UNIVERSIDAD DE LAMBAYEQUE

FACULTAD DE CIENCIAS DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

TESIS

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 cómputo – Universidad de Lambayeque

PRESENTADA PARA OBTAR EL TÍTULO DE INGENIERO DE SISTEMAS

AUTORES

FRANKZ OLIVOS GUERRA

ERICK WILLIAM GUEVARA SALDAÑA

Chiclayo, *Diciembre del 2017*

FIRMA DEL ASESOR Y JURADO DE TESIS:

_____

Ing. Francisco Richard Herrera Piscoya

ASESOR

_____ _____

Mg. Ernesto Karlo Celi Arévalo

PRESIDENTE

Ing. Vladimir Sabino Gonzales Mechán

SECRETARIO

_____

Ing. Nilton César German REYES

VOCAL

DEDICATORIA

Dedicado a mi madre y a mis tías que siempre me han sacado adelante a pesar de las dificultades siempre lucharon conmigo y me animaron a seguir adelante y a mis hermanos para que vean en mi un ejemplo de superación.

A mis profesores que siempre me impulsaron a seguir cuando creí tener todo perdido siempre su ayuda fue indispensable para lograr lo que ahora soy.

Dedicado a mi hija que hoy no lo entiende pero cuando lo haga sabrá que siempre luché por ella; junto a mi esposa que nunca me abandonó y me acompañó en este duro camino.

Dedicado a mí novia que siempre confío en mí y siempre tuve su apoyo incondicional en todo momento

AGRADECIMIENTO

Quiero agradecer a todos mis maestros ya que ellos me enseñaron valorar los estudios y a superarme cada día, también agradezco a mi compañero de tesis porque con él nos ayudamos a realizar y terminar nuestra tesis para obtener el grado académico de Ingeniero de Sistemas.

Y agradezco a Dios por darme la salud que tengo, por tener una cabeza con la que puedo pensar muy bien y además un cuerpo sano y una mente de bien.

Estoy seguro que mis metas planteadas darán fruto en el futuro y por ende me debo esforzar cada día para ser mejor en el ámbito profesional y en todo lugar sin olvidar el respeto que engrandece a la persona.

INDICE

INDICE DE GRÁFICOS

INFORMACIÓN GENERAL

TÍTULO DEL PROYECTO DE INVESTIGACIÓN

Formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma peruana NTP-ISO/IEC 17799 para la mejora de la gestión en la Oficina Central de Cómputo – Universidad de Lambayeque.

AUTORES

Apellidos y Nombres : Olivos Guerra, Frankz

Apellidos y Nombres : Guevara Saldaña, Erick William

Coordinador.

Apellidos y Nombres : Castillo Zumaran, Segundo José

TIPO DE INVESTIGACIÓN

Por el fin que persigue : Aplicativa
Por el nivel de alcance : Correlacional
Por el diseño de investigación : Pre-Experimental

LÍNEA DE INVESTIGACIÓN.

Tecnologías de la Información

LOCALIDAD E INSTITUCIÓN DONDE DESARROLLARÁ EL PROYECTO

Oficina de Centro De Cómputo - Universidad de Lambayeque.
Dirección: Tacna 065 – Chiclayo.

DURACIÓN DEL PROYECTO:

Periodo que dura el proyecto: 14 meses
Fecha de inicio: Octubre del 2016.

FECHA DE PRESENTACIÓN:

Chiclayo, Diciembre del 2017

RESUMEN

La presente investigación titulada Formulación de Políticas de control de accesos y seguridad física y del entorno basado en la norma Peruana NTP-ISO/IEC 17799 para mejorar la gestión en la oficina central de computo – Universidad de Lambayeque.

En la actualidad, muchas empresas que están o desean incursionar en el ámbito educativo, tienen problemas para resguardar la seguridad de su información; en consecuencia esta corre riesgos al igual que sus activos.

El propósito de este trabajo se centró en la Formulación de Políticas de Seguridad Física y Control de accesos, bajo una metodología de análisis y evaluación de riesgos desarrollada y diseñada por los autores de este trabajo; también se usó la norma peruana NTP-ISO/IEC 17799.

La problemática de la Oficina Central de Computo de la Universidad de Lambayeque – UDL es no utilizar al menos un código de buenas prácticas que le permita asegurar los principios fundamentales y básicos de la información, por lo tanto carece de políticas de seguridad de la información.

Es por ello, partiendo de esa necesidad es que se formula políticas de control de acceso y seguridad física y del entorno, para mejorar la gestión en la oficina central de Computo (OCC).

El Impacto que resulta de la investigación es que la universidad como entidad formación profesional estará con los estándares de seguridad de la información, lo que le permitirá su continuidad.

El resultado de la investigación es que nuestra propuesta existe un 53% de la formulación de políticas basado en la NTP-ISO/IEC 17799, permitirá mejorar el grado de satisfacción en la gestión de la seguridad de la información en la OCC de la UDL.

Palabras claves:

Seguridad Física, Control de accesos, Políticas de seguridad de la información, NTP ISO/IEC 17799.

ABSTRACT

This research entitled Formulation of access control policies and physical and environmental security based on the Peruvian standard NTP-ISO / IEC 17799 to improve management at the central computer office - University of Lambayeque.

Currently, many companies that are or want to venture into the educational field, have problems to safeguard the security of their information; consequently, it runs risks as well as its assets.

The purpose of this work was focused on the Formulation of Physical Security Policies and Access Control, under a risk assessment and analysis methodology developed and designed by the authors of this work; The Peruvian standard NTP-ISO / IEC 17799 was also used.

The problem of the Central Office of Computation of the University of Lambayeque - UDL is not to use at least a code of good practices that allows it to assure the fundamental and basic principles of the information, therefore it lacks information security policies.

That is why, based on this need, it is formulated policies for access control and physical security and the environment, to improve management in the central office of Computo (OCC).

The impact that results from the research is that the university as a professional training entity will be with the standards of information security, which will allow its continuity.

The result of the research is that our proposal exists 53% of the formulation of policies based on the NTP-ISO / IEC 17799, will improve the degree of satisfaction in the management of information security in the OCC of the UDL.

Keywords:

Physical Security, Access control, Information security policies, NTP ISO / IEC 17799.

I. INTRODUCCIÓN

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

Las organizaciones públicas y privadas día a día generan conocimientos, datos, reportes, actas y material de diferente índole de suma importancia para ellas, lo cual representa toda la información que requieren para su funcionalidad. Esta información en la mayoría de los casos, es almacenada en diferentes medios tanto físicos como electrónicos, además es puesta a disposición del personal que requiere hacer uso de esta información para toma de decisiones, realización de planes, reportes, inventarios, entre otros.

Las tecnologías de la información (TI) se convierten entonces, en un elemento clave para que las organizaciones modernas puedan dar soporte a la gestión de su información, generando a través de ellas valor a sus servicios, por ende, en una herramienta estratégica que les permite generar ventaja competitiva. Las TI ofrecen la oportunidad de estar más cerca, más enfocado y de responder con mayor rapidez a los clientes, y puede redefinir tanto la eficacia como la eficiencia de las operaciones. Sin embargo, conforme crece la oportunidad, también aumenta el riesgo. La administración eficaz de riesgos de TI le ayuda a mejorar la ventaja competitiva de sus operaciones en la materia al hacer que estas sean más rentables y al reducir los riesgos relacionados con el funcionamiento de sus sistemas (Mancera, 2011).

Las TI y los sistemas informáticos (SI) en particular se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones; también ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios los cuales se están volviendo cada vez más comunes, ambiciosos y sofisticados (Wenceslao, Vasquez Montenegro, & De la Cruz Guerrero, 2008).

La dependencia a los SI requiere dotar de seguridad a los mismos para preservar la calidad de los servicios y velar por la eficacia y eficiencia de los procesos de negocio y el valor de sus activos. Ya no es suficiente con establecer controles en forma aislada ni ad hoc, tampoco es suficiente actuar de modo meramente reactivo y defensivo, se requiere de un sistema de gestión de seguridad de la información (SGSI) y un accionar proactivo (Pallas, 2009).

Por lo tanto, es necesario gestionar la seguridad de la información como un proceso continúo en el tiempo y evitar así fallos de seguridad en los sistemas que utilice la institución.

Según Poveda (s/a) un fallo de seguridad es cualquier incidente que la compromete, es decir que pone en peligro cualquiera de los parámetros con los que se valora la seguridad: la confidencialidad, la disponibilidad o la integridad de la información. Es difícil hacerse una idea del reto que presenta evitar que sucedan cosas como:

a) Fallos en las comunicaciones.

b) Fallos en el suministro eléctrico.

c) Fallos humanos de usuarios internos, usuarios externos, administradores, programadores, etc.

d) Fallos en los sistemas de información: redes, aplicaciones, equipos, etc.

e) Virus informáticos, gusanos, troyanos, etc. que inundan la red.

f) Accesos no autorizados a los sistemas o la información.

g) Incumplimiento de una ley o un reglamento.

Es común observar que las instituciones van parcheando los agujeros de seguridad con medidas puntuales y descoordinadas, las cuales no son controladas de manera planificada y por consiguiente el resultado será el mismo, ya que igual se seguirá manteniendo altos niveles de riesgo frente a las amenazas.

Todos estos incidentes que amenazan la seguridad de la información requieren, cada día más, de sistemas de gestión acordes con el valor de la propia información y de los sistemas informáticos que los tratan. Las directrices, procedimientos y controles de seguridad que se utilizan para gestionar esta seguridad es lo que conocemos por Sistema de Gestión de Seguridad de la Información o SGSI (Proveda, s/a).

La adopción de un SGSI debe ser de una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.

Un SGSI establece un completo plan de acciones que ayudará a su empresa a solucionar los problemas de seguridad técnicos, organizativos y legislativos mediante el análisis de riesgos, mejorando y manteniendo la seguridad de la información empresarial y garantizando una continuidad de negocio. En una organización, el diseño e implementación de un SGSI está influenciado por sus necesidades y objetivos, requerimientos de seguridad, procesos empleados y el tamaño y estructura de la organización.

La problemática de la Oficina Central de Cómputo – Universidad de Lambayeque radica en que siendo ésta el órgano rector encargado de la administración y gestión de la información en la Universidad, no utiliza un código de buenas prácticas que le

permitan asegurar los principios fundamentales y básicos de la información, y por ende no cuenta con una guía en la implementación del sistema de administración y gestión de la seguridad de la información como lo es la NTP-ISO/IEC 17799, careciendo de esta manera con políticas de seguridad organizacional y control de sus activos.

Por lo tanto, la OCC no cuenta con una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información dentro de ésta, no definiéndose claramente las responsabilidades para la protección de los activos individuales y para la ejecución de los procesos específicos de seguridad.

Asimismo, no presenta un listado detallado de sus activos de información, ni la clasificación de estos activos, lo que origina que no se tenga esta información disponible para establecer niveles de protección proporcionales a dicho valor e importancia de los mismos.

El propósito del estudio es para proveer en la OCC una guía genérica que permita gestionar la seguridad de la información partiendo de dos dominios fundamentales de la NTP ISO/IEC 17799, Estructura Organizacional y Control de Activos.

Esta guía debe establecer un marco de trabajo de gestión para iniciar y controlar el proceso de seguridad, por tal motivo, se formulará:

a) Un ente coordinador de todos los aspectos relativos a la implementación de controles para la seguridad de la información..

b) Procedimientos de autorización para la adopción de facilidades de procesamiento de información.

c) Una protección adecuada de los activos de información.

d) Directivas para la clasificación de información.

De esta manera se sustentará bases sólidas y formales de trabajo tanto en la Estructura Organizacional, como en el Control de Activos, asegurando su confidencialidad, disponibilidad e integridad, permitiendo:

a) Una gestión adecuada que brinde la forma de poder maximizar los beneficios de la inversión tecnológica.

b) Proteger los activos de TI/SI.

c) Fortalecer el proceso de toma de decisiones de la alta gerencia, ya que se contaría con información del riesgo inmerso en cada una de dichos activos de TI/SI.

d) Se denotará a la entidad de un sistema de análisis adecuado, que le permitirá asignar recursos para cada activo crítico de TI/SI, en función de sus reales necesidades y objetivos fijados.

e) Fortalecer la imagen de la O.C.C. y la diversidad frente a los organismos gubernamentales encargados de las verificaciones de cumplimiento de normas y estándares, ya que éstos tendrían la certeza de seguridad y continuidad de funcionamiento.

1.2. FORMULACIÓN DEL PROBLEMA

¿La formulación de Políticas de Control de Accesos y Seguridad Física y del entorno basado en la Norma Peruana NTP/IEC 17799 contribuirá a mejorar la gestión de la Oficina Central de Computo de la Universidad de Lambayeque?

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. OBJETIVO GENERAL

Formulación de Políticas de Control de Accesos y Seguridad Física y del entorno basado en la Norma Peruana NTP/IEC 17799 para mejorar la gestión de seguridad de la Oficina Central de Computo de la Universidad de Lambayeque

1.3.2. OBJETIVOS ESPECÍFICOS

a) Diagnosticar el estado actual de los procesos de seguridad de la OCC de la Universidad de Lambayeque.

b) Enumerar cuales son los fallos de comunicación, suministro eléctrico, usuarios internos, usuarios externos, sistemas de información o incumplimiento de una ley o un reglamento.

c) Diseñar un conjunto de políticas de Seguridad física y del entorno, y Control de accesos basado en la Norma Peruana ISO/IEC 17799.

d) Validar los resultados de la formulación de políticas basado en Seguridad Física y control de accesos cumpliendo las buenas prácticas de la norma Peruana ISO/IEC 17799.

1.4. JUSTIFICACIÓN

1.4.1. INSTITUCIONAL

Se definió desarrollar la Norma Peruana NTP-ISO/IEC 17799 la cual trajo los siguientes beneficios:

a) Oportunidad de detectar y corregir debilidades.

b) Seguridad por la alta directiva de que sus activos están fuera del alcance de cualquier vulnerabilidad tanto físico como virtual.

c) Mayor difusión y concientización de la seguridad en la información en la organización tanto en la parte administrativa, como docentes y los alumnos.

d) Revisión independiente de estado actual de la seguridad.

e) Dar confianza a los dueños de la información, a los clientes y a los socios estratégicos.

1.4.2. RELEVANCIA SOCIAL

El beneficio que generará la investigación será guía para otras investigaciones relacionadas a procesos, Asimismo un buen servicio de calidad.

a) Confianza a la población que la institución hace uso de normas de alto nivel.

b) Seguridad de la comunidad que opta por elegir la institución del nivel universitario.

II. MARCO TEÓRICO

2.1. ANTECEDENTES DEL PROBLEMA

2.1.1. A NIVEL INTERNACIONAL

Realizo la tesis sobre “propuesta de BEST PRACTICE para el análisis de vulnerabilidades, métodos de prevención y protección aplicados a la infraestructura de red del laboratorio de sistemas”; El presente trabajo propone como objetivo, las BEST PRACTICE para el análisis de vulnerabilidades, métodos de prevención y protección aplicados a la infraestructura de red del laboratorio de Sistemas-FIE donde uno de sus objetivos específicos son: Aplicar el método de hacking ético para el análisis de vulnerabilidades, prevención y protección de fallos de seguridad encontrados en la red, de esta manera realizar la corrección de los mismos y especificarlos en la guía de BEST PRACTICE propuesta basada en el Estándar Internacional ISO/IEC 17799. En conclusión Por medio del análisis de vulnerabilidades, del cual se desprende que dentro de la infraestructura de red de la Escuela de Ingeniería en Sistemas de la ESPOCH existen efectivamente vulnerabilidades tales como desbordamiento de buffer en el servicio de NETBIOS, ENVENAMIENTO ARP, DNS spoof entre las principales, las cuales siguiendo la metodología de un profesional de seguridad (hacker ético) se ha llegado a explotar un número limitado de dichas deficiencias de seguridad; para prevenir futuros ataques se ha llevado a cabo una propuesta de BEST PRACTICE para la mitigación de las deficiencias de seguridad (Orellana P. & Villaroel V., 2012).

Elaboró la tesis “modelo de administración de seguridad de ´información para procesos básicos de tecnología de información basado en marco de trabajo de ITIL y el estándar ISO/IEC-17799”; este trabajo uno de sus objetivo fue Proponer normas de seguridad para los procedimientos de TI antes mencionados, las cuales estén basadas tanto en las mejores prácticas

determinadas por ITIL y el estándar ISO/IEC-17799, y el alcance de este proyecto La empresa de Telecomunicaciones Alestra, a través del Área de Seguridad de la Información, ha realizado estudios de Análisis de Riesgos, basados en estándares de gestión y seguridad de información; tales como, el ITIL y el ISO/IEC-17799, en el que de acuerdo al resultado de dichos análisis se ha concluido que los siguientes procedimientos operativos son los de mayor impacto en las propiedades de Confidencialidad, Integridad y Disponibilidad de la Información. En conclusión determino que, Para las compañías hoy en día la información es un activo, que como todo activo importante del negocio, tiene valor para la empresa y consecuentemente necesita ser debidamente protegida en cualquiera de sus formas de almacenamiento, escrita en papel, impresa, en un correo electrónico, en una base de datos, etc. El valor de la información es tan alto que debe ser protegida a través de la administración de la seguridad de la información contra una amplia gama de amenazas y vulnerabilidades que permita asegurar la continuidad del negocio, reducir al mínimo el posible daño al negocio y maximizar el retorno de inversión y oportunidades de negocio. Las amenazas pueden provenir de diferentes fuentes, como son humanas, con personas maliciosas externas o internas y no maliciosas (empleados ignorantes), desastres naturales (terremotos, inundaciones, incendios), fallas de equipos, errores de software, etc. Según [Manu00] en su libro “Seguridad, una introducción” plantea que el concepto de seguridad es multidimensional, significando cosas diferentes a diferentes personas en diferentes contextos (Jaramillo Islas, 2004).

Realizó la siguiente tesis “Metodología de Implantación de un SGSI en un grupo empresarial jerárquico”; tuvo como propósito de dar lineamientos metodológicos, de aplicación sistemática para el diseño, implantación, mantenimiento, gestión, monitoreo y evolución de un SGSI según la norma ISO 27.001, para una empresa perteneciente a un grupo empresarial, la cual además está subordinada con respecto a una empresa principal del grupo. Además se ilustra con un Caso de Estudio, los principales aspectos de aplicación de la misma. Puesto que sus conclusiones fueron que Un grupo

empresarial, con una estructura de relación jerárquica o de subordinación, requiere de una metodología que permita gestionar la seguridad de la información atendiendo este aspecto estructural y jerárquico, con criterios alineados a la estrategia empresarial, y además de cooperación en todas las etapas del ciclo PHVA (PDCA), pero a su vez con la flexibilidad y agilidad operativa suficiente para alcanzar los niveles de seguridad necesarios y específicos a cada empresa, respetando los lineamientos corporativos. Este trabajo aporta una metodología con esta concepción de enfoque global y sistémico, atendiendo a la pertenencia de la empresa a un grupo empresarial, y a su vez pragmático, a los efectos que la misma sea, no sólo viable, sino conveniente y efectiva, dando una estructura u organigrama para lograr la coordinación necesaria y especificando los procedimientos que deben cumplirse en cada fase, promoviendo no sólo la reutilización y coherencia integral de la seguridad sino también fomentando la sinergia entre las empresas del grupo. Un producto parcial y homónimo de este trabajo de tesis, se ha constituido en una ponencia en el marco del "V Congreso Iberoamericano de Seguridad Informática (CIBSI'09)" en Montevideo, Uruguay, en noviembre de 2009 (Pallas, 2009).

2.1.2. A NIVEL NACIONAL

Desarrollaron el tema de tesis "Plan de mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT"; La tesis presenta como objetivo general, Realizar un Estudio de Auditoría de Sistemas para La Gerencia Regional de Educación La Libertad, que permita evaluar la operación, uso de los sistemas de información, niveles de seguridad, procedimiento de respaldo, seguridad de los equipos de cómputo, redes y comunicaciones, evaluar el nivel de prestación de 55 servicios informáticos y de tecnología de información, con el fin de brindar las recomendaciones necesarias que se incorporen en forma integral a los sistemas de control y gestión de riesgos de tecnologías de información de la organización.

La cual uso como metodología y estándares para el desarrollo del trabajo de investigación tales como, MAIGTI (Metodología para la Auditoría Integral de Gestión de las Tecnologías de la Información, El COBIT, Los estándares ISO/IEC 12207, ISO/IEC 17799 e ISO/IEC 20000 y PMBOK. Y en sus conclusiones determino finalmente de, Desarrollar la funcionalidad que actualmente no está soportada por los Sistemas de Información, en base a un estudio integral de requerimientos, Revisar el procedimiento de contratación de servicios con terceros que afecten servicios de TI en que se considere un análisis de riesgo previo por cambios de proveedores o cambios en el alcance del servicio (Yan Carranza & Zavala Velasquez, 2013).

Realizó una tesis sobre “el diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano”; la tesis tiene como objetivo, Establecer un procedimiento de auditoría de cumplimiento para la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 en las instituciones del Estado Peruano basado en el marco COBIT 5.0, como parte del proceso de implantación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 con la finalidad de mejorar la gestión de la seguridad de la información. Y concluye Por la efectividad de las pruebas realizadas el presente proyecto de fin de carrera se presenta como una herramienta muy útil en el proceso de evaluación en el cumplimiento de las Normas Técnicas Peruanas NTP-ISO/IEC 17799 y NTPISO/IEC 27001 que se quiera realizar a las empresas del estado que estén regidas por la regulación pertinente que las obliga a tenerlas implementadas. La presentación de estos procedimientos de auditoría de cumplimiento es resultado de la motivación generada por las capacidades obtenidas al llevar los cursos del área de Tecnologías de Información del plan de estudios de la especialidad Ingeniería Informática de la Pontificia Universidad Católica del Perú. Esto es una llamada a poder tener más atención en esta área ya que se necesitan cubrir estos vacíos que se presentan en el escenario informático nacional, pues se declara la obligatoriedad de las NTP tener los mecanismos de poder verificar su cumplimiento.

Es vital reconocer que estos procedimientos están enfocados únicamente para escenarios de empresas del estado, por lo que se recomienda poder trasladarlo a empresas del sector privado, para ocasionar una mejor calidad en Seguridad de Información en ambos grupos (público y privado) dónde el mayor beneficiario serán los ciudadanos y por consiguiente las empresas y/u organizaciones. La actualización de las normas ISO 27001 e ISO 27002 en su versión del año 2013 no afectan a la aplicabilidad de los procedimientos presentados en este proyecto ya que éstos se basan en las NTP que son equivalentes a las normas ISO 27001 e ISO 27002 en su versión del año 2005 (Huáman Monzón, 2014).

Realizó una tesis acerca de “Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo”; donde el objetivo general del proyecto de tesis es, analizar y diseñar un sistema de gestión de seguridad de información, basado en la norma ISO/IEC 27001:2005 para una empresa dedicada a la producción y comercialización de alimentos de consumo masivo. Uno de los resultados esperado del proyecto a desarrollar fue, RE3: Documento con la declaración de aplicabilidad de la norma ISO 27001 para el SGSI que se quiere diseñar. Se verifica con el documento en sí. (Relacionado con el OE3). RE4: Documentación obligatoria exigida por la norma ISO 27001 para implantar un SGSI. (Relacionado con el OE4). Y al finalizar el desarrollo del proyecto de tesis concluye, Tal como se describió y presento a lo largo de este proyecto de fin de carrera, la adecuada gestión de la seguridad de información es algo que debe estar ya incluido en la cultura organizacional de las empresas; y en todas ellas esta adecuada gestión no se lograría sin el apoyo de la alta gerencia como promotor activo de la seguridad en la empresa. Debe tenerse en cuenta que el diseño de SGSI presentado se adapta a los objetivos actuales del proceso de producción, en el cual se ha basado el proyecto, y que este diseño podría variar ya que los objetivos estratégicos y de gobierno de le empresa pueden cambiar y por ello algunos sub procesos que forman parte del alcance del proyecto, también lo harán. Y por

ello finalmente su recomendaciones es, En primera instancia se recomienda a la empresa de producción de alimentos de consumo masivo que en base al diseño presentado en este proyecto, se dedique en concientizar a todos los empleados que forman parte de dicha empresa, sobre la seguridad de la información y su importancia, y realizar evaluaciones periódicas a los indicadores de seguridad de la empresa y de los riesgos encontrados. Luego, se recomienda aplicar esfuerzos para poder realizar la implementación de este diseño para que permita que en el futuro se pueda gestionar la seguridad de información de tal manera que se pueda aspirar a una certificación, ya que el diseño ha sido realizado con la norma ISO/IEC 27001, la cual es certificable (Espinoza Aguinaga, 2013).

2.1.3. A NIVEL REGIONAL

Desarrolló la tesis de “Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo”; La realización de esta tesis es elabora una guía de seguridad la cual ha tomado gran importancia en la organizaciones, para ello menciona como hipótesis Con una Guía de Implementación de la Seguridad de la Información basada en la Norma ISO/IEC 27001, se apoyará en la mejora de la Seguridad en las Aplicaciones Informáticas de la comisaria del Norte –Chiclayo. Y para ello hace uso de la metodología, Norma ISO/IEC 27001. Finalmente concluye, Con la Guía de Implementación, se logró incrementar el nivel de la seguridad en las aplicaciones informáticas de la institución policial, y esto se vio reflejado en el incremento de políticas de seguridad que fueron puestas en marcha que beneficiaron a la institución y ayudaron a incrementar el nivel de seguridad en la misma.

El uso de la Guía de Implementación, se logró mejorar el proceso para detectar las anomalías en la seguridad de la información, reflejado en distintos

mecanismos de seguridad para salvaguardarla y prevenir su mal uso y divulgación no adecuada que perjudiquen a la institución.

Con el Plan de tratamiento de Riesgos, se permitió la disminución de los niveles de riesgos con respecto a los activos de información, considerados amenazas y vulnerabilidades en la institución, esto manifestado en un plan adecuado para abordar estos riesgos, con mecanismos preventivos y correctivos, tomando las precauciones necesarias que minimicen los impactos respectivamente (Alcantara Flores, 2015).

Realizó una tesis acerca de" Políticas de seguridad organizacional y control de activos basado en NTP 17799 para la gestión de la información de la empresa DELTRON SA."; Cuyo objetivo general establece Formular Políticas de seguridad organizacional y control de activos según la Norma Técnica Peruana NTP-ISO/IEC 17799 en la Empresa DELTRON). El propósito de esta tesis de estudio es para proveer en DELTRON una guía genérica que permita gestionar la seguridad de la información partiendo de dos dominios fundamentales de la NTP ISO/IEC 17799, Estructura Organizacional y Control de Activos. El resultado de las conclusiones es, La correcta formulación de políticas de seguridad organizacional y control de activos, en base a estándares y normas nacionales e internacionales, repercute directamente en una Efectiva gestión de la información dentro de la empresa, porque dicha formulación se orienta a cumplir con los principios básicos de seguridad: integridad, disponibilidad, confidencialidad, confiabilidad y cumplimiento de leyes. La existencia de documentos formales, facilitan y uniformizan el desempeño de la actividad informática dentro de la empresa, porque cada persona sabe lo que tiene y debe hacer, la no existencia de estos conlleva a incongruencias dentro de la misma, porque cada persona piensa en aplicar las mejores prácticas que a ellos les parece. Finalmente se recomienda Para el logro de los resultados obtenidos en la investigación, la organización deberá de tener en cuenta, factores estratégicos como el apoyo de la Alta Dirección, la necesidad de

disponer de amplios espacios de difusión, la fácil implementación de la estructura organizacional planteada, así como los mecanismos de gestión de riesgos en activos de TI/SI, la necesidad de orientar a la empresa hacia la formalización de procesos y actividades, una permanente verificación y pruebas de control que garanticen la disponibilidad, integridad y confidencialidad de información y finalmente un adecuado plan de despliegue de la cultura de riesgos que garantice la participación general de los empleados. 2. Se recomienda que el personal que trabaje en la implantación de la formulación de las políticas planteadas en la investigación, debe tener experiencia y compromiso en implantación de proyectos de seguridad, además deben de recibir una Capacitación previa a su participación (Mezones Flores & Tineo Requejo, 2015).

2.2. BASES TEÓRICO-CIENTÍFICAS

2.2.1. SEGURIDAD DE LA INFORMACIÓN

La “Seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella”[1]

Desde el surgimiento de la raza humana en el planeta, la información estuvo presente bajo diversas formas y técnicas. El hombre buscaba representar sus hábitos, costumbres e intenciones en diversos medios que pudiesen ser utilizados por él y por otras personas, además de la posibilidad de ser llevados de un lugar a otro. La información valiosa era registrada en objetos preciosos y sofisticados, pinturas magníficas, entre otros, que se almacenaban con mucho cuidado en locales de difícil acceso, a cuya forma y contenido sólo tenían acceso quienes estuviesen autorizados o listos para interpretarla.

En la actualidad la información es el objeto de mayor valor para las empresas.

El progreso de la informática y de las redes de comunicación nos presenta un nuevo escenario, donde los objetos del mundo real están representados por bits y bytes, que ocupan lugar en otra dimensión y poseen formas diferentes de las originales, no dejando de tener el mismo valor que sus objetos reales, y, en muchos casos, llegando a tener un valor superior.

[1] Presentación del libro “Seguridad: una Introducción”. Dr Manunta, Giovanni. Consultor y Profesor de Seguridad de Cranfield University. Revista Seguridad Corporativa. *http://www.seguridadcorporativa.org*

2.1.1.1. DEFINICIONES DE SEGURIDAD INFORMÁTICA

La Seguridad Informática tiene diferentes acepciones entre ellas podemos destacar:

"La Seguridad Informática permite compartir los sistemas de información de la empresa entre sus empleados, e incluso con terceros, pero garantizando su protección. La seguridad tiene tres aspectos básicos que son esenciales para el crecimiento del negocio, el cumplimiento de la legalidad vigente y la imagen de la propia empresa, estos aspectos son: confidencialidad, integridad y disponibilidad".[2]

"La Seguridad de la Información son los controles que tratan de mantener la confidencialidad, la integridad y la disponibilidad de la información".[3]

"Medidas de resguardo contra el acceso no autorizado a los datos. Los programas y datos se pueden asegurar entregando números de identificación y contraseñas a los usuarios autorizados de una computadora".[4]

"La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles deben establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la organización.".[5]

[2] Guía de Seguridad Informática. SEDISI (Asociación Española de Empresas de Tecnologías de la Información), 5p.
[3] Asociación de Auditoría y Control de Sistemas de Información (ISACA). 15° Edición, Manual de Preparación al examen CISA, 2005. 365p.
[4] www.inei.gob.pe/web/metodologias/attach/lib614/cap03.htm
[5] Norma Técnica Peruana. ISO/IEC 17799. 1° Edición, Lima, 2004, 1p.

Por lo que, definimos Seguridad Informática, como: El proceso continuo que contribuye a disminuir los riesgos que la organización soporta, y a minimizar los daños en los activos de información, si alguno de los riesgos llega a materializarse; preservando la confidencialidad, integridad y disponibilidad de la información.

GRÁFICO N° 1: ASPECTOS BÁSICOS DE LA SEGURIDAD INFORMÁTICA[6]

OBJETIVO DE LA SEGURIDAD INFORMÁTICA

"El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Confidencialidad (sus aspectos fundamentales), Control y Autenticidad de la información manejada por computadora."[6]

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

c) "La Integridad de la Información: es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

[6] ALDEGANI, Gustavo Miguel. Seguridad Informática. MP Ediciones. Argentina. 1997, 22p.

d) La Disponibilidad de la Información: es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

e) La Confidencialidad de la Información: es la necesidad de que la misma sólo sea conocida por personas autorizadas."[7] En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

f) "El Control sobre la información: permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma".[8]

g) "La Autenticidad: permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución."[9] Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

La seguridad informática es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia de un conjunto de acciones y medidas destinadas a proteger y preservar la información de la entidad y sus medios de proceso.

[7] Governance, Control and Audit. for information and Related Technology. 3° Edición. COBIT. 2000. 22 p.

[8] Seguridad informática sus Implicancias e Implementación. Tesis. UTN. Argentina. 2001. Borghello, Cristian Fabián, 8p.

[9] Ídem, 9p.

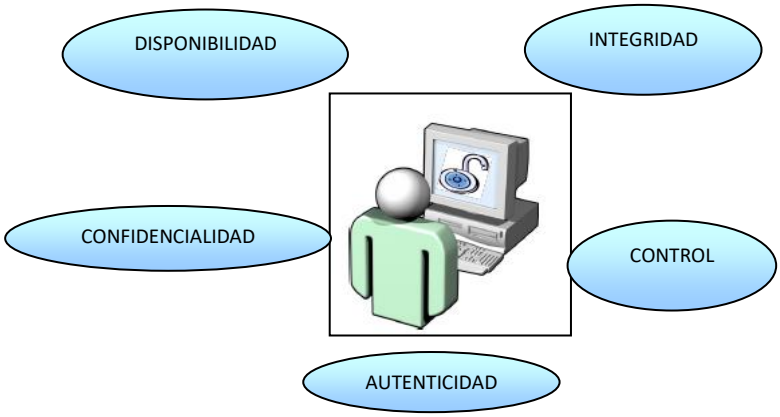


GRÁFICO N° 2 OBJETIVO DE LA SEGURIDAD INFORMÁTICA

2.2.2. POLÍTICAS DE SEGURIDAD INFORMATICA

2.2.2.1. DEFINICIÓN DE POLÍTICA DE SEGURIDAD

El proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero, ante todo, “Una política de seguridad es una forma de

comunicarse con los usuarios […]. Siempre hay que tener en cuenta que la seguridad comienza y termina con personas."[10]

En este sentido, las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos.

2.2.2.2. DEFINICIONES DE POLÍTICA DE SEGURIDAD INFORMÁTICA

Entre las definiciones de Política de seguridad informática, tenemos:

"Una Política de Seguridad informática es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema."[11]

ISACA define Política de Seguridad informática como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán."[12]

"Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización".

---

[10] SPAFFORD, Gene. "Manual de seguridad en redes". Arcert. Argentina. 2000. *http://www.arcert.gov.ar*

[11] HUERTA, Antonio Villalón. Seguridad en Unix y redes. (Versión 1.2). Capítulo 16. 259p.

[12] Asociación de Auditoría y Control de Sistemas de Información (ISACA). 15° Edición, Manual de Preparación al examen CISA, 2005.

Por lo tanto, una política de seguridad de información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

2.2.2.3. ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

a) Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

b) Objetivos de la política y descripción clara de los elementos involucrados en su definición.

c) Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.

d) Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.

e) Definición de violaciones y sanciones por no cumplir con las políticas.

f) Responsabilidades de los usuarios con respecto a la información a la que tiene acceso."[13]

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes.

2.2.2.4. PROPÓSITO DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA

"El propósito de tener políticas escritas en una organización es cumplir con regulaciones legales o técnicas, utilizándolas como guía para el comportamiento profesional y personal permitiendo así unificar la forma de trabajo de personas en diferentes lugares o momentos que tengan responsabilidades y tareas similares y encontrar las mejores prácticas en el trabajo."[14]

---

[13] *http://www.pc-news.com/detalle.asp?sid=&id=11&Ida=1255*

[14] Texto traducido y adaptado de "The Security Policy Life Cycle: Functions and Responsibilities", de Patrick D. Howard, Information Security Management Handbook, Edited by Tipton & Krause, CRC Press LLC, 2003. 1p.

Concluyendo, el propósito de las políticas de seguridad de la información es proteger la información y los activos de la organización. Las políticas son guías para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales.

Según el estudio que hemos elegido hablaremos dos módulos de:

2.2.3. SEGURIDAD FÍSICA Y DEL ENTORNO

2.2.3.1. ÁREAS SEGURAS

Su objetivo principal es de evitar accesos no autorizados e interferencias contra los locales y la información de la organización.

a) Perímetro de Seguridad física

Control: Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información e recursos de procesamiento de información.

b) Controles físicos de Entradas

Control: Las áreas de seguridad deberían estar protegidas por controles de entrada adecuadas que aseguren el permiso de acceso solo al personal autorizado.

c) Seguridad de Oficinas, despachos y Recursos.

Control: La seguridad Física para oficinas, despachos y recursos debe ser asignada y aplicada.

d) Protección contra amenazas externas y ambientales.

Control: Se debe asignar y aplicar protección física de fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastres natural o humana.

e) El trabajo en las Áreas Seguras

Control: Se debería diseñar y aplicar protección física y pautas para trabajar en áreas seguras.

f) El Acceso público, áreas de carga y descarga

Control: Se deberían controlar las áreas de carga y descarga, y si es posible de los recursos de tratamiento de información para evitar accesos no autorizados.

2.2.4. SEGURIDAD DE LOS EQUIPOS

Su objetivo principal es de evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.

a) Instalación y protección de los Equipos.

Control: El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados.

b) Suministro Eléctrico

Control: Se deberían proteger los equipos contra fallos de energía u otras anomalías eléctricas en los equipos de apoyo.

c) Seguridad de Cableado

Control: Se debería proteger contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.

d) Mantenimiento de Equipos

Control: Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.

e) Seguridad de Equipos fuera de los locales de la organización

Control: Se debe aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización tomando en cuenta los diversos riesgos a los que se está expuesto.

f) Seguridad en el rehusó o eliminación de Equipos

Control: Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.

g) Retiro de la propiedad

Control: El equipo de información o software no debe ser sacado del local sin autorización.

2.2.5. CONTROL DE ACCESOS[15]

2.2.5.1. REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESOS

Su objetivo principal es de evitar accesos no autorizados e interferencias contra los locales y la información de la organización

a) Política de Control de accesos.

Control: Una política de control de acceso debe ser establecida, documentada y revisada y debe estar basada en los requerimientos de seguridad y del negocio.

[15] Seguridad de la Información: http://www.aenorperu.com/seguridad-de-la-informaci%C3%B3n.aspx

2.2.5.2. GESTIÓN DE ACCESOS A USUARIOS

Su objetivo principal es de evitar accesos no autorizados e interferencias contra los locales y la información de la organización.

a) Registros de Usuarios

Control: Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario.

b) Gestión de privilegios

Control: Se debe restringir y controlar el uso y asignación de privilegios.

c) Gestión de contraseñas de usuarios

Control: Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal.

d) Revisión de los derechos de accesos de los usuarios

Control: La gerencia debería establecer un proceso formal de revisión periódica de los derechos de accesos de los usuarios.

2.2.5.3. RESPONSABILIDAD DE LOS USUARIOS.

Su objetivo es evitar el acceso de usuarios no autorizados y el compromiso o hurto de la información y de las instalaciones del procesamiento de información. Una protección eficaz necesita la cooperación de los usuarios autorizados.

Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

Un escritorio limpio, así como una política de pantalla clara debe ser implementado con el fin de reducir el riesgo de acceso no autorizado o de daño a los papeles, medios e instalaciones del procesamiento de información.

a) Uso de Contraseñas

Control: Los usuarios deberían seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas.

b) Equipo informático de usuario desatendido

Control: Los usuarios deberían asegurar que los equipos informáticos desatendidos estén debidamente protegidos.

c) Política de pantalla y escritorio limpio

Control: Se debería adoptar una política de escritorio limpio para papeles y medios removibles del almacenamiento así como una política de pantalla limpia para instalaciones de procesamiento de información.

2.2.5.4. CONTROL DE ACCESO A LA RED

Su objetivo es prevenir el acceso no autorizado de los servicios de la red. Debería controlarse el acceso a los servicios a las redes internas y externas.

Hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por medio de:

- Interfaces adecuadas entre la red de la organización y las redes públicas o las privadas de otras organizaciones.

- Mecanismos adecuados de autenticación para los usuarios y los equipos.

- Control de los accesos de los usuarios a los servicios de información.

d) Política de uso de los servicios de la Red

Control: Los usuarios sólo deberían tener acceso directo a los Servicios para los que tengan autorizados de una forma específica.

e) Autentificación de usuario para conexiones externas

Control: Se deben utilizar métodos apropiados de autentificación para controlar el acceso de usuarios remotos.

f) Identificación de Equipos en las Redes

Control: Las identificaciones automáticas de equipo deben ser consideradas como medios para autentificar conexiones desde locales y equipos específicos.

g) Diagnostico remoto y configuración de protección de puertos

Control: Se debería controlar el acceso físico y logístico para diagnosticar y configurar puertos.

h) Segregación en la Redes

Control: Los grupos de servicios de información, usuarios y sistemas de información deben ser segregados en las redes.

i) Control de conexiones a las Redes

Control: Los requisitos de la política de control de accesos para redes compartidas, sobre todo para las que atraviesan las fronteras de la organización, se deberían basar en los requisitos de las aplicaciones del negocio.

j) Control de Enrutamiento en la Red

Control: Se deberían implementar controles de enrutamiento que garanticen que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso a las aplicaciones.

2.2.5.5. CONTROL DE ACCESO AL SISTEMA OPERATIVO (SO)

Su objetivo es evitar accesos no autorizados a los computadores. Las prestaciones de seguridad a nivel de sistema operativo se deberían utilizar para restringir el acceso a los recursos del computador. Estos servicios deberían ser capaces de:

- Identificar y verificar la identidad de cada usuario autorizado en concordancia con una política definida de control de acceso.
- Registrar los accesos satisfactorios y fallidos al sistema.
- Registrar el uso de privilegios especiales del sistema.
- Alarmas para cuando la política del sistema de seguridad sea abierta.
- Suministrar mecanismos, adecuados de autenticación.
- Cuando proceda, restringir los tiempos de conexión de usuarios.

a) Procedimiento de conexiones de terminales

Control: El acceso a los servicios de información debería estar disponible mediante un proceso de conexión seguro.

b) Identificación y autentificación del usuario

Control: Todos los usuarios deberían disponer de un identificador único para su uso personal y debería ser escogida una técnica de autentificación adecuada para verificar la identidad de estos.

c) Sistema de gestión de contraseñas

Control: Los sistemas de gestión de contraseñas deberían proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas.

d) Utilización de las facilidades del Sistema

Control: La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restrinja y se mantenga fuertemente controlado.

e) Desconexión automática de sesiones

Control: Las sesiones se deberían desactivar tras un periodo definido de inactividad.

f) Limitación de tiempo de conexión

Control: Las restricciones en los tiempos de conexión ofrecen seguridad adicional para aplicaciones de alto riesgo.

2.2.5.6. CONTROL DE ACCESO A LAS APLICACIONES Y LA INFORMACIÓN

Su objetivo es prevenir el acceso no autorizado a la información contenida en los sistemas.

Se deberían usar las facilidades de seguridad lógica dentro de los sistemas de aplicación para restringir el acceso.

Se deberían restringir el acceso lógico al software y a la información sólo a los usuarios autorizados. Las aplicaciones deberían:

- Controlar el acceso de los usuarios a la información y las funciones del sistema de aplicación, de acuerdo con la política de control de accesos;

- Protegerse de accesos no autorizados desde otras facilidades o software de sistemas operativos que sean capaces de eludir los controles del sistema o de las aplicaciones;

- No comprometer la seguridad de otros sistemas con los que se compartan recursos de información.

2.2.5.7. INFORMÁTICA MÓVIL Y COMUNICACIONES

Su objetivo es garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y teletrabajo.

La protección requerida debería ser proporcional a los riesgos que causan estas formas específicas de trabajo. Se deberían considerar los riesgos de trabajar en un entorno desprotegido cuando se usa informática móvil y aplicar la protección adecuada. En el caso del teletrabajo la organización debería implantar protección en el lugar del teletrabajo y asegurar que existen los acuerdos adecuados para este tipo de trabajo.

a) Informática móvil y telecomunicaciones

Control: Se debería adoptar una política formal y medidas de seguridad apropiadas con el fin de protegernos contra los riesgos cuando se usan dispositivos de informática.

b) Teletrabajo

Control: Se deberían desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de teletrabajo.

2.2.6. ESTÁNDARES DE SEGURIDAD

Las empresas deben realizar una gestión que demuestre competencia y efectividad de la seguridad de sus recursos y los datos que obtienen, gestionan y envían.

Deben identificar y detectar los posibles riesgos que estén sujetos y se adopten medidas adecuadas y establecidas para que esta seguridad este completa y monitoreada y cumpliendo las normas para completar.

2.2.6.1. ISO 17799

Denominada también como ISO 27002; es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization for Standardizationy por la Comisión Electrotécnica Internacional en el año2000, ISO/IEC 17799 plantea las siguientes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información para el control de accesos y seguridad ambiental y del entorno (Gutierrez Rios, 2010).

Que por cada riesgo identificado se debe realizar una decisión de tratamiento del riesgo, la cual se deberá tomar los siguientes controles:

a) Aplicación de controles apropiados para disminuir los riesgos.

b) Los riesgos aceptados satisfacen el criterio para la aceptación del riesgo y la política de la empresa.

c) Evitar riesgos no se permita para realizar acciones que puedan causar que estos riesgos sucedan.

d) Se transfieren los riesgos asociados a terceros como son los proveedores y las aseguradoras.

2.2.6.2. CARACTERÍSTICA DE LA ISO 17799

Las principales secciones de esta norma son:

a) Política de Seguridad.

b) Organización de la seguridad de la información.

c) Gestión de activos de información.

d) Seguridad de los Recursos Humanos.

e) Seguridad Física y del entorno

f) Gestión de Comunicaciones y Operaciones.

g) Control de Accesos.

h) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

i) Gestión de incidentes en la Seguridad de Información.

j) Gestión de Continuidad del Negocio.

k) Cumplimiento[16]

[16] Historia del ISO 17799: http://studylib.es/doc/845974/3.-historia-y-evoluci%C3%B3n-de-la-iso-serie-27000-iso-17799

III. DESARROLLO DE LA PROPUESTA

3.1. FORMULACIÓN DE POLÍTICAS PARA LA SEGURIDAD FÍSICA Y DEL ENTORNO.

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la UDL. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental, mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible de la UDL, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas de la UDL.

3.1.1. CONTROL FÍSICO DE ENTRADA

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por la Gerencia de Administración y Finanzas, en conjunto con el Responsable de Logística a fin de permitir el

acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área.

b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.

c) Implementar el uso de una identificación única visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

d) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará el Oficial de Seguridad de la Información.

e) El espacio ocupado por el personal del Área de TI, está considerado como un Área de acceso limitado. La puerta de acceso debe permanecer cerrada las 24 horas del día durante los 7 días de la semana, con la finalidad de no permitir el ingreso de personal no autorizado.

f) Ante la posibilidad de que alguien pretenda ingresar sin autorización a las Áreas de acceso restringido, el Área de TI o personal a cargo, dará aviso de inmediato al personal de vigilancia, quedando registrado dicho incidente en la bitácora de Incidencias de Seguridad.

g) Solo personal autorizado contará con acceso a los equipos de cómputo instalados en TI, la libertad de acceso en especial a los servidores principales, pueden crear un significativo problema de seguridad. El acceso solo está permitido a las personas que regularmente trabajan en esta Área.

h) Los usuarios deberán acatar estos lineamientos para cualquier computadora o red usada dentro o fuera de la UDL. Está terminantemente prohibido el ingreso y salida de equipos, software, sin la autorización correspondiente y/o la conformidad de la Gerencia de Administración.

3.1.2. PROTECCIÓN DE LOS EQUIPOS

a) Las instalaciones del Área de TI, están provistos de equipos para la extinción de incendios como son extintores de tipo gas Carbónico (CO2), ya que estos no dañan los equipos de cómputo y sensores de humo.

b) Los mecanismos de ventilación en el Área de Tecnología de la Información y Procesos, se han colocado en razón al hardware en el Área. La temperatura se mantiene no menor de 18° C ni mayor 22° C (estándares internacionales).

c) La UDL realizara acciones necesarias para asegurar la buena condición y continuidad de los equipos de cómputo, tomando en cuenta aspectos de temperatura ambiental, seguridad física, control de incendios, entre otros.

d) Queda terminantemente prohibido fumar y el consumo de alimentos y bebidas en el interior de las Áreas de acceso restringido.

3.1.3. INSTALACIONES DE SUMINISTRO

a) El centro de cómputo o data center cuenta con un sistema de alimentación ininterrumpida (UPS), en situación normal el mismo debe ser probado por lo menos una vez cada seis (6) meses. El jefe de TI y el encargado en Soporte son responsables de esta actividad, así como de coordinar que el personal a su cargo reciba la capacitación del manejo del equipo.

b) El suministro de energía establecido donde se encuentra situado el hardware de red, enrutadores y otros dispositivos que son necesarios para el buen funcionamiento normal de la UDL, mantiene un suministro estable y continuo de energía eléctrica, utilizando sistemas UPS (Sistema de suministro interrumpido de energía), la cual se encarga de regular la tensión llegando a evitar los picos de voltaje, además de proporcionar un tiempo de autonomía por medio de baterías en caso de corte de suministro eléctrico. La ubicación de los UPS se encuentra dentro de la misma sala de servidores, en el cual no puedan ser desactivados por un supuesto intruso o por una falla de usuario.

c) El área de TI, coordinara con logística, la realización de una prueba para evaluar la operatividad del UPS, ante una contingencia.

d) Realizar pruebas de operatividad de los equipos UPS, a fin de evaluar su tiempo respaldo ante una contingencia.

e) Las instalaciones eléctricas de las Áreas de acceso restringido deberán contar con un sistema de conexión a tierra, en lo posible independiente, de alta calidad y dentro de los rangos permisibles

3.1.4. SEGURIDAD DEL CABLEADO

a) El cableado de red, se encuentra físicamente separado de cualquier otro tipo de cables, siendo estos de corriente o energía eléctrica. Para evitar interferencias, los servidores se encuentran localmente separados, para lo cual estos equipos críticos de información y proceso se encuentran aislados y seguros, protegidos con un nivel de seguridad verificable y manejable por los administradores de seguridad y las personas responsables por estos activos.

b) Proteger el cableado de red contra intercepción no autorizada o daño (ejemplo: el uso de conductos o evitando trayectos que atraviesen áreas públicas).

c) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.

3.1.5. MANTENIMIENTO DE EQUIPOS

a) El mantenimiento y supervisión permanente de las condiciones de seguridad física y ambiental del centro de cómputo o data center, así como de los denominados otros activos de informática de alto riesgo ubicados fuera del centro de cómputo, es responsabilidad del Área de TI.

b) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del área de Tecnologías de la Información y Procesos.

c) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

d) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

3.2. FORMULACIÓN DE POLÍTICAS PARA EL CONTROL DE ACCESO

Con el objetivo de impedir el acceso no autorizado a la información, se definen políticas para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

3.2.1. GESTIÓN DE ACCESOS USUARIOS

3.2.1.1 REGISTRO DE USUARIOS

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.

b) Verificar que el usuario tiene la autorización de la Gerencia de Administración, para el uso de los sistemas, base de datos o servicio de información.

c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario.

d) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.

e) Mantener un registro formal de todas las personas registradas para utilizar el sistema.

f) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la UDL.

g) Efectuar revisiones periódicas con el objeto de:

- Cancelar identificadores y cuentas de usuario redundantes.
- Inhabilitar cuentas inactivas por más de 60 días.
- Bloquear cuentas inactivas por más de 120 días.

h) En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.

i) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

3.2.1.2 GESTIÓN DE PRIVILEGIOS

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

Se deben tener en cuenta los siguientes pasos:

a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los accesos.

b) Asignar los privilegios al personal teniendo en cuenta las actividades que realizara como parte de sus funciones asignadas.

c) Mantener un proceso de autorización y un registro de todos los privilegios asignados.

d) Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

e) El mal uso de los privilegios concedidos (por ser necesarios realizar actividades de soporte, mantenimiento y operación), se considerara

como abuso de autoridad y como tal será sancionada de acuerdo al Reglamento interno de trabajo.

f) El acceso a los subsistemas, módulos, sub módulos, transacciones, menús, opciones, y cualquier otro componente de un sistema deberá definirse mediante el uso de los perfiles de usuario, de acuerdo con el rol o función que los usuarios tienen asignados para el cumplimiento adecuado de sus funciones y que serán definidos por la Oficina Central de Computo (OCC). en coordinación con las Gerencias / Jefaturas de las Áreas involucradas.

3.2.1.3 GESTIÓN DE CONTRASEÑAS DE USUARIO.

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos.

a) Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de claves.

b) Toda sospecha de vulnerabilidad en la seguridad debe ser notificada inmediatamente a la Oficina Central de Computo (OCC).

c) No se deben revelar las claves a otras personas, incluyendo la gerencia y los administradores del sistema.

d) No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por la Oficina Central de Computo (OCC).

e) Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.).

f) Las claves deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad).

g) Se deben escoger claves seguras de la siguiente forma:

- Utilizando al menos ocho caracteres;
- Utilizando al menos un carácter numérico;
- Utilizando al menos un carácter alfabético en mayúscula y uno en minúscula.
- Una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma; como tampoco ninguna de estas palabras escritas hacia atrás.
- Las claves no deben estar relacionadas con datos personales
- No se deben usar nuevamente las últimas tres claves.

h) Se deben cambiar las claves cada mes.

i) Se deben cambiar las claves en el primer ingreso al sistema.

j) Las cuentas tendrán una duración limitada y se regularan por un procedimiento específico.

k) Los intentos infructuosos de acceso a los sistemas se limitaran a tres (3) intentos, luego de los cuales la contraseña será revocada y/o el usuario bloqueado.

l) Al firmar la Declaración de aceptación de los documentos del SGSI, los usuarios aceptan la obligación de mantener sus claves en forma confidencial. Este documento deberá ser entregado por Recursos Humanos al personal antiguo y nuevo que ingresa a la UDL, a fin de dar a conocer las medidas de seguridad que se han establecido para la protección de los activos de información.

m) Cada usuario debe utilizar su propio nombre de usuario asignado de forma exclusiva.

n) Cada usuario tienen la posibilidad de escoger su propia clave.

o) Las claves de primer acceso deben ser comunicadas al usuario de forma segura, y se debe verificar previamente la identidad del usuario.

p) El sistema de gestión de claves debe requerir que el usuario modifique la clave de primer acceso cuando ingrese al sistema por primera vez, además de requerir que el usuario escoja contraseñas seguras y que cambien sus claves cada mes.

3.2.2. REVISIÓN DE DERECHOS DE ACCESO DE USUARIOS

A fin de mantener un control eficaz del acceso a los datos y software contable CONCAR, el Encargado de Soporte revisara los accesos de los usuarios. Para ello se deberán contemplar los siguientes controles.

a) Revisar los derechos de acceso de los usuarios a intervalos de 2 a 6 meses.

b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 1 a 3 meses. Este seguimiento será realizado por el Oficial de Seguridad de la Información.

c) Revisar las asignaciones de privilegios a intervalos de 2 a 6 meses, a fin de garantizar que no se obtengan privilegios no autorizados. Este seguimiento será realizado por el Jefe de Recursos Humanos.

3.2.3. RESPONSABILIDADES DE LOS USUARIOS.

3.2.3.1. USO DE CONTRASEÑAS

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.

b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:

- Sean fáciles de recordar.

- No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.

- No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

e) Cambiar las contraseñas provisorias en el primer inicio de sesión.

f) Notificar mediante “El procedimiento para el registro de Incidentes”, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

3.2.3.2. EQUIPOS DESATENDIDOS EN ÁREAS DE USUARIOS

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

Los usuarios cumplirán con las siguientes pautas:

a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.

b) Proteger las PC’s o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

c) Política de pantalla y escritorio limpio

d) Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán las siguientes medidas:

3.2.3.3. POLÍTICA DE ESCRITORIO LIMPIO

a) Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, etiquetados como sensibles, deben ser retirados del escritorio o de otros lugares (impresoras, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

3.2.3.4. POLÍTICA DE PANTALLA LIMPIA

a) Si la persona autorizada no se encuentra en su puesto de trabajo, deberá quitar toda la información sensible de la pantalla, y deberá denegar el acceso a todos los sistemas para los cuales tiene autorización.

b) En el caso de una ausencia corta (hasta 30 minutos), la política de

pantalla limpia se implementa finalizando la sesión en todos los sistemas o bloqueando la pantalla con una clave. Si la persona se ausenta por un período más prolongado (superior a 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas y apagando el puesto de trabajo.

c) Está permitido el acceso al personal a todas las instalaciones de la UDL, excepto a aquellas áreas que han sido consideradas como áreas de acceso restringido.

3.2.3.5. Control de acceso a la red.

a) Las conexiones no seguras a los servicios de red pueden afectar a toda la UDL, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

b) El Responsable de Soporte tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del Jefe de una Área o Unidad Organizativa que lo solicite para personal de su incumbencia.

c) Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la UDL.

d) El Responsable de Soporte junto con el Jefe de sistemas definirán las pautas para garantizar la seguridad de los servicios de red de la UDL, tanto públicos como privados.

- ✓ Para ello se tendrán en cuenta las siguientes directivas.

- ✓ Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.

- ✓ Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.

- ✓ Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.

- ✓ Instalar periódicamente las actualizaciones de seguridad.

e) Dicha configuración será revisada periódicamente por el Responsable de Soporte.

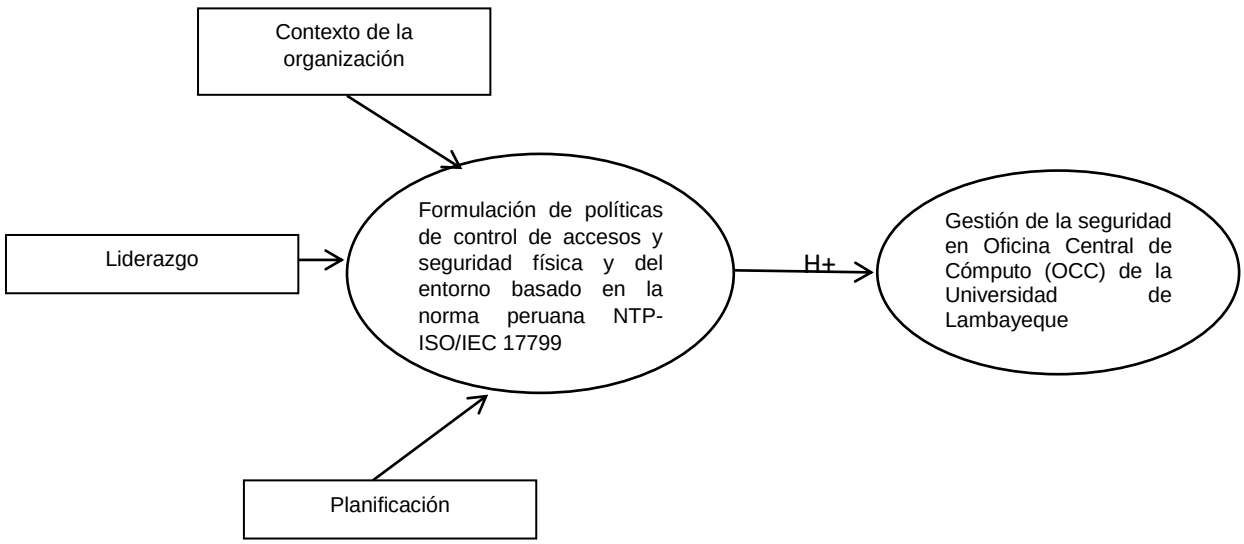
IV. MATERIALES Y MÉTODOS

4.1. HIPÓTESIS

La formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma peruana NTP-ISO/IEC 17799 contribuye a mejorar la gestión de la seguridad en la Oficina Central de Cómputo (OCC) de la Universidad de Lambayeque

4.2. MODELO CONCEPTUAL DE LA INVESTIGACIÓN

El modelo conceptual muestra las variables de la investigación y las dimensiones que se evaluarán para contrastar la hipótesis:



4.3. OPERACIONALIZACIÓN DE VARIABLES

La tabla siguiente muestra los indicadores que se obtendrán para cada uno de las dimensiones consideradas en la evaluación de la variable independiente, que es la variable que se va a manipular.

Variable independiente	formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma peruana NTP-ISO/IEC 17799
Variable dependiente	gestión de la seguridad en la Oficina Central de Cómputo (OCC) de la Universidad de Lambayeque

VARIABLE	DIMENSIÓN	INDICADOR	INSTRUMENTO PARA LA EVALUACIÓN	ESCALA
Formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma peruana NTP-ISO/IEC 17799	Contexto de la organización	Grado de adecuamiento del modelo de SGSI planteado a la estructura organizativa, a la normativa interna y a los procesos internos de la UDL	Cuestionario	Escala Likert: (1) "muy en desacuerdo" - (5) "fuertemente de acuerdo"
		Nivel de satisfacción de las necesidades y expectativas de las partes interesadas		
		Nivel de conformidad del alcance del SGSI		
		Nivel de cumplimiento de los requisitos de la Norma NTP 17799		
	Liderazgo	Nivel de compromiso de la alta gerencia	Cuestionario	Escala Likert: (1) "muy en desacuerdo" - (5) "fuertemente de acuerdo"
		Nivel Efectividad de las políticas de TI		
		Nivel de consistencia de los roles, responsabilidades y autoridades organizacionales del SGSI propuesto.		
	Planificación	Nivel de Efectividad de las acciones para tratar los riesgos	Cuestionario	Escala Likert: (1) "muy en desacuerdo" - (5) "fuertemente de acuerdo"
		Nivel de consistencia en los objetivos de seguridad y su planificación para conseguirlos.		
Gestión de la seguridad en la Oficina Central de Cómputo (OCC) de la Universidad de Lambayeque	Grado de satisfacción en la gestión de la seguridad de la información		Cuestionario	Escala Likert: (1) "muy en desacuerdo" - (5) "fuertemente de acuerdo"

4.4. DISEÑO DE CONTRASTACIÓN DE LA HIPÓTESIS

El modelo lógico de contrastación es del tipo Pre Experimental porque se realizará un post test, mediante el diseño siguiente:

GE: OX r OY

Donde:

OX: Observación a la formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma peruana NTP-ISO/IEC 17799.

OY: Observación a la gestión de la seguridad en la Oficina Central de Cómputo (OCC) de la Universidad de Lambayeque

R: impacto

Para evaluar los indicadores de las dimensiones de la tabla de operacionalización de las variables se aplicará la estrategia de evaluación de factores con la finalidad de determinar los coeficientes de influencia que tienen cada uno de los indicadores/dimensiones sobre el modelo del Sistema de Gestión de Seguridad de la Información propuesto.

4.5. POBLACIÓN Y MUESTRA DE ESTUDIO

Unidad de Análisis: Usuarios de los servicios de TI ofrecidos por la Oficina Central de Cómputo (OCC) de la Universidad de Lambayeque.

Población: La población de la investigación está conformada de la siguiente manera:

TIPO DE USUARIO/CLIENTE	N° USUARIOS
Personal Directivo (autoridades y responsables de jefaturas)	11
Personal Administrativo (secretarias, asistentes, coordinadores y personal de laboratorio)	36
TOTAL	47

FUENTE: DESARROLLO PROPIO

OBSERVACIÓN:

La cantidad considerada en la tabla, considera usuarios, al personal de la UDL que tienen acceso y utiliza algún terminal de computador, conectado a la red de datos y comunicaciones que utiliza como parte de sus funciones diarias.

4.6. TÉCNICA DE RECOPILACIÓN DE LOS DATOS

Se aplicó una encuesta de satisfacción sobre los dominios del Sistema de Gestión de la Seguridad de la Información propuesto a la población indicada.

Esta encuesta fue diseñada de tal forma que sea compatible con los indicadores que se desean evaluar en esta investigación.

Para ello se elaboró la siguiente tabla que muestra la relación de las preguntas diseñadas en la encuesta con los correspondientes indicadores que permiten medirlo con la información recopilada.

TABLA MATRIZ DE CONSISTENCIA ENTRE LOS INDICADORES Y LAS PREGUNTAS DE LA ENCUESTA

DIM	INDICADOR	PREGUNTA	
Contexto de la organización	Grado de adecuamiento del modelo de SGSI planteado a la estructura organizativa, a la normativa interna y a los procesos internos de la UDL	P1	Usted considera que el Sistema de Gestión de Seguridad de la Información se adecuada a la estructura organizativa, a la normativa interna y a los procesos internos de la UDL.
	Nivel de satisfacción de las necesidades y expectativas de las partes interesadas	P2	El SGSI propuesto permite satisfacer las necesidades y expectativas de las partes interesadas en la gestión de la seguridad de la información.
	Nivel de conformidad del alcance del SGSI	P3	Usted está conforme del modo como se determinó el alcance del Sistema de Gestión de Seguridad de la Información propuesto.
	Nivel de cumplimiento de los requisitos de la Norma NTP 17799	P4	En qué grado usted cree que el SGSI propuesto cumple con las exigencias o los requisitos de la Norma Técnica Peruana 17799.
Liderazgo	Nivel de compromiso de la alta gerencia	P5	Cree usted que en el SGSI propuesto se han establecido con claridad los liderazgos y compromisos para un adecuado gobierno de la seguridad de la información en la UDL.
	Nivel Efectividad de las políticas de TI	P6	Usted cree que la declaración de las políticas de seguridad en el SGSI permite establecer los objetivos de seguridad y permite la mejora continua del mismo.
	Nivel de consistencia de los roles, responsabilidades y autoridades organizacionales del SGSI propuesto.	P7	Usted cree que los roles, responsabilidades y autoridades organizacionales del SGSI son adecuadas para la gestión de la seguridad de la información en la UDL.
Planificación	Nivel de Efectividad de las acciones para tratar los riesgos	P8	Considera usted que se definió y aplico adecuadamente un proceso de valorización del riesgo de seguridad de la información
	Nivel de consistencia en los objetivos de seguridad y su planificación para conseguirlos.	P9	Usted cree que los objetivos de seguridad de la información y su plan de ejecución planteados en el SGSI son adecuados para la gestión de la seguridad de la información en la UDL.
Grado de satisfacción en la gestión de la seguridad de la información		P10	Según usted cuál es su nivel de satisfacción de que los dominios del SGSI propuesto logra mejorar la gestión de la seguridad de la información

FUENTE: DESARROLLO PROPIO

4.7. TRATAMIENTO DE LOS DATOS Y DISCUSIÓN DE RESULTADOS

Para el tratamiento de los datos, se utilizó el aplicativo SPSS v 21, obteniéndose los siguientes resultados:

4.7.1. FIABILIDAD DEL INSTRUMENTO (ENCUESTA)

Se determinó el nivel de fiabilidad del instrumento (la encuesta) utilizando el estadístico Alfa de Cronbach.

El método de consistencia interna basado en el alfa de Cronbach permite estimar la fiabilidad de un instrumento de medida a través de un conjunto de ítems que se espera que midan el mismo constructo o dimensión teórica.

La validez de un instrumento se refiere al grado en que el instrumento mide aquello que pretende medir. Y la fiabilidad de la consistencia interna del instrumento se puede estimar con el alfa de Cronbach.

La medida de la fiabilidad mediante el alfa de Cronbach asume que los ítems (medidos en escala tipo Likert) miden un mismo constructo y que están altamente correlacionados (Welch & Comer, 1988)

Cuanto más cerca se encuentre el valor del alfa a 1 mayor es la consistencia interna de los ítems analizados.

La fiabilidad de la escala debe obtenerse siempre con los datos de cada muestra para garantizar la medida fiable del constructo en la muestra concreta de investigación.

Procesados los datos se obtuvo lo siguiente:

ESTADÍSTICOS DE FIABILIDAD

ALFA DE CRONBACH	N DE ELEMENTOS
0,890	10

RESUMEN DEL PROCESAMIENTO DE LOS CASOS

		N	%
Casos	Válidos	31	100,0
	Excluidos	0	,0
	Total	31	100,0

ELIMINACIÓN POR LISTA BASADA EN TODAS LAS VARIABLES DEL PROCEDIMIENTO.

Nota: solo se procesaron 31 encuestas.

Como criterio general, George & Mallery (2003) sugieren las recomendaciones siguientes para evaluar los coeficientes de Alfa de Cronbach:

- Coeficiente alfa >0.9 es excelente
- Coeficiente alfa >0.8 es bueno
- Coeficiente alfa >0.7 es aceptable
- Coeficiente alfa >0.6 es cuestionable
- Coeficiente alfa >0.5 es pobre
- Coeficiente alfa <0.5 es inaceptable

Es este caso se ha alcanzado 0.89, confirmándose que la encuesta aplicada es buena.

4.7.2. ANÁLISIS DE LA REGRESIÓN MÚLTIPLE

Utilizamos regresión múltiple porque nuestra hipótesis pretende estudiar la posible relación entre las variables independientes (predictoras o explicativas) y la variable dependiente (criterio, explicada, respuesta). En este caso, nuestras variables son:

a) Variable Independiente (Xi): formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma peruana NTP-ISO/IEC 17799, descrita a través de las dimensiones de contexto de la organización (X1), liderazgo (X2) y Planificación (X3)

b) Variable dependiente (Y): Grado de satisfacción en la gestión de la seguridad de la información en la Oficina Central de Cómputo (OCC) de la Universidad de Lambayeque

c) Por tanto, el modelo a evaluar es un modelo de regresión múltiple de la forma:

$$Y = C_0 + C_1X_1 + C_2X_2 + C_3X_3 + e$$

Esto significa que se pretende evaluar la relación existente entre la variable dependiente “Grado de satisfacción en la gestión de la seguridad de la información en la Oficina Central de Cómputo (OCC) de la Universidad de Lambayeque” y la variable independiente “formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma peruana NTP-ISO/IEC 17799”, esta última explicada por tres dimensiones: Contexto de la organización (X1), liderazgo (X2) y Planificación (X3)

Para lograr este objetivo, se desarrolló el siguiente procedimiento:

Reducción de ítems de cada dimensión evaluada

Dado que cada una de las dimensiones tiene más de un ítem a evaluar se tuvo que reducir a un solo ítem, de la siguiente manera:

MATRIZ DE REDUCCIÓN DE ÍTEMS EVALUADOS

DIMENSIÓN	ÍTEM		ÍTEM REDUCIDO
Contexto de la organización(X_1)	Grado de adecuamiento del modelo de SGSI planteado a la estructura organizativa, a la normativa interna y a los procesos internos de la UDL	P1	Dim_contexto = (P1 + P2 + P3 + P4)/4
	Nivel de satisfacción de las necesidades y expectativas de las partes interesadas	P2	
	Nivel de conformidad del alcance del SGSI	P3	
	Nivel de cumplimiento de los requisitos de la Norma NTP 17799	P4	
Liderazgo(X_2)	Nivel de compromiso de la alta gerencia	P5	Dim_liderazgo = (P5 + P6 + P7)/3
	Nivel Efectividad de las políticas de TI	P6	
	Nivel de consistencia de los roles, responsabilidades y autoridades organizacionales del SGSI propuesto.	P7	
Planificación(X_3)	Nivel de Efectividad de las acciones para tratar los riesgos	P8	Dim_planificacion = (P8 + P9 + P10)/2
	Nivel de consistencia en los objetivos de seguridad y su planificación para conseguirlos	P9	

FUENTE: DESARROLLO PROPIO

d) Aplicación de la metodología de regresión múltiple

Para nuestro análisis se aplicará la metodología de regresión múltiple jerárquica con tres bloques, donde se fueron tomando variable por variable independiente con las que estamos trabajando, con la finalidad de generar diferentes modelos. Los modelos que esperamos generar son los siguientes:

- Modelo 1: sólo con la variable Contexto de la organización(X1)

- Modelo 2: sólo con las variables Contexto de la organización (X1) y Liderazgo (X2)

- Modelo 3: con las tres variables Contexto de la organización (X1), Liderazgo (X2) y Planificación (X3)

Esto nos permitirá identificar mayor información de las variables independientes con las que estamos trabajando; así como también nos permite identificar si alguna de esas variables independientes no aporta al modelo, por tanto puede ser excluida del modelo.

LOS RESULTADOS OBTENIDOS SE MUESTRAN A CONTINUACIÓN:

RESUMEN DEL MODELO					
MODELO	R	R CUADRADO	R CUADRADO CORREGIDA	ERROR TÍP. DE LA ESTIMACIÓN	DURBIN-WATSON
1	,598[a]	,357	,335	,468	
2	,632[b]	,399	,356	,460	
3	,728[c]	,530	,478	,415	1,645
a. Variables predictoras: (Constante), Dim_contexto					
b. Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo					
c. Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo, Dim_planificacion					
d. Variable dependiente: P10					

Del cuadro se deduce que:

- El Modelo 1 (sólo con la variable Contexto de la organización (X1)) explica el 35.7% de la varianza de la variable dependiente.

- El Modelo 2 (sólo con las variables Contexto de la organización (X1) y Liderazgo (X2)) explica el 39.9% de la varianza de la variable dependiente.

- El Modelo 3 (con las tres variables Contexto de la organización (X1), Liderazgo (X2) y Planificación (X3)) explica el 53.0% de la varianza de la variable dependiente.

Para efectos de la demostración de la hipótesis seleccionamos el Modelo 3 donde se incluyen las tres variables independientes.

Por otro lado, en el mismo cuadro observamos el resultado de la prueba de Durbin-Watson que nos da un valor para determinar la independencia de errores, pero no una significancia; por lo que tenemos que tener algunos criterios de identificación de cuando este valor es bueno o no bueno. El valor esperado de la prueba Durbin-Watson es que sea lo más cercano a 2, en este caso tenemos un valor de 1.645 que es bueno. El rango que se debe tener en cuenta para aceptar el resultado de la prueba de Durbin-Watson es 1 ± 2, es decir entre 1 y 3.

La interpretación de este resultado es que no existe dependencia de las observaciones recogidas, por lo tanto se demuestra que la recogida de la información ha sido aleatoria, evitando así invalidar por completo las conclusiones del análisis estadístico.

A. ANÁLISIS DE VARIANZA (ANOVA)

Los resultados del ANOVA se muestran en el siguiente cuadro:

ANOVA						
MODELO		SUMA DE CUADRADOS	GL	MEDIA CUADRÁTICA	F	SIG.
1	Regresión	3,524	1	3,524	16,104	0,000[b]
	Residual	6,347	29	,219		
	Total	9,871	30			
2	Regresión	3,942	2	1,971	9,309	0,001[c]
	Residual	5,929	28	,212		
	Total	9,871	30			
3	Regresión	5,232	3	1,744	10,151	0,000[d]
	Residual	4,639	27	,172		
	Total	9,871	30			
A) Variable dependiente: P10						
B) Variables predictoras: (Constante), Dim_contexto						
C) Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo						
D) Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo, Dim_planificacion						

Como el modelo de regresión que estamos trabajando es saber si las tres variables independientes están prediciendo la variable dependiente, entonces

nos quedamos con los resultados del último modelo (Modelo 3) que se muestra en la tabla ANOVA.

Aquí se observa que hay una significancia menor al 0.05 (0.00 ≤ 0.05) y la interpretación en términos de hipótesis es que el modelo que estamos probando mejora significativamente la predicción de la variable dependiente.

B. ANÁLISIS DE COEFICIENTE DE LA ECUACIÓN DE REGRESIÓN

COEFICIENTES								
MODELO		COEFICIENTES NO ESTANDARIZADOS		COEFICIENTES TIPIFICADOS	T	SIG.	ESTADÍSTICOS DE COLINEALIDAD	
		B	ERROR TÍP.	BETA			TOLERANCIA	FIV
1	(Constante)	,826	,779		1,059	,298		
	Dim_contexto	,829	,207	,598	4,013	,000	1,000	1,000
2	(Constante)	,534	,794		,672	,507		
	Dim_contexto	,550	,284	,396	1,933	,063	,511	1,958
	Dim_liderazgo	,358	,255	,288	1,405	,171	,511	1,958
3	(Constante)	,733	,719		1,019	,317		
	Dim_contexto	-,025	,331	-,018	-,075	,941	,306	3,270
	Dim_liderazgo	,277	,232	,223	1,199	,241	,502	1,990
	Dim_planificacion	,632	,231	,586	2,740	,011	,380	2,631
Variable dependiente: P10								

En la tabla de coeficientes siguientes se observa que nuestro modelo de regresión es:

$$Y = C_0 + C_1X_1 + C_2X_2 + C_3X_3 + E$$

$$Y = .733 - .025X_1 + .277X_2 + .632X_3 + E$$

De los coeficientes obtenidos concluimos que solo la variable Contexto de la Organización (X_1) no aporta en la explicación del modelo propuesto, porque su coeficiente es -.025.

De la misma tabla, también podemos observar los valores t y su significancia, que son valores que nos demuestran que tanto podemos generalizar el modelo de predicción a la población, son: t = -0.75, 1.199 y 2,740. La cual nos confirma que el modelo puede generalizarse a toda la población solo con las variables de Liderazgo (X_2) y de la variable de Planificación (X_3).

V. CONCLUSIONES, LIMITACIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

A partir del desarrollo del proyecto se concluye lo siguiente:

Se acepta la hipótesis propuesta ya que existe un 53% de la formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma peruana NTP-ISO/IEC 17799 planteado permita mejorar el grado de satisfacción en la gestión de la seguridad de la información en la Oficina Central de Cómputo (OCC) de la Universidad de Lambayeque.

Así mismo el modelo propuesto con las 3 dimensiones evaluadas, en la que se explica la varianza de la variable dependiente en 53%, señala que falta casi un 50% de explicación de la varianza de la variable dependiente, por lo que sería conveniente realizar otras investigaciones para encontrar otras dimensiones que explique mejor el modelo propuesto.

Según el diagnóstico de la situación actual de la seguridad de la información realizada, nos muestra que el nivel de cumplimiento de la UDL frente a los requerimientos de la NTP ISO/IEC 17799:2007, es del 30%, lo que significa que la implementación del Sistema de Gestión de Seguridad de la información le implicará a la institución un refuerzo considerable debido a la ausencia de controles o al bajo grado de cumplimiento de muchos de ellos.

Para que este proyecto tenga éxito, es de vital importancia que se defina formalmente el comité de Seguridad de la Información, órgano que debería encargarse del proyecto de implementación del SGSI y que deberá contar con el apoyo de la Universidad de Lambayeque; de modo que se facilite el acceso a la información de todas las áreas pertinentes.

Para contrarrestar la falta de concientización de seguridad de la información se deberá incluir sesiones de capacitación en las que se concientice al personal sobre la importancia de la información con la cual se realizan las labores institucionales, así como fomentar el cumplimiento de las políticas que garantice la seguridad de la misma.

Es probable que la implantación de las nuevas condiciones de empleo para los colaboradores antiguos sea recibida con rechazo dado que muchos de ellos se encuentran trabajando mucho tiempo en la institución y puedan percibir este cambio como una amenaza. Este posible obstáculo deberá ser debidamente manejado en conjunto con el área de recursos humanos.

5.2. LIMITACIONES

Como bien se indicó dentro del presente proyecto, el apoyo de la Alta Dirección es vital para el éxito de este tipo de proyectos, en este aspecto no hubo problemas pero si algunas demoras en la aprobación de algunos documentos importantes para la implementación del SGSI. Sin embargo si se recibió el apoyo necesario.

Se encontró una gran dificultad al no contar con la documentación correspondiente a los procesos que forman parte del alcance del proyecto lo que obligo a acordar varias reuniones con diferentes áreas de la UDL para el levantamiento de información de dichos procesos, los cuales de haber contado con la documentación, hubieran sido innecesarias.

Otro aspecto importante fue el número de reuniones que se realizaron con el área de sistemas y otras áreas que formaron parte del alcance de proyecto para concretar la definición de los distintos criterios usados en el proyecto, como también para la valorización que se realizaron en el mismo.

Adicionalmente, se pudo observar en la mayoría de áreas de UDL, el poco interés y la poca concientización que se tiene con respecto a la seguridad de la información dentro del personal operativo.

5.3. RECOMENDACIONES Y TRABAJOS FUTUROS

Para lograr una efectiva implementación del Sistema de Gestión de Seguridad de Información en la UDL, se recomienda seguir con los siguientes factores de éxito; en primer lugar seguir teniendo el apoyo constante de la Alta Dirección, segundo, seguir con el diseño del SGSI planteado, el cual se desarrolló a lo largo del proyecto; y tercero, generar conciencia en la institución. Este último aspecto no siempre se logra de inmediato, pues muchas personas se muestran reacias al cambio, lo que puede ocasionar inconvenientes en la implementación del SGSI.

Por ello, es necesario generar una cultura de seguridad dentro de la institución, es decir concientizar a cada colaborador de la importancia de sus actividades de seguridad de información y la manera de cómo contribuye a los objetivos del SGSI, se recomienda realizar capacitaciones permanentes a todo el personal de la UDL.

VI. REFERENCIAS BIBLIOGRAFÍCAS

Alcantara Flores, J. C. (2015). Guía de implementación de la seguridad basado en la norma ISO/IEC 27001. Obtenido de Comisaria del Norte P.N.P: http://tesis.usat.edu.pe/jspui/bitstream/123456789/491/1/TL_Alcantara_Flores_JulioCesar.pdf

Espinoza Aguinaga, H. R. (Octubre de 2013). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005. Obtenido de Pontificia Universidad Católica del Perú: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/4957/ESPINOZA_HANS_ANALISIS_SISTEMA_GESTION_SEGURIDAD_INFORMACION_ISO_IEC%27001_2005_COMERCIALIZACION_PRODUCTOS_CONSUMO_MASIVO.pdf?sequence=1

Gutierrez Rios, O. A. (2010). Historia y evolución del ISO 27000, ISO 17799. Obtenido de Universidad Nacional Sede Mizales: http://studylib.es/doc/845974/3.-historia-y-evoluci%C3%B3n-de-la-iso-serie-27000--iso-17799

Huáman Monzón, F. M. (Julio de 2014). Cumplimiento de la normal NTP-ISO/IEC 17799:2007. Obtenido de Pontifica Universidad Católica del Perú: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5582/HUAMAN_FERNANDO_AUDITORIA_NORMA_TECNICA_INSTITUCIONES.pdf?sequence=1

Jaramillo Islas, R. S. (01 de Diciembre de 2004). Marco de trabajo de ITIL y el estándar ISO/IEC-17799. Obtenido de Tecnólogico de Monterrey: https://repositorio.itesm.mx/ortec/bitstream/11285/572230/1/DocsTec_1977.pdf

Mancera, S. C. (2011). Perspectivas sobre los riesgos de TI. Obtenido de Seguridad de la información en un mundo sin fronteras: http://www.aenorperu.com/seguridad-de-la-informaci%C3%B3n.aspx

Mezones Flores, Y. K., & Tineo Requejo, D. (2015). Politicas de seguridad organizacional y control de activos. Obtenido de Deltron S.A.: http://repositorio.unprg.edu.pe/handle/UNPRG/179

Orellana P., J. B., & Villaroel V., C. F. (01 de Abril de 2012). Derechos de autoría. Obtenido de Escuela superior politécnica de Chimborazo: http://dspace.espoch.edu.ec/bitstream/123456789/1943/1/98T00013.pdf

Pallas, G. (2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Sistemas de gestión de seguridad informática. Montevido, Uruguay.

Proveda, J. M. (s/a). Auditoria Informatica. Auditoria. Universidad del Norte.

Wenceslao, C., Vasquez Montenegro, J. C., & De la Cruz Guerrero. (2008). Elaboración y aplicación de un Sistema de Gestión de la Seguridad de la Información para la realidad Tecnólogica de la USAT. Gestión de la Seguridad de la información . Chiclayo: Universidad Catolica Santo Toribio de Mogrovejo.

Yan Carranza, F., & Zavala Velasquez, C. L. (27 de Febrero de 2013). Lineamientos ISO 27001 y buenas prácticas COBIT. Obtenido de Universidad privada Antenor Orrego: http://repositorio.upao.edu.pe/bitstream/upaorep/645/1/YAN_FREDDY_MEJORA_SEGURIDAD_COBIT.pdf

FORMATO DE ENCUESTA.

CARTA DE PRESENTACIÓN

Chiclayo, Agosto 2017

Estimado Sr. (a) (ita):

Le presentamos nuestro saludo y a la vez solicitarle su apoyo respondiendo la presente encuesta que permitirá realizar el trabajo de campo de nuestra investigación, relacionada con el sector educativo - universitario.

Le informamos que es un cuestionario diseñado estrictamente con los parámetros de investigación, por lo tanto, respetando los principios de la investigación científica los datos consignados en cada encuesta son de absoluta reserva.

Las interrogantes han sido diseñadas para que usted marque con una "X" el nivel de intensidad según considere por interrogante, aquí presentamos un ejemplo:

PREGUNTA	NIVEL DE INTESIDAD
1. Cree usted que es muy importante la seguridad de la información	Muy desacuerdo 1 | 2 | 3 | 4 | Fuertemente de acuerdo 5

NOTA: Responder todas las preguntas, caso contrario invalidaría la encuesta.

Agradecidos por la atención nos despedimos de usted.

Atentamente;

Bach. Erick W. Guevara Saldaña.

Bach. Frankz Olivos Guerra.

UNIVERSIDAD DE LAMBAYEQUE
FACULTAD DE CIENCIAS DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPORTANTE: CONTESTAR TODAS LAS PREGUNTAS, DEJAR UNA DE ELLAS SIN CONTESTAR INVALIDA LA ENCUESTA

PREGUNTA	NIVEL DE INTESIDAD
1. Usted considera que el Sistema de Gestión de Seguridad de la Información se adecuada a la estructura organizativa, a la normativa interna y a los procesos internos de la UDL.	Muy en desacuerdo 1 | 2 | 3 | 4 | Fuertemente de acuerdo 5
2. El SGSI propuesto permite satisfacer las necesidades y expectativas de las partes interesadas en la gestión de la seguridad de la información.	Muy en desacuerdo 1 | 2 | 3 | 4 | Fuertemente de acuerdo 5
3. Usted está conforme del modo como se determinó el alcance del Sistema de Gestión de Seguridad de la Información propuesto.	Muy en desacuerdo 1 | 2 | 3 | 4 | Fuertemente de acuerdo 5
4. En qué grado usted cree que el SGSI propuesto cumple con las exigencias o los requisitos de la Norma Técnica Peruana 17799.	Muy en desacuerdo 1 | 2 | 3 | 4 | Fuertemente de acuerdo 5
5. Cree usted que en el SGSI propuesto se han establecido con claridad los liderazgos y compromisos para un adecuado gobierno de la seguridad de	Muy en desacuerdo 1 | 2 | 3 | 4 | Fuertemente de acuerdo 5

la información en la UDL.	
6. Usted cree que la declaración de las políticas de seguridad en el SGSI permite establecer los objetivos de seguridad y permite la mejora continua del mismo.	Muy en desacuerdo 1 | 2 | 3 | 4 | Fuertemente de acuerdo 5
7. Usted cree que los roles, responsabilidades y autoridades organizacionales del SGSI son adecuadas para la gestión de la seguridad de la información en la UDL.	Muy en desacuerdo 1 | 2 | 3 | 4 | Fuertemente de acuerdo 5
8. Considera usted que se definió y aplico adecuadamente un proceso de valorización del riesgo de seguridad de la información	Muy en desacuerdo 1 | 2 | 3 | 4 | Fuertemente de acuerdo 5
9. Usted cree que los objetivos de seguridad de la información y su plan de ejecución planteados en el SGSI son adecuados para la gestión de la seguridad de la información en la UDL.	Muy en desacuerdo 1 | 2 | 3 | 4 | Fuertemente de acuerdo 5
10. Según usted cuál es su nivel de satisfacción de que los dominios del SGSI propuesto logra mejorar la gestión de la seguridad de la información	Muy en desacuerdo 1 | 2 | 3 | 4 | Fuertemente de acuerdo 5