UNIVERSIDAD JOSÉ CARLOS MARIÁTEGUI

VICERRECTORADO DE INVESTIGACIÓN

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

PLAN DE GESTIÓN DE LA CALIDAD PARA MEJORAR LA ESTRATEGIA DE SEGURIDAD Y AUDITORÍAS INFORMÁTICAS EN LOS CENTROS DE EDUCACIÓN TÉCNICO PRODUCTIVA (CETPRO) PARTICULARES DE ENSEÑANZA DE COMPUTACIÓN EN LA CIUDAD DE ILO – 2016

PRESENTADO POR:

BACH. RUSO ALEXANDER MORALES GONZALES

ASESOR:

MGR. NILTON JUAN ZEBALLOS HURTADO

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA, CON MENCIÓN EN SEGURIDAD Y AUDITORÍA INFORMÁTICA

MOQUEGUA – PERÚ

2019

ÍNDICE DE CONTENIDO

CAPÍTULO III: MÉTODO

CAPÍTULO IV: PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Esta investigación muestra temas de las áreas de *gestiones tanto de la seguridad informática como de la calidad*. Expone la problemática de las deficiencias de las estrategias de los *Centros de Educación Técnico Productiva* privados (en adelante sólo llamado CETPRO) de enseñanza de computación de la ciudad de Ilo respecto a la seguridad y auditorías informáticas. Emplea siete etapas como parte del diseño de investigación, y como solución se utilizó la norma técnica peruana ISO 27001:2014, a su vez esta norma fue implantada por el método de Rincón (2002). Se hizo una labor de campo en beneficio de los *CETPROS* privados de la ciudad de Ilo. Se redactó y entregó un *plan de gestión de la calidad* dónde están los detalles a favor de mejorar la estrategia de seguridad y auditorías informáticas. Para medir los planes de gestión de la calidad y las estrategias de seguridad y auditorías informáticas, se adaptó dos cuestionarios existentes en la literatura; luego se buscó a dos expertos adicionales para la validación correspondiente. Se siguió un diseño experimental la cual dividió en dos a la población de estudio, logrando así un grupo experimental y uno de control, luego se ejecutaron pruebas antes y después, la data obtenida se depuró con el software de estadística *SPSS*, finalmente se interpretaron los datos dando las conclusiones de la tesis.

Palabras claves: Seguridad informática. ISO 27001. Gestión de la calidad. CETPRO

ABSTRACT

This research shows topics from the areas of management of both computer security and quality. It exposes the problematic of the deficiencies of the strategies of the private Technical Productive Education Centers (hereinafter called only CETPRO) of computer teaching of the Ilo city regarding security and computer audits. It uses seven stages as part of the research design, and as a solution the Peruvian technical standard ISO 27001: 2014 was used, in turn this standard was implemented by the Rincón method (2002). Field work was done to benefit the private CETPROS of the Ilo city. A quality management plan was drafted and delivered where the details are in favor of improving the security strategy and computer audits. To measure the quality management plans and the security strategies and computer audits, two existing questionnaires were adapted in the literature; then two additional experts were sought for the corresponding validation. An experimental design was followed which divided the study population into two, thus achieving an experimental group and a control group, then tests were performed before and after, the data obtained was purified with the statistical software SPSS, finally the data giving the conclusions of the thesis.

Keywords: Computer security. ISO 27001. Quality management. CETPRO.

INTRODUCCIÓN

La tesis recolecta información respecto a los *planes de gestión de la calidad* de la ISO9001 y de la ISO27001, y los orienta hacia la seguridad y auditorias informáticas de los *CETPROs* de enseñanza de computación para poder influenciar y mejorar la débil estrategia de seguridad informática que los CETPROs actualmente tienen. La ubicación en donde tuvo lugar la investigación fue en puerto de Ilo, departamento de Moquegua, y estuvo llevada a cabo por el bachiller Ruso Alexander Morales Gonzales como formalismo del proceso de la obtención del grado académico de maestro en ingeniería de sistemas e informática. Este documento contiene en total cinco capítulos, el primer capítulo explica la problemática y definición del problema, también se ahonda los objetivos, las hipótesis y variables. El segundo capítulo muestra el marco teórico, se encontrará los antecedentes, y la disgregación de las dos variables de estudio. Un tercer capítulo titulado *método*, allí muestra toda la metodología científica empleada. El capítulo número cuatro manifiesta todos los resultados obtenidos y da el análisis de ellos. Finalmente, el quinto capítulo titulado *conclusiones*, en ella también se dan las recomendaciones. Este documento cierra con las referencias a las citas bibliográficas y todos los anexos correspondientes.

El autor

CAPÍTULO I:

EL PROBLEMA DE LA INVESTIGACIÓN

1.1. Descripción de la realidad problemática

La empresa encuestadora GSISS (Global State of Information Security Survey) en el 2011 explicó que todas las instituciones que ellos han encuestado manifestaron que el 20% no saben sobre los accidentes, circunstancias, incidentes, sucesos o simulares que pasan dentro de la empresa en temas de seguridad informática y de la información que ocurrieron en el último año. Otra empresa encuestadora como la SSMBIPS (Symantec) en el 2010 contaron que hay un 49% de caídas en el flujo da datos en los servidores de las instituciones investigadas, muchos de estos datos que ellos informan son la manifestación de supuestos ataques cibernéticos, pero que a certeza no se tiene bien definidas las causas de ellos, quizá se pueda deber a razones que de contar con planes de seguridad pudieron preverse según informan Symantec. La Asociación de académica denominada ACIS (Asociación Colombiana de Ingenieros de Sistemas) en el 2010 informaron a los medios web que la barrare que se tiene que sobre pasar esa encausada en la alta

gerencia de cada institución, ya que son ellos los que desmerecen los nuevos aportes, e inclusive destinan fondos a otras áreas de menos interés, aproximadamente más de un 15% es por la casi nulo apoyo y empuje de los directivos en la cúspide empresarial, hay un 18% aproximadamente de las causas estudiadas que recae en que simplemente los profesionales que están trabajando en el área de sistemas no entiendes sobres tópicos muy elevados en seguridad de la información, seguridad electrónico o similares. La GSISS (2011) argumentaron que en Sudamérica cerca del 33% de las instituciones, empresas, organizaciones, pymes, etc., cuentan con registro tipo inventarios en donde se señale todas las características, distribución, propiedades, e importancia del hardware y software importante para la empresa porque allí se guardan los datos más valiosos para ellos, es decir hay más de un 66% de instituciones en en continente sudamericano que no les importa ni saben dónde se guardan sus datos para procesar. Una vez más Symantec (2010) explica que hay más de un 47% de instituciones que se dedican a cualquier ámbito económico que jamás en su existencia hicieron resguardo de información por medio de backup o copias de resguardo, esto último es muy lamentable ya que, de perderse la data, las perdidas pueden ser múltiples e incluso la bancarrota de la empresa en ejecución. La revista PC World en el 2011 hablaron sobre ciberseguridad y en ella se comentó por medio de varias páginas que en el mundo hay muchas empresas dedicadas al desarrollo, venta y distribución de programas informáticos espías, pero que estos son destinados para la ejecución de medidas de seguridad en empresas y organismos vinculadas al gobierno de los países del mundo, pero se presume que muchos de estos software que solamente

deberían ser de uso militar o gubernamental se filtran en el mercado negro y pasan a manos privadas para fines competitivo ocultos.

Sobre la gestión de la calidad Ruiz-Canela (2004) explica tener un plan de gestión sea de lo que sea, desde la calidad, pasando por lo ambiental hasta llegar a lo informático, siempre presenta mejorar la oportunidad competitiva, es decir el cliente se beneficia de un plan de la calidad. Bañeras (2014), argumenta que la carencia de calidad en la administración o gestión es contraproducente para cualquier institución y porque produce un aumento de la *espontaneidad* dentro de nuestros procesos, se debería acarrear procesos completamente administrados y planificados de los que se tenga conocimiento de cada instante la forma de interactuar en circunstancias normales y condiciones recomendables en el funcionamiento. Los autores Piattini & Del Peso (2001) explican que las compañías invierten monumentales montos recursos financieros y de tiempo en adquirir, programar o desarrollar sistemas informáticos que ofrezca la más alta calidad posible, es por eso que los temas relacionados con auditoría informática atesoran más notabilidad. Piattini & Del Peso (2001) dicen la calidad se vincula se quiere o no se quiera con la seguridad informática, ya que en la actualidad todas las empresas grandes, medianas, pequeñas, y micros usan, mantiene, administran y se ayudan de computadoras. Los autores Piattini & Del Peso (2001) explican que la eficacia y calidad es un acumulado de medidas y acciones a salvaguardar y resguardar la información de la empresa.

El consultor Portantier (2012) comenta que se necesita tener políticas y documentos diversos para con la seguridad informática, pero estos documentos deben contar con una visión que va desde la alta administración y asentándose por completo por niveles organizativos más bajos. Portantier (2012) indica que en los niveles más elevados de la organización será menos complejo pero que a medida se va bajando en la pirámide institucional la complejidad o dificultad ira en ascenso. La BSI (Institución de estandarización británica) en el 2011 explico sobre la importancia de emplear formas estructuradas de acción para dar calidad, y para esta tesis esas palabras calzan muy bien ya que daremos calidad por medio de la ISO27001 que es un estándar como los que defiende la BSI, el famoso autor de artículos en ciberseguridad Alvarez en el 2013 habló que todos los profesionales y en especial los que están ligados a la enseñanza de informática deben de saber, manejar y dominar herramientas como software y hardware para proteger los activos en donde se resguardan la información. En nuestro país partiendo desde las escuelas primarias, secundarias, academias, institutos, y universidades los docentes solo enseñan los cursos asignados, pero muy poco lo vinculan a temas como la seguridad informática.

Panda Security, The Cloud Security Company (2013), hizo un estudio de seguridad informática en colegios americanos, donde se han dado prácticas de seguridad del tema; se descubrió que el 63% de los centros educativos han sufrido problemas derivados de infecciones de malware dos veces al año en media, también se descubrió que el personal de tecnología pasa el 38% de su tiempo a la semana

desinfectando de virus y otras amenazas informáticas sus sistemas; el 21% confirma que esta tarea es diaria; el 90% de las escuelas tienen antivirus o antimalware, pero cerca del 25% no cuentan con firewalls. En el puesto sureño de Ilo no existen investigaciones o información de fuentes académicas que expliquen con características y altos detalles la inseguridad informática de las instituciones educativas no universitarias; pero por la labor y experiencia reunida del tesista de este documento que para el año vigente (20190) reúne más de nueve años de labor docente en colegios, academias, institutos y universidades, logra declarar que las dificultades más evidentes tanto para los escolares, alumnos y universitarios y como también para las instituciones académicas universitarias y no universitarias son las sustracciones de contraseñas, software malicioso que da como consecuencia lentitud de la red, desperfectos de las computadoras, gasto de recursos y tiempo en reparaciones cotidianas, en gran mesura se alcanza aplicar el inventario que el experto Roa (2013) proporciona sobre las tipologías de agresiones que las compañías logran sobrellevar en los típicos ataques informáticos, para mencionar sólo algunos como la denegación de servicios, las interceptaciones de datos, el hombre en el medio, búsqueda de claves por fuerza bruta, búsquedas inteligentes, virus y troyanos. Asimismo las fundaciones educativas del puerto ileño serían torturadas y victimas por las deficientes estrategias de seguridad y auditorias informáticas porque en la actualidad desconocen la importancia de tener planeado y documentado las estrategias de seguridad informáticas con procedimientos documentados, un manual de calidad ajustado a la institución, lista coherente de objetivos de calidad y una clara política de calidad y demás temas secundarios y subtemas necesarios (normas, protocolos, estándares, directivas) Portantier (2012)

reveló otros tipos de documentos que las sociedades empresariales están abandonando de tener en relación a la seguridad informática, como son *procedimientos*, *estándares* y *políticas*; aclara también el consultor que la seguridad informática tiene mucho que ver con las *responsabilidades*, la *planeación* y la *protección*; por ello se vislumbra que las irresponsabilidades, los malos planes, y las protecciones parciales para los CETPROS privados de enseñanza de computación de la ciudad de Ilo ocasionarían la lista de Bañeras (2014) da a falta de un *plan de gestión de la calidad*, según él los percances, el colapso económico, institucional, credibilidad, imagen pueden desplomarse con completo, al inicio sería el aumento de precios en los servicios que se brindan o lo productos que se ofrecen, luego, existiría una mala imagen que se traduce en un boca a boca de mala reputación, las acciones de la empresa podrían disminuir, perdidas de clientes o socios y la carente insatisfacción de miembro de la empresa.

La sociedad española para la calidad (2010) puntualiza que concurren superioridades en la dispersión y automatismo de *planes de gestión de la calidad*, por ello y para sortear un presente y futuro cercano con problemas de seguridad informática de los CETPROs privados de enseñanza de computación de la ciudad de Ilo, el investigador redactará un *plan de gestión de la calidad*. Mateo (2014) comenta que un *plan de gestión de la calidad* son las tareas encadenadas estructuradas, enlazadas y coordinadas que disemina sobre un conjunto o grupo de elementos para adquirir calidad (en el servicio o en el producto) que se da al cliente; en resumen, consiste en planificar, controlar y perfeccionar todas las partes de la

compañía que influyen en satisfacer al consumidor por medio del respeto y cumplimiento de los requisitos de los servicios o productos que se le ofrecen.

El *Instituto Nacional de Calidad* (INACAL) es una corporación pública y técnica especializada, vinculada al *Ministerio de la Producción* del Perú. La *Dirección de Normalización* es la autoridad adscrita a INACAL, encargada de aprobar las **normas técnicas peruanas** (NTP) como también dirigir el progreso de ellas. El *plan de gestión de la calidad* se apoyará en el estándar NTP-ISO/IEC 27001:2014; esta norma técnica peruana, consiste en diez títulos, ordenados así: 1) objetivo u objeto del área de aplicación, 2) reseñas normativas, 3) conceptos o definiciones y términos de referencias, 4) contenido de la organización, 5) liderazgo de la organización, 6) planificación de la organización, 7) soporte de la organización, 8) operaciones de la organización, 9) valoración del ejercicio, y 10) mejoras. Gómez & Andrés (2012) explican que la norma ISO 27001 son sistemas de gestión, específicamente denominados como *sistemas de gestión de seguridad de la información* (SGSI), también ellos argumentan que poseer ISO 27001, o ISO 9001, o ISO 14001 o cualquier otra norma ISO, vienen a hacer muy compatibles porque tienen requisitos comunes y estructura idéntica. Esta pesquisa se basa en la hipótesis que *un plan de gestión de la calidad* (ISO 27001) *influirá significativamente en la estrategia de seguridad y auditorías informáticas de los CETPROs de enseñanza de computación de la ciudad de Ilo*.

1.2. Definición del Problema

1.2.1 Problema principal. ¿En qué medida un plan de gestión de la calidad influye en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo?

1.2.2 Problemas secundarios.

P_1. ¿Cómo una política de calidad, basado en el esquema adaptado del estándar ISO27001:2014 influye en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo?

P_2. ¿En qué medida objetivos de calidad, basado en el esquema adaptado del estándar ISO27001:2014 influye en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo?

P_3. ¿Por qué un manual de calidad, basado en el esquema adaptado del estándar ISO27001:2014 influye en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo?

P_4. ¿Cómo procedimientos basados en el esquema adaptado del estándar ISO27001:2014 influye en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo?

1.3. Objetivo de la Investigación

1.3.1 Objetivo general. Determinar la influencia de un plan de gestión de la calidad en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de computación de la ciudad de Ilo.

1.3.2 Objetivos específicos.

1) Establecer la influencia de una política de calidad, basado en el esquema adaptado del estándar ISO27001:2014 en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

2) Determinar la influencia de objetivos de calidad, basado en el esquema adaptado del estándar ISO27001:2014 en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

3) Hallar la influencia de un manual de calidad, basado en el esquema adaptado del estándar ISO27001:2014 en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

4) Descubrir la influencia de procedimientos, basados en el esquema adaptado del estándar ISO27001:2014 en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

1.4. Justificación y Limitaciones de la Investigación

1.4.1 Justificación de la investigación.

Existió una justificación práctica para el desarrollo de esta investigación, cuyo eje primordial fue dar una solución a la inseguridad informática en los *CETPROs* privados de enseñanza de computación de la ciudad de Ilo proponiendo un plan de gestión de la calidad, asentado a modo de referencia en la norma o regla de referencia ISO27001:2014.

1.4.2 Limitaciones de la investigación.

Este proyecto tuvo limitaciones de tiempo la cual fue de doce meses de estudio comprendidos desde el 01 de diciembre de 2016 al 11 de noviembre de 2017, existieron también limitaciones de espacio demarcadas dentro de la ciudad de Ilo, por último, se tuvo limitaciones de recursos financieros los cuales ascendieron a S/. 3 505.00 soles.

1.5. Variables

1.5.1 Variable independiente. La variable es el *plan de gestión de la calidad*. Para la medición se usó una adaptación del cuestionario del software MSAT (Microsoft Security Assessment Tool 4.0), esta aplicación fue publicada el primero de marzo del 2009; ofrece información y recomendaciones para la seguridad de ambientes informáticos para empresas con menos de mil empleados a fin de ayudar a comprender los riesgos potenciales que se afrontan, este software evalúa y proporciona recomendaciones, su forma de proceder es por medio de preguntas a las cuales el responsable de informática elije opciones, después que se acabe el asunto de preguntas y respuestas, el sistema nos da un informe detallado sobre la medición de la seguridad informática de nuestra institución. Microsoft es de las mejores compañías de desarrollo de software del mundo, por tal motivo el instrumento de medición de la variable independiente no necesitaba juicio de experto, se considera validado por la empresa desarrolladora de software, pero como se empleó una adaptación de ella se buscó a dos magísteres para que den sus juicios de expertos.

1.5.2 Variable dependiente. La variable es la *estrategia de seguridad y auditorias informáticas de los CETPROs particulares de enseñanza de computación de la ciudad de Ilo*. Para la medición se usó una adaptación del cuestionario del *Ministerio de Economía, Fomento y Turismo* de la República de

Chile, el cuestionario está conformado por 94 ítems, dicho cuestionario sirve para el diagnóstico del despliegue de la ISO27001, es descargable de su portal web del ministerio chileno. El instrumento original (cuestionario) no necesitaba confiabilidad ni validación adicional, por haber pasado por un riguroso escrutinio técnico por parte del *Ministerio de Economía, Fomento y Turismo* de Chileno para su utilización, pero el cuestionario se adaptó para esta tesis entonces se buscó a dos profesionales para que den sus juicios de expertos.

Tabla 1

Operacionalización de la variable independiente: plan de gestión de la calidad

Definición conceptual	Definición operacional	Dimensiones	Indicadores	Instru-mento	Varia-ble
Camisón, Cruz & González (2006) dicen es la vía como las empresas serias y responsables emplean sus conceptos de calidad en un documento basado en la gestión procesos y afinando las ideas en la gestión de la calidad.	Es la redacción sistemática y analítica de procedimientos en donde al detalle lo que se debe hacer, también implica la confección de un manual especial que se le considera de calidad ya que en el están los objetivos y política que también son de calidad y se vinculan a la seguridad informática.	Política de calidad. Objetivos de calidad. Manual de calidad. Procedimientos.	Adaptación del test Microsoft Security Assessment Tool version 4.0.	Cuestionario	Categórica nominal dicotómica

Fuente: Autor de esta investigación.

Tabla 2

Operacionalización de la variable dependiente: estrategia de seguridad y auditorias informáticas de los Centros de Educación Técnico Productiva particulares de enseñanza de computación de la ciudad de Ilo.

Definición conceptual	Definición operacional	Dimensiones	Indicadores	Intru-mento	Vari-able
Conjunto de reglas que aseguran la decisión óptima en asuntos de privacidad e integridad de datos almacenada en sistemas informáticos, a la par de revisar sistemáticamente la actividad de seguridad informática por medio de evaluaciones que se llaman auditoría informática.	Planear, diseñar e implementar métodos de seguridad informática, además desarrollar evaluaciones periódicas con el fin de conservar la privacidad e integridad de datos.	− Estrategia de la política de calidad. − Estrategia de la organización. − Estrategia de la administración del hardware. − Estrategia de seguridad informática hacia el personal. − Estrategia de seguridad física y del ambiente. − Estrategia de gestión de comunicaciones y operaciones. − Estrategia del control de accesos. − Estrategia de mantenimiento de los sistemas. − Estrategia de administración de riesgos.	Adaptación del cuestionario de diagnóstico ISO 27001 del Ministerio de Economía, Fomento y Turismo de Chile.	Cuestionario	Categórica nominal dicotómica

Fuente: Autor de esta investigación.

1.6. Hipótesis de la Investigación

1.6.1 Hipótesis general.

H_1. Un plan de gestión de la ca1idad inf1uirá significativamente en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

1.6.2 Hipótesis específicas.

$H_{e1.}$ Una po1ítica de ca1idad, basado en el esquema adaptado del estándar ISO27001:2014 influirá significativamente en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

$H_{e2.}$ Objetivos de calidad, basado en el esquema adaptado del estándar ISO27001:2014 influirá significativamente en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

$H_{e3.}$ Un manual de calidad, basado en el esquema adaptado del estándar ISO27001:2014 influirá significativamente en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

$H_{e4.}$ Procedimientos basados en el esquema adaptado del estándar ISO27001:2014 influirá significativamente en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

CAPÍTULO II:

MARCO TEÓRICO

2.1. Antecedentes de la Investigación

Se investigo, buscó, y se entró a repositorios institucionales libres y de paga y en todas esas diversas fuentes bibliográficas se obtuvieron resultados negativos en la similitud de esta investigación con otras del pasado, también se indagó en archivos históricos, y bibliotecas virtuales, encontrando muy coca información sobre temas similares al expuesto en esta tesis, también se buscó en libros, revistas, periódicos, se indagó en planes de tesis y tesis de pregrado, maestría y doctorado, y en ningún momento de visualizo o encontró información que guarde reacción con las dos variables en estudio de esta tesis de maestría, se presume que deben haber información en contextos similares al estudiado acá, pero no se pudo tener acceso a pesar de las horas invertidas en la búsqueda de ella, finalmente se logró encontrar tesis que hablan o relacionan alguna de las dos variables que se estudia en contextos diferentes, siendo un indicador de la originalidad de esta misma tesis para su estudio, a continuación se explican los autores, nombre de la investigación y un resumen.

2.1.1 **Investigaciones del plan de tesis a nivel internacional.** Se leyó y analizó las tesis de los siguientes investigadores Abarca, Pandilla, & Portillo (2005), Álvarez (2005). Villatoro, Villalobos, & Posada (2007), Pallas (2009). Pinzón (2010), Corletti (2011), Aucancela (2012), Sandoval (2014), Parra (2014), Perafán & Caicedo (2014), Díaz (2015), Lanche (2015), y Morantes (2016). En las siguientes hojas se describen sus principales hallazgos.

- La tesis de Abarca, Pandilla, & Portillo (2005) explica que los centros educativos biculturales se conforman por empresas medianas y empresas grandes, también añade que estos centros usan tecnología como parte del trabajo que realizan, esta tecnología está conformada por equipos informáticos y es parte fundamental para el despliegue del modelo de auditoría en tecnologías de información, este modelo de auditoría ayudó a toda la administración de los recursos, detectando fallas y dando soluciones para luego corregirse. Los autores concluyen explicando que el diseño de un modelo de auditoria en tecnologías de información usado como herramienta de evaluación y control ayudó significativamente en las funciones de los centros educativos biculturales de la república del Salvador.

- La tesis de Álvarez (2005) titulada Se*guridad en informática (Auditoría de Sistemas).* Concluye narrando que todas las empresas modernas que hacen uso del internet sean para sus negocios o para la comunicación, deben contar con sistemas que gestionen la seguridad informática, esto último ayuda a una continua sostenibilidad y desenvolvimiento empresarial. Queda claro que el activo más valioso de cualquier organización es la información que se maneja, y es por ello que se debe asegurar a integridad completa, confidencialidad de lo que se envía y recibe y disponibilidad en todo el tiempo de la data. Todos los estudiosos de la

información y los tecnólogos de comunicación apuntan a responder la pregunta de cómo mantener la confidencialidad y usabilidad de la información de las empresas, las respuestas podrían ser diversas, pero al parecer hay que darle prioridad a los métodos idóneos que ayuden a salvaguardar los sistemas y redes frente a cualquier peligro o amenaza futuras. Una solución de las idóneas mencionadas radica en el uso de las auditorías de los sistemas informáticos, ya que es solo por ellos como se logra conocer la situación real de los dispositivos, sistemas, políticas y demás temas respecto a la información, la auditoría da control y esto se traduce en protección de la información. Se recomienda encarecidamente realizar auditorías de forma programada y continua en periodos, sólo así se sabrá el estado de la red, las configuraciones de los equipos, el estado del software y del hardware. Se concluye que la seguridad informática se focaliza en el proceso de auditorías, ya que esta es una radiografía detallada que dará a revelar problemas que la administración luego tendrá que corregir.

- La tesis de Villatoro, Villalobos, & Posada (2007). Concluye argumentando que para perfeccionar la realidad administrativa educativa respecto al empleo de los patrimonios de tecnologías es fundamental aplicar un plan de auditoría informática, en ese sentido para conocer los controles internos la institución educativa debe estar comprometida con la auditoría, también la institución educativa debe establecer planes de evaluación e identificación de los requisitos primordiales para que cuando se diseñe un plan de auditoría informática esta tenga todos los lineamientos importantes para revisar los centros educativos. Por último, un plan de auditoría informática logra la efectividad administrativa de los recursos tecnológicos de los centros de cómputo educativos.

- La tesis de Pallas (2009). Concluye comentando que para una empresa con estructura jerárquica es fundamental el uso de un método que logre gestionar la seguridad de la información, este método (metodología) debe contener criterios correctamente alineados al plan y estrategia empresarial y estar en concordancia a las etapas del círculo de la mejora continua, sin olvidar la agilidad y flexibilidad operativa para así lograr el nivel necesario de seguridad. Se propuso un enfoque variado, pero con autonomía necesaria por cada nivel de dominio, centrándose en la gestión de controles y en la visualización del riesgo local que se puede tener, esto logra optimizar los recursos. Se recomienda el uso de modelos y estándares para con el negocio, asimismo la utilización de herramientas que ayuden la comunicación entre los actores y la empresa. En la alineación de los criterios se recomienda un enfoque de arriba hacia abajo, compatibles con el modelo de negocio, compatibles con la estrategia y con la política de seguridad de la información, todo esto armonizará los SGSI. Se concluye también que el sistema de SGSI debe estar adjunto en cada etapa del ciclo de la mejora continua.

- En la tesis de Pinzón (2010) se presentó la arquitectura AIDeMaS, esta tecnología está basado en integrar los multiagentes, los sistemas de razonamiento (inspirados en temas) y el aprendizaje automático. Estos sistemas multiagentes han resultado muy recomendables para solucionar problemas, ya que facilitan culminar tareas desde un foco puramente distribuido. De esta forma la base de la arquitectura AIDeMas es la arquitectura multiagente inspirada en el modelo jerárquico por medio de capas. La clave de la arquitectura es su mecanismo de clasificación, les proporciona adaptabilidad frente a los ataques. Entonces esta arquitectura AIDeMaS detecta intrusos por medio de técnicas de aprendizaje. También el investigador añade que AIDeMaS da una forma mucho más propicia de clasificación respecto al tiempo de respuesta. Por medio de la experimentación se concluyó que la arquitectura AIDeMaS manifiesta características innovadoras para la detección intrusos.

- La tesis de Corletti (2011), señala que hay cuatro puntos a tratar como las comparativas y análisis de NIDS, la detección con NIDS relacionado con los métodos de generación de ciberataques, las matrices de seguridad, y el uso de técnicas y métodos militares en ámbitos de ciberseguridad. El autor lo llama acción retardante, ese es su diseño para contrarrestar la ciberdelincuencia, el autor hace hincapié que la clave es entenderlo desde la idea de la defensa en profundidad, es decir mientras más barreras se tiene, mientras más obstáculos se le da al atacante, el más recursos el indeseable necesitará, por tanto las técnicas no deben de ser las mejores ya que siempre son susceptibles de ser violadas, pero en cambio mientras más cantidad sean menos apetitoso será para el atacante, es por ello que el experto de la investigación lo denomina como acción retardante.

- La tesis de Aucancela (2012), el ensayista concluye diciendo que hay estándares que sirven para la administración del riesgo basados en tres puntos importantes: seguridad de la tecnología de información, transmisión de valores y administración del riesgo, algunos ejemplos de estos estándares son COBIT, ISO 207001 e ITIL. Se puede crear controles integrados para la gestión del riesgo en tecnología en las medianas y pequeñas empresas que estén en base de ISO 17799 y COBIT. Los roles de los auditores han cambiado en la última década, en este contexto el auditor informático se convirtió en pieza clave en la evaluación del riesgo en tecnología, también hay que añadir que estas herramientas ayudan a la mejora continua de los procesos institucionales por medio de herramientas tecnológicas que sirven en el análisis, evaluación y planificación.

- La tesis de Sandoval (2014), expresa que poner en marcha un SGSI afianzado en la ISO/IEC27001 permite ejecutar procesos que apunten a la administración del correcto acceso de la información en la compañía. Ejecutar este estándar partiendo de las cuatro etapas primitivas del círculo de la mejora continua, dará el desarrollo de una estructura de trabajo clara y metodológica. Para reducir los riesgos de robo o pérdida hay que visualizar periódicamente los controles. Se pueden hacer varias certificaciones simultáneas dado que la ISO27001 e ISO9001 están muy emparejadas. Se manifiesta que usar un plan de tratamientos de riesgos facilita la aplicación de políticas y procedimientos de seguridad. Se termina concluyendo que la ISO27001 otorga la disminución del riesgo de forma significativa.

- La tesis de Parra (2014) titulada *ISO 27001 para PYMES*. El investigador expresa que las PYMES en su investigación usaron tecnologías distintas a lo largo del estudio y que los usuarios tenían privilegios de libertad sobre los equipos que usaba, esto último se presta a potenciales ataques desde la misma empresa. Mientras más extensa la empresa, más infraestructura en tecnología poseen, y con ello más inversión deben invertir en capacitación tecnología para sus empleados usuarios. Es insuficiente la implementación de seguridad informática sí estas no van de la mano con procedimientos y políticas que apunten a mecanismos defensivos. La clave es hacer esfuerzos en adiestramiento a al personal en seguridad informática. Si las políticas y procedimientos están bien orientados, estas mismas deben ser generalizadas a todas las otras empresas que tienen rubros similares, como es obvio se pueden hacer algunos cambios ligeros, pero la idea es reciclar las políticas y procedimientos que ya funcionan. Aun cuando se trató el tema de las PYMES, esta tesis puede calzar para empresas más grandes también.

- La tesis de Díaz (2015). El autor concluye explicando que la popularización del uso de la automatización de la información, la ciber-navegación por la web y la gran penetración de las redes sociales, no son garantía de su correcto uso, ni siquiera por parte de los alumnos universitarios que se forman en esas tecnologías. Tampoco los de mejores conocimientos han sido capaces de asimilarlos y ponerlos en práctica, diferenciándose de sus compañeros. El hecho de utilizar esos recursos muy frecuentemente no es razón suficiente para asumir la motivación de un uso seguro. Como si se tratase de otro tipo de aprendizajes, menos incorporados a la vida diaria, no podemos dejar de atraer su atención hacia casos reales, prácticos, con ejemplos y experiencias que fomenten su inquietud con el objetivo de sensibilizarlos adecuadamente. El investigador obtuvo información, a través de las dos pruebas piloto del cuestionario, que vaticinaba unos resultados que parecían confirmar que nuestra preocupación estaba sustentada por los datos de los análisis que estábamos haciendo, siendo muy similares a los que ya disponíamos de los alumnos de Comunicación Audiovisual. Desafección hacia el uso de contraseñas, escasa garantía en preservar la información mediante copias de seguridad, falta de protección en la navegación inalámbrica en sitios públicos, asunción de compromisos con los proveedores de aplicaciones de Redes Sociales, etc. son características comunes que igualaban el comportamiento de unos y otros estudiantes. Todas estas conclusiones dan respuesta a las preguntas que, como objetivos de la presente tesis, nos planteamos en la tabla 1 y que justifican la recomendación de revisar los planes de estudio, teniendo en cuenta las motivaciones de los alumnos.

- La tesis de Lanche (2015). Explica que, respecto a la parte física, es menester que se hagan mejorías a la seguridad del acceso a las áreas, y por tanto se mejore las señalizaciones de las mismas. Se ha detectado que la red tiene vulnerabilidades, esto se debe a su topología, Otra

falencia resaltante es el uso de un único servidor para las múltiples tareas existentes (corta fuegos, proxy virtualización, intranet). Faltan estrategias y con ello también procedimientos en caso de algún evento relacionado con la ciberseguridad. De la normativa existente debe nacer políticas, procedimientos y procesos, esto dará el soporte adecuado en casos problemas legales.

- La tesis de Morantes (2016) de título *Análisis Forense*. Narra que, de los datos expuestos, se hizo el análisis respecto a un usuario en especial llamado Ann; el administrador de esa cuanta tiene capacitación técnica a nivel intermedio en informática, es por ello que el administrador tiene el conocimiento para tomar decisiones en seguridad informática, dos de las técnicas usadas fueron la esteganografía y el cifrado de datos, son con estas técnicas que se aumentó la seguridad en los documentos. También hay que añadir que hay una relación lógica entre la imagen del disco duro y la imagen espejo del dispositivo de almacenamiento externo USB. Se analizó los datos del análisis realizado de las copias imágenes por separado, este análisis es crucial y sirve como evidencia.

2.1.2 Investigaciones del plan de tesis a nivel nacional. Se leyeron las investigaciones de origen peruano de los siguientes tesistas Ramírez (2002), Alfaro (2008), Liñán (2008). Barrantes & Hugo (2012), Carbajal (2013), Fernández Peñaloza, D. A., & Pacheco Vargas, O. A. (2014), Vento Mesa, M. L. (2014), Alcántara Flores, J. C. (2015), Tamayo Arana, D. P. (2015), Zeña Ortiz, V. E. (2015), Seclén Arana, J. A. (2016), Huamán Monzón, F. M. (2017). En las próximas paginas se comenta sus principales hallazgos.

- La tesis de Ramírez (2002). *Metodología para auditoría informática en entidades públicas*. Expresa que el método (metodología) permite usar técnicas para reunir información con el objetivo de evaluar controles y descubrir riegos. Los cuestionarios son instrumentos que logran reunir los motivos que el auditor emplea para hacer las mismas auditorias. Para facilitar este método se obtuvo inspiración de otras normas como MAGU, NAGU y NIAS. Las entidades públicas disponen de la auditoría informática como medio para la evaluación de controles y riesgos en el uso de las tecnologías de información. También la auditoría informática logra que las entidades públicas tengan normas internacionales por medio de la búsqueda de la certificación de la calidad. Se concluye que la metodología funciona para realizar auditoria en entidades públicas.

- La tesis de Alfaro (2008). Concluye que se tiene un método con estas características: se heredan las mejores prácticas de las normas COBIT, ISO 17799, ISO 12207, ISO 20000, PMBOK e ISO 19011. El autor narra que hay gestión por procesos y uso del pensamiento del círculo de la mejora continua, añade también el autor que toda auditoría debe partir por dentro (auditoría interna) y para ello es importante contar con personas altamente capacitadas en auditoria.

- La tesis de Liñán (2008). Concluye que demostrando que, si hay carencia de algún plan o guía referente a la seguridad informática, habrá deficiencia en la seguridad informática. De existir algún plan o guía se demostró que hay mejora importante en lo referente a la ciberseguridad. Se demostró que también se maximiza la percepción, es decir un cambio a positivo la seguridad informática. Por último, se aprecia que un método de seguridad informática beneficio a la facultad de postgrado de la Universidad Nacional Federico Villarreal.

- La tesis de Barrantes & Hugo (2012). Los investigadores concluyen demostrando que toda documentación de procesos es una forma inteligente de mejora de sistemas de gestión en la institución, esta documentación debe basarse en el despliegue de políticas de seguridad y sobre todo formas para divulgar estas políticas, las políticas de calidad deben ser claras y apuntar a los objetivos empresariales. Se descubrió que luego de desplegar el sistema de gestión de seguridad de información, las vulnerabilidades y amenazas no disminuyen radicalmente, pero los escenarios de peligro bajaron por que el personal ya sabe qué hacer y está calificado para afrontar ataques. De todas formas, implementar un método que calce en las necesidades de la institución es saber gestionar los riesgos reduciéndolos al mínimo. Otro punto importante en el despliegue de un sistema de gestión es el factor humano, por ello hay que incentivar e instruir continuamente. Concluimos dando a conocer que hay que documentar todos los procesos involucrados con el manejo de información vital para la empresa.

- La tesis de Carbajal (2013). Concluye diciendo que, para un uso apropiado del método propuesto la Contraloría General de la Republica, en especial la Oficina Nacional de Gobierno Electrónico e Informática debe dar conocimiento de los temas que están desarrollando en relación a esta propuesta. Luego de esto se logró aplicar el método en seis trabajos de auditorías informáticas en la Sunat, esto se fue permitido gracias a la oficina del Control Interno (años 2011 al 2012), se debe aclarar que el investigador de esta tesis actuó como auditor. Luego de aplicar esta nueva metodología se evidenció mejorías, y se vio reflejado en los objetivos del Plan Anual de Control de la Sunat. La Sunat no dio ninguna observación en contra de las auditorías, por tanto, se asegura la calidad del método.

- Fernández Peñaloza, D. A., & Pacheco Vargas, O. A. (2014). De sus conclusiones se obtiene el siguiente resumen, se concluye que se logró diseñar un plan de sistema de gestión de seguridad de la información inspirada en la ISO/IEC27001:2008, dicho plan abarcó el 100% de los activos de información de SIMTRAC y COSPAS-SARSAT. También se obtuvo el 100% del análisis en riegos de la comandancia de operaciones guardacostas. La auditoría encontró un 48% vulnerabilidades. Se realizó la comparación entre la NTP-ISO/IEC 27001:2008 y la evaluación selectiva, logrando así un plan de SGSI que cuenta con el 25% de los controles que la Comandancia de Operaciones Guardacostas utilizan. Al utilizar el plan se disminuyó un 73% las amenazas y vulnerabilidades. También se alcanzó el compromiso de la alta administración dando como resultado un 80% en la sensibilización del personal.

- Vento Mesa, M. L. (2014). El estudioso consiguió identificar la totalidad de activos empresariales, también se identificó falencias en la seguridad de la información, se logró saber los riesgos y posteriormente se mapearon para identificar niveles críticos. Se tiene conocimiento de los controles relacionados a riesgos, finamente se concientizó al personal de la organización en temas de seguridad de la información.

- Alcántara Flores, J. C. (2015). Su tesis dice que con la implementación se consiguió aumentar la seguridad en los softwares de la policía, esto se logró gracias al mejoramiento de las políticas de seguridad y sobre todo a la puesta en marcha. También esta guía mejora el proceso de visualización de anomalías informáticas. La guía logró tratar los riesgos por medio de la disminución de las vulnerabilidades, y esto último se alcanzó con mecanismos de correcciones preventivas y correctivas. Finalmente, la guía comprende la capacitación del personal de la institución en temas de seguridad informática.

- Tamayo Arana, D. P. (2015). El autor manifiesta que el software que usa la empresa no es el ideal porque no garantiza la consistencia de la información. Para lograr madurez en los controles se tuvo que redactar un plan de acciones. Este nuevo plan de acciones contiene el enfoque de la mejora continua. Se usó también herramientas de software especializados en auditoría informática.

- Zeña Ortiz, V. E. (2015) señala que luego de la implantación del sistema de gestión de la seguridad de la información para el proceso de Tecnología de Información en la Oficina Central de Informática de la UNPRG, el riesgo se logró diezmar de 6 a 4,4 esto se traduce en el 26,67%. El logro fue por la aplicación del método de análisis de riesgos y evaluación. La ISO 27001 y sus controles del anexo A, ayudaron bastante a la disminución del riesgo. Cuando el riesgo disminuyó paso a convertirse en riesgo residual, la misma que puede ser sujeta a más controles para diezmarlo más y así poseer el control del riesgo total. Con el sistema de seguridad puesta en marcha se obtuvo una disminución del riesgo en 40,94%, hubo controles inexistentes que asedian a 95 y con la ISO 27001 se redujo a 24; antes de instalar la ISO 27001 se tenía 43 controles y luego se logró 81 controles existentes y aplicados. Este sistema de seguridad nos ahorró perdidas monetarias del 40%.

- Seclén Arana, J. A. (2016). Argumenta que lo importante es promover desde el gobierno central, temas de políticas estratégicas sobre asuntos de seguridad de la información. Por tanto, el diseño principal es iniciar por las políticas para luego pasar al desarrollo de un departamento de gobierno de la seguridad de la información. Este nuevo departamento tendría que estar conformado por un equipo de especialistas en seguridad de la información. En el análisis que

se hizo en esta investigación se descubrió que, en las instituciones públicas, el punto de inicio es por medio de la ISO 9001, para luego pasar a una ISO 27001, es por esta razón que implementar un SGSI es una fase proveniente de la búsqueda de la calidad. Por tal motivo de concluye se vea por donde se vea, todos los factores que afectan a la implementación de un SGSI es importante y positivo.

- Huamán Monzón, F. M. (2017), aclara que los trabajadores saben y manipulan un 50% más los temas básicos de seguridad de la información. Un 72% de los involucrados conocen las vías de comunicación en el interior de la organización. Un 37% de los administrativos adoptan y saben buenas prácticas. Al implementar herramientas de ciencias de gestión, el proyecto mejoró enormemente.

2.2. Bases Teóricas

2.2.1 Estrategia y calidad. Carrión (2007) explica lo difícil de conceptualizar el término estrategia (antiguamente para el ámbito militar y ahora para el entorno empresarial) muchos tipos de estrategias han surgido, tenemos la estrategia como plan, como patrón, estrategias premeditadas (se realizan por completo), no realizadas (no se concretan), emergentes (simplemente surgió), sombrilla (en el camino salen los detalles), estrategia como posición (ubicación del producto o servicio), estrategia como perspectiva (dentro de la organización), estrategia como estratagema (aprovecharse de los competidores). Carrión (2007) narra que la estrategia son acciones cuya finalidad es el cambio inteligente, continuo y proactivo de la institución. Sobre la calidad Deming (1986), aclara que calidad únicamente puede ser definida

en relación de quien califica o juzga la calidad. Un responsable de calidad ve la calidad a su manera, un oficinista observa la calidad de otro modo y el gerente percibe la calidad diferente. Es por ello que definir la calidad de algo es difícil.

2.2.2 Plan de gestión de la calidad. En las siguientes líneas se expondrá la po1ítica, objetivos, manua1 y procedimientos emp1eados en 1a muestra experimenta1.

a) ***Política de calidad.*** Esta política aprovecha 1a adaptación de 1a *Norma Técnica Peruana ISO27001:2014* a modo de referencia; e1 CETPRO *José Manue1 Ubalde Zeballos* es una institución educativa dedicada principalmente a brindar enseñanza de cursos de computación con e1 mejor rendimiento de sus recursos a todo niño, joven y adulto en 1a ciudad de Ilo por medio de docentes altamente capacitados, de un grupo responsable de 1a infraestructura de red y de sistemas, y e1 empleo de procedimientos específicos para salvaguardar 1a integridad de sus equipos informáticos, garantizando e1 buen funcionamiento de los softwares, cuidando 1a información que hay en e1los, restringiendo accesos no autorizados, empleando modernos sistemas de seguridad, utilizando controles, mecanismos y herramientas de seguridad informáticas y finalmente realizar auditorías internas y para 1as auditorías externas haciendo evaluaciones para obtener al mejor postor; todo a favor de una mejor seguridad informática que también ayude a 1a divulgación y 1a capacitación de sus alumnos, personal administrativo y docente cuando forman parte de1 CETPRO.

b) ***Objetivos de calidad.*** Son 1os siguientes.

- Sa1vaguardar 1a integridad de1 hardware.
- Garantizar 1a operaciona1ización de1 software.
- Resguardar datos de 1os a1umnos y persona1 administrativo y docente.
- Restringir e1 acceso no autorizado.
- Emp1ear sistemas de seguridad.
- Uti1izar contro1es de seguridad.
- Ap1icar mecanismos de seguridad.
- Usar herramientas de seguridad.
- Auditar periódicamente de forma interna 1os sistemas de1 CETPRO.
- Auditar periódicamente de forma externa 1os sistemas de1 CETPRO.

c) ***Manual de calidad.*** Se expone en que consiste el manual.

	PLANEAR	***HACER***	***VERIFICAR***	***ACTUAR***
INTEGRIDAD DEL HARDWARE	METAS − Asegurar más del 90% el buen estado del hardware cada semana. − Solucionar el 100% de las anomalías del hardware cada día. − Revisar el 100% de las PC y hardware de red cada semana. − Inventariar del 100% hardware existente. − Catalogar el hardware según los datos, software y servicios. − Analizar el nivel de importancia o criticidad de la información que administra el hardware. − Clasificar las características del hardware. − Etiquetar el 100% de los cables de red. MÉTODOS PARA CUMPLIR LAS METAS − Observación. − Revisiones retrospectivas, introspectivas e introspectivas. − Diagnostico. − Proactividad.	− Limpieza del hardware. − Monitoreo. − Inventario del hardware. − Mantenimiento preventivo del hardware. − Mantenimiento correctivo del hardware. − Catálogos del hardware. − Análisis de importancia o criticidad de información administrable por el hardware. − Clasificación de las características del hardware. − Etiquetado de cables.	− Comprobar estado de limpieza de las PC y hardware. − Contrastar las características principales y secundarias del hardware. − Verificar los reportes del monitorio diario. − Examinar los reportes del mantenimiento preventivo. − Inspeccionar los reportes del mantenimiento correctivo. − Revisar el etiquetado.	− Realizar una limpieza más profunda. − Realizar un mantenimiento correctivo inmediato. − Revisar todos los reportes de la última semana. − Actualizar inventario del hardware. − Corregir inventario del hardware. − Etiquetar correctamente.

	PLANEAR	*HACER*	*VERIFICAR*	*ACTUAR*
OPERACIONALIZACIÓN DEL SOFTWARE	METAS − Asegurar más del 95% el buen estado del software cada semana. − Limpiar archivos duplicados. − Emplear antivirus. − Solucionar el 100% de las anomalías del software cada día. − Emplear cortafuegos. − Revisar el 100% de los sistemas y programas de PC cada semana. − Escanear puertos. − Cambiar sistemas operativos. − Instalar actualizaciones licenciadas. MÉTODOS PARA CUMPLIR LAS METAS − Observación, diagnostico, proactividad. − Revisiones retrospectivas, introspectivas e introspectivas.	− Administración de espacios. − Monitoreo. − Mantenimiento preventivo del software. − Mantenimiento correctivo del software. − Limpieza o eliminación de archivos. − Empleo de antivirus. − Escaneo de puertos. − Instalación de sistemas operativos y actualizaciones.	− Comprobar estado de memoria y espacios empleados en el sistema. − Verificar los reportes del monitorio diario. − Examinar los reportes del mantenimiento preventivo del software. − Inspeccionar los reportes del mantenimiento correctivo del software. − Reportes de antivirus y corta fuegos. − Sistemas operativos instalados. − Comprobar estado de los programas.	− Liberar espacios del sistema. − Realizar un mantenimiento correctivo inmediato. − Revisar todos los reportes de la última semana. − Eliminar no conformidades encontradas.
RESGUARDO DE DATOS	METAS − Almacenar el 100% de los documentos de los usuarios diariamente. − Archivar el 100% de los datos del programa importantes. − Realizar copias de seguridad de todos los registros del sistema y reportes de programas cada semana. MÉTODOS PARA CUMPLIR LAS METAS − Observación y proactividad.	− Copiar archivos a las unidades de almacenamiento internos y externos. − Realizar copias de seguridad.	− Comprobar archivos copiados. − Verificar existencia de copias de seguridad. − Examinar los reportes de la creación de backup.	− Crear copia de registros del sistema. − Realizar copia inmediata de backup. − Revisar todos los reportes de creación de backup de la última semana.

	PLANEAR	*HACER*	*VERIFICAR*	*ACTUAR*
RESTRICCIÓN DE ACCESOS	METAS − Procesar el 100% de las solicitudes de accesos. − Verificar el 100% de los nombres de los usuarios. − Validar la totalidad de las claves de accesos. − Redactar plan de accesos a los dispositivos − Registrar de accesos y la baja de ellos − Controlar la asignación y uso de privilegios − Gestionar las contraseñas para los docentes, alumnos y administrativos − Controlar los derechos de accesos a los estudiantes − Gestionar las contraseñas a los sistemas − Controlar los accesos a los equipos desatendidos − Controlar el acceso cuando se hace limpieza − Administrar los servicios de red − Analizar la información obtenida en la auditoria informática − Controlar los equipos fuera de la institución − Administrar la red inalámbrica − Administrar la compartición archivos en la red − Administrar el acceso al router − Administrar la asignación de números IP − Administrar el acceso al servidor − Administrar los accesos a las laptops de los estudiantes − Administrar el tratamiento de dispositivos USB. MÉTODOS PARA CUMPLIR LAS METAS − Observación, revisión, proactividad.	− Procesar solicitudes de acceso. − Verificar nombres de usuarios. − Validar contraseñas. − Plan de accesos a los dispositivos. − Registro de accesos y baja de ellos. − Asignación y uso de privilegios − Otorgar contraseñas para los docentes, alumnos y administrativos − Control de derechos de accesos a los estudiantes − Gestión de las contraseñas a los sistemas − Control de accesos a los equipos desatendidos − Control de accesos cuando se hace limpieza − Administración a los servicios de red − Análisis de la información obtenida en la auditoria. − Control de equipos fuera de la institución − Administración de la red inalámbrica − Administración de la compartición archivos en la red − Administración del acceso al router − Administración de la asignación de números IP − Administración del acceso al servidor − Administración de los accesos a las laptops de los estudiantes − Administración del tratamiento de dispositivos USB.	Verificar los resultados de las actividades ejecutadas	− Restringir usuarios. − Eliminar no conformidades encontradas.

	PLANEAR	*HACER*	*VERIFICAR*	*ACTUAR*
SISTEMAS DE SEGURIDAD	METAS − Planear comunicación de las actividades de seguridad. − Planear comunicación de las debilidades de seguridad. − Planear responsabilidades ante un riesgo. − Planear respuesta inmediata. − Planear forma de cuantificar las pérdidas de un riesgo. MÉTODOS PARA CUMPLIR LAS METAS − Observación, revisión, análisis, proactividad.	− Comunicar de las actividades de seguridad. − Comunicar las debilidades de seguridad. − Analizar las responsabilidades ante un riesgo. − Realizar respuesta inmediata. − Cuantificar las pérdidas de un riesgo.	− Verificar los resultados de las comunicaciones de las actividades y debilidades en temas de seguridad. − Comprobar y verificar lista de responsabilidades y perdidas ante un riesgo.	− Eliminar no conformidades encontradas en la planeación.
CONTROLES DE SEGURIDAD	METAS − Estudiar la seguridad informática para el CETPRO − Analizar el 100% de la seguridad física y del ambiente informático del CETPRO. − Analizar un perímetro seguro. − Estudiar acciones frente a extraños. − Buscar áreas seguras. − Reubicar equipos. − Proteger el cableado. − Analizar la disponibilidad e integridad de equipos. − Estudiar el tratamiento de equipos retirados. − Estudiar el tratamiento de seguridad en equipos móviles. MÉTODOS PARA CUMPLIR LAS METAS − Observación, revisión, análisis, proactividad.	− Confeccionar y actualizar continuamente planes de seguridad informática. − Redactar y ejecutar planes de seguridad física informática. − Hacer un perímetro seguro. − Redactar protocolos frente a desconocidos. − Señalar áreas seguras. − Reubicar equipos estratégicamente. − Usar canaletas en cables. − Retirar equipos. − Proteger dispositivos móviles.	− Verificar planes de seguridad. − Verificar la ejecución de los planes. − Verificar perímetros. − Verificar ubicación de equipos retirados. − Revisar la protección del cableado. − Verificar áreas seguras.	− Eliminar no conformidades encontradas.

	PLANEAR	*HACER*	*VERIFICAR*	*ACTUAR*
MECANISMOS DE SEGURIDAD	METAS – Analizar las responsabilidades de los docentes y administrativos. – Estudiar la selección y baja del personal. – Examinar las condiciones de confidencialidad y responsabilidades en los documentos. – Impartir formación adecuada de seguridad informática al personal – Indagar los procedimientos en caso de incidente de seguridad – Analizar procedimientos de recolección de datos de los incidentes informáticos. – Incentivar la comunicación de los usuarios. – Estudiar el comportamiento. – Incentivar e incrementar la colaboración del personal. MÉTODOS PARA CUMPLIR LAS METAS – Observación, revisión, análisis, proactividad.	Redactar y ejecutar planes de: – responsabilidades de los docentes y administrativos, – selección y baja del personal, – condiciones de confidencialidad y responsabilidades en los documentos, – formación adecuada de seguridad informática al personal, – procedimientos en caso de incidente, – de las vulnerabilidades observadas – buen comportamiento. – participación en las auditorias.	– Verificar planes de seguridad. – Verificar la ejecución de los planes.	– Eliminar no conformidades en los planes.

	PLANEAR	*HACER*	*VERIFICAR*	*ACTUAR*
HERRAMIENTAS DE SEGURIDAD	METAS – Planificación de las adquisiciones y empleo de herramientas preventivas, detectivas y correctivas. MÉTODOS PARA CUMPLIR LAS METAS – Observación, revisión, análisis y proactividad.	– Emplear de software para el análisis y acciones preventivas, detectivas y correctivas.	– Verificar la instalación y ejecución de los sistemas.	– Eliminar no conformidades de las herramientas usadas.
AUDITORÍA INTERNA	METAS – Revisar más del 80% de los controles y características físicas, técnicas y administrativas. MÉTODOS PARA CUMPLIR LAS METAS – Observación, revisión, análisis y proactividad.	– Auditar controles y características físicas, técnicas y administrativas.	– Verificar los resultados de las actividades a la auditoría.	– Eliminar no conformidades encontradas en la auditoría.
AUDITORÍA EXTERNA	METAS – Revisar más del 90% de los controles y características físicas, técnicas y administrativas. MÉTODOS PARA CUMPLIR LAS METAS – Observación, revisión, análisis y proactividad.	– Auditar controles y características físicas, técnicas y administrativas.	– Verificar los resultados de las actividades a la auditoría.	– Eliminar no conformidades encontradas en la auditoría.

d) ***Procedimientos.*** A continuación, se exponen todos los procesos.

Proceso: PLAN PARA LA INTEGRIDAD DEL HARDWARE

INTEGRIDAD DEL HARDWARE	
Entradas	− Hardware en mal estado. − Hardware con anomalías. − PC y hardware de red para revisar. − Lista de hardware del CETPRO. − Características del hardware.
Salidas	− Hardware en buen estado. − Hardware sin anomalías. − PC y hardware de red revisados. − Clasificación del hardware.
Objetivo	Asegurar el funcionamiento óptimo de todo el hardware existente.
Responsable	Soporte informático
Clientes	− Usuarios del CETPRO. − Alumnos del CETPRO. − Docentes del CETPRO.
RRHH	Jefe de laboratorio
Equipos o materiales	Software de monitoreo y diagnóstico, herramientas de mantenimiento preventivo y correctivo.
Costos	− Relacionado con el contrato del responsable. − Relacionado con las herramientas y software necesarios.
Tiempo	Lunes – sábado, 8 horas diarias.

Proceso: PLAN PARA LA OPERACIONALIZACIÓN DEL SOFTWARE

OPERACIONALIZACIÓN DEL SOFTWARE	
Entradas	− Software en mal estado. − Software con anomalías. − Sistemas y programas de PC para revisar.
Salidas	− Software en buen estado. − Software sin anomalías. − Sistemas y programas de PC revisados.
Objetivo	Asegurar el funcionamiento óptimo de todo el software instalado.
Responsable	Soporte informático
Clientes	− Usuarios del CETPRO. − Alumnos del CETPRO. − Docentes del CETPRO.
RRHH	Jefe de laboratorio
Equipos o materiales	Software de monitoreo y diagnóstico, herramientas de mantenimiento preventivo y correctivo.
Costos	− Relacionado con el contrato del responsable. − Relacionado con las herramientas y software necesarios.
Tiempo	Lunes – sábado, 8 horas diarias.

Proceso: PLAN PARA EL RESGUARDO DE DATOS

RESGUARDO DE DATOS	
Entradas	− Documentos variados. − Datos específicos de programas. − Registros y reportes originales.
Salidas	− Documentos variados almacenados. − Datos específicos de programas archivados. − Copia de seguridad de registros y reportes.
Objetivo	Resguardar la información de los usuarios.
Responsable	Soporte informático
Clientes	− Usuarios del CETPRO. − Alumnos del CETPRO. − Docentes del CETPRO.
RRHH	Jefe de laboratorio
Equipos o materiales	Discos duros, dispositivos USB, software para copias de backup.
Costos	− Relacionado con el contrato del responsable. − Relacionado con las herramientas y software necesarios.
Tiempo	Lunes – sábado, 8 horas diarias.

Proceso: PLAN PARA LA RESTRICCIÓN DE ACCESOS

RESTRICCIÓN DE ACCESOS	
Entradas	− Solicitud de acceso. − Nombre de usuario. − Clave de acceso.
Salidas	− Solicitud de acceso procesada. − Nombre de usuario verificado. − Clave de acceso validado.
Objetivo	Controlar accesos a los sistemas y servicios a los usuarios.
Responsable	Soporte informático
Clientes	− Usuarios del CETPRO. − Alumnos del CETPRO. − Docentes del CETPRO.
RRHH	Jefe de laboratorio
Equipos o materiales	Programas y dispositivos especializados.
Costos	− Relacionado con el contrato del responsable. − Relacionado con las herramientas y software necesarios.
Tiempo	Lunes – sábado, 8 horas diarias.

Proceso: PLAN PARA LOS SISTEMAS DE SEGURIDAD

SISTEMAS DE SEGURIDAD	
Entradas	− Lista de actividades de seguridad. − Lista de debilidades en la seguridad. − Lista de responsabilidades ante los riesgos. − Lista de preguntas de seguridad. − Lista de inventarios informáticos.
Salidas	− Plan de comunicación de las actividades de seguridad. − Plan de comunicación de las debilidades en la seguridad. − Plan para definir las responsabilidades ante los riesgos. − Plan de respuestas inmediatas. − Plan para cuantificar las pérdidas de un riesgo
Objetivo	Controlar los riesgos informáticos.
Responsable	Soporte informático
Clientes	− Usuarios del CETPRO. − Alumnos del CETPRO. − Docentes del CETPRO.
RRHH	Jefe de laboratorio
Equipos o materiales	Planes, programas y dispositivos especializados.
Costos	− Relacionado con el contrato del responsable. − Relacionado con las herramientas y software necesarios.
Tiempo	Lunes – sábado, 8 horas diarias.

Proceso: PLAN PARA LOS CONTROLES DE SEGURIDAD

CONTROLES DE SEGURIDAD	
Entradas	– Lista de roles y responsabilidades sin definir. – Lista de adquisiciones y cambios del hardware y software. – Lista de ideas de temas de seguridad informática. – Lista de ideas para las auditorías externas. – Lista de ideas para *tercerizar* de la seguridad informática. – Lista de ideas de las capacitaciones para el personal y alumnos. – Lista de ideas para la confidencialidad de la información del CETPRO. – Lista de ideas para las auditorías internas. – Lista de ideas para un perímetro seguro. – Lista de ideas de controles frente a extraños. – Lista de ideas para áreas seguras. – Lista de ideas para reubicar equipos. – Lista de ideas para proteger el cableado. – Lista de ideas para disponibilidad e integridad de equipos. – Lista de ideas para la seguridad de equipos retirados. – Lista de ideas para la seguridad de equipos móviles.
Salidas	– Ro1es y responsabi1idades definidos. – Responsab1e de 1a adquisiciones y cambios de1 hardware y software. – P1anes para 1os temas de seguridad informática. – P1anes para 1as auditorías externas. – P1anes para *tercerizar* de 1a seguridad informática. – P1anes para 1as capacitaciones para e1 persona1 y a1umnos. – P1anes para 1a confidencia1idad de 1a información de1 CETPRO. – P1anes para 1as auditorías internas. – P1anes para un perímetro seguro. – P1anes de contro1es frente a extraños. – P1anes para áreas seguras. – P1anes para reubicar equipos.

	– Planes para proteger el cableado. – Planes para disponibilidad e integridad de equipos. – Planes para la seguridad de equipos retirados. – Planes para la seguridad de equipos móviles.
Objetivo	Administrar la seguridad informática.
Responsable	Soporte informático
Clientes	– Usuarios del CETPRO. – Alumnos del CETPRO. – Docentes del CETPRO.
RRHH	Jefe de laboratorio
Equipos o materiales	Planes, programas, dispositivos y herramientas especializados.
Costos	– Relacionado con el contrato del responsable. – Relacionado con las herramientas y software necesarios.
Tiempo	Lunes – sábado, 8 horas diarias.

Proceso: PLAN PARA LOS MECANISMOS DE SEGURIDAD

SISTEMAS DE SEGURIDAD	
Entradas	− Lista de responsabilidades o roles de los docentes y administrativos respecto a la seguridad informática. − Lista de ideas para la selección y baja del personal − Lista de ideas de las condiciones de confidencialidad y responsabilidades en los documentos de contratos − Lista de ideas para impartir formación adecuada de seguridad informática al personal − Lista de ideas para los procedimientos en caso de incidente de seguridad − Lista de ideas para los procedimientos de recolección de datos de los incidentes informáticos. − Lista de ideas para que informen los usuarios de las vulnerabilidades observadas − Lista de ideas para que los usuarios tengan un buen comportamiento. − Lista de ideas para que el personal participe en las auditorias.
Salidas	− Planes de responsabilidades o roles de los docentes y administrativos respecto a la seguridad informática. − Planes para la selección y baja del personal − Planes para las condiciones de confidencialidad y responsabilidades en los documentos de contratos − Planes para impartir formación adecuada de seguridad informática al personal − Planes para los procedimientos en caso de incidente de seguridad − Planes para los procedimientos de recolección de datos de los incidentes informáticos. − Planes para que informen los usuarios de las vulnerabilidades observadas − Planes para que los usuarios tengan un buen comportamiento. − Planes para que el personal participe en las auditorias.
Objetivo	Asegurar la seguridad informática hacia el personal
Responsable	Soporte informático
Clientes	− Usuarios del CETPRO. − Docentes del CETPRO.
RRHH	Jefe de laboratorio
Equipos o materiales	Planes, programas y dispositivos especializados.
Costos	− Relacionado con el contrato del responsable. − Relacionado con las herramientas y software necesarios.
Tiempo	Lunes – sábado, 8 horas diarias.

Proceso: PLAN PARA LAS HERRAMIENTAS DE SEGURIDAD

HERRAMIENTAS DE SEGURIDAD	
Entradas	− Lista de necesidades de seguridad preventivas. − Lista de necesidades de seguridad detectivas. − Lista de necesidades de seguridad correctivas.
Salidas	− Adquisición y empleo de herramientas preventivas. − Adquisición y empleo de herramientas detectivas. − Adquisición y empleo de herramientas correctivas.
Objetivo	Emplear correctamente herramientas de seguridad informática.
Responsable	Soporte informático
Clientes	− Usuarios del CETPRO. − Docentes del CETPRO. − Alumnado.
RRHH	Jefe de laboratorio
Equipos o materiales	Planes, programas y dispositivos especializados.
Costos	− Relacionado con el contrato del responsable. − Relacionado con las herramientas y software necesarios.
Tiempo	Lunes – sábado, 8 horas diarias.

Proceso: PLAN PARA LA AUDITORÍA INTERNA

AUDITORÍA INTERNA	
Entradas	Lista de controles y características físicas, técnicas y administrativas.
Salidas	Revisión detallada de los controles y características físicas, técnicas y administrativas.
Objetivo	Auditar infraestructura tecnológica del CETPRO
Responsable	Calidad informática
Clientes	− Usuarios del CETPRO. − Docentes del CETPRO. − Alumnado.
RRHH	Responsable de calidad
Equipos o materiales	Plan de auditoría, programas y dispositivos especializados.
Costos	− Relacionado con el contrato del responsable. − Relacionado con las herramientas y software necesarios.
Tiempo	Cada dos meses.

Proceso: PLAN PARA LA AUDITORÍA EXTERNA

AUDITORÍA EXTERNA	
Entradas	Lista de controles y características físicas, técnicas y administrativas.
Salidas	Revisión detallada de los controles y características físicas, técnicas y administrativas.
Objetivo	Auditar infraestructura tecnológica del CETPRO
Responsable	Empresa auditora.
Clientes	CETPRO.
RRHH	Los que la empresa auditora provea.
Equipos o materiales	Los que la empresa auditora provea.
Costos	Relacionado con el contrato de la empresa auditora.
Tiempo	Cada fin de semestre.

2.2.3 Auditoría informática. Castello (2006) explica que etimológicamente el término auditoría proviene del idioma latín con la palabra *audire*, esta última tiene un significado referente al *oír*, cuando se emplea el sustantivo del latín se traduce como *el que oye*. En antaño las personas que tenían la función de *oír* se les llamaba auditores, estas personas poseían la potestad de juzgar la verdad o la falsedad de lo que estaban verificando. Muñoz (2002) nos explica que la auditoría es buscar, observar e indagar de forma totalmente independiente la actividad o las actividades de un grupo de personas o alguna persona en particular, luego de esta observación sistemática se debe documentar y esto debe conllevar al análisis profesional que visto de otra manera es una opinión con autoridad. Para Muñoz (2002) hablar de auditoría de *sistemas computacionales* es lo mismo que *auditoría informática*, el autor menciona que esta es la primera definición que se debe aprender ya que con ella se conceptualiza en forma global todas las demás definiciones de auditoría en sistemas. Tomando en cuenta las definiciones de los expertos anteriormente mencionados, en esta investigación auditoría lo conceptualizaremos como una revisión ética, estructurada y sistemática de una o unas actividades para valorar el desempeño de los juicios de los objetivos a que aquellas corresponden acatarse.

a) ***Procedimientos para realizar auditoría informática.*** Los académicos Piattini & Del Peso (2001) hablan sobre los **procedimientos**, sucede que existe un profesional (hablamos del auditor), y su acción de auditar se demuestra por medio de procedimientos específicos tendientes a proveer seguridad sensata a los que se afirma.

Es natural para todos los tipos o clases de auditoría se poseen sus propios profesionales y con ellos sus procedimientos propios para conseguir el fin predicho que se plantea al iniciar cada auditoria. Estos procedimientos, valgan la redundancia sirven para proceder, y proceder es la ejecución de la auditoría que a palabras de Piattini & Del Peso (2001), se resumen en tres puntos que el audito debe pasar:

a. La labor se planifica y se supervisará apropiadamente.
b. Estudiar y evaluar el control interno.
c. Observar la evidencia.

b) ***Control interno.*** Otro aspecto importante en la auditoria, no solo informática sino cualquier clase de auditoría es el **control interno.** No existe autor serio que desligue este aspecto importantísimo.

Una pregunta que nos planteamos sería *¿de qué tipo de control hablamos?,* Piattini & Del Peso (2001) nos da ciertos ejemplos sobre los **controles**, son los contrales sobre la producción del día a día, sobre eficiencia y calidad del mantenimiento y desarrollo del software, sobre las redes de comunicación, de los sistemas operativos, de los sistemas microinformáticos, y controles sobre la seguridad informática.

Castello (2006) nos habla sobre los elementos para realizar un sistema de control, entre ellos tenemos:

a. **El elemento**, es lo que se quiere controlar puede ser una condición o también una característica.

b. **Sensor**, es un instrumento que sirve para medir, cuantificar o acotar al elemento (o elementos) a controlar,

c. **Grupo de control**, tan igual como en un experimento, el grupo control sirve para contrastar o comparar todos los datos que han sido medidos. Es un punto de apoyo para observar el rendimiento esperado.

c) ***Planeación de la auditoría.*** Es el momento de preguntarnos ¿cómo se planea o se hace el plan de auditoría informática?, Echenique (2001) dice que antes de realizar una planeación de la auditoría informática se necesitan unos pasos previos que ayudaran a:

a. Dimensionar el tamaño de lo que se va a auditar.

b. Dimensionar las características del espacio dentro del organismo que se va observar (auditar).

c. Sus sistemas involucrados en lo que se va a auditar.

d. La organización comprometida en lo que se va a auditar.

e. El equipo responsable de la auditoria.

Todo ello mencionado anteriormente sirven para saber el número y cualidades de los auditores, los instrumentos que se necesitarán para la auditoría, el costo y tiempo, así como el alcance de la misma auditoría. Pero aún no explica cómo se da en sí una **planeación** de la auditoría informática. Echenique (2001) explica que los pasos para la planeación son los mismos que se dan para una *auditoría en general*. Esta debe ser documentada e incluirá:

a. Alcance y objetos de la labor.

b. Obtención de los datos de soporte sobre lo auditable.

c. Recursos para la auditoría.

d. La comunicación necesaria con los implicados en el trabajo de auditoría.

e. Inspección física afín habituarse con los controles a auditar.

f. El preparativo altamente documentado y por escrito de lo que se va a auditar.

g. El conocimiento del cómo, cuándo y a quién se le dará los resultados.

h. Obtener el consentimiento del plan de auditoría.

Echenique (2001) nos sigue explicando que la planeación de una auditoría informática tiene todas las *características* de la planeación de una **auditoria en general**, pero siempre se tiene que tener las apreciaciones de vista de los objetivos propia de la especialidad, como son valoración administrativa del área de los procesos electrónicos, valoración de los sistemas y procedimientos, evaluación de los equipos de cómputo, valoración del sistema, de dispositivos, del software, del hardware, de las redes, de las bases de datos, procesamiento de datos, etc., evaluación de la seguridad y confidencialidad de la información, y temas legales de los sistemas y de la información.

Algunos consejos que el autor Echenique (2001) nos da para tener éxito en la planeación es tener metas, tener programas de trabajo de auditoría, tener un plan de contratación de personal que nos puedan ayudar en la auditoría, y tener informes de actividades siempre.

d) ***Fases de la auditoría.*** Para Echenique (2001) en su libro ***auditoría en informática*** señala que son siete las fases de la auditoria informática:

a. Planeación de la auditoría.

b. Examen preliminar.

c. Estudio detallado.

d. Análisis y valoración de la información.

e. Ensayos de consentimiento.

f. Ensayos de controles del usuario.

g. Ensayos sustantivos.

Todo auditor en informática, deben usar una serie de técnicas, métodos, procedimientos o herramientas para que en cada una de las siete fases de la auditoria mencionadas por Echenique (2001), tenga el alcance y los resultados previstos y sobre todo estén documentados. Entre ellos tenemos el examen propiamente dicho, inspecciones, confirmaciones, comparaciones, revisiones documentales, acta testimonial, matriz de evaluación, y matriz FODA.

2.2.4 Centros de educación técnico productiva. Todo el marco normativo de la Educación Técnico Productiva recae en la Resolución Directoral 0920-2008-ED (2008). En las siguientes líneas se expone una síntesis de la resolución.

a) ***Objetivos.*** Los objetivos de la educación técnico productiva según la Resolución Directoral 0920-2008-ED (2008) se centran en desarrollar las capacidades y competencias que se necesitan en las actividades laborales ya sean de forma independiente o dependiente, para ello la preparación y motivación no

sólo apunta a la aplicación de lo aprendido en clases, sino que también se incentiva el desenvolvimiento empresarial que promueva el desarrollo nacional.

b) ***Ciclos en la educación técnico productiva.*** La Resolución Directoral 0920-2008-ED (2008) manifiesta lo siguientes ciclos:

- **Ciclo Básico:** Da al alumno capacidades y competencias laborales necesarias para realizar trabajos de menor dificultad.

- **Ciclo Medio:** Da al alumno competencias para el desarrollo de actividades ocupacionales especializadas.

c) ***Curso de computación.*** Según la Resolución Directoral 0920-2008-ED (2008) hay curso que son exclusivamente de instrucción complementaria, como orientación profesional, inglés, informática, y administración empresarial.

2.3. Marco Conceptual

- **Amenaza:** Natural Disasters and Vulnerability Analysis (1979) dijeron que es una probabilidad de que ocurra un suceso desastroso durante un periodo de tiempo en un lugar determinado.

- **Calidad**: Guajardo (1996) explica que es el nivel adicional con que se percibe con mucho agrado del bien o servicio que se adquiere.

- **Estrategia:** Porter (2015) comenta que es una serie de pasos cuidadosamente estudiados que son para mejorar los resultados en algo.

- **Gestión de la calidad:** Porter (2015) expone que son tareas estructuradas para administrar la empresa en el contexto de la calidad.

- **Gestión:** Gómez (2012) dice: "Es llevar a cabo acciones que hagan posible la realización de una operación comercial." (p. 10).

- **Plan:** Gómez (2012) dice: "Es un modelo sistemático elaborado antes de realizar una acción, con el fin de tomar la decisión de realizarla ya tenga una dirección establecida." (p. 10).

- **Riesgo:** Natural Disasters and Vulnerability Analysis (1979) dijeron que son las perdidas, daños y efectos indeseados sobre las actividades normales de la institución.

- **Seguridad:** Ramírez (2005) explicó que es el bienestar de un sistema correlacionado con sus actividades cotidianas de cada elemento que lo conforma.

- **Sistema de gestión de la calidad:** Porter (2015) comenta que es o son los segmentos de un sistema de gestión concerniente con todos los puntos y temas de la calidad.

- **Sistema de gestión:** Porter (2015) lo vincula con un grupo de compendios de una formación relacionados para instituir procesos, objetivos de calidad y políticas y así alcanzar estos objetivos.

- **Vulnerabilidad:** Natural Disasters and Vulnerability Analysis (1979) dijeron que es el grado de pérdida de algún elemento del sistema bajo riesgo del posible suceso desastroso.

CAPÍTULO III:

MÉTODO

3.1. Tipo de Investigación

Esta investigación se consideró de **tipo aplicada**, porque se puso en ejecución una solución inmediata a un problema observado, en contra posición a una investigación de tipo *pura* que es muy posible que se guarde en la biblioteca y sirva únicamente para obtención del grado.

3.2. Diseño de Investigación

Hernández et al. (2010) nos expone que hay bastante literatura científica en donde se puede encontrar diferentes diseños para la investigación; pero él adopta la postura de clasificarlos en dos, *diseño experimental* y *diseño no experimental*. Por lo expuesto y en vista que la variable independiente de esta investigación (p1an de gestión de 1a ca1idad) va a tener una *relación de causalidad* (causa - efecto) sobre

la variable dependiente (estrategia de seguridad y auditorías informáticas); y sobre todo desestimando la idea de la inutilización preparada de variables donde simplemente se miran los fenómenos en su contexto para luego estudiarlos, es por ello que **esta investigación fue de tipo experimental,** y estuvo por fases, en las siguientes líneas se las describe.

- **Primera fase** Identificación de los problemas de seguridad informática de los *CETPROs a* de la muestra de estudio por medio de pre-pruebas (auditoria informática).
- **Segunda fase:** Elaboración del plan de gestión de la calidad para los *Centros de Educación Técnico Productiva* de la muestra de estudio.
- **Tercera fase:** Aplicación del p1an de gestión de 1a ca1idad.
- **Cuarta fase**: Utilización de técnicas de recojo de datos en la muestra estudiada a través pospruebas (auditoria informática)
- **Quinta fase:** Observación estadística de la data obtenida en las fases uno y cuatro.
- **Sexta fase:** Contratar la hipótesis de la tesis.
- **Séptima fase:** Conclusiones y recomendaciones a nivel general y específicas.

3.3. Población y Muestra

3.3.1 Población. Conformada por el total de *estrategias de seguridad y auditorias informáticas* de los CETPROs que existieron hasta el año 2016 en la ciudad de Ilo. El Ministerio de Educación, por medio de su sitio web (llamado *mapa de escuelas*) usa una herramienta interactiva que permite a los visitantes, situar la oferta del servicio educativo en cada ciudad del Perú.

Tabla 3

Relación de Centros de Educación Técnico Productiva en la ciudad de Ilo.

Departamento	Provincia	Nombre	Dirección
Moquegua	Ilo	José Manuel Ubalde Zeballos	Jr. Pichincha 431
Moquegua	Ilo	Mariscal Domingo Nieto	Jr. Mirave 441

Fuente: http://sigmed.minedu.gob.pe/mapaeducativo/

3.3.2 Muestra. La muestra utilizada en la esta investigación fue de tipo **censal**. Como la población del estudio es pequeña **se tomó la totalidad de la población**.

3.4. Técnicas e Instrumentos para la Recolección de Datos

La pericia manejada fue el análisis de contenido. Zapata (2005) explica que el análisis de contenido es adecuado para la pesquisa cuantitativa o experimental y

que se puede ejecutar por múltiples intenciones. La herramienta de cogida de la data empleada fue la hoja de verificación (ver anexos 2 y 3). Summers (2006) dice: “Una hoja de verificación tiene muchas aplicaciones y el usuario puede adaptarlas a cualquier situación particular” (p. 242).

3.5. Técnicas de Procesamiento y Análisis de Datos

3.5.1 Técnicas de procesamiento de datos. Hernández et al. (2014) explica que hay que hacer varios pasos para resolver la data de la pesquisa, él menciona los siguientes cuatro pasos que fueron los mismos que esta investigación usó como técnica:

a. Codificación de los datos recolectados.

b. Transferencia a una matriz.

c. Guardarlo en un archivo.

d. Depurar los errores.

Adicionalmente Hernández et al. (2014) nos narra que en la actualidad ya no se hace de manera manual el procesamiento de los datos, sino que al contrario buscando siempre ahorrar tiempo y no cometer errores, esta se efectúa en un archivo digital. El experto Hernández et al. (2014) recomienda usar softwares informáticos

para el proceso de la data obtenidas en la investigación, a su experiencia personal Hernández et al. (2014) sugiere software como IBM SPSS (Statistical Product and Service Solutions) y Minitab.

3.5.2 Técnicas de análisis de datos. Esta investigación siguió siete fases que Hernández et al. (2014) nos recomienda:

a. Elegir un programa adecuado para análisis de la data.

b. Ejecutar el programa informático.

c. Analizar descriptivamente y observar la data por variables.

d. Verificar la confiabilidad y validez logradas por los instrumentos de medición.

e. Examinar mediante ensayos estadísticos las suposiciones iniciales.

f. Realizar exámenes anexos.

g. Preparar los resultados para mostrarlos en, figuras, cuadros, tablas y gráficos.

CAPÍTULO IV:

PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

4.1. Presentación de Resultados por Variables

Se usó la prueba de hipótesis de *McNemar* por ser una investigación donde se provoca un cambio en la respuesta dicotómica en un antes y después, dicha prueba se empleó para cada caso de estudio de la población. El computo fue ejecutado en el software de estadística *IBM SPSS Statistics* v. 23. La variable independiente (p1an de gestión de 1a ca1idad) fue medida a través de 58 indicadores y la variable dependiente (estrategia de seguridad y auditorías informáticas) con 94 indicadores. Se usó una escala de valores decimales de cero a uno para calificar ambas variables por medio del cociente resultante del número de respuestas positivas y el número total de indicadores, esto se realizó en la pre-prueba y pos-prueba del *CETPRO* control y experimental, obteniéndose los siguientes resultados.

Tabla 4
Cantidad de valores afirmativos de la pre y pos-prueba de las variables.

	Variables	Total de respuestas positivas	Cantidad de indicadores	Valor del cociente
PRE - PRUEBA	Variable indep.[1] CETPRO control	8	58	0,13
	Variable dep.[2] CETPRO control	17	94	0,18
	Variable indep. CETPRO experimental	8	58	0,13
	Variable dep. CETPRO experimental	16	94	0,17
POS - PRUEBA	Variable indep. CETPRO control	8	58	0,13
	Variable dep. CETPRO control	17	94	0,18
	Variable indep. CETPRO experimental	52	58	0,89
	Variable dep. CETPRO experimental	85	94	0,90

Independiente[1], Dependiente[2].

Fuente, elaboración propia.

El cociente oscila entre cero (valor más indeseable) y uno (valor más deseable), este cociente y se adquiere dividiendo la cantidad total de respuestas positivas entre su cantidad de indicadores; la tabla manifiesta la sinopsis de los resultados hallados de la pre-prueba y pos-prueba para las dos variables de estudio en los dos grupos investigados. El cociente obtenido en las pre-pruebas del grupo control y

experimental son bajos, las pos-pruebas del CETPRO control también son bajos, en cambio las pos-pruebas del grupo experimental se consideran cocientes altos.

4.1.1. Presentación de resultados de la variable dependiente. La variable dependiente (estrategia de seguridad y auditorías informáticas) fue medida en la primera y cuarta etapa del diseño de investigación, la siguiente tabla muestra los resultados hallados.

Tabla 5
Resultados finales de la pre-prueba y pos-prueba - variable dependiente.

		CETPRO CONTROL Mariscal Domingo Nieto			CETPRO EXPERIMENTAL José Manuel Ubalde Zeballos		
		DESPUÉS			**DESPUÉS**		
		No	**Si**	**Total**	**No**	**Si**	**Total**
ANTES	**No**	77	0	77	9	69	78
	Si	0	17	17	0	16	16
Total		77	17	94	9	85	94

Fuente elaboración propia, calculado con el software *IBM SPSS Statistics v23*.

Esta tabla explica que en la primera observación con la carencia o supresión de un plan de la gestión de la calidad el *CETPRO control* tenía antes 77 ítems marcados de forma negativa y diecisiete de forma positiva, posteriormente en la segunda observación, continuando con la ausencia de un plan de la gestión de la calidad el *CETPRO control* volvió a tener 77 ítems marcados de forma negativa y diecisiete

ítems marcados de manera positiva. Para el *CETPRO experimental* en la pre-prueba tuvo 78 ítems marcados de forma negativa, y dieciséis ítems positivos, en cambio luego se tuvo 85 ítems marcados positivamente y sólo nueve ítems marcados negativamente.

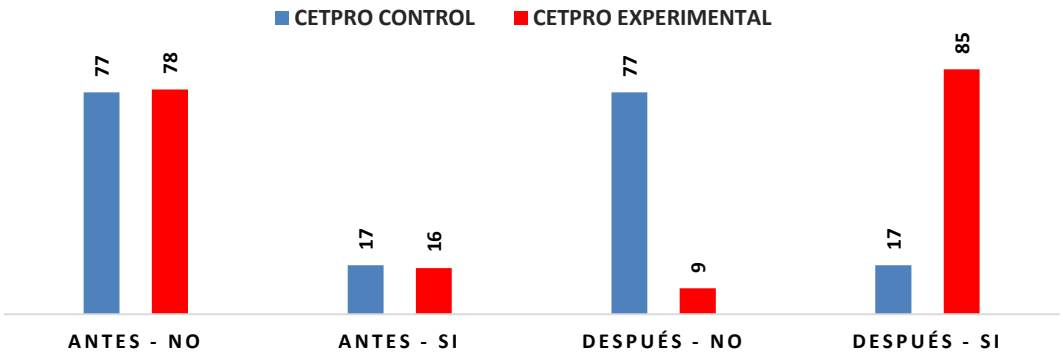

Figura 1. Gráfico de barras correspondiente a los efectos de la pre-prueba y pos-prueba de la variable dependiente. Fuente propia.

4.1.2. Presentación de resultados de la variable independiente. A continuación, se describe en la tabla de abajo los resultados computados por el software estadístico *IBM SPSS Statistics,* resultantes de medir de la variable independiente (plan de gestión de la calidad).

Tabla 6
Resultados finales de la pre-prueba y pos-prueba - variable independiente.

		CETPRO CONTROL Mariscal Domingo Nieto			CETPRO EXPERIMENTAL José Manuel Ubalde Zeballos		
		DESPUÉS			**DESPUÉS**		
		No	**Si**	**Total**	**No**	**Si**	**Total**
ANTES	**No**	50	0	50	6	44	50
	Si	0	8	8	0	8	8
Total		50	8	58	6	52	58

Fuente elaboración propia, calculado con el software *IBM SPSS Statistics v23*.

El *CETPRO control,* antes en su primera observación se poseyó cincuenta ítems marcados negativamente y ocho marcados positivamente, luego en la segunda observación cincuenta ítems se señalaron como negativos y ocho como positivos, es decir sin cambios. Para el CETPRO experimental, en la primera observación se obtuvo cincuenta indicadores marcados negativamente y ocho positivamente, en la segunda observación seis ítems fueron marcados negativamente y 52 ítems positivamente, existiendo una diferencia entre un antes y después.

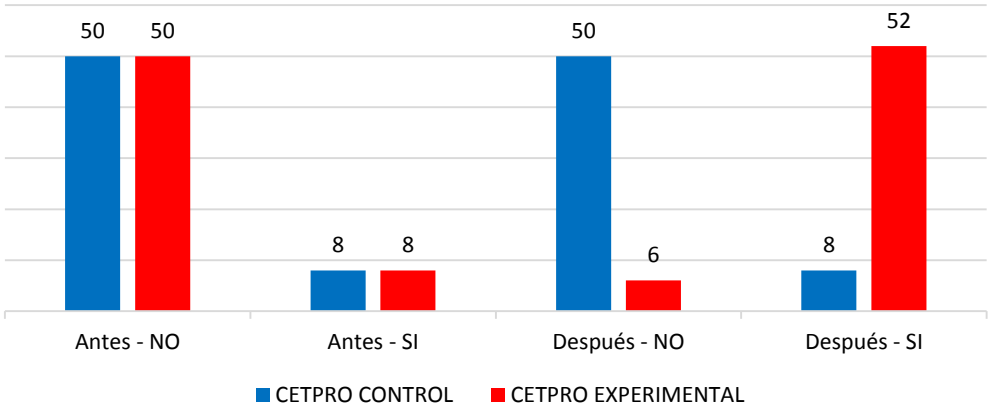

Figura 2. Resultados finales de la pre-prueba y pos-prueba - variable independiente. Fuente propia.

En el gráfico se ven los resultados de la recolección de datos antes y posteriormente de la implantación de un *plan de gestión a la calidad* para el CETPRO experimental, también se ven los resultados del antes y después del CETPRO control que no fue expuesto a un plan de gestión de la calidad.

4.2. Contrastación de Hipótesis

En la siguiente tabla se muestra el contraste de hipótesis específicas.

Tabla 7
Prueba de hipótesis específicas.

Hipótesis	p-valor	Nivel de significancia
Primera hipótesis específica.	0,000	0,05
Segunda hipótesis específica.	0,031	0,05
Tercera hipótesis específica.	0,000	0,05
Cuarta hipótesis específica.	0,000	0,05

Fuente, elaboración propia, calculado en el software IBM SPSS Statistics v23.

En la tabla se observa el *p-valor* de cada hipótesis específica realizada en este estudio; obsérvese que en cada caso los *p-valores* son menores al nivel de significancia convencional del 5%, es decir $p<0,05$ **entonces rechazamos las hipótesis nulas específicas, y nos quedamos con las hipótesis específicas del investigador.**

- **Hipótesis general del investigador.** H_1. Un p1an de gestión de 1a ca1idad influirá significativamente en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

- **Hipótesis general nula.** H_0. Un p1an de gestión de 1a ca1idad no influirá significativamente en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

Tabla 8
Prueba de hipótesis general.

	Valor	Significación exacta (bilateral)
Prueba de Mc. Nemar		0,000[a]
N° de casos legítimos	94	
[a.] *Distribución binomial utilizada.*		

Fuente, elaboración propia, calculado con el software IBM SPSS Statistics v23.

Para contrastar en esta tesis la hipótesis general se manipuló un nivel de significancia convencional del 5%. El software *IBM SPSS Statistics* mostró un p-valor (valor de probabilidad) de 0,000. **La estimación del p-valor es menor que e1 nive1 de significancia, es decir p<0,05 entonces rechazamos la H_0 (hipótesis nu1a) y nos quedamos con 1a H_1 (hipótesis del investigador).**

4.3. Discusión de Resultados

A partir de los descubrimientos expuestos, damos por aceptado todas las hipótesis alternativas específicas y la hipótesis alternativa general, esta última establece que la aplicación de un p1an de gestión de 1a ca1idad influirá significativamente en la

estrategia de seguridad y auditorías informáticas en los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo.

Estos resultados guardan relación con lo que sostienen Villatoro Segovia, Villalobos Meza, & Posada Pineda (2007). Los autores explican que un plan de gestión que se relacione en mejorar las auditorías informáticas favorece a perfeccionar 1a efectividad administrativa relacionado con e1 uso de los recursos de tecnología. Lo dicho se acomoda con lo que en este estudio halló.

También los resultados de esta investigación tienen coherencia con lo que el autor Parra Giraldo (2014). explica diciendo que las medidas de seguridad informática deben estar conducidas por procedimientos y po1íticas que favorezcan a consolidar dispositivos de defensa, en ayuda de 1a seguridad informática.

Esta investigación tiene relación con lo hallado por Liñán Salinas (2008), el autor explica que, sin la aplicación de un plan de seguridad informática, la situación de es deficiente respecto a la seguridad, al contrario que cuando se aplica un plan de gestión en donde si hay una mejora sustancial en la seguridad informática.

Por otra parte, el segundo objetivo específico de esta investigación está muy relacionada con lo que descubrieron Barrantes Porras, & Hugo Herrera (2012), ellos narran que la implementación de políticas, es de gran utilidad cuando se quiere implementar cualquier sistema de gestión en una cualquier organización privada, estatal, gubernamental, empresa o institución.

Esta tesis tiene coherencia con lo que investigó Aucancela (2012), el autor explica que para llevar a cabo un sistema de gestión de seguridad es necesario tener antes un plan de seguridad.

Por ninguna fuente se ha encontrado que esta investigación no guarde relación con los beneficios del empleo de un p1an de gestión de 1a ca1idad. Por 1os resultados obtenidos, aceptamos todas las hipótesis específicas del investigador. Factorizando la lista de hipótesis específicas se atribuye que el empleo de una po1ítica de ca1idad para el personal, el manejo de objetivos de ca1idad para las aplicaciones, la utilización de un manual de ca1idad para las operaciones, y el desarrollo de procedimientos para la infraestructura, influyeron significativamente en la estrategia de seguridad y auditorías informáticas en los CETPROs particulares de enseñanza de computación de la ciudad de Ilo.

CAPÍTULO V:

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

5.1.1. Conclusión general. En esta tesis se determinó la influencia de un p1an de gestión de 1a ca1idad en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de computación de la ciudad de Ilo. La estrategia de seguridad y auditoría informática fue medida por 94 ítems respondidos por el CETPRO control y experimental en un antes y después, usando una escala de cero a uno. El CETPRO control obtuvo resultados positivos en diecisiete ítems tanto en la pre y pos prueba, los cuales dan para la estrategia el valor de cociente de 0,18. En la pre-prueba, el CETPRO experimental logro resultados positivos en dieciséis ítems, luego de desarrollar el sistema de gestión de 1a ca1idad la pos-prueba arrojó 85 ítems marcados positivamente, dando como cociente el valor de 0,90. El contraste de hipótesis rechazo la hipótesis nula, quedándonos con la hipótesis que: un p1an de gestión de 1a ca1idad influyó significativamente en la estrategia de seguridad y auditorías informáticas de los CETPRO particulares de enseñanza de computación de la ciudad de Ilo.

5.1.2. Conclusiones específicas. Lo mostrado a lo largo de esta tesis permite arribar las siguientes conclusiones específicas, ellas fueron obtenidas mediante las influencias de indicadores en un antes y después, empleando una escala de cero a uno, tanto para el CETPRO control como para el experimental, y fueron contrastadas con la prueba de hipótesis de *McNemar*, a continuación, se explica.

- **Primera conclusión específica**. La investigación se estableció la influencia de una política de calidad, basado en el esquema adaptado del estándar ISO27001:2014 en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo. La influencia de una política de calidad fue medida por seis ítems, el cociente para el CETPRO control fue de 0,16 y para el experimental de uno, su prueba de hipótesis tuvo un p-valor de 0,000 demostrando así que la política de calidad redactada influyó significativamente en la estrategia de seguridad y auditorías informáticas.

- **Segunda conclusión específica**. A través de este estudio se determinó la influencia de objetivos de calidad, basado en el esquema adaptado del estándar ISO27001:2014 en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo. La influencia de los objetivos de calidad fue medida por ocho ítems, siendo sólo un ítem positivo en la pre y post prueba del CETPRO control, en el caso del CETPRO experimental se consiguió siete ítems marcados positivamente en la pos prueba,

obteniéndose así para el CETPRO control y experimental, cocientes de 0,12 y 0,87 respectivamente.

- **Tercera conclusión específica**. En esta pesquisa se halló la influencia de un manual de ca1idad, basado en el esquema adaptado del estándar ISO27001:2014 en la estrategia la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo. Fueron 23 ítems los que midieron la influencia del manual de calidad, para el CETPRO control se tuvo cuatro ítems positivos tanto en el pre como en la post prueba, en cambio en el CETPRO experimental se alcanzó dieciocho ítems positivos en la post prueba. Dando cocientes para el CETPRO control y experimental de 0,17 y 0,78 respectivamente.

- **Cuarta conclusión específica**. Se descubrió la influencia de procedimientos basado en el esquema adaptado del estándar ISO27001:2014 en la estrategia de seguridad y auditorías informáticas de los *CETPROs* particulares de enseñanza de computación de la ciudad de Ilo. El CETPRO control alcanzó en el antes y después, once ítems positivos, en cambio el CETPRO experimental consiguió 54 ítems positivos en el después de un total de 57 ítems, esto señalo un cociente de 0,19 para el CETPRO control y 0,94 para el CETPRO experimental.

5.2. Recomendaciones

5.2.1. Recomendación general. Esta investigación recomienda emplear un número igual de ítems por cada dimensión de las variables de estudio a fin de otorgar equidad entre ellas; se invita hacer la experimentación en más de una oportunidad y analizar la varianza de los resultados obtenidos en dichos experimentos, también se recomienda otorgar significados a los rangos del cociente obtenido sin importar la escala que se emplee. Se aconseja continuar computando y estudiando los resultados positivos de los indicadores. Se sugiere que la alta dirección se vincule con estrategias de mercadotecnia en concordancia a los p1anes de sistemas de calidad y seguridad informática, se recomienda investigar sobre los p1anes de gestión de 1a ca1idad y su influencia en la educación virtual.

5.2.2. Recomendaciones específicas. Considerando el valor que tiene esta tesis en las investigaciones a futuro en la ciudad de Ilo, y en función de 1os resu1tados obtenidos se dan las siguientes recomendaciones.

- **Primera recomendación específica**. Se aconseja que la política de calidad tenga tantos ítems de medición como directrices posea esta, se recomienda que el rango del resultado del cociente tenga calificativos diferenciados de las demás partes del

p1an de gestión de 1a ca1idad. Aparte de escribir la po1ítica de ca1idad para el grupo experimental se aconseja redactar una política placebo para el grupo control.

- **Segunda recomendación específica**. Se recomienda confeccionar objetivos paliativos para el grupo control y que estos tengan la misma cantidad en el grupo experimental. También se recomienda que para medir la estrategia que es influenciada por los objetivos de calidad, esta estrategia se cuantifique con la misma cantidad de ítems como cantidad de objetivos existan.

- **Tercera recomendación específica**. Se sugiere que el instrumento de medición de la estrategia influenciada por el manual de calidad posea menos de veinte ítems afín de ser más sencillo y directo. Se recomienda proporcionar un manual básico al grupo control que incluya política placebo, objetivos paliativos, y lista de acciones.

- **Cuarta recomendación específica**. Se encomienda a todas las investigaciones futuras que el instrumento de medición de la estrategia influenciada por los procedimientos basados en algún estándar internacional tenga un promedio de treinta ítems esto ayudaría a identificar las partes más importantes de los procesos, obviando aquello que no es relevante.

REFERENCIAS BIBLIOGRÁFICAS

Abarca Alvarado, V. E., Pandilla Calderón, W. E. & Portillo López, M. L. (2005). *Diseño de un modelo de auditoría TI como herramienta de evaluación y control para la adecuada utilización de los recursos tecnológicos en las áreas funcionales de los centros educativos biculturales en el Salvador* (Tesis de pregrado). Universidad Francisco Gavidia, San Salvador.

Alcántara Flores, J. C. (2015). *Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P. en la ciudad de Chiclayo* (Tesis de pregrado). Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Perú.

Alfaro Paredes, E. A. (2008). *Metodología para la auditoría integral de la gestión de la tecnología de información* (Tesis de pregrado). Pontificia Universidad Católica del Perú, Lima, Perú.

Álvarez Basaldúa, L. D. (2005). *Seguridad en informática (Auditoría de Sistemas)* (Tesis de maestría). Universidad Iberoamericana, México D. F., México.

Álvarez, M. (6 de agosto de 2013). *Es importante que un profesor esté capacitado en temas de seguridad informática*. Lima, Perú: Repensar Educativo. Recuperado de http://repensareducativo.com/

Arens, A. A., Elder, R. J. & Beasley, M. S. (2007). *Auditoría Un enfoque integral*. México D. F., México: Pearson Educación.

Asociación Colombiana de Ingenieros de Sistemas (2010). *Cultura de la seguridad de la información*. Bogotá, Colombia: ACIS. Recuperado de http://www.acis.org.co/

Asociación Española para la Calidad (27 de agosto 2010). *Ventajas de los sistemas de gestión de calidad.* Madrid, España: AEC. Recuperado de https://www.aec.es/c/document_library/get_file?uuid=0fed9322-3dea-4211-b748-a1e041a60b01&groupId=10128

Atehortúa Hurtado, F. A., Bustamante Vélez, R. E., & Valencia de Ríos, J. A. (2008). *Sistema de gestión integral: Una sola gestión, un solo equipo.* Medellín, Colombia: Editorial Universidad de Antioquia.

Aucancela Soliz, J. G. (2012). *Auditoría de riesgos informáticos del departamento de sistemas de CAVES SA EMA utilizando COBIT como marco de referencia* (Tesis de maestría). Escuela Politécnica del Ejercito, Sangolqui, Ecuador.

Bañeras, J. (11 de junio de 2014). *La importancia de la calidad en la Gestión Empresarial*. Madrid, España: IMF Business School. Recuperado de http://www.imf-formacion.com/

Barrantes Porras, C. E., & Hugo Herrera, J. R. (2012). *Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos* (Tesis de pregrado). Universidad San Martin de Porres, Lima, Perú.

Baud, J. L. (2015). *Preparación para la certificación ITIL Foundation V3: ITIL V3-2011*. Barcelona, España: ENI ediciones.

British Standards Institution (2011). *Sistemas de Gestión Integrados: Aprovechar al máximo los diferentes sistemas de gestión*. Madrid, España: The British Standards Institution. Recuperado de https://www.bsigroup.com/

Buitrago Estrada, J. C., Bonilla Pineda, D. H., & Murillo Varon, C. E. (2012). *Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - SGSI, en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001* (Tesis de maestría). Universidad Escuela de Administración y Negocios, Bogotá, Colombia.

Calder, A. & Watkins, S. (2015). IT *Governance: An international guide to data segurity and ISO27001/ISO27001*. London, United Kingdom:Kogan Page.

Camisón, C., Cruz, S. & González, T. (2006). *Gestión de la calidad: Conceptos, enfoques, modelos y sistemas*. Madrid, España: Editorial Pearson Prentice Hall.

Carbajal Romero, J. (2013). *Definición de una metodología para la elaboración de auditorías de sistemas informáticos en entidades del sistema nacional de control peruano* (Tesis de maestría). Universidad de Piura, Lima, Perú.

Carpentier, J. F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Barcelona, España: ENI ediciones.

Castello, R. J. (2006). *Auditoría en entornos informáticos*. Argentina: Universidad Nacional de Córdoba.

Cortés, J. M. (2017). *Sistemas de Gestión de Calidad (ISO 9001:2015).* Málaga, España: Interconsulting Bureau S. L.

Corletti Estrada, A. (2011). *Estrategia de seguridad informática por capas, aplicando el concepto de Operación Militar por Acción Retardante* (Tesis de doctorado). Universidad Nacional de Educación a Distancia, Madrid, España.

Decreto Supremo N° 029-2004-MINCETUR (2004). *Reglamento de Establecimientos de Hospedaje*. Lima, Perú: MINCETUR.

Díaz Sáenz, J. R. (2015). *Factores críticos en la adopción de las medidas de seguridad utilizadas por los alumnos de los Centros formativos universitarios de tecnologías TIC al usar herramientas 2.0* (Tesis de doctorado). Universitat Politècnica de València, Valencia, España.

Fontalvo, T. & Vergara, J. (2010). *La gestión de la calidad en los servicios ISO 9001:2008.* Málaga: Editorial Eumed - Universidad de Málaga.

Global State of Information Security Survey (2011). *Global State of Information Security® survey 2017 - Webcast replay*. USA: PwC network. Recuperado de http://www.pwc.com/

Gómez Fernández, L. & Andrés Álvarez, A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.* Madrid, España: AENOR.

Gómez, I. (2011). *Preguntas frecuentes ISO 9001:2008*. Madrid, España: Hedera Consultores. Recuperado de www.hederaconsultores.com/docs/preguntas_frecuentes_ISO_9001

Gonzáles Ortiz, O. C. & Arciniegas Ortiz, J. A. (2016). *Sistemas de gestión de calidad.* Bogotá, Colombia: ECOE Ediciones Ltda.

Guasch, J. L., Racine, J. L., Sánchez, I. & Diop, M. (2008). *Sistemas de calidad y estándares hacia la construcción de ventaja competitiva*. Bogotá, Colombia: Ediciones Mayol.

Hernández Sampieri, R., Fernández Collado, C. & Baptista Lucio, M. (2014). *Metodología de la investigación.* México D.F., México: Editorial Mc Graw Hill.

Huamán Monzón, F. M. (2017). *Plan de comunicaciones en seguridad de la información para el personal administrativo de la Pontificia Universidad Católica del Perú* (Tesis de maestría). Pontificia Universidad Católica del Perú, Lima, Perú.

Instituto Nacional de Calidad. (2016). *INACAL*. Lima, Perú: Ministerio de la Producción. Recuperado de https://www.inacal.gob.pe/

Jara, H. & Pacheco, F. (2011). *Hacking desde Cero: Conozca sus vulnerabilidades y proteja su información*. Buenos Aires, Argentina: Fox Andina, Red USERS.

Jiménez Paneque, R. (1998), *Metodología de la Investigación. Elementos básicos para la investigación clínica.* La Habana, Cuba: Editorial Centro Nacional de información de Ciencias Médicas.

Lanche Capa, D. S. (2015). *Diseño de un sistema de seguridad de la información para la compañía ACOTECNIC Cía. Ltda. basado en la norma NTE INEN ISO/IEC 27002* (Tesis de maestría). Universidad de Cuenca, Cuenca, Ecuador.

Liñán Salinas, E. (2008). *Plan de seguridad informática en la Escuela Universitaria de Posgrado de la Universidad Nacional Federico Villarreal* (Tesis de pregrado). Universidad Wiener, Lima, Perú.

Martin, M. (2008). *Guía de Seguridad: 9 Pasos para Implementar la Seguridad Informática en su Empresa*. Madrid, España: Microsoft.

Mateo, R. J. (6 de julio 2014). *Sistemas de gestión de la calidad: Un camino hacia la satisfacción del cliente.* República Dominicana: Quality Trends. Recuperado de http://qualitytrends.squalitas.com/index.php/item/108-sistemas-de-gestion-de-la-calidad-un-camino-hacia-la-satisfaccion-del-cliente-parte-i

Membrado, J. (2007). *Metodologías avanzadas para la planificación y mejora.* Madrid, España: Editorial Díaz de Santos S.A.

Ministerio de Educación (2008). *Diseño curricular básico de la Educación Técnico Productiva: Ciclo Medio*. Lima, Perú: Ministerio de Educación.

Ministerio de Educación (2015). *Mapas*. Lima, Perú: Unidad de Estadística Educativa. Recuperado de http://escale.minedu.gob.pe/mapas

Ministerio de Fomento (2005, mayo). Modelos para implantar la mejora continua en la gestión de empresas de transporte de carretera. *Sistema de Gestión de la Calidad según ISO 9001:2000*. Recuperado de https://www.fomento.gob.es/

Morantes Moreno, F. O. (2016). *Análisis Forense* (Tesis de maestría). Universitat Oberta de Catalunya, Barcelona, España.

Muñoz, C. (2002). *Auditoría en sistemas computacionales*. México D. F., México: Pearson Educación.

Natural Disasters and Vulnerability Analysis (1979). *Natural disasters and vulnerability analysis : report of Expert Group Meeting* (01). Recuperado de https://archive.org/details/naturaldisasters00offi/page/n1

Organización Internacional de Normalización (2014). *Tecnología de la información. Técnicas de seguridad. Sistemas de seguridad de la información. Requisitos*. Lima, Perú: INDECOPI.

Organización Internacional de Normalización (2016). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Ginebra, Suiza: ISO.

Pallas Mega, G. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico* (Tesis de maestría). Universidad de la República, Montevideo, Uruguay.

Panda Security, The Cloud Security Company (2013). *Panda Solutions for Companies*. USA: Panda Security. Recuperado de http://www.pandasecurity.com/

Parra Giraldo, A. M. (2014). *ISO 27001 para PYMES* (Tesis de maestría). Universidad Internacional de La Rioja, Medellín, Colombia.

Piattini, M. G. & Del Peso, E. (2001). *Auditoría Informática: Un enfoque práctico*. Madrid, España: RA-MA Editorial.

Pinzón Trejos, C. I. (2010). *Arquitectura multi-agente adaptativa para la detección de ataques en entornos dinámicos y distribuidos* (Tesis de doctorado). Universidad de Salamanca, Salamanca, España.

PC World (2011, 7 de septiembre). La seguridad informática continúa siendo el principal riesgo para las empresas. *PCWorld*. Recuperado de http://pcworldmexico.com/

Portantier, F. (2012). *Seguridad Informática por Fabian Portantier: Aprenda cómo implementar soluciones desde la visión del experto*. Buenos Aires, Argentina: Fox Andina, Dalaga

Ramírez Cavassa, C. (2005). Seguridad Industrial: Un Enfoque Integral. México D. F., México: Editorial Limusa S. A.

Ramírez Reyes, G. (2002). *Metodología para auditoría informática en entidades públicas* (Tesis de maestría). Universidad Nacional de Ingeniería, Lima, Perú.

Rincón Bermúdez, R. D. (2002). Modelo para la implementación de un sistema de gestión de la calidad basado en la Norma ISO 9001. *Revista Universitaria EAFIT*, (126), 47-55.

Roa Buendía, J. F. (2013). *Seguridad informática*. Madrid, España: McGraw-Hill Interamericana de España.

Ruiz-Canela, J. (2004): *La gestión por Calidad Total en la empresa moderna*. Madrid, España: RA-MA Editorial.

Sandoval Vargas, C. A. (2014). *Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa* (Tesis de maestría). Universidad Católica de Santiago de Guayaquil, Guayaquil, Ecuador.

Seclén Arana, J. A. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001* (Tesis de maestría). Universidad Nacional Mayor de San Marcos, Lima, Perú.

Securosis Data Security Survey (2010). *The Securosis 2010 Data Security Survey Report Rates the Top 5 Data Security Controls*. USA: Securosis. Recuperado de https://securosis.com/

Sifuentes, G. (8 de agosto de 2015). Seguridad Informática: Información Comprometida. *Muy Interesante*, (28), p. 16.

Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa (2015). *Acreditación*. Lima, Perú: Ministerio de Educación. Recuperado de https://www.sineace.gob.pe/

Summers, D. (2006). *Administración de la calidad*. Naucalpan de Juárez, México: Pearson Educación.

Symantec SMB Information Protection Survey (2010). *Cyber Security Services*. USA: Symantec Corporation. Recuperado de https://www.symantec.com/

Tamayo Arana, D. P. (2015). *Modelo de auditoría informática orientada a procesos de seguridad en redes computacionales* (Tesis de pregrado). Universidad Andina Néstor Cáceres Velásquez, Juliaca, Perú.

Vento Mesa, M. L. (2014). *Aplicación de normativas de seguridad de la información para Systems Support & Services S. A.* (Tesis de pregrado). Universidad San Martin de Porres, Lima, Perú.

Villatoro Segovia, G. Y., Villalobos Meza, N. A. & Posada Pineda, G. (2007). *Plan de auditoría informática en los centros de cómputo educativos del nivel medio de las instituciones públicas de la ciudad de San Miguel, para lograr la efectividad administrativa en el uso de los recursos tecnológicos* (Tesis de pregrado). Universidad de Oriente, San Miguel, El Salvador.

Zapata, O. A. (2005). *La aventura del pensamiento crítico: Herramientas para elaborar tesis e investigaciones socioeducativas*. México D. F., México: Editorial Pax México.

Zeña Ortiz, V. E. (2015). *Estándar internacional ISO 27001 para la gestión de seguridad de la información en la oficina central de informática de la UNPRG* (Tesis de pregrado). Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú.