Tipo de artículo: Artículo original

Plan estratégico de seguridad informática para la protección de los recursos informáticos en el laboratorio de telecomunicaciones

Strategic plan for computer security for the protection of computer resources in the telecommunications laboratory

Julio Pedro Paladines Morán [1*], **https://orcid.org/0000-0002-8121-3360**
Grace Liliana Figueroa-Morán [2], **https://orcid.org/0000-0003-2520-765X**
José Nevardo Paladines Morán [3], **https://orcid.org/0000-0003-1991-1894**

[1] Universidad Estatal del Sur de Manabí, Jipijapa Ecuador. julio.paladines@unesum.edu.ec
[2] Universidad Estatal del Sur de Manabí, Jipijapa Ecuador. grace.figueroa@unesum.edu.ec
[3] Universidad Estatal del Sur de Manabí, Jipijapa Ecuador. jose.paladines@unesum.edu.ec

*** Autor para correspondencia: julio.paladines@unesum.edu.ec**

Resumen

La nueva sociedad del conocimiento propone el plan estratégico de seguridad informática para la protección de los recursos informáticos se basa en la estrategia de innovación en la enseñanza aprendizaje, para la recolección, análisis e integración de datos que permita de una manera eficaz optimizar se basa en la elaboración del diseño de un plan estratégico, que permitirá describir y solucionar una necesidad en cuanto a la seguridad informática del laboratorio de telecomunicaciones en el que se mejoraran los métodos, y políticas para la protección de los recursos y equipos informáticos que se encuentren a disposición del laboratorio de telecomunicaciones de la Carrera de Tecnologías de la Información. Actualmente la Universidad Estatal del Sur de Manabí tiene a su disposición diferentes equipos tecnológicos por ende se necesitan medidas y contravenciones para asegurar la disponibilidad de esos recursos en todo momento. Las metodologías cuantitativa y cualitativa fueron recursos importantes para realizar esta investigación y en base a los datos recogidos se realizaron tabulaciones permitiendo así descubrir la necesidad y seleccionar la mejor opción para resolverla. Este proyecto mantiene un cronograma previamente analizado y cumplido en el lapso estipulado además de que contó con un recurso económico propiamente del autor.

Palabras clave: Disponibilidad; Seguridad; Informática; Recursos; Contravenciones; Disposición.

Abstract

The new knowledge society proposes the strategic plan for computer security for the protection of computer resources is based on the innovation strategy in teaching-learning, project is based on the design of a strategic plan, which will describe and solve a need in terms of computer security of the telecommunications laboratory in which the methods will be improved, and policies for the protection of resources and computer equipment that is available to the laboratory of the Computer and Network Engineering Career. Currently, the State University of the South of Manabí has different technological equipment at its disposal, therefore measures and contraventions are needed to ensure the availability of these resources at all times. The quantitative and qualitative methods were important resources to carry out this research and, based on the collected data, tabulations were made, allowing us to discover the need and select the best option to solve it. This project maintains a chronogram previously analyzed and completed within the stipulated period, in addition to having an economic resource of the author's own.

Keywords: *Availability*; *Security*; *Computing*; *Resources*; *Contraventions*; *Disposition.*

Recibido: 02/04/2021
Aceptado: 03/09/2021

Introducción

La última década ha marcado la forma de vivir y pensar de la sociedad, debido al acelerado avance de las Tecnologías de la Información y la Comunicación, las cuales se han hecho presentes en todas las áreas del conocimiento humano. La seguridad informática hace referencia a la seguridad de la información, que se basa en principios básicos que son proteger la confidencialidad, integridad e incluso la disponibilidad de la información de una organización o institución.

Tal es el caso que para una buena seguridad de la información se debe proteger tres elementos principales, que son: la información, equipos y usuarios. Con respecto a la información, esta es la entidad más importante de la empresa o institución; en los equipos se debe proteger lo que es el hardware y software; y, en lo que concierne a los usuarios se refiere a las personas que hacen uso de la tecnología de la empresa.

Si bien es cierto, para dar inicio al diseño de un plan estratégico de seguridad, hay que tener presente lo siguiente ¿Qué es lo que se requiere proteger y con qué nivel de seguridad lo queremos hacer?, obviamente que la información será protegida con el mejor y más alto nivel de seguridad.

En la actualidad los equipos informáticos son herramientas muy usadas y necesarias para las empresas, organizaciones e instituciones, donde se generan gran cantidad de información. Sin embargo, el uso de las tecnologías en las empresas pone en riesgo la información de la misma, es allí donde se debe implementar técnicas para proteger la integridad de los recursos informáticos a la vez la privacidad de la información, para así evitar daños o pérdidas de datos, ya que esa es el alma de la institución.

Por otra parte, la información se protege con seguridad lógica, por ende; se aplican barreras y procedimientos que resguardan al acceso a la misma así mismo restringir el acceso a usuarios autorizados. Tal es el caso que es necesario la implementación de ciertas medidas técnicas en el laboratorio de telecomunicaciones las cuales resguardan las infraestructuras de comunicación que lleva la operación de dicho laboratorio, al hablar de eso se refiere a la parte física y lógica de equipos informáticos que se encuentran dentro del laboratorio ya mencionado.

Formulación del problema

En la actualidad el laboratorio de telecomunicaciones de Ingeniería en Computación y Redes no cuenta con un plan estratégico de seguridad informática para la protección de los recursos informáticos en el laboratorio de telecomunicaciones y es aquí donde nace esta necesidad la cual es imprescindible del diseño del mismo para mantener la información con un alto grado de seguridad.

Teniendo en cuenta los elementos antes planteados, se define como problema de la investigación: ¿De qué manera beneficiaria el diseño de un plan estratégico de seguridad informática para la protección de los recursos informáticos en el laboratorio de telecomunicaciones de la Carrera de Tecnologías de la Información (TI)?

De la definición del problema de la investigación se derivan las siguientes preguntas:

- ¿Cuál será el impacto que tendrá el diseño de un plan estratégico de seguridad informática para la protección de los recursos informáticos en el laboratorio de telecomunicaciones de la Carrera de TI?
- ¿Cómo contribuye el diseño de un plan estratégico de seguridad informática para la protección de los recursos informáticos en el laboratorio de telecomunicaciones a la Carrera de TI?
- ¿De qué manera el diseño de un plan estratégico de seguridad informática permitirá proteger los recursos informáticos del laboratorio de telecomunicaciones de la Carrera de TI. ?

El objetivo de la presente investigación es el diseño de un plan estratégico de seguridad informática para la protección de los recursos informáticos en el laboratorio de telecomunicaciones de la Carrera de Tecnologías de la Información. El desarrollo del mismo tiene como objetivo llevar una adecuada gestión de la seguridad de la respectiva información y evitar incidentes que puedan perjudicar la operación del laboratorio antes mencionado.

Materiales y métodos

Las investigaciones que son del tipo aplicada, “se caracterizan porque busca la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la práctica basada en investigación. El uso del conocimiento y los resultados de investigación que da como resultado una forma rigurosa, organizada y sistemática de conocer la realidad” (Vargas Cordero, 2009).

Una investigación de nivel descriptivo, estudia y mide conceptos o variables con el objetivo de describirlas; por lo que podría decirse que en forma general describen algunos fenómenos. Su objetivo central es principalmente medir de

forma precisa una o más variables, de una población en específico o una muestra de esa población. “Los estudios descriptivos sirven para analizar cómo es y se manifiesta un fenómeno y sus componentes; pueden ofrecer también la posibilidad de hacer predicciones incipientes, aunque sean rudimentarias.” (Cazau, 2006).

Para la presente investigación se define como hipótesis: El diseño de un plan estratégico de seguridad informática permitirá proteger los recursos informáticos en el laboratorio de telecomunicaciones de la Carrera de TI.

La metodología utilizada en este proyecto se basa en los métodos cualitativo y cuantitativo en el cual se recogieron y se analizaron datos para conocer una realidad que es el punto principal de esta investigación, además se utilizaron métodos inductivos y deductivos para obtener un análisis de la teoría previamente investigada.

En este trabajo se emplearon métodos teóricos y empíricos de la investigación científica, como se listan a continuación:

- **Hipotético-deductivo:** A través de este método se desarrolló la investigación, en base a información de fuentes externas se permitió determinar un conjunto de teorías para cumplir los objetivos del proyecto de la misma manera se desarrolló la hipótesis de este proyecto.
- **Exploratorio:** Se realizó la propuesta en base a las normas establecidas con el que se desarrolló el plan estratégico de seguridad informática para la protección de los recursos informáticos en el laboratorio de telecomunicaciones de la carrera de ingeniería en computación y redes solucionando el problema previamente establecido.
- **Estadístico**: Con este método se realizaron las tabulaciones para obtener resultados de las encuestas y entrevistas realizadas a los estudiantes de la Carrera de TI.
- **Documental:** Este método permitió documentar toda la información obtenida mediante las encuestas y entrevistas realizada a los estudiantes de la Carrera de TI.

Las técnicas utilizadas en este proyecto de investigación son las siguientes:

- **Encuesta:** Se utilizó esta técnica mediante la selección de un conjunto de preguntas en forma de cuestionario y que se les realizo a los estudiantes de la Carrera de TI.
- **Observación**: Esta técnica se utilizó para determinar el problema de este proyecto y las soluciones que se describirán en el plan estratégico mediante un conjunto de políticas y normas.

Plan estratégico de seguridad informática

De acuerdo a (Sinnexus, 2016) un plan estratégico es un programa constituido por un documento formal que rigen políticas, normas, procedimientos, donde se plasma la visión que una organización o una empresa pretende alcanzar a largo plazo obteniendo resultados positivos en un futuro. Por lo consiguiente las estrategias que presiden este plan son de vital importancia debido a que su función principal es organizar, dirigir, motivar y comunicar a las personas encargadas de ejecutar este documento.

Además, un plan estratégico ofrece el diseño y la construcción de la misión y visión que proyecta cumplir la organización mediante las acciones impuestas en dicho plan. Asimismo, es el conjunto de análisis, decisiones y acciones que se deben ejecutar en una organización para crear y mantener ventajas comparativas sostenibles a lo largo del tiempo.

Para (Díaz, 2013) "El plan estratégico es un documento integrado en el plan de negocio que recoge la planificación a nivel económico-financiera, estratégica y organizativa con la que una empresa u organización cuenta para abordar sus objetivos y alcanzar su misión de futuro."

De igual forma el desarrollo y ejecución de un Plan Estratégico está relacionado con la seguridad ya que tiene como finalidad establecer los procedimientos para llevar adelante la organización además avalar una correcta gestión de la seguridad de la información y mitigar los sucesos que podrían afectar las actividades de la misma.

Un plan estratégico en una institución sirve de apoyo en muchos aspectos relacionados con la eficiencia y capacidad para desarrollar las tareas y tomar medidas de precaución cuando ocurra un suceso inesperado, todos estos aspectos en concreto se basan en un objetivo que es el de asegurar y precautelar el bienestar de la empresa como de sus empleados.

Fases de un plan estratégico

Por lo general, todo plan estratégico se compone de las siguientes fases como indica (Manrique, 2016)

Análisis de la situación: analizar lo que ocurre internamente y externamente en la institución, así conocer la realidad en la que opera la organización.

- **Diagnóstico de la situación:** permite conocer las condiciones actuales en la que se desempeña la organización.
- **Declaración de objetivos estratégicos:** son los puntos futuros que se deben cumplir, por ende, deben ser cuantificables, medibles y reales.

- **Estratégica corporativa:** se basa a las necesidades de las empresas para responder a las necesidades del mercado interno o externo.
- **Planes de actuación:** Son planes integrados por los objetivos, las políticas y la secuencia de las principales acciones de una organización en un todo coherente.
- **Seguimiento:** esta etapa el permite el monitoreo, control y evaluación de la aplicación de las estrategias corporativas en las distintas organizaciones, es decir, se permite el conocimiento de la manera en que se vienen aplicando y desarrollando las estrategias.
- **Evaluación:** se miden los resultados y se verifica como se cumplen los objetivos que fueron planteados.

Modelo de plan estratégico

Como indica (FMK, 2016), es fundamental tener conocimiento sobre los modelos de un plan estratégico, para tener la visión de cómo trabaja y de cómo se puede optimizar la situación dentro de la organización, ya que los modelos estratégicos se centran en verificar nuevas representaciones con la finalidad de operar efectivamente.

El modelo de un plan estratégico ayuda a minimizar el impacto de amenazas externas, asimismo, permite utilizar las fortalezas internas con el objetivo de refrenar las amenazas internas dentro de una organización, efectuando estrategias pertinentes para corregir y mejorar los resultados, para así, alcanzar los objetivos propuestos.

Fases de un modelo de un plan estratégico

Según (Romero 2014), el modelo o proceso de plan estratégico se puede sintetizar en doce pasos, para realizar un análisis interno o externo de la organización:

Establecer los objetivos, estrategias y la misión actual.

- Realizar un sondeo externo con el fin de identificar amenazas y oportunidades ambientales.
- Realizar un sondeo interno con el objeto de identificar fortalezas y debilidades de la empresa.
- Fijar la misión de la empresa.
- Llevar a cabo análisis de formulación de estrategias con el objeto de generar y evaluar alternativas factibles.
- Fijar objetivos.
- Fijar estrategias.
- Fijar metas.
- Fijar políticas.

- Asignar recursos.
- Analizar bases internas y externas para estrategias actuales.
- Medir resultados y tomar las medidas correctivas del caso.

Plan estratégico de seguridad informática

Según (Pajaro & Vergara, 2014) un plan estratégico informático es una herramienta que sirve de guía para los usuarios que manipulan el sistema, además está compuesto por múltiples procedimientos, reglas y políticas integradas en un documento con el fin de satisfacer las necesidades de captación, registro y procesamiento de datos de un sistema.

Un plan estratégico informático beneficia a la unidad informática de una institución o empresa pública o privada, permitiendo mantener de manera seguir los activos informáticos basándose en un conjunto de políticas, normas y estándares destinados a evaluar y minimizar los riesgos que se puedan presentar en un futuro. La elaboración de dicho plan informático debe diseñarse de acuerdo a las características, actividades, funciones y acorde a la tecnología que maneje la institución.

Etapas de plan estratégico de seguridad informática

Para el desarrollo de un plan estratégico de seguridad informática se distingue tres etapas que permite, prevenir, detectar y responder a cualquier amenaza que afecte el proceso informático de la organización. A continuación, se detallan cada una de las fases:

Evaluación de riesgos

La evaluación de riesgos informáticos es el procedimiento por el cual se identifican los activos informáticos y se determina las vulnerabilidades y amenazas a las que se encuentran exhibidas, con el objeto de establecer controles específicos para aceptar, disminuir, transferir y evitar la ocurrencia del riesgo (Lema, 2016).

Se puede identificar el origen de los riesgos potenciales a los que no está exenta la organización y de la misma manera cuantificarlos para que los encargados o administradores puedan contar con la información adecuada para optar por el diseño e implementación de controles de seguridad y todo esto se puede ejecutar gracias a la evaluación de riesgos.

Ferrer, (2016), expresa que dentro de la evaluación de riesgos se debe considerar la probabilidad de una amenaza y la magnitud de impacto que puede tener el sistema, además para realizar una valoración de riesgos se deben realizar los pasos: identificar y analizar los riesgos. A continuación, se detallan cada uno de ellos:

Identificar los riesgos

La misión de esta fase es descubrir, reconocer y registrar los riesgos que afectan a la organización, es decir, identificar las causas y origen de las amenazas que pueden tener gran impacto para el cumplimiento de los objetivos de la organización.

De acuerdo a (Sonia Cienfuegos, 2016), hay varios métodos que se emplean para identificar los riesgos, dentro de los cuales podemos mencionar los siguientes:

- **Métodos basados en evidencias:** se refiere a las listas de verificación y a revisiones de datos.
- **Enfoques sistemáticos de equipos**: expertos aplican preguntan estructuradas para identificar riesgos.
- **Técnicas de razonamiento inductivo:** aplicando el método HAZOP.

Análisis de riesgos

Esta etapa determina las consecuencias y probabilidades, las partes más débiles de la infraestructura tecnológica, por lo que es importante para la implementación de un plan estratégico. “Define si es necesario implementar esquemas de recuperación de desastres; provee una guía para las medidas de protección que son viables con respecto al costo; y, permite obtener información sobre los activos (Tapias, 2013).

Figura 1: Esquema del análisis de riesgo.

Fuente: https://sites.google.com/site/misitiowebnmqp/3-fundamentacion/a-humanos-básicos

Recursos informáticos

Según (Prada, 2016) indica que los recursos informáticos son componentes de hardware y software que son empleados para la conformación de un sistema informático el cual está constituido por computadoras, periféricos y programas que trabajan en conjunto para garantizar el funcionamiento de los mismos.

Los recursos informáticos son elementos tecnológicos que se pueden encontrar en todo tipo de organizaciones o instituciones que trabajen con sistemas de información, complementan la mayor parte de la infraestructura comprendida en redes, laboratorio de cómputo, y área de servidores.

(Quitian, 2017) Señala cuando se utilizan recursos informáticos en una empresa se debe trabajar con mucha precaución, debido a que contienen información importante y esta puede ser filtrada por medio de ataques informáticos. Por esta razón se necesita la seguridad informática.

El uso de los recursos informáticos conlleva a la protección de los mismos, debido a que pueden contener información relevante asegurando la integridad y privacidad de los recursos, permitiendo que solo personas autorizadas tengan acceso a la modificación de los datos y así minimizar riesgos y amenazas tanto físicos como lógicos a la que se encuentre expuesta dichos recursos.

Por otra parte (Tool, 2017) afirma que la seguridad informática es una rama de la ingeniería de sistemas que se encarga de organizar, ordenar, clasificar y coordinar las acciones para proteger la integridad y la privacidad de la información ante cualquier ataque por hacker o virus informático.

Normas / Estándares Internacionales

Según ISOTools – Software de Gestión para la Excelencia Empresarial, (2015), la información es parte vital de toda organización por lo que se lo considera como la columna vertebral, por ello debe ser protegida ante cualquier amenaza aplicando normas o estándares de seguridad.

Por ello, a continuación, se describen algunas normas y estándares internacionales de alto nivel relacionados a la seguridad informática, con el objeto, de evitar vulnerabilidades en los sistemas y también para que más adelante sirvan de guía para el desarrollo de un plan estratégico de seguridad informática aplicado a un laboratorio de cómputo.

ISO/IEC 27001

La institución de estándares británico BSI, (2017), afirma que ISO 27001 es una norma internacional que regula la SGSI – Sistema de Gestión de Seguridad de la Información, ya que permite asegurar de manera más eficiente los datos financieros y confidenciales dándole la oportunidad a las organizaciones a desarrollarse e innovar cada día, y de esta forma minimizar los riesgos de acceso ilegales o sin autorización.

La principal función de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información de toda organización, realizando un análisis mediante la evaluación de riesgos para verificar los principales problemas

que pueden afectar los datos, luego aplicar los mecanismos de seguridad para el tratamiento o corrección de los riesgos. Sin embargo, para Segovia, (2017), la filosofía principal de ISO 27001 se basa en la gestión de riesgo:

Figura 2*:* Estructura de ISO 27001

Fuente: (Segovia, 2017)

Aseguramiento de la calidad

La calidad comprende la mejora de forma permanente con respecto a la eficacia y eficiencia de las organizaciones y sus procesos, así como también a la opinión del cliente respecto a su producto o servicio. Los procesos se deben planificar, depurar y controlar para que mejore el rendimiento de la empresa. Pero también se debe tener en cuenta la opinión del usuario sobre el producto o servicio, por lo que se debe hacer investigaciones acerca de esto cada cierto tiempo.

La calidad depende de la manera en la que la empresa realiza sus procesos, lo cual afecta directamente en la opinión que el cliente tiene del producto o servicio, estos procesos pueden ser la contratación de empleados, contrataciones, compras, *outsourcing*, mantener y controlar los servicios, capacitación del personal, detectar y corregir fallas, entre otros.

Todo esto, sumado al entorno cambiante en el que vivimos, donde la tecnología se desarrolla de una manera acelerada, y los competidores mejoran continuamente, hace que las necesidades de los clientes evolucionen, haciendo más difícil para las empresas el poder satisfacerlo.

Es por esto que los sistemas de gestión de calidad se están desarrollando cada vez más, y cobrando una mayor importancia, ya que permiten una vista panorámica y una rápida adaptación a los entornos cambiantes del mercado.

Norma ISO 9001

Luego de haber visto términos con respecto a la calidad y a los sistemas de gestión de calidad, se verá la norma ISO 9001 que corresponde al uso de las tecnologías de información, para lograr implementar sistemas de gestión de calidad.

En la actualidad se exige continuamente más eficiencia para gestionar recursos, es por eso que Universidades Nacionales están empezando a aplicar la implementación de estos sistemas en la serie de Normas ISO 9000. "En la versión más reciente de la Norma ISO 9001, que data del año 2015, se realizaron algunas modificaciones que permiten obtener una mejoría notable en la gestión, y esto se puede apalancar utilizando inteligentemente las Tecnologías de la Información y las Comunicaciones." (Martínez & Faraldi).

Resultados y discusión

La siguiente encuesta estuvo dirigida a los estudiantes de la Carrera de TI, con el objetivo de conocer la factibilidad y los niveles de aceptación para realizar este proyecto. Está conformada de un conjunto de preguntas realizadas y seleccionadas para identificar la problemática y obtener una solución.

¿Cree usted que el laboratorio de telecomunicaciones cuenta con normas y estándares de seguridad informática?

Tabla 1. Respuesta a la pregunta sobre normas y estándares.

Opciones	Frecuencia	Porcentaje
Sí	23	18%
No	102	82%
Total	125	100%

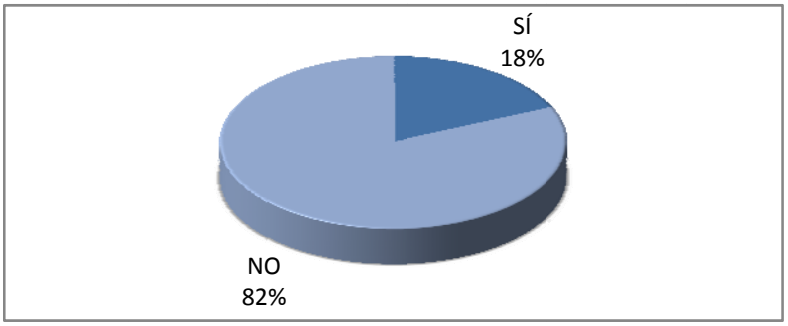

Figura 3: Respuesta a la pregunta sobre normas y estándares.

En la figura 3 el resultado de la primera pregunta de la encuesta referente a si el laboratorio de telecomunicaciones cuenta con normas de seguridad, 102 que representan el 82% de la muestra, respondieron que no, demostrando así

que no tienen conocimiento sobre la existencia de normas y estándares de seguridad en el laboratorio de telecomunicaciones, 23 estudiante encuestados que comprende el 18% de la muestra contestaron si conocen, pero demuestran dudas. Con esto se conoce que el desarrollo del plan estratégico de seguridad informática es necesario para proponer las normas y estándares que necesita el laboratorio.

1. ¿Conoce usted sobre las normas y estándares para la seguridad informática que se aplican en un laboratorio de informática?

Tabla 2: Respuesta a la pregunta sobre Seguridad Informática

Opciones	Frecuencia	Porcentaje
Sí	26	21%
No	2	2%
Poco	97	77%
Total	125	100%

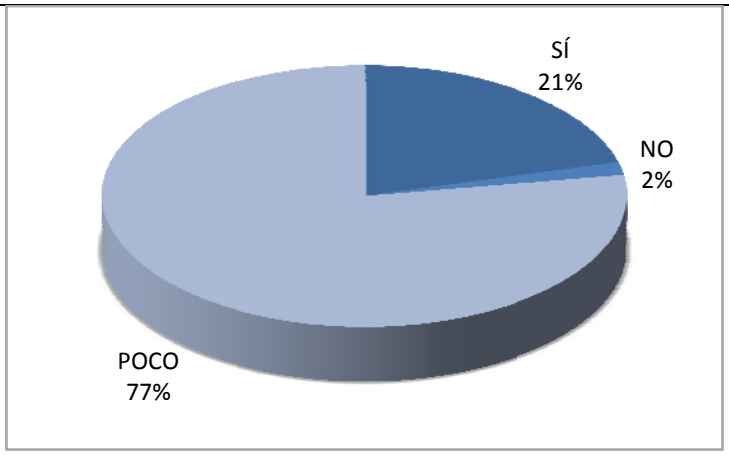

Figura 4: Respuesta a la pregunta sobre Seguridad Informática.

Análisis e interpretación: Como resultado de la segunda pregunta de la encuesta referente sobre el conocimiento de normas y estándares se obtuvieron los siguientes resultados, del total de la muestra el 21% que comprende a 26 estudiantes respondieron que, sí conocen, el 77% indicó que conocen muy poco las normas y estándares y el 2% indicó que no. Por lo que se refleja claramente que existen dudas y que no están claras todos los puntos que se deben aplicar para la seguridad informática en el laboratorio de telecomunicaciones, por lo que el desarrollo de este proyecto permitirá reforzar los conocimientos referentes a la seguridad informática.

Formulación de Estrategias

Para el desarrollo de las estrategias del laboratorio de telecomunicaciones de la Carrera de TI. Cuenta con recursos informáticos que están a disposición de los estudiantes y los docentes quienes imparten sus clases. Todas estas tecnologías se mantienen en un uso constante por lo que se necesitas monitorear periódicamente para prevenir que existan daños tanto en el hardware como el software.

Se ha tomado en cuenta la guía PMBOK, la cual menciona los procesos en la planificación, gestión y control de los requisitos de calidad del proyecto y del producto, para cumplir con los objetivos de negocio de la organización. Además, se ha considerado realizar un diagnóstico antes de realizar la planificación, gestión y control. También se incluye la medición de madurez que tiene cada proceso, según el CMMI, para alcanzar la optimización es estos.

A partir de lo antes mencionado se tendrán cuatro procesos para el aseguramiento de calidad, los cuales son: Diagnóstico de calidad, planificación de calidad, aseguramiento de calidad y control de calidad. Estos procesos tienen sus respectivas entradas, herramientas y técnicas, y salidas. Las salidas de cada proceso alimentarán las entradas.

Comprobación y discusión de los resultados obtenidos

El modelo de Estrategias propuesto gestiona y controla los procesos de una organización para el Aseguramiento de la Calidad, ya que integra prácticas de los procesos para:

- Diagnosticar si se está asegurando la calidad.
- Planificar la calidad.
- Asegurar la calidad.
- Controlar la calidad.

Mediante encuestas para medir el Nivel de Aceptación de los formatos propuestos para el Modelo de Estrategias TICs, se pudo observar que, con relación a Aspectos Generales del Modelo, el 55% de los entrevistados (colaboradores de la empresa 1) opinaron que es Excelente, debido a que proporciona formatos adecuados y entendibles, el 15% dijo que los formatos eran Regulares y no cumplen con los objetivos de las estrategias.

Los recursos que se utilizan para realizar este proyecto fueron inversión propia del autor por lo que son gastos considerablemente menores. Además, en un periodo a largo plazo este proyecto permitirá ahorrar gastos en equipos que sufran desperfectos por no ser manipulados de manera correcta.

Mediante un análisis de costos en base al presupuesto se comprueba que todos los recursos son utilizados completamente obteniendo una excelente relación costo/beneficio y de la misma manera al aplicar el proyecto se obtendrán una disminución de gastos y perduración de los equipos.

La Carrera de TI. Posee un laboratorio de telecomunicaciones en el que se encuentra un sistema informático compuesto por diferentes equipos tecnológicos. En el mismo no existe un plan estratégico de seguridad informática por lo que este proyecto se justifica desde el punto de vista tecnológico, con el fin de brindar un plan estratégico de seguridad informática para proteger los equipos que se encuentran en el laboratorio.

Los beneficiarios directos son los estudiantes y los docentes de la Carrera de TI, que mediante el uso correcto de las pautas, políticas y normas descritas en el plan estratégico de seguridad informática se asegurará la protección de los equipos y contribuirá con el desarrollo y calidad de la educación para futuras generaciones.

Conclusiones

Se realizó el inventario de los recursos informáticos con los que cuenta actualmente el laboratorio de telecomunicaciones en el que se describieron puntos importantes como sus características y detalles técnicos para la elaboración del plan estratégico.

Se identificó el estado actual de los recursos informáticos mediante un estudio de funcionamiento de cada equipo en el que se concluyó que los recursos informáticos no contaban con un plan estratégico de seguridad informática.

Se elaboró el plan estratégico de seguridad informática para la protección de los recursos informáticos del laboratorio de telecomunicaciones de manera correcta y detallada en base a la norma ISO 207001:2013, el cual se implementó en conjunto con el software libre Adware

Recomendaciones

Después de haber culminado con la investigación, se proponen las siguientes recomendaciones:

- Implementar nuevas herramientas tecnológicas de seguridad informática y actualizar constantemente los softwares que usan los equipos para evitar que se vuelvan obsoletas para aumentar su tiempo de vida y mantener actualizado el laboratorio.

- Mantener el laboratorio en constante mantenimiento para que los equipos se encuentren siempre funcionales y en buen estado, asegurando la continuidad de los recursos informáticos y evitar vulnerabilidades que puedan afectar a toda la institución.
- Aplicar el plan estratégico de seguridad informática de manera que se motive a los estudiantes a seguir las políticas y cuidar el espacio de trabajo mediante anuncios o señales en el interior del laboratorio de telecomunicaciones.

Conflictos de intereses

Los autores de la investigación declaran que no existe conflicto de intereses.

Contribución de los autores

1. Conceptualización: Julio Pedro Paladines Morán, Grace Liliana Figueroa-Morán, José Nevardo Paladines Morán.
2. Curación de datos: Grace Liliana Figueroa-Morán, José Nevardo Paladines Morán.
3. Análisis formal: Julio Pedro Paladines Morán.
4. Adquisición de fondos: Grace Liliana Figueroa-Morán, José Nevardo Paladines Morán.
5. Investigación: Julio Pedro Paladines Morán.
6. Metodología: Julio Pedro Paladines Morán.
7. Administración del proyecto: José Nevardo Paladines Morán.
8. Recursos: Grace Liliana Figueroa-Morán, José Nevardo Paladines Morán.
9. Software: Grace Liliana Figueroa-Morán, José Nevardo Paladines Morán.
10. Supervisión: Julio Pedro Paladines Morán.
11. Validación: Julio Pedro Paladines Morán.
12. Visualización: Julio Pedro Paladines Morán.
13. Redacción – borrador original: Julio Pedro Paladines Morán, Grace Liliana Figueroa-Morán, José Nevardo Paladines Morán.
14. Redacción – revisión y edición: Julio Pedro Paladines Morán, Grace Liliana Figueroa-Morán, José Nevardo Paladines Morán.

Financiamiento

La investigación fue financiada por los autores.

Referencias

Alvarado, V. C. (Enero de 2013). Plan de seguridad de la información basado en el estándar ISO 13335 aplicado a un caso de estudio. Obtenido de Repositorio de la Escuela Politécnica Nacional: http://bibdigital.epn.edu.ec/bitstream/15000/5617/1/CD-4645.pdf

Amaya, C. G. (14 de Mayo de 2013). MAGERIT: metodología práctica para gestionar riesgos. Obtenido de WeliveSecurity: https://www.welivesecurity.com/la-es/magerit-metodologia-practica-para-gestionar-riesgos/

Aparici, J. G. (2017). Seguridad informática - Tecnologías de la Información y Comunicación. Ecuador - Ambato: PublicacionesDidácticas.

Arrieta, I. A. (2013). Políticas y normas de seguridad informática. CVS.

Aula Virtual FCEQyN. (2016). Metodologías de Control Interno, Seguridad y Auditoría Informática. Obtenido de http://www.aulavirtual-exactas.dyndns.org/claroline/backends/download.php?

Barrera, C. R. (2014). Metodologías Para el análisis de riesgos en los sgsi. Tunja, Boyacá, Colombia: Fundación Universitaria Juan de Castellanos.

Bautista, A. (2013). Aplicación de estándares de protección de la información. Lima.

BSI. (2017). Seguridad de la Información ISO/IEC 27001. Obtenido de Instutición de estándares británicos : https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion

Cruz, C. (06 de Diciembre de 2014). Metodologías Coras para el análisis de riesgos. Obtenido de http://camilo-cruz-ucatolica-riesgos.blogspot.com/2014/12/coras.html

DELTA. (2016). Planeación Estratégica de Tecnología Informática. Argentina: DeltaAsesores.

Díaz, A. (15 de Diciembre de 2013). Qué es y cómo se hace un Plan Estratégico. Obtenido de http://www.blogtrw.com/2011/12/que-es-y-como-se-hace-un-plan-estrategico/

Ferrer, R. (2016). Metodología de análisis de riesgo. Bogota - Colombia: SISTESEG.

FMK. (29 de Junio de 2016). Cómo elaborar el Plan Estratégico de una empresa. Obtenido de ForoMarketing.com: https://www.foromarketing.com/libros-de-marketing/

Gómez, R., Pérez, D. H., & Donoso, Y. (2013). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. SCielo, 112.

Guarniz, E. H. (2017). Caracterícticas y proceso de la planeación estratégica. Lima: Universidad Privada del Norte.

Gutiérrez, J. D., & Zuccardi, G. (2015). Seguridad Informática. México: ISO-27001.

Guzman, D. F. (2014). Metodologías para el análisis de riesgos. España: POT.

Herrera, C. C. (2013). Conceptos gerencia y gestion. Lima: Publicaciones SCielo.

Laudon, K. C., & Laudon, J. P. (2012). Sistemas de información gerencial. México: PEARSON EDUCACIÓN.

Lucas Alonso, P. (2014). Gestión de las empresas por procesos. Barcelona.

Martinez, A., & Faraldi, R. (s.f.). Norma ISO 9001: La utilización de las TIC para la implementación de sistemas de gestion de la calidad.

Mejía, M. I. (2013). Arquitectura empresarial, el caminos hacia un gobierno integrado. CIO@GOV, 4-5.

Orozco Murillo, N., Rodriguez Cruz, C., & Serrano Zambrano, W. (2012). PLANEACIÓN ESTRATÉGICA DE TIC PARA LA EMPRESA DIEZ Y MEDIOS LTDA. Bogotá.

Osorio Guzmán, M. (2016). Las tecnologías de la información y la comunicación (TIC): Avances, retos y desafíos en la transformación educativa. II Congreso Internacional de transformación educativa (pág. 381). México D.F.: Amapsi Editorial.

Project Management Institute. (2017). Guía del PMBOK.

Project Management Institute, Inc. (2008). Guía de los fundamentos para la dirección de proyectos (Guía del PMBOK). EE.UU: PMI Publications,.

Renata, E. (s.f.). Planeación y Gestión estratégica de las TI (Versión adaptada al ecuador).

Rodríguez, J. R., & Lamarca, I. (s.f.). Planificación estratégica de sistemas de información. Cataluña.

Romaní, J. C. (2009). El concepto de tecnologías de la información. México.

Salinas La Roca, A. (2010). Inteligencia de Negocio. Auditoría y Control. Prototipo de herramienta de calidad de datos. Madrid.

Vargas Cordero , Z. (2009). La investigación aplicada: una forma de conocer las realidades con evidencia científica. Revista educación, 159-160.