UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO-JUNIO 2017

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRACTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

Estudio Para la Implementación de un Sistema de Gestión de Riesgos de Equipos Informáticos para la Universidad Técnica de Babahoyo.

EGRESADO:

Jorge Luis Quiñonez Palma

TUTORA:

Ing. Zoila Noemí Merino Acosta, Mim

AÑO 2017

TEMA

ESTUDIO PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE RIESGOS DE EQUIPOS INFORMÁTICOS PARA LA UNIVERSIDAD TÉCNICA DE BABAHOYO.

INTRODUCCIÓN

En los últimos años se han vulnerado diversos equipos informáticos “Hardware” lo cual ha llevado a los encargados de gestionar la parte física de los equipos informáticos, para ver de qué forma pueden controlar esta situación, dar soluciones al respecto para que se pueda prevenir la pérdida de información.

Una de las principales falencias que se presentan en la Universidad Técnica de Babahoyo, son las fragilidades que se muestran en ciertos laboratorios, donde los estudiantes toman ciertas piezas encajadas al equipo como disco duro, que puede ser de mucho riesgo, este puede contener información que es confidencial y que se la pueden utilizar para fines que atenten contra el estado de los procesos de integridad de la información, mediante la investigación realizada se pudo observar que todo el proceso antes mencionado es de vital importancia.

Para poder hacer el estudio de riesgos de los equipos informáticos hay que analizar los procesos internos de los equipos y a su vez analizar el contexto en el cual están brindando servicios y ver de qué forma se puede llegar a las bases, se establecen parámetros que se precisen para el análisis de las causas por las que se da la vulnerabilidad de la sustracción de dispositivos físicos de los equipos, por lo que es necesario y de vital interés tomar medidas que conlleven a una solución prudente y eficaz, por lo que es de gran importancia mantener un buen control para que los usuarios no puedan violar el hardware que es un activo significativo dentro de la institución.

El caso que se presenta en la Universidad Técnica de Babahoyo es identificar las causas que se muestran, al ver que los usuarios infringen las partes físicas de los equipos de una manera muy sencilla, lo cual es un síntoma de que algo está pasando en la institución.

En el área de equipos informáticos de la Universidad Técnica de Babahoyo existe un bajo control de restricción del uso de los equipos de cómputo, hay que tomar en cuenta que debido a la cantidad de computadoras posiblemente se le dificulte controlar todas las maquinas en uso, por lo que con esta investigación propuesta se intenta analizar las distintas soluciones para llegar a un fin específico el cual nos permita tener un control permanente y estrictamente confidencial.

Esta investigación propone identificar las debilidades y fortalezas en las que están inmiscuidos los equipos informáticos de la universidad técnica de Babahoyo ubicada en la provincia de los Ríos, con el fin de establecer objetivos, controles para minimizar las ocurrencias de las amenazas que pueden explorar vulnerabilidades en la infraestructura de los equipos de cómputo. Este estudio permite recoger información a través de instrumentos de recolección de datos, como entrevistas reuniones de trabajo y revisión bibliográfica, además de visitas a las instalaciones de la Universidad Técnica de Babahoyo.

Frente a esta realidad se plantean las siguientes interrogantes:

¿Qué importancia tiene la implementación de un sistema de gestión de riesgo?

¿Cuáles son las directrices en la cual se basa la implementación de un sistema de gestión de riesgo?

¿En que se basa la implementación de un sistema de gestión de riesgo?

Para resolver estas interrogantes, en el actual caso de estudio se desarrollarán los siguientes pasos:

Realizar una investigación que permita detectar las falencias que se muestren al momento, para poder hacer un estudio para la implementación de un sistema en un futuro cercano.

Encontrar los orígenes que generan las falencias en un posible sistema de gestión de riesgos de equipos informáticos.

Emplear el conocimiento adquirido, con el apoyo de fundamentos teóricos, para determinar soluciones factibles que puedan corregir las falencias encontradas.

Objetivo de estudio: Efectuar un estudio exhaustivo que en un tiempo dado permita desarrollar un sistema de gestión de riesgo de los equipos informáticos en la Universidad Técnica de Babahoyo.

Campo de acción: La investigación se desarrollará en la Universidad Técnica de Babahoyo; población de estudio: Estudio para la implementación de un sistema de gestión de riesgo de equipos informáticos, para que un futuro muy cercano se pueda llevar a cabo el desarrollo del sistema que se pretende alcanzar, para llevar un mejor control tanto de equipos como de la información que en estos residen.

DESARROLLO

A lo largo de estos últimos tiempos, los equipos informáticos se ha convertido en una de las bases trascendentales dentro de una institución, por lo general la información es un ente indispensable para la Universidad Técnica de Babahoyo, por lo que desde ahí se manejan las bases fundamentadas de las demás ramas de dicha Institución, resulta de trascendente importancia el cuidado que se les dé a las fuentes fidedignas para que no se alteren sus rasgos instaurados desde un inicio y se pueda tener la tranquilidad, de que las bases están bien protegidas y seguras a posibles fuentes de vulnerabilidad.

La Universidad Técnica de Babahoyo no cuenta con un sistema de gestión de riesgo, el cual permita controlar las fragilidades de equipos informáticos, que puede ser utilizada para fines prejuiciosos para la institución, de esta forma se busca controlar de una forma fiable la protección, seguridad e integridad de la información dentro de lo que corresponde, una vista desde otra perspectiva brindando seguridad para la institución responsable.

La factibilidad de un sistema de gestión de riesgo cera una gran ventaja porque forma parte de un proceso de seguridad informática, el cual se debería llevar acabo en la gran mayoría de Universidades a nivel General, formando un precedente que se pueda llevar acabo en otras instituciones de cualquier dependencia donde se pueda implementar este método, que puede ser un buen comienzo para un inicio de un proceso a futuro que conlleve a ayudar a muchos entes institucionales.

En la Universidad Técnica de Babahoyo se hace necesaria la implementación de un sistema de gestión de riegos, por todo lo que significa implementar un método seguro para que este pueda controlar todo tipo de robo de información, equipos informáticos, la seguridad hoy en día es indispensable en todo ámbito y más si se trata de un ente en el cual la información forma parte esencial de la estabilidad de una institución.

Otra de las motivaciones para analizar la implementación es la preocupación de los encargados de vigilar los equipos informáticos, para que no se distorsione y se pierda información confidencial, esta preocupación se debe a que los usuarios de hoy en día buscan la forma de vulnerar o sustraer información y empaquetados que resultan de gran importancia, hoy en día las personas con buen entendimiento en seguridades informáticas pueden alterar o robar información con herramientas que puedan ayudarles a realizar sus fines que atenten con la integridad de la información, esto es uno de los problemas por lo cual se llevó a cabo el estudio para la implementación de un sistema de gestión de riesgo en la Universidad Técnica de Babahoyo.

Se establecen las expectativas para este tipo de tecnologías actual con el interés de mantener un ente seguro para que, al momento del uso del mismo, existan ciertas normas de restricción las cuales no puedan ser violadas por el usuario y de esta forma brindar confianza, tanto para los usuarios, así como para el encargado de controlar su área de trabajo.

Para poder determinar los problemas que se presentan en cuanto al rendimiento del sistema de gestión de riesgos, es necesario hacer un estudio de ciertos parámetros que conlleven al planteamiento de los controles estipulados en las normas insertadas dentro de un proceso que se sigue bajo estrictos reglamentos que se deben cumplir.

El hecho permite realizar diversos estudios, detectar amenazas en los equipos, analizar la vulnerabilidad, ver inconvenientes futuros en los procesos, detectar los principales síntomas que surgen al momento del apartado de la información, sus causas y efectos en tiempo real y demás circunstancias que se presentan en la Institución.

Otro de los impulsos para analizar la falta de la implementación de un sistema gestión de riesgo es la preocupación de los encargados de la vigilancia de la información, ya que hay niveles de usuarios que tienen la habilidad de poder vulnerar los permisos y restricción para poder infiltrarse sin que nadie lo detecte y de esta forma acceder a información confidencial de la institución a la cual se le realiza esta acción.

Es necesario que exista una persona encargada al momento en cada laboratorio y sobre todo en la entidad que se encarga de controlar los equipos informáticos, para que de esta manera se pueda estar pendiente de cada acción que se pretenda hacer para mantener un entorno de mayor confiabilidad para los que conservan información.

El caso de estudio para la implementación de un sistema de gestión de riesgo se basa en las principales falencias que pueden existir en un entorno basado en equipos informáticos, por ende, la investigación trata de analizar detalladamente las posibles soluciones a corto plazo que se le pueda establecer a los procesos informáticos.

El estudio de caso para la implementación de un sistema de gestión de riesgo se basará principalmente en el control, entorno de los equipos informáticos, los procesos informáticos que se estén realizando al momento, para constatar los acontecimientos en cada movimiento, y verificar que la información y los procesos no han sido alterados por los usuarios o estudiantes y de esta forma mantener un control que garantice la estabilidad de los procesos informáticos.

La perspectiva de un sistema de gestión de riesgos de equipos informáticos, tienen mucho que ver con los posibles problemas que se estén presentando en la institución, para que de un modo practico resolverlos o tratar de reducir los riesgos que se producen de la forma tradicional, este sistema servirá como una herramienta de gran ayuda para proteger los recursos informáticos

Al no existir un sistema de gestión de riesgos de equipos informáticos, se ha hecho un estudio y se ha llevado a la determinación, de que es una herramienta que va a ser de gran importancia para llevar un control de los equipos informáticos, de forma que garanticen la seguridad y resguardo de los equipos para mantener una adecuada protección de la información.

Este sistema de gestión de riesgos de equipos informáticos es el que va a llevar todos los registros básicos de una computadora, lo más importante, un balance que se ara cada semana para constatar que todos los implementos estén completos y que no existan novedades.

La investigación de este trabajo se la realizo aplicando la metodología de campo. Esta clase de investigación se apoya en informaciones que provienen entre otras, de entrevistas, cuestionarios, encuestas y observaciones. En todo caso es importante realizar siempre la consulta documental con el fin de evitar una duplicidad de trabajos, puesto que se reconoce la existencia de investigaciones anteriores efectuadas sobre la misma materia y de las que se pueden usar sus conclusiones como insumos iniciales de la actual investigación. Utilizando los métodos de observación científica el cual nos permite realizar un análisis profundo de la realidad y de lo que se observa para de esta forma poder llegar a el propósito establecido desde un inicio.

La mayoría de nuestras actividades implican manejar DATOS para producir IMFORMACION y posteriormente tomar decisiones con base a esta información que se produjo, por lo tanto, se necesita de los computadores para almacenar gran cantidad de datos para luego procesarlos y obtener información. (Zambrano, 2017, pág. 2)

Consiste en una serie de programas que tiene como función optima administración de recursos del computador es el encargado de controlar las operaciones de entrada y salida, el funcionamiento del CPU, memoria, periféricos (Jesus, 2017, pág. 8)

Es un circuito impreso el cual se encuentra dentro de los computadores u ordenadores y otros sistemas expansibles, este lleva a cabo mucho de los componentes electrónicos los cuales son esenciales para el sistema. Tales como la CPU y la memoria también proporcionan conectores para otros periféricos. (Castillo, 2014, pág. 3)

Hardware son las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos y el soporte lógico y es llamado software. El hardware se divide en dos, hardware básico (board, procesador, memoria RAM, torre) y periféricos. (Zambrano, 2017, pág. 5)

El software de computadora es el producto que construyen los programadores profesionales y al que después le dan mantenimiento durante un largo tiempo. Incluye programas que se ejecutan en una computadora de cualquier tamaño y arquitectura, contenido que se presenta a medida que se ejecutan los programas de cómputo (Pressman, 2015, pág. 1).

Microprocesador: o simplemente procesador, es el circuito integrado central y más complejo de un sistema informático; a modo de ilustración, se le suele asociar por analogía como

el “cerebro” de un sistema informático. El procesador puede definirse, como un circuito integrado constituido por millones de componentes electrónicos agrupados en un paquete. (Ávalos Pérez, 2016, pág. 10)

Memoria RAM: acrónimo de Random Access Memory, o memoria de acceso aleatorio. Es el dispositivo que puede ser considerado como espacio de trabajo de la CPU. Es una memoria volátil, la misma que pierde su contenido al momento de perder energía la maimboard. (Ávalos Pérez, 2016, pág. 14)

La ingeniería de software es un enfoque sistemático para la producción de software que toma en cuenta los temas prácticos de costo, fecha y confiabilidad, así como las necesidades de clientes y fabricantes de software. (Villanueva Montoya, 2015, pág. 28)

Un sistema de información se puede definir como un conjunto de elementos interrelacionados (entre los que podemos considerar los distintos medios técnicos, las personas y los procedimientos), cuyo cometido es capturar datos, almacenarlos y transformarlos de manera adecuada y distribuir la información obtenida mediante este proceso. (Gomez Vieites & Suares Rey, 2016, pág. 37)

La información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La

seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad institucional, minimizar el daño y maximizar el retorno sobre las inversiones y las oportunidades. (Priale, 2017, pág. 3)

Con unas buenas políticas de seguridad, tanto físicas como lógicas, conseguiremos que nuestros sistemas sean menos vulnerables a las distintas amenazas. Si menos vulnerables: nadie puede asegurar que su sistema sea cien por ciento seguro, hasta la seguridad entre los técnicos protectores del sistema y los que buscan rendimiento económico fáciles, o simplemente su minuto de gloria al superar al reto de asomarse al otro lado de la barrera de protección. (Seaone Ruano, Saiz Herrera, Fernandez Álvarez, & Fern;andez Aranda, 2013, pág. 10)

La seguridad de la información trata por tanto de proteger activos, tanto tangibles, como por ejemplo un disco duro o una base de datos con la información de clientes, como intangibles, como por ejemplo la reputación, la privacidad o el nombre de marca. (Álvarez Marañón & Peréz García, 2017, pág. 4)

Se puede definir el riesgo como: la posibilidad de que ocurra algún evento negativo para las personas y/o empresas. Ya que cualquier persona o entidad está expuesta a una serie de riesgos derivados de factores internos y externos, tan variables como su propio personal, su actividad, la situación económica, la asignación de sus recursos financieros o la tecnología utilizada. (Rodriguez, s.f.).

Es imposible evitar las vulnerabilidades al 100% incluso cuando se tiene operando en muestro sistema cortafuegos, anti spam, antivirus, y detectores de código maligno. Lo que si es posible es tratar de evitarlas al máximo posible, tengamos presente que las comunicaciones en la

red constan de 7 capas según el modelo OSI, y las vulnerabilidades pueden estar presentes en varias capas, o incluso dentro del núcleo de nuestro sistema. (Betancourt, 2016, pág. 8)

La información tiene una importancia fundamental para el funcionamiento y quizá incluso sea decisiva para la supervivencia de la organización. El hecho de disponer de la certificación según ISO/IEC 27001 le ayuda a gestionar uy proteger sus valiosos activos de información. (Betancourt, 2016, pág. 15)

CONCLUSIONES

1.- La falta de un sistema de gestión de riesgos de equipos informáticos es una falencia que se ve en la Universidad Técnica de Babahoyo, es necesario para llevar un control de los equipos establecidos en cada laboratorio desde un sistema que permita llevar un control de los equipos informáticos.

Es importante para que los usuarios tomen conciencia y no hagan cosas imprudentes que puedan afectar los dispositivos, de esta forma lograr reducir los problemas generados por aquellas personas que tienen un propósito de alterar ciertas restricciones

Llevar un control de los equipos informáticos para que no existan escenarios de alteración de equipos informáticos, para que de este modo se mantenga una protección dentro de lo que se

quiere lograr, de este modo se lleva a cabo el control estipulado por el sistema que se pretende crear

El encargado del Sistema debe obtener un balance semanal de los controles que se les está brindando a los equipos, para que, de esta forma, se pueda llevar una inspección de los dispositivos y de esta forma reducir el riesgo de pérdidas de accesorios que forman parte de los complementos de equipos informáticos

Los encargados de los laboratorios deben encargarse de revisar a la hora de entrada y de salida que no existan novedades, para que al finalizar la semana hagan un informe dirigido al encargado del sistema, el cual en sus observaciones conste con todo lo inherente a el balance de los equipos informáticos, esto quiere decir que no hubo perdida de ningún dispositivo si este es el caso, de lo contrario informar las falencias que están ocurriendo dentro del laboratorio

Lo que se pretende con este sistema es dar mayor seguridad a los equipos informáticos, ya que en estos tiempos es de gran importancia el cuidado de los mismos, porque no solo se afectan los equipos, sino algo más importante que es la información de la institución

Los motivos por los cuales se estudia la factibilidad de un sistema de gestión de riesgos de equipos informáticos, es reducir la perdida de información, mantener un control el cual permita llevar de forma ordenada cada uno de los dispositivos que se consideran de vital importancia que por lo general son las bases de información las cuales son la clave de toda

Universidad, proteger todos sus recursos intangibles y que no se vean alterados por personas ajenas a la institución.

ENCUESTA

Luego de las encuestas que se realizó en los laboratorios de cómputo en la Universidad Técnica de Babahoyo se pudo obtener el siguiente análisis:

Dada la encuesta se observó que es de suma importancia la implementación de un sistema de gestión de riesgos de equipos informáticos

Es importante esta clase de sistemas para brindar mayor seguridad tanto a la información y a los equipos informáticos

La integridad de la información es indispensable en toda institución para poder garantizar la información que se procesa periódicamente

Los ingenieros encargados de los laboratorios deben estar pendiente de cada detalle que note que se está realizando de forma indebida

Los ingenieros encargados de los laboratorios tienen parecidas perspectivas sobre las posibles afectaciones de los riesgos en su lugar de trabajo

Se ha detectado que los riesgos más frecuentes en el entorno de trabajo de los ingenieros encargado de los laboratorios es la perdida de información y daños en los equipos informáticos

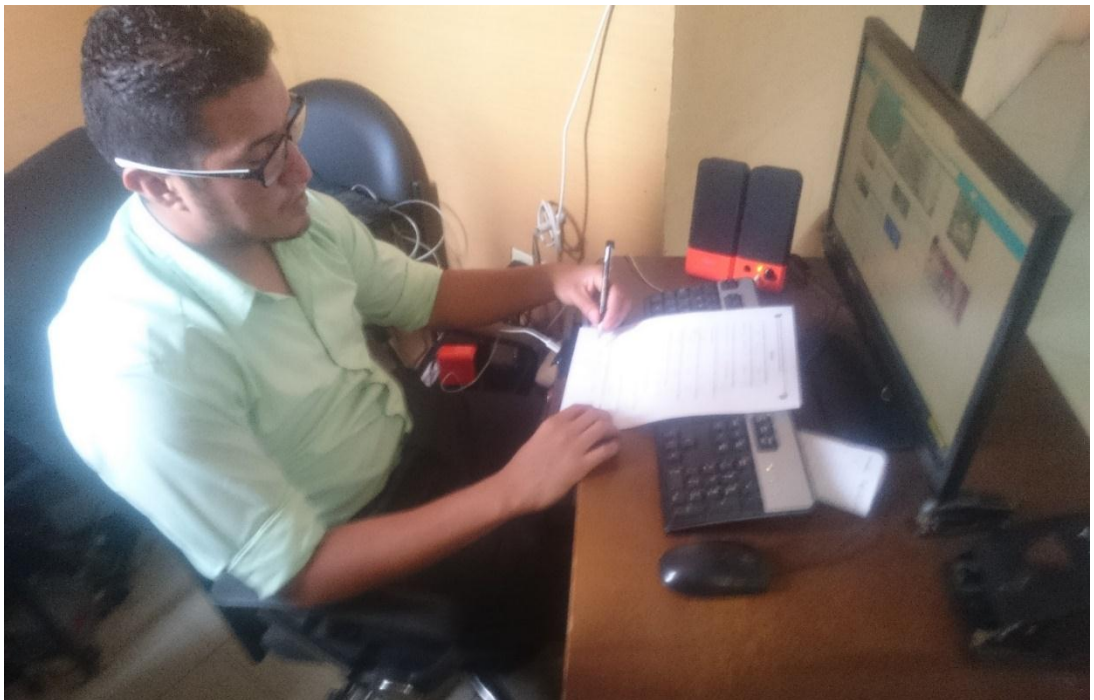
Que no existe un sistema de gestión de riesgos que lleve un control de la información de los equipos informáticos

Hay cierta probabilidad de ocurrencia en el impacto de los riesgos en su entorno de trabajo

Que tienen una cierta idea de donde afectan los riesgos más comunes que afectan su entorno de trabajo

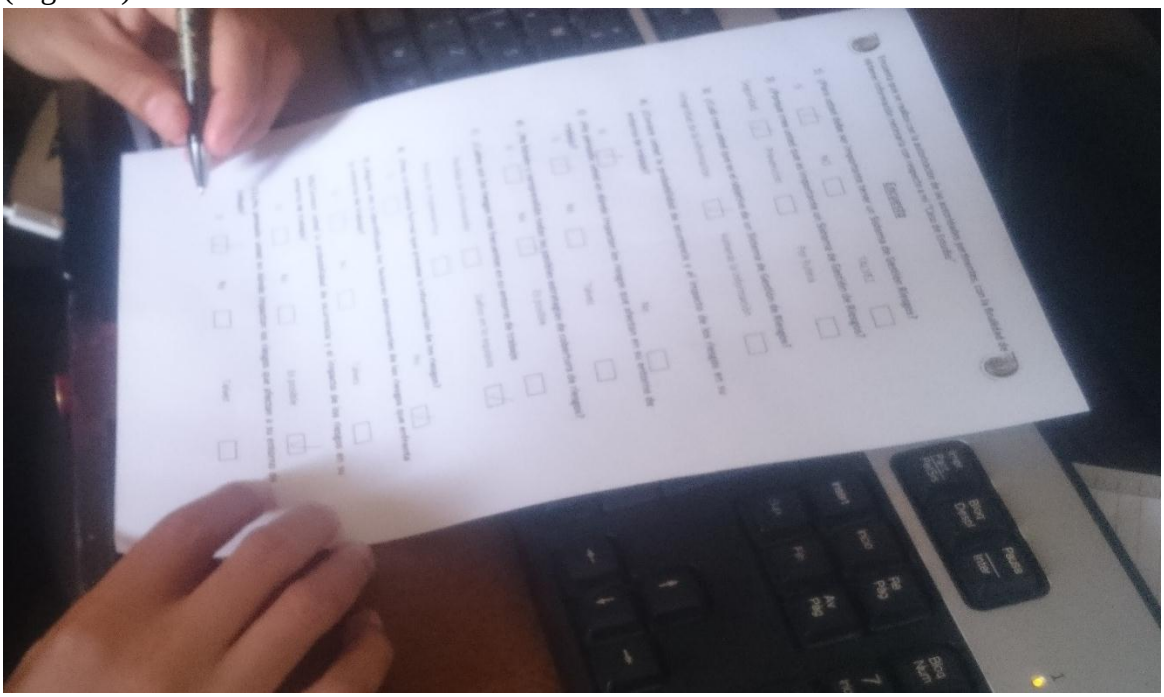
La presente encuesta tiene como finalidad identificar la situación actual que se presenta en los laboratorios de sistema de la Universidad Técnica de Babahoyo y si es o no factible el estudio para la implementación de un sistema de gestión de riesgos de equipos informáticos.

(Figura 1).



Según observación de las encuestas se pudo observar que el estudio para la implementación de un sistema de gestión de riesgo es necesario dado el balance de los encuestados

(Figura 2).



Como se puede verificar son encuestas hechas al personal encargado de los laboratorios, de las diferentes facultades para observar el entorno y lo que piensan cada uno de los Ingenieros

de cada laboratorio, con la finalidad de que nos den sus percepciones acerca de las preguntas planteadas.

Se puede constatar después de realizar las encuestas al personal encargado de los laboratorios en sus diferentes facultades que dada la encuesta el 99% de los encuestados, creen que es necesario implementar un sistema de gestión de riesgos de equipos informáticos para tener un mayor control de todos los elementos que están a su cargo.

Mediante las encuestas realizadas que en la mayoría de los puntos señalados se obtuvo una respuesta favorable, acorde a las conclusiones que se querían sacar sobre las preguntas realizadas, para tener una pauta de que el estudio que se está realizando si es factible y que en un determinado tiempo se lo puede poner en práctica mediante el sistema de gestión de riesgos de equipos informáticos.

Hoy en día se torna de gran importancia tener un sistema de gestión de riesgos de equipos informáticos por todo lo que esto implica, para la seguridad de la información dentro de un ente tan importante como lo es la Universidad Técnica de Babahoyo.

FODA del Proyecto	
Fortalezas	**Oportunidades**
Un sistema que se acerca a los parámetros que se busca para que su funcionamiento y eficiencia sea acorde con la tarea que se le ha encomendado, en este caso resguardar la información y las partes esenciales de los equipos	Se basa en las medidas establecidas para que su funcionamiento sea eficiente, es un proyecto que puede ser muy útil en un futuro muy cercano para poder contribuir con sus funcionalidades especificas

Debilidades	**Amenazas**
Algunas políticas de seguridad con las que no cumple el estudio para la implementación de un sistema de gestión de riesgo, pueden ser que en ese momento no cuente con una certificación de una norma que lo califique para ver si este cumple todos los roles que se le han encomendado	Acceso al sistema de personas no autorizadas o capacitadas para el mismo, probablemente con fines no confiables que terminen perjudicando a la institución

Bibliografía

Álvarez Marañón, G., & Peréz García, P. P. (2017). *Seguridad informática para empresas y particulares.*

Ávalos Pérez, M. (2016). El computador. *Breve historia del computador Hardware y Software del computador*, 1-25.

Betancourt, T. (2016). Seguridad Informatica. *Vulnerabilidades y Riesgos Informaticos*.

Castillo, P. (2014). Motherboard definicion y partes. *Descripcion de que es la board y que la compone*, 1-9.

Gomez Vieites, A., & Suares Rey, C. (2016). *Sistemas de informacion - herramientas practicas para la gestion* .

Jesus. (2017). Esta revista esta basada en conocer los inicios y la evolucion del computador . *Revista digital el computador*, 1-12.

Pressman, R. (2015). *Ingenieria del Software Un enfoque practico.* Connecticut: Mexico.

Priale. (2017). *Normas y Estandares: Seguridad Informatica.*

Rodriguez. (s.f.). *http://redyseguridad.fi-p.unam.mx*. Obtenido de http://redyseguridad.fi-p.unam.mx: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/AnalisisRiesgos.php

Seaone Ruano, C., Saiz Herrera, A., Fernandez Álvarez, E., & Fern;andez Aranda, L. (2013). *SEGURIDAD INFORMATICA.*

Tejada, E. C. (2014). *Gestion de servicios en el sistema informatico* (1 ed.). (I. Editorial, Ed.) IC. Obtenido de https://www.ecured.cu/Sistema_de_Informaci%C3%B3n

VARGAS, A. (9 de 12 de 2010). *Ingenieria d software.* Obtenido de Ingenieria d software: http://arielvargasu.blogspot.com/2010/12/reingenieria-del-software.html

Villanueva Montoya, D. (2015). *Ingeniería de software - Ian Sommerville Parte 1*.

Zambrano, A. (2017). Capitulo 1 de hardware (2016 2017). *En este manual se estudiara division de los equipos, perifericos de entrada y salida.*, 1-29.

esus. (2017). Esta revista esta basada en conocer los inicios y la evolucion del computador . *Revista digital el computador*, 1-12.

Pressman, R. (2015). *Ingenieria del Software Un enfoque practico.* Connecticut: Mexico.

Priale. (2017). *Normas y Estandares: Seguridad Informatica.*