UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de la ISO/IEC 17799 para la Seguridad de la Información en la Empresa Nuevo Mundo Viajes

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

Chicoma Gutarra, Miguel Angel ORCID: 0000-0003-4461-8171

ASESOR:

Dr. Hilario Falcón, Francisco Manuel ORCID: 0000-0003-3153-9343

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LIMA – PERÚ

2018

DEDICATORIA

Dedico esta tesis a mis Padres y a mis Hermanos quienes me apoyaron y me orientaron todo este tiempo.

AGRADECIMIENTO

Son muchas las personas que han formado parte de mi vida profesional a los que me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón.

ÍNDICE

RESUMEN

La presente investigación tuvo como objetivo la “Implementación de la ISO/IEC 17799 para la seguridad de la información en la empresa Nuevo Mundo Viajes”, y así determinar el efecto del mismo para así dar explicación sobre las deficiencias que existe sobre seguridad de la información en la organización y lograr mejoras en las mismas.

La investigación realizada fue de tipo aplicada, con un diseño pre experimental. Para realizar el presente trabajo se tomó como población 30 registros de incidencias sobre seguridad de la información. Esto permitirá un mejor manejo de reducir dichos incidentes. Se usó como técnica de recolección de datos la observación que se hizo como instrumentos una ficha de observación. El instrumento de recolección de datos fue validado por el Jefe de Plataforma y soporte TI, y el director de TI.

De los resultados obtenidos con esta investigación se llegó a la conclusión que la implementación de la ISO/IEC 17799 tuvo un efecto significativo en la seguridad de la información en la empresa Nuevo Mundo Viajes, en cuanto a número de accesos no autorizados se redujo de 395 registros se redujo a 167, además en manipulación de datos se redujo de 239 registros a 110 luego de la implementación. Para el tiempo en el que un sistema está disponible aumento siendo al inicio un 70.67% a un 98.37% luego de la implementación de la ISO/IEC 17799.

Palabras claves: Seguridad de la información, confidencialidad, integridad, disponibilidad, ISO/IEC 17799.

ABSTRACT

The objective of this research was "Implementation of ISO / IEC 17799 for information security in the company Nuevo Mundo Viajes", as well as the result of the same information on the deficiencies that exist regarding the security of information in the organization and achieve improvements in them.

The research carried out was of an applied type, with a pre-experimental design. In order to carry out the present work, 30 records of incidents on information security were taken as a population. This will allow a better management of reducing said incidents. The observation made as an observation card was used as a data collection technique. The data collection instrument was validated by the IT Platform and Support Manager, and the IT Director.

From the results obtained with this research, it was concluded that the implementation of ISO / IEC 17799 had a significant effect on the security of information in the company Nuevo Mundo Viajes, in terms of the number of unauthorized accesses it was reduced from 395 records were reduced to 167, in addition data manipulation was reduced from 239 records to 110 after the implementation. For the time in which a system is available, the increase is initially 70.67% to 98.37% after the implementation of ISO / IEC 17799.

Keywords: Information security, confidentiality, integrity, availability, ISO / IEC 17799.

TABLA DE FIGURAS

I. INTRODUCCIÓN

1.1. Realidad Problemática

La tecnología ha ido cambiando de una manera impresionante en los últimos años, la interconectividad con los objetos, la forma de comunicarnos, búsqueda de información, la manera de comprar sin movernos de casa, y las demás cosas que nos facilita las redes e internet. La Tecnologías e información se han vuelto una necesidad para cualquier tipo de negocio ya que esta les da el soporte necesario a la gestión, control y planificación que manejen; Muy aparte de optimizar y volver eficiente los procesos de negocio.

La información a través de los tiempos se ha convertido en un activo muy importante para las organizaciones ya que ahora vivimos en un mundo mucho más interactuado e interconectado, gracias al inmenso crecimiento, la información de las organizaciones se encuentra más expuestas y vulnerables, por lo que se requiere una mayor protección, control y monitoreo constante para poder asegurar la integridad de la información.

Al tiempo que las organizaciones se sientan más cómodas usando la tecnología para hacer cualquier tipo de negocio, crear redes y transferir fondos, surgen personas que ven una oportunidad de realizar acciones ilícitas, para así poder aprovecharse y conseguir beneficios. Al ver esta situación, se puede decir que la perdida de información cree a medida que las organizaciones implementan más tecnología. (Portantier, 2013, p. 12)

En el 2014, se realizó la V encuesta en Latinoamérica acerca de la gestión de seguridad de la información, en donde podemos visualizar:

Las fallas más comunes sobre la seguridad de la información. Como mayor problema con un 33% es la instalación de software no autorizado ya que común mente algunas empresas no compran licencias corporativas y terminan instalando programas piratas tan solo para ahorrar costos. El 50% de las empresas cuenta con políticas de seguridad formales, el 35% se encuentran en el proceso de desarrollo de sus políticas mientras que el 15% no cuenta con políticas de seguridad definidas o no tiene conocimiento para desarrollarlas.

La encuesta llego a la conclusión de que el 42% de las empresas latinoamericanas tienen falta de apoyo directivo en seguridad TI además de 45% no tiene procesos de evaluación de riesgos. Dichos resultados nos reflejan el poco conocimiento de las organizaciones sobre seguridad de la información, además de pensar que implementar políticas o herramientas sea complejo y costoso.

Por otro lado, en el Perú existen varias empresas que no ven a la información como un activo que pueda generar valor y no le dan la debida atención. Existe un alto índice de falta de conciencia en los usuarios ya que es gran parte del problema, además de la falta de políticas preventivas y correctivas. En una reciente encuesta, el 44% de las personas encuestadas indican que no tienen una estrategia de seguridad de la información, por su parte el 48% no tiene programas de concientización y capacitación en seguridad para los empleados y el 54% de los encuestados no ha cuenta con un proceso de respuesta a incidentes. (Gestión, 2017) En este campo existen diversas herramientas, metodologías y buenas prácticas para ayudar y mejorar la calidad de la información de las organizaciones.

Nuevo Mundo Viajes es una empresa del sector turismo fundada el año 1980, cuenta actualmente con más de 600 colaboradores, muy bien posicionada, además de contar con múltiples servicios y diversos puntos de venta a nivel nacional. Su oficina principal se encuentra ubicada en Miraflores dedicada a la venta de boletos aéreos, paquetes y servicio especiales de turismo. Dentro de la organización existe una deficiencia en la gestión de seguridad de la información ya que posee políticas de seguridad deficientes lo cual conlleva un deficiente monitoreo de accesos de los usuarios, falta de concientización de los usuarios acerca de los riesgos, mal clasificación y control de activos, falta de fidelización de los usuarios con normativas deficientes; ahí se puede visualizar la falta de integridad que carece la información en la organización. Alrededor del 70% de los empleados no tiene conocimiento de los contratos de confidencialidad que se realizan al firmar el contrato para empezar a laborar. Además de que casi el 75% desconoce las políticas de seguridad que maneja la empresa con los activos de información, lo cual permitiría hacerle saber a los usuarios la disponibilidad limitada con las que ellos trabajarían.

De seguir en esta situación se podría sufrir un alto impacto negativo en el negocio generando grandes pérdidas a nivel de costos, credibilidad en el mercado, además de influir directamente en los principales activos de la organización.

Por este motivo lo que se quiere es auxiliar a la empresa a implementar controles pertinentes que sean eficientes y eficaces, además de brindar el conocimiento respecto a seguridad de la información y la necesidad para mantener competitividad, rentabilidad y continuidad del negocio; con las buenas prácticas que posee la ISO/IEEC 17799 para la gestión de seguridad de la información, mejorando la calidad de los servicios, como también mejorara los controles de acceso y clasificaciones de los activos.

1.2. Trabajos Anteriores

En la tesis de Jacqueline Suca, titulada **"Implementación de la Norma Técnica Peruana ISO / IEC 27001: Recomendaciones Metodológicas de Seguridad de la Información 2008 en Entidades Públicas Nacionales"**, el objetivo es obtener el título de ingeniero de sistemas en la Ciudad de México. Arequipa - En Perú en 2014 traté de presentar una propuesta a través del método provisto por la norma técnica peruana ISO 27001, para que el sistema de seguridad de la información se pueda implementar en la agencia nacional, para que haya una mejor gestión de la seguridad y se reduzca todo lo que afecta a la entidad. riesgo.

En el trabajo de Edsson Tarrillo y Juan Correa, el título **es "Métodos del Gobierno Distrital de Lambayeque en el Sistema de Gestión de Seguridad de la Información Basado en la Norma Técnica de Perú NTP-17799"** para obtener el grado de Ingeniero de Sistemas en la ciudad de Lambayeque, Perú en 2014. Esta posición Tiene como objetivo proponer un método y sistema de gestión basado en ISO 17799 para una ciudad de Lambayeque. Bajo este marco de referencia, se divide en tres etapas: diagnóstico de la situación actual, evaluación y entrega de la metodología en base al marco de referencia. Como resultado, se permite establecer metas, procesos y procedimientos relacionados para que se puedan formar estrategias de seguridad y medidas de control de seguridad para mejorar los riesgos de seguridad de la información, que de esta manera se pueden gestionar internamente. Municipio en base a los objetivos que se han planteado.

En el trabajo de Frank Olivos y Erick Guevara, el título es **"Desarrollando políticas de control de acceso y seguridad física y ambiental basadas en la norma técnica peruana NTP-ISO / IEC 17799 para mejorar la gestión de la Oficina Central de Computación-Universidad de Lambayeque**", con motivo de ser galardonado con el título de Ingeniero de Sistemas en Chiclayo, Perú en 2017, en el proceso de documentación de políticas de seguridad y control de acceso, los diseñadores basados en esta investigación no solo utilizaron la norma ISO / IEC 17799, sino también por Lambayeque El centro de computación de la universidad no usa estándares que garanticen instrucciones básicas de seguridad de la información. En las universidades, el impacto de ser una entidad formadora es que cumple con los estándares para garantizar la seguridad de la información, garantizando así la continuidad de la información. Como resultado existe que más del 53% de las políticas formuladas bajo la norma técnica peruana permitirá mejorar la satisfacción, esta se utiliza para la gestión de la seguridad de la información.

El título de la tesis de David Aguirre es "**El Diseño del Sistema de Gestión de Seguridad de la Información Postal de Perú SA**", su propósito es obtener el título de Ingeniero en Computación en Lima, Perú en 2014 debido a la necesidad de implementar el Perú en una entidad pública. Estándares técnicos de seguridad de la información, por lo que el autor decidió cooperar con dichas entidades para crear diseños de SGSI que cumplan con la normativa utilizada por dicha entidad. Su posible realización puede jugar un papel en el futuro. El alcance y la estrategia de seguridad de la información se definen a través de una serie de reuniones y entrevistas con la alta dirección para comprender y verificar el valor de los activos clave de la organización. Como parte de los resultados, donde se especificaron las medidas de control aplicables a la norma técnica peruana ISO / IEC 17799, se realizó una declaración de aplicabilidad.son posibles de implementar en la organización.

En el trabajo de Briggette Bravo y Adriana Daudo, el título **es "Diseño de Gestión de Seguridad de la Información Basado en la Norma ISO 27002 e Investigación sobre el Estado Actual de las Empresas Prestadoras de**

Internet" Posorja en Accióncia. Para obtener el título de Ingeniero en Sistemas Computacionales en Guayaquil (Ecuador) en 2017, ltda "" se compromete a brindar un diseño de gestión de seguridad de la información que oriente al administrador del centro de cómputo del centro de gestión de seguridad de la información. De esta forma, la empresa puede mitigar los riesgos existentes y desarrollar medidas de control para evitar estos riesgos. Se utiliza el método MAGERIT, que utiliza el software PILAR como herramienta de análisis y gestión de riesgos para identificar amenazas. En resumen, el diseño ayudará a los miembros de la entidad a comprender los riesgos que enfrentan. Tome precauciones para prevenir ataques y proporcionar referencias para empresas que realicen actividades similares.

En el trabajo de Carlos Barrantes y Javier Hugo, el título es **"El Diseño e Implementación del Sistema de Gestión de Seguridad de la Información en el Proceso Técnico"** con el fin de obtener la Título de ingeniero informático y de sistemas. En 2012, además de utilizar marcos como ISO 27001 e ISO 17799, se intentó implementar SGSI, aplicando un método de análisis y evaluación de riesgos desarrollado por los diseñadores de este trabajo. Esto puede mejorar la seguridad de los activos. La informática de Card Peru SA también garantiza que los posibles peligros sean conocidos, asumidos, gestionados y minimizados de manera ordenada y estructurada, y que pueda responder con flexibilidad a los Riesgo, tecnología y el entorno en constante cambio creado por la tecnología.

En la tesis de Jhony Martínez, su título **es "Control de seguridad para reducir el número de incidentes de seguridad de la información en el Servicio de Gestión Tributaria de Huancayo en 2012"**, con el objetivo de elegir esta maestría en ingeniería de sistemas. En 2014, la ciudad de Waikayo, Perú, nos informó que tomó tres medidas de seguridad (confidencialidad, integridad y disponibilidad) para proteger la información, implementando así mecanismos de seguridad para prevenir emergencias por eventos internos y externos. Para ello, Martínez realizó un análisis de riesgos para ver qué activos de información deben protegerse y poder determinar qué amenazas pueden tener un impacto. Finalmente en base a la 17799(27002):2005 códigos de buenas prácticas en seguridad de la información, se logró implementar algunos controles de

seguridad a fin de reducir los riesgos del activo información y minimizar los incidentes registrados.

En la tesis de Jack Flores y Gino Puppi con el título **"Gestión de la seguridad física y lógica para un centro de datos"** para poder obtener el título de ingeniero de sistemas de información en la ciudad de Lima – Perú en el año 2013 nos dicen que la problemática era la manera cuantificar y detallar de manera actual el estado del centro de datos analizado del centro de datos de la carrera de ingeniería durante el 2010 y uno de los primeros semestres de 2011. Para poder verificar cual era el estado real del centro de datos, se hizo necesario averiguar sobre los estándares y/o normas nacionales e internacionales; siendo la base de la tesis. Se hizo notorio la falta de normativas y estándares que le permita asegurar la gestión de seguridad para dicho centro de datos. Los estándares que se definieron permitió iniciar una evaluación real creando 2 checklist con enfoques de seguridad. Los resultados arrojaron que los frentes de seguridad estaban a un nivel muy bajo. Unos de los entregables fue la política de seguridad que se basó en la ISO/IEC 17799:2007. Por último se dieron conclusiones y recomendaciones del proyecto.

En la tesis de Ronald Leiva con el título **"Diseño de un sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la red de salud de Lambayeque 2015"** con el motivo de optar el título de ingeniero de sistemas de información en Lima – Perú en el año 2016, cuyo proyecto se centró en diseñar un SGSI, que se basó en las ISO 27001 y 27002, además del uso del ciclo de Deming. Para lograr el diseño esperado se hizo necesario emplear ciertas técnicas, como recolectar datos, y como herramienta se utilizó la encuesta y fichas de observación, con el objetivo de la obtener las principales causas por lo que se necesitaba un sistema de gestión de información. En la primera parte del proyecto se identificó los procesos del negocio y se definió los alcances del sistema de gestión. De igual forma se determinó la metodología en la evaluación de los riesgos. Por último, al finalizar el proyecto se preparó un plan que permita gestionar los riesgos y

aplicarlos como parte de los documentos de la ISO a fin de poder elaborar las políticas, procesos y controles.

En la tesis de Ericka Molina, Oscar Rodríguez, Yalide Sánchez y John Vergel con el título **"Guía para la seguridad basada en la norma ISO/IEC 27002, para la dependencia división de sistemas de la universidad francisco de paula Santander Ocaña"** con el fin de obtener el título de especialista en auditoria de sistemas en la ciudad de Ocaña – Colombia en el año 2014. En dicha investigación se indica que la información es uno de los activos más relevantes que tiene toda institución, esto significa que requiere ser resguardada frente a toda amenazas que ponga en riesgo su confidencialidad, integridad y disponibilidad, para lo cual se da un manual de buenas prácticas donde se describe de manera muy detallada, todas las acciones que es necesario para poder cumplir con los requerimientos de seguridad dados por las normas internacionales que es la ISO/IEC27002.

En la tesis de Margarita Filian, el título es **"Implementando un programa de seguridad informática aplicable a los activos de FIEC según la norma ISO 27002"**, con el objetivo de obtener una maestría en seguridad informática para su uso en la ciudad. Guayaquil-Colombia nos informó en 2015 que esto incluye la implementación de un plan de seguridad basado en ISO 27002, en el cual se identifican las potenciales amenazas y riesgos de los activos administrados por el área de soporte. Lo cual primero se tuvo que definir los objetivos y de acuerdo a ello poder implementar una solución con un esquema de seguridad. Se realizó una identificación de los activos que se administran en el área para poder dar inicio a analizar los riesgos de estos basados en la metodología magerit. Una vez detallado el tratamiento de los riesgos se seleccionaron los controles basados en la iso 27002 para reducirlos, además definieron las políticas de seguridad y procedimientos que serán difundidos mediante una estrategia de seguridad.

En la tesis de Luis Guallpa con el título **"Plan de seguridad informática basada en la norma ISO 27002 para el control de accesos indebidos a la red de Uniandes Puyo"** con el motivo de tener la titulación de magíster en informática empresarial en la ciudad Ambato – Ecuador en el año 2017, en el cual se buscó elaborar un plan de seguridad informático que se alinee con la normativa ISO

27002 que puede ser aplicado en dicha universidad. En la investigación se aplicó el método descriptivo para que se puedan explicar las causas y efectos que origina el problema. Se establecieron políticas de seguridad que eran capaces de ayudar en la tarea de proteger física, lógica y perimetralmente la red LAN y los activos informáticos institucionales. Dichas políticas deberán ser revisadas periódicamente y se incorporarán mejoras según el crecimiento de la organización. También se implementó un sistema de detección de intrusos como estrategias para monitorear y controlar los accesos indebidos a la red interna.

En la tesis de Dorys Ledezma con el título **"Desarrollo de políticas de seguridad de la información basadas en las normas ISO 27002 para una coordinación zonal del INEC"** con el motivo de obtener el título de magister en gerencia informática en la cuidad de Ambato – Ecuador en el año 2015, en donde se determinó el problema referido a la inseguridad que hay en la coordinación Zonal 3 del INEC, en donde se detectó el fácil acceso que tienen tercera personas para acceder a la información la cual tenía el carácter de confidencial, el cual abarcaba no sólo el INEC zonal, sino también el nacional, existiendo la posibilidad de que se modifique o adultere la información, el cual obviamente perjudica al negocio. El objetivo que se trazo fue en desarrollar políticas que estén basadas en la ISO 27002, con la finalidad de aplicar en forma adecuada las normas y procedimiento sobre la información. En la tesis se ha analizado los requerimientos de la forma como se expone la información de la institución, siendo necesario para esto recolectar los datos mediante entrevistas personales a personeros de la coordinación zonal 3 del INEC, empleando posteriormente la metodología cascada. Lo que se pretende al desarrollar las políticas es permitir una protección a la información mediante la gestión de TI, a fin de que ésta sea precisa, confiable y concisa tanto para las personas dentro y fuera de la sociedad.

En la tesis de Karla Castro con el título **"Formulación de controles basados en la norma NTC- ISO 27002 para la seguridad de la información en el comité departamental de Cafeteros del cauca"** con el fin de optar el título de ingeniero de sistemas en la ciudad de Ocaña – Colombia en el año 2015, expone su tesis en donde resalta la importancia de la información, llegando a ser considerada como un activo importante de la empresa, siendo necesario establecer controles de

seguridad en base a la norma ISO 27002, con la finalidad de proteger la información contra las posibles amenazas a la que puede estar expuesta.

En la tesis de Ronald de la Cruz con el título **"Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la municipalidad provincial de Paita; 2016"** con el motivo de obtener el título de profesional de ingeniero de sistemas en la ciudad de Piura – Perú en el año 2016, tuvo como fin establecer propuestas de políticas que se basan en mejores prácticas, a fin de poder obtener la seguridad sobre la información para el municipio. Se realizó una evaluación primeramente del estado de seguridad compuesto por 152 empleados. Se obtuvieron que el 73.37% opina que la información se encuentra expuesta a vulnerabilidades, el 100% nos dice que no existen controles en cuanto a materia de seguridad. Por consiguiente, se obtuvo que la municipalidad no tiene políticas y controles pertinentes lo cual hace necesario brindarles una propuesta para minimizar la perdida.

En la tesis de Julio Alcántara con el título **"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 cuidad de Chiclayo"** con el fin de obtener el título de ingeniero de sistemas y computación en la cuidad de Chiclayo – Perú en el año 2015, se enfocaron en la hacer la guía de implementación que se basa en la ISO 27001para incrementar la seguridad de los sistemas de la comisaria. Los resultados se obtuvieron determinaron que al incorporar la norma ISO 27001, Se logró mejorar procesos que eran utilizados en pro del negocio detectando posible vulnerabilidades en la seguridad. El plan de tratamiento de riesgo les permitió disminuir el nivel de riesgo frente a toda amenaza y vulnerabilidad, fue gracias a esto que permitió incrementar el nivel de porcentaje de conocimiento del personal en temas de políticas de seguridad, y así poder comprometerlas con dichas políticas.

En la tesis de Miguel Cruz y Senyi Fukusaki con el título **"Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica MEDCAM Perú"** con el fin de obtener el título de ingeniero de computación y sistemas en la ciudad de Lima – Perú en el año 2015 nos dice que el estudio tuvo como principal objetivo

diseñar e implementar un SGSI para proteger el activo importantísimo como se ha convertido la información. Utilizando como metodología el ciclo de Deming que es sugerida la ISO 27001, y aplicando controles que se obtuvieron de la norma ISO 27002. El resultado fue la implementación de un SGSI, de esta menea se pudo disminuir las vulnerabilidades, amenazas y debilidades sobre los activos informáticos, permitiendo que haya mayor confidencialidad, disponibilidad e integridad. Se llegó a la conclusión de que la seguridad hace que se proteja los activos, cumpliendo de esta manera el objeto del negocio.

En la tesis de Iván Pizarro con el título **"Diseño de un modelo de gestión de seguridad de la información con un enfoque en el factor humano para el ICPNA Región centro en el año 2017"** con el fin de obtener el título de ingeniero de sistemas e informática en la ciudad de Huancayo – Perú en el año 2018 se dice que tuvo como propósito hacer un diseño que permita fortalecer la seguridad de la información en el personal de la institución. El estudio es diseño pre experimental de tipo transversal. Los resultados fueron realizar un modelo de seguridad el cual permita fortalecer al personal y gestionar riesgos además de proteger y salvaguardar la información según normativas internacionales vigentes, permitiendo de esta manera hacer más fuerte la seguridad de la información, tratar riesgos de seguridad y permitir gestionarlas.

En el artículo de Víctor Baca con el título **"Diseño de un sistema de gestión de la seguridad de la información para la unidad de gestión educativa local – Chiclayo"** en la cuidad de Chiclayo – Perú en el año 2016 nos dice que tuvo como objetivo el modelo un sistema de seguridad basada en las normas intencionales 27001 y 27002. Su importancia permitió determinar objetivos y procesos para establecer políticas y controles para la seguridad, los cuales nos permitirá poder analizar los posibles riesgos sobre la información que se emplea en la unidad de gestión educativa local de Chiclayo. La población se conformó por empleados de la unidad, la recolección de datos se hizo mediante la evaluación de documentos, encuestas personales, entrevistas y observación directa. Se concluyó que el diseño de un sistema de gestión de seguridad de la información permite la mejora de la situación actual de la seguridad de la

información, utilizando normativas de estándares internacionales que afectan en una buena gestión de la información.

En el artículo de Orivaldo Lima, Vania da Silva y Jose de Almeida con el título **"Mejores prácticas del COBIT, ITIL e ISO / IEC 27002 para la implantación de la política de seguridad de la información en las Instituciones Federales de Educación Superior"** en Brasil en el año 2017 nos dice: El mantenimiento de la seguridad de la información de las Instituciones Federales de Educación Superior es un factor importante llegar a los objetivos planteados estratégicamente. Sin embargo, esa garantía debería seguir a través procesos que permitan que se asegure la fiabilidad, autenticidad, integridad y disponibilidad de la información. Primeramente, poner en práctica las políticas de seguridad de la información. Como objetivo principal se tuvo que definir las mejores prácticas para la información de gestión de seguridad. Los datos fueron extraídos de manera documental y revisión sistemática de una de las guías de mejores prácticas Postit. Después de la preparación, la guía fue evaluada con tecnología un modelo de aceptación, lo cual nos permite tales como la facilidad de uso de un sistema nuevo o un nuevo enfoque teórico o metodológico. Los gestores de seguridad opinan que este documento puede ser utilizado en otras instituciones educativas para agregar un valor agregado en el proceso de implementación.

En el artículo de Winfred Yaokumah con el título **"Investigación sobre el estado de la práctica de la gestión de la seguridad de las operaciones según ISO / IEC 27002" en** el año 2016 podemos observar que este estudio evaluó la gestión de la seguridad de la información en las organizaciones a través de un cuestionario basado en la norma ISO / IEC 27002, con un enfoque especial en la seguridad de las operaciones. Se realizó una encuesta con diseño de investigación transversal y se recopilaron datos de 223 participantes de 56 organizaciones. En general, el nivel de madurez de seguridad de las operaciones fue de 61.2%, que es el Nivel de madurez 3 (bien definido). Este nivel sugirió que los controles y procesos de seguridad de operaciones se documentaron, aprobaron e implementaron en toda la organización. Las copias de seguridad y la protección contra malware fueron los controles de seguridad más implementados, mientras que el registro, la auditoría y el monitoreo fueron los controles menos implementados. La evaluación de la

seguridad de las operaciones entre organizaciones encontró diferencias significativas entre las organizaciones. Las instituciones financieras y de atención médica superan a las instituciones educativas y al servicio público gubernamental. El estudio proporcionó información sobre los niveles de madurez de los controles de seguridad de las operaciones y los resultados útiles para evaluar el desempeño interorganizativo, la competitividad y la mejora de la seguridad de la información.

En el artículo de Robert Van Wessel con el título **"Implementación de estándares internacionales para la gestión de la seguridad de la información en China y Europa: un estudio comparativo de varios casos"** en el año 2011 no dice que los principales estándares internacionales para la gestión de seguridad de la información, ISO / IEC 27001 y 27002 se originan en el Reino Unido, pero se aplican en todo el mundo. Este documento explora si los procesos de selección, implementación y uso de estos estándares interrelacionados difieren entre China y Europa al estudiar los casos de compañías chinas y europeas. Las compañías chinas enfrentan algunos problemas adicionales con los estándares, pero logran que se implementen con éxito en un corto período de tiempo. Las principales diferencias se relacionan con la gobernanza y la gestión de la adopción estándar. Este estudio es innovador en el método utilizado para la investigación de estandarización (estudio comparativo de varios casos) y en el tema: implementación e impacto de los estándares de gestión para seguridad de la información.

En el artículo de Pavel Nastase, Floarea Nastase y Corina Lonusca **"Desafíos generados por la implementación de las normas de ti cobit 4.1, itil v3 e iso / iec 27002 en las empresas"** nos dice que se centra en el estudio que enfatiza la importancia de implementar las mejores prácticas o estándares de tecnología de la información (TI) que incluyen COBIT, ISO / IEC 27002 e ITIL para empresas comerciales en 2009. Afirma que COBIT ayuda a los gerentes al permitirles comprender la estructura de TI y manejar la inversión en TI. Cita que ITIL promueve la eficiencia empresarial en la gestión de servicios de TI. La iso 27002 tiene como objetivo mejorar la confiabilidad de la seguridad de la información. Señala que debe haber una alineación entre las mejores prácticas de TI y los requisitos del negocio para lograr la efectividad del negocio.

En el artículo de Luiz Schneider, Adolfo Vanti, Angel Cobo y Joao Peruchena con el título **"Evaluación de los procesos de seguridad de la información integrando el control y las áreas de TI"** en el año 2014 nos dice que La Contraloría es responsable de todo el proceso en la toma de decisiones de soporte en las organizaciones y es por eso que es necesaria su participación en los procesos de seguridad de la información. Por lo tanto, este estudio evaluó la forma en que se aplican los procesos de seguridad de la información al integrar las áreas de Controllership y TI. Respecto a la metodología, el trabajo se basa en una investigación descriptiva en un proceso cualitativo, considerando la percepción de los encuestados en 30 preguntas relacionadas con el problema propuesto. Se aplicó un cuestionario complementario basado en la norma ISO / IEC 27002 que implica una explicación causal de las áreas de integración y la conceptualización de diferentes categorías de profesionales respecto a la seguridad de la información. Desarrollamos un estudio de caso aplicado a instrumentos de recopilación de datos relacionados con cuestionarios y entrevistas, análisis de contenido para identificar los procesos de negocio críticos y los riesgos asociados con el entorno de la información. Por lo tanto, fue posible mejorar los procesos operacionales de estas dos áreas, reduciendo los riesgos operacionales a través de diferentes acciones relacionadas con la participación de los usuarios, creando equipos, mayor estandarización, alineación de la comunicación, mayor control en los sistemas cambiantes, mejoras a las políticas e información de estándares de seguridad, uso de herramientas de inteligencia empresarial, capacitación, integración de información y enfoque en el proceso central. Finalmente, respondió al objetivo de evaluar los procesos de seguridad de la información mediante la integración de las áreas de Controllership y IT.

En el artículo de Hui Lin, Meghann Cefaratti y Linda Wallace con el título **"Gestión de riesgos empresariales, COBIT e ISO 27002: un análisis conceptual"** en el año 2012 se puede visualizar que se examina y compara tres marcos de control utilizados por las organizaciones para diseñar procesos de control interno y controlar el uso de la tecnología de la información (TI) dentro del entorno de control interno de una organización. El marco ERM proporciona información sobre los procedimientos de gestión de riesgos empresariales para las organizaciones e identifica las interrelaciones entre

la gestión de riesgos empresariales y los controles internos. COBIT, publicado por ISACA, se utiliza como un modelo de gobierno para las operaciones de TI en las organizaciones. Por último, la norma ISO 27002 es un marco aplicado a la implementación de programas de seguridad de la información, y define una variedad de controles y esquemas de seguridad utilizando un enfoque de administración de riesgos de seguridad de la información. Específicamente, el artículo realizó un mapeo conceptual de los elementos de ERM, COBIT e ISO 27002 para identificar sus puntos en común y diferencias. Los resultados del mapeo permitirán a los auditores internos realizar referencias cruzadas de marcos para evitar la duplicación de esfuerzos y "reinventar la rueda" en el proceso de control de implementación y cumplimiento.

En el artículo de Stephen Fenz, Stephanie Plieschneger y Heidi Hobel con el título **"Mapeo de la norma de seguridad de la información ISO 27002 a una estructura ontológica"** en el año 2016 se no dice que El propósito de este documento es aumentar el grado de automatización dentro de los proyectos de cumplimiento de seguridad de la información mediante la introducción de una representación formal de la norma ISO 27002. A medida que la información se vuelve más valiosa y las empresas actuales se enfrentan a frecuentes ataques a su infraestructura, las empresas necesitan apoyo para proteger sus activos basados en la información. Las normas y directrices de seguridad de la información proporcionan conocimientos básicos para salvaguardar los activos corporativos. Sin embargo, los esfuerzos para verificar si las medidas implementadas de una organización se adhieren a los estándares y directrices propuestos siguen siendo significativamente altos. Este documento muestra cómo se puede respaldar el proceso de verificación de cumplimiento utilizando descripciones de control ISO 27002 legibles por máquina en combinación con una representación formal de los activos de la organización. Los autores crearon una representación formal de la norma ISO 27002 y mostraron cómo se puede utilizar una ontología de seguridad para aumentar la eficiencia del proceso de verificación de cumplimiento.

En el artículo de Nicolae Anton y Anior Nedelcu con el título **"Seguridad de la información y evaluación de gestión de riesgos"** en el año 2015 se puede apreciar que el trabajo aborda la evaluación de los riesgos de seguridad e información para

encontrar los valores óptimos de los riesgos aplicando y comparando diferentes métodos para medir y evaluar los riesgos de seguridad. Al describir las características estructurales de los estándares y los métodos implementados en el sistema de gestión de seguridad de la información (SGSI), este documento subraya la necesidad, los medios y la eficacia de los modelos de seguridad de la información. Las conclusiones de este documento resaltan la importancia de los estándares y los métodos de evaluación de la gestión de riesgos.

En el artículo de Daniel Sora con el título **"Securing IT networks with isms family of standards (iso 27001 series)"** en el año 2012 nos dice que: La información de toda organización en estos días se ha vuelto muy dependiente de la tecnología de la información y las comunicaciones. La tecnología representa un aspecto fundamental en cualquier institución y ayuda a facilitar la elaboración, los procesos, el almacenamiento, la transferencia, la protección y la eliminación de la información. Donde el alcance del entorno global de negocios interconectado se expande, también lo hace el requisito de resguardar la información, ya que esta información ahora está expuesta a una variedad más amplia de ataque y vulnerabilidades.

1.3.Teorías relacionadas al tema

1.3.1. Información

La información es la representación de datos mutados de una manera que tengan una significancia para el receptor, es decir tiene un valor agregado para la toma de decisiones y para las acciones correspondientes. (Lapiedra, Devece y Guiral, 2011, p. 6).

Además, sabemos que la información representa un activo de gran importancia para el negocio por tanto como tiene valor como otros activos de la empresa requieren una adecuada protección. (NTP, 2007, p. 1).

1.3.2. Seguridad de la información

En base a la Norma Técnica Peruana ISO/IEC 17799: la seguridad de la información sirve, valga la redundancia, para proteger al activo "información" frente a las diversas amenazas a fin de asegurar que continúe el negocio, minimizar los daños que se puedan ocasionar a las organizaciones y generar un valor agregado a las inversiones y oportunidades del negocio. (2007, p. 1)

La seguridad que se implementa para poder proteger la información tiene por finalidad proteger los sistemas ante los posibles peligros y amenazas a la que pueden estar expuestas, es por eso necesario aplicar medidas preventivas de seguridad el cual se tiene que hacer de una manera planeada y racional, para evitar emplear esfuerzos donde no hacen falta y dirigirlos de manera correcto donde se los necesite. Para que estas medidas y la estructura de protección sean eficaces, deben integrar todo dentro de un sistema de gestión de seguridad de la información. (Álvarez y Pérez, 2004, p. 2)

La seguridad de la información se relaciona con los medios de prevención que se aplican con la finalidad de asegurar la información bajo parámetros de confidencialidad, disponibilidad e integridad. La información se manifiesta de diversas formas y medios. Por tanto, las

grandes empresas adoptan y adaptan métodos a fin de salvaguardar los archivos y registros. (2015, p. 6)

1.3.3 ISO/IEC 17799

La ISO/IEC 27002 se trata de un cuerpo normativo de buenas prácticas que nos muestra el objetivo de control y además los controles que se recomiendan acerca de seguridad de la información. Posee 39 objetivos con 133 controles que estan agrupados respectivamente en 11 dominios. No es certificable. Desde 2006, su traducción en Colombia como ISO 17799 y a partir del 2007 en Perú. (iso.org)

La norma indica cuales son los principios y directrices generales para dar inicio, para la implementación, mantención y mejoramiento de la gestión de seguridad de la información dentro de la organización. Llámese una relación de prácticas, que se ha logrado mediante la experiencia y colaboración de varios intervinientes. No obstante, tiene como objetivo el de guiarnos a fin de poder desarrollar las medidas de seguridad interna, y aplicar los métodos necesario en la gestión de la seguridad, por lo tanto, la selección de los controles se sujeta a lo detectado en un análisis de riesgos previo, de igual forma el grado de cómo se implementa cada control en base a los requisitos de seguridad que serán determinados y los recursos disponibles de la organización para alcanzar la equidad entre seguridad y costos.

1.3.4 Normas ISO

Las normas ISO es una documentación que especifican requerimientos que deben ser empleados en las empresas para que se garantice que los productos y servicios que brinden cumplan con su objetivo. Hasta el momento se han publicado más de 19500 normas que se descargar de la página oficial de ISO. Para las empresas estas herramientas hacen que se minimicen los costos, además de reducir errores y además ayudan a elevar la productividad de los procesos. (isotools.org/normas)

1.3.5 Integridad

Para Álvarez y Pérez la integridad significa que se garanticen que los datos, objetos y recursos no sean alterados, que se mantengan completos y que sean fiables. Modificación no autorizada de la información puede ocurrir durante es almacenado, transportado o procesado. Por consiguiente, se torna necesario que se implemente controles de integridad en todos los estados de la información. La integridad puede tener 3 enfoques:

- Los sujetos que no posean autorización no deben poder hacer modificación de la información en lo absoluto.
- Los sujetos con autorización no deben realizar cambios que no se hayan tenido autorización previa.
- Los datos deben ser consistentes de manera que sean correctos y verdaderos siempre. (2004, p. 117)

Para Amutio, mantener las características como que la información este completa y sea corregida. Contra el indicador integridad, se debe considerar la posible detección de información incompleta, afectando le normal desempeño de la organización. (2012, p. 9)

1.3.6 Confidencialidad

El objetivo de La confidencialidad es que los datos, objetos y recursos solo puedan ser observados por los usuarios legítimos. Estos datos bien se hallan almacenados en algún tipo de hardware o si no en una red de comunicaciones entre 2 o más equipos. En estos estados los recursos requieren de controles vitales. (2004, p. 95)

Además de ser una cualidad de un mensaje o datos para que solo se entienda como una manera compresible para el usuario o sistema que esté autorizado. Tanto como la privacidad o protección de tal mensaje y datos que posea. (Costas, 2011)

1.3.7 Disponibilidad

Consiste en que la información se mantenga accesible cuando y donde se la necesite sin que se interrumpa el servicio. La disponibilidad hace sé que se implementen controles para que alcanzar un rendimiento razonable, rápida y sea eficiente la gestión de las interrupciones, redundancia y además mantener copias de seguridad a fin de evitar la pérdida de información. (2004, p. 122)

Para Costas, la disponibilidad viene a ser la capacidad de un servicio, de datos o un sistema, a ser accesible y que se pueda utilizar por los usuarios autorizados cuando ellos lo necesiten, evitando una pérdida o robo de dicha información. (2011, p. 12).

Además, Amutio nos dice que la disposición de los servicios se da cucan se usa el servicio cuando se requiere, por ende la carencia de este implica la interrupción del servicio. La disponibilidad del servicio está relacionada con la productividad de la organización. (2012, p. 9)

1.3.8 ISO 27001 e ISO 27002

Las normas ISO/IEC 27001 y la ISO/IEC 27002 establecen cuales son los requerimientos que se deben de dar, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI, de igual forma va a determinar lo que se requiere para poder implementar el control en la seguridad, en caso sea necesario.

Corti, Betarte & De la Fuente (2005) en el artículo “Hacia una implementación exitosa de un SGSI” citado por Pallas Mega (2009) trata sobre las etapas del ciclo de Deming y los productos o entregables exigidos por la norma. El cuadro que se presenta nos indica cuales son los principales procesos que establece la norma mapeado con las etapas del ciclo PHVA.

La norma ISO/IEC 27002, detalla el sistema de control que se aplica a la seguridad en la información de acuerdo a la norma ISO/IEC

27001 en cada dominio y proceso. La norma va a guiar en la aplicación del control en la seguridad de la información como políticas y procedimientos.

Nos dice Ureña león (2011), l La norma iso 27002 incluye: una estructura y descripción de las buenas practicas, evaluación del riesgo, políticas de seguridad y sus gestiona miento, aspectos

Ciclo PHVA	Procesos
Planear (*Plan*)	Establecer el contexto. Alcance y Limites Definir Política del SGSI Definir Enfoque de Evaluación de Riesgos Identificación de riesgos Análisis y Evaluación de riesgos Evaluar alternativas para el Plan de tratamiento de riesgos Aceptación de riesgos Declaración de Aplicabilidad
Hacer (*Do*)	Implementar plan de tratamiento de riesgos Implementar los controles seleccionados Definir las métricas Implementar programas de formación y sensibilización Gestionar la operación del SGSI Gestionar recursos Implementar procedimientos y controles para la gestión de incidentes de seguridad
Verificar (*Check*)	Ejecutar procedimientos de seguimiento y revisión de controles. Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. Revisión de la evaluación de riesgos periódicamente. Realizar auditorías internas Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de seguridad Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI
Actuar (*Act*)	Implementar las mejoras identificadas para el SGSI Implementar las acciones correctivas y preventivas pertinentes. Comunicar acciones y mejoras a todas las partes involucradas. Asegurarse que las mejoras logren los objetivos previstos.

Figura 1. Ciclo de Deming. Fuente Gustavo Pallas Mega, 2009

organizacionales de seguridad sobre la información, la gestión de activos está muy ligado al talento humano, seguridad física y de equipos informáticos, ambiental, comunicaciones, servicios brindado por terceros, contra códigos maliciosos, respaldos de seguridad, manipulación de datos de soporte, el intercambio de datos, gestión de accesos a los usuarios, a la red, accesos al sistema operativo, accesos a las aplicaciones y a la información, seguridad de archivos del

sistema, mejoras en la gestión de continuidad del negocio, cumplimientos de normativas legales, políticas y normas de seguridad.

Amenazas físicas y lógicas

Una amenaza lógica es software o código que de una forma u otra entre otros encontramos:

- Herramientas de seguridad: Hay una amplia gama de herramientas que nos permiten detectar y resolver fallas que se presenten en los sistemas, pero a su vez estas herramientas que nos ayudan a detectarlos son utilizadas para realizar ataques.
- Rogueware o falsos programas de seguridad: Estos son programas que son utilizados malintencionados disfrazados de antivirus falsos o los famosos antispyware.
- Backdoors: También llamados puertas traseras, son aquellos atajos que son dejados por programadores, con poco nivel de seguridad.
- Virus: Son un conjunto de códigos malintencionados insertados en archivo de tipo ejecutable, una vez ejecutado dicho programa se activa el virus.
- Gusano: es un archivo capaz de auto propagarse a través de la red, usualmente de forma de correo electrónico basura o spam.
- Troyanos: Son aplicativos que tiene definida instrucciones ocultas de tal manera que el usuario piensa que son las tareas que él manda, pero en segundo plano va ejecutándose tareas sin autorización del usuario.
- Programas conejo o bacterias; Son aplicaciones que generan la negación de los servicios de la PC.

Generando el colapso de los recursos del sistema ya sea: memoria, procesador, disco, etc.

- Canales cubiertos: son medios de comunicación las cuales dan acceso a que otros usuarios malintencionados información confidencial, generando la violación de las políticas de seguridad.

1.3.9 Modelo MAGERIT

Expresa Amutio:

Según la norma ISO31000, magerit se denomina proceso de gestión de riesgos, en otras palabras, magerit busca implementar una gestión de riesgos en el marco referencial para que las organizaciones generen sus propias decisiones teniendo en cuenta los percances que pueda tener derivados de la tecnología. (2012, p. 07).

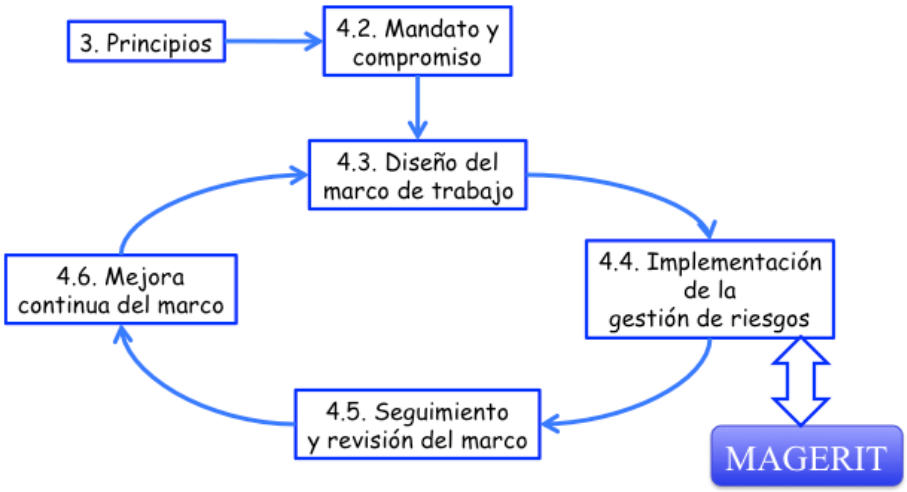


Figura 2. Marco de trabajo de la gestión de riesgos. ISO 31000

1.3.1.0 Análisis y gestión de riesgo

Riesgo:

Es la exposición a una amenaza, el cual se puede materializar mediante uno o más activos pudiendo originar graves perjuicios en la Organización.

El riesgo nos muestra el supuesto que puede suceder en caso no se cuide adecuadamente a los activos. Es fundamental determinar las características de cada activo, así como determinar los peligros que puedan afectarla, es decir, es necesario analizar el sistema:

Análisis de riesgos:

Se trata de un proceso sistemático que tiene por finalidad determinar el volumen del riesgo del que puede vulnerar a una organización.

Conociendo estos riesgos se puede tomar decisiones.

Tratamiento de los riesgos

El proceso que está orientado a cambiar el riesgo

Puede haber varias formas de trata el riesgo, veamos: evitando las circunstancias que la van a iniciar, disminuir toda posibilidad de que se dé, establecer las consecuencias, el contar con otra organización mediante la contratación de un servicio o un seguro, en caso se dé el riesgo es importante prever los recursos a fin de accionar cuando es necesario.

Es importante entender que el riesgo puede darse, ya que una seguridad en forma completa no existe, por lo que se debe aceptar la posibilidad de la presencia de un riesgo, debiendo someterlo al umbral de calidad que implica el servicio. Incluso es posible que se acepten riesgos operacionales en la realización de actividades que pueden

generar beneficios superando incluso el riesgo, es por tal motivo que se suelen utilizar definiciones más generales de riesgo:

Considerando que no es técnico el aceptar un cierto grado de riesgo, es necesario determinar las condiciones en que se trabaja, con la finalidad de poder dar la confianza necesaria que debe ofrecer el sistema, siendo necesario la aplicación metódica a fin de poder asumir decisiones fundamentadas, explicando en forma racional las decisiones que se tomarán. (2012, p. 10).

1.3.10 Control y configuración de activos

Para ITIL, la configuración de activos tiene como objetivo brindar un modelo lógico sobre la infraestructura de TI e donde se pueda visualizar como los servicios estén relacionados con los distintos componentes. Para lo cual es trascendente:

- Que todos los activos y los elementos de configuración cuenten con protección.
- Que la totalidad de activos y elementos de configuración estén determinados dentro del sistema de gestión de la configuración.
- Que los procesos de gestión del servicio y operativos cuenten con un soporte eficaz.

Esto garantiza que todos los componentes que forman parte del producto o servicio estén identificados y se mantengan actualizados. (2011, p. 72)

Para la ISO 17799, tiene la finalidad de otorgar la protección necesaria de la información dentro de la organización, asimismo, se deber considerar a los activos, teniendo un propietario asignado. Por consiguiente, se debe identificar todos los propietarios de todos los activos importantes y tener designado el mantenimiento de controles apropiados. Pero la responsabilidad en si lo debe tener el propietario designado. (2007, p.32)

1.3.11 Gestión y control de accesos

Para ITIL, el proceso de gestión de accesos nos permite dos cosas, en primer lugar el poder emplear el servicio por parte de los usuarios autorizados y por otro lado la limitación en el ingreso por parte de usuarios que no cuente con autorización. Estas medidas nos permiten garantizar un acceso disponible cuando se necesite, lo que implica que haya disponibilidad. Usualmente se inicia con la petición de un servicio mediante el centro de atención al usuario, el cual implica el requerir el acceso, verificar, asignación de derechos de acceso, monitorización del estado de identidad. (2010, p. 30).

Para la ISO 17799, el objetivo que cumple los controles de acceso es justamente el vigilar la accesibilidad de la información, al igual que los procesos del negocio sobre la base de la seguridad y actividad. Para ello es necesario considerar las políticas de información que se hayan planteado y alineado al Core de negocio.

1.3.12 IDS

1.3.13 COBIT, ITIL e ISO 27002

Según el profesor NĂSTASE, Pavel, NĂSTASE, Floarea y IONESCU, Corina: **Una** primera diferencia de los tres estándares es el hecho de que son emitidos por diferentes organizaciones con diferentes áreas de actividades y objetivos. Las funciones generales de los estándares también son levemente diferentes. COBIT proporciona mejores prácticas y herramientas para monitorear y mapear procesos de TI mientras que ITIL busca mapear el nivel de servicio de TI gestión e ISO 27002 otorga directrices para la implementación de un estándar marco de seguridad de la información. COBIT consta de 4 dominios y 34 procesos que son importantes para poder implementar la auditoría del sistema de información. Lo mejor de ITIL El marco de práctica cubre un total de 9 procesos y permite la implementación de la gestión del nivel de servicio de TI con

enfoque en lograr la efectividad del negocio y eficiencia en la gestión de servicios de TI. Al elegir el estándar correcto, los gerentes también deben considerar el tipo de proveedor que

STAND / AREA	COBIT	ITIL	ISO27002
Function	Mapping IT Process	Mapping IT Service Level Management	Information Security Framework
Area	34 Processes and 4 Domains	9 Processes	10 Domains
Issuer	ISACA	OGC	ISO Board
Implementation	Information System Audit	Manage Service Level	Compliance with security standards
Consultant	Accounting Company, IT Consulting Company	IT Consulting Company	IT Consulting Company, Security Company, Network Consultant

Figura 3. Vista general de COBIT, ITIL y la ISO/IEC 27002.

puede ofrecerles la solución deseada para implementar los estándares de TI. Los tres los estándares pueden ser provistos en general por una compañía de consultoría de TI, pero COBIT es exclusivamente proporcionado por una empresa de contabilidad e ISO 27002 por un valor o empresa consultora de redes. (2009, p. 7)

COBIT

COBIT proporciona mejores prácticas y herramientas a fin de poder monitorear y administrar las actividades de TI.

El uso de las TI es una inversión significativa y gestionada, COBIT ayuda comprender y administrar a los ejecutivos dichas inversiones a lo largo de todo el periodo de vida y brinda un método que permite la evolución de si los servicios de TI y las iniciativas cumplen con los requisitos del negocio y que entreguen el valor esperado. El marco COBIT, en las versiones 4.0 y posteriores, centra su actividad en 5 áreas que permiten la gobernanza de TI: marco, descripciones de procesos, objetivos de control, directrices de gestión y modelos de madurez. (2009, p. 8)

ITIL

La gestión de servicios de TI está al tanto de planificación, diseño, transición, operación y mejora continua de estos servicios, los cuales son imperativos para el negocio. ITIL permite un marco referencial de buenas prácticas para la gestión de dichos servicios y los procesos relacionados a ellos, con un enfoque más pegado a la alta calidad logrando la eficacia y eficiencia. Además, comprende apuntalar, pero no dar directrices sobre que procesos llevar a cabo procesos de negocio en una organización. Su función principal es brindar un marco en el cual la organización encuentre los enfoques, funciones y procesos que ellos requieran para enfocar las buenas prácticas apropiadas y brindar orientación al nivel más bajo que generalmente se aplica. Cuando se trata de un nivel inferior y a fin de poder implementar el ITIL en una organización, se requiere un conocimiento específico de sus procesos comerciales para impulsar ITIL para una efectividad óptima. (2009, p.9)

ISO 27002

La finalidad, el objetivo se orienta a dar información a las gerencias, administradores de la organización sobre las medidas de seguridad de la información dentro de la empresa. Se puede observar como una buena práctica y obtener estándares de seguridad a nivel internacional dentro de una institución para tener una mejor confiabilidad de la información en relaciones interorganizacionales. Plantea 133 controles bajo 11 encabezados principales. La norma se enfoca en la gestión de riesgo estableciendo que no necesariamente hay que implementar todas las pautas establecidas, solo las que sean importantes para la empresa.

Los principios en la ISO 27002 es un inicio para lograr implementar la seguridad para la información. Las medidas se basan su mayor parte en requisitos legales incluyendo la ley de protección y no divulgación

de datos personales. Las buenas practicas mencionadas en el estandar va incluido: políticas de seguridad, asignación de responsabilidades y la continuidad del negocio, Calder (2006). (2009, p. 10)

La alineación de COBIT 4.1, ITIL V3 e ISO 27002 es de particular valor para las empresas que están experimentando cambios o reestructuraciones. Como Robert Stroud, VP internacional de ITGI confirmó en una declaración escrita, "las asignaciones de COBIT a otros marcos y estándares, incluidos ITIL e ISO / IEC 27002, son especialmente útiles en situaciones de fusiones y adquisiciones". Si la otra organización involucrada usa un estándar u orientación diferente, el mapeo aclara cómo encajan los procesos de ambas organizaciones. El uso eficaz de TI es importante para el logro de la estrategia empresarial, ya que hay el potencial de ser el principal impulsor de la riqueza económica en el siglo XXI. Por lo tanto, las buenas prácticas de TI deben alinearse en base a los requerimientos del negocio, debiendo de haber una integración con los procesos internos. COBIT se puede utilizar al más alto nivel, proporcionando un marco centralizado que se base en un modelo de proceso de TI que se adapte a todas las organizaciones en general. Las prácticas y estándares específicos como ITIL e ISO 27002 cubren la mayoría de ámbitos laborales y se pueden mapear con COBIT, proporcionando así una jerarquía de materiales de orientación. (2009, p. 15)

1.4 Formulación del problema

Se presentan como problemas de la investigación:

Problema general

¿Cuál es el efecto de la ISO/IEC 17799 para la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes?

Problemas específicos

Los problemas específicos de la investigación fueron los siguientes:

- ¿Cuál es el efecto de la ISO/IEC 17799 en la confidencialidad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes?
- ¿Cuál es el efecto de la ISO/IEC 17799 en la integridad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes?
- ¿Cuál es el efecto de la ISO/IEC 17799 en la disponibilidad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes?

1.5 Justificación del estudio

Justificación teórica

Según Cortes e Iglesias, la justificación teórica se argumenta por el deseo de que se verifique, rechace o aporte teoría con respecto al objeto de estudio o conocimiento. Donde se plantean interrogantes como: ¿se busca mejorar un modelo teórico?, ¿se desea contrastar la forma de cómo se esa teoría se presenta en la vida real?, ¿Se espera que los resultados sean complementos a la teoría que fundamentaste? (2004, p. 15)

Esta tesis se justifica teóricamente porque busca crear conocimiento sobre la gestión de seguridad de la información y contrastar los resultados obtenidos con otras investigaciones, como también podrá ser usada para posteriores investigaciones.

Justificación metodológica

Según Cortes e Iglesias, la justificación metodológica necesita que se tengan sustentos del aporte por la cual sea factible el empleo o creación de instrumentos y modelos de investigación. ¿El resultado dará pautas a seguir que se puedan usar en investigaciones en esa línea?, ¿El resultado es un tipo de instrumento, un modelo o software que se permita ser usado en otra investigación? (2004, p. 15)

La ISO/IEC 17799 respecto a la gestión de seguridad de la información en la empresa Nuevo Mundo Viajes podrá ser utilizada en casos de empresas similares una vez que se demuestre su validez y confiabilidad.

Según Cortes e Iglesias, la justificación practica nos dice que nos deberás sustentar que la investigación ayudara a resolver problemas o hacer toma de decisiones. ¿La investigación tendrá un resultado que tenga alguna aplicación y que pueda mostrar los resultados? ¿La investigación tendrá un resultado que permitirá ayudar a mejorar procesos y sistemas de una empresa?, ¿La investigación tendrá un resultado que dé solución económica, administrativa u otro caso práctico? (2004, p. 15)

La implementación de la norma internacional estándar se desarrollará con la finalidad de mejorar la seguridad de la información en la empresa nuevo mundo viajes, lo cual contará con la ayuda de una solución práctica con estándares de calidad a nivel mundial.

Justificación Tecnológica

La tecnología es una herramienta muy importante en los últimos de uso fundamental para cualquier negocio, por lo que es necesario considerar los lineamientos a fin de poder mejorar la calidad de la seguridad de la información, en base al ISO 27002, lo cual nos permitirá gestionar de manera correcta las amenazas y poder mitigarlas haciendo uso de herramientas pertinentes, con la finalidad de poder reducir las ocurrencias sobre la seguridad en los activos de información.

1.6 Hipótesis

Hipótesis general

HG: La ISO/IEC 17799 tiene un efecto significativo en la Seguridad de la Información en la empresa Nuevo Mundo Viajes

Hipótesis específicas

HE1: La ISO/IEC 17799 tiene un efecto positivo en la Confidencialidad de la Seguridad de la Información en la empresa Nuevo Mundo Viajes

HE2: La ISO/IEC 17799 tiene un efecto positivo en la Integridad de la Seguridad de la Información en la empresa Nuevo Mundo Viajes

HE3: La ISO/IEC 17799 tiene un efecto positivo en la disponibilidad de la Seguridad de la Información en la empresa Nuevo Mundo Viajes

1.7 Objetivos

Objetivo general

Determinar el efecto de la ISO/IEC 17799 en la Seguridad de la Información en la empresa Nuevo Mundo Viajes

Objetivos específicos

Como objetivos específicos tenemos:

OE1: Determinar efecto de la ISO/IEC 17799 en la confidencialidad de la Seguridad de la Información en la empresa Nuevo Mundo Viajes

OE2: Determinar efecto de la ISO/IEC 17799 en la integridad de la Seguridad de la Información en la empresa Nuevo Mundo Viajes

OE3: Determinar efecto de la ISO/IEC 17799 en la disponibilidad de la Seguridad de la Información en la empresa Nuevo Mundo Viajes.

II. MÉTODO

2.1. Diseño de Investigación

2.1.1. Enfoque de investigación

De acuerdo a Hernández, Fernández y Baptista el enfoque cuantitativo emplea la recolección de datos a fin de demostrar las hipótesis, con fundamento matemático y un análisis estadístico que permiten definir patrones de comportamiento que permiten probar teorías. Es como un conjunto de procesos secuenciales y probatorios. De manera escalable, esto quiere decir que no se debe prescindir de ningún proceso antecesor. Parte de una idea que se tenga, se aterriza de la cual se desprenden los objetivos y las interrogantes de la investigación. Así mismo, partimos a realizar nuestro marco teórico. De las preguntas de investigación se van a desprender las hipótesis y a su vez las variables de estudio, estableciendo un diseño para probarlas, midiendo las variables, se analizan los resultados que se obtengan. Finalmente se realizan las conclusiones de las hipótesis correspondientes. (2010, p. 4)

Esta investigación ha sido desarrollada en base a un enfoque cuantitativo en tanto se ha recolectado datos para efectuar las mediciones correspondientes para luego definir las conclusiones con las hipótesis formuladas.

2.1.2. Tipo de estudio

La investigación científica plasma dos objetivos principales los cuales son generar conocimiento, conocido como investigación básica, y solucionar problemas, conocido como investigación aplicada. (Hernández, 2014)

Esta investigación es aplicada porque usa la teoría existente para dar solución a un determinado problema.

2.1.3. Diseño de estudio

De acuerdo a Hernández, Fernández y Baptista el diseño pre-experimental Puros consiste en que se pueda utilizar la pre prueba y la pos prueba para poder analizar cómo lo grupos han evolucionado antes y después de realizar el realizar el experimento. Por otro lado, no todos los diseños experimentales utilizan la pre prueba, aunque si es necesaria la pos prueba ya que te ayuda definir los efectos que causo el experimento que se realizó en el grupo de control definido. (2010, p. 137)

RG_1	O_1	X	O_2
RG_2	O_3	—	O_4

A fin de poder desarrollar la presente tesis se empleara el diseño pre experimental, considerando la aplicación de la causa y efectos entre las variables. Además, la realización de un pre test; en el cual se realizó las métricas previas a la implementación de la ISO/IEC 17799 y el post test se realizará cuando ya esté implementada la ISO/IEC 17799 para corroborar las hipótesis planteadas.

2.2. Variable, operacionalización

2.2.1. Variable

Variable Independiente: ISO/IEC 17799

La ISO/IEC 17799 es un código de buenas prácticas que nos muestra el objetivo de control y además los controles que se recomiendan acerca de seguridad de la información. Posee 39 objetivos con 133 controles que están contenidos respectivamente en 11 dominios. (iso.org)

Variable Dependiente: Seguridad de la Información

La seguridad de la información tiene como facultad la protección de los sistemas de información ante las amenazas que se enfrentan. La aplicación de las medidas preventivas de seguridad se tiene que

hacer de una manera planeada y racional, para evitar emplear esfuerzos donde no hacen falta y dirigirlos de manera correcto donde se los necesite. Para que estas medidas y la estructura de protección sean eficaces, deben integrar todo dentro de un sistema de gestión de seguridad de la información. (Álvarez y Pérez, 2004, p. 2)

2.2.2. Operacionalización de las variables

Variable Independiente: ISO/IEC 17799

Variable Dependiente: Seguridad de la Información

Según la norma técnica peruana ISO/IEC 17799:

La seguridad de la información sirve, valga la redundancia, para proteger al activo "información" frente a las diversas amenazas con la finalidad de permitir que continúe el negocio, minimizar los daños que se puedan ocasionar a las organizaciones y generar un valor agregado a las inversiones y oportunidades del negocio. (2007, p. 1)

2.2.3. Matriz de Operacionalización de las variables

MATRIZ DE OPERACIONALIZACION DE LA VARIABLE SEGURIDAD DE LA INFORMACION

DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES	Instrumento	ESCALA Y VALORES
"La seguridad de la información tiene como facultad la protección de los sistemas de información ante las amenazas que se enfrentan. La aplicación de las medidas preventivas de seguridad se tiene que hacer de una manera planeada y racional, para evitar emplear esfuerzos donde no hacen falta y dirigirlos de manera correcto donde se los necesite. Para que estas medidas y la estructura de protección sean eficaces, deben integrar todo dentro de un sistema de gestión de seguridad de la información" (Álvarez y Pérez, 2004, p. 2).	La seguridad de la información sirve, para salvaguardar el activo "información" ante las diversas amenazas de tal forma que permita la seguridad de la continuidad del negocio, minimizar los daños que se puedan ocasionar a las organizaciones y generar un valor agregado a las inversiones y oportunidades del negocio. (2007)	Confidencialidad	Numero de accesos no autorizados	Ficha de observación	Razón
		Integridad	Manipulación de Datos		
		Disponibilidad	Tiempo en el cual un sistema se encuentra disponible =(tiempo real transcurrido - suma de tiempo de inactividad) / tiempo total transcurrido		

2.3. Población y muestra

Población

De acuerdo a Bernal (2010), cuando se habla de población nos referimos a todos los elementos que son objeto de la investigación, también se habla del conjunto. (p. 160). En esta investigación la población está representada por 30 registros mensuales de incidentes acerca de seguridad de la información de la empresa nuevo mundo.

Muestra

Según la investigación de Bernal (2010), la muestra se define como una pequeña parte de la población seleccionada, independientemente de la medición y observación de la variable, de ella se obtendrá información para la investigación. Castro (2003, p. 69) citó una vez a Hernández para decirnos: "Si la población es menor de cincuenta (50) individuos, entonces la población es igual a la muestra". Para este proyecto, el tamaño de la muestra será el mismo que nuestros 30 registros. .

Muestreo

Según Cortes e Iglesias (2010) Indica que el muestreo aleatorio simple o al azar representa la manera más común para tener la muestra representativa al azar. Ya que esto nos permite que cada uno de los individuos u objetos tenga las mismas posibilidades de ser elegidos. (p.91)

El tipo de muestreo que se empleara para la investigación será el probabilístico de tipo aleatorio simple.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

2.4.1. Técnica

- **Observación**

  Nos dice Bernal (2010), esa técnica posee más credibilidad cada día además de que su uso que empieza a generalizar, ya que permite a obtener la información de forma muy directa y

que es confiable de manera que se haya hecho mediante procesos sistematizado y controlado. (p, 194).

2.4.2. Instrumento

- Ficha de observación

  Es un sistema que permite registrar, valido de observación o conducta de un determinado objeto, situación o proceso. Es un método utilizado para estudios conductuales. Los pasos para poder armar un sistema de observación son:

  - Se define primero con mucha precisión el universo de lo que se piensa observar
  - Luego se extrae la muestra representativa de lo que tenemos pensado en observación.
  - Repertorio de las conductas que serán observadas
  - Se estable y define las unidades observadas
  - Se estable y define categorías y sub-categorías de la observación. (p.130)

2.4.3. Validez del instrumento

Según Bernal (2010), cuando una herramienta mide todo aquello a lo que estamos destinados, se puede ver su efectividad. Esto nos permite determinar en qué medida nos dan conclusiones en función de los resultados que obtuvimos. (Página 248)

Para este instrumento se ha empleado el método de juico de experto, lo que permite definir la validez del instrumento, por lo cual se seleccionó a 2 personas expertas que son: Jefe de Plataforma y soporte TI, y el director de TI.

2.4.4. Confiabilidad del instrumento

Para Bernal (2010), Citando a McDaniel y Gates nos dice que la Confiabilidad se asume como la capacidad del mismo instrumento pueda a brindar los mismos resultados congruentes cuando lo aplicamos por segunda vez en el mismo ambiente. (1992, p. 302)

Las fichas de observación no necesitan un cálculo de confiabilidad, ya que la información que se obtendrá mediante un sistema desarrollado.

2.5. Método de análisis de datos

Lo primero que se hace es describir los valores, datos o puntuaciones que se han conseguido para cada variable. (Hernández *et al.*, 2014, p. 282).

En este proyecto se aplicará la herramienta estadística SPSS para el respectivo análisis de la muestra. Luego se representará los resultados en diagramas de barras comparativas. Para las pruebas de pre-test y post-test se han empleado métodos, tenemos la prueba de normalidad, y además de la prueba de hipótesis que esta detallada seguidamente:

2.5.1. Prueba de normalidad

A fin de corroborar la probabilidad se ha empleado las pruebas de kolgomorov-smirov (K-S) y de Shapiro, su aplicabilidad está en base a la cantidad de la muestra.

Donde podemos observar:

N>50 Kolgomorov-Smirov

N<50 Shapiro Wilk

No obstante, utilizar el programa SPSS para sacar el valor sig., a fin de poder adoptar la distribución normal o no normal.

Significancia<0.05 No normal

Significancia >0.05 Normal

En la presente investigación se empleara el método shapiro wilk para todos los indicadores, considerando que la población es inferior a 50, de igual forma se empleará pruebas paramétricas, en tanto los resultados de normalidad fueron mayores a 0.05, siendo una distribución normal. En el caso de la prueba de hipótesis se empleará el método T-student ya que esta es una prueba para dos muestras normales paramétricas de tipo relacionadas.

2.5.2. Desviación estándar

Ésta es la desviación de la puntuación del promedio. Use el símbolo "σ" porque la desviación de cada puntaje de la media será al cuadrado, así que sume las desviaciones al cuadrado, divida por el número total de puntajes y luego saque la raíz cuadrada de esta división (Hernández, Fernández y Baptista, 2010, p. 355).

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(X - \bar{x})^2}{N}}$$

2.5.3. Varianza

Nos dicen Hernández, Fernández y Baptista (2010, p.357), que sobre este tema se emplea el valor elevado al cuadro de la desviación estándar y se simboliza como σ2.

$$\sigma^2 = \frac{\sum_{i=1}^{N}(X - \bar{x})^2}{N}$$

2.5.4. Prueba para muestras relacionadas

El empleo de esta prueba nos permitirá verificar si alguna diferencia entre la distribución de las poblaciones en cuestión, partiendo de 2

> poblaciones, ya sea dependientes o relacionadas, que cada unidad de muestra se relacione con otra unidad de la posterior muestra. Además, deben ser los más parecido posible para que lo que se va a medir sea lo más relevante. (Alea, 2000, p. 117)

2.6. Aspectos éticos

Se respetará la propiedad intelectual y lo referente al derecho de autor, igualmente se respetara la confidencialidad de la información brindada por la Oficina de Plataforma y Soporte TI de la empresa Nuevo Mundo Viajes. De igual forma se respetara la confidencialidad de la identidad de las personas que apoyaron a la investigación.

III. RESULTADOS

Los resultados que se dan en la investigación han sido dados usando los indicadores Número de accesos no autorizados, Manipulación de datos. Además, se observa la aplicación de la ISO/IEC 17799 para la gestión de seguridad de la información aplicable a la empresa Nuevo Mundo Viajes, de igual forma se ejecutará el procesamiento de los datos que se hayan alcanzado con las muestras de cada indicador (tanto para el pre test y el post test) con el software IBM SPSS Statistics v.21.

3.1. Pruebas de Normalidad

A fin de poder llevar a cabo la prueba de normalidad se ha empleado el método de Shapiro-Wilk, para los indicadores de las dimensiones, en tanto que:

Cuando $n \geq 50$, utilizamos el método de Kolmogorov-Smirnov.

Cuando $n < 50$, utilizamos el método Shapiro-Wilk.

Se pudo apreciar previamente, que la muestra de los indicadores planteados es menos de 50, por lo que la prueba de normalidad se efectuó ingresando datos recolectados por indicador, así como en la pre prueba como en la post prueba en la herramienta IBM SPSS Statistics v.21 con el nivel de confiabilidad del 95% con las condiciones:

Significancia < 0.05, distribución no normal.

Significancia ≥ 0.05, distribución normal.

3.2. Indicador: Número de accesos no autorizados

PRE-PRUEBA

Se presenta una tabla con los resultados descriptivos del indicador número de accesos no autorizados previo a la aplicación de la ISO/IEC 17799:

Descriptivos

Tipo				Estadístico	Error típ.
Valor	Accesos_	Media		13.17	.565
		Intervalo de confianza para la media al 95%	Límite inferior	12.01	
			Límite superior	14.32	
		Media recortada al 5%		13.13	
		Mediana		13.00	
		Varianza		9.592	
		Desv. típ.		3.097	
		Mínimo		8	
		Máximo		19	
		Rango		11	
		Amplitud intercuartil		5	
		Asimetría		.191	.427
		Curtosis		-.987	.833

Figura 4. Medidas descriptivas de números de accesos no autorizados antes de la implementación de la ISO 17799

Como podemos ver en la tabla, encontramos los datos obtenidos de la prueba de normalidad, que corresponde al número de indicadores de acceso no autorizado en la preprueba, porque es menor a 50, usamos "shapiro-wilk"

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
Tipo		Estadístico	gl	Sig.	Estadístico	gl	Sig.
Valor	Accesos_	.125	30	.200*	.957	30	.252

*Figura 5**. Prueba de normalidad para número de accesos no autorizados antes de la implementación de la ISO 17799***

Como se muestra en la figura, el nivel de significancia previa a la prueba del número de indicadores de acceso no autorizado es 0.252, que es mayor que el 0.05 indicado, y los indicadores seguirán una distribución normal.

POST-PRUEBA

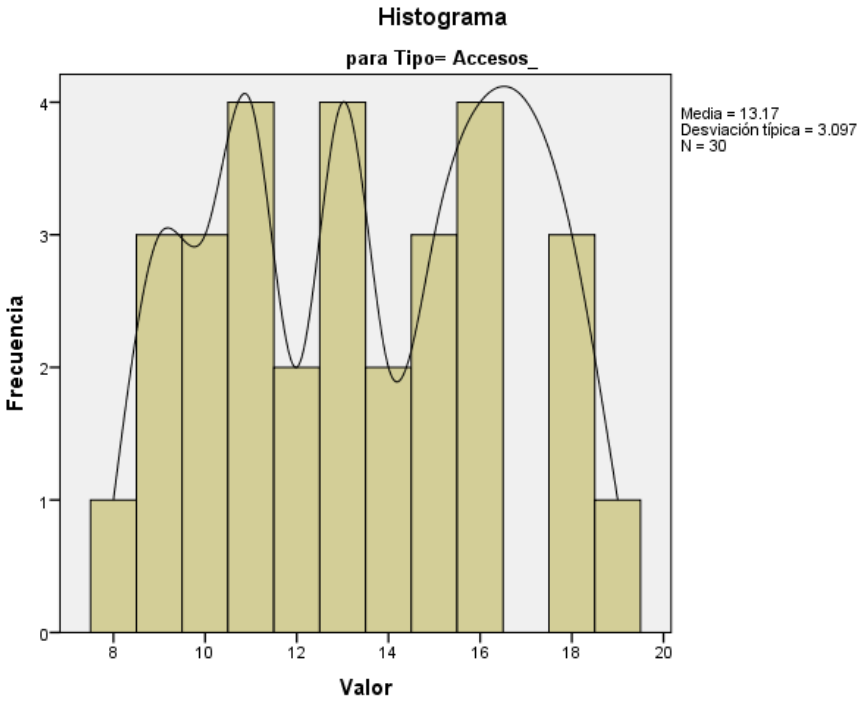


Figura 6. Histograma de número de accesos no permitidos previo a la aplicación de la ISO/IEC 17799

En presente tabla, están los datos obtenidos descriptivos del indicador número de accesos no autorizados posterior a la aplicación de la ISO/IEC 17799:

Descriptivos

Tipo				Estadístico	Error típ.
Valor	Accesos_	Media		5.57	.409
		Intervalo de confianza para la media al 95%	Límite inferior	4.73	
			Límite superior	6.40	
		Media recortada al 5%		5.57	
		Mediana		5.50	
		Varianza		5.013	
		Desv. típ.		2.239	
		Mínimo		2	
		Máximo		9	
		Rango		7	
		Amplitud intercuartil		3	
		Asimetría		.034	.427
		Curtosis		-1.102	.833

Figura 7. Medidas descriptivas de números de accesos no permitidos después de la aplicación de la ISO 17799

En la tabla se pueden apreciar los datos obtenidos de la prueba de normalidad para el indicador número de accesos no autorizados que corresponde al pre-test, como es menos que 50 se trabaja con “shapiro – wilk”

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Tipo	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Valor	Accesos_	.125	30	.200*	.939	30	.088

Figura 8. ***Prueba de normalidad para número de accesos no autorizados después de la implementación de la ISO 17799***

Se puede observar que, para el indicador en la prueba posterior, es 0.088 mayor que 0.05, entonces se puede concluir que el indicador obtendrá una distribución normal. Finalmente, cuando la prueba de normalidad se realiza en el número de indicadores de acceso no autorizado, los resultados de significancia antes y después de la implementación de ISO / IEC 17799 son ambos mayores que 0.05. Por lo tanto, se utilizarán pruebas paramétricas para probar hipótesis.

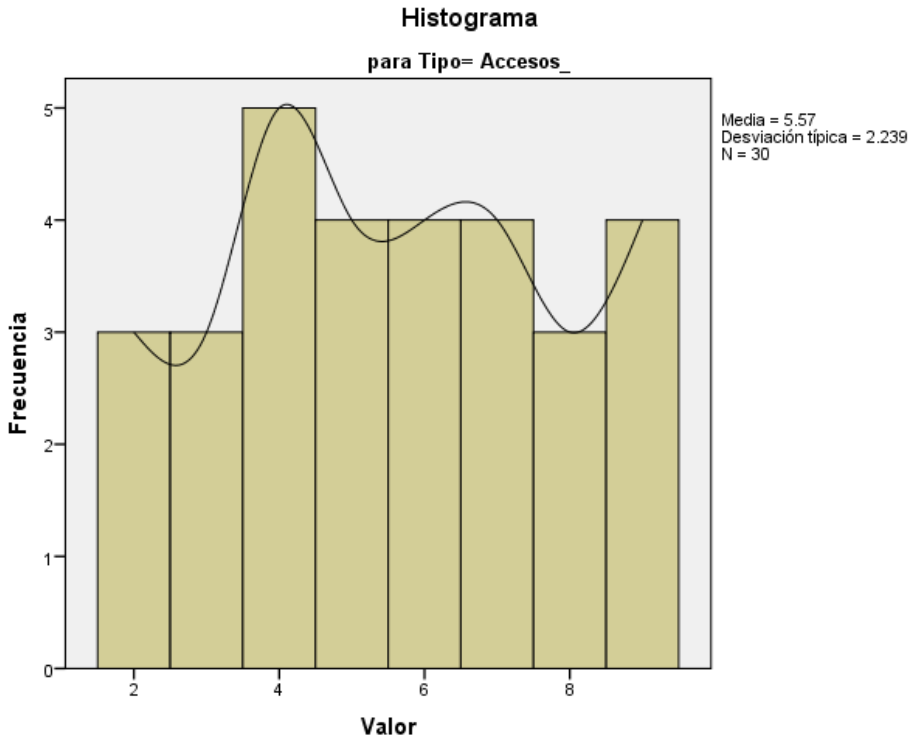


Figura 9. Histograma de número de accesos no autorizados posterior a la implementación de la ISO/IEC 17799

Prueba de Hipótesis
Se procede a ser verificada:

- **Hipótesis especifica 1**

  La ISO/IEC 17799 presenta efectos positivos en la Confidencialidad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes

  Indicador:

  Número de accesos no autorizados

  Hipótesis Estadística:

  Hipótesis Nula (H10): La ISO/IEC 17799 no tiene un efecto positivo en la Confidencialidad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes.

  Hipótesis Alternativa (H1A): La ISO/IEC 17799 tiene un efecto positivo en la Confidencialidad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes.

Prueba de muestras relacionadas

		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia Inferior	Superior			
Par 1	Accesos_no_autori_Pre - Accesos_no_autori_Post	7.833	2.451	.447	6.918	8.748	17.507	29	.000

Figura 10. Prueba de T-Student para la cantidad de accesos no permitidos

De los resultados obtenidos de la prueba t-student se obtuvo una probabilidad de 0.000, inferior a la probabilidad que asumimos de 0.005, por lo tanto no se acepta la hipótesis nula, entonces la cantidad de accesos no permitidos previo a la aplicación de la ISO/IEC 17799 es superior a lo que se observa posterior a la implementación de la ISO/IEC 17799

Estadísticos de muestras relacionadas

		Media	N	Desviación típ.	Error típ. de la media
Par 1	Accesos_no_autori_Pre	13.17	30	3.097	.565
	Accesos_no_autori_Post	5.33	30	1.605	.293

Figura 11. Paralelo entre medidas para el número de accesos no permitidos previo y posterior a la aplicación de la ISO/IEC 17799

Además, se evidencia que la cantidad de accesos no autorizados resulta inferior en el post test con una media de 5.33 en comparación del pre-test que posee una media de 13.17; por ende, la aplicación de la ISO/IEC 17799 tienen un efecto positivo en el número de accesos no autorizados.

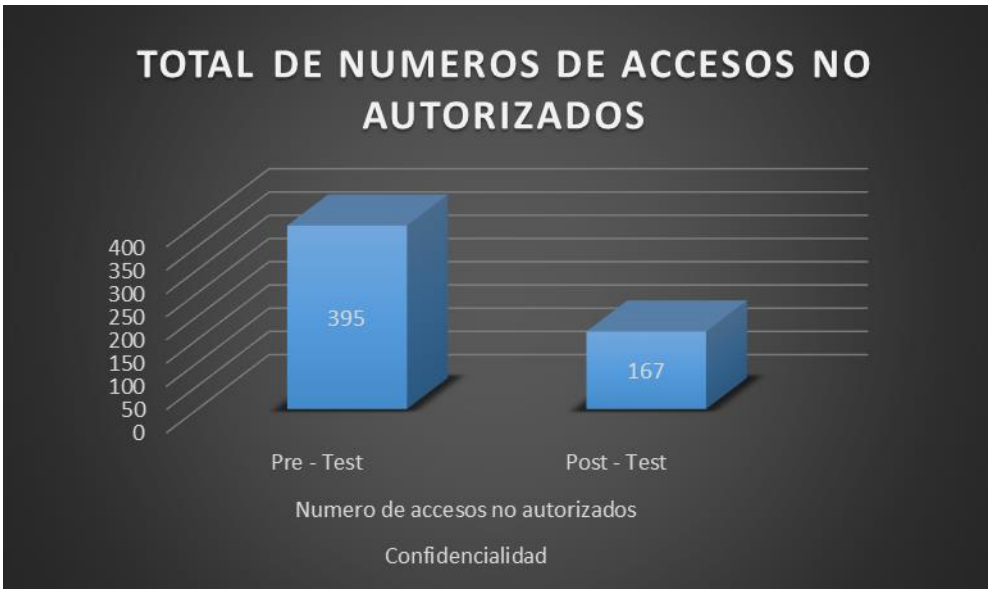


Figura 12. ***Resultados comparativos posterior de la implementación de la ISO/IEC 17799***

Como se aprecia luego de la implementación de la ISO/IEC 17799 se redujo de manera considerable la cantidad de accesos no autorizados, disminuyendo de 395 registros a 167 en el periodo de un mes.

3.3. Indicador: Manipulación de datos

PRE-PRUEBA

En esta tabla, los resultados descriptivos del indicador de manipulación de datos antes de aplicar ISO / IEC 17799:

Descriptivos

	Tipo			Estadístico	Error típ.
Valor	Manipula	Media		7.97	.367
		Intervalo de confianza para la media al 95%	Límite inferior	7.22	
			Límite superior	8.72	
		Media recortada al 5%		7.96	
		Mediana		8.00	
		Varianza		4.033	
		Desv. típ.		2.008	
		Mínimo		4	
		Máximo		12	
		Rango		8	
		Amplitud intercuartil		3	
		Asimetría		.104	.427
		Curtosis		-.586	.833

Figura 13. Medidas descriptivas de la manipulación de datos previa a la aplicación de la ISO/IEC 17799

Como podemos ver, es obvio que la prueba de normalidad del índice de procesamiento de datos corresponde a la pre-prueba, porque es menor a 50, usamos "shapiro-wilk" para trabajar.

Pruebas de normalidad

	Tipo	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
		Estadístico	gl	Sig.	Estadístico	gl	Sig.
Valor	Manipula	.127	30	.200*	.970	30	.536

*. Este es un límite inferior de la significación verdade

a. Corrección de la significación de Lilliefors

Figura 14. ***Prueba de normalidad para*** *de la manipulación de datos previo a la aplicación de la ISO/IEC 17799*

Tal como se visualiza, el nivel de significancia en el pre-test para el indicador manipulación de datos es de 0.536 siendo mayor que 0.05 que se había indicado, el indicador seguirá una distribución normal.

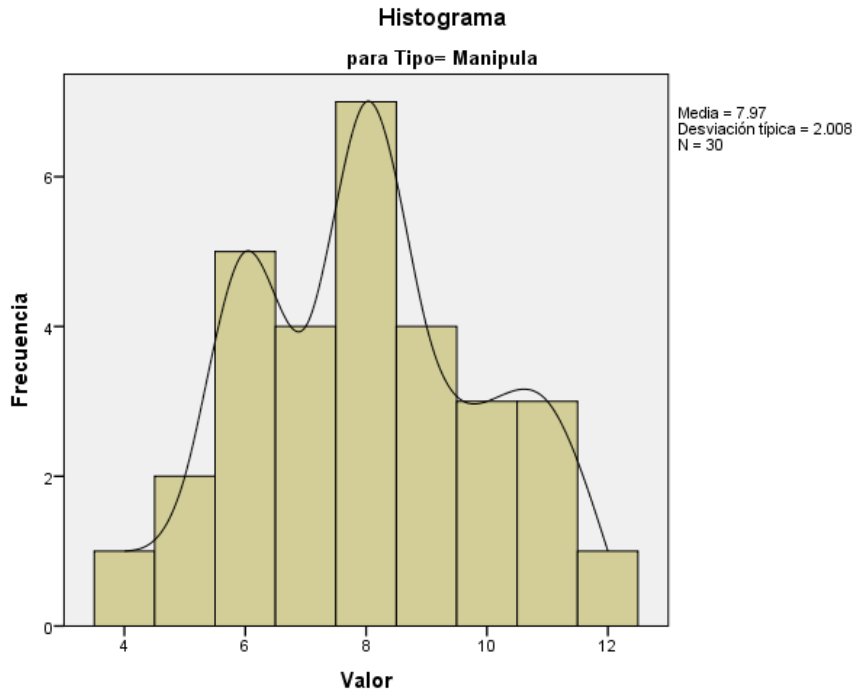


Figura 15. Histograma de la manipulación de datos antes de la aplicación de la ISO/IEC 17799

POST-PRUEBA

La tabla nos muestra resultados descriptivos del indicador manipulación de datos posterior a la aplicación de la ISO/IEC 17799:

Descriptivos

Tipo				Estadístico	Error típ.
Valor	Manipula	Media		3.67	.293
		Intervalo de confianza para la media al 95%	Límite inferior	3.07	
			Límite superior	4.27	
		Media recortada al 5%		3.63	
		Mediana		3.00	
		Varianza		2.575	
		Desv. típ.		1.605	
		Mínimo		1	
		Máximo		7	
		Rango		6	
		Amplitud intercuartil		2	
		Asimetría		.427	.427
		Curtosis		-.371	.833

Figura 16. Medidas descriptivas de la manipulación de datos posterior a la aplicación de la ISO/IEC 17799

Esta tabla nos permite ver visualmente el índice de operación de los datos correspondientes al post test obtenido de la prueba de funcionamiento normal, porque es menor a 50, por lo que usamos "shapiro-wilk"

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
Tipo		Estadístico	gl	Sig.	Estadístico	gl	Sig.
Valor	Manipula	.194	30	.005	.942	30	.101

a. Corrección de la significación de Lilliefors

*Figura 17. **Prueba de normalidad para** de la manipulación de datos después de la aplicación de la ISO/IEC 17799*

Se puede observar que el nivel de significancia en la prueba previa del indicador de manipulación de datos es 0.536, que es mayor que el 0.05 indicado, y el indicador seguirá una distribución normal.

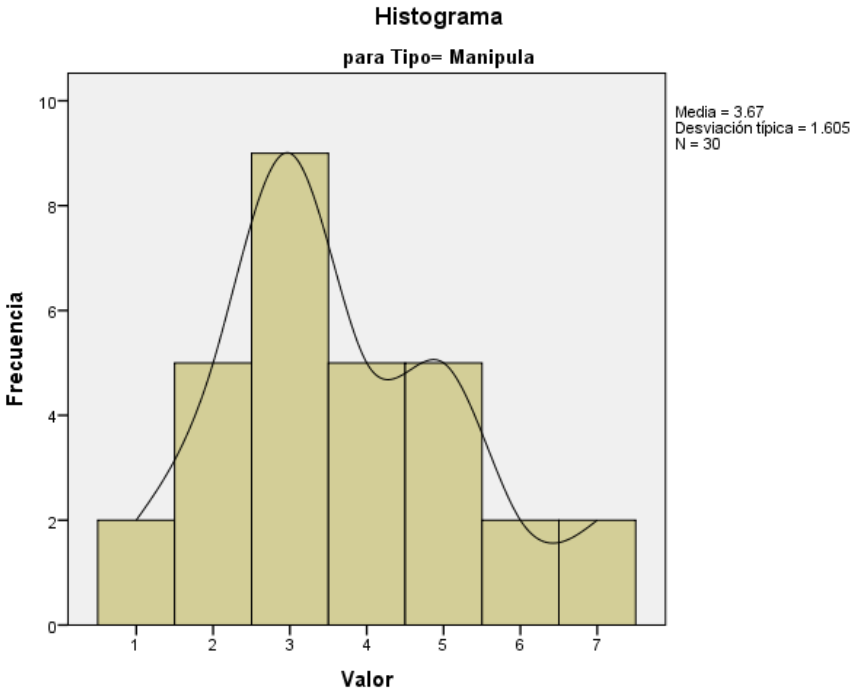


Figura 18. Histograma de la manipulación de datos posterior a la implementación de la ISO/IEC 17799

Prueba de Hipótesis
Se procede a ser verificada:

- **Hipótesis especifica 2**

  La ISO/IEC 17799 tiene un efecto positivo en toda la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes

  Indicador:

  Manipulación de Datos

  Hipótesis Estadística:

Hipótesis Nula (H20): La ISO/IEC 17799 no tiene un efecto positivo en toda la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes.

Hipótesis Alternativa (H2A): La ISO/IEC 17799 tiene un efecto positivo en toda la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes

Prueba de muestras relacionadas

		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
					Inferior	Superior			
Par 1	manipulacion_datos_Pre - manipulacion_datos_Post	4.300	1.291	.236	3.818	4.782	18.250	29	.000

Figura 19. Prueba de T-Student para la manipulación de datos

Los resultados obtenidos de la prueba t-student nos muestra la probabilidad de 0.000, inferior a la probabilidad que nosotros asumimos que es de 0.005, por ende, no es permisible la hipótesis nula, por lo que la manipulación de datos previo de la aplicación de la ISO/IEC 17799 es mucho mayor a lo que observamos posterior de la aplicación de la ISO/IEC 17799.

Estadísticos de muestras relacionadas

		Media	N	Desviación típ.	Error típ. de la media
Par 1	manipulacion_datos_Pre	7.97	30	2.008	.367
	manipulacion_datos_Post	3.67	30	1.605	.293

Figura 20. Comparación de medias para la manipulación de datos antes y después de la implementación de la ISO/IEC 17799

Además, se muestra que la manipulación de datos resulta inferior en el post-test con una media de 3.67 en comparación del pre-test que posee una media de 7.97; por ende, la implementación de la ISO/IEC 17799:2007 tienen un efecto positivo en la manipulación de datos.

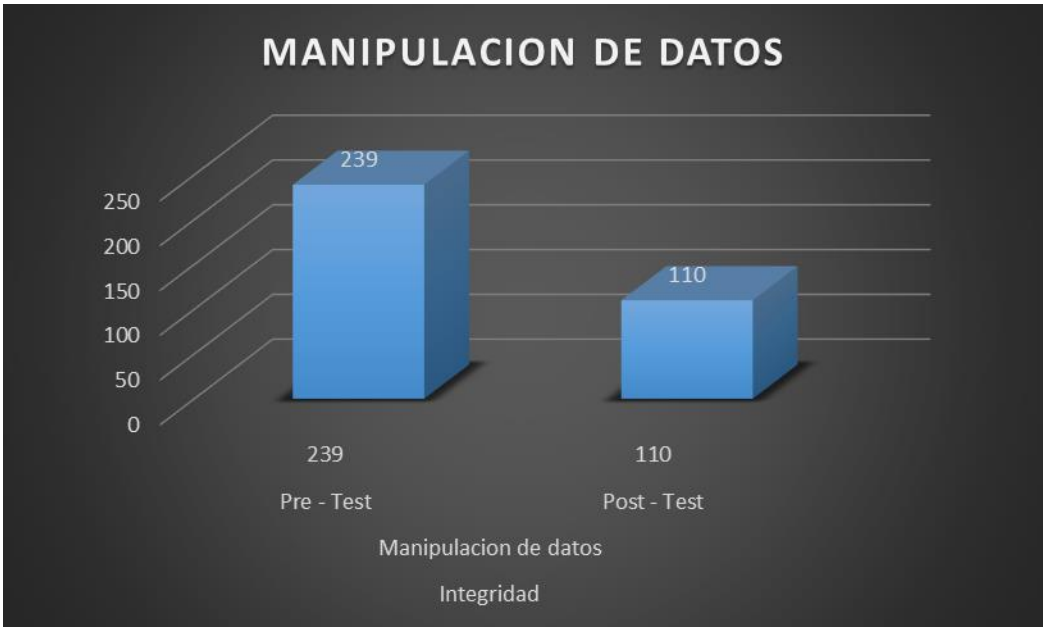


Figura 21. ***Resultados comparativos después de la aplicación de la ISO/IEC 17799***

Como conclusiones ante la aplicación de la ISO/IEC 17799 se redujo de manera considerable el número de manipulación de datos, disminuyendo de 239 registros a 110 en el periodo de un mes.

3.4. Indicador: tiempo en el que un sistema está disponible

PRE-PRUEBA

La tabla nos muestra los resultados descriptivos del indicador Tiempo en que un sistema se encuentra disponible antes de la implementación de la SO/IEC 17799:

Descriptivos

Tipo				Estadístico	Error típ.
Valor	Diponibi	Media		.7067	.00480
		Intervalo de confianza para la media al 95%	Límite inferior	.6968	
			Límite superior	.7165	
		Media recortada al 5%		.7072	
		Mediana		.7100	
		Varianza		.001	
		Desv. típ.		.02631	
		Mínimo		.66	
		Máximo		.74	
		Rango		.08	
		Amplitud intercuartil		.05	
		Asimetría		-.122	.427
		Curtosis		-1.412	.833

Figura 22. Medidas descriptivas del tiempo en el que un sistema está disponible previo a la implementación de la ISO/IEC 17799

En la tabla, se visualiza que los datos obtenidos de la prueba de normalidad para el indicador manipulación de datos que corresponde al pre-test, como es menos que 50 se trabaja con “shapiro – wilk”

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
Tipo		Estadístico	gl	Sig.	Estadístico	gl	Sig.
Valor	Diponibi	.211	30	.001	.887	30	.004

a. Corrección de la significación de Lilliefors

Figura 23. Prueba de normalidad para el tiempo en el que un sistema está disponible antes de la implementación de la ISO/IEC 17799

Tal como se visualiza, el nivel de significancia en el pre-test para el indicador manipulación de datos es de 0.004 siendo inferior que 0.05 que se había indicado, el indicador seguirá una distribución no normal.

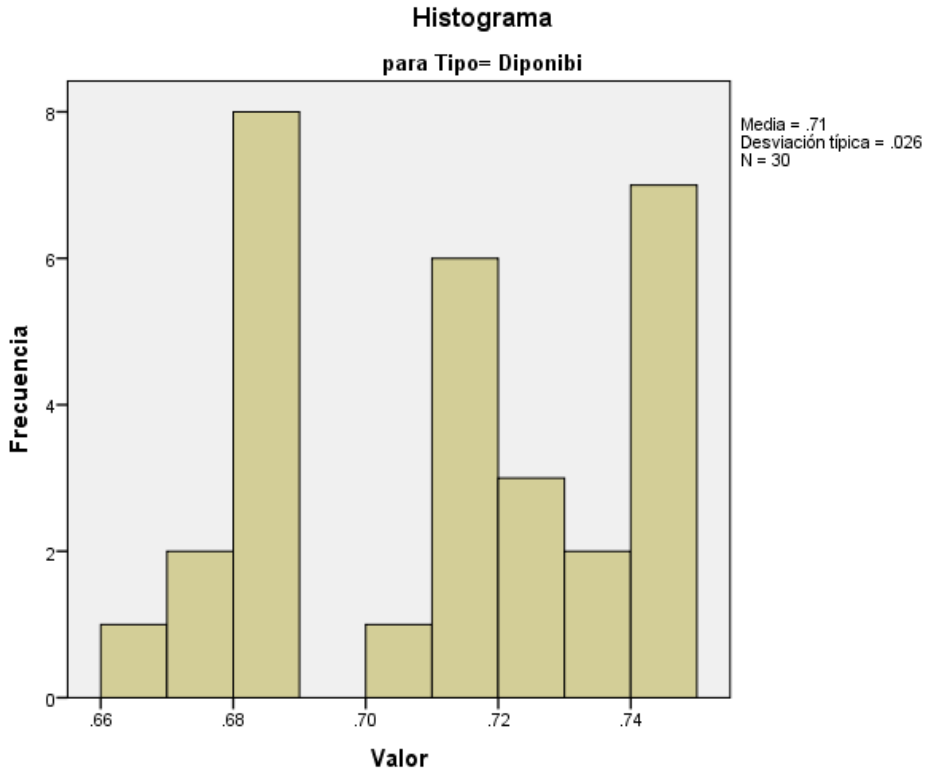


Figura 24 Histograma del tiempo en el que un sistema está disponible antes que se implemente la ISO/IEC 17799

POST-PRUEBA

En la presente tabla, se muestra los resultados descriptivos del indicador Tiempo en que un sistema se encuentra disponible posterior a la implementación de la ISO/IEC 17799:

Descriptivos

Tipo				Estadístico	Error típ.
Valor	Diponibi	Media		.9837	.00148
		Intervalo de confianza para la media al 95%	Límite inferior	.9806	
			Límite superior	.9867	
		Media recortada al 5%		.9841	
		Mediana		.9900	
		Varianza		.000	
		Desv. típ.		.00809	
		Mínimo		.97	
		Máximo		.99	
		Rango		.02	
		Amplitud intercuartil		.01	
		Asimetría		-.792	.427
		Curtosis		-.978	.833

Figura 25. Medidas descriptivas del tiempo en el que un sistema está disponible posterior a la implementación de la ISO/IEC 17799

La tabla nos permite apreciar que los resultados de la prueba de normalidad para el indicador manipulación de datos que corresponde al post-test, como es menos que 50 se trabaja con “shapiro – wilk”

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
Tipo		Estadístico	gl	Sig.	Estadístico	gl	Sig.
Valor	Diponibi	.350	30	.000	.720	30	.000

a. Corrección de la significación de Lilliefors

Figura 26. Prueba de normalidad para el tiempo en el que un sistema está disponible posterior a la implementación de la ISO/IEC 17799

Tal como se visualiza, el nivel de significancia en el pre test para el indicador manipulación de datos es de 0.000 siendo inferior que 0.05 que se había indicado, el indicador seguirá una distribución no normal.

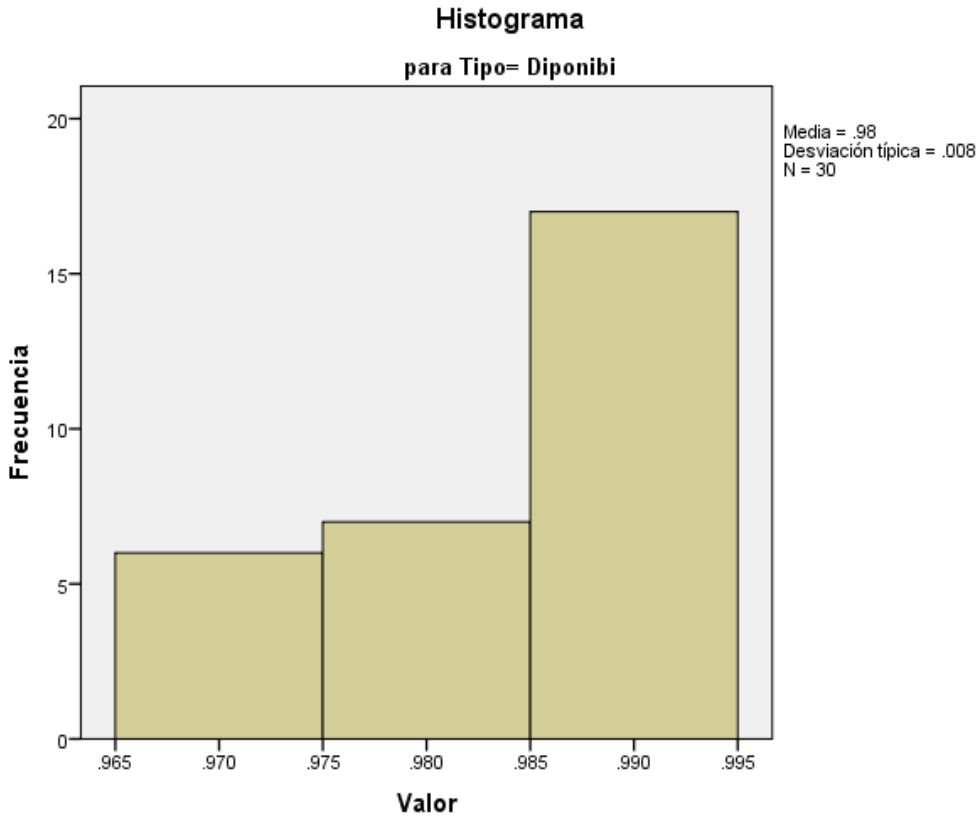


Figura 27. Histograma del tiempo en el que un sistema está disponible posterior a la implementación de la ISO/IEC 17799

Prueba de Hipótesis
Se procede a ser verificada:

- **Hipótesis especifica 3**

  La ISO/IEC 17799 tiene un efecto positivo en la Disponibilidad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes

  Indicador:

  Tiempo en el que un sistema se encuentra disponible

  Hipótesis Estadística:

  Hipótesis Nula (H20): La ISO/IEC 17799 no tiene un efecto positivo en la disponibilidad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes.

  Hipótesis Alternativa (H2A): La ISO/IEC 17799 tiene un efecto positivo en la disponibilidad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes.

En este indicador se realizó la prueba de wilcoxon ya que nuestros datos no tenían una distribución normal. El resultado obtenido de la prueba evidencia que el nivel de significancia es inferior a 0,05 rechazándose la hipótesis nula.

Resumen de prueba de hipótesis

	Hipótesis nula	Test	Sig.	Decisión
1	La mediana de las diferencias entre manipulacion_datos_Pre y manipulacion_datos_Post es igual a 0.	Prueba de Wilcoxon de los rangos con signo de muestras relacionadas	.000	Rechazar la hipótesis nula.

Se muestran las significancias asintóticas. El nivel de significancia es .05.

Figura 28. Prueba de wilcoxon para el tiempo en el que un sistema se encuentra disponible.

IV. DISCUSIÓN

Considerando los resultados que se han alcanzado en la investigación, se ha analizado y comparado el número de accesos no autorizados, la manipulación de datos y el porcentaje en el que un sistema se encuentra disponible antes y después información en la empresa Nuevo Mundo Viajes.

- En el caso del número de accesos no autorizados, el resultado del pre test fue de un promedio de 13.13 de accesos no autorizados, y luego de implementar la ISO/IEC 17799 se redujo a un promedio de 5.57. Esto demuestra que si existo una reducción de 7.56 en los números de accesos no autorizados, afirmándose que con la implementación de la ISO se logró una disminución en un 57.57% en el número de accesos no autorizados en la empresa nuevo mundo viajes.

  En la investigación que fue realizada por Barrantes, se puede observar que tanto el diseño como la implementación mejoro en un 78.5% implementado políticas de seguridad, relacionado con confidencialidad; en la relación a los números de accesos no autorizados se redujo en un 57.57% en la presente investigación. Además, en la investigación por Olaza, los resultados nos demuestran que la implementación de la NTP ISO/IEC 27001 redujo en un 72.5% la cantidad de información sobre confidencialidad que fue divulgada.

- La manipulación de datos, los resultados del pre test fueron de un promedio de 7.96 datos manipulados, posteriormente de la implementación de la ISO/IEC 17799 se redujo a un promedio de 3.63. Se puede decir que si existió una reducción de 4.06 en los datos manipulados, pudiendo afirmar que con la implementación de la ISO se logró una disminución en un 54.4% en la cantidad de datos manipulados en la empresa nuevo mundo viajes.

  En la investigación de Alcántara (2015), se aprecia que la implementación de la ISO/IEC 27001, logro disminuir los riesgos hasta en un 10%, con relación a los datos que se obtuvieron en la manipulación de datos, se redujeron en un 54,4%, permitiendo así la integridad de la información en la empresa nuevo mundo viajes.

- El tiempo en el que un sistema se encuentra disponible, en los resultados del pre test fue de un promedio de 0.7072, con la implementación de la ISO/IEC 17799 se incrementó con un promedio de 0.9841, con lo que se puede afirmar que el tiempo en el que un sistema está disponible aumento en un 27.7% en la empresa nuevo mundo viajes.

  Según la investigación realizada por Olaza, A (2017), se demostró que la implementación basada en la ISO/IEC 27001, ha mejorado el porcentaje de tiempo en el que el sistema se encuentra disponible para el usuario, incrementándose en un 39.7%. Además, Alcántara, J (2015), en su investigación mejoro en un 4% el proceso empleado para el descubrimiento de aspectos extraños en la seguridad de la información; así en base a los datos obtenidos en el tiempo en el que un sistema se encuentra disponible se incrementó en un 27.7%, siendo ahora el 98.37% el tiempo en el que un sistema se encuentra disponible, teniendo así un impacto significativo en la disponibilidad de la seguridad de la información en la empresa nuevo mundo viajes

V. CONCLUSIONES

En la presente investigación las conclusiones fueron las siguientes:

- La cantidad de accesos no autorizados en la empresa nuevo mundo viajes antes de que se implemente el ISO/IEC 17799 para una muestra de 30 registros fue de un promedio de 13.13 de accesos son autorización, ya con la implementación de la ISO/IEC 17799 fue de 5.57 lo que representa una reducción en un 57.57% en la cantidad de accesos no autorizados, lo cual incremento la confidencialidad de la información en la empresa nuevo mundo viajes.

- Se determinó que la manipulación de datos en la empresa nuevo mundo viajes antes de que se implementará la ISO/IEC 17799 para una muestra de 30 registros fue un promedio de 7.96 datos manipulados, luego de la implementación de la ISO/IEC 17799 se obtuvo un promedio de 3.63 de datos manipulados, lo cual representa una reducción en un 54.4% en la cantidad de datos manipulados en la empresa nuevo mundo viajes. Lo cual significa que si hubo un impacto significativo en la integridad de la seguridad de la información en la empresa nuevo mundo viajes.

- Se determinó que el tiempo en el que un sistema está disponible en la empresa nuevo mundo viajes antes de que se implementara la ISO/IEC 17799 para una muestra de 30 registros fue un promedio de 0.7072 en el tiempo en el que un sistema estaba disponible y con la implementación de la ISO/IEC 17799 se incrementó con un promedio de 0.9841, lo cual se representa en un incremento del 27.7%, siendo ahora el 98.37% el tiempo en el que un sistema se encuentra disponible, teniendo así un impacto significativo en la disponibilidad de la seguridad de la información en la empresa nuevo mundo viajes.

- Concluyentemente, considerando los buenos resultados obtenidos en la presente de los indicadores propuestos, podemos concluir que la

implementación de la ISO/IEC 17799 ha sido positivo en la seguridad de la información, reduciendo los incidentes de seguridad alineados a los numero de accesos no autorizados, manipulación de datos e interrupciones de los activos de información en la empresa nuevo mundo viajes.

VI. RECOMENDACIONES

En el presente trabajo investigatorio presento las siguientes recomendaciones:

- Se recomienda analizar la situación de los activos informáticos de las demás franquicias de la corporación, para así poder aplicar y mitigar lo debilidades respecto a la seguridad de la información, como se puede ver realizado en la presente investigación.
- Se recomienda la capacitación a los usuarios con respecto a la seguridad de la información, lograr la concientización de estos, para así mejorar la seguridad por parte del talento humano el cual es sumamente importante en una organización y lograr controlar de una manera más efectiva las vulnerabilidades por esa parte de la organización.
- Se recomienda implementar las ISO/IEC 17799 en las demás franquicias de la empresa para así poder lograr un mejor manejo de TI; para así lograr un gobierno de TI y así tener un mejor panorama del negocio alineado a TI.

REFERENCIAS

Aguirre, D. (2014). Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. Título de Ingeniero Informático. Pontificia Universidad Católica del Perú.

Alavarez, G. y Perez, P. (2004). Seguridad Informática para empresas y particulares. Madrid. McGraw-Hill/INTERAMERICANA DE ESPAÑA, S. A. U.

Alcántara, J. (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 cuidad de Chiclayo. Título de ingeniero de Sistemas y computación. Universidad católica Santo Toribio de Mogrovejo

Antonpass:[_]nicolae_07, yahoo. com. A. N., & a.nedelcu, unitbv. ro. N. A. (2015). Security Information and Risk Management Assessment. Applied Mechanics & Materials, 809/810, 1522–1527. https://doi.org/10.4028/www.scientific.net/AMM.809-810.1522

Barrantes C. y Hugo J. (2012). Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos. Título de Ingeniero de computación y de Sistemas. Universidad San Martin de Porres

Bravo, B. y Daudo, A. (2017). Diseño de gestión de seguridad de la información en base a la norma ISO 27002 y al estudio de situación actual de la empresa proveedora de internet “Posorja en acción cia. Ltda. Título de Ingeniero de sistemas computacionales. Universidad de Guayaquil

Castro, K. (2012). Formulacion de controles Basados en la norma NTC-ISO 27002 para la seguridad de la información en el comité departamental de cafeteros del Cauca. Título de Ingeniero de Sistemas. Universidad Francisco de Paula Santander Ocaña

Cortes, M. y Iglesias, M. (2004). Generalidades sobre metodología de la investigación. Campeche. Universidad Autónoma del Carmen

Cruz, L. y Fukusaki, L. (2017). Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información para proteger

los activos de información de la clínica MEDCAM Perú SAC. Título profesional de ingeniero de computación y sistemas. Universidad San Martin de Porres

David, B. (31 de Octubre de 2017). *Gestion*. Obtenido de Gestion: https://gestion.pe/tecnologia/54-empresas-procesos-respuesta-incidentes-ciberneticos-221651

De la Cruz, R. (2016). Propuesta de políticas, basadas en buenas practicas, para la gestión de seguridad de la información en la municipalidad provincial de Paita;2016. Título profesional de ingeniero de sistemas. Universidad Católica de Los Ángeles.

Doria, A. (2015). Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la universidad de Córdoba. Título de Especialista en seguridad informática. Universidad Nacional Abierta y a Distancia

Fenz, S., Plieschnegger, S., & Hobel, H. (2016). Mapping information security standard ISO 27002 to an ontological structure. *Information and Computer Security, 24*(5), 452-473. doi:http://dx.doi.org/10.1108/ICS-07-2015-0030

Filian, M. (2015). Implementación de un esquema de seguridad de informatica aplicado a los activos de la FIEC, basado en el estándar ISO 27002. Título de Magister en seguridad informática aplicada. Escuela superior Politécnica del Litoral

Flores, J. and Puppi, G. (2013). *"Gestión de la seguridad fisica y lógica para un centro de datos*. Titulo de Ingeniero de sistemas de informacion. Universidad Peruana de Ciencias Aplicadas.

Gavidia, S. y Torres, L. (2018). Implementacion de los controles de la ISO/IEC27002:2013 para la mejora del nivel de seguridad fisica y logica de la informacion en el area de TI de la Unión Peruana del Norte. Titulo de Ingeniero de sistemas. Universidad Peruana Union

García, J. y Del Águila, C. (2017). Análisis e implementacion de la seguridad de la información del centro de datos de la universidad nacional de la amazonia peruana bajo la norma ISO 27002. Título profesional de ingeniero de sistemas e informática. Universidad Nacional de la Amazonia Peruana.

Guallpa, L. (2017). Plan de Seguridad informática basada en la norma ISO 27002 para el control de accesos indebidos a la red de unidades Puyo. Título de Magister en informática empresarial.

Hernandez, R. , Fernandez, C. y Baptista, M. (2010). Metodología de la Investigación. México D.F. McGraw-Hill / INTERAMERICANA EDITORES, S.A. DE C.V.

Hernández, S., Fernández, C. y Baptista, M. (2014) Roberto. Metodología de la Investigación. 6° ed., Editorial McGraw-Hill.

ITGI: New guide aligning COBIT 4.1, ITIL V3 and ISO 27002 helps enterprises achieve maximum governance and value in a volatile economy. (2008, Nov 12). *M2 Presswire* Retrieved from HYPERLINK "https://search.proquest.com/docview/446159537?accountid=37408" https://search.proquest.com/docview/446159537?accountid=37408

Lapiedra, R., Devece, C. y Guiral, J. (2011). Introducción a la gestión de sistemas de información en la empresa. Recuperado de: HYPERLINK "http://www.sapientia.uji.es" www.sapientia.uji.es

Ledezma, D. (2015). Desarrollo de políticas de seguridad de la información basadas en las normas ISO 27002 para una coordinación zonal del INEC. Título de Magister en Gerencia Informática. Pontificia Universidad Católica del Ecuador Sede Ambato

Leiva, R. (2016). Diseño de un sistema de gestión de seguridad de la informacion basado en las normas ISO/IEC27001 e ISO/IEC 27002 para proteger los activos de la informacion en el proceso de suministros de medicamentos de la red de salud de Lambayeque 2015. Universidad Nacional Pedro Ruiz Gallo.

Lima Rios, O. K., da Silva Rios, V. P., & de Almeida Teixeira Filho, J. G. (2017). Melhores práticas do COBIT, ITlL e ISO/IEC 27002 para implantação de política de segurança da informação em Instituições Federais do Ensino Superior. Revista Gestão & Tecnologia, 17(1), 130–154. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=123244300&lang=es&site=ehost-live

Lin, H., Cefaratti, M., & Wallace, L. (2012). ENTERPRISE RISK MANAGEMENT, COBIT, AND ISO 27002: A CONCEPTUAL ANALYSIS. *Internal Auditing*, *27*(2), 3-12. Retrieved from HYPERLINK "https://search.proquest.com/docview/1002719391?accountid=37408" https://search.proquest.com/docview/1002719391?accountid=37408

Martínez, J. (2014). Controles de seguridad para reducir la cantidad de incidencias de seguridad de la información del año 2012 en el servicio de administración tributaria de Huancayo. Magister en Ingeniería de sistemas. Universidad Nacional del Centro del Perú

Mesones, Y. y Tineo, D. (2015). Políticas de seguridad organizacional y control de activos basado en NTP 17799 para la gestión de la Información de la empresa DELTRON SA. Título profesional de Ingeniero en computación e informática. Universidad Nacional Pedro Ruiz Gallo

Moscaiza, O. (2018). Diseño de un sistema de gestión de la seguridad de la informacion (SGSI) para la cooperativa de ahorro y crédito ABC, basado en la norma ISO 27701:2013. Título de Ingeniero de redes y comunicaciones. Universidad Peruana de Ciencias Aplicadas.

Molina, E., Rodríguez, O., Sánchez, Y. y Vergel, J. (2012). Guía para la seguridad basada en la norma ISO/IEC 27002, para la dependencia división de sistemas de la universidad francisco de paula Santander Ocaña. Título de especialista en auditoria de sistemas. Universidad francisco de Paula Santander Ocaña

Nastase, P, Nastase, F y IONESCU, C (2009). Challenges generated by the implementation of the IT Standards cobit 4.1, ITIL v3 and ISO/IEC27002 in enterprises. The Bucharest academy of economic studies.

NORMA TECNICA PERUANA. 2014. NTP-ISO/IEC 27001– 2014 – 2da Edición. LIMA. 2014. 45pp.

Olaza, H. (2017). Implementación de NTP ISO/IEC 27001 para la seguridad de información en el área de configuración y activos del ministerio de educación - Sede Centromin. Título profesional de ingeniero de sistemas. Universidad Cesar Vallejo

Olivos, F. y Guevara, E. (2017). Formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma técnica peruana NTP-ISO/IEC 17799 para la mejora de la gestión en la oficina central de computo – universidad de Lambayeque. Título de Ingeniero de Sistemas. Universidad de Lambayeque.

Palomino, K. (2017). Buenas practicas en seguridad de la información basada en ISO 27002 en la asociacion para el desarrollo empresarial en Apurímac - ADEA. Titulo profesional de ingeniero de sistemas. Universidad Nacional José María Arguedas

Pizaaro, I. (2018). Diseño de un modelo de gestión de seguridad de la información con un enfoque en el factor humano para el ICPNA Región centro en el año 2017. Titulo profesional de ingeniero en sistemas e informática. Universidad Continental.

Priandoyo, A. (2008), *Comparison between COBIT, ITIL and ISO 27001,* available on-line at http://www.securityprocedure.com/comparison-between-COBITitil-and-iso-27001;

Portantier, F. (2013). *Gestion de la seguridad informatica.* Buenos Aires, Dalaga, Argentina: Fox Andina.

Robalino, J. (2018). Propuesta Metodológica y simulación de la implementación de un SIEM basado en la norma ISO 27001 y/o 27002. Título de Magister en Conectividad y Redes de telecomunicaciones. Escuela Politécnica Nacional.

Schneider, L. C., Vanti, A. A., Cobo, A., & João Luis, P. T. (2014). EVALUATION OF INFORMATION SECURITY PROCESSES INTEGRATING THE CONTROLLERSHIP AND IT AREAS. *Revista Universo Contabil, 10*(4), 68-85. doi:http://dx.doi.org/10.4270/ruc.2014430

Solarte, F, Enriquez, E y Benaviddes, M. (2015). Metodologia de análisis y evaluación de riesgos aplicados a la seguridad de informática y de la información bajo la norma ISO/IEC 27001. Nariño. Universidad Nacional Abierta y a Distancia UNAD.

SORA, D. (2012). SECURING IT NETWORKS WITH ISMS FAMILY OF STANDARDS (ISO 27001 SERIES). Paper presented at the Retrieved from HYPERLINK

"https://search.proquest.com/docview/1328332933?accountid=37408"
https://search.proquest.com/docview/1328332933?accountid=37408

Suca, J. (2014). *Propuesta metodológica para implementar la norma técnica peruana ISO/IEC 27001:2008 de seguridad de la información en entidades públicas del estado*. Título de Ingeniera de Sistema. UNIVERSIDAD CATOLICA DE SANTA MARIA.

Tarrillo, E. y Correa, J. (2015). Metodología para un sistema de gestión de la seguridad de la información basado en la norma técnica peruana NTP-17799 en la administración de la municipalidad distrital de Lambayeque. Título de ingeniería de sistemas. Universidad Nacional Pedro Ruiz Gallo.

van Wessel, R. (2011). Implementing international standards for Information Security Management in China and Europe: a comparative multi-case study. Technology Analysis & Strategic Management, 23(8), 865–879. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=eoah&AN=25842420&lang=es&site=ehost-live

Vilca, E. (2017). Diseño e implementacion de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de Lima. Título profesional de Ingeniero de sistemas e Informática. Universidad de Huanuco.

Yaokumah, W. (2016). Investigation into the State-of-Practice of Operations Security Management Based on ISO/IEC 27002. International Journal of Technology Diffusion (IJTD), 7(1), 53–72. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=eoah&AN=44525464&lang=es&site=ehost-live

ANEXOS

Anexo 1: Ficha de Observación sobre Seguridad de la Información

Dimensiones						
ITEM	Numero de accesos no autorizados		Manipulacion de datos		Tiempo en el que un sistema está disponible	
DIAS	Pre - Test	Post - Test	Pre - Test	Post - Test	Pre - Test	Post - Test
1	18	9	7	3	68.00%	98.00%
2	15	7	6	2	68.00%	97.00%
3	10	3	9	4	68.00%	98.00%
4	12	6	5	1	73.00%	99.00%
5	9	3	8	3	71.00%	99.00%
6	11	8	11	6	71.00%	97.00%
7	13	5	10	5	72.00%	99.00%
8	19	7	12	7	74.00%	99.00%
9	11	2	8	3	74.00%	99.00%
10	8	3	6	2	68.00%	98.00%
11	10	5	8	4	66.00%	97.00%
12	16	4	5	3	68.00%	99.00%
13	9	2	9	7	67.00%	99.00%
14	13	4	10	4	74.00%	99.00%
15	15	7	7	3	71.00%	99.00%
16	16	4	8	4	71.00%	98.00%
17	14	6	6	2	67.00%	97.00%
18	16	8	8	6	74.00%	99.00%
19	18	9	9	5	74.00%	99.00%
20	12	5	11	3	74.00%	99.00%
21	13	9	7	2	68.00%	98.00%
22	10	4	8	4	68.00%	99.00%

23	9	2	4	2	68.00%	99.00%
24	11	8	6	3	73.00%	99.00%
25	15	7	9	5	71.00%	98.00%
26	18	6	8	3	71.00%	97.00%
27	13	6	10	5	72.00%	99.00%
28	11	5	6	1	74.00%	99.00%
29	16	9	11	5	72.00%	97.00%
30	14	4	7	3	70.00%	98.00%
TOTAL	395	167	239	110	70.67%	98.37%

Anexo 2: Matriz de Consistencia

Matriz de Consistencia					
Implementación de la ISO/IEC 17799 para la Seguridad de la Información en la Empresa Nuevo Mundo Viajes					
Problemas	**Objetivos**	**Hipotesis**	**Variable**	**Dimensiones**	**Indicador**
General	**General**	**General**			
¿Cuál es el efecto de la ISO/IEC 17799 para la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes?	Determinar el efecto de la ISO/IEC 17799 en la Seguridad de la Información en la empresa Nuevo Mundo Viajes	La ISO/IEC 17799 tiene un efecto significativo en la Seguridad de la Información en la empresa Nuevo Mundo Viajes	ISO/IEC 17799	******	******
Especificos	**Especificos**	**Especificos**	**Variable**	**Dimensiones**	**Indicador**
¿Cuál es el efecto de la ISO/IEC 17799 en la disponibilidad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes?	Determinar efecto de la ISO/IEC 17799 en la disponibilidad de la Seguridad de la Información en la empresa Nuevo Mundo Viajes	La ISO/IEC 17799 tiene un efecto positivo en la disponibilidad de la Seguridad de la Información en la empresa Nuevo Mundo Viajes	Seguridad de la Informacion	Confidencialidad	Numero de accesos no autorizados
¿Cuál es el efecto de la ISO/IEC 17799 en la integridad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes?	Determinar efecto de la ISO/IEC 17799 en la integridad de la Seguridad de la Información en la empresa Nuevo Mundo	La ISO/IEC 17799 tiene un efecto positivo en la Integridad de la Seguridad de la Información en la empresa Nuevo Mundo Viajes		Integridad	Manipulación de Datos
¿Cuál es el efecto de la ISO/IEC 17799 en la confidencialidad de la Gestión de la Seguridad de la Información en la empresa Nuevo Mundo Viajes?	Determinar efecto de la ISO/IEC 17799 en la confidencialidad de la Seguridad de la Información en la empresa Nuevo Mundo Viajes	La ISO/IEC 17799 tiene un efecto positivo en la Confidencialidad de la Seguridad de la Información en la empresa Nuevo Mundo Viajes		Disponibilidad	Tiempo en el cual un sistema esta disponible=(tiempo real transcurrido - suma de tiempo de inactividad) / tiempo total transcurrido

Anexo 3: Formato de solicitud de accesos

expertia

SOLICITUD DE EQUIPOS Y ACCESO AL SISTEMA

APELLIDO PATERNO	APELLIDO MATERNO	NOMBRES
FECHA NACIMIENTO	CARGO	AREA
DIVISION	EMPRESA	DNI
FECHA DE INGRESO	FECHA DE PASE A AREA	PERFIL DE REFERENCIA

SOLICITUD DE EQUIPOS

PC	LAPTOP	TABLET	IPAD	MOVIL BASICO	SMARTPHONE	IPHONE	MODEM	TELEF. ANEXO

ACCESO TELEFÓNICO:

Acceso llamadas locales	Acceso llamadas Internacionales	Acceso Llamadas a Móviles

ACCESO A APLICACIONES:

APLICACIONES		APLICACIONES		APLICACIONES	
ACCESOS SABRE		ACCESO A EMERGENTES		ANVIZ	
ACCESO AMADEUS		ACCESO A CONDORLINK		VIRTUAL ASSIST	

ACCESO KIU		ACCESO A PERÚRAIL		TSIBNET (PERUVIAN)	
ACCESO WORLDSPAN		ACCESO A INCARAIL		ACCESO PAYSISTEM	
ACCESO CORREO		ACCESOS RB			
ACCESO CRM		ACCESO ACD			
ACCESO EXACTUS		ACCESO INTRANET EXPERTIA			
ACCESOS PTA		ACCESO SRV			

ACCESO OFFICE ID GDS SABRE

QP75	QP35	QF05	XX05	HW57	X1A2	QQ05	S0X7	OTRO

ACCESO OFFICE ID GDS AMADEUS

LIMPE31 ZS	**LIMPE23 90**	**LIMPE31 UC**	**LIMPE32 VY**	**LIMPE24 31**	**LIMPE32 PN**	**OTR OS**

OBSERVACIONES:

Anexo 4: Formato de Entrega de equipos Portátiles

expertia	FORMATO DE ENTREGA DE EQUIPO INFORMÁTICO		Código:	TIC-PL-001
			Revisión:	01
	TIPO:	EQUIPO LAPTOP	Fecha:	23/10/2018
			Página:	1 de 3

Por medio del Presente el Sr(a). _____

Correo Electrónico: _____

Recibe la Computadora Portátil con las Siguientes Características:

Tipo de Asignación:			
Marca:			
Modelo:			
Serie:			
Serie de Cargador:			
Accesorios:			

I. **Recomendaciones de Seguridad de los equipos Informáticos.**

1. Mantener los computadores portátiles de propiedad de ExpertisTravel bajo llave o con candado de seguridad. Siempre que el usuario este utilizando su equipo deberá hacerlo con el candado de seguridad puesto, ya sea dentro de las instalaciones de ExpertisTravel o en cualquier otro lugar donde tenga que realizar sus actividades diarias; si tiene que dejar el equipo dentro de estas instalaciones deberá asegurase de dejarlo bajo llave.
2. Nunca separarse del equipo cuando se está movilizando en un vehículo de transporte público.
3. Nunca dejar los equipos sin candado de seguridad en cualquier establecimiento, hotel o vehículo de transporte (sobre todo en viajes largos para este último caso).
4. No dejar los equipos abandonados en los vehículos estacionados en ningún instante. Este motivo además de elevar la probabilidad de robo.
5. Guardar en el domicilio los equipos en un lugar que no sea visible cuando se sale del mismo o con candado en caso la salida sea breve.
6. No caminar por la calle con los equipos y si no hay alternativa, hacer notar que se está atento.
7. Tomar las precauciones necesarias al tomar un taxi y procurar no transitar por zonas peligrosas (tanto en taxi como en vehículo particular).
8. Ante un siniestro se debe realizar la denuncia policial de inmediato, indicando la marca.
9. Si el oficial insiste con alguna otra información, pueden indicar el color de la computadora portátil, el número de serie y el modelo sin ningún error, ya que un error generaría problemas en el reclamo ante la aseguradora.
10. Cualquiera otra indicación que nos de la Compañía de Seguros contratada (Según las coberturas negociadas en la Póliza de Seguro).

11. El equipo no debe ser alterado ni manipulado internamente en Hardware o Software por el usuario o tercero no autorizados.
12. Es muy importante mantener la copia de este documento para cualquier eventualidad que se presente.

II. POLITICAS

1. *Pautas para la Reposición de Equipos Informáticos.*

1.1 En casos de daño del equipo, el costo de la reposición o reparación será asumido el 50 % por la empresa solo el primer incidente, la diferencia deberá ser asumida por el trabajador. El monto a pagar será el cotizado por el servicio técnico.

1.2 En casos de falla del equipo, se procederá con el envío del mismo al servicio técnico del operador con el fin de recibir el reporte correspondiente y determinar si los costos serán cubiertos por la garantía. (para ello el equipo no debe presentar golpes, quiñes, rupturas, rajaduras, derrame de líquido de pantalla, evidencia de residuos líquidos, sólidos, humedad o sulfatación entre otros daños). En caso la garantía no procede por razones atribuibles al uso del equipo, el usuario asumirá el 50% de costo, que será cotizado por el servicio técnico.

1.3 En caso de pérdida o hurto (a.1) del equipo, el costo de la reposición será asumido el 100% por el usuario, esto será aplicado desde el primer incidente. El monto a pagar será cotizado por el operador.

1.4 En caso de robo (a.2) o asalto (a.3) el costo de la reposición será asumido el 100% por la empresa solo para el primer incidente previa evaluación del hecho y siempre que este claramente establecido, para lo cual el usuario debe presentar la denuncia policial no mayor a 2 días laborables indicando la fecha, lugar y las circunstancias detallada en las que ocurrió el hecho.

2. *Seguridad y Control de los Equipos Informáticos*

2.1 El usuario deberá brindar las facilidades del equipo para el control del inventario que se realizan anualmente en la empresa, para ello el usuario deberá mostrar todos los accesorios completos que se le fue asignado.

2.2 La empresa se reserva el derecho de auditar y revisar el equipo asignado. El usuario autoriza expresamente la revisión del equipo, archivos e información que contenga el mismo.

2.3 El equipo no puede ser reasignado por el mismo usuario, es el departamento de Sistemas quien realizara la reasignación del equipo con un acta de asignación de Equipos.

2.4 Si el Colaborador se retira de la empresa, deberá devolver el equipo con los accesorios que se le fue asignado por el área de Sistemas y debe estar en óptimas condiciones, caso contrario asumirá el costo de la reposición.

III. ANEXOS

- (a.1) Hurto: delito que consiste en tomar o retener bienes contra la voluntad de su dueño. En este caso no existe intimidación, violencia o fuerza. El infractor aprovecha una oportunidad y se apodera de un bien.

- (a.2) Robo: apropiación de algo ajeno con violencia, fuerza o intimidación, donde el infractor se apodera de las cosas con ánimo de lucro, empleando fuerza sobre las cosas o las personas.

- (a.3) Asalto: delito que se da cuando el delincuente se apodera de algo por la fuerza, con armas blancas o de fuego, intimidación y generalmente por sorpresa.

Se Firma el presente a la recepción del Equipo, en Señal de conformidad con lo Dispuesto.

martes, 23 de octubre de 2018

Sr(a).....
FIRMA DE USUARIO

.....
Plataformas TI y Soporte
DEPARTAMENTO DE SISTEMAS

Anexo 5: Formato de Entrega de equipos desktop

expertia	FORMATO DE ENTREGA DE EQUIPO INFORMÁTICO		Código:	TIC-PL-001
			Revisión:	01
	TIPO:	EQUIPO DESKTOP	Fecha:	05/11/2018
			Página:	1 de 3

Por medio del Presente el Sr(a). _____

Correo Electrónico: _____

Recibe la Computadora Portátil con las Siguientes Características:

Tipo de Asignación:	Equipo Nuevo
Marca:	
Modelo:	
Serie:	
Serie de Cargador:	

Teclado		Serie:
Mouse		Serie:

I. **Recomendaciones para el Cuidado y Seguridad de los equipos Informáticos.**

1. No llevar consigo el equipo de cómputo a ninguna parte, solo el equipo de soporte es el autorizado para trasladar los equipos de cómputo dentro de la oficina y fuera de ella.
2. En el caso de encontrarse ubicado fuera de oficina comunicar a las personas necesarias para informar de los equipos que está dejando bajo cuidado.
3. Mantener fuera del alcance de los líquidos como café, gaseosas, etc.
4. El equipo no debe ser alterado ni manipulado internamente en Hardware o Software por el usuario o tercero no autorizados.
5. Si sales de Vacaciones y no vas a usar el equipo es mejor Apagarlo completamente y hazlo también los fines de semana al salir de oficina.
6. No comer sobre el teclado, si se ensucia no podría funcionar correctamente.
7. Evita pegar sticker u objetos que pueden dañar o deteriorar el Monitor ya que esto podría interrumpirle garantía.
8. Si ocurriera alguna perdida o desaparición informar inmediatamente al área de Soporte Técnico.
9. Es muy importante mantener la copia de este documento para cualquier eventualidad que se presente.

II. POLITICAS

1. *Pautas para la Reposición de Equipos Informáticos.*

   1.1 En casos de daño del equipo, el costo de la reposición o reparación será asumido al 50 % por la empresa solo el primer incidente, la diferencia deberá ser asumida por el trabajador. El monto a pagar será el cotizado por el servicio técnico.

   1.2 En casos de falla del equipo, se procederá con el envío del mismo al servicio técnico del operador con el fin de recibir el reporte correspondiente y determinar si los costos serán cubiertos por la garantía. (para ello el equipo no debe presentar golpes, quiñes, rupturas, rejaduras, derrame de líquido de pantalla, evidencia de residuos líquidos, sólidos, humedad o sulfatación entre otros daños). En caso la garantía no procede por razones atribuibles al uso del equipo, el usuario asumirá el 50% de costo, que será cotizado por el servicio técnico.

   1.3 En caso de pérdida o hurto (a.1) del equipo, el costo de la reposición será asumido al 100% por el usuario, esto será aplicado desde el primer incidente. El monto a pagar será cotizado por el operador.

   1.4 En caso de robo (a.2) o asalto (a.3) el costo de la reposición será asumido al 100% por la empresa solo para el primer incidente previa evaluación del hecho y siempre que este claramente establecido, para lo cual el usuario debe presentar la denuncia policial no mayor a 2 días laborables indicando la fecha, lugar y las circunstancias detallada en las que ocurrió el hecho.

2. *Seguridad y Control de los Equipos Informáticos*

   2.1 El usuario deberá brindar las facilidades del equipo para el control del inventario que se realizan anualmente en la empresa, para ello el usuario deberá mostrar todos los accesorios completos que se le fue asignado.

   2.2 La empresa se reserva el derecho de auditar y revisar el equipo asignado. El usuario autoriza expresamente la revisión del equipo, archivos e información que contenga el mismo.

   2.3 El equipo no puede ser reasignado por el mismo usuario, es el departamento de Sistemas quien realizara la reasignación del equipo con un acta de asignación de Equipos.

2.4 Si el Colaborador se retira de la empresa, deberá devolver el equipo con los accesorios que se le fue asignado por el área de Sistemas y debe estar en óptimas condiciones, caso contrario asumirá el costo de la reposición.

III. ANEXOS

- (a.1) **Hurto:** delito que consiste en tomar o retener bienes contra la voluntad de su dueño. En este caso no existe intimidación, violencia o fuerza. El infractor aprovecha una oportunidad y se apodera de un bien.

- (a.2) **Robo:** apropiación de algo ajeno con violencia, fuerza o intimidación, donde el infractor se apodera de las cosas con ánimo de lucro, empleando fuerza sobre las cosas o las personas.

- (a.3) **Asalto:** delito que se da cuando el delincuente se apodera de algo por la fuerza, con armas blancas o de fuego, intimidación y generalmente por sorpresa.

Se Firma el presente a la recepción del Equipo, en Señal de conformidad con lo Dispuesto.

lunes, 05 de noviembre de 2018

Sr(a).....
FIRMA DE USUARIO

.....
Plataformas TI y Soporte
DEPARTAMENTO DE SISTEMAS

Anexo 6: Políticas de estandarización de AD

ESTANDARIZACIÓN DIRECTORIO ACTIVO EXPERTIA TRAVEL

CONTENIDO:

I. INTRODUCCIÓN:

El presente documento detalla la estandarización de todos los elementos que constituyen el sistema de Directorio Activo, la administración y el buen uso de los objetos que en este sistema residen así como la incorporación de las estaciones de trabajo al dominio.

II. ESTÁNDARES DE NOMBRES

El objetivo principal de establecer estándares de nombres es mantener la uniformidad en la red y en los elementos que conforman el directorio. Estos estándares dan a cada organización características para seguir un orden y control adecuado de los recursos pero a nivel general se definen para poder tener la capacidad de determinar con solo ver el nombre en el directorio saber la ubicación y la función que representa.

Los estándares de nombres a utilizar tendrán entradas en el servicio DNS Interno y deben restringirse administrativamente y lograr así la máxima interoperabilidad y seguridad.

Notas Importantes:

- Los estándares aquí definidos aplican sobre recursos propiedad del grupo Expertia Travel o aquellos que van a permanecer en la organización durante un tiempo considerable.
- Se recomienda no usar el subrayado (_) para la creación de nombres ya que este carácter no es parte de los estándares definidos para nombres DNS.

2.1.Servidores:

La definición de un adecuado nombre para un servidor apoya las labores administrativas, esto conlleva una rápida identificación y control del recurso ya sea en una terminal o por acceso remoto. Así el administrador del servidor podrá determinar fácilmente el servicio función o localización.

La recomendación establecida es definida por el siguiente formato: XXYYYZZ##. A continuación se explica la confirmación de este nombre:

- La longitud máxima de un nombre de servidor debe ser de 10 caracteres.
- XX: nemotécnico de la empresa.
- YYY: Letras que definen el servicio, los códigos utilizados pueden revisarse en el Anexo de tablas N° 1.
- ZZZ: Letras que corresponden al código IATA de la ciudad más cercana donde se encuentra el servidor. Los códigos pueden revisarse en la página web: http://www.iata.org/publications/Pages/code-search.aspx
- ##: Dígitos consecutivos cuando se tienen más de un servidor con las mismas funciones.

Aspectos a tener en cuenta por el administrador

Se debe mover el servidor a la Unidad Organizacional correspondiente según la estructura del directorio Activo. Para tal efecto se ha definido una OU llamada Servidores la cual se ha segmentado según la función en la red.

Ejemplo:

ETDCSLIM01:

Dónde:
ET = Expertia Travel
DCS = Domain Controler Server
LIM = Lima
01 = Correlativo

2.2.Equipos de Comunicación[1]:

[1] Si bien los equipos de comunicación no se administran por Directorio Activo, se establece estandarización para su tratamiento por servicio DNS en descripción de nombres.

Dentro de los equipos de comunicación se contemplan Switches, Routers, Access Point, y demás dispositivos que trabajen con funciones de red de distribución de paquetes capa 2 o capa3.

La recomendación establecida es definida por el siguiente formato: XXYYYZZ##. A continuación se explica la confirmación de este nombre:

- La longitud máxima de un nombre de servidor debe ser de 11 caracteres.
- XXX: Letras que definen campo de acción dentro de la red:
    - SWC: Switch de Core
    - SWA: Switch de Acceso
    - ACP: Punto de Acceso
    - ROU: Router
- YYY: Letras que definen la ubicación dentro del edificio (P01 = Piso 1)
- ZZZ: Letras que corresponden al código IATA de la ciudad más cercana donde se encuentra el servidor. Los códigos pueden revisarse en la página web http://www.iata.org/publications/Pages/code-search.aspx
- ##: Dígitos consecutivos cuando se tienen más de un equipo con las mismas funciones.

Ejemplo:

SWCP01LIM01: Switch de core N° 1 ubicado en Lima.
SWAP04LIM02: Switch de Acceso N° 2 ubicado en el Piso 4.

2.3.Estaciones de Trabajo

Con la definición de estándar de estaciones de trabajo se pretende identificar aspectos relacionados a la empresa, ubicación geográfica, nombre del usuario al que está asignada la computadora o laptop, ciudad a la cual pertenece y el tipo de maquina (Laptop, Desktop).

La recomendación para este tipo de dispositivos es definir el nombre de la maquina como el "hostname" TCP/IP, el cual si es menor de 15 caracteres es también asignado como nombre NetBIOS, en caso sea mayor a los 15 caracteres este es truncado hasta el 11vo carácter.

De esta manera, para las estaciones se recomienda definir un nombre con la siguiente estructura:

XXYYY-ZZZZZZZZ, A continuación se explica los detalles de la conformación de este nombre:

- Se utilizará una estructura de nombre de hostname de máximo 15 caracteres de longitud que serán truncados.
- XX: letras que corresponde a la abreviación de la empresa (ver anexo 2 para tabla de mnemotecnicos).
- YYY: Letras que corresponden al código IATA de la ciudad más cercana donde se encuentra el equipo. Los códigos IATA pueden revisarse en la página web en la siguiente URL: http://www.iata.org/publications/Pages/code-search.aspx.
- '-' utilizaremos un guión para separar el país y ciudad del nombre de usuario o área.
- ZZZZZZZZ es el nombre de usuarios de la persona que tiene asignado el cual corresponde al nombre de la cuenta en el dominio este debe ser máximo de 8 caracteres o si es un puesto muy rotativo se puede usar un mnemotécnico de área seguido de un numero correlativo que no pasen los 8 caracteres.

Ejemplo

CTLIM-RPEREZ => Estación de trabajo, perteneciente al usuario "rperez" en Lima – Perú, perteneciente a Condor Travel.

Debe tener en cuenta:

- Se debe Mover a la unidad organizacional correspondiente según la estructura del directorio activo. Existe una unidad organizacional llamada Estaciones el cual esta segmentada por país y después por área de trabajo.
- Si un usuario tiene varias máquinas se agrega un digito consecutivo al final del nombre.
- Para equipos comunes donde son usados por varios usuarios o si el puesto es muy rotativo es recomendable establecer en lugar del nombre del usuario el nombre del área considerando que si son varios equipos usar números correlativos. Ejemplo: NMLIM-MARKET01, NMLIM-MARKET02, tenemos 02 equipos comunes del área de Marketing ubicados en Lima Perú.

2.4.Impresoras

Con la definición de un estándar en los nombres para las colas de impresión se debería buscar identificar aspectos relacionados con el país, la función, la locación, la descripción y el tipo de impresora.

De esta manera los estándares que regirán la construcción de colas de impresión será:

XXXYY-ZZZZZZZZ#, A continuación, se explica los detalles de la conformación de este nombre:

- La longitud máxima de los nombres de las máquinas deberá ser de máximo de 15 caracteres.
- XXX Corresponde a los 3 caracteres nemotécnicos de la ciudad según código IATA.
- YY que corresponde al código ISO 3166 del país en la cual está ubicada la impresora.
- '-' utilizaremos un guion para separar el nombre de la compañía, país y la función de la impresora.
- ZZZZZZZZ es la función que va a desempeñar la impresora, Ej.: nomina, tesorería, marketing, sistemas, etc. (máximo 8 caracteres).
- # Identifica un consecutivo que se manejará para los dispositivos físicos.
- En el campo descripción se debe agregar la descripción de la ciudad en la cual está la impresora; y la identificación de la tecnología de impresión del dispositivo de impresión. Sus valores podrán ser:
    - LM Láser Monocromática
    - LC Láser Color
    - IM Inyección Monocromática
    - IC Inyección color
    - MP Matriz de puntos

2.5.Cuentas de usuarios

La longitud máxima de los nombres de los usuarios es de 8 caracteres y su creación se regirá por las siguientes reglas de creación de cuentas, se toma como ejemplo el usuario Ronald Jesús Pérez León:

Regla No. 1.

Inicial del primer nombre + Apellido Paterno que no sobre pase los 8 caracteres en total. Si el nombre del usuario ya existe, aplique la regla número 2.

Ejemplo:

Tomando como ejemplo el usuario Ronald Pérez León

Cuenta de usuario seria: rperez

Regla No. 2.

Inicial del primer nombre + Apellido Paterno + Inicial Apellido Materno, que no sobre pase los 8 caracteres en total. Si el nombre del usuario ya existe, aplique la regla número 3.

Ejemplo: ya existe rperez, podemos utilizar rperezl

Regla No. 3.

Inicial del primer nombre+ inicial del segundo nombre+Apellido Paterno.

Ejemplo: rjperez

Debe tener en cuenta:

El tamaño de las cuentas podrá ser menor a 8 caracteres en caso de que el tamaño de las cuentas no llegue a 8, después de aplicarse las reglas de creación.

Se debe colocar los nombres completos en los campos de solicitados en el momento de crear la cuenta.

Las reglas anteriormente descritas no son estrictamente establecidas según el orden indicado, pero es una recomendación para poder establecer el nombre de usuario.

III. CATEGORIZACIÓN DE OUs

Es indispensable para llevar un correto control de la ubicación de los objetos en el directorio Activo seguir las siguientes pautas luego de crearlos y luego de haber llenado los campos necesarios:

3.1.Mover estaciones y servidores a la ou correspondiente

Para mantener un orden en el directorio activo se debe hacer un movimiento de los equipos que ingresan en el dominio de Nuevo Mundo. Cuando estos ingresan, automáticamente se asocia en la unidad organizacional llamada Computers. Una vez identificado y llenos el campo mencionado anteriormente, se procede a mover el objeto a la unidad organizacional que le corresponde; para ello existe una unidad organizacional llamada Estaciones el cual esta segmentada por país y después por área de trabajo o rol que desempeña el usuario final.

Nota: los equipos que se encuentre en la unidad organizacional "Computer" se desactivaran y se moverán a una unidad organizacional llamada "Estaciones QRT", que es una OU creada especialmente para colocar equipos en Quarentena, es decir equipos que por algún motivo se solicita desactivar por medida se seguridad o labores administrativas.

3.2.Mover usuarios a la OU correspondiente

Para mantener un orden de las cuentas de usuario en el directorio activo se debe hacer un movimiento de las cuentas de usuario una vez que estas han sido creadas o cuando los usuarios han sido cambiados de área. Cuando se crea una cuenta de usuario esta automáticamente se asocia en la unidad organizacional llamada USERS. Una vez identificado y llenos los campos correspondientes, se procede a mover el objeto a la unidad organizacional que le corresponde; para ello existe una unidad organizacional creada para cada Área a la que corresponde.

Nota: los usuarios que se encuentre en la unidad organizacional "USERS" o que tengan más de 60 días de inactividad se desactivarán y se moverán a una unidad organizacional llamada "Usuarios QRT", que es una OU creada especialmente para colocar usuarios en Quarentena, es decir cuentas de usuario que por algún motivo se solicita desactivar por medida se seguridad o labores administrativas.

ANEXO 01: Tabla mnemotécnicos de servicios

Nemotécnico	Función
DCS	Controladores dominio
FSS	File Server
WEB	Intranet servidores Web
MXS	Correo
FWP	Firewall
ANT	Antivirus
TSE	Servidores Terminal Server
VPN	VPN Server
TMP	Temporal, Prueba o Demos
MON	Monitoreo, Administración de red (Nagios, Cacti, Zabbix, etc)
DBS	Servidor de Base de Datos
SRV	Servidor Genérico o que cumple varias funciones
WSA	Servidor de Actualizaciones

ANEXO02: Tabla mnemotécnicos de Empresas

Nemotécnico	Función
ET	Expertia Travel
NM	Nuevo Mundo
DM	Destinos Mundiales
TA	Travel Ace
AG	AG Corp
CT	Condor Travel
IA	Interagencias

Anexo 7: Formato para baja de activos

Departamento de Tecnologia
Oficina de Plataforma y Soporte TI

Formato para baja computador de activos fijos

Fecha	**11 de diciembre de 2018**	**No.**	

Usuario	
Responsable actual	
Oficina	
Oficina	
Dependencia	Oficina de Plataforma y Soporte TI

Soporte Tecnico	
Nombre y Apellido	
Firma soporte tecnico	

Información básica del activo fijo									
ITEM	**Descripción del activo**					**No. Inventario (Computer Id)**		**No. Serie**	**No. Mac o IP**
	"Modelo del Equipo"								
	Información del equipo de computo								
	Fragmento			***Entrego***		***Funciona***		***Observaciones***	
	Monitor			*SI*	*NO*	*SI*	*NO*		
	Teclado			*SI*	*NO*	*SI*	*NO*		
	Mouse			*SI*	*NO*	*SI*	*NO*		
	Disco Duro	*Capacidad GB*		*SI*	*NO*	*SI*	*NO*		
	Memoria	*Capacidad RAM*		*SI*	*NO*	*SI*	*NO*		
	CPU								

	Información del equipo de computo						
	Procesador			*SI*	*NO*	*SI*	*NO*
	Board			*SI*	*NO*	*SI*	*NO*
	Lector Optico	*CD*		*DVD*		*SI*	*NO*	*SI*	*NO*
	Fuente			*SI*	*NO*	*SI*	*NO*
	Tarjeta de Red			*SI*	*NO*	*SI*	*NO*
	Tarjeta de Video			*SI*	*NO*	*SI*	*NO*
	Tarjeta de Sonido			*SI*	*NO*	*SI*	*NO*
	Impresora						
	Información del equipo de computo						
	Mutifuncional			*SI*	*NO*	*SI*	*NO*
	Colores			*SI*	*NO*	*SI*	*NO*
	Tarjeta de Red			*SI*	*NO*	*SI*	*NO*

Total Activos

Observaciones

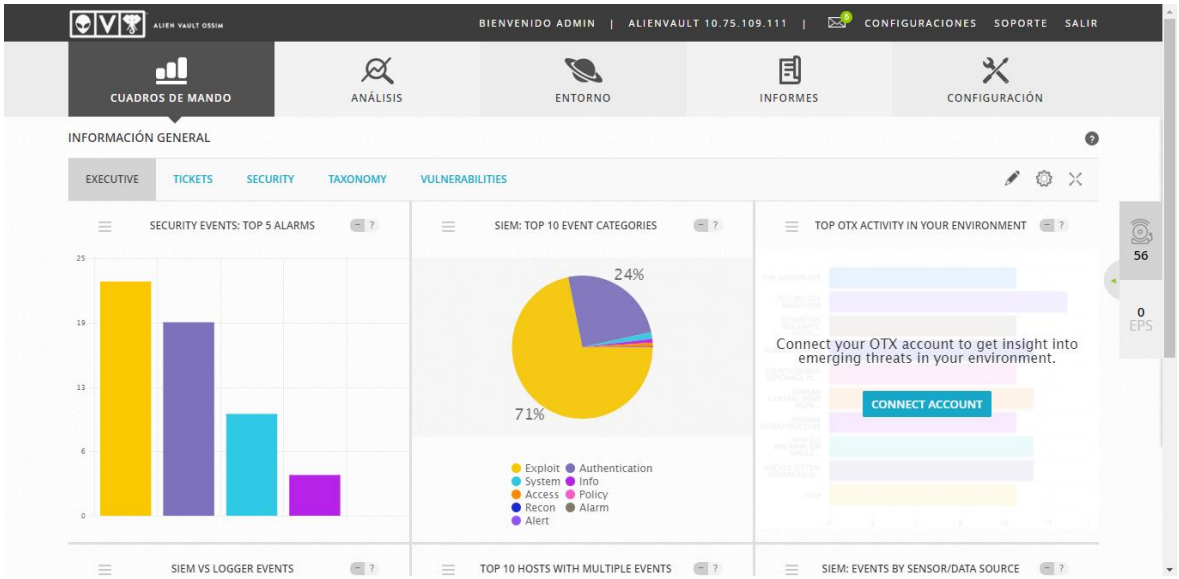
Firmas de Usuario	**Firma de Coordinador de Soporte TI**
Firma y sello de Jefe de Plataforma y soporte TI	**Firma y sello de Contabilidad**

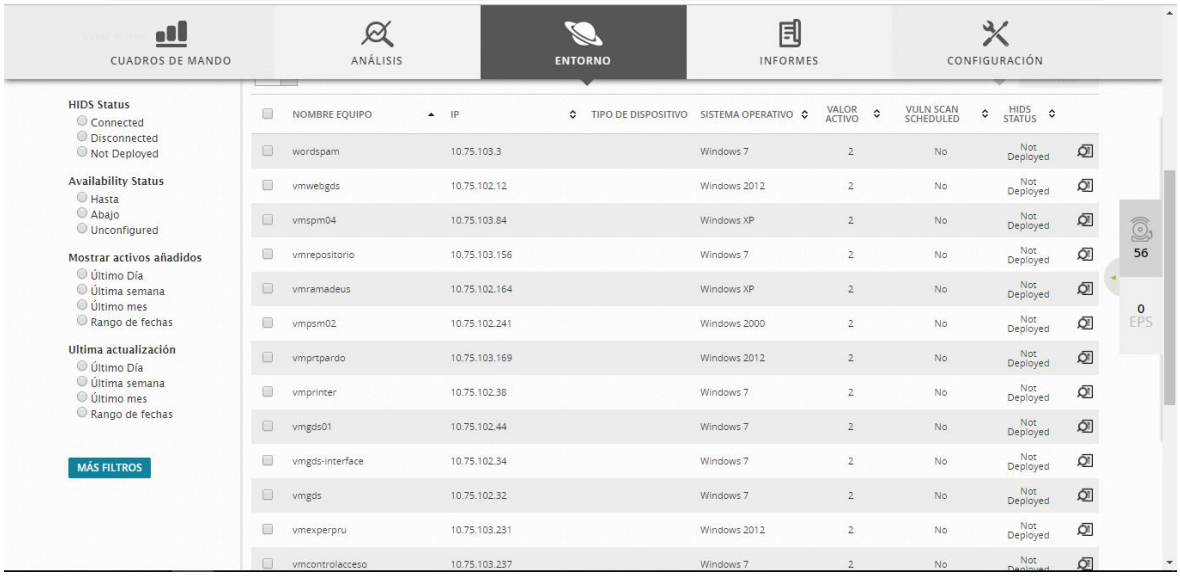
COPIAS

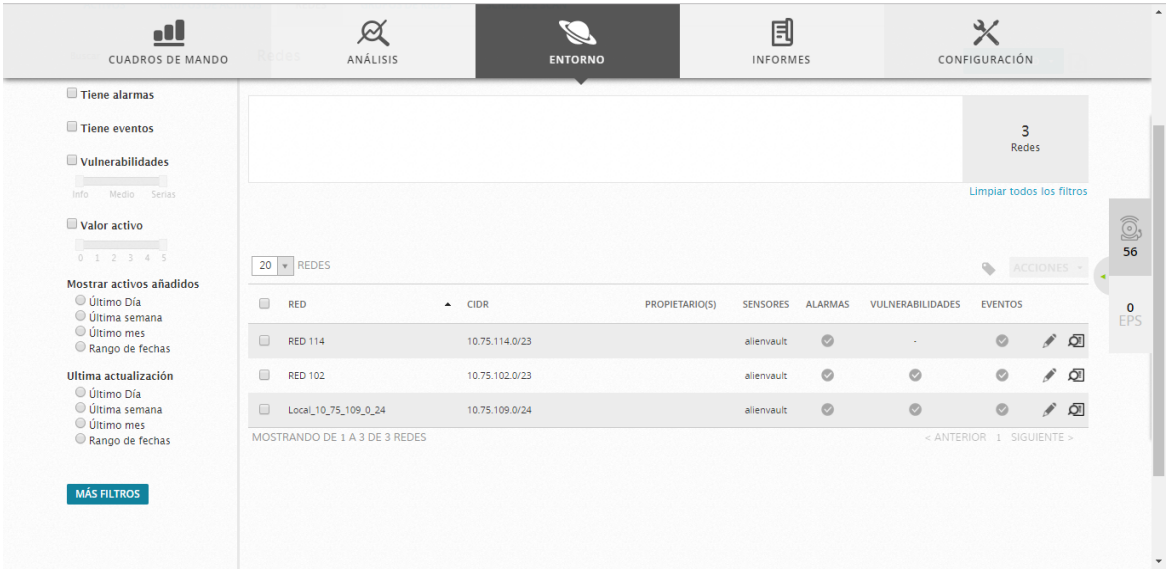
Original: ***Oficina de Plataforma y Soporte TI***

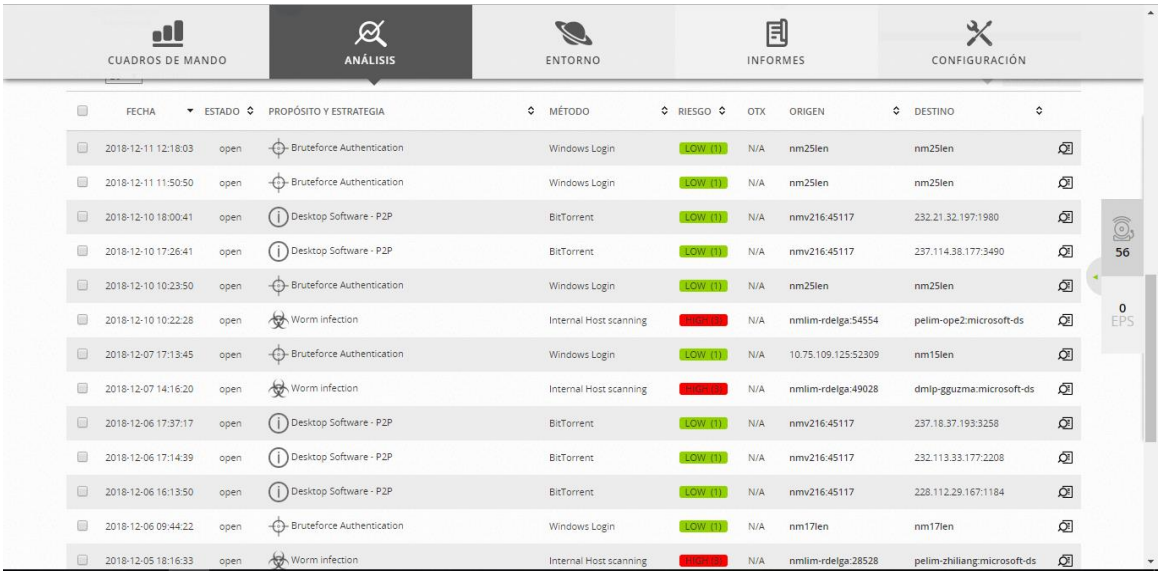
Copia 1: ***Oficina de Contabilidad***

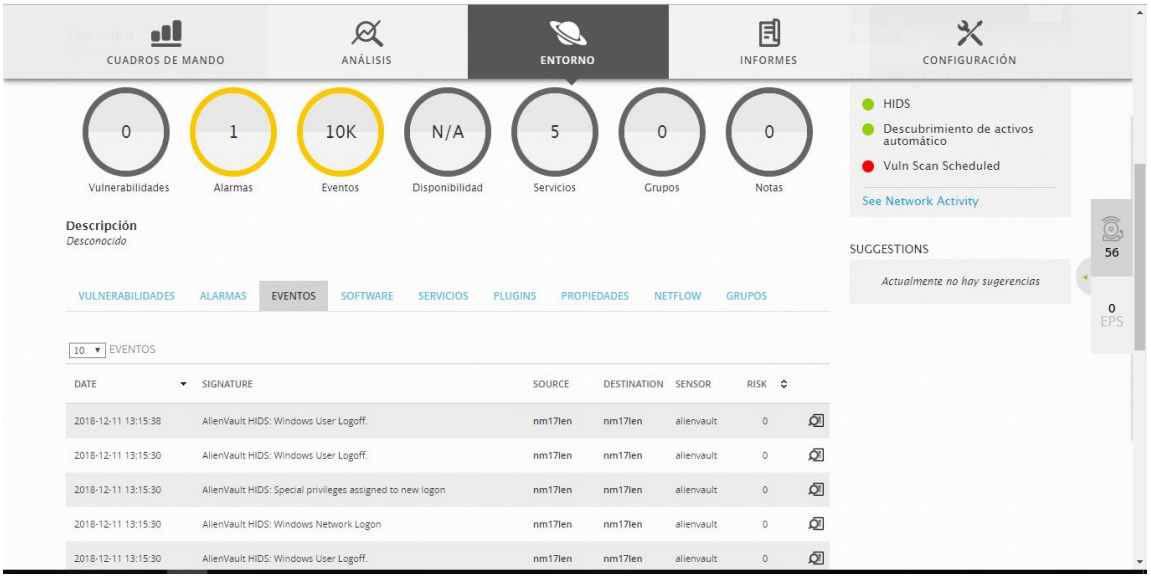
Anexo 7: Sistema para la seguridad de la Información






CUADROS DE MANDO
ANÁLISIS
ENTORNO
INFORMES
CONFIGURACIÓN
Tiene alarmas
Tiene eventos
Vulnerabilidades
Info Medio Serias
Valor activo
0 1 2 3 4 5
Mostrar activos añadidos
Último Día
Última semana
Último mes
Rango de fechas
Ultima actualización
Último Día
Última semana
Último mes
Rango de fechas
MÁS FILTROS
3
Redes
Limpiar todos los filtros
20 REDES
ACCIONES
RED
CIDR
PROPIETARIO(S)
SENSORES
ALARMAS
VULNERABILIDADES
EVENTOS
RED 114
10.75.114.0/23
alienvault
RED 102
10.75.102.0/23
alienvault
Local_10_75_109_0_24
10.75.109.0/24
alienvault
MOSTRANDO DE 1 A 3 DE 3 REDES
< ANTERIOR 1 SIGUIENTE >
56
0
EPS


CUADROS DE MANDO
ANÁLISIS
ENTORNO
INFORMES
CONFIGURACIÓN
FECHA
ESTADO
PROPÓSITO Y ESTRATEGIA
MÉTODO
RIESGO
OTX
ORIGEN
DESTINO
2018-12-11 12:18:03 open Bruteforce Authentication Windows Login LOW (1) N/A nm25len nm25len
2018-12-11 11:50:50 open Bruteforce Authentication Windows Login LOW (1) N/A nm25len nm25len
2018-12-10 18:00:41 open Desktop Software - P2P BitTorrent LOW (1) N/A nmv216:45117 232.21.32.197:1980
2018-12-10 17:26:41 open Desktop Software - P2P BitTorrent LOW (1) N/A nmv216:45117 237.114.38.177:3490
2018-12-10 10:23:50 open Bruteforce Authentication Windows Login LOW (1) N/A nm25len nm25len
2018-12-10 10:22:28 open Worm infection Internal Host scanning N/A nmlim-rdelga:54554 pelim-ope2:microsoft-ds
2018-12-07 17:13:45 open Bruteforce Authentication Windows Login LOW (1) N/A 10.75.109.125:52309 nm15len
2018-12-07 14:16:20 open Worm infection Internal Host scanning N/A nmlim-rdelga:49028 dmlp-gguzma:microsoft-ds
2018-12-06 17:37:17 open Desktop Software - P2P BitTorrent LOW (1) N/A nmv216:45117 237.18.37.193:3258
2018-12-06 17:14:39 open Desktop Software - P2P BitTorrent LOW (1) N/A nmv216:45117 232.113.33.177:2208
2018-12-06 16:13:50 open Desktop Software - P2P BitTorrent LOW (1) N/A nmv216:45117 228.112.29.167:1184
2018-12-06 09:44:22 open Bruteforce Authentication Windows Login LOW (1) N/A nm17len nm17len
2018-12-05 18:16:33 open Worm infection Internal Host scanning N/A nmlim-rdelga:28528 pelim-zhiliang:microsoft-ds
56
0
EPS


CUADROS DE MANDO
ANÁLISIS
ENTORNO
INFORMES
CONFIGURACIÓN
0 Vulnerabilidades
1 Alarmas
10K Eventos
N/A Disponibilidad
5 Servicios
0 Grupos
0 Notas
HIDS
Descubrimiento de activos automático
Vuln Scan Scheduled
See Network Activity
SUGGESTIONS
Actualmente no hay sugerencias
Descripción
Desconocido
VULNERABILIDADES
ALARMAS
EVENTOS
SOFTWARE
SERVICIOS
PLUGINS
PROPIEDADES
NETFLOW
GRUPOS
10 EVENTOS
DATE
SIGNATURE
SOURCE
DESTINATION
SENSOR
RISK
2018-12-11 13:15:38 AlienVault HIDS: Windows User Logoff. nm17len nm17len alienvault 0
2018-12-11 13:15:30 AlienVault HIDS: Windows User Logoff. nm17len nm17len alienvault 0
2018-12-11 13:15:30 AlienVault HIDS: Special privileges assigned to new logon nm17len nm17len alienvault 0
2018-12-11 13:15:30 AlienVault HIDS: Windows Network Logon nm17len nm17len alienvault 0
2018-12-11 13:15:30 AlienVault HIDS: Windows User Logoff. nm17len nm17len alienvault 0
56
0
EPS