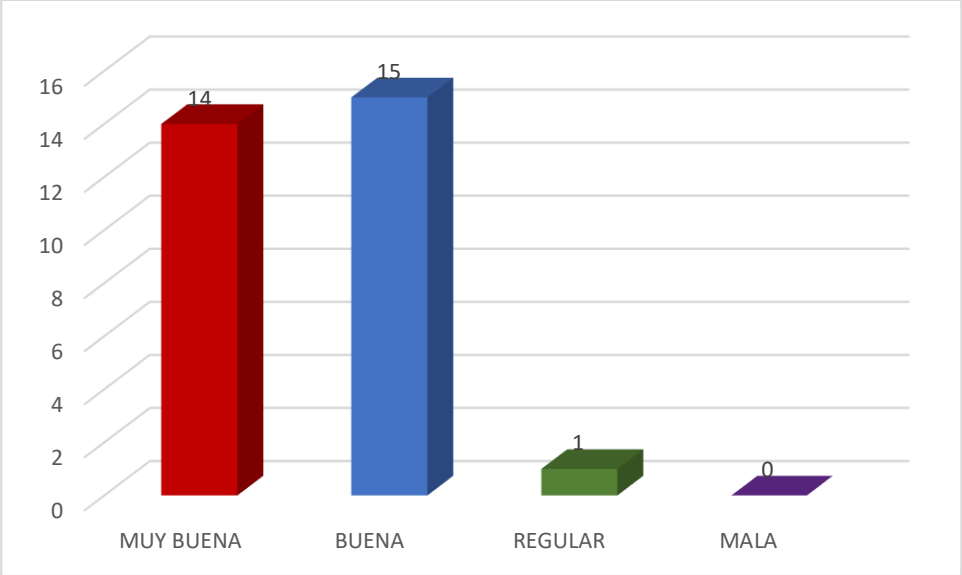
		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	MUY BUENA	14	46,7%	46,7%
	BUENA	15	50,0%	96,7%
	REGULAR	1	3,3%	100,0%%
	MALA	0	0,0%	100,0%
	Total	30	100,0%	

Fuente: Datos obtenidos en la investigación al personal de SENCICO.

Como se observó en la Tabla 02, los participantes en proporción mayoritaria opinaron 50% y 46,7% Buena y Muy buena respectivamente, mientras sólo 3,3% de participantes opinó respecto a nivel de seguridad es Regular; sin embargo, no hubo ningún participante que opinó Mala al nivel de seguridad; con esta información se aseveró que el nivel se seguridad bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO hay garantía y confianza para guardar información. En consecuencia, 96,7% de

participantes garantizan que el nivel se seguridad en el centro de capacitación SENCICO está entre muy buena y Buena.

Figura 2. Descripción de los participantes que respondieron referente a la variable Nivel de seguridad de información bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO



Fuente: Datos obtenidos en la investigación al personal de SENCICO.

Según la figura 02, se observó de los 30 participantes que respondieron según la variable nivel de seguridad, 15 participantes opinaron respecto a nivel de seguridad es Buena mientras 14 participantes opinaron que el nivel de seguridad es Muy bueno, sin embargo, solo un participante opinó que el nivel se seguridad es Regular; mientras ningún participante opinó que el nivel seguridad es Mala. En efecto esta información demostró que el nivel de seguridad en centro de capacitación SENCICO presta seguridad.

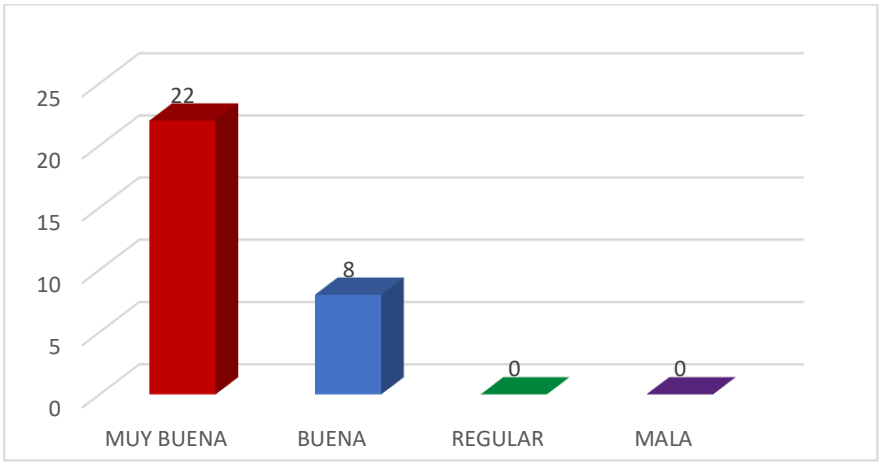
Tabla 3. Distribución de frecuencias sobre Opinión de Identificación de riesgos respecto a Nivel de seguridad de información bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	MUY BUENA	22	73,3%	73,3%
	BUENA	8	26,7%	100,0%
	REGULAR	0	0%	100,0%
	MALA	0	0%	100,0%
	Total	30	100,0%	

Fuente: Datos obtenidos en la investigación al personal de SENCICO

Como se observó en la Tabla 03, los participantes en proporción mayoritaria opinaron 26,7% y 73,3% Buena y Muy buena respectivamente, mientras absolutamente ningún participante opinó respecto a la identificación de riesgos Regular tampoco Mala; en consecuencia, con esta información se afirmó que la identificación de riesgos bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO se está realizando en estricto cumplimiento con las normas bajo la supervisión del personal responsable en esa área.

Figura 3. Descripción de los participantes que respondieron referente a la dimensión Identificación de riesgos respecto a Nivel de seguridad de información bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO



Fuente: Datos obtenidos en la investigación al personal de SENCICO.

Según la figura 03, observó los participantes que respondieron respecto a la dimensión identificación de riesgos referente a nivel de seguridad 22 participantes opinaron Muy bueno; mientras 8 participantes opinaron Bueno el identificacion de riesgos. En efecto, según esta dimensión los participantes opinaron Muy bueno y Bueno sobre identificacion de riesgos teniendo en cuenta nivel se seguridad en el centro de capacitación SENCICO.

Tabla 4. Distribución de frecuencias sobre Opinión de Estimación de riesgo respecto a Nivel de seguridad de información bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO

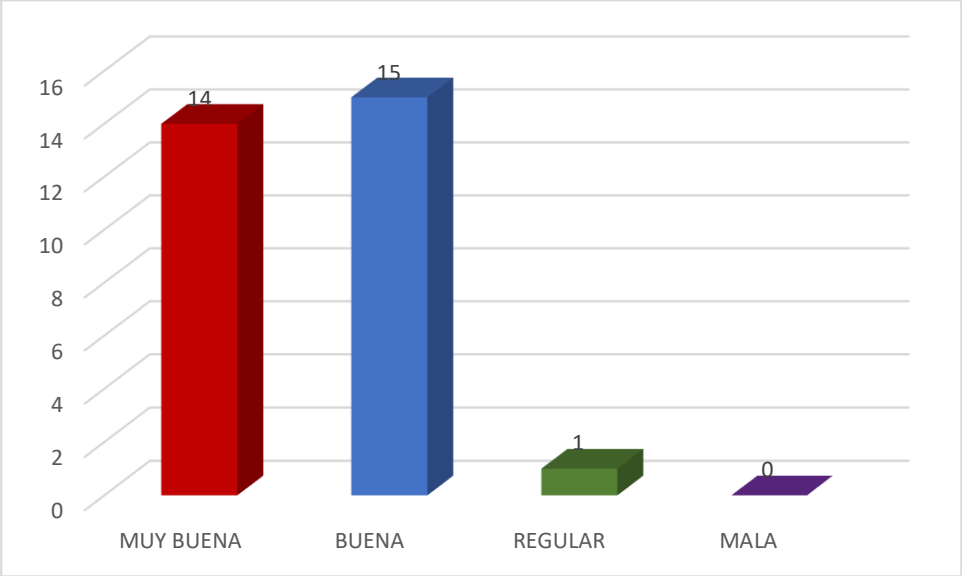
		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	MUY BUENA	14	46,7%	46,7%
	BUENA	15	50,0%	96,7
	REGULAR	1	3,3%	100,0%
	MALA	0	0,0%	100,0%
	Total	30	100,0	

Fuente: Datos obtenidos en la investigación al personal de SENCICO.

Como se observó en la Tabla 04, los participantes en su mayoría opinaron respecto a Estimación de riesgo con opiniones Buena y Muy buena con de 50% y 46,7% respectivamente, mientras solamente 3,3% de participantes opinó respecto a nivel de seguridad es Regular; mientras ningún participante opinó Mala respecto a Estimacion de riesgos; con esta información se constató los Estimación de riesgo bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO están totalmente garantizado la seguridad

de cualquier evento no deseado que puede originar daño a la gente, equipos y materiales.

Figura 4. Descripción de los participantes que respondieron referente a la dimensión Estimación de riesgo respecto a Nivel de seguridad de información bajo la norma ISO/IEC 27001:2013 en el centro de capacitaciones SENCICO



Fuente: Datos obtenidos en la investigación al personal de SENCICO.

Según la figura 04, se observó que los participantes opinaron sobre Estimación de riesgo 15 participantes afirmaron Buena, sin embargo 14 de participantes afirmaron Muy buena, mientras solo un participante opinó es Regular. En efecto, casi un total de participantes afirmaron Muy buen y Buena sobre Estimación de riesgo en el centro de capacitación SENCICO.

RESULTADOS INFERENCIALES, SEGÚN LOS OBEJETIVOS Y LAS HIPÓTESIS.

Objetivo específico (1): Establecer la relación que existe entre la identificación de riesgo, bajo la Norma ISO/IEC 27001:2013 y el identificacion de riesgos

para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018.

Contrastación de hipótesis especifica N° 01

"La relación que existe entre la Guía de Implementación de la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la identificación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, es positivo"

Proponiendo las hipótesis de contraste:

Ho: La relación que existe entre la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la **identificación de riesgo** para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, no es positivo.

Ha: La relación que existe entre la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la **identificación de riesgo** para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, es positivo**.**

Teniendo en cuenta la investigación corresponde al nivel relacional y las dos variables en estudio son: variable asociado y variable de supervisión ambos son categóricos ordinales, se usó el estadístico de prueba correlación de Spearman, cuyos resultados se obtuvo luego de aplicar el programa SPSS versión 23.

Tabla 5. Contraste de Seguridad de información, bajo la Norma ISO/IEC 27001:2013, y la identificación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali 2018.

			Sumatoria de seguridad de información, bajo la Norma ISO/IEC 27001:2013.	Sumatoria de identificación de riesgo
Rho de Spearman	Sumatoria de seguridad de información, bajo la Norma ISO/IEC 27001:2013.	Coeficiente de correlación	1,000	0,894**
		Sig. (bilateral)	.	0,000
		N	30	30
	Sumatoria de la identificación de riesgo	Coeficiente de correlación	0,894**	1,000
		Sig. (bilateral)	0,000	.
		N	30	30

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

De acuerdo a la Tabla 05, se observó que la significación fue de 0.000, valor inferior al nivel de significación propuesto (α = 0.05), por lo que se decidió aceptar la hipótesis alterna, afirmando con 95% de confianza, existe asociación entre las puntuaciones de Seguridad de información, bajo la Norma ISO/IEC 27001:2013, y la identificación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación. Es decir, resultó coherente con el coeficiente de Rho de Spearman que mostró, el grado de asociación entre estas dos variables fue 0.894, Según Hernández Sampieri (Metodología de Investigación Capitulo 10 análisis de datos pág. 312), esto significó la intensidad o grado de asociación positiva o directa de moderada a muy buena, es decir cada vez que aumenta la puntuación de Seguridad de información, bajo la Norma ISO/IEC 27001:2013, puntuación de la identificación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación también aumentó en forma positiva de moderada a muy buena siempre.

Objetivo específico (2): Establecer la relación que existe entre la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la estimación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018

Contrastación de hipótesis especifica N° 02

"La relación que existe entre la Guía de Implementación de la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la estimación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, es positivo".

Proponiendo las hipótesis de contraste:

Ho: La relación que existe entre la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la estimación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, no es positivo.

Ha: La relación que existe entre la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la estimación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, es positivo.

Tabla 6. Contraste de Seguridad de información, bajo la Norma ISO/IEC 27001:2013, y la estimación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali 2018.

			Sumatoria de seguridad de información, bajo la Norma ISO/IEC 27001:2013.	Sumatoria de estimación de riesgo
Rho de Spearman	Sumatoria de seguridad de información, bajo la Norma ISO/IEC 27001:2013.	Coeficiente de correlación	1,000	0,659**
		Sig. (bilateral)	.	0,000
		N	30	30
	Sumatoria de la estimación de riesgo	Coeficiente de correlación	0,659**	1,000
		Sig. (bilateral)	0,000	.
		N	30	30

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

De acuerdo a la Tabla 06, los resultados fueron similares que el objetivo específico N° 01, la significación fue de 0.000, valor inferior al nivel de significación propuesto (α = 0.05), por lo que se decidió aceptar la hipótesis alterna y rechazar la hipótesis nula, afirmando con 95% de confianza existe asociación entre las puntuaciones de Seguridad de información, bajo la Norma ISO/IEC 27001:2013, y la estimación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación. También, resultó coherente con el coeficiente de Rho de Spearman que mostró el grado de asociación entre estas dos variables 0.659, Según Hernández Sampieri, esto significa grado de asociación positiva o directa moderada, es decir cada vez que aumentó la puntuación de Seguridad de información, bajo la Norma ISO/IEC 27001:2013, puntuación de la estimación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación también aumentó en forma positiva moderada siempre.

Objetivo General, Determinar la relación entre la seguridad de información, basada

en la Norma ISO/IEC 27001:2013 y el Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018.

Así mismo el planteamiento de hipótesis general entre los variables, la seguridad de información, basada en la Norma ISO/IEC 27001:2013 y el Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, es positivo

Proponiendo las hipótesis de contraste:

Ho: No existe relación entre la seguridad de información, basada en la Norma ISO/IEC 27001:2013 y el Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, de manera positiva.

Ha: Existe relación entre la seguridad de información, basada en la Norma ISO/IEC 27001:2013 y el Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, de manera positiva.

Tabla 7. Contraste de Seguridad de información, bajo la Norma ISO/IEC 27001:2013, y el Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali 2018.

			Sumatoria de seguridad de información, bajo la Norma ISO/IEC 27001:2013.	Sumatoria de Nivel de seguridad
Rho de Spearman	Sumatoria de seguridad de información, bajo la Norma ISO/IEC 27001:2013.	Coeficiente de correlación	1,000	0,819**
		Sig. (bilateral)	.	0,000
		N	30	30
	Sumatoria de Nivel de seguridad	Coeficiente de correlación	0,819**	1,000
		Sig. (bilateral)	0,000	.
		N	30	30

De acuerdo a la Tabla 03, la significación fue de 0.000, valor inferior al nivel de significación propuesto (α = 0.05), por lo que se decidió aceptar la hipótesis alterna y rechazar la hipótesis nula, afirmando con 0.05 de probabilidad de error, existe asociación de relación positiva entre las puntuaciones de Seguridad de información, bajo la Norma ISO/IEC 27001:2013 y el Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018.

Además, el coeficiente de Rho de Spearman que muestra el grado de asociación entre estas dos variables 0.819, Según Hernández Sampieri, esto significó grado de asociación positiva o directa de moderada a muy buena, es decir cada vez que aumentó la puntuación de Seguridad de información, bajo la Norma ISO/IEC 27001:2013, también aumentó las puntuación del Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018 de manera positiva o directa de moderada a muy buena siempre.

4.2. Discusión

Cuando se determinó el nivel de asociación que existe entre la seguridad

de información, bajo la Norma ISO/IEC 27001:2013 y el Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018 se evidenció que hubo coeficiente de asociación positiva de moderado a muy buena, esto demuestra el nivel de seguridad en los sistemas de información del centro de capacitación SENCICO proporciona garantía para las empresas que puedan aplicar estas normas, también considerando otros estándares de seguridad pueda complementar, de esta manera para mayor consistencia e integral y tal como lo observó Daniel Santos (2016) aportando con establecimiento, implementación, mantenimiento y mejora de un sistema de seguridad de la información consideró que el estándar 27001 se complementa con otros estándares de la ISO que explican a mayor detalle cómo se puede cumplir con sus requisitos. Por otra parte también se demostró que existe una asociación y su grado de intensidad es positiva moderada las dimensiones: la identificación de riesgo para apoyar la seguridad en los sistemas de información del objetivo específico 01 y los la estimación de riesgo para apoyar la seguridad en los sistemas de información del objetivo específico 02, estas afirmaciones adicionalmente pueda ser lucrativos específicamente para empresas privadas que prestan servicio en capacitar al personal y además a empresas dedicadas a auditorias de sistema de gestión, teniendo coherencia con lo obtenido por Tola (2015) en su tesis titulada "implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001", fue realizado en la empresa A & C Group SA dedicada al rubro de Auditoria, implementó un sistema de gestión de seguridad de información tomando como base el estándar ISO 27001:20005; y adicionalmente se tuvo mínimas diferencias en estas dos dimensiones en cuanto a su intensidad de asociación en efecto debería implementarse en las instituciones públicas y privadas tal como indica NTP ISO/IEC 27001:2014 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información, Norma técnica peruana de requisitos para implementar un SGSI que es una traducción del estándar ISO/IEC 27001:2013 [02], razón por la cual cambia mucho respecto a la versión precedente (2008), actualmente se encuentra vigente y es de cumplimiento obligatorio para las entidades del estado peruano, por resolución aprobada por la Presidencia del Consejo de Ministros

(PCM). Las entidades privadas pueden tomarlo como marco referencial. Así mismo la correcta implementación de un SGSI dentro de las empresas, ayudará a prevenir estimacion de riesgos, que generan pérdidas económicas e interrupciones en la continuidad del negocio, mediante la reducción de las probabilidades o impactos que los riesgos identificados pudieran ocasionar a su información. De esta manera las empresas puedan brindar servicios con seguridad y garantía, es decir las informaciones que tienen estarían seguros de cualquier riesgo de pérdida, copias, alteraciones o cambios. En ese sentido el acrónimo de evaluación de las amenazas, activos y vulnerabilidades operacionalmente críticas (OCTAVE, por sus siglas en inglés). Contiene una metodología de análisis de riesgo desarrollada por Computer Emergency Response Team (CERT), enfocada en el estudio de riesgos para organizaciones pequeñas. La evaluación parte de la identificación de activos relacionados con la información, para identificar amenazas y vulnerabilidades, a partir de los cuales se pueden determinar riesgos de seguridad de información. A partir de estos resultados se plantean estrategias y planes, para mitigar los riesgos identificados.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Se concluye lo siguiente:

- Existió una asociación entre Seguridad de información, bajo la Norma ISO/IEC 27001:2013 y Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018. En efecto Cada vez que aumenta la puntuación Seguridad de información aumenta en forma positiva o directa de moderada a muy buena, puntuación de Nivel de seguridad en los sistemas de información siempre, porque así se arrojó los datos. Es decir, el coeficiente de Rho de Spearman fue 0.819.

- Existió una asociación entre Seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la identificación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO. En consecuencia, sí aumenta la puntuación Seguridad de información aumenta en forma positiva o de moderada a muy buena, puntuación de la identificación de riesgo para apoyar la seguridad en los sistemas de información constantemente, ya que los resultados fueron obtenidos el coeficiente de Rho de Spearman fue 0.894.

- Existió una asociación entre Seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la estimación de riesgo para apoyar la seguridad en los sistemas de información del centro de capacitación SENCICO. En

- consecuencia, cada vez que varía en forma positiva puntuación de Seguridad de información aumenta en forma positiva o moderada, puntuación de la estimación de riesgo para apoyar la seguridad en los sistemas de información permanente, ya que los resultados fueron obtenidos como el coeficiente de Rho de Spearman fue 0.659.

5.2. Recomendaciones

Se recomienda lo siguiente:

- A SENCICO se le sugiere incidir en las capacitaciones de su personal para seguir manteniendo un buen nivel de seguridad de información y el cumplimiento de las normas.

- SENCICO debe seguir capacitando a su personal y alumnos sobre manejo de información, cumplimiento de normas y nivel de seguridad de información para seguir brindado un servicio de calidad.

- A los investigadores se les sugiere ampliar más en temas de área de diseño de redes dentro de SENCICO.

REFERENCIAS BIBLIOGRÀFICAS

ADVISERA (2019). *¿Qué es norma ISO 27001?* Recuperado de https://advisera.com/27001academy/es/que-es-iso-27001.

Andrade, J. C., y Chávez, C. E. (2018). *Generación de un plan para la gestión integral de seguridad de la información basado en el marco de la norma ISO 27001 y las mejores prácticas de seguridad de la norma ISO 27002 para la compañía international Gym Ecuaintergym S.A.* de la ciudad de Guayaquil. Tesis. Recuperado a partir de http://repositorio.ug.edu.ec/handle/redug/32606

Belmonte, M (2016). "*Sistemas de Gestión de seguridad*". Recuperado de https://www.coursehero.com/file/p7s5qtu/La-existencia-de-ciertos-procesos-y-el-uso-de-servicios-en-la-nube-facilit%C3%B3/

Carlos Franco (7 de mayo del 2012), *COBIT 5- seguridad de información*. Recuperado de http://cafrancavilla.wordpress.com/

Diana, E. 2015, *"Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001*". Recuperado de http://www.dspace.espol.edu.ec/xmlui/handle/123456789/31114

Diego, E, (2016), "*Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software"*. Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/7616

ESAN (4 de abril del 2016), NTP ISO/IEC 17799:2007. Recuperado de https://www.esan.edu.pe/apuntes-empresariales/2016/04/norma-técnica-peruana-políticas-procedimientos-seguridad-información/.

Espinoza, P. (13 de marzo del 2013), *Marco Risk IT para la gestión de TI relacionadas a riesgos del negocio*. Recuperado de https://pamela7913.wixsite.com/pamvic/risk-it/.

Fernández, A (2 de junio de 2016), *OCTAVE – Allegro*. Recuperado de https://calidadengestiondeproyectos.com/el-analisis-riesgo-de-octave-allegr.

Horna, C. (2014). NTP-ISO/IEC 27001:2014 *Técnicas de Seguridad. Sistemas de gestión de seguridad.* Recuperado de https://www.inacal.gob.pe/inacal/files/27001-Carlos_Hornafinal.pdf

ISOTools (2019). "*Sistemas de Gestión de Seguridad de Información*". Recuperado de https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion.

Laudon, K. C, y Laudon J. P. (2012). *Sistemas de Información Gerencial. Naulcalpan de Juares*, México.

Magerit Versión 3 (7 de mayo del 2012*), MAGERIT VERSION 3*. Recuperado de https://www.um.es/docencia/barzana/GESESI/GESESI-Metodo-MAGERIT.

NovaSec (2021). ¿Qué es la gestión de activos de información?. Recuperado de: https://www.novasec.co/blog/67-gestion-de-activos-de-informacion

Robin. J y Salcedo. B (2014) *"Plan de implementación del SGSI".* Recuperado de https://pdfslide.tips/documents/plan-de-implementacin-del-sgsi-basado-en-la-documental-del-sistema-de-gestin.html.

Santos, D. E. (2016). *Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software*. Recuperado de: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/7616/SANTOS_DANIEL_SISTEMA_GESTI%c3%93N.pdf?sequence=1&isAllowed=y

SENCICO (2016). *Manual de Organización y Funciones – MOF de SENCICO. Aprobado con Resolución de Presidencia Ejecutiva N° 44-2016-02.00 de fecha 25m de abril del 2016*. Lima-Perú

Tola, D. E. (2015), *"Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001*". Recuperado de http://www.dspace.espol.edu.ec/xmlui/handle/123456789/31114

ANEXOS

Anexo 01: Matriz de consistencia

"SEGURIDAD DE INFORMACIÓN BASADA EN LA NORMA ISO / IEC 27001:2013 Y NIVEL DE SEGURIDAD EN EL CENTRO DE CAPACITACIÓN SENCICO UCAYALI, 2018"

<table>
<tr><th>Problema General</th><th>Objetivo General</th><th>Hipótesis General</th><th colspan="2">Variables / Dimensiones</th><th>Metodología</th></tr>
<tr><td>¿Qué relación existe entre la seguridad de información, basada en la Norma ISO/IEC 27001:2013. y el Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018?</td><td>Determinar la relación entre la seguridad de información, basada en la Norma ISO/IEC 27001:2013. y el Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018.</td><td>La relación entre la seguridad de información, basada en la Norma ISO/IEC 27001:2013. y el Nivel de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, es positivo.</td><td rowspan="3">Seguridad de información, basada en la Norma ISO/IEC 27001:2013</td><td>Organización de la seguridad de información.</td><td rowspan="4">Tipo de investigación
Aplicada

Nivel de investigación
Descriptivo
Correlacional

Diseño de investigación
No Experimental

Población y Muestra:
30 personas

Fuente
Primaria

Técnicas
Encuesta

Instrumento
Cuestionario</td></tr>
<tr><th>Problemas específicos</th><th>Objetivos Específicos.</th><th>Hipótesis Específicas</th><td rowspan="2">Cubrimiento del SGIS en activos de información.</td></tr>
<tr><td>a. ¿Cuál es la relación que existe entre la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la identificación de riegos en la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018?

b. ¿Cuál es la relación que existe entre la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la estimación de riesgos en la seguridad para apoyar la seguridad en los sistemas de información del centro de capacitación</td><td>a. Establecer la relación que existe entre la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la identificación de riegos de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018

b. Establecer la relación que existe entre la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la estimación de riegos de la seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018.</td><td>a. La relación que existe entre la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la identificación de riegos de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, es positivo.

b. La relación que existe entre la seguridad de información, bajo la Norma ISO/IEC 27001:2013 y la estimación de riegos de seguridad en los sistemas de información del centro de capacitación SENCICO de Ucayali, 2018, es positivo.</td><td rowspan="2">Nivel de seguridad</td><td>Identificación de riesgo</td></tr>
<tr><td></td><td></td><td></td><td>Estimación de riesgo</td><td></td></tr>
</table>

Anexo 03: Validación del Instrumento

Anexo 02: validación de Instrumentos

"SEGURIDAD DE INFORMACIÓN BASADA EN LA NORMA ISO / IEC 27001:2013 PARA APOYAR LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN DEL CENTRO DE CAPACITACIÓN SENCICO UCAYALI, 2018"

Variables	Dimensiones	Indicadores	Ítems	Opción de respuesta				Criterio de evaluación								
				MUY BUENA	BUENA	REGULAR	MALA	Relación entre la variable y la dimensión		Relación entre la dimensión y el indicador		Relación entre el indicador y el ítem		Relación entre el ítems y la opción de respuesta		Observación y/o recomendación
								SI	NO	SI	NO	SI	NO	SI	NO	
Seguridad de información bajo la norma ISO/IEC 27001:2013	Organización de seguridad de la información.	Evaluación de desempeño.	1		X			X		X		X		X		
		Nivel de capacitaciones.	2			X		X		X		X		X		
	Cumplimiento del SGSI en activos de información.	Numero de activos fijos.	3		X			X		X		X		X		
		Inventario de activos.	4		X			X		X		X		X		
Nivel de seguridad	Identificación de riesgos	Primario.	5	X				X		X		X		X		
		Soporte	6	X				X		X		X		X		
	Estimación de riegos	Probabilidad	7		X			X		X		X		X		
		Impacto	8		X			X		X		X		X		

FIRMA DEL VALIDADOR

Mg. Juan Carlos Guillermo Lazaro

Anexo 02: validación de Instrumentos

"SEGURIDAD DE INFORMACIÓN BASADA EN LA NORMA ISO / IEC 27001:2013 PARA APOYAR LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN DEL CENTRO DE CAPACITACIÓN SENCICO UCAYALI, 2018"

Variables	Dimensiones	Indicadores	Ítems	Opción de respuesta				Criterio de evaluación								Observación y/o recomendación
				MUY BUENA	BUENA	REGULAR	MALA	Relación entre la variable y la dimensión		Relación entre la dimensión y el indicador		Relación entre el indicador y el ítem		Relación entre el ítems y la opción de respuesta		
								SI	NO	SI	NO	SI	NO	SI	NO	
Seguridad de información bajo la norma ISO/IEC 27001:2013	Organización de seguridad de la información.	Evaluación de desempeño.	1	X				X		X		X		X		
		Nivel de capacitaciones.	2	X				X		X		X		X		
	Cumplimiento del SGSI en activos de información.	Numero de activos fijos.	3		X			X		X		X		X		
		Inventario de activos.	4		X			X		X		X		X		
Nivel de seguridad	Identificación de riesgos	Primario.	5	X				X		X		X		X		
		Soporte	6		X			X		X		X		X		
	Estimación de riegos	Probabilidad	7	X				X		X		X		X		
		Impacto	8		X			X		X		X		X		
		Seguridad														

FIRMA DEL VALIDADOR

Dr. Lida Maribel Cosme Solano

DNI 42922609

Anexo 02: validación de Instrumentos

"SEGURIDAD DE INFORMACIÓN BASADA EN LA NORMA ISO / IEC 27001:2013 PARA APOYAR LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN DEL CENTRO DE CAPACITACIÓN SENCICO UCAYALI, 2018"

Variables	Dimensiones	Indicadores	Ítems	Opción de respuesta				Criterio de evaluación								Observación y/o recomendación
				MUY BUENA	BUENA	REGULAR	MALA	Relación entre la variable y la dimensión		Relación entre la dimensión y el indicador		Relación entre el indicador y el ítem		Relación entre el ítems y la opción de respuesta		
								SI	NO	SI	NO	SI	NO	SI	NO	
Seguridad de información bajo la norma ISO/IEC 27001:2013	Organización de seguridad de la información.	Evaluación de desempeño.	1		X			X		X		X		X		
		Nivel de capacitaciones.	2		X			X		X		X		X		
	Cumplimiento del SGSI en activos de información.	Numero de activos fijos.	3		X			X		X		X		X		
		Inventario de activos.	4		X			X		X		X		X		
Nivel de seguridad	Identificación de riesgos	Primario.	5		X			X		X		X		X		
		Soporte	6		X			X		X		X		X		
	Estimación de riegos	Probabilidad	7		X			X		X		X		X		
		Impacto	8		X			X		X		X		X		

FIRMA DEL VALIDADOR

Dr. Walter A. Quispe Cutipa

DNI 05313398

CONFIABILIDAD DEL INSTRUMENTO

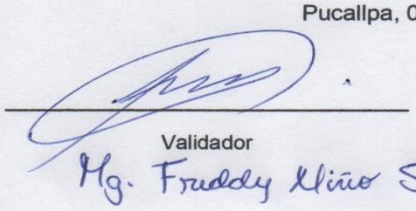
Variable: Nivel de Seguridad

Nombre de la prueba de confiabilidad	
Alfa de Cronbach	**Ítems**
0,917	4

Fuente: Propia, aplicando el programa SPSS V22.0

Interpretación: El Estadístico de fiabilidad de Alfa de Cronbach aplicada al instrumento de investigación arrojo 0,917, por ende, el instrumento es altamente confiable para la investigación por el resultado que arrojó.

Pucallpa, 05 de noviembre de 2019.



Validador

Mg. Freddy Niño Soto

3

Anexo 03: Confiabilidad de los instrumentos

CONFIABILIDAD DEL INSTRUMENTO

Variable: Seguridad de la Información bajo la Norma ISO/IEC 27001:2013

Nombre de la prueba de confiabilidad	
Alfa de Cronbach	**Ítems**
0,917	4

Fuente: Propia, aplicando el programa SPSS V22.0

Interpretación: El Estadístico de fiabilidad de Alfa de Cronbach aplicada al instrumento de investigación arrojo 0,917, por ende, el instrumento es altamente confiable para la investigación por el resultado que arrojó.

Pucallpa, 05 de noviembre de 2019.

Validador

Mg. Freddy Niño Soto

1

Anexo N° 05

Instrumento de la investigación

Escuela Profesional de Ingeniería de Sistemas

"SEGURIDAD DE INFORMACIÓN BASADA EN LA NORMA ISO/IEC 27001:2013 Y NIVEL DE SEGURIDAD EN EL CENTRO DE CAPACITACIÓN SENCICO DE UCAYALI, 2018."

Encuesta

VV1	**1.- ¿Cómo evaluarías tu desempeño en el cumplimento de tu puesto dentro de SENCICO?** **a) Muy Buena b) Buena c) Regular d) Mala**
	2.- ¿Qué opinión tiene usted sobre la capacitación recibida para la utilización de nuevos programas? **a) Muy Buena b) Buena c) Regular d) Mala**
	3.- ¿Cómo calificaría los activos críticos de información dentro de SENCICO? **a) Muy Buena b) Buena c) Regular d) Mala**
	4.- ¿Cómo calificarías el inventario de activos de información dentro de SENCICO? **a) Muy Buena b) Buena c) Regular d) Mala**

VV2	**5.- ¿Cómo evaluarías los activos de información primarios dentro de SENCICO?** **a) Muy Buena b) Buena c) Regular d) Mala**
	6.- ¿Cómo evaluarías el soporte dado a los activos de información dentro de SENCICO? **a) Muy Buena b) Buena c) Regular d) Mala**
	7.- ¿Cómo calificaría la posibilidad que ocurra un riesgo dentro de SENCICO? **a) Muy Buena b) Buena c) Regular d) Mala**
	8.- ¿Cómo calificarías el impacto de eventuales riegos dentro de SENCICO? **a) Muy Buena b) Buena c) Regular d) Mala**

ANEXO N° 06 CUADRO DE BASE DE DATOS

ID	Seguridad de la información, bajo la Norma ISO/IEC 27001:2013.				V1	Nivel de seguridad.					
	Evaluación de desempeño	Nivel de capacitación	Activos críticos de información	Inventario de activos		Primario	Soporte	V2 D1	Probabilidad	Impacto	V2D2
1	2	3	2	2	9	2	3	5	3	3	6
2	3	1	1	2	7	2	2	4	2	1	3
3	3	2	2	2	9	2	3	5	2	2	4
4	2	2	2	2	8	2	3	5	2	2	4
5	2	2	2	1	7	2	2	4	1	2	3
6	2	3	3	3	11	2	3	5	2	3	5
7	3	2	3	3	11	2	3	5	2	2	4
8	2	2	3	2	9	2	3	5	2	2	4
9	3	3	2	3	11	3	3	6	3	2	5
10	3	3	3	3	12	3	3	6	3	3	6
11	2	3	2	2	9	2	3	5	3	2	5
12	3	3	3	2	11	2	3	5	2	2	4
13	3	2	2	2	9	2	3	5	2	3	5
14	2	2	2	2	8	2	2	4	2	2	4
15	2	2	1	3	8	2	2	4	2	2	4

16	2	3	2	3	10	2	3	5	2	3	5	10
17	3	2	3	3	11	2	3	5	2	2	4	9
18	2	2	2	2	8	2	2	4	3	2	5	9
19	3	3	3	3	12	3	3	6	3	3	6	12
20	3	3	3	3	12	3	3	6	3	3	6	12
21	2	3	1	2	8	2	2	4	2	2	4	8
22	3	2	3	2	10	2	3	5	2	2	4	9
23	3	3	2	2	10	2	3	5	2	3	5	10
24	2	2	1	1	6	2	2	4	1	0	1	5
25	2	2	2	3	9	2	3	5	2	2	4	9
26	2	3	3	3	11	2	3	5	3	3	6	11
27	3	2	1	1	7	2	2	4	2	1	3	7
28	2	2	3	3	10	2	3	5	3	2	5	10
29	3	3	3	3	12	3	3	6	3	3	6	12
30	3	3	3	3	12	3	3	6	2	2	4	10
								0.8844 0625			0.709707	