UNIVERSIDAD NACIONAL DE LOJA

PFC-CIS

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios"

Tesis Previa a la Obtención del Título de Ingeniero en Sistemas

Autor:

- Franklin Mauricio Vega Hidalgo

Director:

- Ing. Luis Antonio Chamba Eras, Mg. Sc.

LOJA-ECUADOR

2014

Certificación Del Director

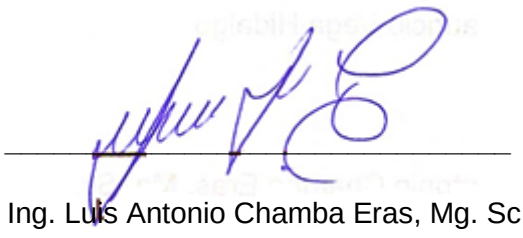
Ing. Luis Antonio Chamba Eras, Mg. Sc.

DIRECTOR DEL TRABAJO DE TITULACIÓN

CERTIFICA:

Haber dirigido, asesorado, revisado y corregido el presente trabajo de tesis de grado, en su proceso de investigación, bajo el tema **"MODELO DE CONFIANZA PARA HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN ENTORNOS UNIVERSITARIOS",** previa a la obtención del título de Ingeniero en Sistemas, realizado por el señor egresado: **Franklin Mauricio Vega Hidalgo**, la misma que cumple con la reglamentación y políticas de investigación, por lo que autorizo su presentación y posterior sustentación y defensa.

Loja, julio del 2014



Ing. Luis Antonio Chamba Eras, Mg. Sc.

DIRECTOR DE TESIS

Autoría

Yo **Franklin Mauricio Vega Hidalgo** declaro ser el autor del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el Repositorio Institucional - Biblioteca Virtual.

Autor: Franklin Mauricio Vega Hidalgo

Firma: 

Cédula: 0705375178

Fecha: 12 Noviembre de 2014

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo **Franklin Mauricio Vega Hidalgo,** declaro ser autor de la tesis titulada: **Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios** como requisito para optar al grado de **Ingeniero en Sistemas**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.
Para constancia de esta autorización, en la ciudad de Loja, doce días del mes de noviembre del dos mil catorce.

Firma: 

Autor: Franklin Mauricio Vega Hidalgo

Cédula: 0705375178

Dirección: Arenillas-El Oro (Calle Jaime Roldós entre 9 de Octubre y 25 de Junio)

Correo Electrónico: fmvegah@unl.edu.ec

Teléfono: 072908284 **Celular:** 0993389471

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Luis Antonio Chamba Eras, Mg. Sc.

Tribunal de Grado: Ing. Ana Lucía Colala Troya, Mgs.
Ing. Lorena Elizabeth Conde Zhingre, Mg. Sc.
Ing. Marco Augusto Ocampo Carpio, Mg. Sc.

Agradecimiento

Infinitamente agradecido, por la realización de este trabajo, a Dios; a mis padres: Hugo y Bertila, y a mis hermanas: Yuli y Dayita. A Dios, porque ha estado conmigo a cada paso que doy, cuidándome y dándome fortaleza para continuar; a mis padres, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi fortaleza en todo momento; a mis hermanas, por la comprensión y la ayuda desinteresada que me han brindado siempre; similar apoyo que me ha brindado Eliza, más que amiga, hermana; quien en estos últimos años ha sido un pilar fundamental de motivación y superación personal.

De igual manera, quiero expresar mis sentimientos de gratitud a la Universidad Nacional de Loja, en particular a la Carrera de Ingeniería en Sistemas; y, de manera especial, a todos los docentes que impartieron sus conocimientos para mi formación académica y personal; los que me servirán para aplicarlos, en el futuro, en el ámbito social y profesional. De la misma forma a mi director de tesis, Ing. Luis Chamba, que sin duda su ayuda ha sido fundamental para la culminación de este trabajo de titulación.

Gracias a todos por haber depositado su entera confianza en cada reto que se me presentaba, sin dudar ni un solo momento en mi inteligencia y capacidad para seguir adelante.

Dedicatoria

La concepción de este trabajo está dedicada a Dios, por haberme dado la vida y poder luchar diariamente para cumplir cada uno mis sueños; **a mis padres: Hugo Vega y Bertila Hidalgo**, pilares fundamentales en mi vida. Sin ellos, jamás hubiese podido conseguir lo que hasta ahora tengo. Su tenacidad y lucha incansable han hecho de ellos el gran ejemplo a seguir y destacar, no solo para mí, sino para mis hermanas y familia en general. **A mis adoradas hermanas: Yuli y Dayita**, que estuvieron presentes en los buenos y malos momentos, y supieron apoyarme en todo para poder concluir este objetivo, sin duda uno de los más importantes en mi vida personal.

Franklin Mauricio Vega Hidalgo

Cesión De Derechos

Franklin Mauricio Vega Hidalgo, autor principal del presente trabajo de titulación, autoriza a la Universidad Nacional de Loja, al Área de la Energía, las Industrias y los Recursos Naturales No Renovables y, por ende, a la Carrera de Ingeniería en Sistemas hacer uso del mismo en lo que estime sea conveniente.

a. Título

"Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios".

b. Resumen

Globalmente, la toma de decisiones en el ámbito de la seguridad informática requiere de eficiencia y eficacia, puesto que de ello depende, en gran parte, el mantener salvaguardada toda la información que transita por la red, tal es el caso de los entornos universitarios. El determinar la factibilidad de implementación de herramientas de seguridad informática conlleva a una gran controversia, específicamente en las instituciones de educación superior que cuentan con un mínimo o casi nulo porcentaje de explotación del área de la seguridad informática, para ello la confianza–reputación, se toma como base principal para el desarrollo de este trabajo de titulación.

El presente trabajo tiene como propósito proponer un modelo de confianza en base a criterios, previamente estudiados y valorados, que permitan determinar la factibilidad de implementación de herramientas de seguridad informática en entornos universitarios, que se encuentran distribuidos en tres escenarios, tales como: Herramienta Propietaria/Privativa, Herramienta Libre/Gratuita, Proyectos Estudiantiles; dentro de los cuales constan los respectivos criterios con sus pesos genéricos y una previa ponderación, lo que permitirá obtener un valor porcentual y determinar el nivel de confianza de la herramienta de seguridad informática en evaluación. Para ello se ha hecho uso de normas ISO así como del método científico Estudio por Casos, que ha permitido obtener conclusiones en base a las decisiones tomadas en diferentes entornos universitarios.

Además, se ha realizado visitas técnicas, encuestas y entrevistas a personal especializado en la áreas de redes y seguridad de la información, tanto de la Unidad de Telecomunicaciones e Información-UNL como en las diferentes unidades y/o departamentos de universidades como: ESPOL, ULVR, UTMACH y UTPL durante todo el desarrollo del trabajo de titulación con el fin de recabar información valedera y confiable de la situación actual, en cuanto a la toma de decisiones en el área de seguridad informática.

Finalmente, se ha tomado como escenario de experimentación la Sección de Mantenimiento Electrónico de la UTI-UNL, con el fin de evaluar la implementación de un programa antivirus dentro de la red universitaria, para lo cual se ha analizado la propuesta de dicha implementación, así como se ha sido partícipe de la instalación del DEMO de dicha herramienta, con el objetivo de evaluar cada uno de los criterios del modelo propuesto en su escenario correspondiente y así, obtener el nivel de confianza para la implemenación del programa antivirus dentro de la Universidad Nacional de Loja.

Summary

Globally, the decision-making in the informatics security requires efficiency and effectiveness, since it depends, most of the part, keeping saved all the information that is in the network, in this case the university environments. To determine the feasibility of implementing tools that keep informatics security saved it takes a big controversy, specifically in the higher educative institutions that have a minimal or almost null percentage of exploitation in the informatics security area, for this reason the trust-reputation, is taken as a main base for the development of this degree work.

The purpose of this work is to propose a trust model based on a criteria, previously studied and valuated to determine the feasibility of implementing security informatics tools in environments such as: university, that are distributed in three scenarios as: Owner/ Custodial Tool, Free Tool, Student projects; in which are the respective criteria with their generic weights and a previous weighing, which will allow to get a percentage value and to determine the trust level of the informatics security tools in the evaluation. For this, the researcher has used ISO standards as well as the Case Study scientific method which has allowed to obtain conclusions based on the taken decisions in different university environments.

Moreover, it has done technical visits, surveys and interviews to personal specialized staff in the network and informatics security areas, both in the Unit of Telecommunications and Information-UNL as in the different units and departments as: ESPOL, ULVR, UTMATCH and UTPL during all the development of this degree work in order to acquire reliable and valid information of the actual situation regarding the decision-making in the informatics security area.

Finally, it has taken as an experimental scenario the Section of Electronic Maintenance of UTI-UNL, with the purpose to evaluate the implementation of an antivirus program inside the university network, for this reason it has been analyzed the proposal of such implementation with the objective to evaluate each of the criteria of the proposed model in their corresponding scenario and this way, to obtain a trust level for implementing the antivirus program inside the Universidad Nacional de Loja.

Índice de Contenidos

Índice General

Índice de Figuras

Índice de Tablas

c. Introducción

Los centros de educación superior son el pilar fundamental para la investigación e innovación, y conforme han avanzado las tecnologías dichas instituciones se han visto en la necesidad indagar y hacer uso de ellas en diversos contextos. Uno de ellos es el campo de la seguridad de la información, el activo estratégico más importante de las organizaciones en general.

Es por ello que han surgido una serie de mecanismos o herramientas de seguridad informática, con el único fin de proteger y optimizar los diferentes servicios que brindan las Universidades, pero existe un gran dilema a la hora de implementar cualquier de estas herramientas que se encuentran actualmente en auge, puesto que se carece de un modelo o estándar que nos indique cuándo es y cuándo no aconsejable la implementación de determinada herramienta en entornos universitarios.

Para el mencionado problema se propone un modelo de confianza que permita determinar la factibilidad de implementación de estos mecanismos de seguridad en entornos universitarios, basándose en la creación de criterios estudiados y valorados por fuentes bibliográficas aceptables y por personal especializado en seguridad de la información y toma de decisiones en cuanto a TIC's[1]. Para dar cumplimiento tanto al objetivo principal como a los específicos del presente trabajo de titulación, se ha cumplido con una serie de actividades que han permitido culminar adecuadamente cada una de las fases establecidas. Partiendo así, con la revisión del estado del arte de las herramientas de seguridad informática mayormente implementadas en entornos universitarios, dándole cumplimiento mediante una comparación de las herramientas, tomando como fuente eje los resultados de la I Encuesta de Seguridad de Información a las Universidades miembro de CEDIA [1] (Ver Anexo 1), la misma que ha permitido realizar un análisis de cuatro de las herramientas más implementadas en los centros de educación superior; consiguiendo así una enfoque mucho más amplio de las ventajas y desventajas que brindan cada uno de estos mecanismos de seguridad.

Luego de haber realizado el análisis de las herramientas mencionadas, se ha

[1] Tecnologías de la Información y Comunicación

revisado la existencia de estándares que evalúen la confiabilidad en las herramientas de seguridad informática [2-5] y tras una profunda búsqueda de información referente a algún modelo o estándar que evalué dicha confiabilidad de implementación se ha obtenido un resultado casi nulo, debido a que se cuenta con modelos, estándares que ofrecen buenas prácticas a la hora de gestionar proyectos en general, pero no se da la existencia de modelos que evalúen la confiabilidad de implementación de este tipo de herramientas.

En lo que respecta a la propuesta del modelo, siendo esta la parte primordial del trabajo de titulación, se ha realizado las respectivas revisiones bibliográficas, visitas técnicas, encuestas y entrevistas, tanto a personal interno como externo (Ver Anexos 4, 6, 8-13) lo que ha concedido el planteamiento de los respectivos criterios y escenarios de evaluación dentro del modelo, así como los pesos porcentuales genéricos en cada escenario. Dichos escenarios han sido puestos en consideración con parte del personal de la UTI[2] de la UNL[3] (Ver Anexos 16-18), accediendo así la asignación de grados o niveles* de confianza tras la evaluación de la implementación de herramientas de seguridad informática con el modelo propuesto.

Con el interés de poner a prueba el modelo propuesto se ha planteado un objetivo de experimentación, dentro del cual se ha palpado las diferentes necesidades de la UTI, siendo una de ellas el carecer de un departamento o sección dedicado al área de la Seguridad de la Información; inmediatamente se ha realizado una reunión con el Director de dicha unidad con el fin de plantear el propósito del trabajo de titulación (Ver Anexo 5 y 15), dando como válido el aporte del modelo propuesto. Mediante las entrevistas y encuestas realizadas a los encargados de las secciones de Redes y Mantenimiento Electrónico (Ver Anexos 4, 6 y 22) se ha conocido del plan de implementación de un programa antivirus con licenciamiento corporativo; el mismo que ha sido ofertado por uno de los proveedores potenciales de la Región Sur del país, lo que ha permitido proceder con la evaluación de la implementación de la herramienta en cuestión, tomando como base la propuesta presentada y la experiencia obtenida tras la participación en la instalación del DEMO del programa antivirus (Ver Anexos 22 y 28), determinando así un nivel de confianza.

[2] Unidad de Telecomunicaciones e Información
[3] Universidad Nacional de Loja

El presente informe está compuesto en base al normativo legal de la Carrera de Ingeniería en Sistemas, el que va enmarcado legalmente a la Universidad Nacional de Loja; es así que en primer lugar se encuentra el Título del trabajo de titulación seguido por un Resumen, el que permite tener una idea clara de qué se trata el presente trabajo. Por su parte la Introducción indica la estructura del informe final; posteriormente, se ubica la Revisión Literaria donde se contempla el estado de arte empleado para la resolución del problema principal, así como casos de estudio; luego de aquello se da a conocer los Materiales y Métodos; dentro de ello, técnicas de recolección de datos y métodos científicos empleados durante el desarrollo del trabajo de titulación. Tras indicar la metodología empleada se da a conocer los Resultados obtenidos durante todo el proceso investigativo y de experimentación, así como se realiza la respectiva Discusión de los mismos; culminando con las Conclusiones y Recomendaciones de trabajo de titulación y sin antes respaldar el cumplimiento de cada actividad con los Anexos.

Cabe demarcar que, el modelo propuesto es un aporte original a la comunidad científica-tecnológica, esperando que el mismo sirva de gran ayuda para futuros trabajos relacionados a la misma línea de investigación. Por otra parte, el modelo en cuestión está compuesto de los criterios más relevantes para la evaluación de una herramienta de seguridad informática previa a su implementación y que los pesos asignados a cada uno de ellos quedan a juzgamiento y acoplamiento de cada uno de los entornos universitarios en donde deseen aplicarlos.

d. Revisión de Literatura

CAPÍTULO I: FUNDAMENTOS BÁSICOS

1. Seguridad Informática

Sin lugar a dudas, el término Seguridad Informática es escuchado únicamente cuando se produce algún problema en equipos o servicios de carácter informáticos. Para ello, es importante mencionar que la Seguridad Informática son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados [6], daños accidentales o mal intencionados que pueden iniciar con una simple vulnerabilidad algún sistema o servicio informático. Con el fin de cambiar este paradigma, se plantea la creación de un modelo de confianza que permita contar con criterios que garanticen la existencia de pautas de implementación para herramientas de seguridad informática.

1.1. Objetivo de la Seguridad Informática.

Si bien es cierto, la seguridad informática tiene como principal objetivo el proteger el activo estratégico más importante que tienen las empresas/instituciones, que es su información; de los riesgos a los que está expuesta y para mantener un alto nivel de protección en los entornos universitarios, es necesario realizar implementaciones de herramientas que garanticen en cierto porcentaje una buena toma de decisiones y por ende un correcto funcionamiento de la misma.

Por lo tanto, mediante el trabajo de titulación en estudio se pretende brindar ayuda en la toma de decisiones a la hora de implementar algún tipo de mecanismo de seguridad dentro de los centros de educación superior para proteger la información que circula por la/s red/es. Cabe recalcar que, la seguridad informática tiene su enfoque principal en el cumplimiento de sus principios fundamentales, Triángulo CIA (Confidentiality/Confidencialidad, Integrity/Integridad y Availability/Disponibilidad [7].

1.2. Principios Fundamentales de Seguridad.

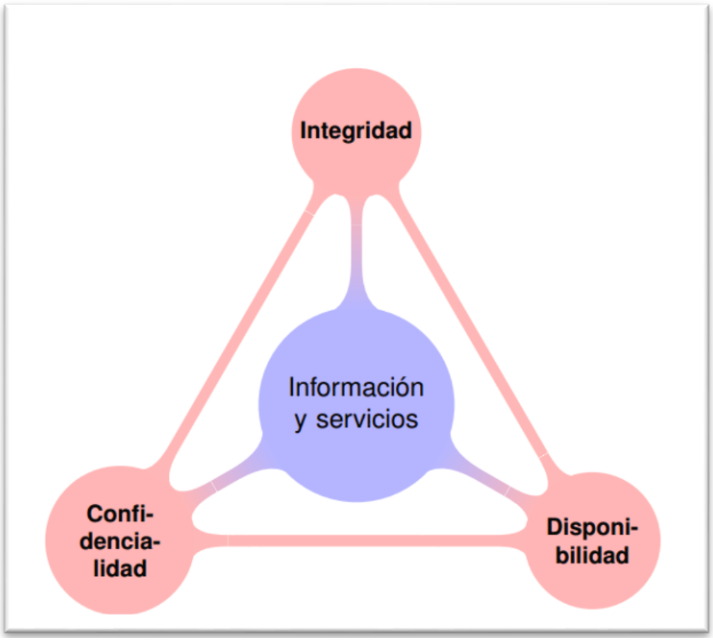


Figura 1 Principios Fundamentales de Seguridad [8]

Los principios de la seguridad son de gran ayuda a la hora de tomar decisiones en esta área, más aún si estas decisiones tienen que ver con implementaciones de herramientas que aportaran al reforzamiento de la protección de todos los dispositivos y sistemas encontrados en la red universitaria. Consecuentemente, el planteamiento de los criterios de evaluación apegados a los principios de la seguridad otorga un valor adicional de confianza al modelo propuesto.

- **Confidencialidad.** Se puede definir como la prevención de la revelación de la información no autorizada [9, 7, 10]. Esto puede ser el resultado de medidas de seguridad escasas o fugas de información por el personal. Para lo cual el modelo propuesto evalúa el cumplimiento de las políticas implementadas en la institución educativa.

- **Integridad.** Puede identificarse con la prevención de modificación errónea de información [6, 9, 10]. Los usuarios autorizados son probablemente la causa más grande de los errores, omisiones y alteraciones de información [7]. El almacenar información incorrecta o más bien manipulada por terceros dentro de un sistema puede resultar ser tan malo como perder información

valiosa. De igual forma que el principio anterior, el modelo evalúa la propuesta del proveedor así como la retribución de la inversión con los beneficios obtenidos tras determinada implementación.

- **Disponibilidad.** Se define como la prevención de retención no autorizada de información o recursos [7]. Esto no únicamente aplica al personal que retiene información. La información debería estar tan libremente sea posible para los usuarios autorizados, todo bajo sus políticas y normas de la institución. Como lo indica la disponibilidad de la información se encuentra involucrada en las políticas establecidas dentro de la institución, políticas que pueden ser configuradas e implementadas en las herramientas de seguridad.

La seguridad informática se preocupa de que la información manejada por un computador no sea dañada o alterada, que esté disponible y en condiciones de ser procesada en cualquier momento y se mantenga confidencial [6]. Específicamente la información es y debe ser protegida como el bien más importante para las organizaciones de todo tipo. Al definir cada uno de los criterios establecidos dentro del modelo creado se ha tomado en cuenta que en cada criterio se aporte al fortalecimiento de los tres principios primordiales de la seguridad.

2. La Investigación de Operaciones en la Toma de Decisiones

2.1. Breve Reseña Histórica

Los inicios de lo que hoy se conoce como Investigación de Operaciones se remonta a los años 1759 cuando el economista Quesnay empieza a usar modelos primitivos de programación matemática. Más tarde, otro economista de nombre Walras, hace uso, en 1874, de técnicas similares. Los modelos lineales de la Investigación de Operaciones tienen como precursores a Jordan en 1873, Minkowsky en 1896 y a Farcas en 1903. El desarrollo de los modelos de inventarios, así como el de tiempos y movimientos ha sido el principio a la creación y propuestas de una serie de modelos para promover la buena toma de decisiones.

Actualmente, la Investigación de Operaciones no solo se aplica en el sector privado (industrias, sistemas de comercialización, sistemas financieros, transportes, etc.) sino también en el sector de servicios públicos, tanto en los países desarrollados como en países de tercer mundo. Siendo así un apoyo y pilar fundamental para que nazca la iniciativa de buscar soluciones que promuevan los objetivos de toda organización, mediante la Investigación de Operaciones.

2.2. Definición

Al hablar de una definición clara de lo que es la Investigación de Operaciones vienen a colación una serie de puntos de vista que divergen con otros. Sin embargo, con el objeto de establecer una base para poder entender la naturaleza de la Investigación de Operaciones se hace uso de la definición de Churchman, Ackoff y Arnoff, bastante aceptada en el grupo de técnicos de Investigación de Operaciones. Esta definición dice:

"La Investigación de Operaciones es la aplicación, por grupos interdisciplinarios, del método científico a problemas relacionados con el control de las organizaciones o sistemas (hombre-máquina) a fin de que se produzcan soluciones que mejor sirvan a los objetivos de toda organización."

2.3. Beneficios de la Investigación de Operaciones

Dentro de la amplia gama de beneficios que brinda el uso de la Investigación de Operaciones, se citan los siguientes:

a) Incrementa la posibilidad de tomar decisiones.
b) Mejora la coordinación entre las múltiples componentes de la organización.
c) Mejora el control del sistema al intuir procedimientos sistemáticos.
d) Logra un mejor sistema al lograr que opere con costos más bajos.

2.4. Construcción de Modelos

Para la creación de un modelo es necesario considerar los tres tipos de modelos de la Investigación de Operaciones: Icónicos, Analógicos y Simbólicos.

a) Los modelos icónicos son imágenes a escala del sistema cuyo problema se requiere resolver.
b) Los modelos analógicos se basan en la representación de las propiedades de un sistema cuyas propiedades son equivalentes.
c) Los modelos simbólicos son conceptualizaciones abstractas del problema real a base del uso de letras, números, variables y ecuaciones. Este tipo de modelos son fáciles de manipular y permiten realizar con ellos un gran número de experimentos.

De las tres clases de modelos, los simbólicos son los más económicos de construir y operar, por tal motivo se ha hecho uso de dicho enfoque para la creación del modelo de confianza propuesto.

Ackoff y Sasieni consideran los siguientes grados de dificultad en la construcción de modelos:

- **Grado de Dificultad 1:** La estructura del sistema es sencilla de observar, analizar, entender y modelar a simple vista y/o como consecuencia de pláticas realizadas con el grupo de individuos que componen en sistema.

- **Grado de Dificulta 2:** La estructura del sistema es más complicada de modelar y, por lo tanto, se requiere de un sistema análogo cuya modelación cae dentro del grado anterior.

- **Grado de Dificultad 3:** La estructura del sistema puede deducirse o aproximarse en base a un análisis de cierta información.

- **Grado de Dificultad 4:** La estructura del sistema no se puede deducir, sino únicamente aproximar a base de pura experimentación.

- **Grado de Dificultad 5:** La estructura del sistema no se puede deducir (ya sea por falta de datos o experimentos) y, por lo tanto, se conceptualiza una estructura artificial.

A tipo conclusión se puede indicar que los modelos siempre deben ser menos complejos que el sistema real, de otra manera, para qué quebrarse la cabeza con modelos si se puede trabajar con el sistema real. De tal manera se indica que la propuesta del modelo de confianza se ubica en un Grado de Dificultad 3, debido a que se basa en el estudio de implementaciones de herramientas de seguridad informática en diversos entornos universitarios que se ha obtenido y palpado mediante observación directa en los diversos escenarios.

CAPÍTULO II: MECANISMOS O HERRAMIENTAS DE SEGURIDAD

2. MECANISMOS DE SEGURIDAD INFORMÁTICA

Es necesario conocer que mecanismo de seguridad puede servir para implementar uno o varios servicios de seguridad, al igual que un servicio de seguridad pueden ser implementados mediante varios mecanismos [2].

Indicando además que un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer los principios fundamentales de esta rama: la confidencialidad, la integridad y/o la disponibilidad de un sistema informático [9]. Siendo este el caso del modelo propuesto, puesto que como ya se lo mencionó en el capítulo anterior se han planteado los criterios acoplados a los principios de seguridad, en su mayoría; permitiéndole así a los sistemas o servicios informáticos contar con mayor nivel de confianza a la hora de operar en su entorno.

Existe una variedad amplia de mecanismos de seguridad informática. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan [9].

Estos mecanismos pueden ser algún dispositivo o herramienta física que permita resguardar un bien, un software o sistema que de igual manera ayude de algún modo a proteger un activo y que no precisamente es algo tangible, o una medida de seguridad que se implemente, por ejemplo las políticas de seguridad.

Cuando se habla del uso de mecanismos de seguridad estamos hablando de una de las estrategias más importantes dentro de una organización, puesto que la misma consiste en ir ascendiendo con tranquilidad pero con firmeza el nivel de seguridad.

Pero es importante recalcar que el simple cumplimiento formal de unas políticas de seguridad que, pese a todo, es bastante laxa, no garantiza que se tenga asegurado el máximo nivel de seguridad dentro de una organización y una protección eficaz.

2.1. Clasificación Según su Función

- **Preventivos.** Consisten en actuar antes de que un hecho ocurra y su función es detener agentes no deseados. Básicamente se concentran en el monitoreo de la información y de los bienes, registro de las actividades que se realizan en la organización y control de todos los activos y de quienes acceden a ellos [9].

- **Detectivos.** Son aquellos que tienen como objetivo detectar todo aquello que pueda ser una amenaza para los bienes. Se caracterizan por enviar un aviso y registrar la incidencia [9].

- **Correctivos.** Este tipo de mecanismos se encargan de reparar los errores cometidos o daños causados una vez que se ha cometido un ataque, o en otras palabras, modifican el estado del sistema de modo que vuelva a su estado original y adecuado [9].

La herramienta que se pretende implementar se incluye como un mecanismo preventivo y correctivo. Preventivo por el hecho de que mediante la implementación del Antivirus, se estaría previniendo la propagación de cualquier tipo de virus que puede afectar significativamente el funcionamiento de los equipos y sistemas informáticos. Detectivo, por el hecho de que mediante las diversas funcionalidades del programa antivirus se puede conocer qué equipos se encuentran en peligro o están expuestos a algún tipo de vulnerabilidad.

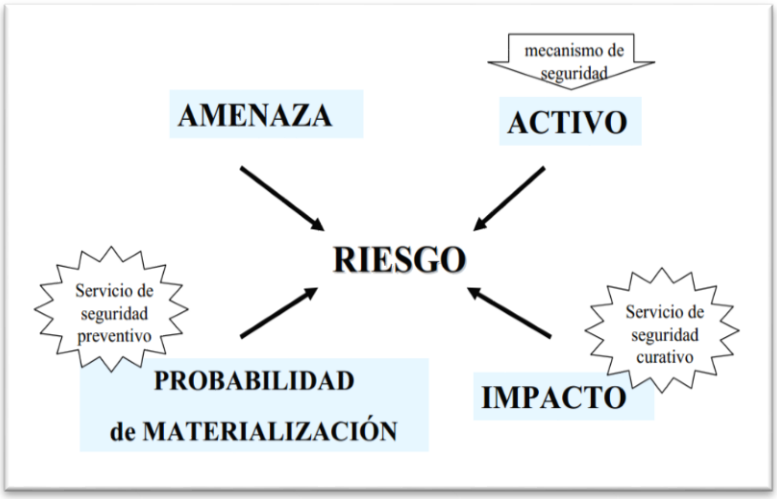


Figura 2: Aplicabilidad de los Mecanismos de Seguridad [11]

2.2. Estándares Internacionales

2.2.1. ISO/IEC 17799:27000

Dentro de los estándares internacionales relacionados con seguridad informática que se consideran importantes en la actualidad o por su importancia histórica, lo que consolida un alto grado de confianza en su contenido, se encuentra la norma ISO[4] 17799:27000 [3].

ISO 17799:27000, una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización [4]. Esta norma tiene como objetivo principal proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre instituciones.

El fragmento empleado para el trabajo de titulación es el relacionado a Gestión de Comunicaciones y Operaciones, específicamente en el apartado de Control de Cambios Operacionales, en donde nos indica que [4, 5]:

"Se deberían controlar los cambios en los sistemas y recursos de tratamiento de información. Un control inadecuado de dichos cambios es una causa habitual de fallos de seguridad o del sistema. Se deberían implantar responsabilidades y procedimientos formales de gestión para asegurar un control satisfactorio de todos los cambios en los equipos, el software o los procedimientos. Los programas operativos deberían estar sujetos a un control estricto de cambios. Cuando se cambien los programas se debería conservar un registro de auditoria conteniendo toda la información importante. Se deberían integrar, siempre que sea posible, los procedimientos de control de los cambios operacionales y aplicativos. En particular se deberían considerar los siguientes controles y medidas:"

a) la identificación y registro de cambios significativos;
b) la evaluación del posible impacto de los cambios;

4 ISO: International Estándar Organization

c) *un procedimiento formal de aprobación de los cambios propuestos;*
d) *la comunicación de los detalles de cambio a todas las personas que corresponda;*
e) *procedimientos que identifiquen las responsabilidades de abortar y recuperar los cambios sin éxito.*

Puesto que para hacer la evaluación de la herramienta con el uso del modelo se ha tomado en cuenta todos los cambios que conllevaría la implementación de un mecanismo de seguridad, desde los beneficios y los perjuicios o riesgos que se pueden suscitar durante el proceso.

2.2.2. ISO/IEC 27004:

La norma 27004 se creó para complementar a la norma ISO 27001, ya que la norma 27001 destaca que los controles tienen que ser medibles, ya que si no se es capaz de medir un control no servirá de nada para nuestro SGSI, por lo tanto hay que hacerlo medible, y es por esa razón por la que se realiza la normativa 27004 en la cual indica cómo debemos medir dichos controles, su objetivo consiste en hacerlos medibles [54].

Esta normativa 27004 sirve de ayuda para guiarnos sobre la creación y el uso de las mediciones con el fin de poder evaluar la eficiencia del sistema de gestión de la información aplicada a los controles y seguridad. Con esta normativa se incluye la gestión de información de seguridad de riesgos, procesos, política, objetivos de control, procedimientos, ayudar al proceso de su revisión, así como ayudar a determinar si alguno de los procesos de SGSI o controles necesitan ser mejorados o modificados[54].

El uso de esta normativa constituye una medición de la seguridad de la información. El sistema de gestión de la seguridad de la información nos ayudará evaluar y a identificar aquellos procesos o normas ineficaces en nuestro sistema de la seguridad de la información, así como los controles y prioridades de las acciones asociadas.

Gracias a esta norma será un punto de partida para el desarrollo de la medida de medición es importante para la comprensión de los riesgos de seguridad de información donde la entidad o la organización se puede

enfrentar o tener problemas. Queda aclarar que el objetivo de dicha normativa consiste en fortalecer la organización y que gracias a la normativa proporciona una información fiable a la entidad sobre los riesgos que corre en relación a la seguridad de información así como el estado de nuestro SGSI aplicado para la gestión de estos riesgos.

Sin lugar a dudas esta norma es de gran ayuda para la asignación de los pesos genéricos a los criterios que componen la propuesta del modelo de confianza en estudio, puesto que permitirán cuantificar mediante la calificación respectiva los aspectos y por ende determinar el valor total de factibilidad.

2.2.2.1. El modelo y método para las mediciones de seguridad

Para llevar a cabo el proceso de aplicación de métricas se necesita crear un programa con el fin de realizar la medición de la seguridad de la información de la entidad. El programa deberá centrarse en las ayudas que aportan dichas mediciones a la hora de tomar decisiones [54]. Por lo tanto este programa de mediciones debe estar basado en un "Modelo" de mediciones de seguridad de la información.

Este Modelo es una estructura que enlaza los atributos medibles con una entidad relevante. Estas entidades, incluyen procesos, productos, proyectos y recursos; que en este caso vendrían a ser los diferentes criterios en evaluación del modelo. Es decir, este modelo debe describir cómo estos criterios son cuantificados y convertidos a indicadores que provean bases para la toma de decisiones, sustentados en necesidades de información específica [54].

Para definir cómo los atributos deben ser medidos, esta norma propone también un Método. Existen dos tipos de métodos para cuantificar los atributos [54]:

- **Subjetivos:** Implica el criterio humano.

- **Objetivos:** Se basan en una regla numérica, que puede ser aplicada por personas o recursos automatizados.

Los métodos de medición pueden abarcar varios tipos de actividades y un mismo método puede aplicar a múltiples atributos. Algunos ejemplos de métodos son [54]:

- Encuestas/indagaciones.
- Observación.
- Cuestionarios.
- Valoración de conocimientos.
- Inspecciones.
- Re-ejecuciones.
- Consulta a sistemas.
- Monitorización ("Testing")
- Muestreo.

Un tema a considerar es la asociación de mediciones con determinadas escalas, de las cuales se proponen los siguientes tipos [54]:

- **Nominal:** Los valores son categóricos.
- **Ordinal:** Los valores son ordenados.
- **Intervalos:** Se poseen máximos y mínimos con distancias entre ellos.
- **Ratio:** Tienen escalas de distancias, relacionadas a mediciones.

2.2.3. ISO/IEC 27005:

Esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información. Corresponde a la organización definir su enfoque para la gestión del riesgo, dependiendo por ejemplo del alcance de su SGSI, del contexto de la gestión del riesgo o del sector industrial. Se puede utilizar una variedad de metodologías existentes bajo

la estructura descrita en esta norma para implementar los requisitos de un sistema de gestión de seguridad de la información [55].

Esta norma es pertinente para los directores y el personal involucrado en la gestión del riesgo en la seguridad de la información dentro de una organización y, cuando corresponda, para las partes externas que dan soporte a dichas actividades.

2.2.4. COBIT 5: Un Marco de negocio para el Gobierno y la Gestión de las TI de la Empresa

La información es un recurso clave para todas las empresas y desde el momento en que la información se crea hasta que es destruida, la tecnología juega un papel importante. La tecnología de la información está avanzando cada vez más y se ha generalizado en las empresas y en entornos sociales, públicos y de negocios [53].

Como resultado, hoy más que nunca, las empresas y sus ejecutivos se esfuerzan en:

- Mantener información de alta calidad para soportar las decisiones del negocio.
- Generar valor al negocio con las inversiones en TI, por ejemplo, alcanzando metas estratégicas y generando beneficios al negocio a través de un uso de las TI eficaz e innovador.
- Alcanzar la excelencia operativa a través de una aplicación de la tecnología fiable y eficiente.
- Mantener los riesgos relacionados con TI en un nivel aceptable
- Optimizar el coste de los servicios y tecnologías de TI
- Cumplir con las constantemente crecientes leyes, regulaciones, acuerdos contractuales y políticas aplicables.

Durante la pasada década, el término “gobierno” ha pasado a la vanguardia del pensamiento empresarial como respuesta a algunos ejemplos que han demostrado la importancia del buen gobierno y, en el otro extremo de la balanza, a incidentes corporativos a nivel global.

Empresas de éxito han reconocido que el comité y los ejecutivos deben aceptar las TI como cualquier otra parte importante de hacer negocios. Los comités y la dirección – tanto en funciones de negocio como de TI – deben colaborar y trabajar juntos, de modo que se incluya la TI en el enfoque del gobierno y la gestión. Además, cada vez se aprueba más legislación y se implementan regulaciones para cubrir esta necesidad [53].

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público [53].

CAPÍTULO III: MODELOS DE CONFIANZA

3. CONFIANZA-REPUTACIÓN

El término confianza se lo puede concebir como la medida en la que una persona está confiada y ansiosa de actuar en base a las palabras, las acciones y las decisiones de otros [12-16].

La confianza en sí, es un concepto abstracto que en la mayoría de las veces es usado indistintamente con términos relacionados como: credibilidad, confiabilidad o lealtad. Aparece un nuevo concepto que va de la mano de la confianza que es la reputación, debido a sus enfoques. En el campo de las Ciencias de la Computación encontramos diferentes modelos de confianza y reputación para variedades de dominio como, entre ellos: comercio electrónico, redes sociales, algoritmos genéticos, correo electrónico, web, comunidades científicas, consumidores y vendedores comerciales, criptografía, etc. Sin embargo, a pesar de la diversidad de las propuestas aún no existe una definición clara de confianza y reputación [15-16].

Para aclarar conceptos, a continuación se conceptualiza algunos términos que serán de gran ayuda para nuestro proyecto de investigación:

- Se considera el término confianza como el nivel de seguridad que se tiene sobre la correcta toma de decisiones a la hora de implementar mecanismos de seguridad en entornos universitarios, los mismos que deben ser evaluados en base a criterios previamente establecidos.

- La reputación es la percepción que una persona tiene sobre las intenciones y normas de otra, se reconoce la confianza de una persona sobre las capacidades, honestidad y formalidad de otra persona, basada en las recomendaciones de otros [12-16].

Se considera que la diferencia entre confianza y reputación depende de quien tenga experiencia previa con los mecanismos, es decir, si una persona tiene experiencia directa con un tipo de mecanismo de seguridad informática se puede decir que la persona tiene un valor de confianza para ese mecanismo. Por lo contrario, cuando el mecanismo de seguridad informática ha sido recomendado por otra persona que

previamente ha tenido experiencia con esta herramienta, entonces se puede decir que la herramienta tiene un valor de reputación.

3.1. Confianza y seguridad en la información

La utilización creciente de la tecnología de la información en virtualmente todos los ámbitos de la actividad económica, pública o privada, parece mostrar que es merecedora de confianza. Basta la experiencia común para percibir la dependencia de las organizaciones (y la sociedad en su conjunto) de una tecnología que se ha desarrollado en cinco décadas a un ritmo desconocido en la historia de las invenciones.

Tampoco es infrecuente encontrar recelos, por ejemplo cuando el público se plantea si es sensato confiar en los ordenadores. Ciertamente fundados, a juzgar por las noticias que con creciente aseidad aparecen en los medios de comunicación.

Los profesionales de la informática que se ocupan de la seguridad alertan acerca de riesgos que pudieran no estar controlados. Y también desde el ámbito político. Por ejemplo la preocupación por la Seguridad de los Sistemas de información se puede rastrear en los máximos niveles mundiales, europeos y nacionales. En el ámbito europeo esta preocupación culmina en la 'Cumbre' del Consejo de la Unión Europea en Lisboa (marzo de 2000), una de cuyas conclusiones reconoce que "la confianza del consumidor es un factor clave en el desarrollo del negocio electrónico". Para desarrollar la construcción de esa confianza, la 'Cumbre' portuguesa de Jefes de Estado y Gobierno europeos de Santa María de Feira (junio de 2000) ha establecido un Plan de Acción que fija tres líneas de actuación:

- Aumento de las soluciones disponibles para conseguir la seguridad en Internet.
- Mejora de la coordinación para combatir la 'ciberdelincuencia'
- Aumento de la seguridad en el acceso a los servicios electrónicos fomentando el uso de las tarjetas inteligentes en todas sus formas.

3.2. Modelos de Confianza y Reputación

Para clarificar un poco más la conceptualización de los modelos de confianza y reputación en vista de que no existe un modelo de este tipo para herramientas/mecanismos de seguridad informática, se realiza una breve descripción de los sistemas que han tenido mayor impacto en la sociedad debido a su amplitud y cobertura, concretamente los sistemas de comercio electrónico y los modelos de confianza basados en agentes, ya que estos han sido el eje principal de los modelos de confianza y reputación [12].

Como es de conocimiento total, los sitios Web[5] de comercio electrónico ofrecen productos y servicios, con la única finalidad de ofrecer un entorno de confianza en donde los usuarios puedan adquirir sus productos o servicios sin temor a ser engañados. Para ello cada sitio de comercio electrónico implementa diferentes mecanismos que garantizan la confianza del cliente al momento de realizar operaciones [12-16, 50-51].

De igual manera, existen otros modelos de confianza y reputación basados en agentes inteligentes. Sin embargo existen modelos de confianza orientados al campo de la seguridad informática, pero si bien es cierto están enfocados al área de la criptografía, los mismos que se basan en Web of Trust[6] , en donde se utilizan técnicas de seguridad informática basadas en la criptografía para estimar valores de confianza y reputación en comunidades virtuales [16].

Por tal motivo, es importante recalcar, que mediante la propuesta de un modelo de confianza que permita determinar cuándo es y cuándo no es factible implementar mecanismos de seguridad informática en entornos universitarios se podrá manejar una toma de decisiones mucho más adecuada en base a una evaluación previa del mecanismo que se pretenda implementar.

[5] Web o World Wide Web (WWW):Red Informática Mundial
[6] WOT: Web of Trust

3.3. Web Of Trust – Confianza en la Web

El concepto de WOT "Web of Trust"[7] se ha venido trabajando desde la creación del mecanismo PGP "Pretty Good Privacy" para seguridad de correos electrónicos[8], el cuál trata de plantear la idea de permitir y aceptar la identidad de un usuario en un sistema de comunicaciones siempre y cuando sea reconocido por otro usuario perteneciente a la plataforma, lo cual garantiza unas condiciones mínimas de Confianza para aceptarlo dentro de la plataforma que están compartiendo [17].

En este sentido nace un concepto que permite la interacción de usuarios sobre Redes Sociales y el cual es relacionado mediante el proyecto SIF (Social Interaction Framework)[9], el cual, en este Framework un agente evalúa la reputación de otro agente basado directamente en observaciones de otros usuarios participantes en la misma plataforma, mientras que los sistemas tradicionales electrónicos se deben fiar de mecanismos externos que sirvan de intermediarios entre las personas que desean comunicarse [17].

Una evolución que ha tenido esta estrategia, se ve reflejado en los plugins de los navegadores de Internet, propuestas planteados por navegadores como Internet Explorer y Mozilla Firefox, mediante componentes conocidos como WOT. Este plugin es un componente que se descarga en el navegador del usuario y evita problemas asociados sobre Internet, como avisos de páginas no confiables, robo de identidad, páginas en Internet de Comercio Electrónico no fiables, amenazas de seguridad de enlaces de páginas antes de ingresar en ellos, entre otros. WOT se basa en un único enfoque de crowdsourcing[10] que recoge las calificaciones y comentarios de una comunidad global de millones de usuarios que votan y hacer comentarios en los sitios web basados en sus experiencias personales.

A través de WOT y de su enfoque nos permite visitar algunos Sitios Webs de proveedores o comercializadoras de herramientas de seguridad informática, otorgándonos así un criterio más para evaluar la confiabilidad de implementación de algún mecanismo de seguridad informático.

---

[7] Sitio Oficial WOT: https://www.mywot.com/

[8] PGP: http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy

[9] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.70.3153&rep=rep1&type=pdf

[10] http://www.crowdsourcing.com/

CAPÍTULO IV: CASOS DE ESTUDIO

4. IMPLEMENTACIONES DE HERRAMIENTAS DE SEGURIDAD INFORMÁTICA.

4.1. CASO 1: Captura y Análisis de los ataques informáticos que sufren las redes de datos de la ESPOL[11], implantando una Honeynet con miras a mejorar la seguridad informática en redes de datos del Ecuador.

Las Honeynets proveen la estrategia de detectar los fallos y mejorar en la defensa cuando se usan en conjunto con otros mecanismos de seguridad. Al recoger información de las intrusiones y estudiarlas podemos conocer nuevas amenazas y herramientas aún no documentadas, determinando así patrones de ataque y los diferentes motivos de los intrusos. Las Honeynets son una herramienta, y puede ser usada para otros fines, como comprobar y desarrollar la capacidad de respuesta ante cualquier incidente. En las universidades pueden ser usadas para estudiar tipos y patrones de ataque o simplemente para investigar amenazas como función principal [18-20]. Por todos los beneficios y oportunidades que brinda este tipo de mecanismos es que se ha considerado como una de las más implementadas actualmente.

Recalcando que es muy importante incursionar en campos en los que la sociedad tecnológica poco lo hace, permitiendo así descubrir nuevas tecnologías en cuanto a seguridad informática, las mismas que vienen con un plus a su funcionalidad en los diversos entornos en los que se desempeña, más aún si estos entornos son universitarios y si estás instituciones como la ESPOL[12] cuentan con una variedad de servicios tanto internos como externos que se ven comprometidos con el cumplimiento de los principios de la seguridad de la información, que tiene como objetivo proteger la misma. El eje principal de todo esto es saber si es factible o no implementar estos mecanismos de seguridad, en este caso se pudo constatar que una de las arquitecturas de Honeynet resultó con muchos problemas debido a la falta de especificaciones técnicas lo que complicó la recolección y análisis del tráfico. Por lo tanto, se cree conveniente

[11] Escuela Superior Politécnica del Litoral: http://www.espol.edu.ec/
[12] Escuela Superior Politécnica del Litoral: http://www.espol.edu.ec/

realizar la elección en base a un modelo y que mejor si el mismo se basa en la confianza establecida por casos de estudio o experiencia de personal especializado con estas herramientas y específicamente con la implementación en entornos universitarios.

4.2. CASO 2: Implementación de un Sistema de Detección y Análisis de Intrusiones no Autorizadas utilizando Honeypots Caso Práctico DESITEL-ESPOCH[13] .

Los sistemas de detección de intrusos se han convertido en un componente importante en la caja de herramientas de un buen administrador de seguridad. Algunos aún no lo tienen claro, y piensan que un IDS (Intrusión Detection System) puede ser el remedio que nos lleve a la más absoluta tranquilidad y a una irreal sensación de seguridad, más peligrosa en muchos casos que la inseguridad en sí misma. Un detector de intrusos no es más que una de las medidas de seguridad que necesariamente hay que tornar para proteger una red. Una de las ventajas de estos sistemas es que proveen de la información necesaria para conocer los riesgos con los cuales contamos en la red. Además de poner de nuestro lado la capacidad de desarrollar seguridad, siendo esto último un punto crucial en la defensa de toda organización o institución [21].

El modelo propuesto se basa específicamente en la confianza y reputación que tienen determinadas herramientas lo que hace mucho más confiable el arriesgarse a implementarlas. Este es el caso del proyecto antes mencionado en donde se planteó la propuesta de implementación de una de las herramientas de seguridad más actuales con el fin de fortalecer el campo de la seguridad de la información dentro de la ESPOCH, permitiéndoles así darse cuenta, mediante los resultados si la decisión de implementación de este tipo de herramientas fue la más acertada o no.

En este contexto de estudio, se podría concluir que la implementación de este tipo de mecanismos de seguridad resultó favorable, quizás no en su totalidad, debido a su amplia gama de funcionalidad. Pero si brindó pautas para una mejor

[13] Escuela Politécnica de Chimborazo: http://www.espoch.edu.ec/

toma decisiones en futuras implementaciones de estas herramientas de seguridad, como los son las de tipo Honeypot.

4.3. CASO 3: Honeynet como apoyo a la Investigación de Seguridad de Redes en entornos Universitarios – UTPL[14] .

Tomando como análisis instituciones del medio local se ha indagado en el presente proyecto con el fin de consolidar mucho más la determinación de los criterios tomados en cuenta a la hora de implementar herramientas de seguridad informática y por ende mejorar la toma de decisiones en los centros de educación superior.

El proyecto ha visto en la tecnología Honeynet, una herramienta de seguridad valiosa, no solo para aportar a una seguridad proactiva, sino para constituir un potencial recurso de investigación; lo que aporta significativamente a la comunidad científica [22, 23, 52]. Tras un arduo espacio de investigación acerca de la tecnología, sus ventajas y desventajas se ha podido culminar el proyecto con éxito, lo que ha motivado a incluir casi en su totalidad los servicios tanto internos como externos de la Universidad, dando cabida a la realización de los siguientes proyectos:

- Análisis del Tráfico Malicioso en los Servicios Críticos Internos de la UTPL[15] [24].
- Análisis del Tráfico Malicioso de los Servicios Externos de la UTPL [25].”

Sin lugar a dudas, el fuerte trabajo investigativo conlleva a buenos y no tan buenos resultados, en este caso se ha obtenido un resultado valioso y que ha sembrado en futuras generaciones el despertar de la habilidad investigativa en este campo tan importante como lo es la seguridad.

[14] Universidad Técnica Particular de Loja: http://www.utpl.edu.ec/
[15] Universidad Técnica Particular de Loja: http://www.utpl.edu.ec/

e. Materiales y Métodos

El Trabajo de Titulación en cuestión, siendo un aporte original ha necesitado de íntegra búsqueda bibliográfica, encuestas, entrevistas a personal especializado en áreas principales como Redes, Seguridad y Administración de TIC's. Por tal motivo a continuación se informa cómo y en qué actividad se hace uso de cada técnica y método.

- **Técnica de la Entrevista**

  La aplicación de la presente técnica ha sido involucrada en gran parte del desarrollo del trabajo de titulación, fue aplicada principalmente para indagar con los especialistas acerca de la existencia de modelos o guías que pauten la confianza (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 2, APARTADO 2.3) en las implementaciones de herramientas de seguridad informática (Ver Anexos 4, 7-13), así como para solicitar información tanto interna en la UNL y externa en la ESPOL, ULVR, UTMACH, UTPL, CEDIA (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 1, APARTADO 1.1 Y 1.4). Es importante mencionar que el tipo de entrevistas empleadas fueron las entrevistas no estructuradas o abiertas, es decir, se partió de un tema específico para luego ir estructurando la misma de acuerdo a las respuestas del entrevistado.

- **Técnica de la Encuesta**

  La encuesta fue aplicada particularmente al momento de proponer el modelo al personal de la UTI (Ver Anexo 16-18) con el fin de verificar la aceptación de los criterios establecidos, así como para la obtención de los niveles o grados de confianza de cada uno de los escenarios (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.4); el tipo de encuesta aplicada fue de tipo estructurada, debido a que existía un orden y una respuesta esperada en cada una de las preguntas planteadas.

- **Búsqueda Bibliográfica**

  Este método o técnica de recolección de información jugó un papel primordial desde el planteamiento del problema así como en la búsqueda de modelos o estándares que se apeguen a los propósitos del modelo propuesto (VER SECCIÓN REVISIÓN LITERARIA), auscultando información de las experiencias de personal capacitado en áreas a fines a la seguridad que han tenido al momento de decidirse por la implementación de determinada herramienta. Tras la buena aplicación de esta técnica se ha logrado avanzar en cada una de las fases de la que está compuesto el presente trabajo de titulación.

- **Método o Técnica Estudio por Casos**

  El Estudio por Casos [26-29], consiste precisamente en proporcionar una serie de casos que representen situaciones problemáticas diversas de la vida real para que se estudien y analicen [30]. Partiendo de aquello se ha empleado dicho método durante el análisis de cada caso de estudio en donde se han realizado implementaciones de herramientas de seguridad informática en entornos universitarios, rescatando las ventajas y desventajas que han traído consigo éstas implementaciones. El uso de esta técnica está indicado especialmente para diagnosticar y decidir en el entorno de los problemas donde las relaciones humanas juegan un papel importante a la hora de tomar decisiones dentro de las organizaciones.

  Alrededor de estos entornos en donde se aplique esta técnica se puede:

  1. Analizar un problema.
  2. Determinar un método de análisis.
  3. Adquirir agilidad en determinar alternativas o cursos de acción.
  4. Tomar decisiones.

Previa a la aplicabilidad del método se ha incursionado en el Modelo Que Busca El Entrenamiento En La Resolución De Situaciones, el que requirió la consideración de un marco teórico y la aplicación de sus reglas

prácticas a la resolución de determinados problemas [26]. Luego de haber elegido uno de los modelos se ha trabajado sobre un caso en específico, los Casos Centrados en Generar Propuestas de Toma de Decisiones, el que permitió una mayor vinculación y apego al estudio del modelo propuesto.

El caso específico seleccionado se estructura mediante un decálogo de actividades que conlleva al análisis de la situación problemática hasta llegar al planteamiento de la propuesta solución para un determinado problema y en un escenario concreto. El decálogo mencionado ha sido dividido en cuatro fases, con el fin de trabajar con una mejor organización y desarrollo del proyecto, fases que están compuestas por tareas necesarias para llevar a cabo el cumplimiento de cada uno de los objetivos específicos y por ende el objetivo general del proyecto. Las fases y las tareas llevadas a cabo son las siguientes:

FASE I: Comparar las herramientas de seguridad informática que han sido implementadas actualmente en entornos universitarios.

- Conocer cuáles son las herramientas de seguridad informática más implementadas en entornos universitarios a nivel nacional (Ver Anexo 2).
- Determinar un número considerable de herramientas de seguridad informática a ser estudiadas.
- Comparar las herramientas seleccionadas anteriormente, rescatando sus ventajas y desventajas.
- Establecer qué tipo de herramientas de seguridad informáticas han sido las más implementadas en las universidades de nuestro país y porqué (Ver Anexos 2, 7-13).

FASE 2: Revisar la existencia de estándares que evalúen la confiabilidad en las herramientas de seguridad informática.

- Revisar exhaustivamente bibliografía para determinar la existencia de estándares internacionales o apartados de los mismos que brinden pautas para una buena toma de decisiones a la hora de implementar herramientas de seguridad informática.
- Seleccionar los estándares o apartados acordes al tema propuesto.

- Determinar la existencia de modelos de confianza que permitan valorar la confiabilidad a la hora de implementar herramientas de seguridad informática.
- Investigar cómo se realiza la toma de decisiones para implementar herramientas de seguridad informática en entornos universitarios mediante técnicas de recolección de datos (entrevistas, encuestas entre otras) a personal capacitado en temas de seguridad informática (Ver Anexos7-13).

FASE3: Proponer el modelo de confianza para la implementación de herramientas de seguridad informática.

- Determinar criterios válidos para juzgar la toma de decisiones a la hora de implementar herramientas de seguridad informática
- Contrastar los criterios establecidos con los principios de la seguridad de la información y estándares que cuiden de su cumplimiento para su validez.
- Establecer pesos genéricos para los criterios determinados a la hora de valorar una herramienta de seguridad informática, previa a su implementación.
- Proponer niveles de confianza para la aceptación de la herramienta de seguridad informática al momento de realizar su implementación (Ver Anexos 16-18).

FASE 4: Experimentar con el modelo propuesto sobre alguna de las herramientas de seguridad informática previamente estudiadas para evaluar su grado de confianza.

- Listar un número considerable de herramientas de seguridad informática más implementadas en entornos universitarios en base al estudio previamente realizado.
- Determinar un escenario de experimentación para evaluar el modelo propuesto (Ver Anexos 15).
- Evaluar la herramienta seleccionada mediante el modelo de confianza propuesta (Ver Anexo 19 y 22).
- Determinar el nivel de confianza de la herramienta de seguridad informática para su posterior implementación en entornos universitarios (Ver Anexo 22).
- Proponer a la comunidad científica la evaluación del modelo propuesto (Ver Anexo 23-24).

Es importante acotar que se surgió la oportunidad y necesidad de capacitación externa en el área de Seguridad Informática, pudiendo clarificar mucho más el entorno de trabajo para el planteamiento de la solución al problema principal.

f. Resultados

El presente trabajo de titulación, denominado “Modelo de Confianza para Herramientas de Seguridad Informática”, tiene como propósito la propuesta de un modelo de confianza en base a criterios, previamente estudiados y valorados con personal especializado, que permitan determinar la factibilidad de implementación de herramientas de seguridad informática en entornos universitarios. Brindando así un gran apoyo a la toma de decisiones en los centros de educación superior de nuestro país en lo que respecta a la seguridad de la información [30-31].

El trabajo antes mencionado fue desarrollado dentro de cuatro fases, las mismas que incluyen actividades siendo éstas últimas las que han permitido llegar al cumplimiento de cada uno de los objetivos planteados inicialmente. A continuación se indica los resultados obtenidos en el trabajo de titulación, mediante tareas y fases:

FASE I: Comparar las herramientas de seguridad informática que han sido implementadas actualmente en entornos universitarios.

1.1. Conocer cuáles son las herramientas de seguridad informática más implementadas en entornos universitarios a nivel nacional.

En base a una sólida revisión bibliográfica [18-25, 32] se ha podido observar de la escaza existencia de información acerca de las herramientas de seguridad que son implementadas en entornos universitarios, específicamente en nuestro país. El lugar en el que se ha podido recabar información importante ha sido por medio de proyectos internos, publicación de artículos o trabajos de titulación por parte de los estudiantes que se han formado en diferentes instituciones de educación superior. Los mismos que de una u otra forma dan un gran aporte en el ámbito de la seguridad de la información en las universidades, permitiéndonos conocer, con qué tipo de herramientas de seguridad informática se está trabajando así como sus fortalezas y debilidades dando paso a la propuesta de soluciones inmediatas a incidentes que se presenten y, por ende, mejorar el nivel de seguridad dentro de cada una de sus instituciones.

Por otro lado, mediante las charlas impartidas en el evento del DISI 2013[16] se pudo esclarecer mucho más el contexto del trabajo de titulación y en particular el área de la Seguridad de Información en Universidades miembros de CEDIA[17]; debido a que durante el evento se hizo partícipes de una serie de información en lo que respecta a la Seguridad Informática a todos los asistentes del evento, dentro de ello se difundió la lista oficial de las herramientas de seguridad informática más implementadas en entornos universitarios. Todo la información antes aludida, se ha logrado recolectar mediante la "I Encuesta de Seguridad de la Información a las Universidades miembros de CEDIA" [1] (Ver Anexos 1 y 2).

1.2. Determinar un número considerable de herramientas de seguridad informática a ser estudiadas.

Tan pronto como se determinó cuáles son las herramientas de seguridad informática más implementadas en entornos universitarios y con el apoyo del docente, Director del Trabajo de Titulación, se ha podido acordar un número considerable y oportuno para el análisis de las mismas; siendo cuatro el número de herramientas a estudiar, las que servirán como muestra para el modelo a proponer.

Tal y como se había indicado, mediante los resultados de las encuestas aplicadas por la UTPL en colaboración con CEDIA a las universidades ecuatorianas que son miembros del mencionado consorcio se consiguió puntualizar qué tipo de herramientas de seguridad informáticas son las que más se implementan en la actualidad en los centros de educación superior a nivel nacional. En lo que respecta a la encuesta, dentro de esta se da la existencia de un grupo en particular de preguntas, en donde se hace hincapié a los mecanismos tecnológicos que se utiliza, como universidad, para proteger los sistemas de información; obteniendo como respuesta un top de los mismos que ubican a los antivirus y firewalls como líderes (Ver Anexo 2).

[16] Día Internacional de la Seguridad Informática : http://csirt.utpl.edu.ec/disi2013
[17] Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado: http://www.cedia.org.ec/

Asimismo, en base a la investigación científica obtenida de los repositorios de las universidades que han implementado mecanismos de seguridad se ha podido determinar que dos de los mecanismos de seguridad más implementados son los IDS y Redes Trampa (Honeypot) [18-25]. Siendo dos alternativas más a la hora de asegurar los sistemas de información que radican en los entornos universitarios.

Tras la contrastación de los dos puntos de vista: entrevistas y revisión bibliográfica se ha resuelto analizar las herramientas de seguridad antes mencionadas, rescatando de cada una de ellas sus ventajas y desventajas; siendo esto el propósito de la siguiente actividad cumplida.

1.3. Comparar las herramientas seleccionadas anteriormente, rescatando sus ventajas y desventajas.

1.3.1. Antivirus

Como ya se lo citado en la actividad que le antecede, dentro de las herramientas de seguridad informática mayoritariamente implementadas se encuentra el conocido antivirus o en algunos casos conocido como antimalware. Es valedero rescatar que este tipo de mecanismos van desde una versión gratuita, que fácilmente se la puede obtener de la Web, hasta paquetes corporativos dotados de muchos servicios para contrarrestar la infección de los sistemas informáticos; así como el mejoramiento en el área de administración de las redes en donde se implementan [33-35].

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus evolucionen de igual manera, siendo más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos [34]. Dentro de las ventajas y desventajas primordiales de este tipo de mecanismos, se han citado las siguientes:

TABLA I

VENTAJAS Y DESVENTAJAS ANTIVIRUS

VENTAJAS	DESVENTAJAS
1. Análisis rápido **2.** Consumo de pocos recursos, según sea el caso de implementación. **3.** No necesita de lugares físicos extras (en equipos finales). **4.** Fácil instalación y uso. **5.** Rápido, Eficaz y Configurable.	**6.** Problemas al analizar archivos comprimidos (.zip, .rar, etc.) **7.** Por lo general, para gozar de todos los beneficios de algún programa antivirus es necesario comprar licencias corporativas. Dando como alternativa los antivirus free que mantienen un nivel mínimo de protección.

Acotando a lo inicialmente mencionado en el análisis de este mecanismo de seguridad, es rescatable indicar que Kaspersky[18] se encuentra entre los antivirus líderes a nivel mundial debido a las grandes prestaciones que brinda y de las certificaciones obtenidas a nivel mundial, seguido de Microsoft Security Essentials[19], Avast[20], entre otros [36].

1.3.2. Firewalls

Los Firewalls o Cortafuegos es otra de las herramientas de seguridad informática más implementadas no solo en entornos universitarios, como lo asegura la Encuesta aplicada a las universidades miembro de CEDIA (Ver Anexo 2), sino también en una variedad de organizaciones que buscan proteger su activo más importante, la información [37-39].

Específicamente, la función del firewall consiste en cortar o dejar pasar los intentos de comunicación que tiene todo el mundo (Internet) hacia nuestro ordenador o hacia nuestra red, según la situación del cortafuegos [40-42]. Acentuando que un cortafuegos actúa basándose en normas que establece

[18] Página Oficial: http://latam.kaspersky.com/
[19] Pagina Oficial: http://www.microsoft.com/
[20] Página Oficial: http://www.avast.com/

el administrador de seguridad, el administrador de red, o bien el usuario final. Estas reglas definen lo que tiene que hacer el cortafuegos cuando encuentre un paquete que cumpla con las características indicadas dentro de las reglas.

Es necesario palpar la realidad y notar que la implementación de un cortafuegos no es un mecanismos de seguridad que mantendrá la red protegida al cien por cien, ya que a diario incrementan las técnicas para acceder a la información de las organizaciones de forma no autorizada. Por tal motivo, en la mayoría de los casos la implementación de cortafuegos radica en el hecho de cubrir determinadas políticas de seguridad dentro de las capas OSI[21] [43-44]. Por ejemplo, así como la implementación de un cortafuegos en el nivel 3 de la capa OSI, es decir a nivel de red o TCP/IP, lo que permitiría determinar los intentos de conexión atendiendo a direcciones IP en donde su función principal es el filtrado de paquetes y determinar que puertos estarán únicamente habilitados. Cubriendo así políticas que se enfoquen en restringir la conexión a servicios específicos dentro de la red.

En sí, alrededor de lo antes mencionado es cómo se maneja la implementación de la mayoría de firewalls dentro de entornos universitarios con respecto a los diferentes niveles de la capa OSI (Nivel de Red, Transporte, Sesión, Presentación, Aplicación) [43-44]. A continuación se cita las más importantes ventajas y desventajas de los firewall:

[21] ***O****pen* ***S****ystem* ***I****nterconnection (sistemas de Interconexión Abiertos)*

TABLA II

VENTAJAS Y DESVENTAJAS FIREWALL

VENTAJAS	DESVENTAJAS
1. Alto grado de eficiencia en las redes, permitiendo, controlando todo el tráfico que entra y sale. 2. Refuerza políticas de seguridad, permitiendo que pasen por el solo servicios autorizados y cumplan las reglas establecidas. 3. Limita la exposición, por el hecho de mantener separada una sección de su red de otra, evitando que los problemas que impacten a una sección, afecten a toda la red. 4. La consola y los cortafuegos conectados directamente son seguros, ya que únicamente tendrán acceso el personal autorizado. 5. No requieren de excesivo espacio físico.	6. No puede protegeré la red contra personas internas. 7. No protege el tránsito de información que no pasa por él. 8. No puede proteger contra amenazas antes desconocidas, es decir un cortafuegos no puede defenderse de forma automática ante nuevas amenazas que surgen. 9. No existe protección eficaz contra virus, por el hecho de que un cortafuegos revisa todo el tránsito que pasa por él, pero no en detalles de datos. Por lo tanto, la protección de los virus en un cortafuegos no es muy práctica, además por la infinidad de novedosos virus informáticos.

1.3.3. IDS (Sistemas de Detección de Intrusos)

Quizás la mayoría de usuarios con conocimientos básicos en el área de Seguridad considerarían que un Sistema de Detección de Intrusos vendría a realizar el mismo trabajo que hace un cortafuegos (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 1, APARTADO 1.3, SUBAPARTADO 1.3.3) Pues es importante aclarar que no es así, ya que el enfoque principal del IDS es monitorear el tráfico de una red y los sistemas de una organización en busca de señales de intrusión, actividades de usuarios no autorizados y la ocurrencia de malas prácticas, como en el caso de los usuarios autorizados que intentan sobrepasar sus límites de restricción de acceso a la información [45].

Los cortafuego son una herramienta indispensable para hacer ejecutar las políticas de seguridad de las organizaciones, pero el hecho de que suelen realizar un análisis muy superficial de la información que circula por la red (generalmente, se quedan a nivel de red), hacen que muchos ataques sean simplemente invisibles para ellos [46]. Un IDS puede ser un dispositivo hardware auto contenido con una o varias interfaces, que se conecta a una o varias redes; o bien a una aplicaciones que se ejecuta en una o varias máquinas y analiza el tráfico de red que sus interfaces ven y/o los eventos generados por el sistema operativo y las aplicaciones locales. Existen muchos IDS en el mercado, desde software con un alto coste económico a ofertas totalmente gratuitas y capaces de asegurar los sistemas [47-49]. Lo que hay que tomar en cuenta es quién se encargará del soporte del IDS y si está lo suficientemente capacitado para actualizar la base de datos del IDS y conocer todos los tipos de ataques y sus variaciones, ya que a diario incrementan las técnicas de ataques. Posteriormente se han citado las principales ventajas y desventajas de los IDS:

TABLA III

VENTAJAS Y DESVENTAJAS IDS

VENTAJAS	DESVENTAJAS
1. Puede rastrear cada paso de un ataque. 2. No puede ser eludido fácilmente. 3. Existen versiones gratuitas con grandes características para reforzar la seguridad de las organizaciones. 4. Permite documentar amenazas existentes para las instituciones. 5. Incrementa la información sobre las intrusiones permitiendo así tomar medidas futuras. 6. No necesitan espacio físico adicional, puesto que puede encontrarse auto contenido junto a una o más interfaces.	7. No se puede bloquear el tráfico de intrusos. 8. Solo tan fuerte como su base de datos de amenazas. 9. Posibilidad de falsas alarmas. 10. Su implementación requiere de un alto nivel de conocimiento de estas tecnologías en lo que respecta a configuración y mantenimiento. 11. Configurar y gestionar la información de cada uno de los host que se está monitoreando. 12. Sólo permiten detectar ataques que conocen, por tanto tenemos que actualizarlos con las firmas de nuevos ataques.

1.3.4. Honeypot – Honeynets

Y como última, pero no menos importante, tenemos a una de las nuevas tecnologías en cuanto a seguridad, los Honeypots, son sistemas que busca atraer la atención del atacante sobre ellos [19-25], principalmente son implementados en los centros universitarios con el fin de estudiar la información acerca de los diferentes tipos de ataques a la red de estas instituciones.

Un Honeypot o “tarro de miel”, en el campo de la seguridad en redes de información, se define como un recurso de la red que se encuentra voluntariamente vulnerable para que el atacante pueda examinarla, atacarla.

Directamente no es la solución a ningún problema; su función principal es recoger información importante sobre el atacante que permita prevenir estas incursiones dentro del ámbito de la red real en casos futuros [22].

Las Honeynets[22] proveen la estrategia de detectar los fallos y mejorar en la defensa cuando se usan en conjunto con otros mecanismos de seguridad. Al recoger información de las intrusiones y estudiarlas podemos conocer nuevas amenazas y herramientas aún no documentadas, determinando así patrones de ataque y los diferentes motivos de los intrusos.

Las Honeynets son una herramienta, y puede ser usada para otros fines, como comprobar y desarrollar la capacidad de respuesta ante cualquier incidente. En las universidades pueden ser usadas para estudiar tipos y patrones de ataque o simplemente para investigar amenazas como función principal [21-25].

Esencialmente, los Honeypots son un concepto increıblemente simple, los cuales ofrecen una fortaleza muy ponderosa. Dentro de sus ventajas y desventajas se plantean las más rescatables en la siguiente tabla:

[22] Honeynets: Redes de Honeypots

TABLA IV

VENTAJAS Y DESVENTAJAS **HO**NEYPOT/HONEYNETS

VENTAJAS	**DESVENTAJAS**
1. Están diseñados para interactuar con cualquier cosa que interactúa con ellos inclusive con herramientas o tácticas nunca antes vistas o conocidas como “zero-days”. 2. Requiere de mínimos recursos para implementar una plataforma suficientemente potente para operar a gran escala. 3. Recopilan información de manera detallada a diferencia de otras herramientas de seguridad. 4. No hay tráfico normal, es decir toda actividad es considerada sospechosa. 5. No existen falsas alarmas o falsos positivos.	6. Tienen visión limitada, es decir solo pueden rastrear y capturar actividad destinada a interactuar directamente con los sistemas Honeypots. 7. Riesgo Inherente, el hecho de usar todas las tecnologías de seguridad implican un riesgo potencial. 8. Los Honeypots al igual que otros mecanismos de seguridad también corren el riesgo de ser secuestrados y por ende manipulados por el intruso para ser utilizados como plataforma de lanzamientos de ataques. 9. El mantenimiento requiere de mucho tiempo y conocimiento del tipo de Honeypot implementado.

Después de haber realizado el análisis de las ventajas y desventajas de cada una de las herramientas/mecanismos se ha podido comprobar que cada uno de ellos tiene su vital importancia y su jerarquía de implementación; dependiendo desde el punto de vista analizado. El hecho de que un centro de educación superior cuente con todas las herramientas analizadas implementadas no garantiza una total protección de los sistemas que permanecen en la red, el factor protección más bien radica en el hecho de que se implementen y usen correctamente con el fin de aprovechar al máximo cada uno de sus beneficios. Por ejemplificar: En el caso de querer implementar alguno de dichos

mecanismos, la primera actividad a verificar sería constatar el estado en que se encuentra la institución educativa en cuanto a Seguridad para luego si proceder a analizar y evaluar el proceso de implementación de un determinado mecanismo o herramienta de seguridad.

1.4. Establecer qué tipo de herramientas de seguridad informáticas han sido las más implementadas en las universidades de nuestro país y porqué.

Sin lugar a dudas, el avance de la tecnología es a diario al igual que las herramientas y tácticas de ataques a redes o sistemas de instituciones educativas, viéndose así en la necesidad de implementar una o más herramientas/mecanismos de seguridad, las mismas que de una u otra manera permitan “mantener segura la información”.

Principalmente, para implementar una herramienta de seguridad informática hay que tomar en cuenta, ¿qué es lo que vamos a proteger? y ¿de quién? Puesto que de esto parte el análisis para determinar la/s herramientas necesarias para éstas instituciones de educación superior. Por ejemplo, en lo que respecta a los equipos de cómputo de los departamentos administrativos, sería indispensable contar con programa antivirus corporativo el mismo que sea administrado desde una consola centralizada para evitar las actualizaciones de las bases de datos individuales lo que garantiza una pérdida de rendimiento en los equipos finales; implementaciones como esta permiten promover la protección de la información local, evitando así la propagación de los virus (Ver Anexos 6 y 8).

De igual manera, al momento de hablar de los sistemas en general, sistemas de información que son vulnerables algún daño, a groso modo, se debería tomar en cuenta en la seguridad de la red (dispositivos networking), optando así como solución principal la implementación de un firewall, el mismo que servirá como filtro para la información que ingresa y sale de la red. En el caso de ya contar con un Firewall se puede pensar en la implementación de otra herramienta de seguridad como lo son los Sistemas de Detección de Intrusos que actúan como complemento a la seguridad que brindan los cortafuegos,

permitiendo ya recoger información de los ataques a la red y sus sistemas (Ver Anexos 6 y 8).

Sin desmerecer las nuevas tecnologías y su implementación, es necesario dar a conocer que la implementación de este tipo de herramientas en instituciones de educación superior necesita de mucha investigación en dichas áreas con el fin de hacer una correcta elección de mecanismos de seguridad y por ende un alto desempeño de dichas herramientas.

Finalmente, se llega a la conclusión de que las herramientas más implementadas en entornos universitarios, sin lugar a dudas son las más conocidas o tradicionales (Antivirus, Firewalls, IDS) incursionando en el campo investigativo los sistemas Honeypots, los mismos que tienen grandes factores por explotar. Para ello, tras la información obtenida, consultada y analizada se propone una pequeña pirámide jerárquica de implementación en entornos universitarios.

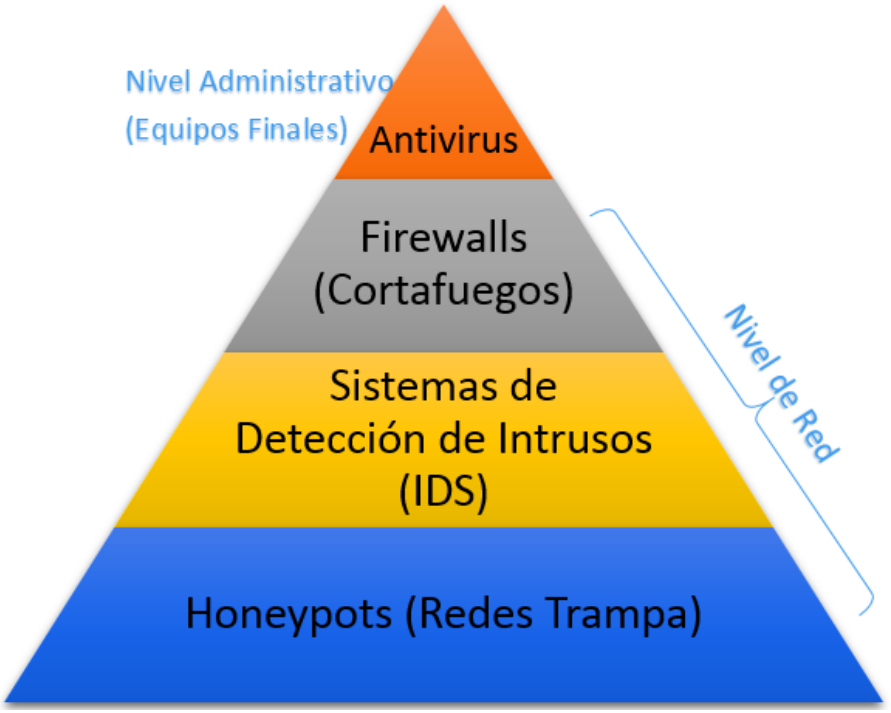


Figura 3: Herramientas más Implementadas en Entornos Universitarios

FASE 2: Revisar la existencia de estándares que evalúen la confiabilidad en las herramientas de seguridad informática.

2.1. Revisar exhaustivamente bibliografía para determinar la existencia de estándares internacionales o apartados de los mismos que brinden pautas para una buena toma de decisiones a la hora de implementar herramientas de seguridad informática.

Para el cumplimiento de esta actividad ha sido primordial la técnica de búsqueda bibliográfica, en lo que respecta a la existencia de estándares que proporcionen pautas para la correcta implementación de herramientas de seguridad informática, comprobando así la escaza existencia de dichos estándares, encontrando así un apartado lo más apegado al trabajo de titulación en la norma ISO 17799 [3-5, 50] en donde se expone una sección orientada al Control de Cambios Operacionales, proponiendo algunos puntos a tomar en cuenta a la hora de cambiar o implementar algún software que involucre la seguridad informática de la institución, en este caso educativa (VER SECCIÓN REVISIÓN LITERARIA CAPÍTULO II).

Otro mecanismo aplicado durante el desarrollo del trabajo de titulación El Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa: COBIT 5 [56]; el mismo que ha sido acoplado en la mayor de las posibilidades con el fin de darle mayor valor y aceptación al modelo propuesto.

De igual manera cabe mencionar que el uso y manejo de la norma ISO/IEC 27004 e ISO/IEC 27005 han sido de gran importancia para el planteamiento de métricas e indicadores que permitan evaluar cada uno de los criterios establecidos dentro del modelo propuesto, así como para mantener una guía de los riesgos que puede incluir cada nivel de confianza.

Es importante indicar que existen guías de buenas prácticas, como PMI, que involucran actividades para gestionar proyectos en ámbitos muy generalizados y por ello se ha visto la necesidad de indagar y aceptar el reto de proponer un modelo que permita contar con una pauta a la hora de implementar herramientas

de seguridad informática que, al final, permitirá conocer un nivel o grado de confianza para su implementación, evitando así la pérdida de tiempo en la toma de decisiones.

2.2. Seleccionar los estándares o apartados acordes al tema propuesto.

Dentro de los estándares internacionales relacionados con la toma de decisiones en el ámbito de la seguridad informática que se consideran importantes en la actualidad o por su importancia histórica, lo que consolida un alto grado de confianza en su contenido, se encuentra la norma ISO 17799 [3-5].
ISO 17799 siendo una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización [3-5, 50-51]. Esta norma tiene como objetivo principal proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre instituciones.

El fragmento a rescatar y a utilizar para el trabajo de titulación es la sección relacionada a Gestión de Comunicaciones y Operaciones, específicamente en el apartado de Control de Cambios Operacionales, en donde nos indica que [3-5]:

"Se deberían controlar los cambios en los sistemas y recursos de tratamiento de información. Un control inadecuado de dichos cambios es una causa habitual de fallos de seguridad o del sistema. Se deberían implantar responsabilidades y procedimientos formales de gestión para asegurar un control satisfactorio de todos los cambios en los equipos, el software o los procedimientos. Los programas operativos deberían estar sujetos a un control estricto de cambios. Cuando se cambien los programas se debería conservar un registro de auditoria conteniendo toda la información importante. Se deberían integrar, siempre que sea posible, los procedimientos de control de los cambios operacionales y aplicativos. En particular se deberían considerar los siguientes controles y medidas:"

f) la identificación y registro de cambios significativos;

g) la evaluación del posible impacto de los cambios;

h) un procedimiento formal de aprobación de los cambios propuestos;

i) la comunicación de los detalles de cambio a todas las personas que corresponda;

j) procedimientos que identifiquen las responsabilidades de abortar y recuperar los cambios sin éxito.

En lo que respecta a COBIT 5 se puede decir que ha permitido tomar un enfoque diferente a la hora de tomar decisiones de Tecnologías de Información en empresas de todo ámbito. Particularmente por el hecho de proporcionar un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas [53].

Como se indicó en el apartado anterior con respecto al uso de las normas ISO 27004, de las medidas y el método para su medición, y de la ISO 27005 que hace referencia a los riesgos; durante esta actividad del proyecto también se hizo uso de dichas normas para el fortalecimiento de la toma de decisiones durante la evaluación de implementaciones con el modelo de confianza propuesto.

En conclusión, ayuda a las empresas a crear el valor optimo desde IT manteniendo el equilibrio en la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos, es decir; permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa [53].

2.3. Determinar la existencia de modelos de confianza que permitan valorar la confiabilidad a la hora de implementar herramientas de seguridad informática.

En la actualidad, no existen modelos de confianza que planteen la factibilidad de implementación de herramientas de seguridad informática, pero es aquí en donde surgen nuevos conceptos y herramientas que de una u otra forma aportan a la fundamentación de este tipo de modelos.

Uno de los conceptos y herramientas es WOT [17] “Web of Trust”[23] el mismo que se ha venido trabajando desde la creación del mecanismo PGP “Pretty Good

[23] Sitio Oficial WOT: https://www.mywot.com/

Privacy" para seguridad de correos electrónicos[24], el cuál trata de plantear la idea de permitir y aceptar la identidad de un usuario en un sistema de comunicaciones siempre y cuando sea reconocido por otro usuario perteneciente a la plataforma, lo cual garantiza unas condiciones mínimas de Confianza para aceptarlo dentro de la plataforma que están compartiendo. En este sentido nace un concepto que permite la interacción de usuarios sobre Redes Sociales y el cual es relacionado mediante el proyecto SIF (Social Interaction Framework)[25], el cual, en este Framework un agente evalúa la reputación de otro agente basado directamente en observaciones de otros usuarios participantes en la misma plataforma, mientras que los sistemas tradicionales electrónicos se deben fiar de mecanismos externos que sirvan de intermediarios entre las personas que desean comunicarse.

Una evolución que ha tenido esta estrategia, se ve reflejado en los plugins de los navegadores de Internet, propuestas planteadas por navegadores como Internet Explorer y Mozilla Firefox, mediante componentes conocidos como WOT [17]. Dicho pluggin es un componente que se descarga en el navegador del usuario y evita problemas asociados sobre Internet, como avisos de páginas no confiables, robo de identidad, páginas en Internet de Comercio electrónico no fiables, amenazas de seguridad de enlaces de páginas antes de ingresar en ellos, entre otros. WOT se basa en un único enfoque de crowdsourcing[26] que recoge las calificaciones y comentarios de una comunidad global de millones de usuarios que votan y hacer comentarios en los sitios web basados en sus experiencias personales [16].

A través de WOT y de su enfoque ha permitido visitar algunos Sitios Webs de proveedores de herramientas de seguridad informática, vislumbrando así un criterio más para evaluar la confiabilidad de implementación de algún mecanismo de seguridad informática.

[24] PGP: http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy
[25] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.70.3153&rep=rep1&type=pdf
[26] http://www.crowdsourcing.com/

2.4. Investigar cómo se realiza la toma de decisiones para implementar herramientas de seguridad informática en entornos universitarios mediante técnicas de recolección de datos (entrevistas, encuestas entre otras) a personal capacitado en temas de seguridad informática.

Para el cumplimiento de esta tarea se ha realizado algunas entrevistas con personal capacitado en temas de seguridad informática y áreas a fines de cinco centros de educación superior, a nivel nacional, de acuerdo a la categorización de universidades establecida por el CEAACES[27] , entre ellos: la Escuela Politécnica del Litoral de Guayaquil, Universidad Nacional de Loja y Universidad Técnica Particular de Loja de la localidad, Universidad Laica Vicente Rocafuerte de Guayaquil y la Universidad Técnica de Machala (Ver Anexos 7-13). Tras realizar las respectivas entrevistas a los directivos de los departamentos, unidades y/o áreas de Tecnologías de Información de las universidades mencionadas se ha logrado una visión más clara del estado su estado actual en lo que respecta a la toma de decisiones en esta importante área, la Seguridad de la Información.

Por tal motivo se ha creído conveniente y apropiado plantear dos escenarios de análisis para el tema (Ver Anexos 6-13):

1. Instituciones educativas que poseen un nulo o mínimo porcentaje de explotación en el área de seguridad.
2. Instituciones que cuentan con departamentos/unidades orientados al campo de la seguridad informática y su toma de decisiones.

Por tal motivo, al hablar de implementación de herramientas de seguridad informática, en primer lugar nos deberíamos preguntar: ¿Estamos capacitados o contamos con personal idóneo para tomar decisiones de éste tipo? ¿En qué nivel de seguridad nos encontramos actualmente? ¿Contamos con las suficientes herramientas y controles de seguridad, ante cualquier

[27] http://www.ceaaces.gob.ec/

incidente informático? ¿Necesitamos más herramientas de seguridad informática en nuestro entorno? ¿Contamos con los recursos necesarios para su implementación? ¿Conocemos lo suficiente de una herramienta para implementarla? ¿En base a qué, escogeremos cierta herramienta?, éstas son algunas o las principales preguntas a tomarse en cuenta previa la elección de una herramienta de seguridad informática para su posterior implementación.

Luego de haber realizado esta autoevaluación dentro de nuestro entorno (universitario) se puede decir que estaríamos encaminados a realizar una confiable y acertada elección de alguna herramienta de seguridad informática, puesto que de ello depende un adecuado funcionamiento de las mismas, devengando los recursos empleados durante y después de su implementación.

Enfocándose en los dos ámbitos antes señalados, podemos recalcar lo siguiente, dentro de cada uno de ellos.

1. En cuanto a las **Instituciones educativas que poseen un nulo o mínimo porcentaje de seguridad**, se puede mencionar que, al hablar de seguridad informática y la implementación de herramientas de este tipo, principalmente se enfoca a brindar seguridad a equipos de Networking, que por lo general son los más propensos a problemas de vulnerabilidades informáticas y por ende a ataques de la misma índole (Ver Anexo 6). Y que las decisiones llevadas a cabo dependen específicamente del jefe o director del departamento de tecnologías con la ayuda del personal de redes y/o telecomunicaciones, puesto que es el personal más cercano al idóneo en la colaboración para este tipo de toma de decisiones.

   Es importante tomar en cuenta cómo se lleva la toma de decisiones en relación a los altos directivos de la institución, ya que por más acertada que resulte la propuesta de una solución por parte del departamento técnico esta puede llegar a ser o no aceptada por diversos motivos, justificables o no.

2. En lo que concierne a aquellas **Instituciones que cuentan con departamentos orientados el campo de la seguridad informática y su toma de decisiones,** se ha podido percibir un gran cambio desde la organización del personal hasta la mejoría en la toma de decisiones principalmente debido a la disponibilidad de presupuesto (Ver Anexo 7-9 y 12).

Es así que, en primer lugar, antes de la elección de herramientas de seguridad informática; se inmiscuye al personal o departamentos cuya función es la gestión tanto interna como externa de proyectos para bienestar de la institución, entre ellos trabajos de titulación, lo que conlleva a realizar estudios vigorosos de factibilidad tanto económica, técnica como operativa de los proyectos en discusión. Lo que fortalece un buen resultado del paso detallado anteriormente.

Asimismo, en caso de contar con herramientas ya implementadas, se puede hacer uso de estas para realizar un FODA, determinado así la factibilidad de implementar nuevas herramientas de seguridad informática; aquello se puede realizar haciendo ataques internos para determinar las “huecos” por los cuales pueden ser perjudicados los sistemas y la información contenida en ellos.

Seguidamente se procede a obtener información acerca de los últimos proveedores de herramientas de seguridad informáticas, elaborando así una etapa de licitación, etapa que incluye la convocatoria de los proveedores a ofertar productos que cubran las necesidades de la institución, es decir se publica un concurso público mediante los diferentes medios de comunicación, generalmente escritos. Es así como, en conjunto con el personal encargado de proyectos para la institución y el personal encargado del área de la seguridad informática, se procede a receptar las ofertas de los proveedores postulantes, dentro de un período establecido.

Ya analizada cada una de las propuesta se procede a escoger un número considerable de las mejores propuestas, (puede ser dos o tres) dependiendo la cantidad de ofertantes y de la reputación-confiabilidad que tienen en los entornos universitarios; para luego comunicarse con cada uno de los representantes y pedir la oferta presencial del producto, en donde cada uno de los proveedores venderá su producto de la mejor manera a los responsables de la institución. En este momento se realizan pruebas técnicas o de evaluación de las herramientas propuestas, en caso de ser necesario, pruebas realizadas por el personal especialista en cada área: desarrollo, redes, telecomunicaciones, seguridades, etc.
Así mismo, existen casos en los que se procede a valorar ciertos criterios establecidos por los departamentos de proyectos, criterios que por lo general están enfocados al PMI (Gestión de Proyectos) y principalmente a las necesidades de la institución.

Luego de la evaluación, calificación y asegurándose de que la oferta escogida brinde las mejores garantías (capacitaciones, soporte técnico), es decir los mejores beneficios en general, para la implantación de las herramientas de seguridad informática se procede a la finalización de la etapa de licitación, es decir la legalización del contrato para la implementación de dicha herramienta. Más allá de la correcta elección de una herramienta de seguridad informática, está el hecho de contar con personal capacitado y dispuesto a brindar soporte, así como a aplicar los controles necesarios para salvaguardar la información que circula por las redes universitarias.

FASE3: Proponer el modelo de confianza para la implementación de herramientas de seguridad informática.

3.1. *Determinar criterios válidos para juzgar la toma de decisiones a la hora de implementar herramientas de seguridad informática.*

Previa la determinación de criterios ha sido fundamental tomar como base el proceso de elaboración de un modelo, de la Investigación de Operaciones, que permite determinar el tipo de modelo así como el grado que implica construirlo en base a la información obtenida y el tipo de problema que se requiere solucionar.

Partiendo de aquello es necesario mencionar que el tipo de modelo a crear es un modelo simbólico, puesto que es una conceptualización abstracta del problema real a base del uso de letras, números, variables. Y que en este caso se hace uso de criterios para la evaluación de implementaciones de herramientas de seguridad informática como parámetros del modelo propuesto. Por otra parte el modelo propuesto a construir tiene un grado de dificultad 3, debido a que su estructura puede deducirse o aproximarse en base al análisis realizado en cada una de las instituciones de educación superior visitadas, lo que otorga un mayor grado de confiabilidad en la construcción del presente modelo de confianza.

Tomando como base lo tratado en líneas anteriores se recalca que la determinación de criterios para el modelo propuesto se ha realizado basándose en las diversas entrevistas con personal especializado en Seguridad y Redes de las universidades visitadas: ESPOL, UNL, UTPL, ULVR y UTMACH; asimismo mediante búsquedas bibliográficas de trabajos de titulación de otras instituciones educativas a nivel nacional en las que se hace referencia a un ¿Por qué? Se implementa determinada herramienta.

Gracias a la información brindada (Ver Anexos 6-13) y consultada se ha podido establecer tres aspectos principales: ECONÓMICO, REPUTACIÓN-CONFIABILIDAD, TÉCNICO. Cada uno de ellos incluye criterios a tomarse en cuenta a la hora de evaluar una herramienta de seguridad informática previa a

su implementación en un entorno universitario. Después del respectivo análisis con el Director del Trabajo de Titulación se ha visto la necesidad de plantear más de un escenario de evaluación, siendo tres los escenarios propuestos dentro del modelo, escenarios que pueden producirse durante la evaluación de la implementación de estas herramientas, entre ellos: cuando la herramienta a implementarse es Propietaria/Privativa, cuando es de acceso abierto Libre/Gratuita y cuando la implementación de herramientas de seguridad informática se la realiza mediante Proyectos Estudiantiles (Desarrollo o Adaptación de Herramientas) siendo este último un escenario opcional tomando en cuenta el riesgo que puede conllevar el realizar una mala implementación.

Recalcando que el modelo presentado es un modelo genérico, que permitirá a las universidades adaptarlos a su entorno actual. El modelo propuesto se encuentra estructurado de la siguiente forma:

a) Escenario 1: Herramienta Propietaria/Privativa

TABLA V

CRITERIOS ESCENARIO 1

CRITERIOS
ASPECTO ECONÓMICO
• Disponibilidad de Presupuesto o Estudios previos de Factibilidad
• Inversión retribuya con los beneficios obtenidos o Estudio y Valoraciones Técnicas del Entorno y Equipos
ASPECTO REPUTACIÓN-CONFIABILIDAD
• Reputación-Confiabilidad de la Herramienta: o WOT (Web Of Trust): Reputación en la Web o Certificaciones Obtenidas
• Reputación-Confiabilidad del Proveedor: o Experiencia con el Producto (Herramienta) o Experiencia en otras Instituciones Educativas
ASPECTO TÉCNICO
• Evaluación de Herramienta o Pruebas Internas-DEMO

○ Lenguaje Base ○ S.O Soportados
• Protección de Equipos de Networking ○ Total o Parcial
• Cumplimiento de las políticas de acceso y controles a los sistemas ○ Políticas Institucionales y/o Departamentales
• Espacio Físico y Lógico ○ Normal o Limitado
• Duración del soporte ○ Meses/Años
• Capacitación al personal ○ Meses/Años
• Garantías ○ Meses/Años

b) Escenario 2: Herramienta Libre/Gratuita

TABLA VI

CRITERIOS ESCENARIO 2

CRITERIOS
ASPECTO ECONÓMICO
• Inversión retribuya con los beneficios obtenidos ○ Estudio y Valoraciones Técnicas del Entorno y Equipos
ASPECTO REPUTACIÓN-CONFIABILIDAD
• Reputación-Confiabilidad de la Herramienta: ○ WOT (Web Of Trust): Reputación en la Web ○ Certificaciones Obtenidas
• Reputación-Confiabilidad del Proveedor: ○ Experiencia con el Producto (Herramienta) ○ Experiencia en otras Instituciones Educativas
ASPECTO TÉCNICO
• Evaluación de Herramienta

○ Pruebas Internas-DEMO ○ Lenguaje Base ○ S.O Soportados
• Protección de Equipos de Networking ○ Total o Parcial
• Cumplimiento de las políticas de acceso y controles a los sistemas ○ Políticas Institucionales y/o Departamentales
• Espacio Físico y Lógico ○ Normal o Limitado
• Soporte ○ Duración Soporte Online ○ Comunidad para Soporte

c) Escenario 3: Proyectos Estudiantiles

TABLA VII

CRITERIOS ESCENARIO 3

CRITERIOS
ASPECTO ECONÓMICO
• Disponibilidad de Presupuesto ○ Estudios previos de Factibilidad
• Inversión retribuya con los beneficios obtenidos ○ Estudio y Valoraciones Técnicas del Entorno y Equipos
ASPECTO REPUTACIÓN-CONFIABILIDAD
• Reputación-Confiabilidad de la Herramienta: ○ WOT (Web Of Trust): Reputación en la Web ○ Certificaciones Obtenidas
• Reputación-Confiabilidad del Proveedor: ○ Experiencia con el Producto (Herramienta) ○ Experiencia en otras Instituciones Educativas

ASPECTO TÉCNICO

• Evaluación de Herramienta
  o Pruebas Internas-DEMO
  o Lenguaje Base
  o S.O Soportados

• Protección de Equipos de Networking   o Total o Parcial
• Cumplimiento de las políticas de acceso y controles a los sistemas   o Políticas Institucionales y/o Departamentales
• Espacio Físico y Lógico   o Normal o Limitado
• Duración de Licencias   o Meses/Años

3.2. *Contrastar los criterios establecidos con los principios de la seguridad de la información y estándares que cuiden de su cumplimiento para su validez.*

La propuesta de este modelo de confianza tiene por objetivo la determinación de criterios que permitan evaluar la confiablidad de implementación de las herramientas de seguridad informática, así como a los proveedores de las mismas; puesto que de ello depende la toma de buenas o malas decisiones de éste tipo de herramientas y por ende su correcto funcionamiento. Partiendo de lo antes mencionado, se procede a contrastar los diferentes criterios planteados con los principios básicos de la seguridad y los apartados que hagan mención a la toma de decisiones, específicamente, en cuanto a cambios operacionales dentro de la institución. Así como con COBIT 5 para una buena gestión de TI en la institución.

3.2.1. *ASPECTO ECONÓMICO:*

- ***Disponibilidad Presupuesto***

  En lo que concierne a la evaluación de este criterio se hace referencia a la Gestión de Comunicaciones dentro de la norma ISO 17799:27000 [3-5] permitiendo así constatar que exista el presupuesto necesario y que sea justificable la implementación de la herramienta de seguridad.

  Por su parte se cubre el proceso de Gestión del Presupuesto y los Costes del Modelo de Referencia de Procesos de COBIT 5 que hace mención al hecho de alinear, planificar y organizar todos las actividades que tengan que ver con el presupuesto, todo ello previo a la aceptación de una propuesta y por ende a la implementación de herramientas de seguridad informática.

  En base a los motivos señalados se considera recomendable realizar estudios de factibilidad previos, que pueden ser llevados a cabo por personal encargado de proyectos estudiantiles o institucionales. Así como ser parte de anteproyectos en el caso de presentarse la implementación de una herramienta de seguridad informática mediante proyectos estudiantiles, como lo indica el escenario 3 del modelo propuesto.

- ***Inversión retribuya los servicios obtenidos tras la implementación.***

  Sin lugar a dudas, el que los beneficios obtenidos con determinada implementación sean los mejores, es uno de los primeros objetivos de todo proyecto. Por tal motivo, este criterio permite evaluar y contrastar que los beneficios obtenidos sean retribuidos con la inversión a realizarse.

  Es por ello que este criterio va de la mano con Estudios y Valoraciones Técnicas del Entorno y Equipos para constatar la existencia de todos los materiales tecnológicos necesarios para la correcta implementación de herramientas de seguridad informática en centros de educación superior.

En el presente trabajo de titulación se ha delimitado dicho análisis puesto que incluye mucha más investigación o, a su vez, un proceso investigativo adicional y minucioso.

3.2.2. *ASPECTO REPUTACIÓN-CONFIABILIDAD*

- ***Reputación-Confiabilidad de la Herramienta:***

  Al hablar de la Reputación y Confiabilidad de la herramienta se está hablando de parte del corazón del modelo propuesto, debido a que de ello depende en gran parte la viabilidad o no de la implementación de herramientas de seguridad informática. Siendo aquí donde se hace referencia a los procesos de Gestión de la Estrategia y Gestión de la Innovación del modelo de referencia de COBIT 5 [53], los que hacen mención al motivo de selección de determinada herramienta y el valor de innovación que podría brindar al entorno universitario en donde se implemente.

  Es así como se plantea hacer uso de herramientas tecnológicas disponibles en la Web para realizar parte de la valoración del mencionado criterio, mediante el uso de WOT.

  WOT (Web Of Trust): Reputación en la Web, permite obtener una valoración Web, es decir el nivel que se les otorga por ser sitios de confianza; al lugar donde se alojan determinadas herramientas de carácter privativo como gratuitas, lo que conlleva hacer adquisiciones de manera honesta y responsable, dicha valoración obtenida a través de millones de usuarios y validada de fuentes terceras, como listas negras.

  Este complemento, específicamente, cubre los tres principios básicos de la seguridad de la seguridad de la información, debido a que WOT toma como ejes principales dichos principios para la calificación de los sitios Web; verificando si sitio es seguro o no? ¿La información contenida es íntegra sin alteraciones? ¿El sitio tiene disponibilidad de sus servicios sin restricción alguna? [17]

Otro aspecto importante a evaluar dentro de este criterio es el de las Certificaciones Obtenidas por parte de las herramientas en discusión, puesto que el haber alcanzado determinadas certificaciones o reconocimientos tanto nacionales como internacionales otorga un gran valor de confiabilidad a la hora de decidir por una solución tecnológica en el campo de la seguridad informática.

- **Reputación-Confiabilidad del Proveedor**:

  La parte complementaria y central del modelo propuesto la compone la evaluación de la Reputación y confiabilidad del Proveedor para con la herramienta y los entornos, en este caso educativos, ya que en este criterio se juzga dos aspectos primordiales a la hora de dar por elegida una oferta de implementación.

  De igual forma que en los criterios anteriores, este no es la excepción, debido a que se complementa con el Proceso de Gestión de Proveedores del Modelo de Referencia de Procesos para la Gestión de TI en Empresas de COBIT 5 [53]. Proceso que da como ejes principales la Planificación y Organización de la evaluación de los proveedores ofertantes.

  El primer aspecto en evaluación dentro de este criterio es la **Experiencia con el Producto (Herramienta),** es decir durante la oferta de la propuesta se solicitara al proveedor dar a conocer y validar la experiencia que tienen con la herramienta que se pretende implementar. El segundo, y no menos importante aspecto a evaluar es la **Experiencia en otras Instituciones Educativas.** Durante la evaluación del presente ítem interviene la perspicacia y relaciones interpersonales con miembros de otras instituciones de educación superior, específicamente con personal encargado de la seguridad informática de la institución o a su vez accediendo a los servicios en donde se tiene implementadas las herramientas y comprobar su funcionamiento. Ya que en este punto se obtiene información de las experiencias que han tenido otras instituciones al implementar herramientas similares o con el mismo proveedor, obteniendo así un valor adicional de evaluación para los proveedores ofertantes de herramientas.

3.2.3. *ASPECTO TÉCNICO:*

- **Evaluación de Herramienta**

  El evaluar la herramienta previamente a su implementación es uno de los puntos más importantes dentro del modelo propuesto, así como en cada uno de sus escenarios. Dentro de dicho criterio se contrasta los riesgos que conllevaría la implementación en el entorno, pudiendo así observar los pro y contras de la misma, gracias a tomar en cuenta el cambio operacional que proporciona la Norma ISO 17799.

  Así como el Proceso de Supervisar, Evaluar y Valorar del Modelo de Referencia de Procesos de COBIT 5 [53], que permite valorar el desempeño total o parcial de la herramienta; tomando en cuenta dos puntos importantes, como: la flexibilidad en cuanto al lenguaje base en el cual fue desarrollada la herramienta y los sistemas operativos en los que se podría llevar a cabo una correcta implementación. Puesto que de gran parte de ello dependerá un correcto funcionamiento y reducción de riesgos en un futuro.

- **Protección de Equipos de Networking[28].**

  En este apartado se hace énfasis en verificar si la herramienta de seguridad en evaluación protege total o parcial y con carácter esencial los dispositivos networking. Asegurando así su buen funcionamiento y protección de la información que se maneja a través de ellos. El presente criterio a evaluar va acorde a la Gestión de Seguridad lo que lleva consigo planificar y organizar el proceso de protección de los equipos de networking. Asimismo, es aplicable el proceso de Gestión de Operaciones del Modelo de Referencia de Procesos de COBIT 5 [53] a la hora de hacer la entrega de la herramienta puesta en marcha o a través de las pruebas necesarias previas a la misma.

  La protección, a groso modo, debe ir desde que los routers empiezan el enrutamiento y transmisión de los paquetes a los diferentes enlaces en la red hasta los equipos finales que sería el área administrativa de los

[28] Equipos Networking: Dispositivos que se encuentran conectados a un segmento de la red

centros de educación superior, permitiéndole así el correcto funcionamiento de todos los Web Services[29] dentro de la institución.

- **Cumplimiento de las políticas de acceso y controles a los sistemas.**

  Uno de los criterios con mayor relevancia, sin desmerecer los demás, pero concibiendo que al implementar una herramienta de seguridad informática se debe tomar muy en cuenta que dicha herramienta sirva como pilar fundamental para hacer cumplir tanto las políticas de seguridad institucionales como departamentales implementadas dentro del centro de educación superior, que van desde el acceso y control a los diferentes sistemas de la institución hasta el acceso físico a los dispositivos networking.

  Este apartado mayoritariamente dependería de la elaboración y del cómo se estén llevando a cabo el cumplimiento de las políticas de seguridad en general del departamento encargado de los sistemas informáticos del entorno universitario en estudio. Puesto que tanto las políticas de seguridad como la puesta en marcha de alguna herramienta de seguridad informática, deben ir de la mano para afianzar mucho más el cuidado de los principios de la seguridad de la información.

  Es importante mencionar que la propuesta del presente modelo, está acorde a las Políticas de la Unidad de Telecomunicaciones de la UNL, en el apartado de la Política del Desarrollo Informático (Ver Anexo 29).

- **Espacio físico y lógico suficiente para la implementación.**

  El espacio físico influye mucho cuando la herramienta a implementar requiere de dispositivos networking adicionales de los que cuenta la institución, por ejemplo: en el caso de necesitar de la compra de router's, se necesita verificar que exista espacio físico en los racks; en caso de que la herramienta necesite de algún servidor, dedicado de igual forma,

[29] Web Services: Tecnologías que sirve para intercambiar datos y servicios entre aplicaciones

constatar de que exista el espacio necesario para su colocación dentro del centro de cómputo de la universidad.

Por otro lado al hablar de espacio lógico, se toma en cuenta el escenario donde ya existe el suficiente espacio lógico en los servidores con los que cuenta la institución y/o asimismo que se cuenta con puertos disponibles en los routers[30] o switchs[31] para poner en funcionamiento la herramienta en evaluación.

Todo lo indicado va contrarrestando el buen manejo del Proceso de la Supervisión, Evaluación y Valorización de Conformidad con los Requerimientos Externos, es decir asegurarse de la existencia total del espacio físico y lógico para la implementación de una determinada herramienta de seguridad informática para luego no presentar problemas durante la entrega y soporte para con la herramienta..

- **Duración del soporte.**

  El planteamiento de este criterio es de vital importancia dentro de la propuesta, ya que se trata de la duración del soporte técnico que brindarán a la institución al momento de optar por alguna herramienta propietaria/privativa, ya que si bien es cierto depende mucho de aquello la necesidad de invertir en capacitación de personal para su administración. Todo aquello debe ser tomado en cuenta al analizar detenidamente las propuestas y negociación de la herramienta a implementar.

  Otro punto importante a considerar radica en el escenario 2, Herramienta Libre/Gratuita, puesto que se toma en cuenta el Soporte Online que nos brinda la herramienta así como la disponibilidad de Comunidades que aporten al mantenimiento de la misma.

[30] Router: Dispositivo que proporciona conectividad a nivel de red enviando paquetes de datos de una red a otra.
[31] Switch: Dispositivo que permite interconectar dos o más segmentos de la red.

Todo lo manifestado con anterioridad se encuentra contemplado dentro de los Procesos para la Gestión de TI del Modelo de Referencia de Procesos que brinda COBIT 5 [53].

- **Capacitación al personal.**

  Como ya se mencionó en el aspecto anterior, la capacitación al personal que va a estar al mando de la herramienta informática en evaluación, es de gran importancia a la hora de optar por alguna herramienta privativa en mayor magnitud; puesto que no resultaría viable adquirir una herramienta de bajo costo, pero que no brindara capacitación para el personal que la manejará en los próximos meses o años. Con esta importancia es considerada la capacitación dentro del Control de Cambios Operacionales de la Norma ISO 17799 así como en el Modelo de Referencia de Procesos COBIT 5 [53] en el área de la Entrega y Soporte de la Herramienta.

- **Garantías.**

  Revisar la viabilidad, de la herramienta en evaluación, si proporciona un tiempo aceptable de garantía (meses/años); al menos mientras el personal de la institución educativa se encuentre capacitado y en condiciones de solucionar problemas de algún tipo, principalmente para cumplir parcial o totalmente con las políticas de la institución.

  O en su caso, se debería tomar en cuenta el criterio que hace énfasis a la Duración de Licencias (VER SECCIÓN RESULTADOS, FASE 3 APARTADO 3.2, SUB APARTADO 3.2.3 **DURACIÓN LICENCIAS**) y las consideraciones que conlleva.

- **Duración Licencias**

  Criterio que al igual que el resto necesita de su respectivo análisis y valoración, puesto que en la mayoría de los casos va de la mano con la Capacitación del Personal (VER SECCIÓN RESULTADOS, FASE 3

APARTADO 3.2, SUB APARTADO 3.2.3 **CAPACITACIÓN**) debido a que la siendo el escenario una Herramienta Propietaria/Privativa, se tomaría muy en cuenta la duración de licencia de la/s herramienta/s a implementarse.

3.3. *Establecer pesos genéricos para los criterios determinados a la hora de valorar una herramienta de seguridad informática, previa a su implementación.*

Al hablar del establecimiento de pesos genéricos es necesario prestarle toda la importancia del caso debido a que el modelo propuesto originalmente es un modelo subjetivo, debido a que su creación se basa fundamentalmente en el criterio humano especializadas en el tema, es necesario darle un valor adicional y objetivo, es así que se empleara el método objetivo para la determinación del porcentaje obtenido en cada criterio y aspecto del modelo propuesto, mediante la aplicación de una regla numérica de ponderación. Es decir, mediante el uso de este método el modelo permitirá describir cómo estos criterios son cuantificados y convertidos a indicadores que provean bases para la toma de decisiones, sustentados en necesidades de información específica.

Es así que antes de proceder con el proceso de asignación de los pesos porcentuales se deberá realizar una pre-valoración en base al impacto obtenido en cada criterio, impacto que permitirá valorar entre 1 y 5 para proceder a la aplicación de una regla de tres con el valor genérico porcentual asignado a cada criterio y aspecto a evaluar en la propuesta del modelo. Todo ello debido a la aplicación del método de medición objetiva y escala de intervalos que pauta la Norma ISO/IEC 27004. Para ejemplificar, se plantea la evaluación del Aspecto Económico:

Aspecto Económico 20%:

- Disponibilidad de Presupuesto 10%
- Inversión retribuya con los Beneficios 10%

Como primer punto se deberá valorar entre 1 y 5 cada aspecto según la situación del entorno a evaluar y de la situación presentada. A modo ejemplo

se podría decir que la Disponibilidad de Presupuesto ha sido calificada con 3 y que la Inversión retribuya con los Beneficios con 5. Para ello es necesario la aplicación de la ecuación establecida mediante el uso del método objetivo con escala de intervalos que indica la ISO 270004, con el fin de determinar el valor real obtenido en peso porcentual. Quedando así:

- Disponibilidad de Presupuesto **3**
- Inversión retribuya con los Beneficios **5**

$$\boldsymbol{Vpo} = \frac{VmaxE}{VoE} x \frac{PgC}{?}$$

Donde:

Vpo: Valor Porcentual Obtenido

E: Escala de Intervalos

VmaxE: Valor Máximo de la Escala de Intervalos

VoE: Valor Obtenido en la Escala

PgC: Porcentaje Genérico del Criterio

$$\boldsymbol{Vpo} = \frac{5}{3} x \frac{10\%}{?} = \frac{10 * 3}{5} = \frac{30}{5} = \mathbf{6}\%$$

Claro está que la asignación porcentual ha sido puesta a consideración tanto a personal interno como externo para mayor confiabilidad del mismo, mediante las diversas entrevistas y encuestas a las diferentes Universidades a nivel nacional (Ver Anexos 7-13).

a. Escenario 1: Herramienta Propietaria/Privativa

TABLA VIII

CRITERIOS CON PESOS GENÉRICOS-ESCENARIO 1

CRITERIOS	**APLICACIÓN ESCALA**					**PESO GENÉRICO**
ASPECTO ECONÓMICO	**1**	**2**	**3**	**4**	**5**	**20%**
• Disponibilidad de Presupuesto o Estudios previos de Factibilidad Econ.						10%

• Inversión retribuya con los beneficios obtenidos o Estudio y Valoraciones Técnicas del Entorno y Equipos						10%
ASPECTO REPUTACIÓN-CONFIABILIDAD	**1**	**2**	**3**	**4**	**5**	**30%**
• Reputación-Confiabilidad de la Herramienta: o WOT (Web Of Trust): Reputación en la Web o Certificaciones Obtenidas						15%
• Reputación-Confiabilidad del Proveedor: o Experiencia con el Producto (Herramienta) o Experiencia en otras Instituciones Educativas						15%
ASPECTO TÉCNICO	**1**	**2**	**3**	**4**	**5**	**50%**
• Evaluación de Herramienta o Pruebas Internas-DEMO o Lenguaje Base o S.O Soportados						10%
• Protección de Equipos de Networking o Total o Parcial						10%
• Cumplimiento de las políticas de acceso y controles a los sistemas o Políticas Institucionales y/o Departamentales						10%
• Espacio Físico y Lógico o Normal o Limitado						5%
• Duración del soporte o Meses/Años						5%

• Capacitación al personal o Meses/Años						5%
• Garantías o Meses/Años						5%

b. Escenario 2: Herramienta Libre/Gratuita

TABLA IX

CRITERIOS CON PESOS GENÉRICOS-ESCENARIO 2

CRITERIOS	**APLICACIÓN ESCALA**					**PESO GENÉRICO**
ASPECTO ECONÓMICO	**1**	**2**	**3**	**4**	**5**	**20%**
• Inversión retribuya con los beneficios obtenidos o Estudio y Valoraciones Técnicas del Entorno y Equipos						10%
ASPECTO REPUTACIÓN-CONFIABILIDAD	**1**	**2**	**3**	**4**	**5**	**30%**
• Reputación-Confiabilidad de la Herramienta: o WOT (Web Of Trust): Reputación en la Web o Certificaciones Obtenidas						20%
• Reputación-Confiabilidad del Proveedor: o Experiencia en otras Instituciones Educativas						10%
ASPECTO TÉCNICO	**1**	**2**	**3**	**4**	**5**	**50%**
• Evaluación de Herramienta o Pruebas Internas-DEMO o Lenguaje Base o S.O Soportados						15%

• Protección de Equipos de Networking o Total o Parcial						10%
• Cumplimiento de las políticas de acceso y controles a los sistemas o Políticas Institucionales y/o Departamentales						10%
• Espacio Físico y Lógico o Normal o Limitado						5%
• Soporte o Duración Soporte Online o Comunidad para Soporte						10%

c. Escenario 3: Proyectos Estudiantiles

TABLA X

CRITERIOS CON PESOS GENÉRICOS-ESCENARIO 3

CRITERIOS	**APLICACIÓN ESCALA**					**PESO GENÉRICO**
ASPECTO ECONÓMICO	**1**	**2**	**3**	**4**	**5**	**20%**
• Disponibilidad de Presupuesto o Estudios previos de Factibilidad						10%
• Inversión retribuya con los beneficios obtenidos o Estudio y Valoraciones Técnicas del Entorno y Equipos						10%
ASPECTO REPUTACIÓN-CONFIABILIDAD	**1**	**2**	**3**	**4**	**5**	**30%**
• Reputación-Confiabilidad de la Herramienta: o WOT (Web Of Trust): Reputación en la Web o Certificaciones Obtenidas						20%
• Reputación-Confiabilidad del Proveedor:						10%

○ Experiencia con el Producto (Herramienta) ○ Experiencia en otras Instituciones Educativas						
ASPECTO TÉCNICO	**1**	**2**	**3**	**4**	**5**	**50%**
• Evaluación de Herramienta ○ Pruebas Internas-DEMO ○ Lenguaje Base ○ S.O Soportados						15%
• Protección de Equipos de Networking ○ Total o Parcial						10%
• Cumplimiento de las políticas de acceso y controles a los sistemas ○ Políticas Institucionales y/o Departamentales						10%
• Espacio Físico y Lógico ○ Normal o Limitado						5%
• Duración de Licencias ○ Meses/Años						10%

3.4. *Proponer niveles de confianza para la aceptación de la herramienta de seguridad informática al momento de realizar su implementación.*

Luego de hacer el pertinente análisis de los tres escenarios planteados, se ha podido determinar y asignar pesos genéricos a cada uno de los criterios a evaluar en una herramienta de seguridad informática, mediante la puesta en consideración de los criterios establecidos en cada escenario al personal de la UTI-UNL, así como a personal externo a la institución, otorgando así indirectamente el nivel de confiabilidad para la implementación de herramientas de seguridad informática, entre ellas las más comunes y analizadas anteriormente. Partiendo de lo previamente indicado se propone niveles para determinar la confiablidad de las herramientas de seguridad informática.

Tomando en cuenta que modelos de confianza en este campo es de existencia nula; por lo tanto, los niveles establecidos a continuación son en base a la bibliografía consultada, entrevistas a personal especializado en redes y seguridad interno y externo, así como el pertinente análisis con el director del trabajo de titulación. Luego de todo el proceso mencionado anteriormente, así como del uso y aplicación de la evaluación de riesgos, y considerando los niveles sugeridos por la norma ISO/IEC 270005 se ha determinado los siguientes niveles de confianza para cada uno de los escenarios, con una escala de intervalos con margen cerrado (Ver Anexos 16-18):

a. Escenario 1: Herramienta Propietaria/Privativa

Siendo este el escenario con muchos más criterios a evaluar por ser una herramienta propietaria o privativa, la misma que es adquirida a alguna empresa dedicada a brindar servicios de esta índole, poniéndonos en la necesidad de analizar mucho más los beneficios ofertados, así como: tiempo de licenciamiento, garantías, capacitación a personal, etc. Se ha designado los siguientes valores porcentuales a cada nivel de confianza, lo que conlleva incluir riesgos a los mismos:

TABLA XI

NIVELES DE CONFIANZA-ESCENARIO 1

NIVEL O GRADO DE CONFIANZA	PORCENTAJE DE ACEPTACIÓN
ALTO	96% - 100%
MEDIO	91% - 95%
BAJO	86% - 90%

b. Escenario 2: Herramienta Libre/Gratuita

Al juzgar el presente escenario estamos frente a la evaluación previa de una herramienta de carácter libre o gratuita, en donde influye mucho la confianza-reputación de la misma, así como se construye un margen mucho más amplio de confiablidad para el modelo propuesto, puesto que al emplear una herramienta que se encuentra en la Web corremos muchos más riesgos que

al utilizar una herramienta privativa y que pude ser evaluada mediante una demostración.

TABLA XII

NIVELES DE CONFIANZA-ESCENARIO 2

NIVEL O GRADO DE CONFIANZA	PORCENTAJE DE ACEPTACIÓN
ALTO	86% - 100%
MEDIO	81% - 85%
BAJO	76% - 80%

c. Escenario 3: Proyectos Estudiantiles

Dentro de la valoración otorgada a este escenario del modelo propuesto se ha planteado intervalos mucho más estrictos, debido a que al implementar herramientas de seguridad informática mediante proyectos estudiantiles se corre mucho más riesgos, ya que se estará implementando una herramienta nueva-desarrollada o adaptada. A continuación se plantean los siguientes niveles:

TABLA XIII

NIVELES DE CONFIANZA-ESCENARIO 3

NIVEL O GRADO DE CONFIANZA	PORCENTAJE DE ACEPTACIÓN
ALTO	96% - 100%
MEDIO	91% - 95%
BAJO	86% - 90%

- **Riesgos para Nivel 1-ALTO (Verde):** En lo que respecta al mencionado nivel se considera factible la implementación en evaluación de una determinada herramienta de seguridad informática, confirmando así la presencia de todas las especificaciones técnicas necesarias. Así como se da por confirmada la obtención de la totalidad de beneficios brindados por la herramienta.

Es así, que este nivel proporciona un alto nivel de confianza tras evaluar y analizar la implementación en cuestión, en cada uno de los aspectos y criterios establecidos con anterioridad. Lo que finalmente garantiza una implementación factible dentro del entorno universitario.

- **Riesgos para Nivel 2-MEDIO (Amarillo):** El presente nivel de confianza considera una factibilidad media de implementación de una herramienta de seguridad informática debido a la falta parcial de las especificaciones técnicas ante una determinada implementación y por ende obtención de puntajes medios en alguno de los criterios de evaluación establecidos en cada escenario. Por consiguiente al realizar una implementación con nivel de confianza 2 conllevaría a realizar una implementación con riesgos de funcionamiento indebido y la presencia de una posible pérdida de información como de recursos invertidos a lo largo de todo el proceso de implementación.

.

- **Riesgos para Nivel 3-BAJO (Rojo):** Sin duda alguna es el nivel más crítico dentro de los niveles de confianza, puesto que no garantiza la factibilidad de una buena implementación para herramientas de seguridad informática, en absoluto; ya sea por falta de especificaciones técnicas o en su caso por la disponibilidad del factor económico. Es así que no es recomendable por ningún motivo realizar una implementación para herramientas de seguridad informática bajo este estado, puesto que se garantiza una pérdida de recursos, así como de parte del activo más importante de toda institución, la información, debido a la baja porcentual notable en la evaluación de la implementación en el escenario respectivo.

FASE 4: Experimentar con el modelo propuesto sobre alguna de las herramientas de seguridad informática previamente estudiadas para evaluar su grado de confianza.

4.1. *Listar un número considerable de herramientas de seguridad informática más implementadas en entornos universitarios en base al estudio previamente realizado.*

Tomando como punto de partida la información proporcionada por la encuesta de seguridad aplicada a las universidades que conforman CEDIA (Ver Anexo 2); y de la re afirmación de la misma en el DISI, desarrollado en la UTPL, se ha podido identificar que las herramientas más implementadas en entornos universitarios, actualmente, son las siguientes:

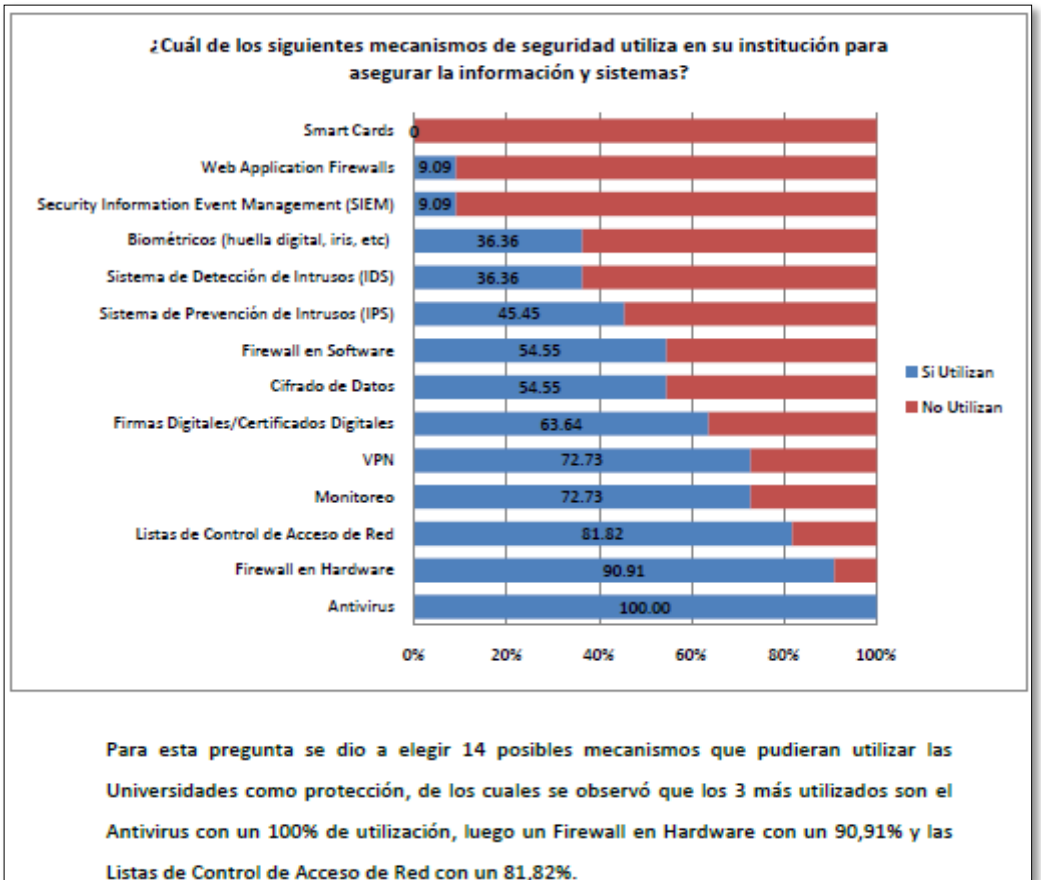


Figura 4: Herramientas más Implementadas en Universidades del Ecuador-Miembros de CEDIA

4.2. Determinar un escenario de experimentación para evaluar el modelo propuesto.

Al observar la poca o casi nula explotación del área de Seguridad de la Información en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, se ha visto factible solicitar, mediante una reunión, el permiso correspondiente para la puesta en experimentación del modelo (Ver Anexo 10).

Durante la reunión establecida con el Director de la UTI: Ing. Milton Palacios, se ha podido conocer del plan que tiene como objetivo adquirir e implementar un programa antivirus con licencias corporativas y beneficios mucho más amplios, con el fin de salvaguardar la información que transita por la redes de la UNL. De igual forma, brindarles a los usuarios de equipos finales un grado más de confiabilidad a la hora de utilizar estos equipos y de navegar por la Web. Al finalizar la reunión, se ha concedido el permiso respectivo para poner en experimentación el modelo creado, designando a la Lcda. Mabel Rodríguez (Encargada de la Sección de Mantenimiento Electrónico de la UTI-UNL), para que preste la ayuda necesaria durante este proceso.

Por su parte, la Lcda. Mabel Rodríguez ha visto como una muy buena iniciativa el uso del modelo en planteamiento, recalcando que a través del mismo se logrará obtener una pauta y valoración de las herramientas de seguridad informática, previa a su implementación (Ver Anexo 22).

Para finalizar, se ha brindado los contactos de la empresa, CoreSolutions, con la que se ha llegado a un acuerdo para la implementación del programa antivirus, Kaspersky, con el fin de obtener mucha más información de la propuesta técnica y económica por parte de dicha empresa (Ver Anexos 19-21). Puesto que en meses anteriores ya se había establecido una propuesta similar, pero con intención de analizar y evaluar una propuesta mucho más actualizada, se ha solicitado la misma, obteniendo un resultado positivo a dicho pedido (Ver Anexo 21).

4.3. Evaluar la herramienta seleccionada mediante el modelo de confianza propuesto.

Tras la previa aceptación de la empresa CoreSolutios S.A. por parte de la UTI para la oferta del programa antivirus Kaspersky, se ha procedido a la revisión de la propuesta actual (Ver Anexo 21), con el fin de utilizar la información contenida en la misma para iniciar el proceso de evaluación de la herramienta mediante el uso del Escenario 1: Herramienta Propietaria/Privativa, del modelo propuesto. Partiendo de lo antes indicado, se ha procedido a realizar la evaluación de la herramienta en cuestión, tomando en cuenta cada uno de los criterios establecidos, así como la previa evaluación mediante la escala establecida y la aplicación de la fórmula establecida en la fase anterior dentro del apartado de designación de pesos genéricos para el modelo de confianza propuesto.

$$\boldsymbol{Vpo} = \frac{VmaxE}{VoE} x \frac{PgC}{?}$$

TABLA XIV

EVALUACIÓN DETALLADA DE ANTIVIRUS CON ESCENARIO 1

CRITERIOS	PESO GENÉRICO	DESCRIPCIÓN DE EVALUACIÓN	ESCALA	PESO ASIGNADO
ASPECTO ECONÓMICO	**20%**		**1-5**	**17%**
Disponibilidad de Presupuesto	10%	En vista de que un programa antivirus con licenciamiento, protección total, es de primordial importancia dentro de toda institución y en especial de carácter educativo; se ve en la necesidad de realizar la adquisición de dicha herramienta que ayudará	5	10%

		a salvaguardar proactivamente la información de la institución. Sin antes indicar que dicho proyecto ya ha sido analizado con anterioridad en diversas ocasiones, pero por falta de iniciativa y decisión se ha dejado de lado tan importante y necesario proyecto. Por otra parte, de acuerdo a la propuesta emitida por la empresa en cuestión se ha indicado que el pago se lo realizará 100% contra entrega de las licencias e instalación. Cabe recalcar que la propuesta en evaluación ha sido modificada, en relación a la primera propuesta emitida en julio del 2013 (Ver Anexo 20), ya que en la actual propuesta (Ver Anexo 21) se ha conseguido que CoreSolutions otorgue el 54% de descuento a la Universidad Nacional de Loja por el hecho de ser miembro de CEDIA,		

		institución que maneja un convenio para implementar mecanismos de seguridad en los centros de educación superior que forman parte de la misma. Luego de haber explorado los beneficios en lo que respecta al aspecto económico y en la necesidad urgente de contar con un programa antivirus con licencias corporativas se ha considerado positiva la disponibilidad del presupuesto para la implementación.		
Inversión retribuya con los beneficios obtenidos	10%	Con la respectiva aceptación previa de la propuesta emitida por parte de CoreSolutions S.A. la misma que consta de tres opciones para uno, dos y tres años de 1500 nuevas licencias Anti-Malware, con suscripción para actualización de firmas y soporte técnico de fábrica, de Kaspersky Endpoint Security for Business o KESB. Todas las opciones ofertadas	3,5	7%

		son del nivel **Total** corporativo, ofreciendo todos los niveles progresivos de protección que brinda este programa antivirus, como: Anti Malware + Firewall, Control de Aplicaciones, Control de Dispositivos, Control Web, Seguridad de Servidor de Archivos, Seguridad de Endpoint Móvil, Manejo del Dispositivo Móvil (MDM), Protección de Datos (Encriptación), Imagen/ Aprovisionamiento, Manejo de Parches, Escaneo de Vulnerabilidad, Manejo de Licencia, Admisión de Red (NAC), Instalación de Software, Colaboración, Correo y Web(Ver Anexo 21). Además, se incluyen los servicios de valor agregados opcionales para instalar la nueva versión de consola de administración en caso de ser requerido, para configurar y capacitar a		

		los administradores de seguridad en TI de tal manera que desarrollen destrezas necesarias para continuar con la gestión de seguridad una vez implementada la solución. Luego de haber analizado de forma generalizada cada uno de los puntos ofertados, se ha concluido que la oferta por parte del proveedor es aceptable debido a que garantiza en gran magnitud la protección de la información que circula por la red universitaria (Ver Anexo 15). Así mismo, cabe acotar que se ha tomado en cuenta las certificaciones obtenidas por parte de KasperskyLab, siendo de gran aporte para la aceptación de la propuesta (Ver Anexo 21). Luego de haber analizado los dos criterios anteriormente detallados se puede corroborar que la		

		inversión a realizarse con la adquisición del programa antivirus Kaspersky retribuye en un 50% con los beneficios que la institución obtendrá. Puesto que actualmente la institución cuenta con aproximadamente la mitad de los equipos con muy bajas características técnicas para instalar un sistema antivirus tan robusto como lo es Kaspersky Endpoint Security versión 10, por lo tanto se ha considerado la opción de implementar en los equipos con bajas características la versión Kaspersky Antivirus 6, la misma que tiene un nivel mucho más bajo de protección en relación a la versión 10 de Kaspersky, pero que mantiene su nivel básico de protección y manipulación desde la consola de administración principal. El porcentaje asignado involucra la variación en		

		cuanto a los beneficios obtenidos con la inversión a realizarse, en definitiva es recomendable que antes de implementar una herramienta como aquella se realice una valoración técnica interna, con el objetivo de ver cómo mejorar y aprovechar al máximo la implementación de nuevas herramientas en la institución. O a su vez se puede optar por realizar un programa de repotenciación de este tipo de equipos dentro de la institución, lo que también permitirá mejorar el funcionamiento de los sistemas en general.		
ASPECTO REPUTACIÓN-CONFIABILIDAD	**30%**		**1-5**	**28%**
Reputación-Confiabilidad de la Herramienta	15%	Dentro de este criterio, como ya se detalló en fases anteriores, se evalúan dos puntos importantes: el primero de ellos es en base a las certificaciones obtenidas por la herramienta y el	4,3	13%

		segundo mediante el uso de WOT. El primer punto dio como resultado el conocimiento de la más de una certificaciones y reconocimientos obtenidos por Kaspersky, entre ellos: Magic Quadrant ubica a Kaspersky Lab como líder de protección Endponit, galardonado por Gartner, Vb 100 Virus, AV Test. Asimismo más de 80 proveedores de TI, seguridad de redes y comunicaciones han elegido incorporar la tecnología anti-malware de Kaspersky Lab dentro de sus propias soluciones, incluyendo Mircosoft, IBM, CheckPoint y Juniper. En cuanto a la valoración que brinda WOT, por la confianza de la herramienta en la Web, se puede decir que la distribuidora de Kaspersky, GSM, de la ciudad de Guayaquil mantiene un alto grado		

		de confiabilidad en la Web, pero no es el caso de la empresa comercializadora, CoreSolutions S.A. Por lo consiguiente, se ha creído conveniente sugerir a la empresa comercializadora la indagación de este tipo de herramientas Web que les permite obtener un alto nivel de confianza y reputación en la Web (Ver Anexo 25).		
• Reputación-Confiabilidad del Proveedor	15%	En el presente criterio se toma en cuenta para su valorización la Experiencia que tiene el Proveedor con la herramienta en general y en entornos de tipo educativo. En base a tales puntos se ha podido analizar y determinar lo siguiente: Trás haber establecido contacto con el Asesor de Ventas, Ing. Olmedo Abril (Cuenca) (Ver Anexo 19) y el Consultor Ricardo Villa (Guayaquil), se ha solicitado información acerca de las	5	15%

		instituciones a las que le brindan sus servicios, mencionaron las siguientes: UTPL, Universidad Agraria, Universidad de Portoviejo, y en lo que respecta a instituciones de otra índole a: Banco Pichincha, Ministerio del Interior, Zonales, entre otras. Con la información obtenida se corroboró con la entrevista brindada por parte de la Líder de Seguridad de la UTPL (Ver Anexo 7 y 8), ya que es el escenario más cercano y palpable de la calidad, reputación y confiabilidad de servicios que brinda CoreSolutions S.A. y por ende Kaspersky.		
ASPECTO TÉCNICO	**50%**		**1-5**	**48%**
Evaluación Previa de la Herramienta	10%	El criterio con mayor valor dentro del aspecto técnico y el mismo que se usa como base para la evaluación de los posteriores. Dentro del mismo se ha realizado el contacto necesario para solicitar una instalación	4,5	9%

		de un DEMO (Ver Anexos 22 Y 28), de 30 días, de Kaspersky Antivirus que permita determinar las ventajas y desventajas de instalar dicho antivirus en la red universitaria. En lo a que se refiere al S.O que soporta Kaspersky Lab no existe mayor problema, ya que cuenta con una gama alta de flexibilidad y portabilidad de instalación, ya sea en: Estaciones de Trabajo, Servidores, Consolas de Administración en los diferentes y más comerciales S.O (Windows, Linux y MAC). Por su parte, y de igual manera, lo tiene con Dispositivos móviles que cuenten con sistemas: Android, Symbian, Windows Mobile y BlackBerry. En conclusión, se puede afirmar el normal funcionamiento de la herramienta en equipos		

		finales los equipos finales, así como en la consola de administración, pero con algo de deficiencia debido al estado actual de los equipos finales administrativos.		
Protección de Equipos de Networking	10%	En cuanto a la protección de equipos networking, es importante recordar que como toda institución mantiene su función principal entorno a la protección de todos los dispositivos, que son parte directa o indirectamente de la red de la Universidad Nacional de Loja, puesto que dé el correcto funcionamiento de estos equipos depende mantener a buen recaudo toda la información que transita por la red universitaria. Los equipos que se protegerán con la implementación de la herramienta van desde los servidores principales, consolas de administración, routers	5	10%

		hasta dispositivos móviles; siendo estos últimos dispositivos los que hacen uso de los nuevos beneficios que brinda este programa antivirus, debido a que brinda la posibilidad de administrar dispositivos móviles desde el momento que los mismos se conectan a la red reduciendo el riesgo de pérdida de información mediante la protección contra virus, spyware, troyanos, gusanos, etc. Todo aquello con el único objetivo de ofrecer a la red múltiples capas de protección a los diferentes sistemas que están alojados en la red interna de la institución. Es importante mencionar que en caso de necesitar añadir más capacidades de seguridad o administración en el entorno de TI, existen soluciones que ofrecen una gama de tecnologías adicionales que pueden complementar la solución		

		de Kaspersky. Puede añadirse protección de almacenamiento, virtualización, correo, puertas de enlace de internet o colaboración, o en su caso funcionalidad de administración de sistemas de gran alcance. Partiendo de lo antes indicado se procede a hacer la valoración del parámetro, verificando que la herramienta a implementar cubre en su totalidad toda la infraestructura de equipos networking con los que cuenta la institución (Ver Anexo 4 y 6).		
Cumplimiento de las políticas de acceso y controles a los sistemas	10%	En lo relacionado a las políticas de seguridad a cubrirse tras la implementación de la herramienta en evaluación, luego de que se ha presenciado la instalación del DEMO (Ver Anexos 12 Y 28) y de la revisión de la propuesta emitida por CoreSolutions S.A. (Ver Anexo 16) se ha	5	10%

		constatado que mediante tecnologías de control de aplicaciones, control de dispositivos y control web de Kaspersky se permitirá brindar un nivel mucho más profundo de defensa de los datos y sistemas, de tal manera que el equipo de Tecnologías de Información pueda controlar fácilmente la manera en que se ejecutan las aplicaciones y administrar cómo los usuarios hacen uso de los diferentes servicios dentro de la red. En base al análisis realizado se ha establecido el porcentaje completo dentro de este criterio, debido a que las políticas implementadas actualmente en la UTI no cuentan con un alto nivel de robustez (Ver Anexo 29), pero se encuentra trabajando en dicho ámbito con la misión de mejorarlas.		
Espacio Físico y Lógico	5%	Dentro de las especificaciones principales por parte de CoreSolutions previa la	5	5%

		implementación de la herramienta, es necesario disponer de un servidor para la instalación de la consola de administración centralizada de Kaspersky la que permitirá actualizaciones automáticas de firmas de malware y de software permitiendo una mejor administración y simplificación en la administración móvil. Tras haber establecido un diálogo con personal de la UTI, entre ellos el Director de la Unidad, (Ver Anexo 10) se ha podido corroborar de la existencia y disponibilidad tanto física como lógica de los equipos necesarios para la implementación de Kaspersky con licencias corporativas. La implementación se la pretende realizar en el servidor principal Blade, del mismo que parten las diversas segmentaciones de la red, sobre el SO		

		Linux puesto que es con el que actualmente trabajan en la Unidad de Telecomunicaciones e Información de la UNL proporcionando así mayor facilidad a la hora de administrar el programa antivirus sobre el mismo Sistema Operativo. Tras la evaluación de este criterio se ha contrastado las especificaciones del proveedor así como la disponibilidad de las mismas por parte de la universidad, dando una respuesta positiva a dichos requisitos.		
Duración del soporte	5%	La propuesta en evaluación (Ver Anexo 21) presenta la siguiente descripción en lo que respecta a la duración del soporte técnico para la herramienta a implementar: Las tres opciones propuestas ofrecen Soporte Técnico de fábrica vía Web en donde se ofrece una serie de herramientas y manuales en lo respecta al soporte técnico de la	5	5%

		herramienta de seguridad informática en cuestión. Dentro de lo que ofrece el Soporte Técnico de Kaspersky Web, incluye, soporte para: Estaciones de Trabajo y Dispositivos Móviles, Servidores de Correo y Colaboración, Servidores de Archivo, Consolas de Administración, Entornos Virtuales, Internet Gateways. Al contar con una alta gama de soporte técnico Web, es mucho más factible al momento de presentarse alguna circunstancia irregular fuera del correcto funcionamiento del programa antivirus a implementar. Cabe recalcar que existe un número de horas de soporte técnico post-instalación, el mismo que se detalla y evalúa en el siguiente criterio en evaluación.		
Capacitación al personal	5%	Dentro del ámbito de capacitación, la propuesta emitida (Ver Anexo 21) por	4	4%

		CoreSolutions S.A., indica: 15 horas de soporte técnico post-instalación (capacitación), anual, para realizar tareas no relacionadas con trámites de garantías como: modificación de la configuración, resolución de consultas, talleres de trabajo. Cabe recalcar que al aceptar la opción número dos, se cuenta con 30 horas de capacitación al personal, y finalmente en caso de contratar la opción tres se dispone de 45 horas de capacitación al personal siempre y cuando no salgan de las restricciones indicadas en líneas anteriores. Por lo expuesto y con personal del Departamento Técnico Electrónico de la UTI se ha considerado que la propuesta debería incrementar el número de horas en la capacitación del personal, puesto que en capacitación al		

		personal es un gasto muy relevante dentro de toda organización. Por parte del Consultor de GSM, se ha sugerido la negociación de dicho ámbito con la empresa comercializadora, en este caso CoreSolutions S.A. La asignación del porcentaje se ha realizado de acuerdo a las situaciones antes ya indicadas.		
Garantías	5%	Cada una de las opciones incluye Garantía Técnica para uno, dos y tres años, según sea el caso de elección. Al analizar las necesidades por parte de la Universidad y la oferta por parte de Coresolutions S.A. se ha podido determinar que es lógica y por ende aceptable el tiempo de garantía de programa antivirus en análisis. Por lo tanto se ha procedido a asignar el respectivo porcentaje a este criterio.	5	5%
TOTAL				**93%**

4.4. Determinar el nivel de confianza de la herramienta de seguridad informática para su posterior implementación en el entorno universitario en experimentación.

Luego del análisis respectivo de cada uno de los criterios que conforman el modelo y de la asignación respectiva del valor porcentual debido a la participación en la instalación del DEMO (Ver Anexo 28), se ha procedido a determinar el nivel o grado de confianza que tiene la implementación de la herramienta de seguridad informática, en este caso el programa antivirus Kaspersky.

TABLA XV

NIVEL DE CONFIANZA DE ANTIVIRUS-ESCENARIO 1

NIVEL O GRADO DE CONFIANZA	PORCENTAJE DE ACEPTACIÓN
ALTO	96% - 100%
MEDIO	91% - 95%
BAJO	85% - 90%

Al haber obtenido un **93%** tras la evaluación de la implementación y por ende de la herramienta en cuestión se cita lo que involucra haber obtenido tal Nivel de Confianza:

Riesgos Nivel 2-MEDIO (Amarillo): El presente nivel de confianza da como aceptación media a la factibilidad de implementación de una herramienta de seguridad informática debido a la baja en el valor porcentual de algún/os de los criterios del Escenario 1: Herramienta Privativa o Propietaria, principalmente debido a que en la institución se cuenta con casi el 50% de equipos finales con características básicas en donde el programa antivirus no funcionaría a plenitud ni se podría aprovechar al máximo sus potencialidades. Por tal motivo, esto involucraría una pérdida de tiempo, así como una implementación un poco nula, al no estar aprovechando todos los beneficios y en todos los equipos finales lo que no retribuiría la inversión realizada.

4.5. Proponer a la comunidad científica la evaluación del modelo propuesto.

En lo que respecta a la propuesta del modelo a la comunidad científica se ha creído conveniente hacerla en algún entorno de tipo científico, debido a que es un aporte a original a la comunidad, por tal motivo el modelo creado se ha propuesto ante el II Concurso de Reconocimiento a la Investigación Universitaria – Galardones 2014 organizado por la Senescyt, cuyo objetivo principal es promover la investigación de estudiantes de los últimos años de carrera universitaria y quienes se encuentran en calidad de egresados para que presenten sus proyectos en las áreas de Educación, Arte, Ciencias Naturales, Matemáticas y Estadística; Tecnologías de la Comunicación e Innovación; Ingeniería, Industria y Construcción; Agricultura, Silvicultura y Pesca; Salud y Bienestar. Partiendo de aquello, el modelo fue presentado en el ámbito de las Tecnologías de la Comunicación e Innovación aplicando al componente de innovación y/o diálogo de saberes. Cabe recalcar que la propuesta fue presentada de forma física y digital el día martes 27 de mayo del año en curso en las oficinas de la Secretaría ubicadas en la ciudad de Loja (Ver Anexo 23). Para mayor información de la finalidad del Concurso, visitar: http://www.educacionsuperior.gob.ec/hasta-el-30-de-mayo-se-podra-participar-en-el-concurso-de-reconocimiento-a-la-investigacion-universitaria-2014/

Luego de transcurrir la etapa de presentación, verificación de requisitos y condiciones de las 273 propuestas de proyectos presentados al concurso, se logra avanzar a la siguiente etapa del mismo (Ver anexo 24); recibiendo la invitación para participar como Proyecto Semifinalista en la Feria Zonal Cuenca, el 24 de Julio del presente año. A continuación se cita el link de los proyectos pre-aprobados, siendo el nuestro uno de ellos: http://www.educacionsuperior.gob.ec/ii-concurso-de-reconocimiento-a-la-investigacion-universitaria-estudiantil-galardones-nacionales-2014/

5. ACTIVIDAD COMPLEMENTARIA - LIMESURVEY[32]

Con el objetivo de darle al usuario final una visión mucho más clara del resultado del modelo propuesto, así como de la forma de evaluación y asignación de niveles de confianza; se ha creído factible emplear LimeSurvey para mediante encuestas realizar pruebas de la evaluación de herramientas de seguridad informática más comunes implementadas en entornos universitarios.

Es necesario indicar que se tiene alojado LimeSurvey en un servidor privado de la empresa de Software y Diseño DRACO[33] en la siguiente dirección Web: http://dracosoft.org/limesurvey/, empresa que ha contratado el Servicio de Alojamiento Web en GoDaddy[34].

5.1. Implementación del modelo propuesto, mediante encuesta con LimeSurvey.

Tras la respectiva instalación de LimeSurvey en el servidor, se ha procedido a crear un cuestionario de prueba denominada PruebaM1 (Ver Figura 5), en donde se incluye una descripción de la misma.

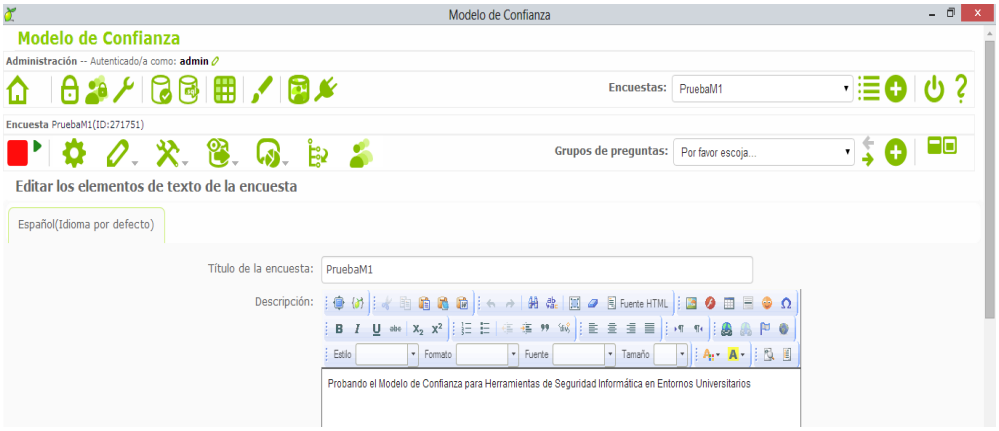


Figura 5: Creación del Cuestionario de Prueba del Modelo

[32] Página Oficial: https://www.limesurvey.org/es/
[33] Página Oficial: http://dracosoft.org/
[34] Página Oficial:

Es importante mencionar que para la creación de esta interfaz del modelo propuesto se ha tomado en cuenta tres de las herramientas de seguridad más comunes de implementación en entornos universitarios.

A continuación se presenta la creación de los diferentes grupos de preguntas, así como las preguntas contenidas en los mismos. Grupos con los que se ha trabajado durante el desarrollo de la prueba del modelo. Dentro de los Grupos de Preguntas creados, tenemos:

1. Herramientas de SI comunes

Dentro de la creación del primer Grupo de Preguntas se ha creado una pregunta (hc1: Seleccione la Herramienta a Evaluar) que permite optar por una de las 3 herramientas de seguridad informática que mayormente se implementa en entornos universitarios, entre ellas: Malware (Antivirus), IDS, Firewall.

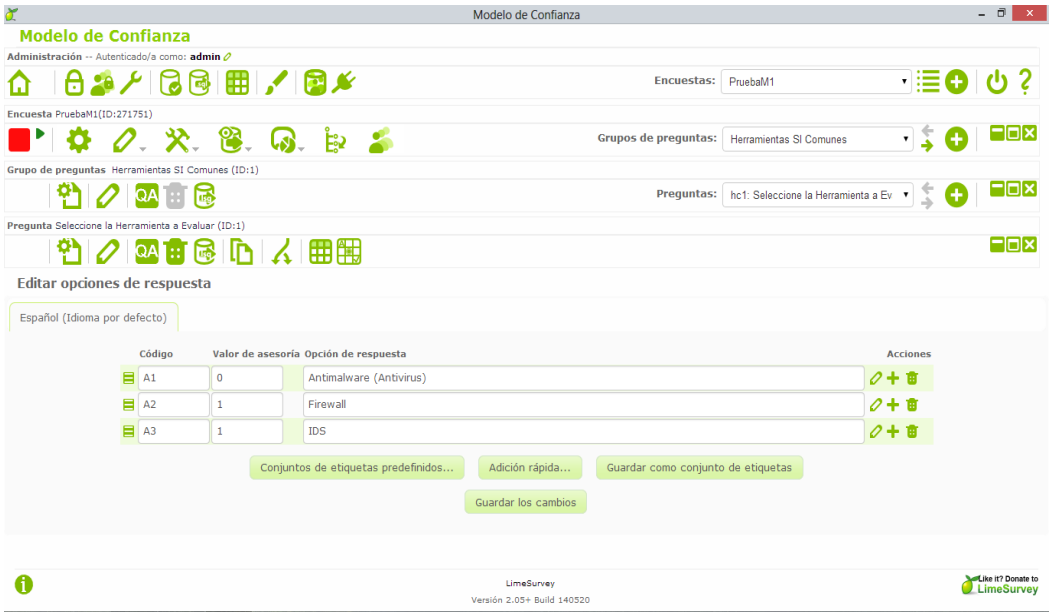


Figura 6: Creación Grupo de Preguntas 1-Herramientas SI Comunes

2. Tipo de Herramienta

En lo que respecta a la creación del segundo Grupo de Preguntas se ha creado una pregunta (hc2: Indique el tipo de herramienta) que permite escoger y por determinar a qué tipo escenario pertenece la herramienta de seguridad informática en evaluación (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.1 Y 3.3).

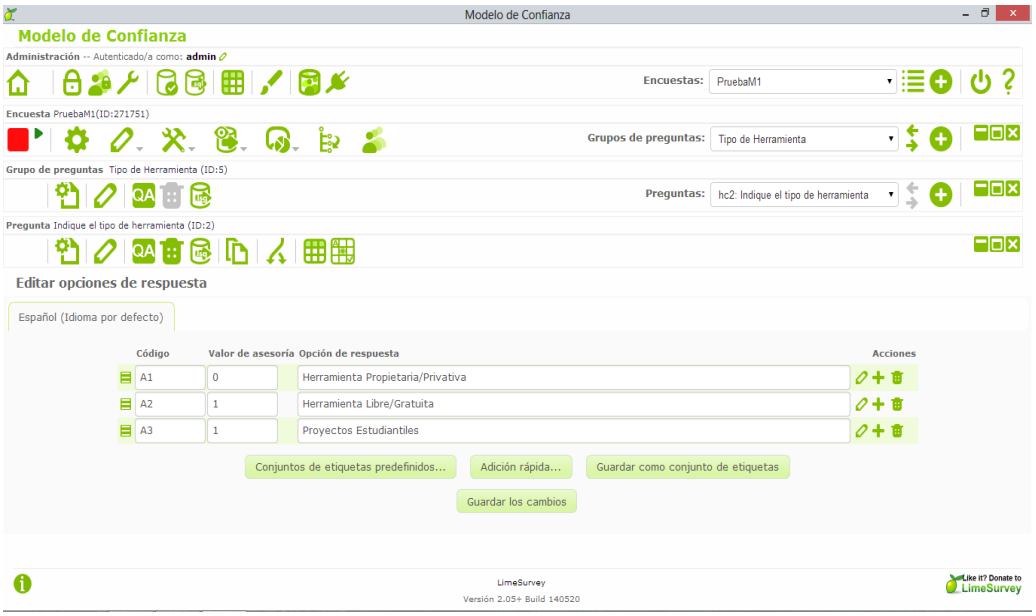


Figura 7: Creación Grupo de Preguntas 2- Tipo de Herramientas.

3. Herramienta Propietaria/Privativa

En lo se refiere a la creación del tercer Grupo de Preguntas se ha creado una pregunta (e1: Evalúe los criterios de los Aspectos: ECONÓMICO 25% REPUTACIÓN - CONFIABILIDAD 15% TÉCNICO 60%) que permite la evaluación de la herramienta y los criterios contenidos en el Escenario 1 del modelo propuesto (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.1 Y 3.3).

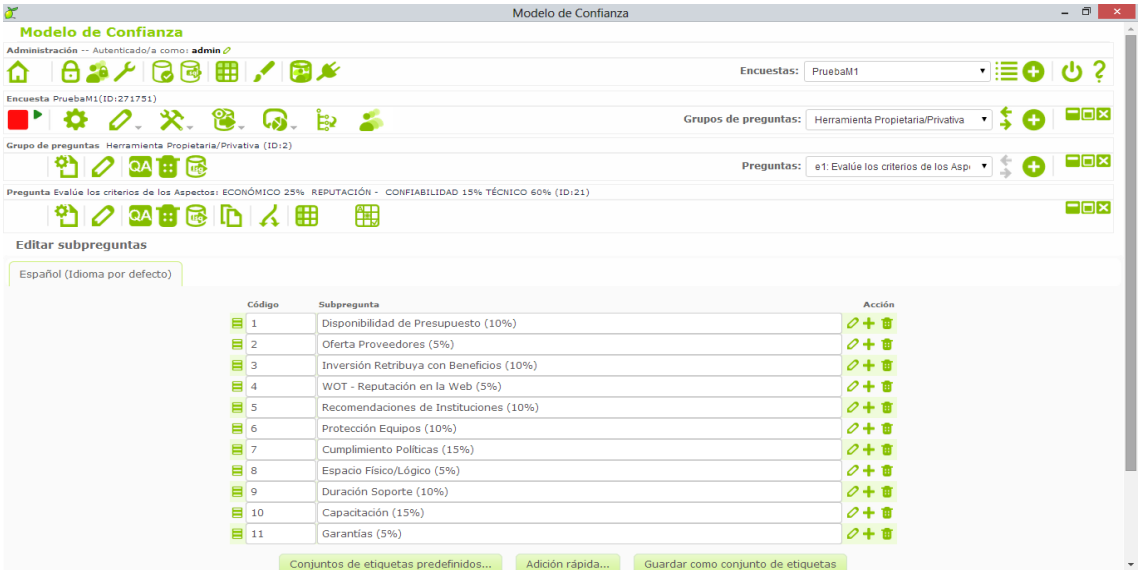


Figura 8: Creación Grupo de Preguntas 3- Herramienta Propietaria/Privativa.

4. Herramienta Libre/Gratuita

En la creación del cuarto Grupo de Preguntas se ha planteado una pregunta (e2: Evalúe los criterios de los Aspectos: ECONÓMICO 10% REPUTACIÓN - CONFIABILIDAD 30% TÉCNICO 60%) que permite la evaluación de la herramienta y los criterios contenidos en el Escenario 2 del modelo propuesto VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.1 Y 3.3).

Figura 9: Creación Grupo de Preguntas 4-Herramienta Libre/Gratuita.

5. Herramienta por Proyecto Estudiantil

El quinto Grupo de Preguntas consta de una pregunta (e3: Evalúe los criterios de los Aspectos: ECONÓMICO 15% REPUTACIÓN - CONFIABILIDAD 25% TÉCNICO 60%) que permite la evaluación de la herramienta y los criterios contenidos en el Escenario 3 del modelo propuesto (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.1 Y 3.3).

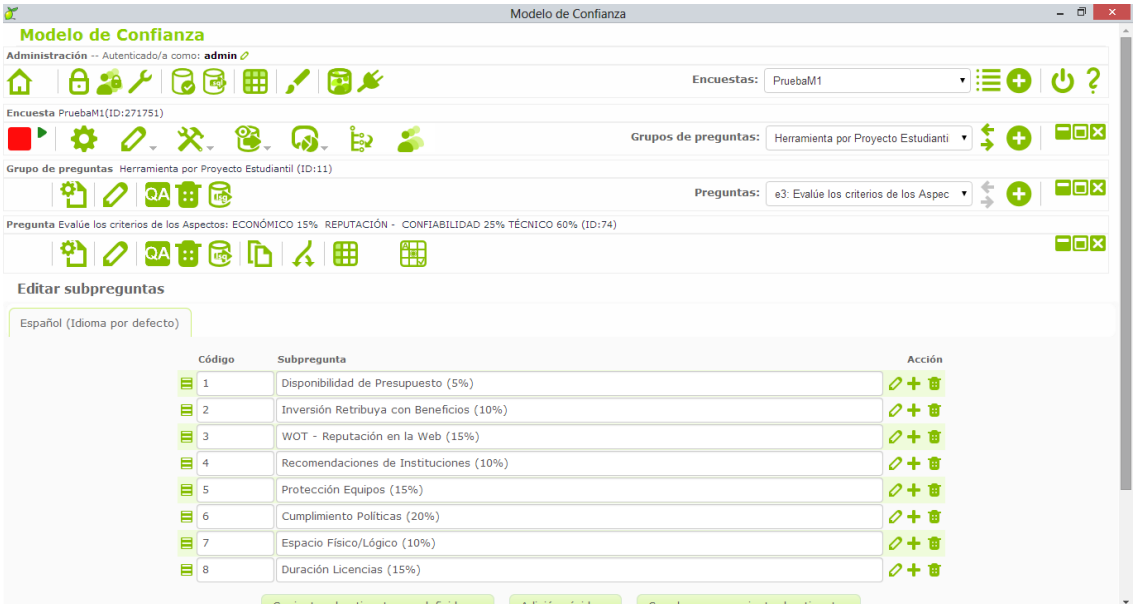


Figura 10: Creación Grupo de Preguntas 5-Herramienta por Proyecto Estudiantil

6. Resultado Evaluación

En la creación del Grupo de Preguntas 6 se ha planteado una pregunta (hc6: Verifique la Suma Total de los Aspectos Evaluados) que permite ingresar la suma total de los aspectos evaluados en el grupo de preguntas anterior (VER SECCIÓN RESULTADOS, SUBSECCIÓN 5 ACTIVIDAD COMPLEMENTARIA, APARTADO 5.1 GRUPO DE PREGUNTAS 3, 4 Y 5), dependiendo del escenario elegido.

Figura 11: Creación Grupo de Preguntas 6-Resultado Evaluación

7. Nivel de Confianza1

La creación del Grupo de Preguntas 7, es para determinar el nivel de confianza de la herramienta (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.4) mediante tres sub preguntas (nc1: El Nivel de Confianza de su Herramienta es ALTO, nc2: El Nivel de Confianza de su Herramienta es MEDIO, nc3: El Nivel de Confianza de su Herramienta es BAJO) contenidas en el grupo, siempre y cuando se haya elegido el Escenario 1.

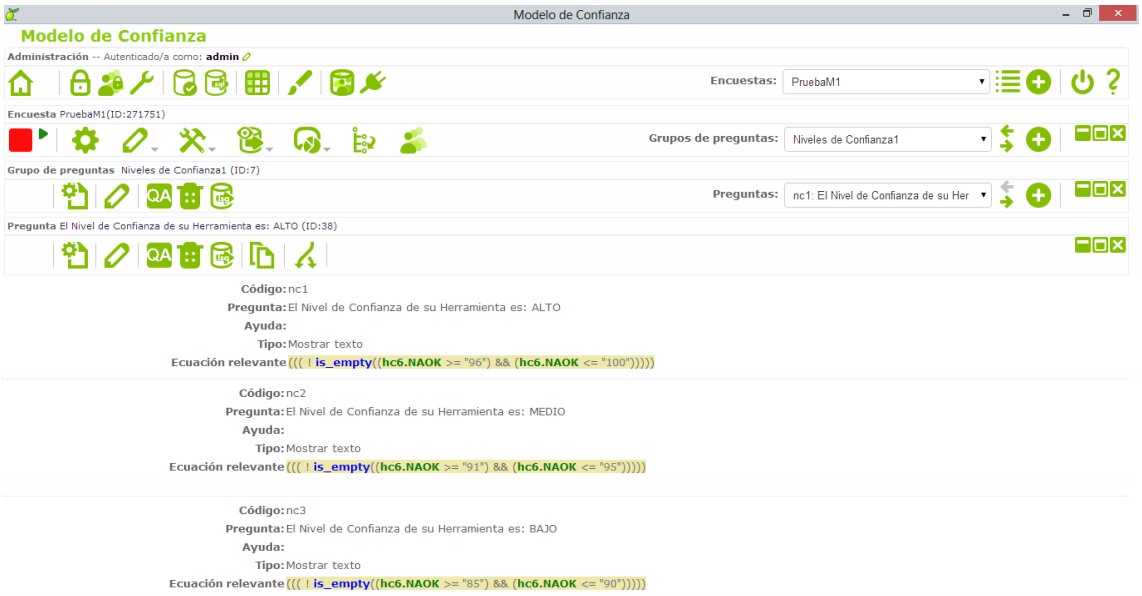


Figura 12: Creación Grupo de Preguntas 7-Niveles de Confianza-Escenario1.

8. Nivel de Confianza2

En la creación del Grupo de Preguntas 8, tiene como fin determinar el nivel de confianza de la herramienta (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.4) mediante tres sub preguntas (nc1: El Nivel de Confianza de su Herramienta es ALTO, nc2: El Nivel de Confianza de su Herramienta es MEDIO, nc3: El Nivel de Confianza de su Herramienta es BAJO) contenidas en el grupo, siempre y cuando se haya elegido el Escenario 2.

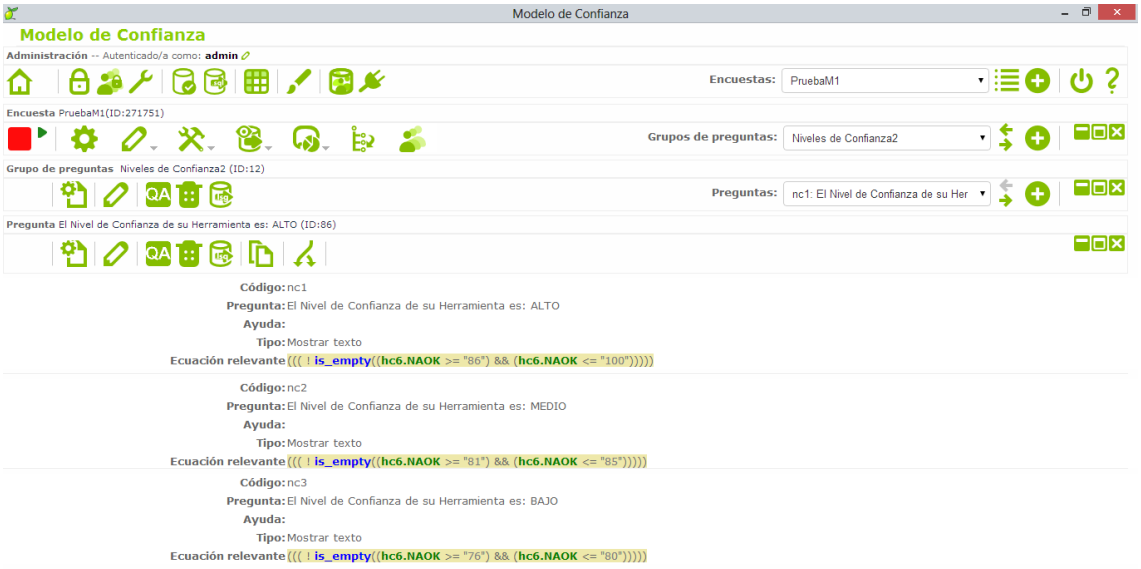


Figura 13: Creación Grupo de Preguntas 8-Niveles de Confianza-Escenario2.

9. Nivel de Confianza3

Dentro de la creación del Grupo de Preguntas 8, se tiene como objetivo determinar el nivel de confianza de la herramienta (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.4) mediante tres sub preguntas (nc1: El Nivel de Confianza de su Herramienta es ALTO, nc2: El Nivel de Confianza de su Herramienta es MEDIO, nc3: El Nivel de Confianza de su Herramienta es BAJO) contenidas en el grupo, siempre y cuando se haya elegido el Escenario 3.

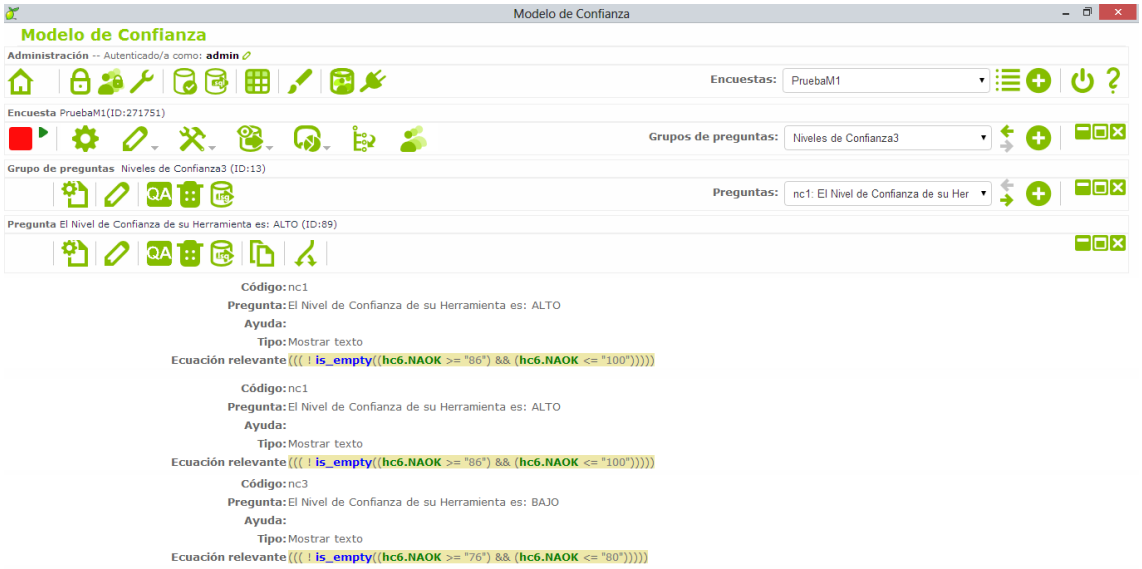


Figura 14: Creación Grupo de Preguntas 9-Niveles de Confianza-Escenario3.

5.2. Evaluación del Antivirus Kaspersky con la implementación del modelo propuesto en LimeSurvey.

El proceso de evaluación de la herramienta Antivirus Kaspersky va de la mano con la evaluación manual y detallada, realizada con anterioridad (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 4, APARTADO 4.3 y 4.4). Es importante reconsiderar que la presente evaluación con el modelo propuesto, implementado en LimeSurvey, tiene como objetivo darle al usuario final la visión de adaptabilidad y flexibilidad del modelo, más no es una plantilla final de la automatización del mismo.

Seguidamente se presenta la prueba del modelo, iniciando con la página inicial de la encuesta, en donde se da una breve descripción del proceso que se llevará a cabo. Cabe acotar que LimeSurvey es una herramienta orientada específicamente a encuestas a usuarios, por lo tanto necesita ser activada, en este caso no ha sido necesario realizar el proceso de activación debido a que no emplearemos los resultados de la evaluación de muchas herramientas, sino de una de ellas en específico.

Figura 15: Evaluación-Interfaz Principal del Modelo.

Tras el inicio de la encuesta, a través del botón “Siguiente” se da paso al primer grupo de pregunta donde se permite escoger entre tres de las herramientas de seguridad informática más comunes (Antivirus, IDS, Firewall) para su respectiva evaluación. En este caso se evaluará una herramienta Antimalware (Antivirus).

Figura 16: Evaluación Grupo de Preguntas 1-Herramientas SI Comunes.

Luego de haber seleccionado el tipo de herramienta se prosigue a indicar sobre qué escenario se va a evaluar, es decir: Escenario 1,2 o 3 (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.1 Y 3.3) en donde cada escenario tiene sus criterios y pesos genéricos respectivos. En la mencionada evaluación se ha seleccionado el Escenario 1: Herramienta Propietaria/Privativa, puesto que la implementación del Antivirus será mediante la adquisición de licencias corporativas a un proveedor en particular.

Figura 17: Evaluación Grupo de Preguntas 2-Tipo de Herramienta.

Después de haber determinado el escenario sobre el que va a ser evaluar la herramienta indicada en pasos anteriores, se cargan los criterios de evaluación para el escenario seleccionado, en este caso los criterios del Escenario 1: Herramienta Propietaria/Privativa (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.1 Y 3.3). Cada criterio tiene su peso genérico porcentual sugerido para no sobrepasar los límites del modelo propuesto, luego de haber colocado los pesos a cada uno de los criterios se genera la suma total de la evaluación de la herramienta en su respectivo escenario.

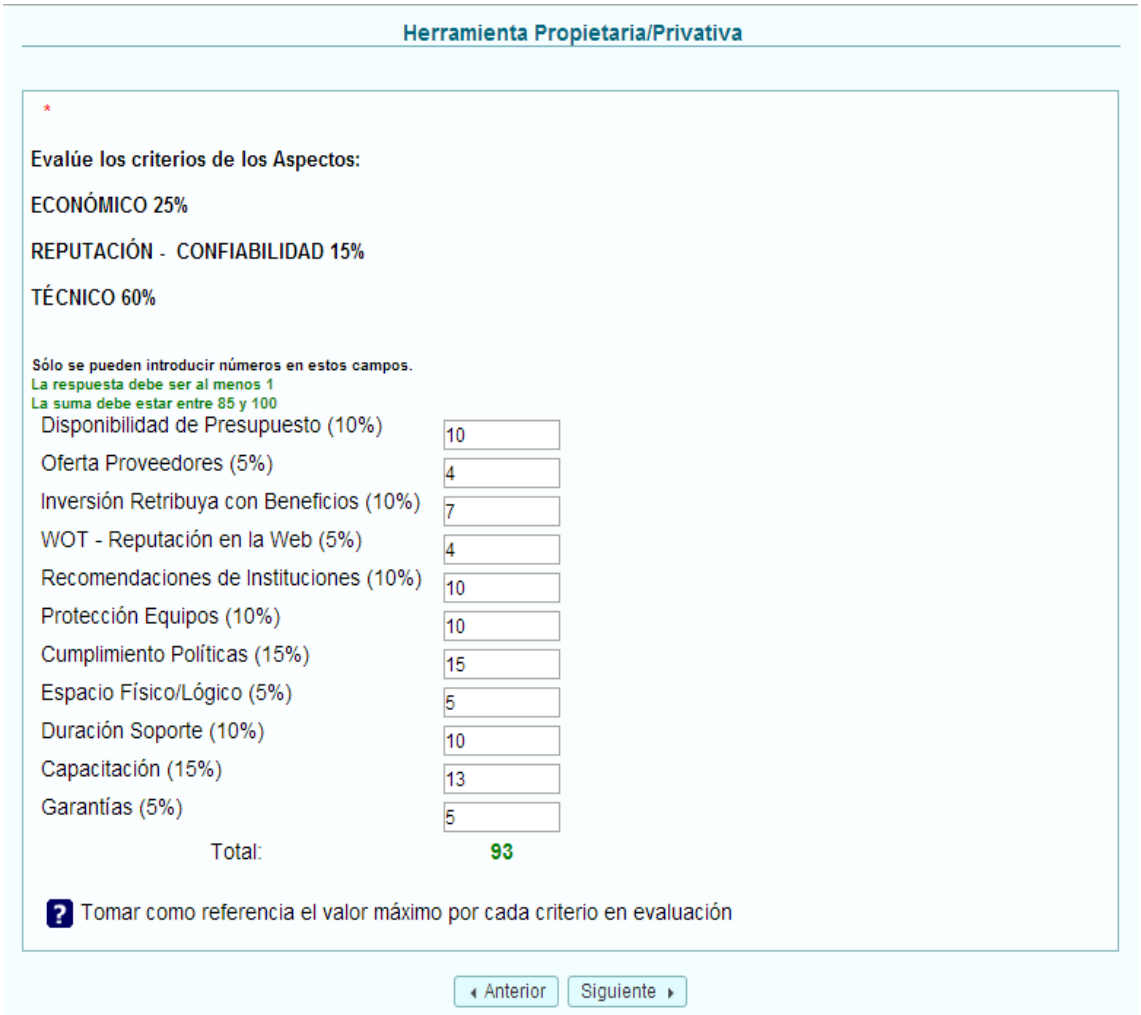


Figura 18: Evaluación Grupo de Preguntas 3-Herramienta Propietaria/Privativa.

Luego de la evaluación exhaustiva de cada uno de los criterios a través de la propuesta presentada, demostraciones de la herramienta, y criterios del personal técnico que manipulará la herramienta etc. Se procede a la verificación del resultado de la evaluación.

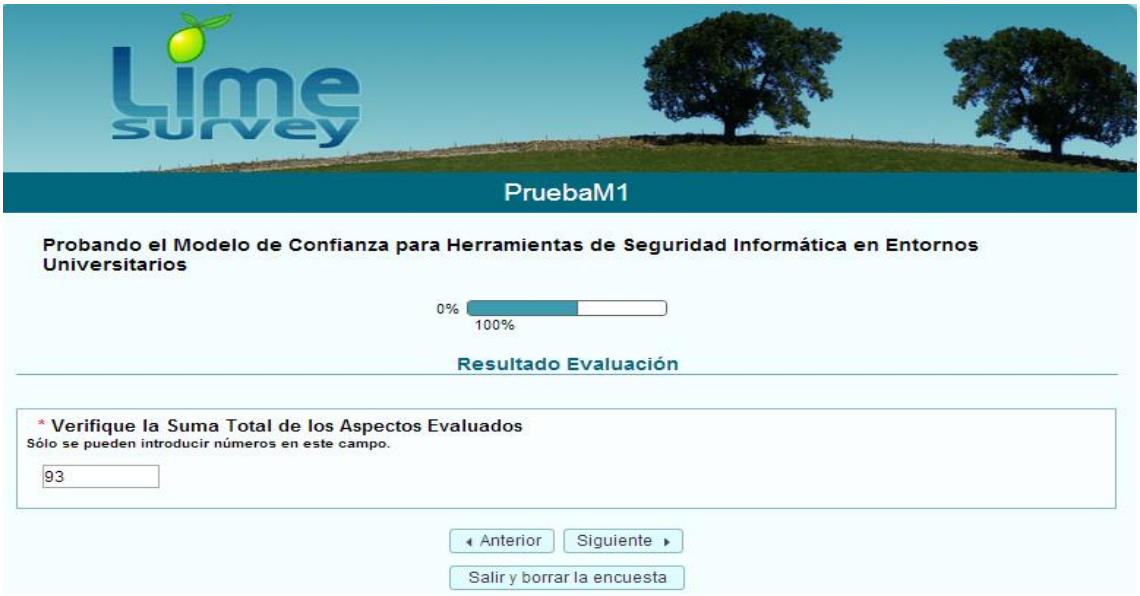


Figura 19: Evaluación Grupo de Preguntas 6-Resultado Evaluación

A continuación se procede a la determinación del nivel de confianza obtenido en base al porcentaje alcanzado tras la evaluación de cada uno de los criterios (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.4), en este caso se ha logrado alcanzar un 93% de confiabilidad de la herramienta evaluada, lo que significa que la factibilidad de implementación de la herramienta Antivirus tiene un Nivel de Confianza MEDIO, de acuerdo a los intervalos del escenario evaluado.

Figura 20: Evaluación Grupo de Preguntas 7-Nivel de Confianza MEDIO-Escenario1.

Finalmente, se presenta una interfaz de culminación de la encuesta empleada como método de evaluación para el modelo propuesto.

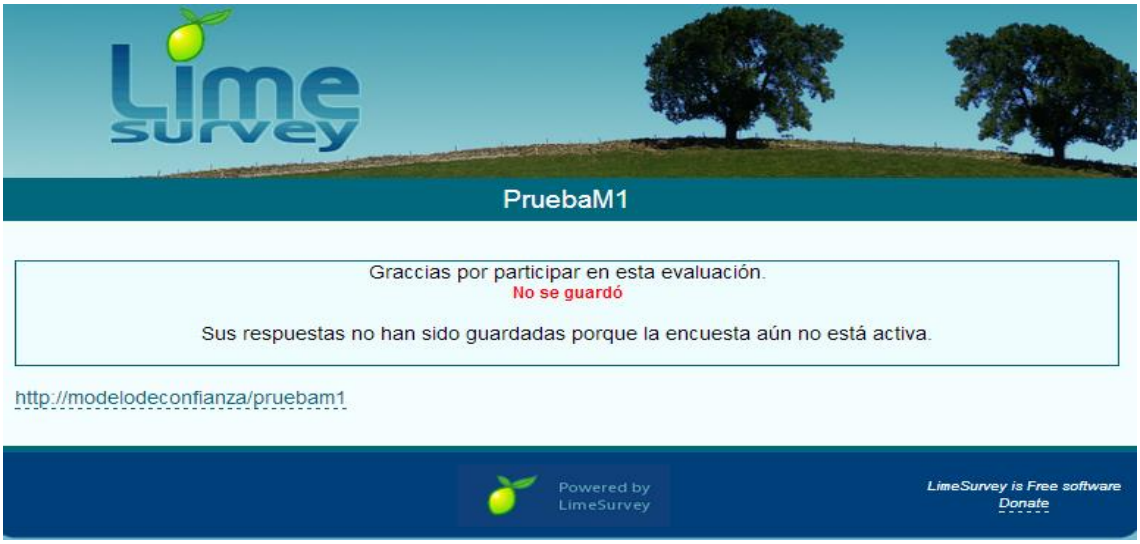


Figura 21: Interfaz de Finalización de la Evaluación.

5.2.1. OTRAS INTERFACES DEL MODELO

Por su parte, a continuación, se muestran las interfaces en caso de seleccionar cualquiera de los otros dos escenarios.

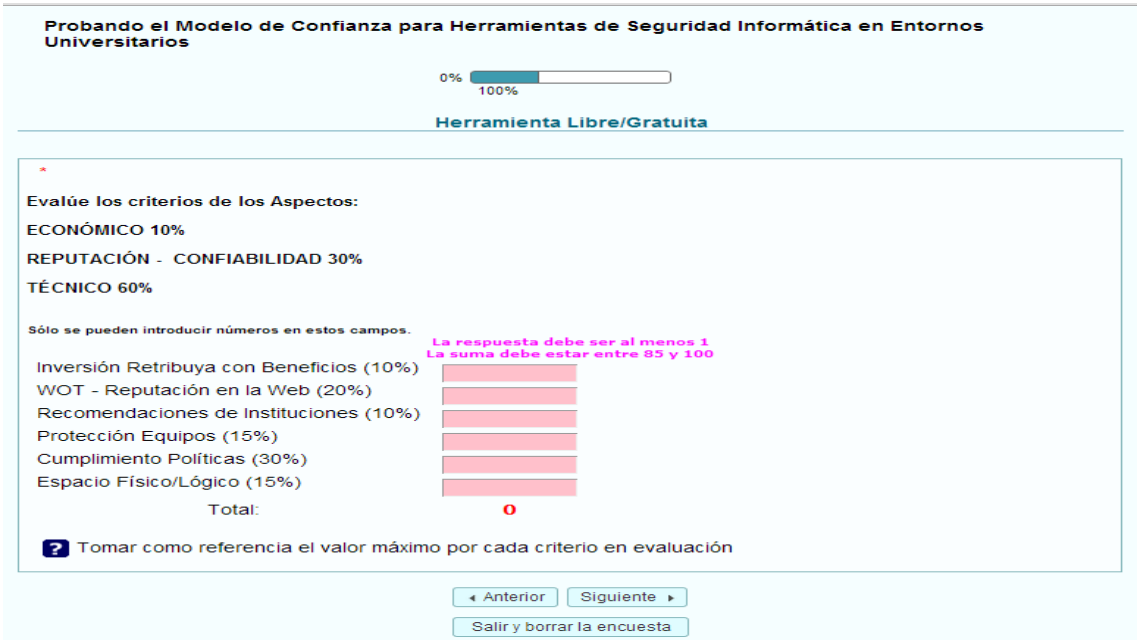


Figura 22: Evaluación Grupo de Preguntas 4-Herramienta Libre/Gratuita.

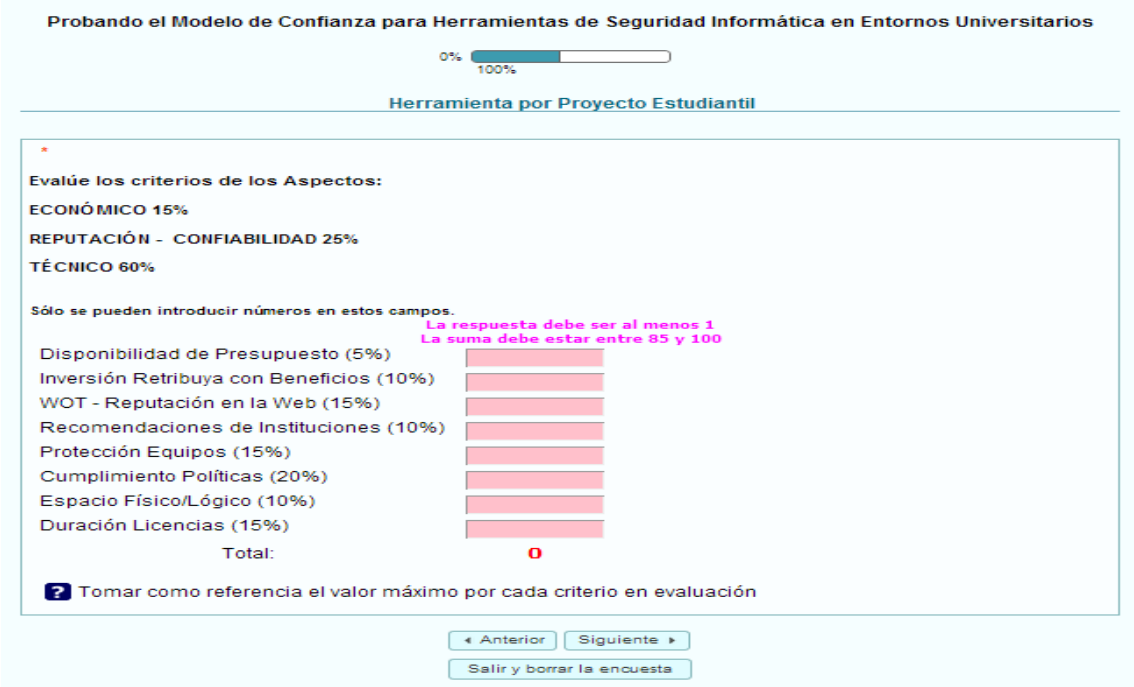


Figura 23: Evaluación Grupo de Preguntas 5-Herramienta por Proyectos Estudiantiles.

Asimismo, se presentan a continuación las interfaces de los otros niveles de confianza, recalcando que cada nivel está enmarcado a los intervalos dentro de cada escenario (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.4).

Figura 24: Evaluación Grupo de Preguntas 7-Nivel de Confianza BAJO-Escenario1.

Figura 25: Evaluación Grupo de Preguntas 7-Nivel de Confianza ALTO-Escenario1.

g. Discusión

1. Desarrollo de la Propuesta Alternativa: Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios empleando el Escenario 1: Herramienta Propietaria/Privativa.

En lo que tiene que ver con la discusión de los resultados obtenidos tras todo el proceso de investigación, desarrollo del modelo propuesto y de la experimentación del mismo, seguidamente se procede a detallar de acuerdo al cumplimiento de cada objetivo.

1.1. Comparar las herramientas de seguridad informática que han sido implementadas actualmente en entornos universitarios.

Dentro del primer objetivo se estableció la necesidad de comparar las herramientas de seguridad informática más implementadas en entornos universitarios y para consumar este objetivo fue necesario la profunda revisión bibliográfica en la Web [18-25] con el fin de obtener una visión más clara de las herramientas mayormente implementadas (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 1). Asimismo de gran ayuda fue la asistencia al DISI 2013 evento realizado en la Universidad Técnica Particular de Loja, en donde se trataron temas de gran importancia dentro del área de la seguridad informática; dentro de los temas se publicaron resultados obtenidos tras la aplicación de la "I Encuesta de Seguridad de la Información en Universidades Ecuatorianas miembros de CEDIA", en donde se conoció las herramientas más implementadas en entornos universitarios (Ver Anexo 2).

Para obtener los resultados digitales de la encuesta se estableció contacto con CEDIA, solicitando los mismos, obteniendo como respuesta el contacto formal con la Ing. Julia Pineda (Líder de Seguridad UTPL), puesto que la encuesta se había realizado en conjunto con el Departamento de Seguridad de la Información de la UTPL (Ver Anexo 1).

Después de haber establecido el contacto respectivo, se vio la necesidad de asistir las oficinas del Departamento a su cargo para una breve entrevista y para la entrega del informe en formato digital (.pdf) de la encuesta en alusión (Ver Anexo 2).

Con la obtención del informe oficial, se ha podido determinar cuáles son las herramientas de seguridad informática más implementadas en entornos universitarios, para proceder a analizar parte de ellas, incluyendo sus ventajas y desventajas; obteniendo como resultado de este objetivo el motivo por el cual se implementan determinadas herramientas y en base a qué se realizan dichas implementación. Añadiendo a los resultados, se plantea una pirámide jerárquica personalizada de la implementación de las herramientas analizadas.

1.2. Revisar la existencia de estándares que evalúen la confiabilidad en las herramientas de seguridad informática.

En lo que concierne a la revisión de estándares que evalúen la confiabilidad de herramientas de seguridad informática, previa a su implementación, se procedió a realizar la búsqueda de estándares o normas que se acoplen en su mayoría a este tipo de toma de decisiones, a la hora de implementar herramientas de seguridad informática. Siendo la búsqueda poco provechosa, debido a que existen guías de buenas prácticas, pero orientadas a gestionar proyectos en general y no precisamente para evaluar la confiabilidad de herramientas específicas, en este caso de seguridad informática. Después de haber buscado normas, estándares se ha podido rescatar un apartado importante de la norma ISO 17799 [3-5], el mismo que hace mención a la Gestión de Comunicaciones y Operaciones, específicamente en el apartado de Control de Cambios Operacionales, en donde se hace referencia a las ventajas y desventajas que puede traer consigo una apropiada y no apropiada toma de decisiones respectivamente; decisiones que en fin repercutirán en el funcionamiento de los sistemas dentro del entorno universitario en estudio (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 2). Por su parte se logró investigar un poco en lo que tiene que ver con COBIT 5: Un Marco del Negocio para

el Gobierno y la Gestión de las TI de la Empresa, lo que permitió brindarle un valor adicional a cada criterio del modelo y escenarios propuestos.

De igual manera se indagó sobre herramientas Web que garanticen confianza en la Web, encontrando a WOT, herramienta que permite saber en qué sitios Webs se puede confiar basado en las experiencias de millones de usuario y validadas con listas negras a nivel mundial, garantizando así una nula manipulación de la valoración de confianza [17]. Por otro lado, se inquirió los criterios tomados en cuenta a la hora de decidir por una implementación de mecanismos de seguridad informática en entornos universitarios, información que se utiliza en el desarrollo y cumplimiento del siguiente objetivo.

1.3. Proponer el modelo de confianza para la implementación de herramientas de seguridad informática.

Al llegar al objetivo específico de mayor relevancia, el cumplimiento del mismo se llevó a cabo mediante la realización de entrevistas, encuestas a personal interno, UTI-UNL (Ver Anexos 4 y 6); y, externo: UTPL, ESPOL, ULVR, UTMACH y Consultores TI (Ver Anexos 7-13), con el fin de conocer la metodología empleada previa a la implementación de mecanismos de seguridad informática (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3).

Cabe recalcar que con el fin de obtener un punto de vista más amplio a nivel profesional y de gestión de mecanismos en el área de la seguridad informática, se asumió como reto personal y profesional la “I Maratón de Certificaciones Tecnológicas: Microsoft – Yachay” postulando a la certificación de Fundamentos de Seguridad, para lo cual fue necesario tomar como base el estudio del Kit otorgado por las instituciones certificadoras [7]. Luego de rendir el examen en la sede Loja de la Universidad Internacional del Ecuador el 17 de Enero del 2014 se logra alcanzar la certificación 98-367 MTA: Security Fundamentals (Ver Anexo 14), certificación que de manera positiva aportó al mejor desarrollo del

presente objetivo y, por ende, llegar a la culminación satisfactoria del trabajo de titulación.

Después de haber realizado las entrevistas señaladas con anterioridad (Ver Anexos 4, 6-13), se ha podido conocer la forma y/o metodología empleada durante el proceso previo a la implementación de mecanismos de seguridad informática, otorgando así una pauta para el establecimiento de los criterios para el modelo propuesto. Con la información recolectada de las entrevistas se ha planteado los criterios de evaluación (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.1) y se ha contrastado que cada uno de ellos vaya de la mano con los principios básicos de la seguridad así como con la norma ISO y el Marco de Negocio de COBIT 5, ya antes indicados (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.2). Luego de haber planteado los criterios de evaluación y de su respectivo análisis se estableció tres posibles escenarios de evaluación (Herramientas Propietaria/Privativa, Herramienta Gratuita/Libre, Proyectos Estudiantiles); cada uno de ellos con criterios variantes (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.1). Apegado al planteamiento de escenarios se cita la asignación de pesos genéricos a cada criterio dentro de cada escenario de evaluación del modelo creado, siendo este peso adaptable a la situación del entorno universitario en donde se ponga a prueba (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.3). De igual manera, mediante encuesta/entrevista con parte del personal de la UTI (Ver Anexos 16-18) se ha procedido determinar los niveles de confianza para el modelo, categorizándolo en niveles: alto, medio, bajo; cada uno de ellos con un rango de porcentaje asignado (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE 3, APARTADO 3.4).

1.4. Experimentar con el modelo propuesto sobre alguna de las herramientas de seguridad informática previamente estudiadas para evaluar su grado de confianza.

Para la culminación y demostración del objetivo de experimentación con el modelo propuesto se inició con la solicitud de una entrevista con el Ing. Milton Palacios Director de la UTI (Ver Anexo 15), solicitándole la apertura para la puesta en marcha del modelo propuesto aplicándolo al proyecto de adquisición e implementación de un Antivirus (Kaspersky) con Licenciamiento Corporativo para la Universidad Nacional de Loja (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE4, APARTADO 4.2), obteniendo una respuesta positiva para la evaluación; así como información de los contactos de la empresa que pretende implementar la herramienta. Partiendo de aquello se establece contacto con la empresa CoreSolutions S.A., haciendo la petición formal de la propuesta para la UNL, la misma que fue base para proceder a determinar el escenario de evaluación del modelo (Ver Anexo 19).

El escenario evaluado fue el Escenario1: Herramientas Propietarias/Privativas (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE4, APARTADO 4.2 y 4.3), en donde se procede a analizar cada criterio y a asignar el peso correspondiente de acuerdo al estado y disponibilidad de los recursos por parte de la UNL, de la misma forma se presenció la instalación, configuración y funcionamiento del DEMO (Ver Anexos 22 y 28) del antivirus en la Sección de Mantenimiento Electrónico de la UTI en donde se adquirió información complementaria para la culminación de la evaluación de la herramienta con el modelo (Ver Anexo 22).

Tras la evaluación de la herramienta con el modelo propuesto (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE4, APARTADO 4.3) se ha determinado que en base al porcentaje final obtenido, el nivel de confiabilidad de la implementación de la herramienta de seguridad informática en cuestión es MEDIO (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE4, APARTADO 4.4), debido a las características de

algunos de los equipos finales donde se pretende instalar el sistema antivirus.

Por su parte, es necesario indicar que el modelo propuesto fue presentado al “II Concurso de Reconocimiento de la Investigación Universitaria – Galardones 2014” (Ver Anexos 23 y 24) con el fin de realizar un aporte original a la comunidad científica, así como obtener una evaluación del mismo; logrando ser Semifinalista del mencionado Concurso Nacional (VER SECCIÓN RESULTADOS, SUBSECCIÓN FASE4, APARTADO 4.5).

Añadiendo un plus a la evaluación manual, detallada y presencial de la implementación de la herramienta se ha realizado la implementación del modelo propuesto mediante el uso de un cuestionario de prueba en LimeSurvey, actividad que sin ser obligatoria en indispensable para el trabajo de titulación ha permitido obtener una visión más clara del funcionamiento del modelo así como del proceso llevado a cabo para determinar el nivel de confianza de la implementación de una herramienta de seguridad informática en entornos universitarios. (VER SECCIÓN RESULTADOS, SUBSECCIÓN 5 ACTIVIDAD COMPLEMENTARIA, APARTADO 5.1 Y 5.2). La presentación de esta prueba adaptada al mencionado software no es la más precisa, pero si una de la más ágiles a la hora de poner a prueba la creación de modelos en diversos ámbitos, rescatando así que la herramienta utilizada es de carácter libre y gratuita, lo que facilita la implementación.

2. Valoración Técnica Económica

La realización del presente trabajo de titulación se llevó a cabo mediante el establecimiento de un presupuesto inicial, en donde se había establecido diferentes valores, tanto en talento humano, recursos de hardware y software, técnicos y de comunicaciones; que fueron primordiales para llegar al cumplimiento de todos los objetivos planteados. Pero también es viable mencionar que existió un desbalance en el cronograma de actividades, así como en el presupuesto de cada uno de los aspectos denotados con anterioridad; puesto que al ser un trabajo más de carácter investigativo, que necesitaba de la obtención de información tanto interna como externa a la Universidad Nacional de Loja, obligó solicitar un periodo de prórroga y, por ende, incrementó ámbitos como el de comunicaciones y de capacitaciones externas para llegar a un buen término en cada fase. A continuación, se pretende describir el presupuesto aproximado real del trabajo de titulación por cada uno de los apartados:

- **Talento Humano**

  En lo que respecta al presupuesto de talento humano, se incluye la participación del estudiante postulante (investigador), el director del mismo, personal interno/externo y de consultor TI. Todo esto tomando en cuenta el tiempo real de la duración del trabajo de titulación.

TABLA XVI

PRESUPUESTO TALENTO HUMANO

Equipo Trabajo	Tiempo (Horas)	Precio/ Hora ($)	Valor Total ($)
Investigador	1120	5.00	5600.00
Director	192	10.00	960.00
Personal UTI	50	10.00	500.00
Personal Externo	10	10.00	1000.00
Consultor TI	4	20.00	80.00
SUBTOTAL ($)			**8140.00**

- **Recursos Técnico y Tecnológicos**

En lo que respecta a los recursos técnicos y tecnológicos dentro del trabajo de titulación, no ha existido mayor alteración al presupuesto establecido inicialmente; en lo que respecta al aumento de recursos, quizás un desfase, pero únicamente en el tiempo utilizado por cada recurso. Importante acotar que todos los elementos técnicos hardware, así como los elementos tecnológicos en general, han servido de gran aporte para el desarrollo y culminación del trabajo de titulación.

TABLA XVII

PRESUPUESTO RECURSOS HARDWARE

Descripción	**Cant.**	**V. Unitario($)**	**Tiempo Utilizado (Meses)**	**Vida Útil/Años**	**Valor Total ($)**
Portátil Xtratech	1	1150.00	10	3	1150.00
Flash Memory 4G	1	10.00	10	1	10.00
Impresora	1	100.00	10	2	100.00
	SUBTOTAL ($)				**1260.00**

TABLA XVIII

PRESUPUESTO RECURSOS SOFTWARE

RECURSOS SOFTWARE			
Descripción	**Cant.**	**V. Unitario($)**	**Valor Total ($)**
Sistemas Operativos Windows 8	1	140.00	140.00
Gantt	1	0.00	0.00
Paquete de Ofimática de Microsoft Office 2013 (licencia estudiantes)	1	170.00	170.00
Google Drive	1	0.00	0.00
Dropbox	1	0.00	0.00

LimeSurvey	1	0.00	0.00
SUBTOTAL($):			**310.00**

Dentro de los recursos software se denota los costos de utilización de aplicaciones tanto propietarias como de código libre. Siendo estas últimas las de mayor utilización y ventajosas a la hora de realizar las diferentes actividades establecidas dentro del trabajo de titulación.

Para ir finalizando, se cita detalladamente los costos unitarios así como los totales de los recursos materiales y los servicios empleados para el desarrollo del presente trabajo; resaltando que en el aspecto de servicios sí ha sido incrementado, debido a la extensión del cronograma para recabar correctamente la información necesaria.

TABLA XIX

PRESUPUESTO RECURSOS MATERIALES Y SERVICIOS

RECURSOS MATERIALES			
Descripción	**Cant.**	**V. Unitario ($)**	**V.Total ($)**
Resma de papel	4	5.00	20.00
Anillados	5	1.50	7.50
Empastados	3	10.00	30.00
Copias	900	0.02	18.00
Cartuchos de Tinta	4	25.00	100.00
CD’s	3	0.75	2.25
SERVICIOS			
Transporte	600	0.25	150.00
Comunicaciones	50	1.00	50.00
Capacitaciones	3	25.00	75.00
Internet	1120 horas	0.70	784.00
SUBTOTAL ($)			**1236.75**

- **Presupuesto General.**

  Finalmente, se indica en la siguiente tabla el costo total aproximado del trabajo de titulación. De igual manera se establece el 10% del coste total aproximado para Imprevistos presentados a lo largo del desarrollo del trabajo.

TABLA XIX

PRESUPUESTO GENERAL

PRESUPUESTO TOTAL	
RECURSOS	**SUBTOTALES ($)**
TALENTO HUMANO	8140.00
HARDWARE	1260.00
SOFTWARE	310.00
MATERIALES Y SERVICIOS	1236.75
SUBTOTAL	**10946.75**
IMPREVISTOS (10%)	1094.68
TOTAL ($)	**12041,43**

2.1. Valoración Ambiental

En lo que concierne a la valoración ambiental del trabajo de titulación, este se respalda ambientalmente por el hecho de desvincularse de algún tipo de daño al medio ambiente en los diferentes momentos que se llevó a cabo las entrevistas, encuestas e investigaciones de campo para la posterior determinación de criterios, que incidieron en cualquiera de los tres escenarios planteados y, finalmente, la asignación de un nivel de confianza a las herramientas de seguridad informática que se pretendan implementar en los entornos universitarios. Si bien es cierto, además de aislarse de algún posible daño al ecosistema, más bien promueve la toma de decisiones ágiles y más apropiada posible, evitando la implementación vana de otras herramientas, lo que si conlleva a mantener los equipos encendidos por más horas fuera de lo normal, esperando instalaciones de paquetes o descargas de actualizaciones; ocasionando el uso excesivo de un recurso natural como lo es la energía.

h. Conclusiones

- Mediante las diferentes visitas técnicas a las universidades del país, el análisis de los diferentes casos de estudio y escenarios, así como la información obtenida a través del personal interno de la UNL y CEDIA se ha podido determinar, verificar y validar que las herramientas con mayor nivel de implementación en entornos universitarios son los Antivirus seguido de los Firewalls, IDS y Redes Trampas (Honeypot).

- El modelo propuesto se encuentra enmarcado en los principios de Seguridad de la Información, en la sección Gestión de Comunicaciones y Operaciones, específicamente en el apartado Control de Cambios Operacionales de la norma ISO/IEC 17799:27000, 270004, 270005 y en el Modelo de Referencia de Procesos de COBIT 5 , lo que le otorga mayor confiabilidad al mismo. Y por ende garantizará que el nivel de confianza obtenido tras la evaluación de una herramienta de seguridad informática sea el más aceptable para determinar la factibilidad de implementación.

- Debido a la ausencia de modelos con propósitos similares al del propuesto, considérese el presente modelo como una base y con visión a mejorar. Puesto que pensando en aquello, los pesos y criterios establecidos en cada uno de los tres escenarios, son genéricos; es decir adaptables al entorno en donde se pretenda aplicarlo.

- Tras la evaluación del proyecto de implementación del programa antivirus Kaspersky en la Universidad Nacional de Loja con el modelo propuesto y el respectivo escenario, se logra identificar la existencia de equipos con falta de especificaciones técnicas para la instalación de la herramienta en cuestión, lo que conlleva a un funcionamiento no adecuado de dichos equipos y, por ende, la disminución al nivel de confianza para la implementación de la herramienta evaluada.

i. Recomendaciones

- Previo al uso del modelo propuesto es necesario el Estudio de Factibilidad Económica así como el Estudio y Valoración Técnica tanto del Entorno como de los Equipos donde se pretende implementar herramientas de seguridad informática, con el fin de determinar si la institución de educación superior cuenta en su totalidad o con la mayoría de especificaciones técnicas y evitar pérdida de tiempo en este tipo de análisis y desconcentrar una serie de procesos que llevan a la toma de decisiones de TIC's.

- En vista de que el modelo propuesto, es una creación en base a revisión bibliográfica, visitas técnicas y entrevistas con personal especializado en áreas a fines, es importante tomar en cuenta que puede darse alteración de ciertos criterios o pesos dentro del mismo, dependiendo del entorno donde se aplique y del tipo de usuarios que lo manipulen.

- El modelo propuesto está adecuado para ser manipulado por personal con conocimientos básicos en Seguridad, Redes y Gestión de TIC's permitiéndole al usuario adaptarse fácilmente al mismo, así como le brinda la posibilidad de realizar cambios necesarios y justificables según las necesidades del entorno, siempre y cuando sean enmarcados a normas o marcos de negocio.

- Considerar la adaptabilidad del modelo propuesto en su totalidad a los Procesos llevados a cabo en el Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa así como a la familia de las normas ISO/IEC 27000, para lograr alcanzar un nivel mayor en la Gestión de Tecnología de Información y Comunicación dentro de la Universidad Nacional de Loja.

j. Bibliografía

Referencias Bibliográficas

[1] CEDIA - UTPL, “I Encuesta de Seguridad de la Información en Universidades Ecuatorianas Miembros de CEDIA”, https://www.dropbox.com/s/9ptnm42rppzcivx/Informe%20de%20ResutladosEcuestaUniversiades.pdf, Accedido el 30 de Enero de 2014

[2] BANCO DE LA REPÚBLICA DE BOGOTÁ, COLOMBIA- DEPARTAMENTO DE SEGURIDAD INFORMÁTICA, “Mecanismos de Seguridad de los Servicios Informáticos”, http://www.banrep.gov.co/sites/default/files/paginas/Mecanismos_de_Seguridad_Informatica.pdf, Accedido el 10 de Octubre de 2013

[3] Yori, J. – MVA, “Un acercamiento a las mejores prácticas de seguridad de información internacionalmente reconocidas en el estándar ISO 17799:2005- ¿Qué es la Norma ISO 17799?”, http://www.mvausa.com/Colombia/Presentaciones/INTRODUCCION_ISO_17799.pdf, Accedido el 09 de Octubre de 2013

[4] Bonilla, G., “Seguridad de la Información Norma ISO 17799”, http://www.ciiasdenic.net/files/doccursos/1196890583_ConferenciaISO17799.pdf, Accedido el 05 de Octubre de 2013

[5] Enríquez, M.E.- NORMA TÉCNICA PERUANA-NORMA ISO 17799, “EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información”, http://www.slideshare.net/marieu.enriquez/norma-iso-17799, Accedido el 09 de Octubre de 2013

[5] Universidad Centro Occidental Lisandro Alvarado, “NORMAS DE SEGURIDAD INFORMÁTICA Y DE TELECOMUNICACIONES”, http://www.ucla.edu.ve/Telecom/NORMAS_de_seguridad_INF_y_de_telecomunicaciones_UCLA.pdf, Accedido el 20 de Agosto de 2013

[6] Hernández Pinto, M.G. – Naranjo Sánchez, B.A., “Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial”, www.dspace.espol.edu.ec/bitstream/123456789/15875/2/CICYT.docxwww.dspace.espol.edu.ec/bitstream/123456789/15875/2/CICYT.docx, Accedido el 05 de Octubre de 2013

[7] KIT de Repaso para el examen de la Certificación Microsoft Technology Associate: FUNDAMENTOS DE SEGURIDAD, MICROSOFT-EDUTEC-YACHAY, “Principios Fundamentales de Seguridad”, Ecuador 2013

[8] Hermoso, R. – Vasirani, M. – Universidad Rey Juan Carlos, “Seguridad Informática-Seguridad en Redes”, http://www.ia.urjc.es/cms/sites/default/files/userfiles/file/SEG-I/2012/introduccion-redes.pdf, Accedido el 08 de Octubre de 2013

[9] Universidad de Sevilla- Departamento de Ciencias de la Computación e Inteligencia Artificial, “Seguridad Informática”, http://www.cs.us.es/cursos/ai-2003/.../8.-**Seguridad**%20**Informatica**.ppt, Accedido el 10 de Octubre de 2013

[10] López Cámara, L.A. – Universidad Veracruzana, “Objetivo de la Seguridad Informática”, http://www.uv.mx/personal/llopez/files/2011/09/presentacion.pdf, Accedido el 06 de Octubre de 2013

[11] Universidad Pontificia de Comillas – Curso de Doctorado en Seguridad de Redes de Ordenadores, “Introducción a la Seguridad Informática”, http://www.iit.upcomillas.es/palacios/seguridad_dr/tema1_intro.pdf, Accedido el 10 de Octubre de 2013

[12] Cortes Argueta, J., “Criptografía- Principio de Kerckhoff”, http://www.openboxer.260mb.com/asignaturas/criptografia/principioKerckhoff.pdf, Accedido el 02 de Octubre de 2013

[13] Rodríguez, D. – Rincón, J., “Modelo, Modelar, Modelo del Sistema Viable, Factibilidad y Viabilidad”, http://www.slideshare.net/toofymen/modelo-informtico, Accedido el 02 de Octubre de 2013

[14] Vogelmann Martínez, E., “Políticas y Modelos de Seguridad”, http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonEste.pdf, Accedido el 02 de Octubre de 2013

[15] Chamba Eras, L.A. Arruarte, A. Elorriaga, J.A. “IMPACTO DE UN FACTOR DE SEGURIDAD DE LA INFORMACIÓN SOBRE OBJETOS DE APRENDIZAJE EN LMS”, http://dspace.unl.edu.ec:8080/jspui/bitstream/123456789/235/1/A_IMPACTO%20DE%20UN%20FACTOR.pdf, Accedido el 25 de Agosto de 2013

[16] Chamba Eras, L.A., TESIS: “MODELO DE CONFIANZA PARA OBJETOS DE APRENDIZAJE EN COMUNIDADES DE APRENDIZAJE”, http://www.ccia-kzaa.ehu.es/s0140-con/es/contenidos/informacion/tesis_master/es_t_master/adjuntos/11lchamba.pdf, Accedido el 25 de Agosto de 2013

[17] WOT – Confianza en la Web, https://www.mywot.com/, Accedido el 19 de Octubre de 2013

[18] Avilés Monroy, J.I. – Pazmiño Castro, M.R., TESIS: “Captura y Análisis de los Ataques Informáticos que Sufren las Redes de Datos de la ESPOL, Implantando una Honeynet con Miras a Mejorar la Seguridad Informática en Redes de Datos del Ecuador”, http://www.dspace.espol.edu.ec/handle/123456789/7781, Accedido el 09 de Octubre de 2013

[19] Avilés Monroy, J.I. – Pazmiño Castro, M.R.- Abad, C., ARTÍCULO: “Captura y Análisis de los Ataques Informáticos que Sufren las Redes de Datos de la ESPOL, Implantando una Honeynet con Miras a Mejorar la Seguridad Informática en Redes de Datos del Ecuador”,

http://www.dspace.espol.edu.ec/handle/123456789/4203, Accedido el 10 de Octubre de 2013

[20] Avilés Monroy, J.I. – Pazmiño Castro, M.R.- Abad, C., ARTÍCULO: "Diseño Preliminar de una Honeynet para Estudiar Patrones de Ataques en las Redes de Datos de la ESPOL", http://www.dspace.espol.edu.ec/handle/123456789/4784, Accedido el 10 de Octubre de 2013

[21] Torres García, D.F. –Zambrano Nuñez, P.S., TESIS: "Implementación de un Sistema de Detección y Análisis de Intrusiones No Autorizadas Utilizando Honeypots Caso Práctico DESITEL-ESPOCH", http://dspace.espoch.edu.ec/handle/123456789/1495, Accedido el 10 de Octubre de 2013

[22] Espinoza, M.P. – Pilco, R. – Montalaván, H., "Honeynet como Apoyo a la Investigación de Seguridad de Redes en entornos Universitarios", http://www.docstoc.com/docs/55437009/proyecto-honeynet---UTPL, Accedido el 27 de Agosto de 2013

[23] Espinoza, M.P. – Pilco, R., Montalván, H., PAPER: "Honeynet como Apoyo a la Investigación de Seguridad de Redes en entornos Universitarios", http://www.docstoc.com/docs/55437009/proyecto-honeynet---UTPL, Accedido el 10 de Octubre de 2013

[24] Ludeña Ramírez, S.F., TESIS: "Análisis del Tráfico Malicioso en los Servicios Críticos Internos de la UTPL", http://dspace.utpl.edu.ec/handle/123456789/2190, Accedido el 10 de Octubre de 2013

[25] Montalván Celi, C.A., TESIS: "Análisis del Tráfico Malicioso de los Servicios Externos de la UTPL", http://dspace.utpl.edu.ec//jspui/handle/123456789/1424, Accedido el 10 de Octubre de 2013

[26] Universidad Católica de Temuco, “Estudio de Casos como técnica didáctica”,http://www.uctemuco.cl/cedid/archivos/apoyo/El%20estudio%20de%20casos%20como%20tecnica%20didactica.pdf, Accedido el 10 de Octubre de 2013

[27] Universidad de las Américas Puebla, “Estudio de Caso”, http://www.udlap.mx/intranetWeb/centrodeescritura/files/notascompletas/estudiodeCaso.pdf, Accedido el 10 de Octubre de 2013

[28] Barrio del Castillo, I. – Jiménez Gonzáles, J. – Padín Moreno, L. – Peral Sánchez, I. – Tarín López, E., Universidad Autónoma de Madrid, “El Estudio de Casos”,http://www.uam.es/personal_pdi/stmaria/jmurillo/InvestigacionEE/Presentaciones/Est_Casos_doc.pdf, Accedido el 10 de Octubre de 2013

[29] Soto Ramírez, R., Universidad Nacional Autónoma de México, “Método: Estudio de Casos – Curso: Investigación Cualitativa”, http://www.paginaspersonales.unam.mx/files/981/estudio_de_caso.pdf, Accedido el 10 de Octubre de 2013

[30] López O, Ochoa I, Pibaque A, Aranda A, Escuela Superior Politécnica del Litoral - ESPOL, “Desarrollo del Producto para Test de Penetración Enfocado en el Fuzzzing de Aplicaciones”, http://www.dspace.espol.edu.ec/bitstream/123456789/19031/1/paper_fuzzing.pdf, Accedido el 20 de Marzo de 2014

[31] Armijos A, Villamar L, García C, Galio G, Escuela Superior Politécnica del Litoral - ESPOL, “Sistema de Gestión en Seguridad Informática como Soporte a la Toma de Decisiones en Respuesta a Incidentes, Basados en Monitoreo de Redes”, http://www.dspace.espol.edu.ec/bitstream/123456789/14922/1/Sistema%20de%20Gestion%20en%20seguridad%20informatica%20como%20soporte%20a%20la%20toma%20de%20decisiones.pdf, Accedido el 20 de Marzo de 2014

[32] Maya, E. – Vinueza, T., PAPER: “Honeynet Virtual Híbrida en el entorno de red de la Universidad Técnica Del Norte de la ciudad de Ibarra”,

http://repositorio.utn.edu.ec/handle/123456789/1058, Accedido el 10 de Octubre de 2013

[33] EcuaRed, “Antivirus Informáticos”, http://www.ecured.cu/index.php/Antivirus_Inform%C3%A1ticos, Accedido el 2 de Noviembre de 2013

[34] INTECAP, SLIDESHARE, “Tipos de Software Utilitario”, http://www.slideshare.net/trist_dos/tarea-intecap-domingo, Accedido el 2 de Noviembre de 2013

[35] Moliner López, F.J, MAD-Eduforma, “Informáticos Generalitat Valenciana. Grupos a Y B Temario Bloque Específico Volumen II”.

[36] PCMag, “The Best Antivirus for 2014”, http://www.ecured.cu/index.php/Antivirus_Inform%C3%A1ticos, Accedido el 29 de Abril de 2014

[37] McNab A, “Firewall”, Simon and Schuster (2003).

[38] Desarrollo Web, “Qué es un Firewall”, http://www.desarrolloweb.com/articulos/513.php, Accedido el 5 de Noviembre de 2013

[39] HowsTuffWorks, “How Firewalls Work”, http://computer.howstuffworks.com/firewall.htm, Accedido el 9 de Noviembre de 2013

[40] Pantazis R, Universidad del CEMA, “Firewalls de Internet”, http://www.ucema.edu.ar/conferencias/download/Firewalls_de_Internet.pdf, Accedido el 20 de Noviembre de 2013

[41] Gallardo J, Universidad Nacional de Patagonia, “Seguridad en Redes – Firewalls”,

http://www.ing.unp.edu.ar/asignaturas/seminarioseguridad/Firewalls_SeminarioSeguridad_JIG1204.pdf, Accedido el 20 de Noviembre de 2013

[42] Morales Tejeda C, "Estudio, Diseño e Implementación de un Firewall", http://users.salleurl.edu/~is06200/proyectos/TFC-is06200.pdf, Accedido el 23 de Noviembre de 2013

[43] Marín Moreno W, "Modelo OSI", http://www.ie.itcr.ac.cr/marin/mpc/redes/Modelo_osi_tcp_ip(oficial).pdf, Accedido el 10 de Diciembre de 2013

[44] Facultad de Ciencias Exactas, Universidad Nacional del Centro de la Provincia de Buenos Aires, "El Modelo OSI", http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf, Accedido el 10 de Diciembre de 2013

[45] González Márquez, V, Instituto Politécnico Nacional, "Sistema de Detección de Intruso Basado en Sistema Experto", http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/5883/1/1382_Centro%20de%20InvestigaciOn%20en%20ComputaciOn%20(CIC)tesis_Febrero_2010_1100548085.pdf, Accedido el 23 de Septiembre de 2013

[46] Bhandarkar S - EsslingerBrown J, "Firewalls and IDS", http://www.ee.tamu.edu/~reddy/ee689_04/pres_sumitha_james.pdf, Accedido el 8 de Diciembre de 2013

[47] González Gómez D, 2003, "Sistema de Detección de Intrusiones", http://derecho-internet.org/docs/ids.pdf, Accedido el 10 de Diciembre de 2013

[48] Mira Alfaro E, Universidad de Valencia, "Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia", http://www.rediris.es/cert/doc/pdf/ids-uv.pdf, Accedido el 15 de Diciembre de 2013

[49] Brown Computer Sciencie, “Firewalls, Tunnels, and Network Intrusion Detection”, http://cs.brown.edu/cgc/net.secbook/se01/handouts/Ch06-Firewalls.pdf, Accedido el 28 de Noviembre de 2013

[50] Burgos Salazar, J. Campos, P., “MODELO PARA LA SEGURIDAD DE LA INFORMACIÓN EN TIC”, http://ceur-ws.org/Vol-488/paper13.pdf, Accedido el 20 de Agosto de 2013

[51] Waissbein, A.-CORE SECURITY TECHNOLOGIES, “Modelos de Seguridad Informática – Software Protection”, http://www.coresecurity.com/files/attachments/Waissbein_UNR_2004.pdf, Accedido el 02 de Octubre de 2013

[52] UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA-UTPL, “CSIRT-UTPL”, http://www.utpl.edu.ec/csirt-utpl/, Accedido el 02 de Septiembre de 2013

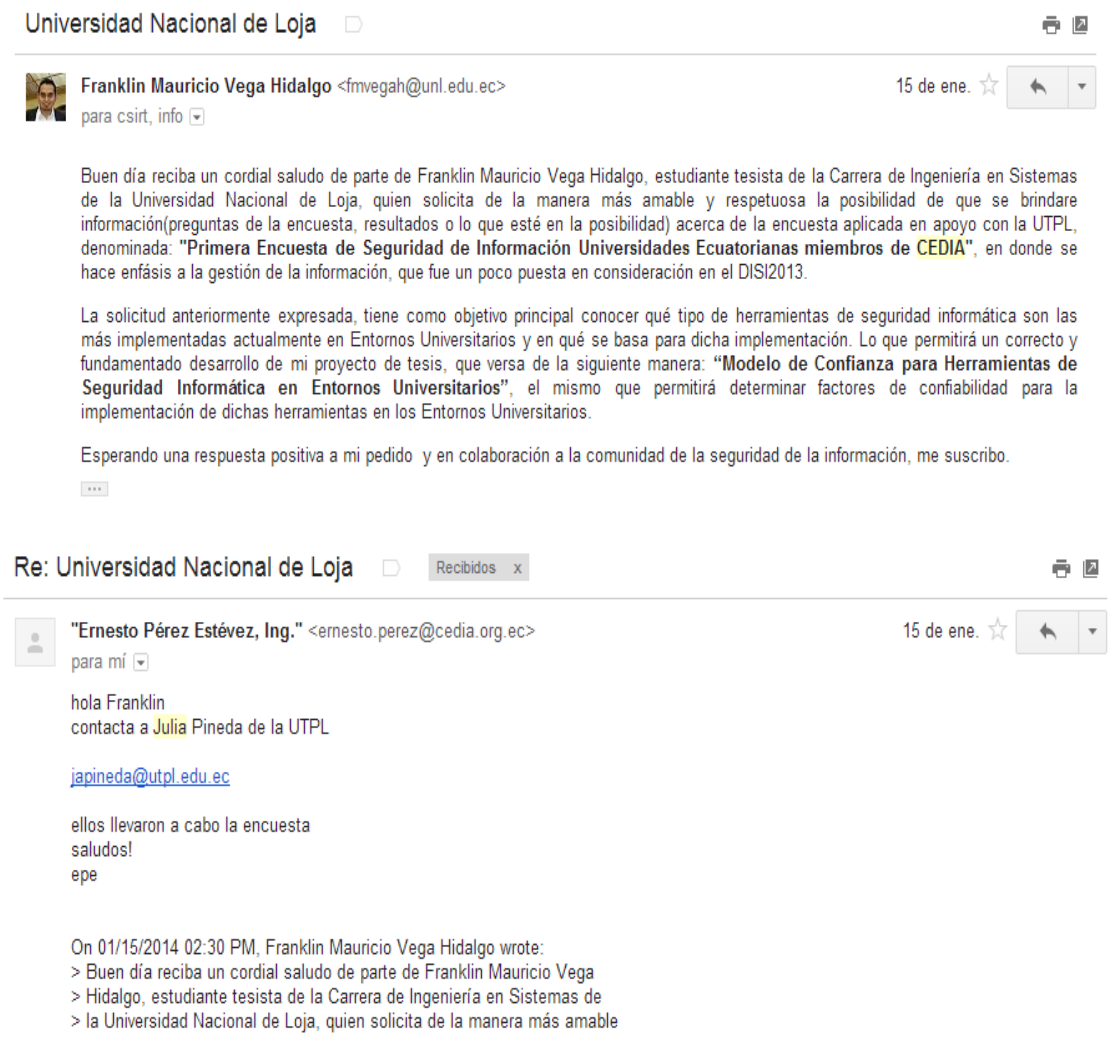
[53] ISACA, “What is COBIT5?”, www.isaca.org/cobit , Accedido el 02 de Julio de 2014

[54] Larrondo Girón, A, Proyecto Fin de Carrera - UNIVERSIDAD SAN CARLOS III DE MADRID, http://e-archivo.uc3m.es/bitstream/handle/10016/10564/PFC_Agustin_Larrondo_Quiros.pdf?sequence=1 , Accedido el 01 de Noviembre de 2014

[55] Larrondo Girón, A, “Proyecto de Norma Técnica Colombiana: NTC-27005”, https://es.scribd.com/doc/236175795/124454177-ISO-27005-espanol-pdf, Accedido el 01 de Noviembre de 2014

k. Anexos

1. Solicitud /Respuesta de CEDIA de la petición de la I Encuesta de Seguridad de Información a las Universidades Miembros de CEDIA



Universidad Nacional de Loja

Franklin Mauricio Vega Hidalgo <fmvegah@unl.edu.ec> 15 de ene.
para csirt, info

Buen día reciba un cordial saludo de parte de Franklin Mauricio Vega Hidalgo, estudiante tesista de la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, quien solicita de la manera más amable y respetuosa la posibilidad de que se brindare información(preguntas de la encuesta, resultados o lo que esté en la posibilidad) acerca de la encuesta aplicada en apoyo con la UTPL, denominada: **"Primera Encuesta de Seguridad de Información Universidades Ecuatorianas miembros de CEDIA"**, en donde se hace enfásis a la gestión de la información, que fue un poco puesta en consideración en el DISI2013.

La solicitud anteriormente expresada, tiene como objetivo principal conocer qué tipo de herramientas de seguridad informática son las más implementadas actualmente en Entornos Universitarios y en qué se basa para dicha implementación. Lo que permitirá un correcto y fundamentado desarrollo de mi proyecto de tesis, que versa de la siguiente manera: **"Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios"**, el mismo que permitirá determinar factores de confiabilidad para la implementación de dichas herramientas en los Entornos Universitarios.

Esperando una respuesta positiva a mi pedido y en colaboración a la comunidad de la seguridad de la información, me suscribo.

Re: Universidad Nacional de Loja Recibidos x

"Ernesto Pérez Estévez, Ing." <ernesto.perez@cedia.org.ec> 15 de ene.
para mí

hola Franklin
contacta a Julia Pineda de la UTPL

japineda@utpl.edu.ec

ellos llevaron a cabo la encuesta
saludos!
epe

On 01/15/2014 02:30 PM, Franklin Mauricio Vega Hidalgo wrote:
> Buen día reciba un cordial saludo de parte de Franklin Mauricio Vega
> Hidalgo, estudiante tesista de la Carrera de Ingeniería en Sistemas de
> la Universidad Nacional de Loja, quien solicita de la manera más amable

Figura 26: Anexo 1- Solicitud/Respuesta CEDIA.

2. **Informe de la I Encuesta de Seguridad de la Información a Universidades miembros de CEDIA.**

INFORME DE RESULTADOS DE LA “1° ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN EN UNIVERSIDADES ECUATORIANAS MIEMBROS DE CEDIA”

INFORME DE RESULTADOS DE LA “1° ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN EN UNIVERSIDADES ECUATORIANAS MIEMBROS DE CEDIA”

RUBRO	NOMBRE – CARGO	FECHA
APROBADO POR:	ING. ERNESTO PÉREZ **RESPONSABLE DEL ÁREA DE SEGURIDAD CEDIA**	
REVISADO POR:	ING. CARLOS CÓRDOVA **DIRECTOR DE LA UNIDAD DE GESTIÓN DE TI UNIVERSIDAD TÉCNICA PARTICUALAR DE LOJA**	
REALIZADO POR	ING. JULIA PINEDA **LÍDER DE SEGURIDAD Y RIESGOS UNIVERSIDAD TÉCNICA PARTICUALAR DE LOJA**	

INFORME DE RESULTADOS DE LA “1° ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN EN UNIVERSIDADES ECUATORIANAS MIEMBROS DE CEDIA”

ANTECEDENTE:

Al celebrar el DÍA INTERNACIONAL DE SEGURIDAD DE LA INFORMACIÓN (DISI), bajo el lema "Creando cultura de seguridad", CEDIA ha creído conveniente realizar un sondeo acerca de la Gestión de la Seguridad de la Información en cada una de sus Universidades miembro a través de la Universidad Técnica Particular de Loja.

OBJETIVO:

Conocer el estado actual de la Gestión de Seguridad en cada Universidad miembro de CEDIA.

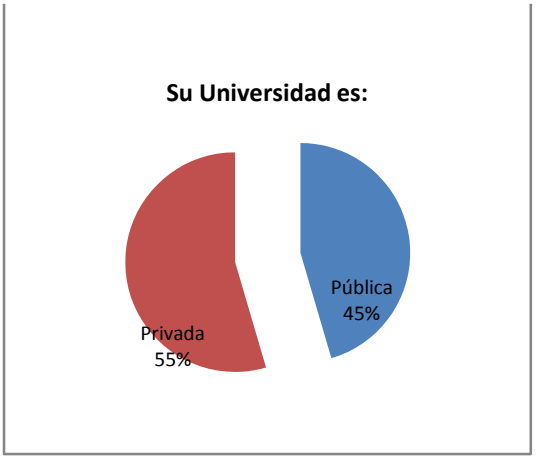
La encuesta fue enviada los representantes de la Universidades miembros de CEDIA (29 universidades), dicha encuesta tuvo el carácter de anónimo y de contestación opcional para los participantes. El 37,97 % (11) de las universidades miembros respondieron al llamado de la encuesta.

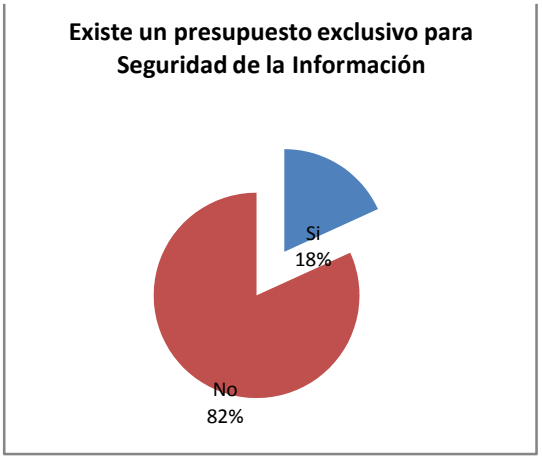
Las fechas en las que se realizó la recolección de las respuestas fueron desde el 14 al 29 de noviembre del 2013.

Los resultados se presentan a continuación.

GENERALIDADES

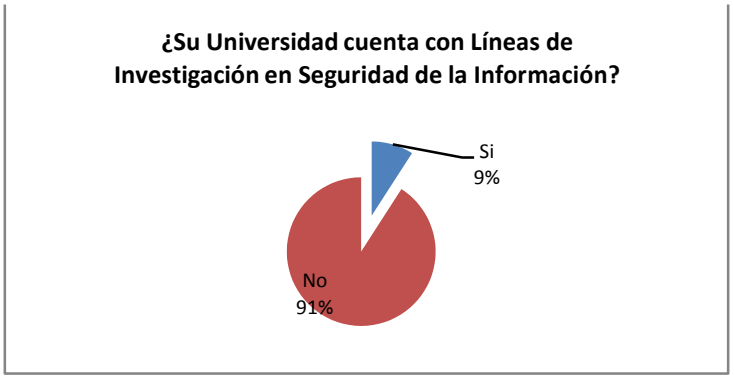
Antes de iniciar con la revisión de las repuestas de las Universidades miembros de CEDIA respecto a la Gestión de la Seguridad es importantes conocer algunas generalidades de estas universidades como es:





De las Universidades que contestaron la encuesta tenemos que el 55% son Universidades Privadas y el 45% Universidades Públicas

También se realizó la pregunta sobre el presupuesto asignado para la Gestión de la Seguridad de la Información y se observó que el 82% de las Universidades no tiene asignado un presupuesto para trabajar exclusivamente para la Gestión de la Seguridad y el 18% si lo tiene.



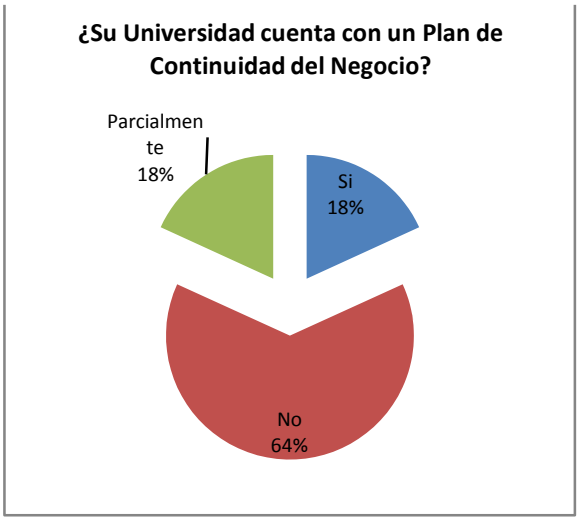
Al ser la Seguridad de la Información un posible línea de investigación y las Universidades tener interés en la investigación se preguntó si tenían alguna línea de Investigación en este campo, de lo cual el 91% no lo tiene y el 9% si, la investigación que se realiza en este 9% corresponde a Vulnerabilidades.

GESTIÓN DE GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN (SI)

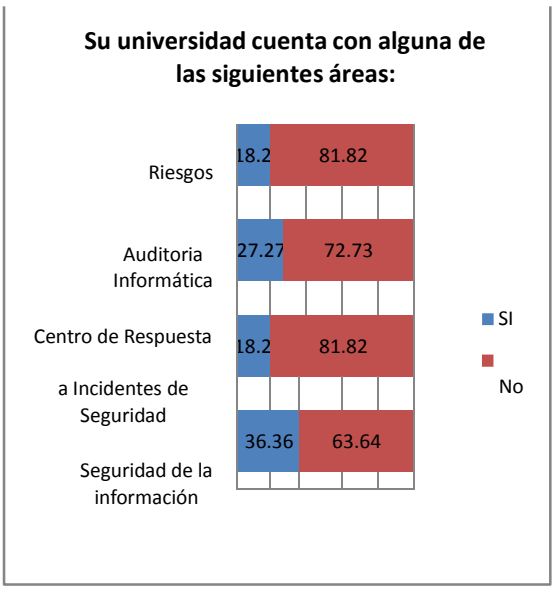
Para analizar este tema se lanzaron 3 preguntas respecto a:

- Políticas de Seguridad de la Información
- Plan de continuidad del negocio
- Áreas o Departamentos claves para la gestión de la Seguridad de la Información

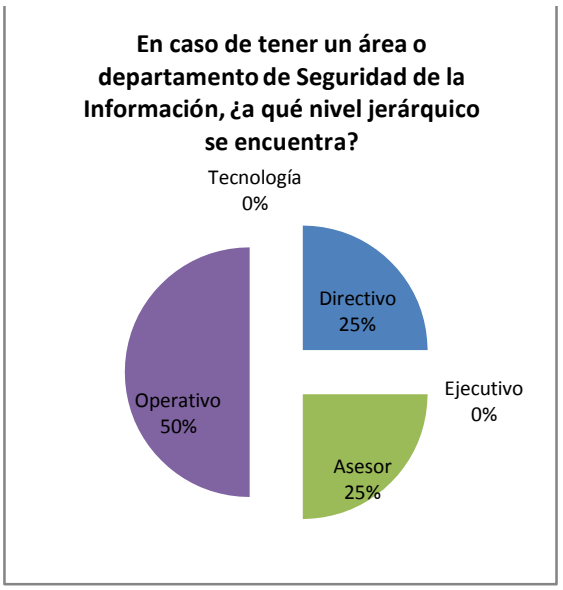
Como se puede observar más del 82% de las universidades que contestaron la encuesta han trabajado y están trabajando en Políticas o Normativas de Seguridad, por lo cual se puede sentir un interés por las instituciones por Gobernar la Seguridad de la Información.



En una empresa es importante un Plan de Continuidad del Negocio (BCP) y como se puede observar en las Universidades también, podemos observar que el 18% de la universidades tiene un BCP otro 18% lo tiene parcialmente lo cual suma un 36% de universidades que demuestran interés por tener un BCP.



Otro punto importante para conocer el estado de la Gestión de la Seguridad es saber si existen Área o Departamentos para esta gestión. Como podemos observar en la gráfica el 36,36% de las Universidades cuenta con un área de Seguridad de la información,

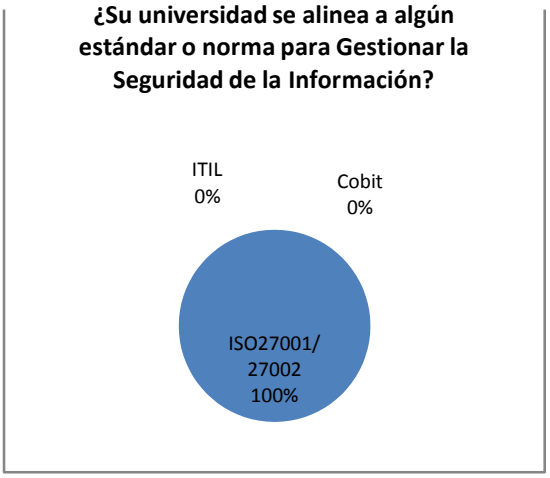


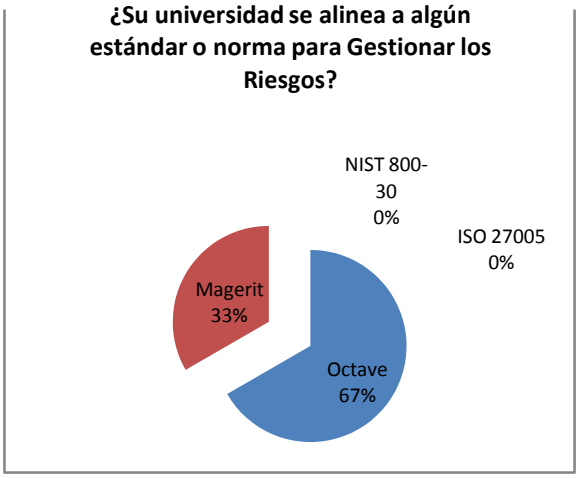
Para las Universidades que tienen un área de Seguridad de la información, se lanzó una pregunta para conocer en qué nivel jerárquico se encuentra dicha área y se observó que el 50% está en un nivel Operativo con un 50% y el resto se reparte entre

un 18,2% un Centro de Respuesta a Incidentes de Seguridad, 27,27% un área de Auditoria Informática y un 18,2% una área de Riesgos

nivel Directivo con un 25% y a nivel Asesor a un 25%.

Es importante poder recalcar que para el Área de Seguridad de la Información tenga fuerza en la organización debería estar en un nivel de Asesor o Directivo, por lo cual se ve necesario trabajar en las Universidades miembros para que esta área pueda tomar la importancia que requiere.



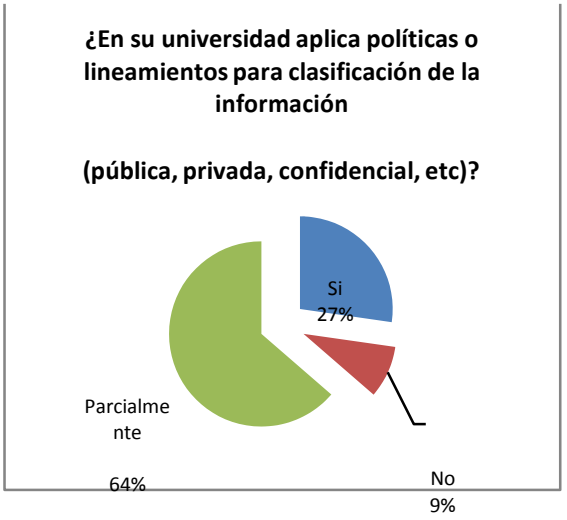


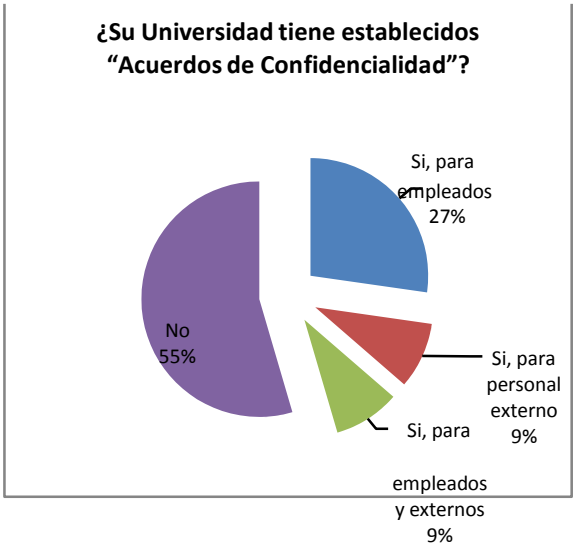
De las Universidades que tienen un área de Seguridad de la Información se preguntó si se alinean a algún estándar o normativa para la Gestión de la Seguridad de la Información y todas contestaron que utilizan la ISO 27001/27002. Así mismo para las universidades que tiene un Área de Riesgos se preguntó si se alinean a algún estándar o norma en esta área y se obtuvo que el 67% utilizan Octave y un 33% Magerit.

CONTROLES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Otro punto que se evaluó son los controles de seguridad general y que se han visto como importantes y básicos para la Gestión de la Seguridad, como son:

- Clasificación de la Información
- Acuerdos de Confidencialidad
- Definición de Roles y privilegios en las aplicaciones
- Concientización y Difusión de la Seguridad de la Información



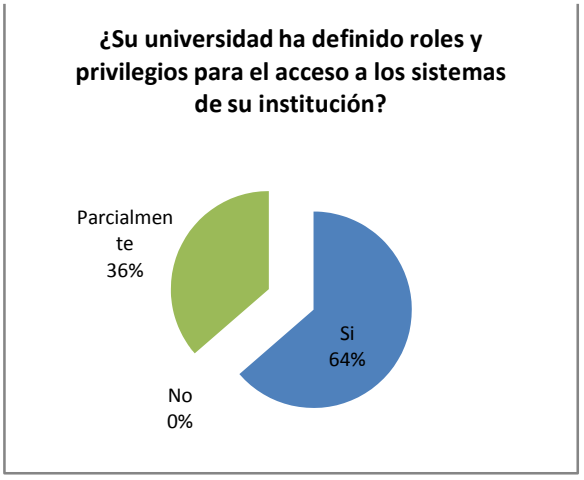


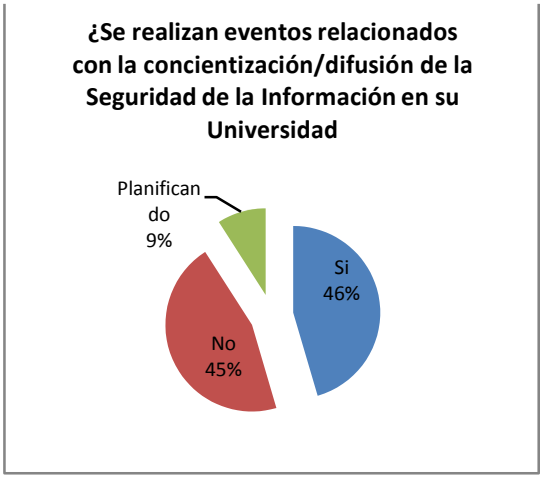
Dentro de la Gestión de la Seguridad es importante definir qué información es pública, privada, confidencial, etc., porque en base a ellos se establece los control de seguridad a ser implementados para su protección.

De la información proporcionada en la encuesta, se puede observar que la mayoría de las Universidades tiene conciencia de la importancia de este control, ya que un 27% de las Universidades tienen clasificada su información, el 67% la tienen parcialmente y un 9% no tiene clasificada.

Un Acuerdo de Confidencialidad es importante en una organización ya que se permite que las personas y externos que trabajan con la organización tomen conciencia del valor de la información y así evitar posibles fugas de información.

De lo que se pudo observar en la encuesta existe un 55% que no aplica acuerdos de confidencialidad, un 27% que si aplica acuerdos de confidencialidad a sus empleados, un 9% aplica acuerdos de confidencialidad a personal externo y el 9% aplica acuerdos de confidencialidad con sus empleados y personal externo. Por lo cual se ve conveniente trabajar en las universidades sobre este punto y fortalecerlo, ya que es bajo el nivel de implementación de este control en las Universidades.





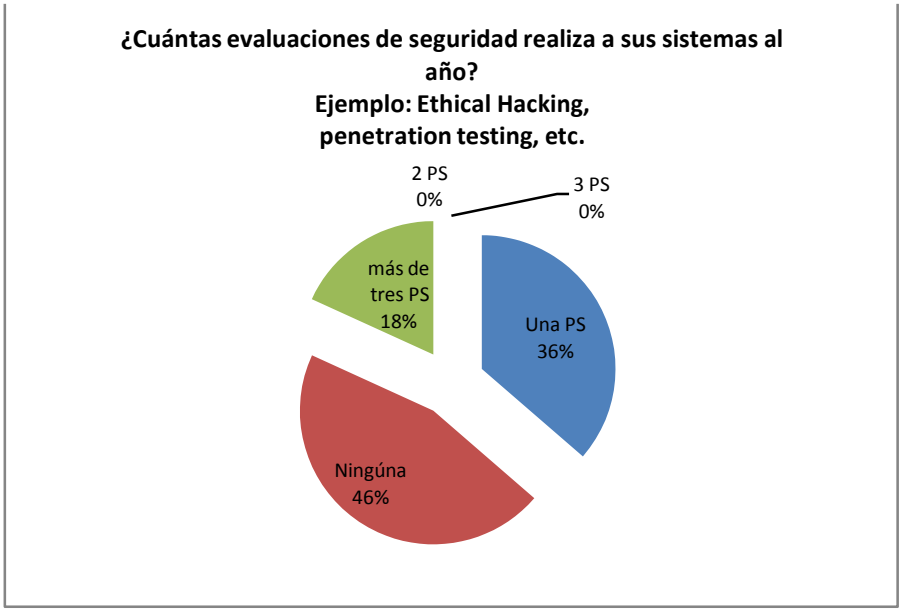
Dentro de la Gestión de Acceso se tiene un control importante para proteger la información y es que la organización defina los roles y privilegios que van a tener sus usuarios dentro del sistemas. De lo observado en las respuestas todas las universidades han y están trabajando sobre este control, ya que se observa que el 64% tiene definido los roles y privilegios en sus sistemas y el resto, un 36%, lo tiene parcialmente.

Se dice que la cadena de seguridad se rompe por el eslabón más débil y se ha catalogado al usuario final con este eslabón débil, por lo cual era necesario conocer que es lo que las Universidades están haciendo por concientizar a sus usuarios. De los datos recolectados en la encuesta podemos ver que un 46% está trabajando por concientizar a sus usuarios, las actividades se están ejecutando son: Eventos de Seguridad, mailing con tips de Seguridad, difusión de políticas de seguridad, reuniones de concientización y mensajes en TV cerrada; un 9% está organizándose y un 45% no realizan ningún tipo de activada de concientización y difusión de la Seguridad de la Información.

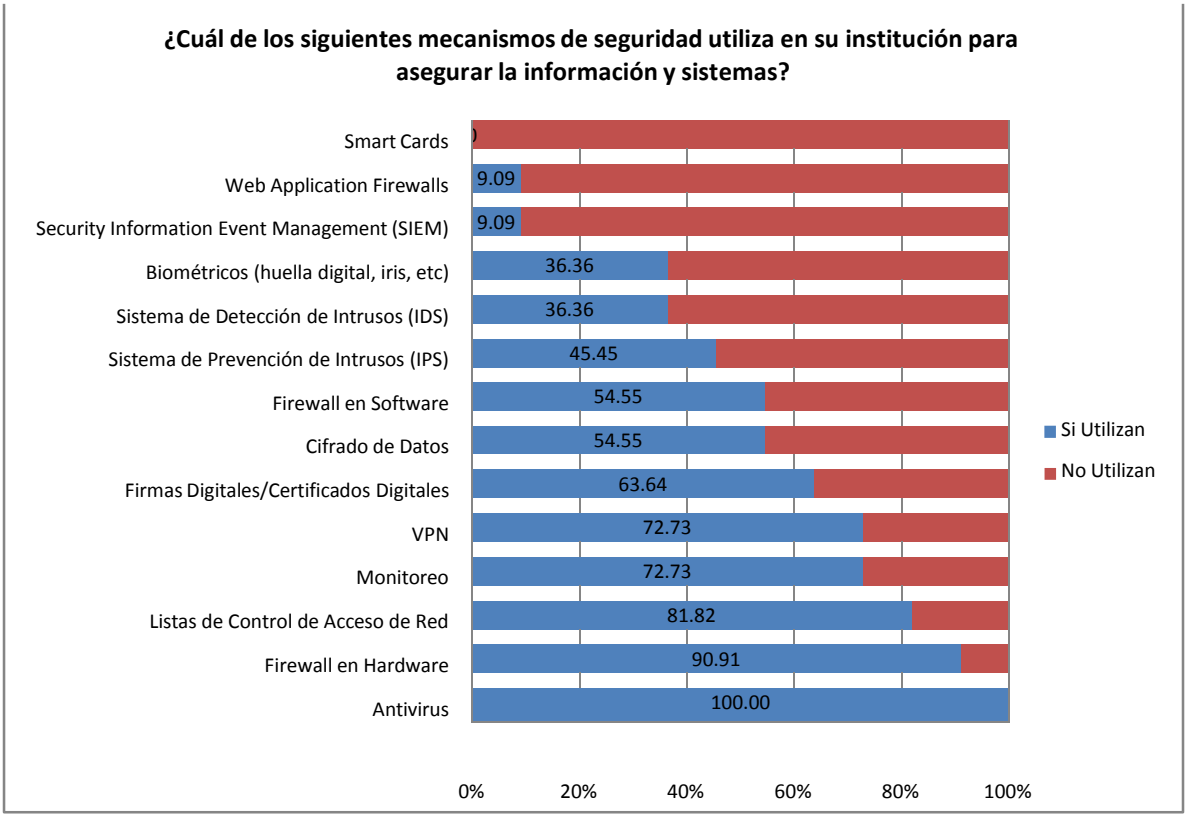
CONTROLES DE SEGURIDAD TÉCNILÓGICOS

Para este punto los temas a evaluar fueron:

- Evaluaciones de Seguridad
- Mecanismos tecnológicos de Seguridad implementados



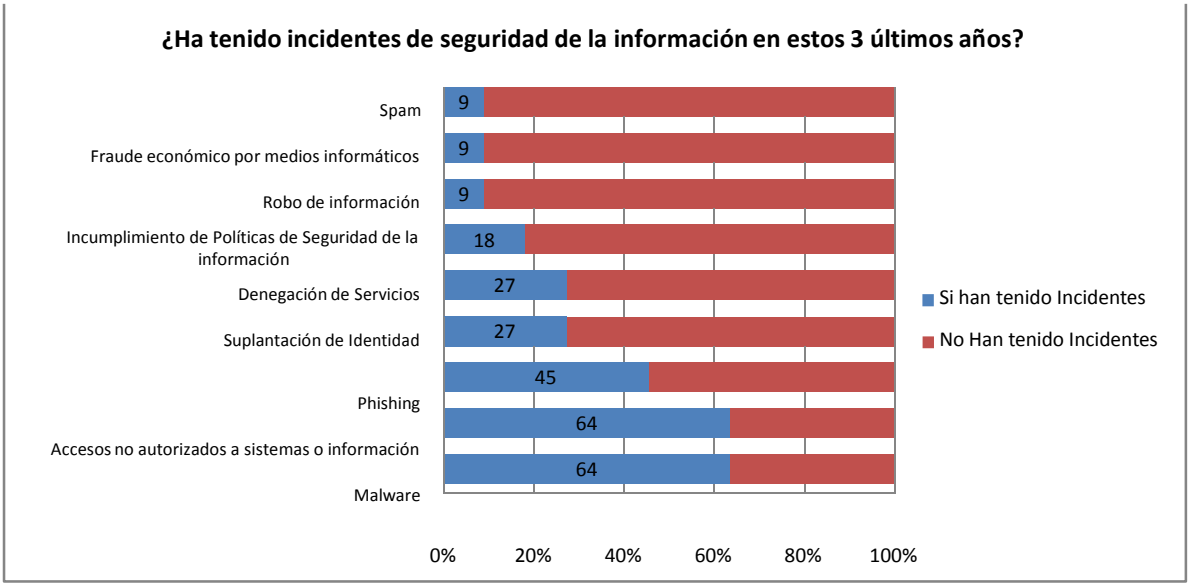
Debido a que las vulnerabilidades son descubiertas a cada momento es importante para la seguridad de un sistema realizar revisiones de seguridad periódicamente, por lo cual se lanzó una pregunta respecto a ello, para conocer cuantas revisiones de seguridad al año realizan a sus sistemas. Los resultados fueron que un 36% al menos hace una revisión al año, el 18% más de tres veces al año y un 46% no hace revisiones de seguridad a sus sistemas.



Para esta pregunta se dio a elegir 14 posibles mecanismos que pudieran utilizar las Universidades como protección, de los cuales se observó que los 3 más utilizados son el Antivirus con un 100% de utilización, luego un Firewall en Hardware con un 90,91% y las Listas de Control de Acceso de Red con un 81,82%.

INCIDENTES DE SEGURIDAD

Para está encuesta era indispensable conocer qué tipo de incidentes de seguridad han tenido las Universidades en los 3 últimos años, los resultados fueron los siguientes.



Los tres principales incidentes que ha tenido la mayoría de las universidades son: Malware con un 64%, Accesos no autorizados con un 64% y Phishing con un 45%.

CONCLUSIONES Y RECOMENDACIONES

- El 37,97% de las Universidades miembros de CEDIA colaboraron con la contestación de la encuesta denominada "1° ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN EN UNIVERSIDADES ECUATORIANAS MIEMBROS DE CEDIA"
- Con esta encuesta se ha observado que la mayoría de las Universidades están trabajando en el fortalecimiento de la Gestión de la Seguridad de la Información.
- Se ha observado que son pocas universidades (18%) que tiene asignado un presupuesto exclusivo para que sea utilizado en la Gestión de la Seguridad.
- Más del 50% de las área de seguridad que existen en las Universidades se encuentran a un nivel operativo, por lo cual se debería trabajar para que esté a un nivel asesor o director, para que los controles que se definan desde esta área tenga el respaldo y la fuerza dentro de la organización.
- Todas las Universidades aseguraron haber tenido un incidente de seguridad en los 3 últimos años, los 3 tipos de incidentes más concurrentes entre las universidades son: Malware (64%), Acceso no autorizado (64%) y Phishing (45%).
- Entre los puntos que se deben fortalecer en la Gestión de la Seguridad, ya que se tiene un trabajo mejor del 50% en las Universidades son:
    - Asignación de un presupuesto exclusivo
    - Plan de Continuidad del Negocio

- Creación de áreas de Seguridad de la Información en cada Universidades miembro.
- Concientización/difusión de la Seguridad de la Información a los usuarios finales.
- Revisiones de Seguridad a los Sistemas
- Acuerdos de confidencialidad

- Se debe fortalecer las acciones que han y están trabajando en algunas Universidades para la Gestión de la Seguridad de la Información e incentivar a otras Universidades que aun no han visto a la Gestión de la Seguridad como algo importante dentro la su organización.
- Se recomienda realizar un solo fuerzo en algunos puntos comunes y que se pueden compartir entre los miembros de CEDIA para la Gestión de la Seguridad como son: campañas de concientización a usuarios finales, capacitaciones de Seguridad, intercambio información para el manejo de incidentes.
- Al ser Universidades e interesar la investigación, se debe fomentar las iniciativas de investigación sobre temas de Seguridad de la Información.

3. Oficio I al Ing. Milton Palacios – Director UTI.

UNIVERSIDAD NACIONAL DE LOJA

OFICIO-CIS-UNL

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

Of. N° 472 CIS-AEIRNNR-UNL
Loja, 31 de octubre de 2013

Señor Ingeniero
Milton Palacios
DIRECTOR DE LA UNIDAD DE TELECOMUNICACIONES DE LA UNL.
Ciudad

De mi consideración:

Mediante el presente me dirijo a Usted para solicitarle de la manera más comedida, se le de las facilidades necesarias al Sr. Franklin Mauricio Vega Hidalgo portadora de la C.I.0705375178, egresado de la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, realice una encuesta a la persona encargada de Redes de la UTI. con la finalidad de que la información obtenida ayude al desarrollo de su proyecto titulado "**MODELO DE CONFIANZA PARA HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN ENTORNOS UNIVERSITARIOS**".

Por la atención que se digne dar a la presente me suscribo de usted.

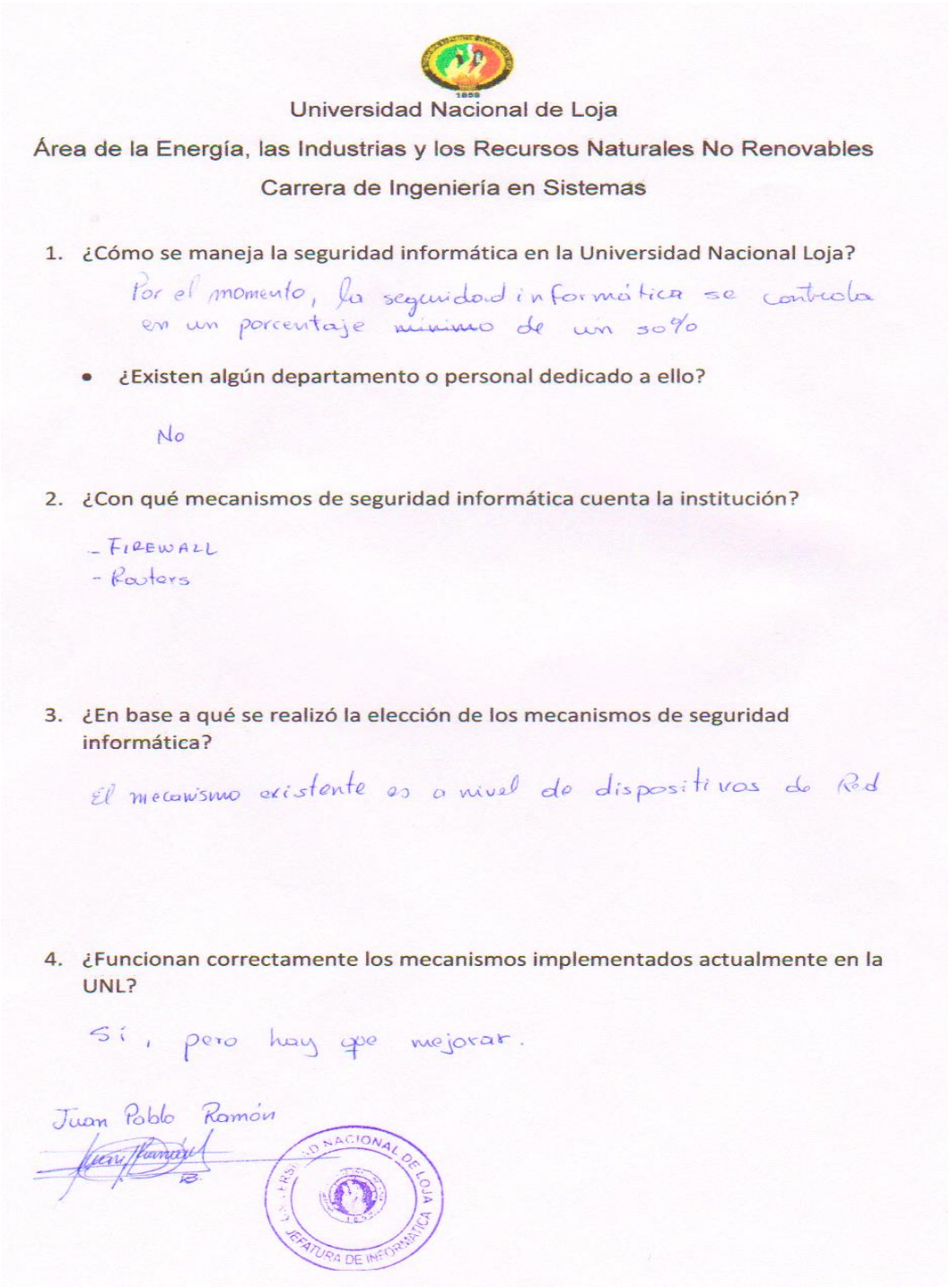
Atentamente,

Ing. Hernán Leonardo Torres Carrión M.Sc.
COORDINADOR DE LA CARRERA DE INGENIERÍA EN SISTEMAS.

c.c archivo
Elisa Orellana

Figura 27: Anexo 3- Oficio I a Director UTI-UNL.

4. **Primera Entrevista/Encuesta al Ing. Juan Pablo Ramón – Encargado del Área de Redes.**



Universidad Nacional de Loja

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

Carrera de Ingeniería en Sistemas

1. ¿Cómo se maneja la seguridad informática en la Universidad Nacional Loja?

   Por el momento, la seguridad informática se controla en un porcentaje mínimo de un 30%

   - ¿Existen algún departamento o personal dedicado a ello?

     No

2. ¿Con qué mecanismos de seguridad informática cuenta la institución?

   - FIREWALL
   - Routers

3. ¿En base a qué se realizó la elección de los mecanismos de seguridad informática?

   El mecanismo existente es a nivel de dispositivos de Red

4. ¿Funcionan correctamente los mecanismos implementados actualmente en la UNL?

   Si, pero hay que mejorar.

Juan Pablo Ramón

UNIVERSIDAD NACIONAL DE LOJA JEFATURA DE INFORMÁTICA

Figura 28: Anexo 4- Entrevista I al Encargado Dpto. Redes de la UTI-UNL.

5. Oficio II al Ing. Milton Palacios – Director UTI

UNIVERSIDAD NACIONAL DE LOJA

1859

OFICIO-CIS-UNL

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

Of. N° 054 CIS-AEIRNNR-UNL
Loja, 23 de enero de 2014

Señor Ingeniero
Milton Palacios
DIRECTOR DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN
Ciudad.

De mi consideración:

Mediante el presente me dirijo a usted, con la finalidad de solicitarle de la manera más comedida se sirva dar las facilidades necesarias para que el Sr. Franklin Mauricio Vega Hidalgo, egresado de la Carrera de Ingeniería en Sistemas pueda recabar información relacionada con uno de los objetivos aprobados de su proyecto "**MODELO DE CONFIANZA PARA HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN ENTORNOS UNIVERSITARIOS**".

Por la atención que se digne dar a la presente, me suscribo de usted.

Atentamente,

UNIVERSIDAD NACIONAL DE LOJA
CARRERA DE INGENIERÍA EN SISTEMAS
Área de la Energía, las Industrias y los Recursos Naturales no Renovables
1859
COORDINACIÓN

Ing. Hernán Leonardo Torres Carrión, Mg. Sc.
COORDINADOR DE LA CARRERA DE INGENIERÍA EN SISTEMAS.

C.C. Archivo.
Elisa Orellana

Figura 29: Anexo 5- Oficio II a Director UTI-UNL.

6. Segunda Entrevista/Encuesta en el ámbito de Seguridad al Ing. Juan Pablo Ramón - Encargado del Área de Redes de la UTI.

Universidad Nacional de Loja
Área de la Energía, las Industrias y los Recursos Naturales No Renovables
Carrera de Ingeniería en Sistemas

Como estudiante Investigador de la Carrera de Ingeniería en Sistemas y de la Universidad Nacional de Loja, con el fin de conocer la realidad de la institución y tener sólidas bases para el desarrollo del Trabajo de Titulación, denominado: **"Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios"** se solicita a Ud.(s) de la manera más respetuosa responder a las siguientes preguntas que de una u otra forma ayudará a fomentar la cultura de la seguridad de la información dentro de la institución.

1. **¿La UTI cuenta con un Departamento dedicado a la seguridad de la información?**
   - ¿Por qué no se ha creado o no se destina personal para este campo?

2. **¿La UTI cuenta actualmente con políticas de seguridad de la información?**
   - ¿Por qué no se ha promovido su creación?
   - O ¿Qué áreas cubre estas políticas?

3. **¿Cuáles fueron las razones para escoger los mecanismos (Firewall, Router) con los que cuenta actualmente la institución?**
   - Ofertas de Proveedores
   - Análisis de las herramientas, etc.

4. **¿Poseen algún tipo de Plan de continuidad del Negocio ante el fallo de las herramientas implementadas?**
   - ¿Cuál es el plan de contingencia para la continuidad del negocio?

5. **¿En qué área se palpa mayoritariamente la seguridad de la información (Software-Hardware)?**
   - ¿Cómo se ha implementado la seguridad en estas áreas?

6. **¿Existe la definición de Roles y Privilegios dentro de la UTI?**
   - ¿Bajo qué criterios se han planteado estos roles y privilegios?

7. **¿Realizan algún tipo de prueba o test anualmente para verificar la seguridad de la información?**
   - ¿En qué consiste la prueba o test?
   - O ¿Por qué no se realiza alguna prueba de monitorización?

8. **La institución ha sido víctima de incidentes de seguridad. ¿De qué tipo?**
   - ¿A qué sistema afectó este ataque informático?

9. **¿Promueven la concientización a los miembros de la UNL en cuanto a la Seguridad de la Información?**
   - ¿Estarían dispuestos a ser partícipes de proyectos que fomenten la creación una cultura de seguridad de la información?

10. **¿Conoce de herramientas de seguridad informática implementadas mayoritariamente en entornos universitarios?**
    - ¿Cuál es su criterio, previa a su implementación?

7. Oficio al Ing. Carlos Córdova - Director De La Unidad De Gestión De Tecnologías De La Información De La UTPL.

UNIVERSIDAD NACIONAL DE LOJA

OFICIO-CIS-UNL

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

Of. N° 083 CIS-AEIRNNR-UNL
Loja, 06 de febrero de 2014

Señor Ingeniero.
Carlos Córdova
DIRECTOR DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UTPL.
Ciudad

De mi consideración:

Con un cordial saludo me dirijo a usted, con la finalidad de solicítale de la manera más comedida se sirva dar las facilidades para que el señor Franklin Mauricio Vega Hidalgo, egresado de la Carrera de Ingeniería en Sistemas, obtenga información sobre los criterios tomados en cuenta a la hora de implementar Herramientas de Seguridad Informática en la unidad que se encuentra bajo su cargo; esta información servirá para el desarrollo de su trabajo de titulación cuyo tema es "**MODELO DE CONFIANZA PARA HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN ENTORNOS UNIVERSITARIOS**"

Por la atención que se digne dar al presente, me suscribo de usted.

Atentamente,

UNIVERSIDAD NACIONAL DE LOJA CARRERA DE INGENIERÍA EN SISTEMAS COORDINACIÓN

Ing. Hernán Leonardo Torres Carrión M.Sc.
COORDINADOR DE LA CARRERA DE INGENIERÍA EN SISTEMAS.

C.c. Archivo,
Elisa Orellana

OK Recibido 10/02/2014

Figura 30: Anexo 7- Oficio al Ing. Carlos Córdova Director de Unidad de Gestión de Tecnologías de la Información - UTPL.

8. Certificación de entrevista a Ing. Julia Pineda – Líder de Seguridad de la Información de la UTPL.

Universidad Nacional de Loja
Área de la Energía, las Industrias y los Recursos Naturales No Renovables
Carrera de Ingeniería en Sistemas

Como estudiante Investigador de la Carrera de Ingeniería en Sistemas y de la Universidad Nacional de Loja, con el fin de conocer la realidad de las instituciones locales que cuentan con bases sólidas en lo que respecta a seguridad de la información, se ha solicitado mediante el Ing. Carlos Córdova, Director De La Unidad De Gestión De Tecnologías De La Información De La UTPL, una entrevista con la Ing. Julia Pineda, Líder de Seguridad de la Información de la institución, con el fin de conocer más, acerca de los temas que actualmente están llevando a cabo dentro de la institución, en el área a su cargo. Dicha información será de gran importancia para fundamentación de mi Trabajo de Titulación, denominado: **"Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios".** Tras la entrevista se ha podido tratar diversos temas puntuales, así como temas a fines a los mismos. A continuación se hace mención de los principales temas tratados:

- Implementación y Mejoramiento de Controles de Seguridad dentro de la Institución.
- Cumplimiento de Políticas de Seguridad y Mejoramiento de las mismas.
- Protección en Equipos Finales.
- Criterios para Elegir Mecanismos de Seguridad.
- Proyectos en Desarrollo en el Campo de Seguridad de la Información.
- Personal Encargado del Área de Seguridad, entre otros.

Ing. Julia Pineda
LÍDER SEGURIDAD DE
LA INFORMACIÓN UTPL

Egdo. Franklin Vega Hidalgo
TESISTA CIS-UNL

Figura 31: Anexo 8- Certificación de Entrevista a la Ing. Julia Pineda-Líder de Seguridad de Información-UTPL.

9. Oficio al Ing. Alfonso León Goyburu-Gerente de Tecnologías y Sistemas de Información de la ESPOL.

UNIVERSIDAD NACIONAL DE LOJA

OFICIO-CIS-UNL

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

ESPOL
GERENCIA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN
07 OCT 2014
RECIBIDO
Por:

Of. N° 885 CIS-AEIRNNR-UNL
Loja, 26 de septiembre de 2014

Señor Ingeniero.
Alfonso León Goyburu
GERENTE DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN DE LA ESPOL.
Guayaquil.

De mi consideración:

Con un cordial saludo me dirijo a usted, con la finalidad de solicítale de la manera más comedida se sirva dar las facilidades para que el señor **Franklin Mauricio Vega Hidalgo**, con cédula Nº 0705375178, egresado de la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, obtenga información sobre los criterios tomados en cuenta a la hora de implementar Herramientas de Seguridad Informática en la unidad que se encuentra bajo su cargo; esta información servirá para el desarrollo de su trabajo de titulación cuyo tema es "**MODELO DE CONFIANZA PARA HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN ENTORNOS UNIVERSITARIOS**".

Por la atención que se digne dar al presente, me suscribo de usted.

Atentamente,

Ing. Luis Roberto Jácome Galarza M.Sc.
COORDINADOR (e) DE LA CARRERA DE INGENIERÍA EN SISTEMAS.

C.c. Archivo.
Elisa Orellana

Figura 32: Anexo 9- Oficio al Ing. Alfonso León Goyburu-Gerente de Tecnologías y Sistemas de Información de la ESPOL.

10. Oficio a la Ing. Johanna Guerrero Flores-Directora del Departamento de Sistemas y Telecomunicaciones de la Universidad Laica Vicente Rocafuerte.

UNIVERSIDAD NACIONAL DE LOJA

OFICIO-CIS-UNL

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

Of. N° 886 CIS-AEIRNNR-UNL
Loja, 26 de septiembre de 2014

Ingeniera.
Johana Guerrero
GERENTE DEL DEPARTAMENTO DE SISTEMAS DE LA UNIVERSIDAD LAICA VICENTE ROCAFUERTE.
Guayaquil.

De mi consideración:

Con un cordial saludo me dirijo a usted, con la finalidad de solicítale de la manera más comedida se sirva dar las facilidades para que el señor **Franklin Mauricio Vega Hidalgo**, con cédula Nº 0705375178, egresado de la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, obtenga información sobre los criterios tomados en cuenta a la hora de implementar Herramientas de Seguridad Informática en la unidad que se encuentra bajo su cargo; esta información servirá para el desarrollo de su trabajo de titulación cuyo tema es "**MODELO DE CONFIANZA PARA HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN ENTORNOS UNIVERSITARIOS".**

Por la atención que se digne dar al presente, me suscribo de usted.

Atentamente,

Roberto Jácome

Ing. Luis Roberto Jácome Galarza M.Sc.
COORDINADOR (e) DE LA CARRERA DE INGENIERÍA EN SISTEMAS.

C.c. Archivo.
Elisa Orellana

11:41 am
08/10/2014

Figura 33: Anexo 10- Oficio a la Ing. Johanna Guerrero Flores-Directora del Departamento de Sistemas y Telecomunicaciones de la Universidad Laica Vicente Rocafuerte.

11. Oficio a la Ing. Betty Marlene Pachucho Hernández-Jefa del Departamento de Sistemas e Informática de la Universidad Técnica de Machala.

UNIVERSIDAD NACIONAL DE LOJA

OFICIO-CIS-UNL

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

Of. N° 887 CIS-AEIRNNR-UNL
Loja, 26 de septiembre de 2014

Ingeniera.
Betty Pachucho
JEFE (E) DEL DEPARTAMENTO DE INFORMÁTICA DE LA UNIVERSIDAD TÉCNICA DE MACHALA.
Machala.

De mi consideración:

Con un cordial saludo me dirijo a usted, con la finalidad de solicítale de la manera más comedida se sirva dar las facilidades para que el señor **Franklin Mauricio Vega Hidalgo**, con cédula Nº 0705375178, egresado de la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, obtenga información sobre los criterios tomados en cuenta a la hora de implementar Herramientas de Seguridad Informática en la unidad que se encuentra bajo su cargo; esta información servirá para el desarrollo de su trabajo de titulación cuyo tema es "**MODELO DE CONFIANZA PARA HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN ENTORNOS UNIVERSITARIOS".**

Por la atención que se digne dar al presente, me suscribo de usted.

Atentamente,

Ing. Luis Roberto Jácome Galarza M.Sc.
COORDINADOR (e) DE LA CARRERA DE INGENIERÍA EN SISTEMAS.

C.c. Archivo,
Elisa Orellana

UNIVERSIDAD TÉCNICA DE MACHALA
RECIBIDO
HORA
09:52 14 OCT 2014
DEPARTAMENTO DE INFORMÁTICA

Figura 34: Anexo 11- Oficio a la Ing. Betty Marlene Pachucho Hernández-Jefa del Departamento de Sistemas e Informática de la Universidad Técnica de Machala.

12. Certificación de Visita Técnica a la Unidad de Tecnologías y Sistemas de Información de la ESPOL.

www.espol.edu.ec

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
"Impulsando la Sociedad del Conocimiento"

A QUIEN INTERESE

Certifico que el **Sr. Franklin Mauricio Vega Hidalgo**, con C.I: 0705375178, Egresado de la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja; ha realizado la visita técnica en la unidad a mi cargo, con el fin de conocer la situación actual de nuestra universidad en el ámbito de Seguridad Informática y la toma de decisiones que conlleva esta importante área. Lo que le será de vital importancia en el desarrollo de su Trabajo de Titulación, denominado: **MODELO DE CONFIANZA PARA HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN ENTORNOS UNIVERSITARIOS**, de acuerdo a lo expresado por la parte interesada.

Es todo cuanto puedo certificar en honor a la verdad, el interesado puede hacer uso del presente certificado como mejor creyera conveniente.

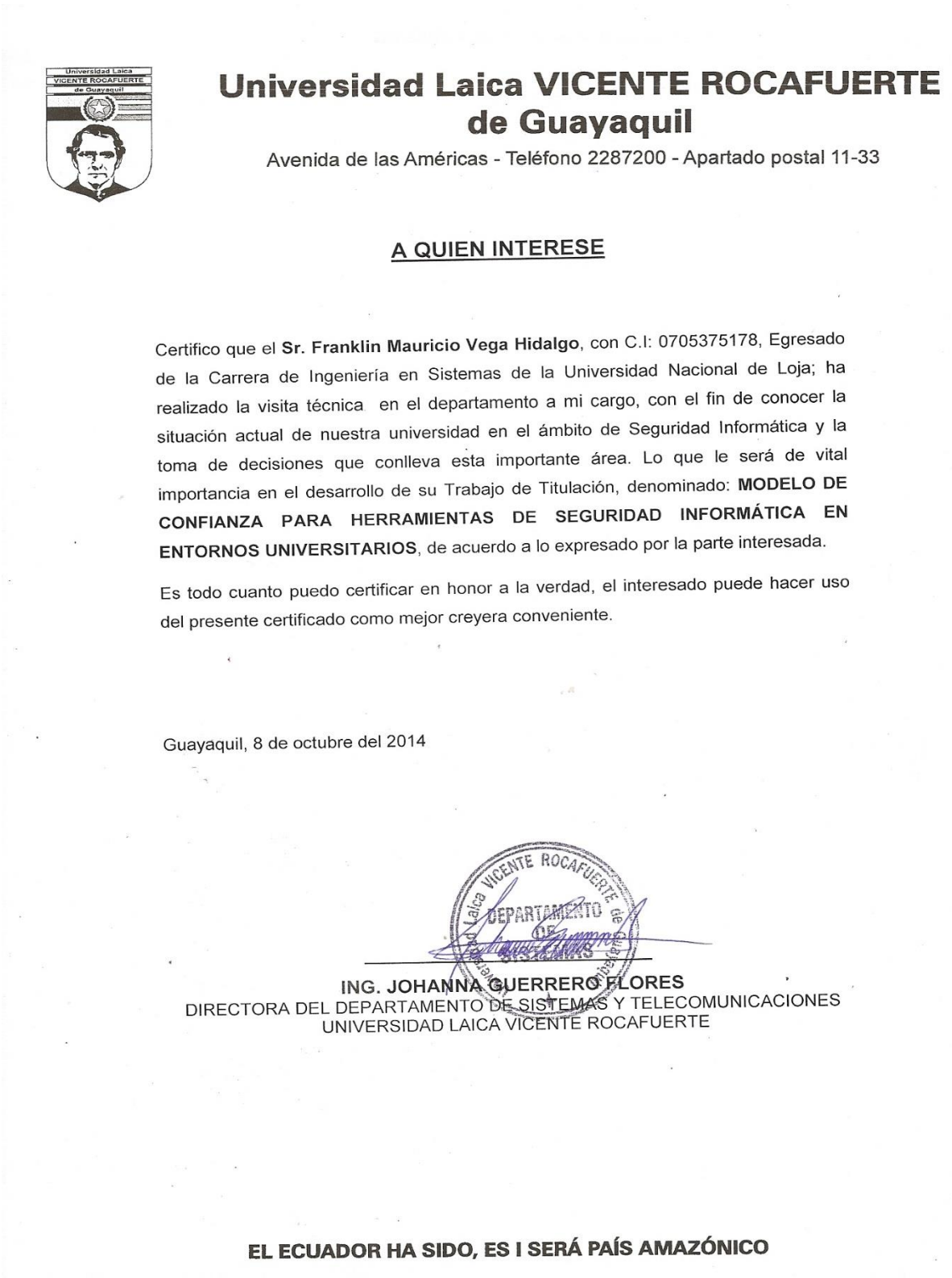
Guayaquil, 7 de octubre del 2014

ING. ALFONSO LEÓN GOYBURU
GERENTE DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN DE LA ESPOL

Guayaquil: *Campus "Gustavo Galindo V.", Km. 30.5 Vía Perimetral, contiguo a la Cdla. Santa Cecilia • Casilla: 09-01-5863*
Fax: (593-4) 2854629 • Teléfonos: 2269269 - 2850341 - 2851094 - 2854482 - 2854560 - 2854518 - 2854486 - 2854501
Campus "Las Peñas" Malecón 100 y Loja • Fax: (593-4) 2530283 • Teléfonos: 2530491 - 2530271
Quito: *Av. 6 de Diciembre N33-55 y Av. Eloy Alfaro, Edif. Torre Blanca, Piso 2 • Casilla: 17-01-1076 • Telefaxes: (593-2) 2521408 - 2561199 - 2235150 - 2527986 - 2550618*

Figura 35: Anexo 12- Certificación de Visita Técnica ESPOL

13. Certificación de Visita Técnica al Departamento de Sistemas y Telecomunicaciones de la Universidad Laica Vicente Rocafuerte.



Universidad Laica VICENTE ROCAFUERTE de Guayaquil

Avenida de las Américas - Teléfono 2287200 - Apartado postal 11-33

A QUIEN INTERESE

Certifico que el **Sr. Franklin Mauricio Vega Hidalgo**, con C.I: 0705375178, Egresado de la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja; ha realizado la visita técnica en el departamento a mi cargo, con el fin de conocer la situación actual de nuestra universidad en el ámbito de Seguridad Informática y la toma de decisiones que conlleva esta importante área. Lo que le será de vital importancia en el desarrollo de su Trabajo de Titulación, denominado: **MODELO DE CONFIANZA PARA HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN ENTORNOS UNIVERSITARIOS**, de acuerdo a lo expresado por la parte interesada.

Es todo cuanto puedo certificar en honor a la verdad, el interesado puede hacer uso del presente certificado como mejor creyera conveniente.

Guayaquil, 8 de octubre del 2014

Laica VICENTE ROCAFUERTE de Guayaquil DEPARTAMENTO DE SISTEMAS

ING. JOHANNA GUERRERO FLORES
DIRECTORA DEL DEPARTAMENTO DE SISTEMAS Y TELECOMUNICACIONES
UNIVERSIDAD LAICA VICENTE ROCAFUERTE

EL ECUADOR HA SIDO, ES I SERÁ PAÍS AMAZÓNICO

Figura 36: Anexo 13- Certificación de Visita Técnica Universidad Laica Vicente Rocafuerte

14. Certificación en Fundamentos de Seguridad obtenida en la "I Maratón de Certificaciones Tecnológicas" Mirosoft – Yachay.

CERTIPORT

Registro digital autenticado de certificaciones

17 de enero de 2014

Franklin Mauricio Vega Hidalgo

0993389471

072908284

593

Loja

fmvegah@unl.edu.ec

Este Registro Digital Certiport en tiempo real se obtiene de una base de datos global que rastrea y autentica los exámenes de certificación administrados por más de 12.000 centros de evaluación en todo el mundo.

MICROSOFT TECHNOLOGY ASSOCIATE

Microsoft Technology Associate

Certificaciones

Microsoft Technology Associate: Security Fundamentals — Otorgadas

Exámenes

98-367: MTA: Security Fundamentals — Aprobado — 17/01/2014

Administrado por: Universidad de Investigación de Tecnología Experimental YACHAY

Idioma: Spanish (Latin America)

*Si desea obtener información acerca de Certiport, visite **www.certiport.com**. Certiport es el proveedor líder de programas y servicios mundiales de certificación basados en el desempeño, diseñados para facilitar el éxito individual y un progreso de por vida gracias a la certificación.*

Figura 37: Anexo 14- Certificación Microsoft- Yachay.

15. Petición Entrevista/Reunión con el Ing. Milton Palacios para la Experimentación del Modelo Creado.

Petición de Entrevista Recibidos x

Franklin Mauricio Vega Hidalgo <fmvegah@unl.edu.ec> 25 de may.

para Milton

Buenas Tardes Ing. reciba un cordial saludo de parte de Franklin Vega Hidalgo, estudiante egresado de la Carrera de Ingeniería en Sistemas, el motivo del mensaje es por solicitarle, en una nueva ocasión, una entrevista con su persona para tratar temas relacionados con la fase de experimentación de mi trabajo de titulación: **"Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios",** ya que después de todo el proceso de desarrollo del modelo propuesto, me es necesario cumplir con la determinación de un escenario de aplicabilidad para el mismo.

Esperando una respuesta favorable a mi solicitud y deseándole éxitos en sus labores diarias, me suscribo.

Saludos

Milton Ricardo Palacios Morocho 26 de may.

para mí

Saludos puede serla reunión el día miércoles 28 de mayo, en la mañana.

El 25 de mayo de 2014, 16:27, Franklin Mauricio Vega Hidalgo <fmvegah@unl.edu.ec> escribió:

Figura 38: Anexo 15- Petición Entrevista/Reunión con Director de la UTI-UNL

16. Entrevista/Encuesta para determinar niveles de confianza en el modelo al Ing. Juan Pablo Ramón – Encargado del Área de Redes de la UTI.

Universidad Nacional de Loja
Área de la Energía, las Industrias y los Recursos Naturales No Renovables
Carrera de Ingeniería en Sistemas

Como estudiante Investigador de la Carrera de Ingeniería en Sistemas y de la Universidad Nacional de Loja me encuentro en el desarrollo de la fase de experimentación de mi Trabajo de Titulación, denominado: **"Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios"**, para lo cual me es importante conocer su criterio mediante una valoración del modelo propuesto en cada uno de los escenarios así como de los criterios que los componen.

a. Escenario 1:Herramienta Propietaria/Privativa

1. Permítase dar una valoración a cada criterio del modelo y en caso de faltar un criterio que crea conveniente, sugiéralo por favor.

CRITERIOS	PESO GENÉRICO	VALOR DE ACEPTACIÓN		
		Baja	Media	Alta
ASPECTO ECONÓMICO	**25%**			
Disponibilidad de Presupuesto	10%			o
Oferta de proveedores	5%		o	
Inversión retribuya con los beneficios obtenidos	10%		o	
ASPECTO REPUTACIÓN-CONFIABILIDAD	**15%**			
WOT (Web Of Trust): Reputación de los proveedores en la Web	5%		o	
Recomendaciones por otras instituciones educativas	10%		o	
ASPECTO TÉCNICO	**60%**			
Protección de Equipos de Networking	10%			o
Cumplimiento de las políticas de acceso y controles a los sistemas	15%			o
Espacio Físico y Lógico	5%		o	
Duración del soporte	10%		o	
Capacitación al personal	15%			o
Garantías	5%			o

Sugerencia respecto a los criterios:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

2. En base al escenario propuesto anteriormente ¿Con qué porcentaje total del modelo cree Ud. Que sería confiable la implementación de una herramienta de seguridad informática en entornos universitarios? ¿Porqué?

con un 90% sería confiable una vez realizada toda la evaluación de acuerdo a los requerimientos de las políticas y seguridad de la información que se mantenga en la institución

Juan Pablo Ramón

Figura 39: Anexo 16- Entrevista/Encuesta al Ing. Juan Pablo Ramón-Determinación Niveles de Confianza-Parte1

b. Escenario 2: Herramienta Libre/Gratuita

1. Permítase dar una valoración a cada criterio del modelo y en caso de faltar un criterio que crea conveniente, sugiéralo por favor.

CRITERIOS	PESO GENÉRICO	VALOR DE ACEPTACIÓN		
		Baja	Media	Alta
ASPECTO ECONÓMICO	**10%**			
Inversión retribuya con los beneficios obtenidos	10%		0	
ASPECTO REPUTACIÓN-CONFIABILIDAD	**30%**			
WOT (Web Of Trust): Reputación de los proveedores en la Web	20%			0
Recomendaciones por otras instituciones educativas	10%		0	
ASPECTO TÉCNICO	**60%**			
Protección de Equipos de Networking	15%			0
Cumplimiento de las políticas de acceso y controles a los sistemas	30%			0
Espacio Físico y Lógico	15%		0	

Sugerencia respecto a los criterios:

.....
.....
.....
.....
.....
.....

2. En base al escenario propuesto anteriormente ¿Con qué porcentaje total del modelo cree Ud. Que sería confiable la implementación de una herramienta de seguridad informática en entornos universitarios? ¿Porqué?

Con un 80%
.....
.....
.....

Figura 40: Anexo 16- Entrevista/Encuesta al Ing. Juan Pablo Ramón-Determinación Niveles de Confianza-Parte2

c. Escenario 3: Proyectos Estudiantiles

1. Permítase dar una valoración a cada criterio del modelo y en caso de faltar un criterio que crea conveniente, sugiéralo por favor.

CRITERIOS	PESO GENÉRICO	VALOR DE ACEPTACIÓN		
		Alta	Media	Baja
ASPECTO ECONÓMICO	**25%**			
Disponibilidad de Presupuesto	10%			
Inversión retribuya con los beneficios obtenidos	15%			
ASPECTO REPUTACIÓN-CONFIABILIDAD	**25%**			
WOT (Web Of Trust): Reputación de los proveedores en la Web	15%			
Recomendaciones por otras instituciones educativas	10%			
ASPECTO TÉCNICO	**60%**			
Protección de Equipos de Networking	15%			
Cumplimiento de las políticas de acceso y controles a los sistemas	20%			
Espacio Físico y Lógico	10%			
Duración de Licencias	15%			

Sugerencia respecto a los criterios:

.....
.....
.....
.....
.....
.....

2. En base al escenario propuesto anteriormente ¿Con qué porcentaje total del modelo cree Ud. Que sería confiable la implementación de una herramienta de seguridad informática en entornos universitarios? ¿Porqué?

Con un 85% sería confiable su implementación debido a los diferentes criterios que se involucran al momento del desarrollo.

Figura 41: Anexo 16- Entrevista/Encuesta al Ing. Juan Pablo Ramón- Determinación Niveles de Confianza-Parte3

17. Entrevista/Encuesta para determinar niveles de confianza en el modelo a la Ing. Nohelia Bustamante – Encargada del Área de Telecomunicaciones de la UTI.

Universidad Nacional de Loja
Área de la Energía, las Industrias y los Recursos Naturales No Renovables
Carrera de Ingeniería en Sistemas

Como estudiante Investigador de la Carrera de Ingeniería en Sistemas y de la Universidad Nacional de Loja me encuentro en el desarrollo de la fase de experimentación de mi Trabajo de Titulación, denominado: **"Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios"**, para lo cual me es importante conocer su criterio mediante una valoración del modelo propuesto en cada uno de los escenarios así como de los criterios que los componen.

a. Escenario 1:Herramienta Propietaria/Privativa

1. Permítase dar una valoración a cada criterio del modelo y en caso de faltar un criterio que crea conveniente, sugiéralo por favor.

CRITERIOS	PESO GENÉRICO	VALOR DE ACEPTACIÓN		
		Baja	Media	Alta
ASPECTO ECONÓMICO	**25%**		X	
Disponibilidad de Presupuesto	10%	X		
Oferta de proveedores	5%		X	
Inversión retribuya con los beneficios obtenidos	10%		X	
ASPECTO REPUTACIÓN-CONFIABILIDAD	**15%**		X	
WOT (Web Of Trust): Reputación de los proveedores en la Web	5%		X	
Recomendaciones por otras instituciones educativas	10%	X		
ASPECTO TÉCNICO	**60%**		X	
Protección de Equipos de Networking	10%		X	
Cumplimiento de las políticas de acceso y controles a los sistemas	15%		X	
Espacio Físico y Lógico	5%	X		
Duración del soporte	10%		X	
Capacitación al personal	15%	X		
Garantías	5%		X	

Sugerencia respecto a los criterios:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

2. En base al escenario propuesto anteriormente ¿Con qué porcentaje total del modelo cree Ud. Que sería confiable la implementación de una herramienta de seguridad informática en entornos universitarios? ¿Porqué?

Una herramienta de seguridad debe cumplir mínimo con un 90% de seguridad

Ing. Nohelia Bustamante.
Telecomunicaciones

Figura 42: Anexo 17- Entrevista/Encuesta a la Ing. Nohelia Bustamante-Determinación Niveles de Confianza-Parte1

b. Escenario 2: Herramienta Libre/Gratuita

1. Permítase dar una valoración a cada criterio del modelo y en caso de faltar un criterio que crea conveniente, sugiéralo por favor.

CRITERIOS	PESO GENÉRICO	VALOR DE ACEPTACIÓN		
		Baja	Media	Alta
ASPECTO ECONÓMICO	**10%**		X	
Inversión retribuya con los beneficios obtenidos	10%		X	
ASPECTO REPUTACIÓN-CONFIABILIDAD	**30%**		X	
WOT (Web Of Trust): Reputación de los proveedores en la Web	20%	X		
Recomendaciones por otras instituciones educativas	10%		X	
ASPECTO TÉCNICO	**60%**			X
Protección de Equipos de Networking	15%		X	
Cumplimiento de las políticas de acceso y controles a los sistemas	30%		X	
Espacio Físico y Lógico	15%		X	

Sugerencia respecto a los criterios:

.....
.....
.....
.....
.....
.....

2. En base al escenario propuesto anteriormente ¿Con qué porcentaje total del modelo cree Ud. Que sería confiable la implementación de una herramienta de seguridad informática en entornos universitarios? ¿Porqué?

Software libre en un entorno universitario es economico y brinda casi los mismos prestaciones esto con un 90 %.....

Figura 43: Anexo 17- Entrevista/Encuesta a la Ing. Nohelia Bustamante-Determinación Niveles de Confianza-Parte2

c. Escenario 3: Proyectos Estudiantiles

1. Permítase dar una valoración a cada criterio del modelo y en caso de faltar un criterio que crea conveniente, sugiéralo por favor.

CRITERIOS	PESO GENÉRICO	VALOR DE ACEPTACIÓN		
		Alta	Media	Baja
ASPECTO ECONÓMICO	**25%**			
Disponibilidad de Presupuesto	10%		X	
Inversión retribuya con los beneficios obtenidos	15%		X	
ASPECTO REPUTACIÓN-CONFIABILIDAD	**25%**		X	
WOT (Web Of Trust): Reputación de los proveedores en la Web	15%	X		
Recomendaciones por otras instituciones educativas	10%		X	
ASPECTO TÉCNICO	**60%**		X	
Protección de Equipos de Networking	15%		X	
Cumplimiento de las políticas de acceso y controles a los sistemas	20%	X		
Espacio Físico y Lógico	10%		X	
Duración de Licencias	15%		X	

Sugerencia respecto a los criterios:

Capacitación estudiante

2. En base al escenario propuesto anteriormente ¿Con qué porcentaje total del modelo cree Ud. Que sería confiable la implementación de una herramienta de seguridad informática en entornos universitarios? ¿Porqué?

Con un 80%.

Figura 44 Anexo 17- Entrevista/Encuesta a la Ing. Nohelia Bustamante-Determinación Niveles de Confianza-Parte3

18. Entrevista/Encuesta para determinar niveles de confianza en el modelo al Ing. Milton Labanda – Encargado del Área de Desarrollo de Software de la UTI.

Universidad Nacional de Loja
Área de la Energía, las Industrias y los Recursos Naturales No Renovables
Carrera de Ingeniería en Sistemas

Como estudiante Investigador de la Carrera de Ingeniería en Sistemas y de la Universidad Nacional de Loja me encuentro en el desarrollo de la fase de experimentación de mi Trabajo de Titulación, denominado: **"Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios"**, para lo cual me es importante conocer su criterio mediante una valoración del modelo propuesto en cada uno de los escenarios así como de los criterios que los componen.

a. Escenario 1:Herramienta Propietaria/Privativa

1. Permítase dar una valoración a cada criterio del modelo y en caso de faltar un criterio que crea conveniente, sugiéralo por favor.

CRITERIOS	PESO GENÉRICO	VALOR DE ACEPTACIÓN		
		Baja	Media	Alta
ASPECTO ECONÓMICO	**25%**			X
Disponibilidad de Presupuesto	10%			X
Oferta de proveedores	5%			
Inversión retribuya con los beneficios obtenidos	10%			X
ASPECTO REPUTACIÓN-CONFIABILIDAD	**15%**		X	
WOT (Web Of Trust): Reputación de los proveedores en la Web	5%	X		
Recomendaciones por otras instituciones educativas	10%		X	
ASPECTO TÉCNICO	**60%**			X
Protección de Equipos de Networking	10%		X	
Cumplimiento de las políticas de acceso y controles a los sistemas	15%			X
Espacio Físico y Lógico	5%		X	
Duración del soporte	10%			X
Capacitación al personal	15%			X
Garantías	5%			X

Sugerencia respecto a los criterios:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

2. En base al escenario propuesto anteriormente ¿Con qué porcentaje total del modelo cree Ud. Que sería confiable la implementación de una herramienta de seguridad informática en entornos universitarios? ¿Porqué?

95%
.....
.....
.....

Milton Labanda.

Figura 45: Anexo 18- Entrevista/Encuesta al Ing. Milton Labanda-Determinación Niveles de Confianza-Parte1

b. Escenario 2: Herramienta Libre/Gratuita

1. Permítase dar una valoración a cada criterio del modelo y en caso de faltar un criterio que crea conveniente, sugiéralo por favor.

CRITERIOS	PESO GENÉRICO	VALOR DE ACEPTACIÓN		
		Baja	Media	Alta
ASPECTO ECONÓMICO	**10%**		X	
Inversión retribuya con los beneficios obtenidos	10%			X
ASPECTO REPUTACIÓN-CONFIABILIDAD	**30%**			X
WOT (Web Of Trust): Reputación de los proveedores en la Web	20%			X
Recomendaciones por otras instituciones educativas	10%		X	
ASPECTO TÉCNICO	**60%**			X
Protección de Equipos de Networking	15%		X	
Cumplimiento de las políticas de acceso y controles a los sistemas	30%			X
Espacio Físico y Lógico	15%		X	

Sugerencia respecto a los criterios:

Falta - Disponibilidad de Proveedores de Servicios Relacionados
Soporte
- SaaS.

2. En base al escenario propuesto anteriormente ¿Con qué porcentaje total del modelo cree Ud. Que sería confiable la implementación de una herramienta de seguridad informática en entornos universitarios? ¿Porqué?

85%

Figura 46: Anexo 18- Entrevista/ Encuesta al Ing. Milton Labanda -Determinación Niveles de Confianza-Parte2

c. Escenario 3: Proyectos Estudiantiles

1. Permítase dar una valoración a cada criterio del modelo y en caso de faltar un criterio que crea conveniente, sugiéralo por favor.

CRITERIOS	PESO GENÉRICO	VALOR DE ACEPTACIÓN		
		Alta	Media	Baja
ASPECTO ECONÓMICO	**25%**		X	
Disponibilidad de Presupuesto	10%		X	
Inversión retribuya con los beneficios obtenidos	15%	X		
ASPECTO REPUTACIÓN-CONFIABILIDAD	**25%**		X	
WOT (Web Of Trust): Reputación de los proveedores en la Web	15%		X	
Recomendaciones por otras instituciones educativas	10%		X	
ASPECTO TÉCNICO	**60%**	X		
Protección de Equipos de Networking	15%	X		
Cumplimiento de las políticas de acceso y controles a los sistemas	20%	X		
Espacio Físico y Lógico	10%		X	
Duración de Licencias	15%			

Sugerencia respecto a los criterios:

.....
.....
.....
.....
.....
.....

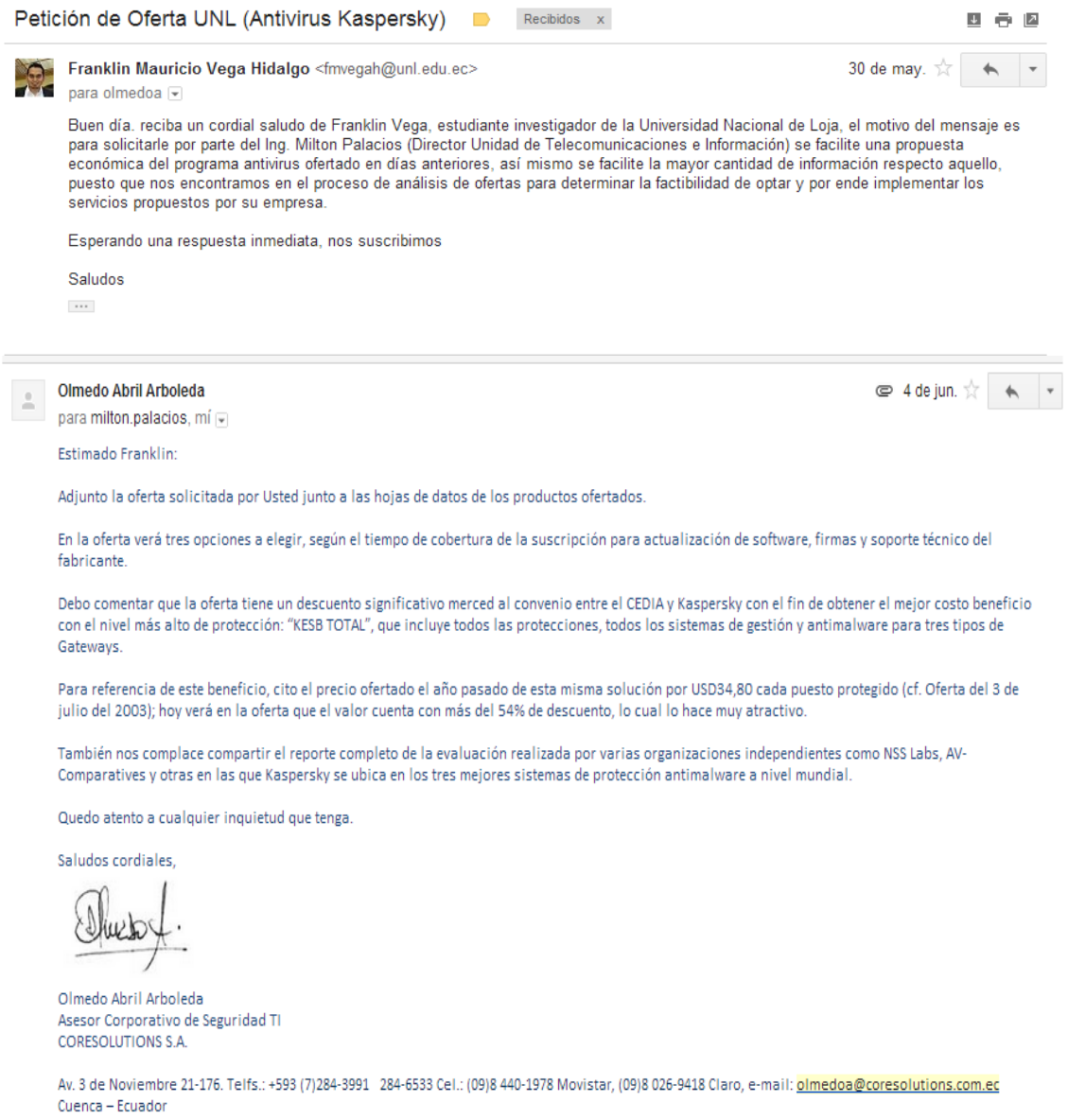
2. En base al escenario propuesto anteriormente ¿Con qué porcentaje total del modelo cree Ud. Que sería confiable la implementación de una herramienta de seguridad informática en entornos universitarios? ¿Porqué?

90%

.....
.....
.....

Figura 47: Anexo 18- Entrevista/ Encuesta al Ing. Milton Labanda -Determinación Niveles de Confianza-Parte3

19. Solicitud/Respuesta de la Propuesta de Antivirus Kaspersky a CoreSolutions S.A.(Ing. Olmedo Abril) para la Universidad Nacional de Loja.



Petición de Oferta UNL (Antivirus Kaspersky) Recibidos x

Franklin Mauricio Vega Hidalgo <fmvegah@unl.edu.ec> 30 de may.
para olmedoa

Buen día. reciba un cordial saludo de Franklin Vega, estudiante investigador de la Universidad Nacional de Loja, el motivo del mensaje es para solicitarle por parte del Ing. Milton Palacios (Director Unidad de Telecomunicaciones e Información) se facilite una propuesta económica del programa antivirus ofertado en días anteriores, así mismo se facilite la mayor cantidad de información respecto aquello, puesto que nos encontramos en el proceso de análisis de ofertas para determinar la factibilidad de optar y por ende implementar los servicios propuestos por su empresa.

Esperando una respuesta inmediata, nos suscribimos

Saludos

Olmedo Abril Arboleda 4 de jun.
para milton.palacios, mí

Estimado Franklin:

Adjunto la oferta solicitada por Usted junto a las hojas de datos de los productos ofertados.

En la oferta verá tres opciones a elegir, según el tiempo de cobertura de la suscripción para actualización de software, firmas y soporte técnico del fabricante.

Debo comentar que la oferta tiene un descuento significativo merced al convenio entre el CEDIA y Kaspersky con el fin de obtener el mejor costo beneficio con el nivel más alto de protección: "KESB TOTAL", que incluye todos las protecciones, todos los sistemas de gestión y antimalware para tres tipos de Gateways.

Para referencia de este beneficio, cito el precio ofertado el año pasado de esta misma solución por USD34,80 cada puesto protegido (cf. Oferta del 3 de julio del 2003); hoy verá en la oferta que el valor cuenta con más del 54% de descuento, lo cual lo hace muy atractivo.

También nos complace compartir el reporte completo de la evaluación realizada por varias organizaciones independientes como NSS Labs, AV-Comparatives y otras en las que Kaspersky se ubica en los tres mejores sistemas de protección antimalware a nivel mundial.

Quedo atento a cualquier inquietud que tenga.

Saludos cordiales,

Olmedo Abril Arboleda
Asesor Corporativo de Seguridad TI
CORESOLUTIONS S.A.

Av. 3 de Noviembre 21-176. Telfs.: +593 (7)284-3991 284-6533 Cel.: (09)8 440-1978 Movistar, (09)8 026-9418 Claro, e-mail: olmedoa@coresolutions.com.ec
Cuenca – Ecuador

Figura 48: Anexo 19- Solicitud/Respuesta de Propuesta por CoreSolutions S.A.

20. Primera Propuesta de Antivirus Kaspersky por parte de CoreSolutions S.A. a la Universidad Nacional de Loja (2013).

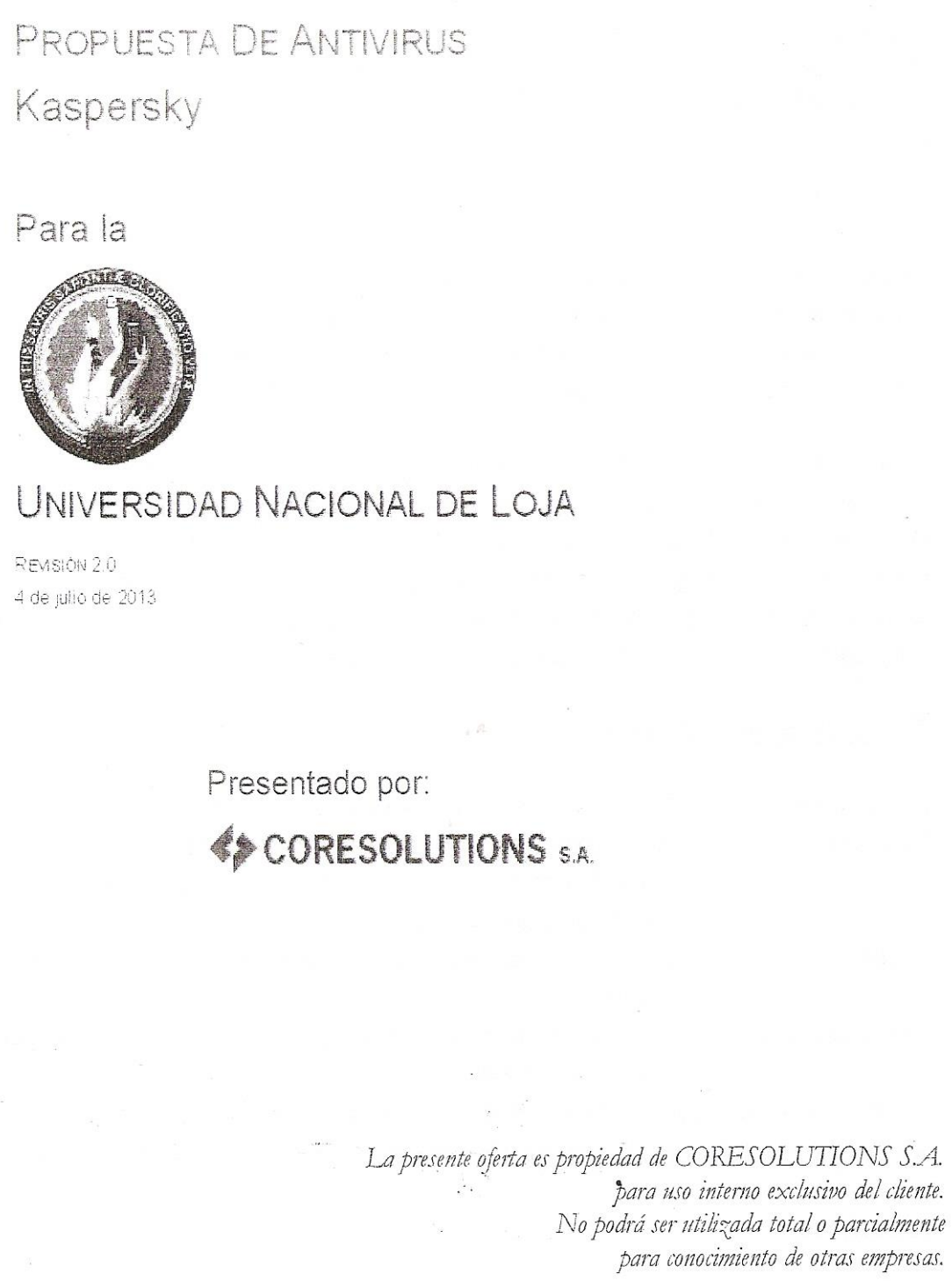


Figura 49: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte1

CORESOLUTIONS S.A.

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

Cuenca, 4 de julio de 2013

Ingeniero
Milton Palacios
Universidad Nacional de Loja
Loja

Estimado Milton:

Coresolutions S.A. con el respaldo de Kaspersky Lab está gustoso de presentar la propuesta de licencias Anti-malware con suscripción para actualización de firmas y soporte técnico de fábrica para una solución de seguridad informática con el nuevo producto antivirus "Kaspersky Endpoint Security for Business" o KESB en lugar del anterior "Kaspersky Open Space Security" o KOSS.

En la oferta se incluyen tres opciones para 1000 y tres opciones para 1500 licencias académicas nuevas. Tanto para el nivel de protección Select como para Advanced, considere el AddOn Anti-Spam de correo. En cambio la opción Total ya cuenta con protección Anti-Spam, Web y de Colaboración. Se incluyen los servicios de valor agregados opcionales para instalar la nueva versión, configurar y capacitar a los administradores de seguridad en TI de tal manera que desarrollen las destrezas necesarias para continuar con la gestión de seguridad una vez montada la solución.

Condiciones generales de la oferta:

Forma de pago:	50% con la orden de compra y 50% contra entrega del producto.
Plazo de entrega:	Hasta ocho días laborables para entrega de las llaves de activación. La instalación se puede hacer en mutuo acuerdo por disponibilidad entre las partes y dura cinco horas.
Garantía:	Un año en firmas y actualizaciones de definiciones de virus. Soporte técnico de fábrica.
Validez de la oferta:	Diez días a partir de la presente fecha y/o mientras se disponga de los productos ofertados.

Si Usted tiene alguna pregunta o quisiera programar una revisión de la propuesta del alcance, por favor contácteme al celular (09)9 026-9418 en Claro o al (09)8 440-1978 en Movistar.

Atentamente,

Ing. Olmedo Abril Arboleda
Asesor Corporativo de Seguridad TI

KASPERSKY lab

Figura 50: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte2

CORESOLUTIONS S.A.

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

Antivirus Kaspersky Opc. 1

Señores
Universidad Nacional de Loja
miércoles, 03 de julio de 2013

Cant.	Descripción	Unitario	Total
1000	Kaspersky Endpoint Security for Business Nivel de protección KESB "Select" Licencia académica nueva suscripción y soporte técnico para un año Protección activa para servidores y estaciones de trabajo Windows, Mac, Linux y dispositivos móviles (teléfonos inteligentes) Seguridad de Archivos, Control de aplicaciones, Control de Dispositivos, Control Web, Anti-malware + Firewall Incluye kit de administración para gestión de clientes centralizado. La licencia del producto sostiene el número de equipos declarados. Es importante no rebasar este número para evitar la revocación del acuerdo.	21.00	21,000.00
1	Servicios de valor agregado para la Nueva versión de Kaspersky · Instalación y configuración de 1 kit de Administración o Kaspersky Security Center 9. · Instalación hasta de 10 clientes físicos con puntos finales Kaspersky Endpoint 8 conectados a la consola de gestión · Instalación en modo de taller a fin de proporcionar una transferencia de conocimientos al personal técnico del cliente.	800.00	800.00
Nota: El precio no incluye el IVA.		**Suman**	21,800.00

KASPERSKY lab

Figura 51: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte3

CORESOLUTIONS S.A.

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

Antivirus Kaspersky Opc. 2

Señores
Universidad Nacional de Loja
miércoles, 03 de julio de 2013

Cant.	Descripción	Unitario	Total
1500	Kaspersky Endpoint Security for Business Nivel de protección KESB "Select" Licencia académica nueva suscripción y soporte técnico para un año Protección activa para servidores y estaciones de trabajo Windows, Mac, Linux y dispositivos móviles (teléfonos inteligentes) Seguridad de Archivos, Control de aplicaciones, Control de Dispositivos, Control Web, Anti-malware + Firewall Incluye kit de administración para gestión de clientes centralizado. La licencia del producto sostiene el número de equipos declarados. Es importante no rebasar este número para evitar la revocación del acuerdo.	19.00	28,500.00
1	Servicios de valor agregado para la Nueva versión de Kaspersky · Instalación y configuración de 1 kit de Administración o Kaspersky Security Center 9. · Instalación hasta de 10 clientes físicos con puntos finales Kaspersky Endpoint 8 conectados a la consola de gestión · Instalación en modo de taller a fin de proporcionar una transferencia de conocimientos al personal técnico del cliente.	800.00	800.00
Nota: El precio no incluye el IVA.		**Suman**	29,300.00

KASPERSKY lab

Figura 52: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte4

CORESOLUTIONS S.A.

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

Antivirus Kaspersky Opc. 3

Señores
Universidad Nacional de Loja
miércoles, 03 de julio de 2013

Cant.	Descripción	Unitario	Total
1000	Kaspersky Endpoint Security for Business Nivel de protección KESB "Advanced" Licencia académica nueva suscripción y soporte técnico para un año Protección activa para servidores y estaciones de trabajo Windows, Mac, Linux y dispositivos móviles (teléfonos inteligentes) Seguridad de Archivos, Control de aplicaciones, Control de Dispositivos, Control Web, Anti-malware + Firewall Manejo de licencias, Admisión de Red (NAC), Instalación de Software Aprovisionamiento de imágenes, Manejo de parches, Escaneo de Vulnerabilidades Incluye kit de administración para gestión de clientes centralizado. La licencia del producto sostiene el número de equipos declarados. Es importante no rebasar este número para evitar la revocación del acuerdo.	27.00	27,000.00
1	Servicios de valor agregado para la Nueva versión de Kaspersky · Instalación y configuración de 1 kit de Administración o Kaspersky Security Center 9. · Instalación hasta de 10 clientes físicos con puntos finales Kaspersky Endpoint 8 conectados a la consola de gestión · Instalación en modo de taller a fin de proporcionar una transferencia de conocimientos al personal técnico del cliente.	1,200.00	1,200.00
Nota: El precio no incluye el IVA.		**Suman**	28,200.00

KASPERSKY lab

Figura 53: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte5

CORESOLUTIONS S.A.

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

Antivirus Kaspersky Opc. 4

Señores
Universidad Nacional de Loja
miércoles, 03 de julio de 2013

Cant.	Descripción	Unitario	Total
1500	Kaspersky Endpoint Security for Business Nivel de protección KESB "Advanced" Licencia académica nueva suscripción y soporte técnico para un año Protección activa para servidores y estaciones de trabajo Windows, Mac, Linux y dispositivos móviles (teléfonos inteligentes) Seguridad de Archivos, Control de aplicaciones, Control de Dispositivos, Control Web, Anti-malware + Firewall Manejo de licencias, Admisión de Red (NAC), Instalación de Software Aprovisionamiento de imágenes, Manejo de parches, Escaneo de Vulnerabilidades Incluye kit de administración para gestión de clientes centralizado. La licencia del producto sostiene el número de equipos declarados. Es importante no rebasar este número para evitar la revocación del acuerdo.	25.00	37,500.00
1	Servicios de valor agregado para la Nueva versión de Kaspersky · Instalación y configuración de 1 kit de Administración o Kaspersky Security Center 9. · Instalación hasta de 10 clientes físicos con puntos finales Kaspersky Endpoint 8 conectados a la consola de gestión · Instalación en modo de taller a fin de proporcionar una transferencia de conocimientos al personal técnico del cliente.	1,200.00	1,200.00
Nota: El precio no incluye el IVA.		**Suman**	38,700.00

KASPERSKY lab

Figura 54: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte6

CORESOLUTIONS S.A.

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

Antivirus Kaspersky Opc. 5

Señores
Universidad Nacional de Loja
miércoles, 03 de julio de 2013

Cant.	Descripción	Unitario	Total
1000	Kaspersky Endpoint Security for Business Nivel de protección KESB "Total" Licencia académica nueva suscripción y soporte técnico para un año Protección activa para servidores y estaciones de trabajo Windows, Mac, Linux y dispositivos móviles (teléfonos inteligentes) Seguridad de Archivos, Control de aplicaciones, Control de Dispositivos, Control Web, Anti-malware + Firewall Manejo de licencias, Admisión de Red (NAC), Instalación de Software Aprovisionamiento de imágenes, Manejo de parches, Escaneo de Vulnerabilidades, Protección antimalware para: Gateway de navegación Web, Servidor de Correo y Colaboración Incluye kit de administración para gestión de clientes centralizado. La licencia del producto sostiene el número de equipos declarados. Es importante no rebasar este número para evitar la revocación del acuerdo.	36.00	36,000.00
1	Servicios de valor agregado para la Nueva versión de Kaspersky · Instalación y configuración de 1 kit de Administración o Kaspersky Security Center 9. · Instalación hasta de 10 clientes físicos con puntos finales Kaspersky Endpoint 8 conectados a la consola de gestión · Instalación en modo de taller a fin de proporcionar una transferencia de conocimientos al personal técnico del cliente. · Instalación de Add-On Mail, Web y Colaboración.	4,000.00	4,000.00
Nota: El precio no incluye el IVA.		**Suman**	40,000.00

KASPERSKY lab

Figura 55: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte7

CORESOLUTIONS S.A.

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

Antivirus Kaspersky Opc. 6

Señores
Universidad Nacional de Loja
miércoles, 03 de julio de 2013

Cant.	Descripción	Unitario	Tota
1500	Kaspersky Endpoint Security for Business Nivel de protección KESB "Total" Licencia académica nueva suscripción y soporte técnico para un año Protección activa para servidores y estaciones de trabajo Windows, Mac, Linux y dispositivos móviles (teléfonos inteligentes) Seguridad de Archivos, Control de aplicaciones, Control de Dispositivos, Control Web, Anti-malware + Firewall Manejo de licencias, Admisión de Red (NAC), Instalación de Software Aprovisionamiento de imágenes, Manejo de parches, Escaneo de Vulnerabilidades, Protección antimalware para: Gateway de navegación Web, Servidor de Correo y Colaboración Incluye kit de administración para gestión de clientes centralizado. La licencia del producto sostiene el número de equipos declarados. Es importante no rebasar este número para evitar la revocación del acuerdo.	34.00	51,00
1	Servicios de valor agregado para la Nueva versión de Kaspersky · Instalación y configuración de 1 kit de Administración o Kaspersky Security Center 9. · Instalación hasta de 10 clientes físicos con puntos finales Kaspersky Endpoint 8 conectados a la consola de gestión · Instalación en modo de taller a fin de proporcionar una transferencia de conocimientos al personal técnico del cliente.	1,200.00	1,20
Nota: El precio no incluye el IVA.		**Suman**	52,20

Figura 56: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte8

KASPERSKY lab

CORESOLUTIONS S.A.
Av. 3 de Noviembre 21-176
Telfs : 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

Kaspersky Plug-in Anti-Spam

Señores
Universidad Nacional de Loja
miércoles, 03 de julio de 2013

Cant.	Descripción	Unitario	Total
1000	Kaspersky Security Mail Server Soporte de buzones para servidores de correo electrónico: • Servidores Microsoft Exchange 2003, 2007, 2010 • IBM Lotus Domino (v. 6.5, 7.0, 8.0, 8.5) • Servidores de correo con base en Linux: Sendmail, Qmail, Postfix, Exim, y CommuniGate Pro. Protección con motor anti-malware en tiempo real Motor anti-spam asistido por la nube de alto desempeño Desempeño superior con uso mínimo de recursos Una administración flexible y fácil en base a roles de usuario Filtración de mensajes por tipo de archivo adjunto	8.00	8,000.00
1	Servicios de valor agregado para instalación del Plug-in · Instalación y configuración en un servidor de correo · Definición de listas negras y listas blancas · Configuración y bloqueo de Spam · Reportes y estado de la protección	1,900.00	1,900.00
		Suman	9,900.00

Nota: El precio no incluye el IVA.

KASPERSKY lab

Figura 57: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte9

CORESOLUTIONS S.A.

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

ALCANCE DEL SERVICIO PARA
KASPERSKY ENDPOINT SECURITY FOR BUSINESS

1. PROPUESTA DE IMPLEMENTACIÓN "KESB SELECT"

Se realizará la instalación de la consola de administración de Kaspersky Security Center, se configurarán las políticas y se establecerán tareas para análisis y actualizaciones programadas a través del servidor de administración, tanto para servidores y estaciones de trabajo. Al ser una instalación "Select" se hace énfasis en el módulo de control web y control de dispositivos. Finalmente se realizará una instalación demo en un dispositivo móvil soportado y se lo vinculará a la consola de administración. Si la organización cuenta con Directorio Activo, el descubrimiento de los equipos para integrarlos a la consola será inmediato. De no contar con este servicio, los equipos serán anclados a la consola en modo manual.

1.1 SERVICIOS

Los servicios serán para instalar hasta diez equipos en total, entre equipos de clientes y servidores incluida la consola de administración o centro de seguridad Kaspersky.

1.1.1 Instalación y Configuración de la consola de administración de Kaspersky

- Instalación del sistema operativo en español de Windows 2008R2 SP1 Standard Edition. La licencia del sistema operativo original, debe ser provista por la organización.
- Instalación y configuración inicial de la consola de administración Kaspersky Security Center con las mejores prácticas de seguridad recomendadas para optimizar recursos limitados del servidor en almacenamiento o memoria si fuera necesario. En caso de actualización del producto de KOSS a KESB, solamente se realizará la migración a la nueva versión a través de la utilidad de seguridad y restauración de Kaspersky Security Center.

1.1.2 Alcance y actividades a realizar para la protección antimalware

- Configuración inicial hasta de 3 políticas y afinamiento de las mismas así como de las tareas programadas para servidores.
- Despliegue del agente y antivirus para 2 servidores con sistema operativo original de servidor compatible con Windows:
  - Windows Server 2003 R2 SP2 o superior,
  - Windows Server 2008 SP2 o superior,
  - Windows Server 2008 R2 SP1.
- Configuración inicial de hasta 3 políticas y afinamiento de las mismas, así como de las tareas programadas para estaciones de trabajo.
- Despliegue del agente y antivirus para 8 estaciones de trabajo con sistemas operativos originales de cliente compatibles con Windows, Linux o Macintosh:
  - Windows XP Pro SP3,
  - Windows Vista Bussines SP1 o superior,
  - Windows 7 Pro SP1 y
  - Windows 8 Pro.
  - Linux Ubuntu (12.04 únicamente) o Fedora (versión 18 únicamente).
  - Max OSX: 10.6.8, 10.7.5 y 10.8.1
  - Dispositivo móvil con Android (versión 2.3 en adelante).

Figura 58: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte10

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail: gerencia@coresolutions.com.ec

1.1.3 Tareas a realizar en cada equipo

Despliegue del agente de Kaspersky.

Despliegue del antivirus en cualquiera de las versiones soportadas Kaspersky EndPoint 6, 8 y 10 en estaciones de trabajo y Kaspersky Antivirus 8.0 for Windows Server en equipos servidores.

Vinculación a la consola de administración del agente Kaspersky.

Verificación de funcionalidad de puntos finales. Los equipos deben pertenecer a una sola ubicación física, por ejemplo dentro del mismo edificio.

1.1.4 Visita guiada de las funciones de protección de terminales

Revisión del control Web para la navegación en el Internet por listas blancas y listas negras.

Explicación para control de dispositivos extraíbles conectados por USB.

Gestión para el control de Aplicaciones.

2. PROPUESTA DE IMPLEMENTACIÓN "KESB ADVANCED"

La cobertura de implementación para esta edición, contempla la misma propuesta para Select descrito en el punto 1 del alcance y sobre ésta, al ser una instalación ADVANCED se hace énfasis en el módulo de despliegue de software/sistemas operativos, así como de encriptación de datos (fase de pruebas) y la configuración de los sistemas de gestión de revisiones: Parches, despliegue remoto de software y Control de admisión de Red (NAC).

2.1 SERVICIOS

Los servicios incluyen los mismos del punto 1.1 para la edición Select y sobre esto se desarrollarán los siguientes puntos adicionales:

2.1.1 Cifrado exhaustivo

Protección de información en dos modalidades: disco completo o por carpetas en 2 equipos de usuarios finales. Se desarrolla en un ambiente controlado de pruebas.

2.1.2 Gestión de parches

Despliegue de 1 política para análisis exhaustivo avanzado de vulnerabilidades y combinación con la distribución de parches en 2 equipos.

2.1.3 Control de admisión en la Red (NAC)

Creación de 1 política para invitados en la Red. Reconocimiento de dispositivos móviles y reenvío al portal para habilitar sus credenciales y asignación de recursos aprobados.

2.2 Visita guiada de funciones de protección de terminales

- Revisión de la gestión de Hardware y licencias de Software a través del informe del inventario.
- Explicación para despliegue remoto de software en los equipos del cliente desde un punto centralizado.
- Revisión de las herramientas antirrobo remotas y vigilancia SIM, bloqueo remoto y borrado de datos corporativos en Smartphones con Android.

Figura 59: Anexo 21- Primera Propuesta Antivirus Kaspersky-Parte11

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

3. IMPLEMENTACIÓN DE ADICIONALES

Para los casos en los que la oferta incluye los módulos adicionales de seguridad o AddOn para correo electrónico y control antimalware de Internet en el Gateway de navegación, los servicios que se incluyen son los siguientes:

3.1 Protección Anti-Spam

- Verificación del correcto funcionamiento del servidor de correo de correo electrónico.
- Instalación y configuración inicial de la base de datos SQL Server 2008 R2 Express (no requiere licencia) cuando es Exchange Server, con las mejores prácticas de seguridad recomendadas o de Kaspersky Antivirus for Linux Mail Server.
- Verificación de los servicios levantados por el correo Exchange en el servidor.
- Instalación del módulo de Kaspersky Security for Mail Servers.
- Configuración de las listas blancas y negras en el módulo de Kaspersky Security for Mail Servers
- Verificación del funcionamiento del módulo de Kaspersky conjuntamente con el servidor de Correo enviando Spam de manera intencional.
- Configuración inicial de hasta 3 reglas de protección para correo de entrada y 3 reglas de protección para correo de salida.

3.2 Protección Antimalware de perímetro

- Verificación del correcto funcionamiento del Gateway de Internet.
- Instalación y configuración inicial de la base de datos SQL Server 2008 R2 Express con las mejores prácticas de seguridad recomendada en caso que tenga MS ForeFront TMG o el módulo correspondiente al Gateway basado en Linux, Kaspersky Antivirus for Linux Gateway Server.
- Verificación de los servicios levantados por Microsoft Forefront TMG en el servidor y servicios de Linux Gateway.
- Configuración de las 3 reglas para escaneo de trafico entrante y 3 reglas de tráfico saliente de Kaspersky Security for Antimalware.

3.3 Protección de la Colaboración

- Instalación de la protección antimalware en el servidor de colaboración Microsoft SharePoint.
- Políticas de colaboración interna.
- Políticas de almacenamiento para control de archivos innecesarios.
- Diccionarios y categorías para filtros de palabras prohibidas.
- Revisión de informes y estado de la protección.

4. METODOLOGÍA

Se propone la provisión de estos servicios a modo de taller, para lo cual se requieren la activa participación del personal de IT de su organización, de tal forma que se consiga una efectiva transferencia de conocimientos.

5. ENTREGABLES

Figura 60: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte12

Al finalizar la prestación del servicio, se entregará un documento con la memoria técnica de los servicios realizados con una lista de verificación del alcance cumplido descrito en este alcance.

6. PLAZO DE EJECUCIÓN

De acuerdo a una configuración típica según el alcance indicado, se estima una duración de 4 días en la instalación de la solución completa con los adicionales en la ciudad de Cuenca. Se coordinarán los horarios de trabajo, en base a la disponibilidad de la organización, de tal forma que se asegure al mayor nivel posible para una adecuada transferencia de conocimientos durante el proceso de implementación, y el máximo aprovechamiento de la capacitación impartida al personal de IT del diente.

7. TRANSFERENCIA DE CONOCIMIENTOS

Nuestros trabajos se caracterizan por ayudar a los clientes a entender el proceso de administración de la herramienta y para alcanzar este fin, es necesario contar con un ingeniero asignado al proyecto que acompaña todo el tiempo en los trabajos que serán realizados a modo taller a fin de realizar una adecuada transferencia de conocimientos. La administración es relativamente fácil y la mayoría de clientes expanden su despliegue más allá del alcance inicial usando sus propios recursos para gestionar la solución independientemente.

8. LIMITACIONES

No Incluye aunque no está restringida la configuración de servicios o productos adicionales como:

- Cambios en el direccionamiento IP a servidores y clientes que puedan verse afectados por la instalación de este servicio de protección antimalware.
- Equipos externos para segmentos de red que no forman parte de la solución como Routers, Switches o PBXs de red adicionales.
- Escaneo completo de equipos contra malware y remediación en caso de infección previa a la instalación de la herramienta.
- Trabajos que dependen de terceros y/o para ejecutar cambios en los que intervenga proveedores adicionales de servicios.
- Licencias de sistema operativo originales, las cuales admiten todos los parches de sistema necesarios para la estabilidad de la solución de seguridad.
- Reinstalación de sistemas operativos de clientes cuando sea necesario al verse afectados por software no original o por contagios previos y qué son graves porque impiden la instalación del agente y/o antivirus.
- Infraestructura necesaria para la implementación de la consola de seguridad tanto en Hardware como en Software.

Coresolutions S.A. puede brindar soporte a estos servicios complementarios con cargos adicionales, previa la oferta y aceptación de los mismos.

9. GARANTÍA TÉCNICA

La presente implementación tiene una garantía técnica de 20 días después de haber sido entregado el documento de memoria técnica y/o acta de entrega recepción del servicio, luego de lo cual revisiones, cambios en configuraciones, etc., tendrán costo adicional. La garantía técnica pierde automáticamente su validez por instalación de nuevo software o aplicativos en el mismo servidor, parches de sistema

Figura 61: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte13

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

operativo aplicados de modo inadecuado, instalación y configuración de nuevos servicios y administración defectuosa por parte del personal de IT interno sobre el/los servidores implementados.

10. RECOMENDACIONES SOBRE REQUERIMIENTOS DEL SISTEMA PARA LA INSTALACIÓN DE KASPERSKY LAB Es IMPORTANTE no tener otro antivirus instalado. En la siguiente tabla, vea las especificaciones técnicas de Hardware.
    - Para Estaciones de Trabajo con Windows
        - Microsoft Windows 8 Pro x86 o x64
        - Microsoft Windows 7 Professional / Enterprise/ Ultimate con SP1
        - Microsoft Windows Vista Professional / Enterprise/ Ultimate con SP2
        - Microsoft Windows Vista x64 Professional / Enterprise/ Ultimate con SP2
        - Microsoft Windows XP Professional (Service Pack 2 o más alto)
        - Microsoft Internet Explorer 7 o más alto
        - Microsoft Windows Installer 3.0
        - Procesador Intel Pentium 1 Gb 32-bit (x86)/ 2GB 64-bit (x64) o más alto (o un CPU compatible) 1GB disponible en RAM
    - Para Servidores con Windows
        - Microsoft Windows Server 2012 (ambiente de pruebas)
        - Microsoft Windows Server 2003 Standard/ Enterprise Edition con todos sus Service Packs y todas sus actualizaciones
        - Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition
        - 60 GB de espacio disponible en HDD mínimo
        - CD-ROM (para la instalación del Kaspersky Anti-Virus desde un CD)
        - 2 GB RAM
        - Microsoft Internet Explorer 7 o más alto (para actualizar las firmas de amenazas y los módulos de la aplicación usando internet)
        - Microsoft Windows Installer 3.0
    - Para Estaciones de Trabajo Linux
        - Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92)
        - Fedora 9 (kernel 2.6.25)
        - SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21)
        - openSUSE Linux 11.0 (kernel 2.6.25)
        - Debian GNU/Linux 4.0 r4 (kernel 2.6.24)
        - Mandriva Corporate Desktop 4 (kernel 2.6.12)
        - Ubuntu 8.04.1 Desktop Edition (kernel 2.6.25)
        - Linux XP Enterprise Desktop 2008 (2.6.25.10-47.3.lxp2008)
        - Intel Pentium 133 MHz o más alto:
        - 64 MB RAM
        - 100 MB de espacio libre en el disco duro para la instalación de la aplicación y el almacenaje de archivos temporales.
    - Para Estaciones de Trabajo Mac
        - Mac OS X 10.6 (32/64-bits), versión Snow Leopard
        - Mac OS X 10.5 (edición de 32 bits), versión Leopard
        - Mac OS X 10.4 (edición de 32 bits), versión Tiger

Figura 62: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte14

- Mac OS X Server 10.6
- Equipo Macintosh basado en Intel:
- 1 GB de RAM
- 500 MB de espacio disponible en el disco duro
- 32 y 64 bits

Para dispositivos móviles

- Android 1.5 – 2.3
- Symbian S60 9.1 - 9.4, Symbian^3 (Nokia)
- Windows Mobile 5.0 - 6.5
- BlackBerry 4.5 - 6.0

Para la Consola de administración o Kaspersky Security Center 9

Requisitos de software:

- Sistema operativo de Windows. La versión compatible del sistema operativo está determinada por los requisitos del servidor de administración
- Microsoft Management Console 2.0 o superior
- El funcionamiento con Microsoft Windows XP, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 o Windows Vista requiere la instalación de Microsoft Internet Explorer 7.0 o superior
- El funcionamiento con Microsoft Windows 7 requiere la instalación de Microsoft Internet Explorer 8.0 o superior

Requisitos de hardware:

- Para sistemas operativos de 32 bits:
- Procesador con frecuencia de operación de 1 GHz o superior
- Tamaño de RAM: 512 MB
- 1 GB de espacio libre en disco
- Para sistemas operativos de 64 bits:
- Procesador con frecuencia de operación de 1,4 GHz o superior
- Tamaño de RAM: 512 MB
- 1 GB de espacio libre en disco

Para Servidores Windows con Exchange Server

- Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition.
- Microsoft Exchange Server 2007 x64 SP1 en adelante o Microsoft Exchange Server 2010 SP1 en adelante.
- Microsoft SQL Server 2008 R2 Express con todas las actualizaciones y parches (debe ser accesible desde la red).
- 60 GB de espacio disponible en HDD mínimo.
- 2 GB RAM.
- Microsoft Internet Explorer 7 o más alto (para actualizar las firmas de amenazas usando internet).
- Microsoft .Net Framework 3.5 con service pack 1.

Para el módulo de administración o Kaspersky Security for Exchange Servers

Requisitos de hardware:

- Procesador con frecuencia de operación de 1 GHz o superior
- Tamaño de RAM: 512 MB
- 500 MB de espacio libre en disco

Para Servidores Windows con Microsoft TMG Forefront

- Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition.

Figura 63: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte15

Av. 3 de Noviembre 21-176
Telfs.: 284-1495 284-3991 284-6533
Fax: 284-4624
Cuenca – Ecuador
E-mail gerencia@coresolutions.com.ec

- Microsoft ISA Server 2006 / Forefront TMG Console
- Microsoft SQL Server 2008 R2 Express con todas las actualizaciones y parches (debe ser accesible desde la red).
- 60 GB de espacio disponible en HDD mínimo.
- 2 GB RAM.
- Microsoft Internet Explorer 7 o más alto (para actualizar las firmas de amenazas usando internet).
- Microsoft .Net Framework 3.5 con service pack 1.

NOTA: Tener presente que los Service Packs son fundamentales en las consolas y en los clientes de Kaspersky para poder asegurar el buen funcionamiento del producto.

Figura 64: Anexo 20- Primera Propuesta Antivirus Kaspersky-Parte16

21. Segunda Propuesta de Antivirus Kaspersky por parte de CoreSolutions S.A. a la Universidad Nacional de Loja (2014).

PROPUESTA DE ANTIVIRUS Kaspersky

Para la

UNIVERSIDAD NACIONAL DE LOJA

REVISIÓN 3
4 de junio de 2014

Presentado por:

CORESOLUTIONS S.A.

Cuenca, 4 de junio de 2014

Ingeniero
Milton Palacios
Universidad Nacional de Loja, UNL
Loja

Estimado Ingeniero:

Coresolutions S.A. con el respaldo de Kaspersky Lab está gustoso de presentar la oferta para nuevas licencias Anti-malware, con suscripción para actualización de firmas y soporte técnico de fábrica, de "Kaspersky Endpoint Security for Business" o KESB.

En la oferta se incluyen tres opciones de licenciamiento con suscripción de uno, dos y tres años a elegir para actualización de software, firmas y soporte técnico del fabricante, con el fin de que pueda evaluar la mejor opción que se ajuste a su presupuesto. Se incluyen servicios de valor agregado para instalar la nueva versión de la consola de administración en caso que sea requerido, para configurar y capacitar a los administradores de seguridad en TI de tal manera que desarrollen las destrezas necesarias para continuar con la gestión de seguridad una vez montada la solución.

Al ser un licenciamiento corporativo, es necesario contar con un servidor físico o virtual para instalación de la consola de administración, la misma que ayuda a gestionar los equipos de clientes para actualización de políticas de seguridad, distribución de firmas y actualización de software con sistema operativo Windows Server.

Condiciones generales de la oferta:

Forma de pago:	100% contra entrega de las licencias e instalación
Plazo de entrega:	Hasta 30 días para entrega de las llaves de activación e instalación, cuya ejecución se puede hacer en mutuo acuerdo por disponibilidad entre las partes.
Garantía:	Indicados en cada caso, según la opción elegida del tiempo suscrito para actualización de software, firmas y soporte técnico del fabricante.
Validez de la oferta:	Treinta días a partir de la presente fecha y/o mientras se disponga de los productos ofertados.

Si Usted tiene alguna pregunta o quisiera programar una revisión de la propuesta del alcance, por favor contácteme al celular (09)8 026-9418 en Claro o al (09)8 440-1978 en Movistar.

Atentamente,

Ing. Olmedo Abril Arboleda
Asesor Corporativo de Seguridad TI
Coresolutions S.A.

BENEFICIOS EMPRESARIALES

Al contar con un personal cada vez más móvil y diversificado, la mayoría de las empresas deben extender su seguridad mucho más allá de los límites tradicionales. Además de ofrecer las galardonadas tecnologías antimalware de Kaspersky, Kaspersky Endpoint Security for Business añade seguridad móvil, seguridad de servidores de archivos y tecnologías de control flexible que le permiten garantizar el cumplimiento con sus políticas de seguridad.

MAYOR PROTECCIÓN DE SU EMPRESA, SUS DATOS Y SU REPUTACIÓN

Las tecnologías antimalware de Kaspersky ofrecen defensas de múltiples capas para proteger sus sistemas y sus datos comerciales confidenciales contra las amenazas cada vez más sofisticadas de la actualidad. Con una combinación de tecnologías proactivas, basadas en firma y activadas para la nube, además de características especiales, como Network Attack Blocker y firewall bidireccional, Kaspersky Endpoint Security for Business hace mucho más que tan solo mantener segura su empresa.

PREVENCIÓN DE LA PROPAGACIÓN DE MALWARE A TRAVÉS DEL ALMACENAMIENTO COMPARTIDO

Un solo archivo infectado en uno de sus servidores tiene el potencial de afectar todas las computadoras de su red corporativa y eso puede dañar gravemente la productividad comercial. Kaspersky Endpoint Security for Business incluye antimalware fundamental para los servidores de archivos con el fin de proteger contra el malware a los servidores que ejecutan Microsoft Windows, Linux y Novell NetWare.

ACCESO MÓVIL Y MODELO BYOD SEGURO

Las tecnologías de seguridad móvil de múltiples capas lo ayudan a defender su empresa contra los riesgos de seguridad que pueden surgir al permitir el acceso móvil a sus sistemas corporativos. Kaspersky Endpoint Security for Business puede ayudarlo a beneficiarse de los ahorros en costos y del aumento en la productividad que puede ofrecer una iniciativa "Traiga su propio dispositivo" (BYOD), mientras que las tecnologías de Kaspersky lo protegen contra virus, spyware, troyanos, gusanos, bots y una amplia variedad de otras amenazas.

AHORRO DE TIEMPO Y DINERO... MEDIANTE LA SIMPLIFICACIÓN DE LA ADMINISTRACIÓN MÓVIL

Con la seguridad móvil y la funcionalidad Mobile Device Management (MDM) integradas, Kaspersky Endpoint Security for Business facilita el control de cómo los dispositivos móviles tienen acceso a sus sistemas comerciales. En cuanto aparece un dispositivo móvil en su red, es visible para sus administradores, de modo que puedan comenzar a administrar rápidamente la seguridad del dispositivo y la manera en que el dispositivo interactúa con sus sistemas.

POTENTES HERRAMIENTAS DE CONTROL PARA AYUDARLO A IMPLEMENTAR SUS POLÍTICAS DE SEGURIDAD

Las tecnologías de control de aplicaciones, control de dispositivos y control web de Kaspersky permiten brindar un nivel mucho más profundo de defensa de sus datos y sistemas, de modo que su equipo de TI pueda controlar con facilidad la manera en que se ejecutan las aplicaciones y administrar cómo los empleados utilizan la web y los dispositivos extraíbles. Kaspersky Endpoint Security for Business lo ayuda a implementar sus políticas de seguridad corporativa en toda su empresa y para todo su personal.

CONFIGURACIÓN PREVIA PARA OFRECER PROTECCIÓN INMEDIATA

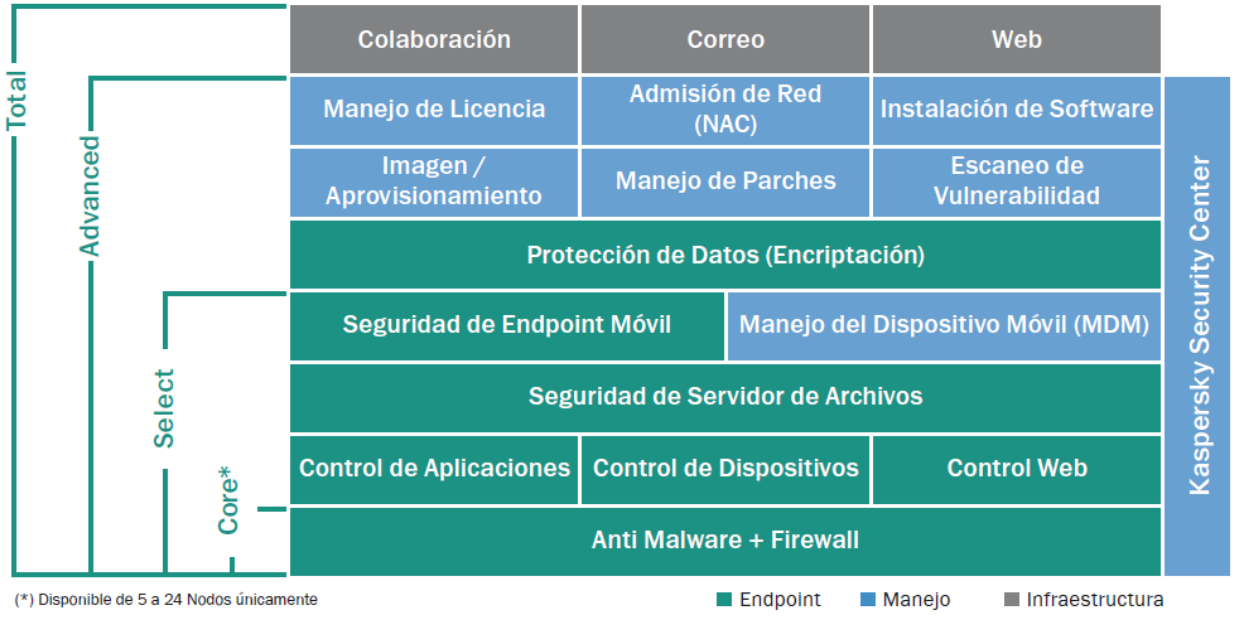
En cuanto Kaspersky Endpoint Security for Business está instalado en su red corporativa, las tecnologías de Kaspersky están listas para comenzar a proteger su empresa. Además, debido a que incluye la consola de administración centralizada de Kaspersky, es fácil adaptar la configuración de todas las tecnologías de seguridad de Kaspersky que ejecuta su empresa, incluidas las soluciones Kaspersky Targeted Security que añada.

ADAPTACIÓN DE SU SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN A SUS REQUISITOS

Si necesita añadir más capacidades de seguridad o administración para su entorno de TI, las soluciones Targeted Security de Kaspersky ofrecen una gama de tecnologías adicionales que pueden complementar su solución Kaspersky Endpoint Security for Business. Puede decidir añadir protección de almacenamiento, virtualización, correo, puertas de enlace de Internet o colaboración... o funcionalidad de administración de sistemas de gran alcance.

LA NUEVA VERSIÓN: KASPESKY END POINT SECURITY FOR BUSINESS

En la siguiente ilustración están los niveles progresivos de protección resumidos para licenciamiento:



COMPARATIVOS DE ANALISTAS

Gartner ubica a Kaspersky Lab como líder en su cuadrante mágico de protección Endpoint en el 2013.

Magic Quadrant

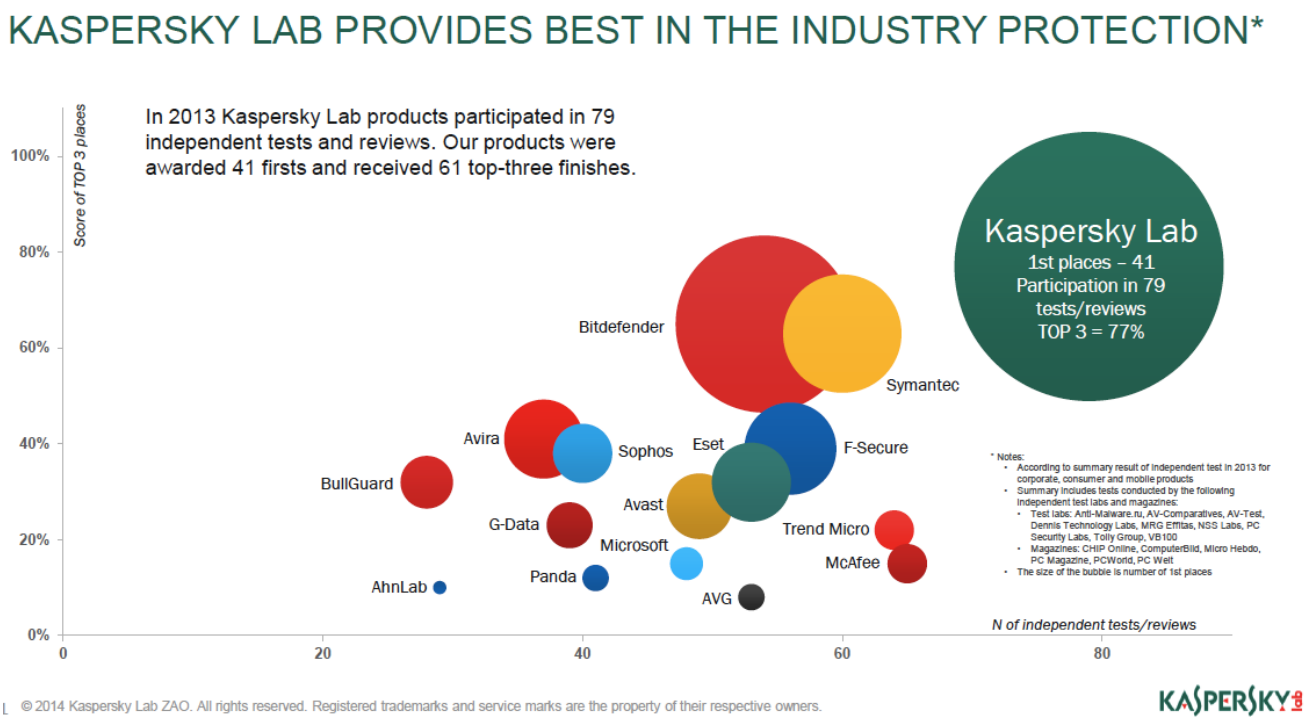
Figure 1. Magic Quadrant for Endpoint Protection Platforms

¿POR QUÉ KASPERSKY PARA SU NEGOCIO?

TOP3 2013

Kaspersky Lab alcanzó posicionarse entre los tres mejores programas de protección anti-malware tras ser evaluado por varias organizaciones independientes entre 96 competidores. Las empresas de evaluación son las siguientes:

AV-Comparatives	AV-Test
CHIP	Computerbild
Dennis Technology Labs	MRG Efitas
NSS Labs	PC Magazine
PC Security Labs	PCWorld
PC Welt	Micro Hebdo
Tolly Group	VB100



Antivirus Kaspersky: Opc. 1 año

Señores

Universidad Nacional de Loja
martes, 03 de junio de 2014

Cant.	Descripción	Unitario	Total
1500	Kaspersky Endpoint Security for Business Protección KESB de nivel **"Total"** corporativo **Licencia Académica** con garantía técnica de **1 año** que incluye: · Actualización de Software y Firmas de Malware · Soporte técnico de fábrica a través de la Web Protección activa para servidores y estaciones de trabajo Windows, Mac, Linux y dispositivos móviles (teléfonos inteligentes) Seguridad de Archivos, Control de aplicaciones, Control de Dispositivos, Control Web, Anti-malware + Firewall Manejo de licencias, Admisión de Red (NAC), Instalación de Software Aprovisionamiento de imágenes, Manejo de parches, Escaneo de Vulnerabilidades, Protección antimalware para: Control antimalware en el Gateway como AddOn en: · Gateway de navegación Web · Gateway de Correo Electrónico · Gateway de Colaboración con MS SharePoint Incluye kit de administración para gestión de clientes centralizado. La licencia del producto sostiene el número de equipos declarados. Es importante no rebasar este número para evitar la revocación del acuerdo. Servicios Profesionales de Valor Agregado y vigencia tecnológica: · Instalación y configuración de 1 kit de Administración o Kaspersky Security Center 9: Un servidor principal y otro esclavo · Instalación hasta de 10 clientes físicos con puntos finales Kaspersky Endpoint 8 conectados a la consola de gestión · Instalación en modo taller a fin de proporcionar una transferencia de conocimientos al personal técnico del cliente. · Configuración para gestión de Parches, despliegue remoto de SW, despliegue de imágenes de SO y Appl, Gestión de HW, SW & Licencias. · 15 horas de soporte técnico post-instalación para realizar tareas no relacionadas con trámites de garantías como: modificación de la configuración, resolución de consultas, talleres de trabajo.	15,81	23.715,00
Nota: El precio no incluye el IVA.		**Suman**	23.715,00

Antivirus Kaspersky: Opc. 2 años

Señores

Universidad Nacional de Loja
martes, 03 de junio de 2014

Cant.	Descripción	Unitario	Total
1500	Kaspersky Endpoint Security for Business Protección KESB de nivel **"Total"** corporativo **Licencia Académica** con garantía técnica de **2 años** que incluye: · Actualización de Software y Firmas de Malware · Soporte técnico de fábrica a través de la Web Protección activa para servidores y estaciones de trabajo Windows, Mac, Linux y dispositivos móviles (teléfonos inteligentes) Seguridad de Archivos, Control de aplicaciones, Control de Dispositivos, Control Web, Anti-malware + Firewall Manejo de licencias, Admisión de Red (NAC), Instalación de Software Aprovisionamiento de imágenes, Manejo de parches, Escaneo de Vulnerabilidades, Protección antimalware para: Control antimalware en el Gateway como AddOn en: · Gateway de navegación Web · Gateway de Correo Electrónico · Gateway de Colaboración con MS SharePoint Incluye kit de administración para gestión de clientes centralizado. La licencia del producto sostiene el número de equipos declarados. Es importante no rebasar este número para evitar la revocación del acuerdo. Servicios Profesionales de Valor Agregado y vigencia tecnológica: · Instalación y configuración de 1 kit de Administración o Kaspersky Security Center 9: Un servidor principal y otro esclavo · Instalación hasta de 10 clientes físicos con puntos finales Kaspersky Endpoint 8 conectados a la consola de gestión · Instalación en modo de taller a fin de proporcionar una transferencia de conocimientos al personal técnico del cliente. · Configuración para gestión de Parches, despliegue remoto de SW, despliegue de imágenes de SO y Appl, Gestión de HW, SW & Licencias. · 30 horas de soporte técnico post-instalación para realizar tareas no relacionadas con trámites de garantías como: modificación de la configuración, resolución de consultas, talleres de trabajo.	20,19	30.285,00
Nota: El precio no incluye el IVA.		**Suman**	30.285,00

Antivirus Kaspersky: Opc. 3 años

Señores

Universidad Nacional de Loja
martes, 03 de junio de 2014

Cant.	Descripción	Unitario	Total
1500	Kaspersky Endpoint Security for Business Protección KESB de nivel **"Total"** corporativo **Licencia Académica** con garantía técnica de 3 **años** que incluye: · Actualización de Software y Firmas de Malware · Soporte técnico de fábrica a través de la Web Protección activa para servidores y estaciones de trabajo Windows, Mac, Linux y dispositivos móviles (teléfonos inteligentes) Seguridad de Archivos, Control de aplicaciones, Control de Dispositivos, Control Web, Anti-malware + Firewall Manejo de licencias, Admisión de Red (NAC), Instalación de Software Aprovisionamiento de imágenes, Manejo de parches, Escaneo de Vulnerabilidades, Protección antimalware para: Control antimalware en el Gateway como AddOn en: · Gateway de navegación Web · Gateway de Correo Electrónico · Gateway de Colaboración con MS SharePoint Incluye kit de administración para gestión de clientes centralizado. La licencia del producto sostiene el número de equipos declarados. Es importante no rebasar este número para evitar la revocación del acuerdo. Servicios Profesionales de Valor Agregado y vigencia tecnológica: · Instalación y configuración de 1 kit de Administración o Kaspersky Security Center 9: Un servidor principal y otro esclavo · Instalación hasta de 10 clientes físicos con puntos finales Kaspersky Endpoint 8 conectados a la consola de gestión · Instalación en modo de taller a fin de proporcionar una transferencia de conocimientos al personal técnico del cliente. · Configuración para gestión de Parches, despliegue remoto de SW, despliegue de imágenes de SO y Appl, Gestión de HW, SW & Licencias. · 45 horas de soporte técnico post-instalación para realizar tareas no relacionadas con trámites de garantías como: modificación de la configuración, resolución de consultas, talleres de trabajo.	29,77	44.655,00
Nota: El precio no incluye el IVA.		**Suman**	44.655,00

VIGENCIA TECNOLÓGICA

Dentro de los precios indicados, se incorpora la aplicación de los principios de vigencia tecnológica establecidos en el decreto ejecutivo No. 1515 y Resolución INCOP No. 85-2013, según se detalla a continuación:

APLICACIÓN DE VIGENCIA TECNOLÓGICA	
Todos las licencias a entregarse deben ser nuevas es decir sin uso	Las licencias serán sin uso y tendrán una suscripción con cobertura durante el tiempo registrado.
Mantenimiento para actualización de Software durante el tiempo de vigencia de la garantía de las licencias	Durante la vigencia de la garantía de las licencias ofrecidas, se deberá contar con la posibilidad de cambiar y actualizar la versión del software sin costo adicional, así como del repositorio de firmas de malware identificado como nuevo. Para cumplir con ésta actualización el Cliente deberá utilizar los procesos y configuraciones especificados por el fabricante en el portal Web de Kaspersky y soporte técnico incluidos.
Mantenimiento correctivo, aplicable a la garantía de los equipos, durante el tiempo de vigencia de la garantía de los equipos	No se aplica en este proceso, porque es para licenciamiento software.
Tiempo y condiciones para la reposición temporal o definitiva de equipos	No se aplica en este proceso, porque es para licenciamiento de software. En caso de fallo del servidor de la consola de administración, el cliente deberá poner en marcha sus procesos de contingencia internos.
Vigencia de la garantía técnica durante la vida útil de las licencias.	La garantía técnica de las licencias está especificada en cada caso dentro de la oferta. Se asume que el tiempo de vida útil de cada equipo corresponde al tiempo de vigencia de la garantía técnica.
Garantía técnica.	CORESOLUTIONS S.A., traslada la garantía que el fabricante, Kaspersky ofrece sobre sus productos. Se adjunta a la presente oferta el documento denominado "CONTRATO DE LICENCIA DE USUARIO FINAL DE KASPERSKY LAB", en el que se especifica las condiciones en las que se provee el producto, CORESOLUTIONS S.A., traslada al Cliente todos los términos y condiciones señalados en este documento. Al tratarse de un producto de software CORESOLUTIONS S.A., no puede agregar ni excluir ninguna condición de la garantía del fabricante señalado en el documento que se adjunta.
Servicio post-instalación	La oferta incorpora un paquete de horas de servicio post-instalación, las cuales podrán ser usadas por el cliente para solicitar soporte en tareas no relacionadas con trámites de garantía, tales como: mantenimientos no programados, talleres de trabajo para capacitación, cambio de configuraciones, determinación de problemas, reubicación de equipos, asesoramiento y consultoría sobre el uso de la plataforma, y/o cualquier otro servicio que el cliente requiera y que CORESOLUTIONS S.A., esté en capacidad de ofrecer
Documentación	Se entregará la documentación que el fabricante incluya con los productos que se entreguen. Documentación adicional se encuentra disponible en los sitios web de los fabricantes

22. Certificación de Trabajo con la Lcda. Mabel Rodríguez – Encargada de la Sección Mantenimiento Electrónico de la UTI.

Universidad Nacional de Loja
Área de la Energía, las Industrias y los Recursos Naturales No Renovables
Carrera de Ingeniería en Sistemas

Como estudiante Investigador de la Carrera de Ingeniería en Sistemas, con el fin de evaluar el proyecto de implementación del programa Antivirus Kaspersky con Licencias Corporativas para la UNL propuesto por la Empresa CoreSolutions S.A.; se ha procedido a recabar información, mediante entrevista, con la Lcda. Mabel Rodríguez Encargada de la Sección de Mantenimiento Electrónico de la UTI-UNL. Así mismo, es importante mencionar que se fue participe de la instalación, configuración y demostración del funcionamiento de Kaspersky Antivirus, realizado en el Dpto. antes indicado dirigido por el Sr. Ricardo Villa, Consultor TI de GSM de la Ciudad de Guayaquil. Toda la información obtenida es de gran importancia para fundamentación de mi Trabajo de Titulación, denominado: **"Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios".** Dentro de los temas tratados y analizados se pueden mencionar los siguientes:

- Instalación y configuración de la consola de administración centralizada y de los equipos finales en sus dos versiones (Kaspersky Enpoint Security 10 y Kaspersky Antivirus 6).
- Demostración del funcionamiento del programa Antivirus desde la consola de administración.
- Detección del estado de los equipos con Kaspersky Antivirus conectados a la red.
- Generación de Reportes Generalizados de los equipos con Kaspersky Antivirus conectados a la red.

Lcda. Mabel Rodríguez
ENCARGADA DE LA SECCIÓN
MANTENIMIENTO ELECTRONICO UTI-UNL

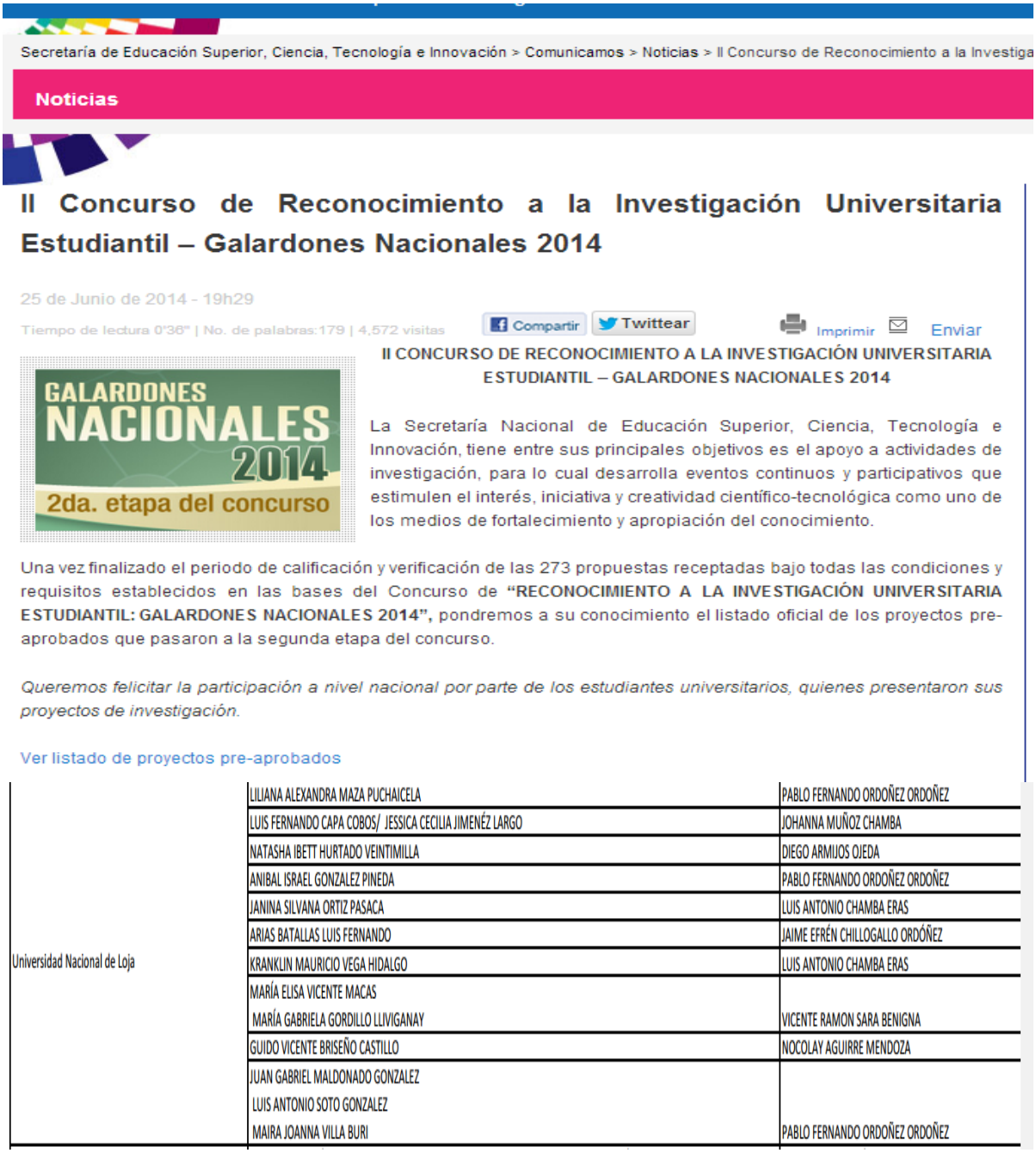
Egdo. Franklin Vega Hidalgo
TESISTA CIS-UNL

Figura 65: Anexo 22- Certificación de Trabajo con la Lcda. Mabel Rodríguez – Encargada de la Sección Mantenimiento Electrónico de la UTI.

23. Propuesta del Modelo Creado al “II Concurso de Reconocimiento a la Investigación Universitaria – Galardones 2014”

Figura 66: Anexo 23- Propuesta del Modelo al “II Concurso de Reconocimiento a la Investigación Universitaria-Galardones 2014”

24. Clasificación del Proyecto con el Modelo Propuesto en el "II Concurso de Reconocimiento a la Investigación Universitaria – Galardones 2014"



Secretaría de Educación Superior, Ciencia, Tecnología e Innovación > Comunicamos > Noticias > II Concurso de Reconocimiento a la Investiga

Noticias

II Concurso de Reconocimiento a la Investigación Universitaria Estudiantil – Galardones Nacionales 2014

25 de Junio de 2014 - 19h29

Tiempo de lectura 0'36" | No. de palabras:179 | 4,572 visitas Compartir Twittear Imprimir Enviar

II CONCURSO DE RECONOCIMIENTO A LA INVESTIGACIÓN UNIVERSITARIA ESTUDIANTIL – GALARDONES NACIONALES 2014

La Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación, tiene entre sus principales objetivos es el apoyo a actividades de investigación, para lo cual desarrolla eventos continuos y participativos que estimulen el interés, iniciativa y creatividad científico-tecnológica como uno de los medios de fortalecimiento y apropiación del conocimiento.

Una vez finalizado el periodo de calificación y verificación de las 273 propuestas receptadas bajo todas las condiciones y requisitos establecidos en las bases del Concurso de **"RECONOCIMIENTO A LA INVESTIGACIÓN UNIVERSITARIA ESTUDIANTIL: GALARDONES NACIONALES 2014"**, pondremos a su conocimiento el listado oficial de los proyectos pre-aprobados que pasaron a la segunda etapa del concurso.

Queremos felicitar la participación a nivel nacional por parte de los estudiantes universitarios, quienes presentaron sus proyectos de investigación.

Ver listado de proyectos pre-aprobados

Universidad Nacional de Loja	LILIANA ALEXANDRA MAZA PUCHAICELA	PABLO FERNANDO ORDOÑEZ ORDOÑEZ
	LUIS FERNANDO CAPA COBOS/ JESSICA CECILIA JIMENÉZ LARGO	JOHANNA MUÑOZ CHAMBA
	NATASHA IBETT HURTADO VEINTIMILLA	DIEGO ARMIJOS OJEDA
	ANIBAL ISRAEL GONZALEZ PINEDA	PABLO FERNANDO ORDOÑEZ ORDOÑEZ
	JANINA SILVANA ORTIZ PASACA	LUIS ANTONIO CHAMBA ERAS
	ARIAS BATALLAS LUIS FERNANDO	JAIME EFRÉN CHILLOGALLO ORDÓÑEZ
	KRANKLIN MAURICIO VEGA HIDALGO	LUIS ANTONIO CHAMBA ERAS
	MARÍA ELISA VICENTE MACAS MARÍA GABRIELA GORDILLO LLIVIGANAY	VICENTE RAMON SARA BENIGNA
	GUIDO VICENTE BRISEÑO CASTILLO	NOCOLAY AGUIRRE MENDOZA
	JUAN GABRIEL MALDONADO GONZALEZ LUIS ANTONIO SOTO GONZALEZ MAIRA JOANNA VILLA BURI	PABLO FERNANDO ORDOÑEZ ORDOÑEZ

Figura 67: Anexo 24- Clasificación del Proyecto en Concurso Senescyt.

25. Sugerencia a Coresolutions S.A. sobre la confiabilidad que mantiene su sitio Web, mediante WOT.

Sugerencia Propuesta Kaspersky - UNL

Franklin Mauricio Vega Hidalgo <fmvegah@unl.edu.ec> 9:07 (hace 5 minutos)

para Olmedo

Buen día Olmedo, con el motivo de agradecerle por la información brindada en lo que respecta a la propuesta de Kaspersky hacia la Universidad Nacional de Loja. Me veo en la necesidad de comunicarle que su propuesta e encuentra en proceso de evaluación mediante un modelo de confianza que otorga nivel de confiabilidad para la implementación de dicha herramienta, en donde se ha tomado en cuenta algunos criterios, de lo cual se ha creído conveniente sugerirle a su empresa indagar acerca de WOT: https://www.mywot.com/ (Confianza en la Web). Herramienta que muestra cuáles son los sitios Webs en los se puede confiar basándose en experiencias de millones de usuarios, permitiéndoles así tener un nivel de reputación más alta ya que Kaspersky en sí mantiene un alto nivel de confiabilidad en su sitio oficial y la empresa comercializadora no. Luego de emitirle la sugerencia indicada, indico que se estableció contacto con el Técnico de GSM (Guayaquil) y se ha procedido a la instalación del DEMO de Kaspersky, actualmente el departamento encargado se encuentra probando la herramienta con el fin de garantizar el correcto funcionamiento dentro de la red universitaria. Cualquier novedad se la hará conocer, deseándole éxitos en sus labores diarias, me suscribo.

-

"El que persevera, alcanza."

franklinvh28@gmail,com
franklinvh_17@hotmail.com
frankmauri_28@yahoo.es
franklinvh28.wordpress.com
FranklinMauricioVH28
@franklinvh28

Figura 68: Anexo 25- Sugerencia de WOT a CoreSolutions S.A.

26. Declaración de Confidencialidad

DECLARACION DE CONFIDENCIALIDAD

Franklin Mauricio Vega Hidalgo (en adelante: el declarante), C.I: 0705375178.
DECLARA lo siguiente:

PRIMERO: Antecedentes

1. El declarante va a participar y ha participado en el trabajo de titulación “Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios”, dirigido por el Ing. Luis Antonio Chamba Eras, en calidad de director de trabajo.
2. Por el presente documento se regula el tratamiento que el declarante ha de dar la información a la que pueda tener acceso en el desarrollo de las tareas de investigación que se realicen en dicho trabajo, el cual se regulará por las disposiciones contenidas en las clausulas siguientes.

SEGUNDO: Información Confidencial

La información referida a materiales, métodos y resultados científicos técnicos y comerciales utilizados u obtenidos durante la realización del trabajo de investigación o una vez realizado el mismo, se considerara siempre Información Confidencial.

TERCERO: Excepciones

No será considerada como información confidencial:

a) La información que el declarante pueda probar que tenía en su legítima posesión con anterioridad al conocimiento de la Información Confidencial.

b) La información que el declarante pueda probar que era de dominio público en la fecha de divulgación o pase a serlo, con posterioridad, por haberse publicado o por otro medio, sin intervención ni negligencia del declarante.

c) La información que el declarante pueda probar que corresponde en esencia a información facilitada por terceros, sin restricción alguna sobre su divulgación, en virtud de un derecho del declarante a recibirla.

CUARTO: Secreto de la Información Confidencial

El declarante se compromete a mantener totalmente en Secreto la Información Confidencial recibida en relación con el trabajo referido anteriormente y no divulgarla a terceros durante la vigencia de esta Declaración de Confidencial

Así mismo, el declarante se compromete a emplear la Información Confidencial, exclusivamente, en el desempeño de las tareas que tenga encomendadas en dicho trabajo.

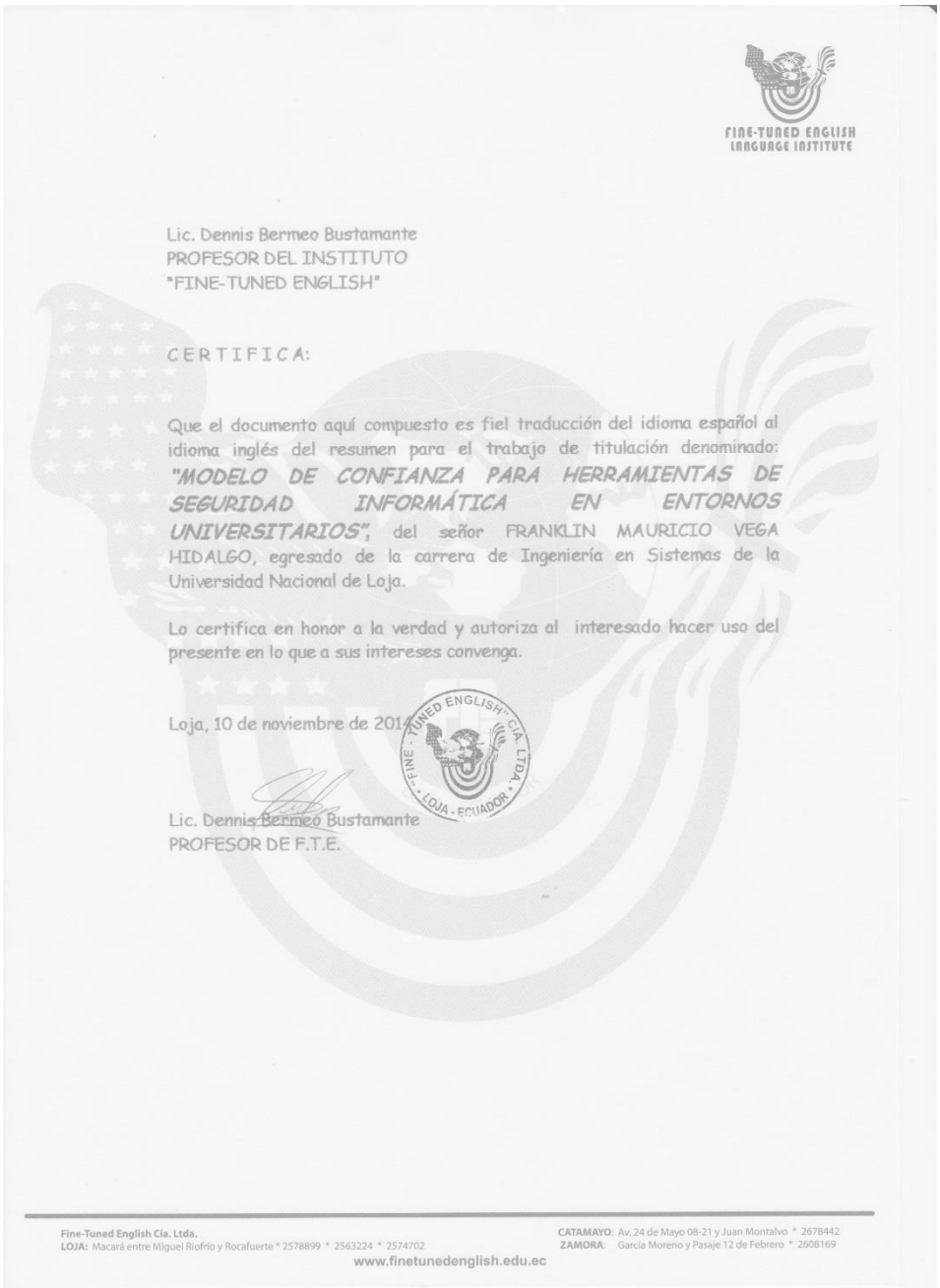
QUINTO: Duración

La obligación del declarante respecto al mantenimiento del compromiso de Secreto de la Información Confidencial, será indefinido para fines de investigación a partir de la fecha de recepción de la Información Confidencial.

Loja, Noviembre 2014

Franklin Mauricio Vega Hidalgo

27. Certificación de Traducción



FINE-TUNED ENGLISH
LANGUAGE INSTITUTE

Lic. Dennis Bermeo Bustamante
PROFESOR DEL INSTITUTO
"FINE-TUNED ENGLISH"

CERTIFICA:

Que el documento aquí compuesto es fiel traducción del idioma español al idioma inglés del resumen para el trabajo de titulación denominado: ***"MODELO DE CONFIANZA PARA HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN ENTORNOS UNIVERSITARIOS"***, del señor FRANKLIN MAURICIO VEGA HIDALGO, egresado de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja.

Lo certifica en honor a la verdad y autoriza al interesado hacer uso del presente en lo que a sus intereses convenga.

Loja, 10 de noviembre de 201

FINE - TUNED ENGLISH CIA. LTDA. LOJA - ECUADOR

Lic. Dennis Bermeo Bustamante
PROFESOR DE F.T.E.

Fine-Tuned English Cía. Ltda.
LOJA: Macará entre Miguel Riofrío y Rocafuerte * 2578899 * 2563224 * 2574702
CATAMAYO: Av. 24 de Mayo 08-21 y Juan Montalvo * 2678442
ZAMORA: García Moreno y Pasaje 12 de Febrero * 2608169
www.finetunedenglish.edu.ec

Figura 69: Anexo 27- Certificación de Traducción.

28. Interfaces del DEMO de Kaspersky Antivirus

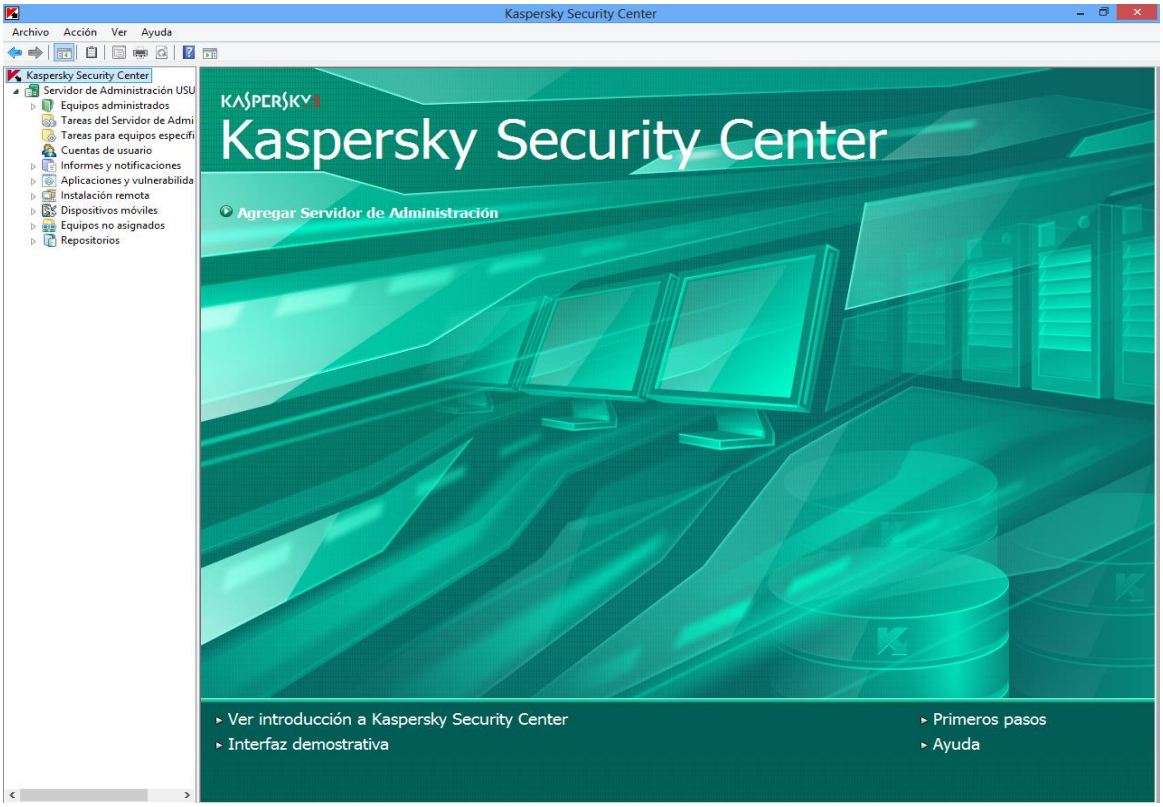


Figura 70: Anexo 28- Interfaz de Consola de Administración Kaspersky.

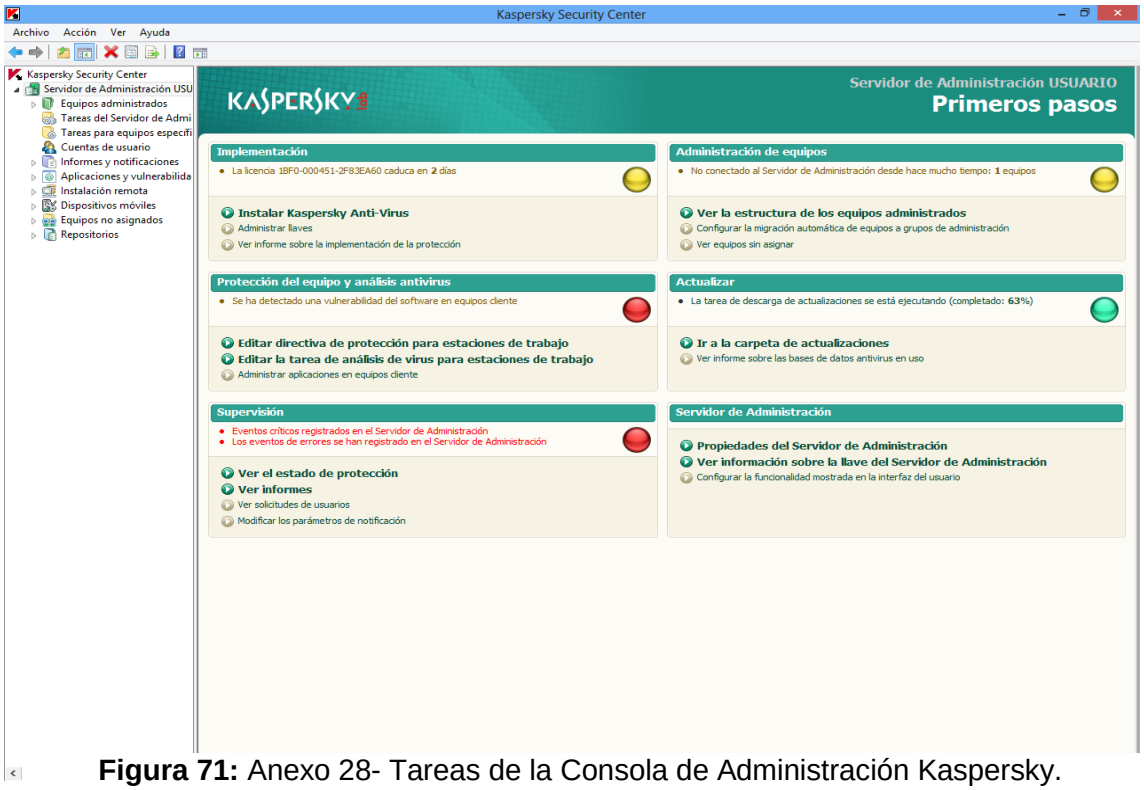


Figura 71: Anexo 28- Tareas de la Consola de Administración Kaspersky.

Figura 72: Anexo 28- Grupos de Equipos Administrados Kaspersky.

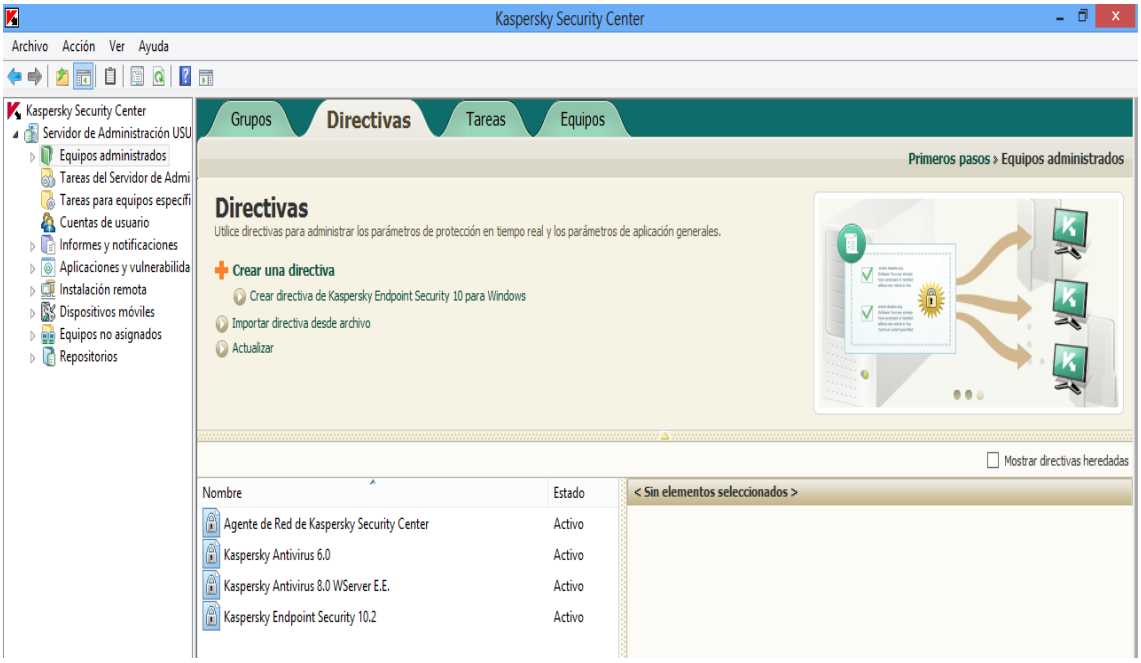


Figura 73: Anexo 29- Directivas para los Grupos Administrados Kaspersky.

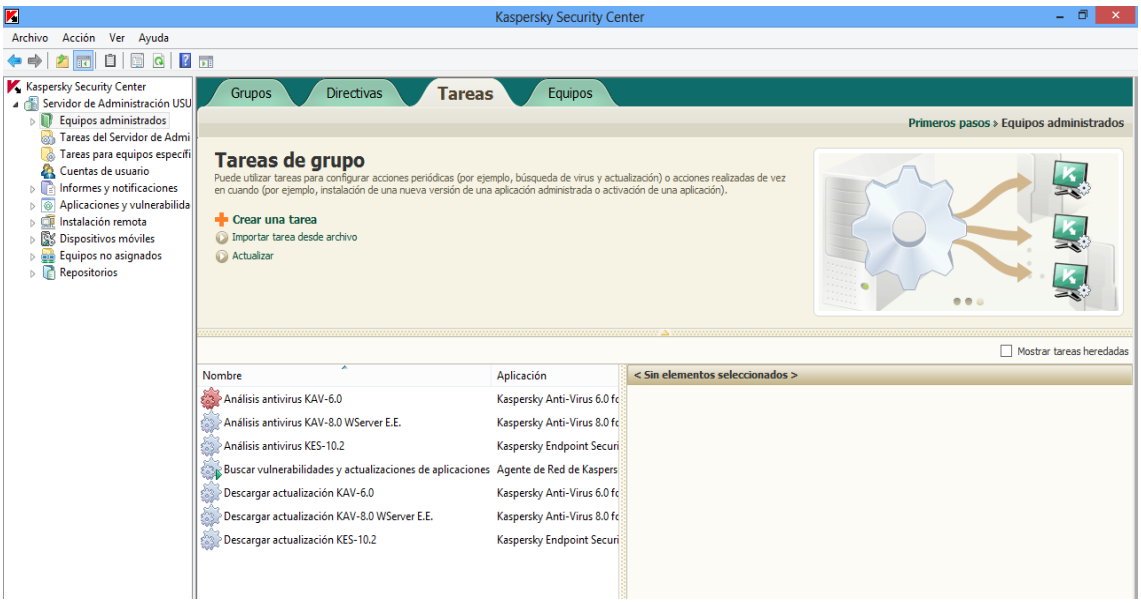


Figura 74: Anexo 28- Tareas de Grupos Administrados Kaspersky.

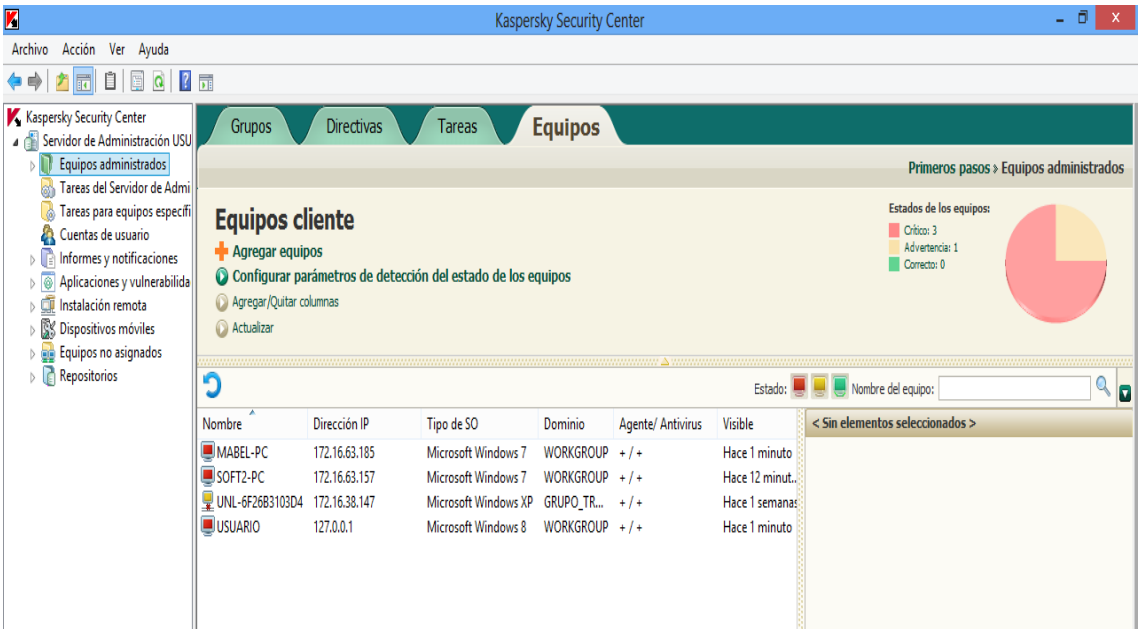


Figura 75: Anexo 28- Equipos Cliente Administrados Kaspersky.

Figura 76: Anexo 28- Tareas del Servidor de Administración Kaspersky.

Figura 77: Anexo 28- Tareas para Equipos Específicos Kaspersky.

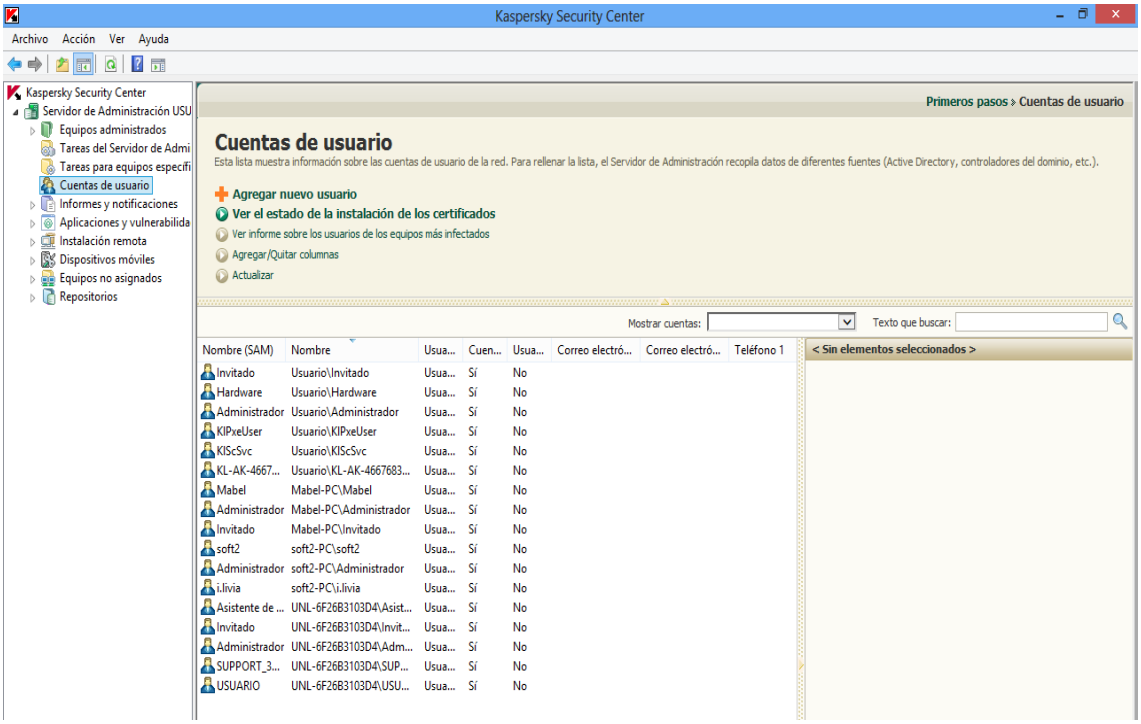


Figura 78: Anexo 28- Cuentas de Usuario Administradas por Kaspersky.

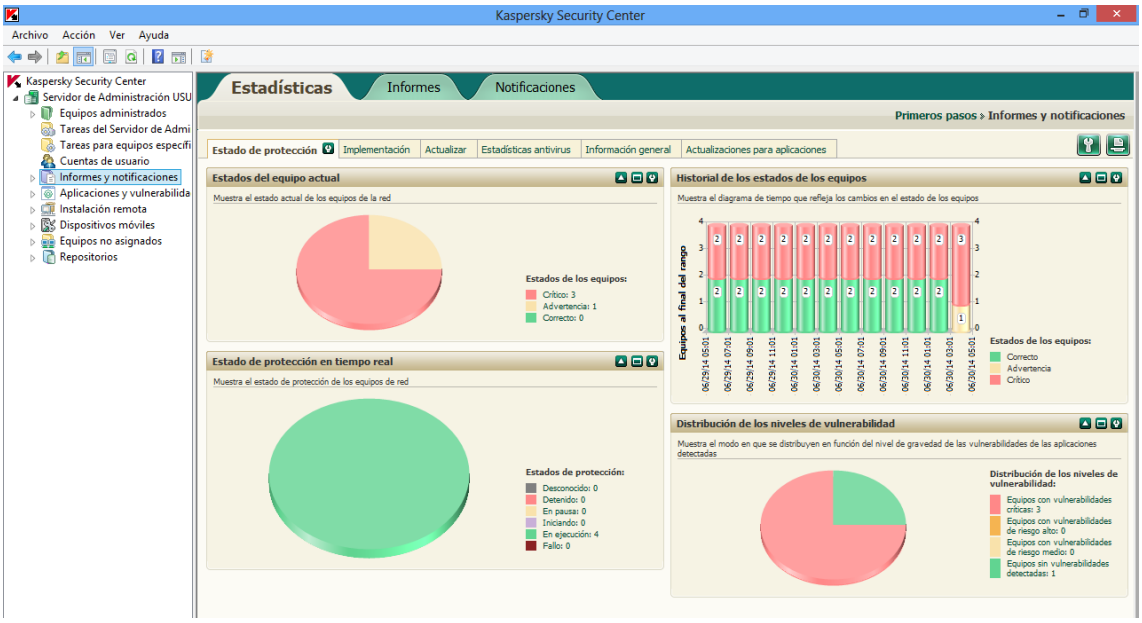


Figura 79: Anexo 28- Estadísticas de Administración Kaspersky.

Figura 80: Anexo 28- Informes Kaspersky.

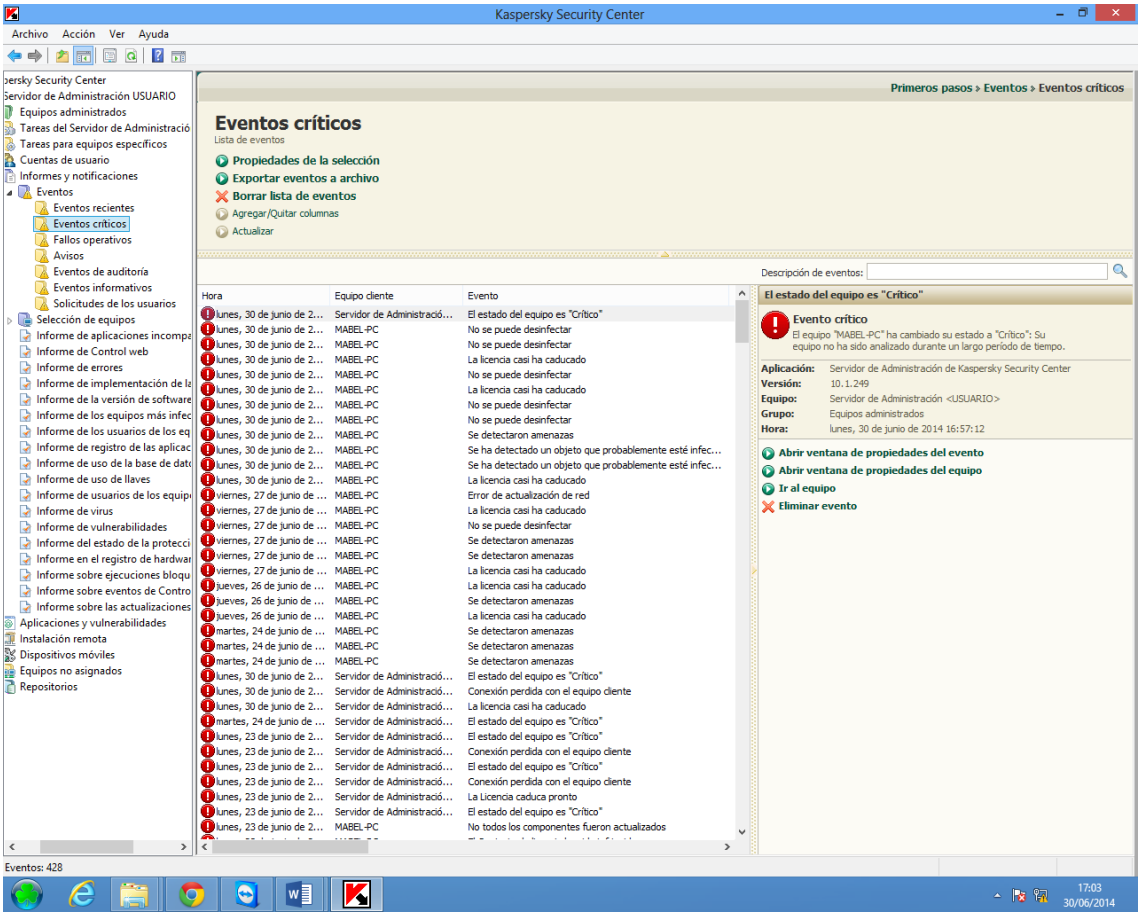


Figura 81: Anexo 28- Eventos Críticos Kaspersky.

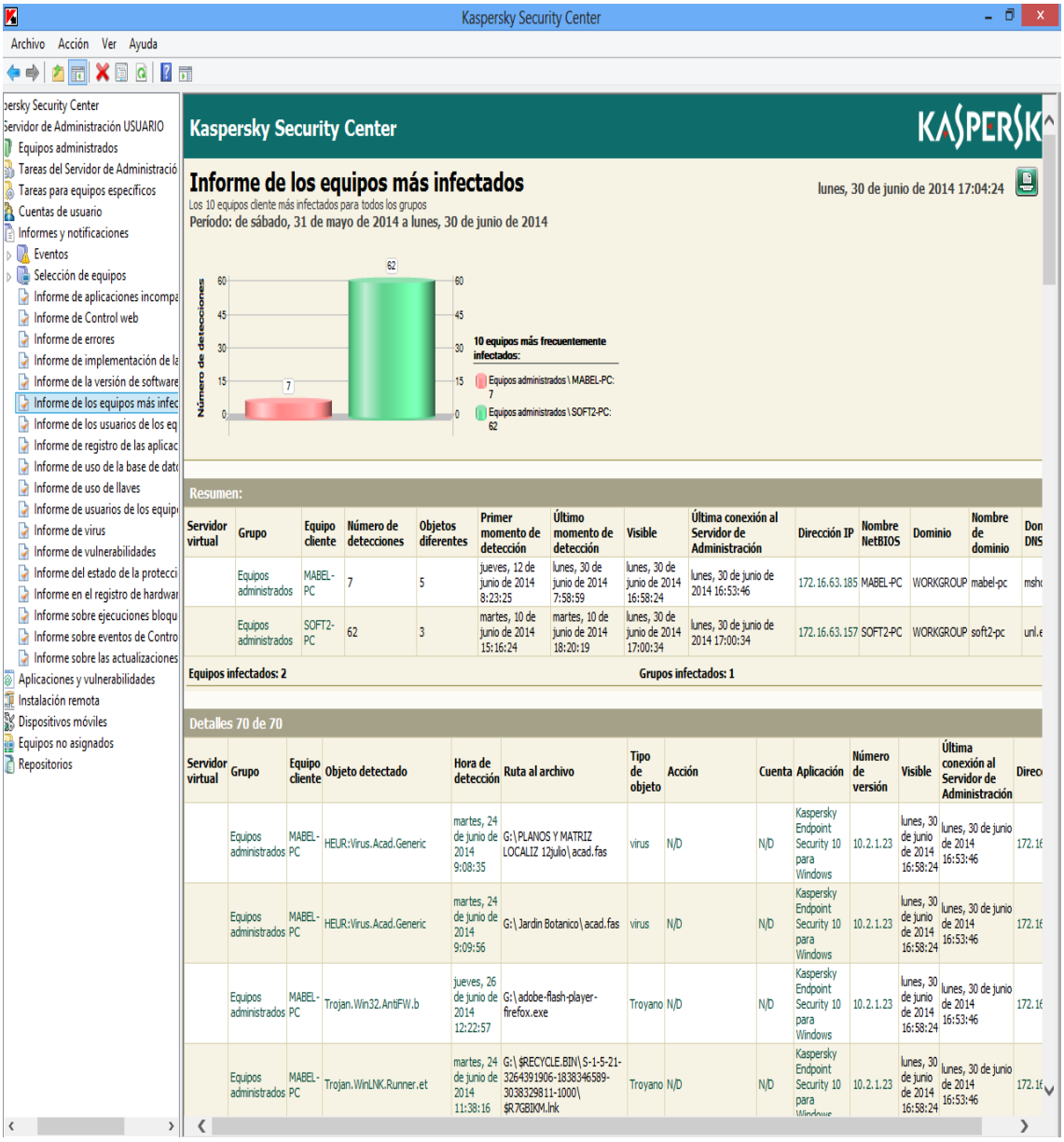


Figura 82: Anexo 28- Informe de Equipos más Infectados Kaspersky.

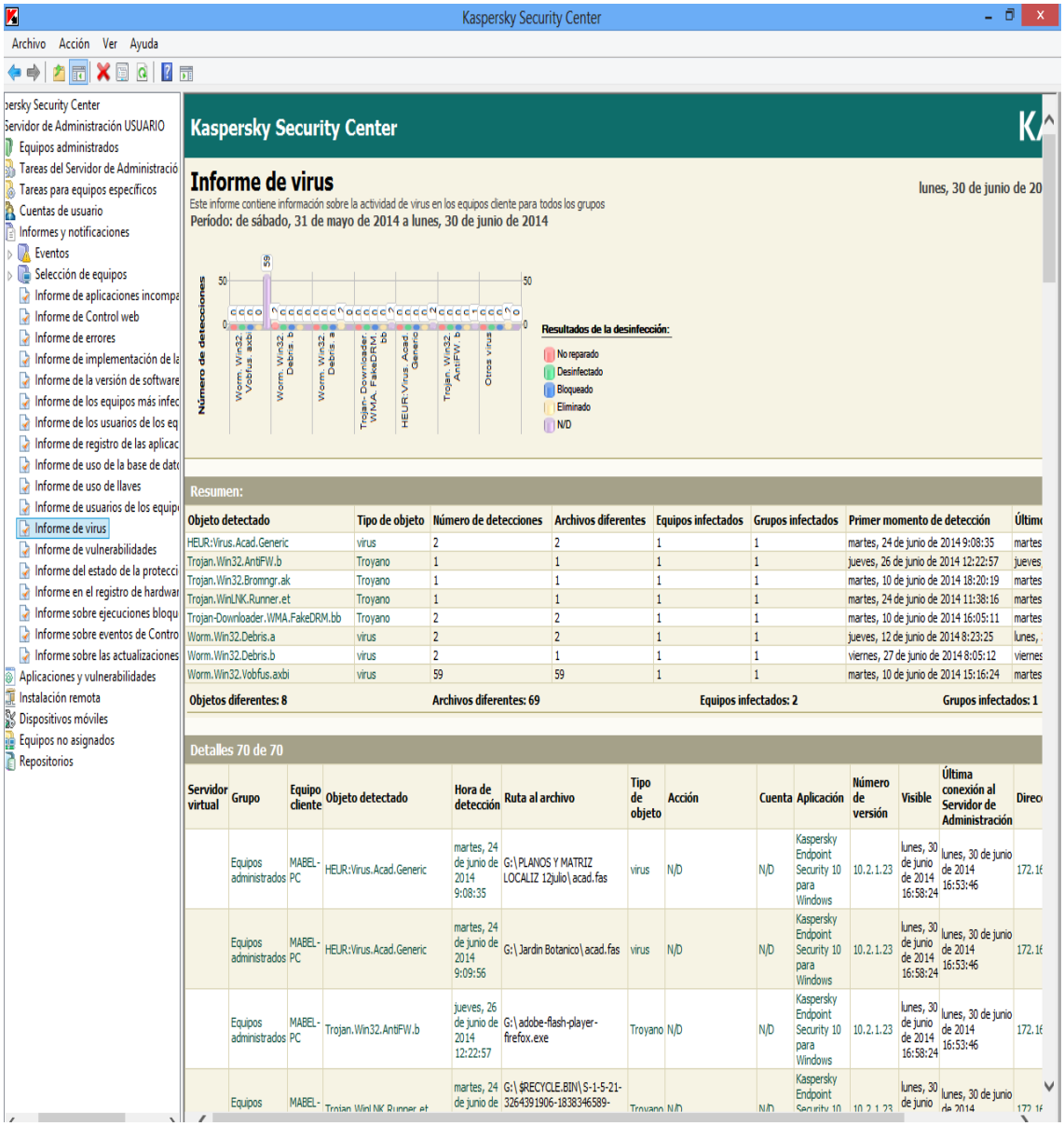


Figura 83: Anexo 28- Informe de Virus Kaspersky.

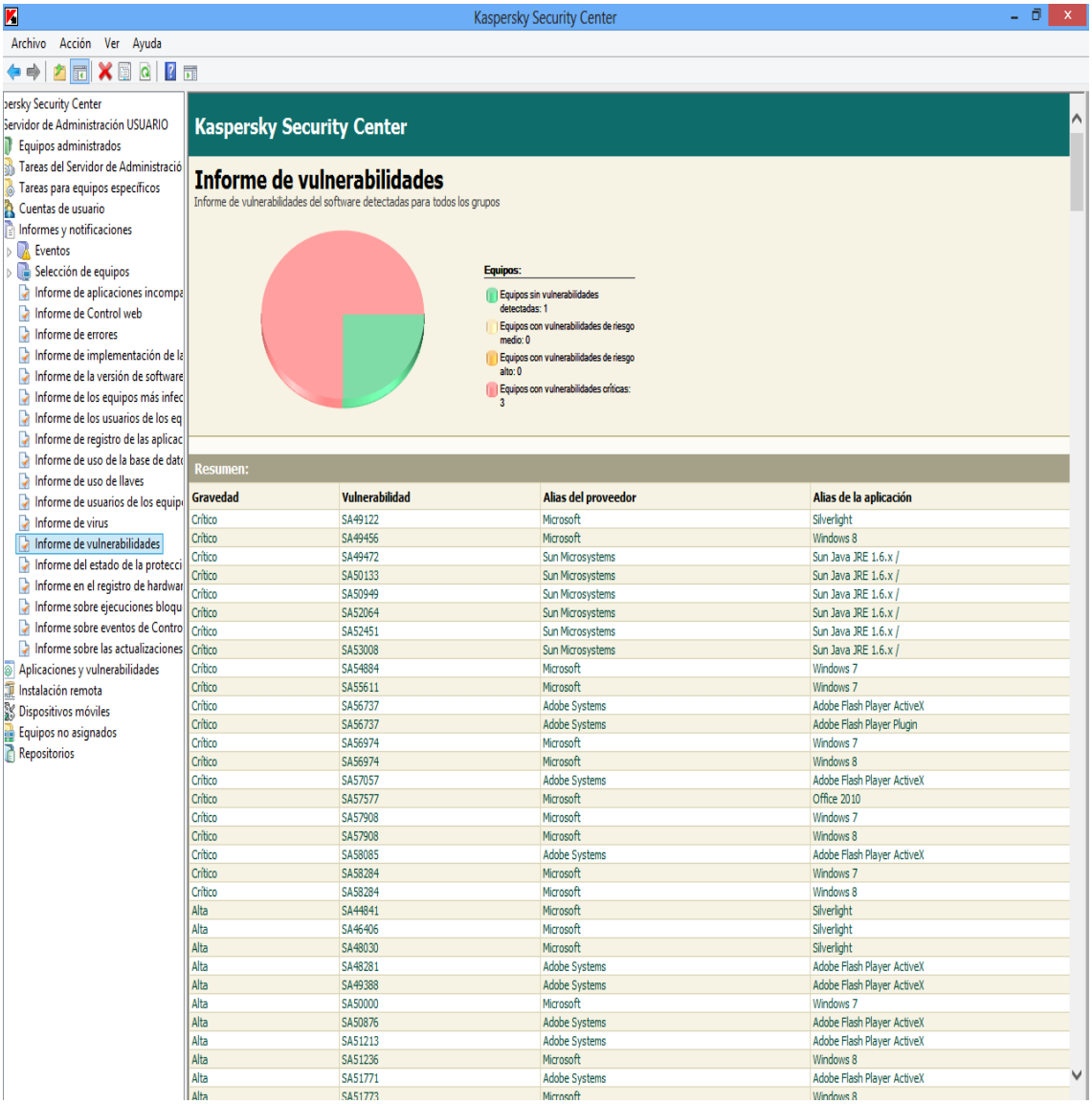


Figura 84: Anexo 28- Informe de Vulnerabilidades Kaspersky.

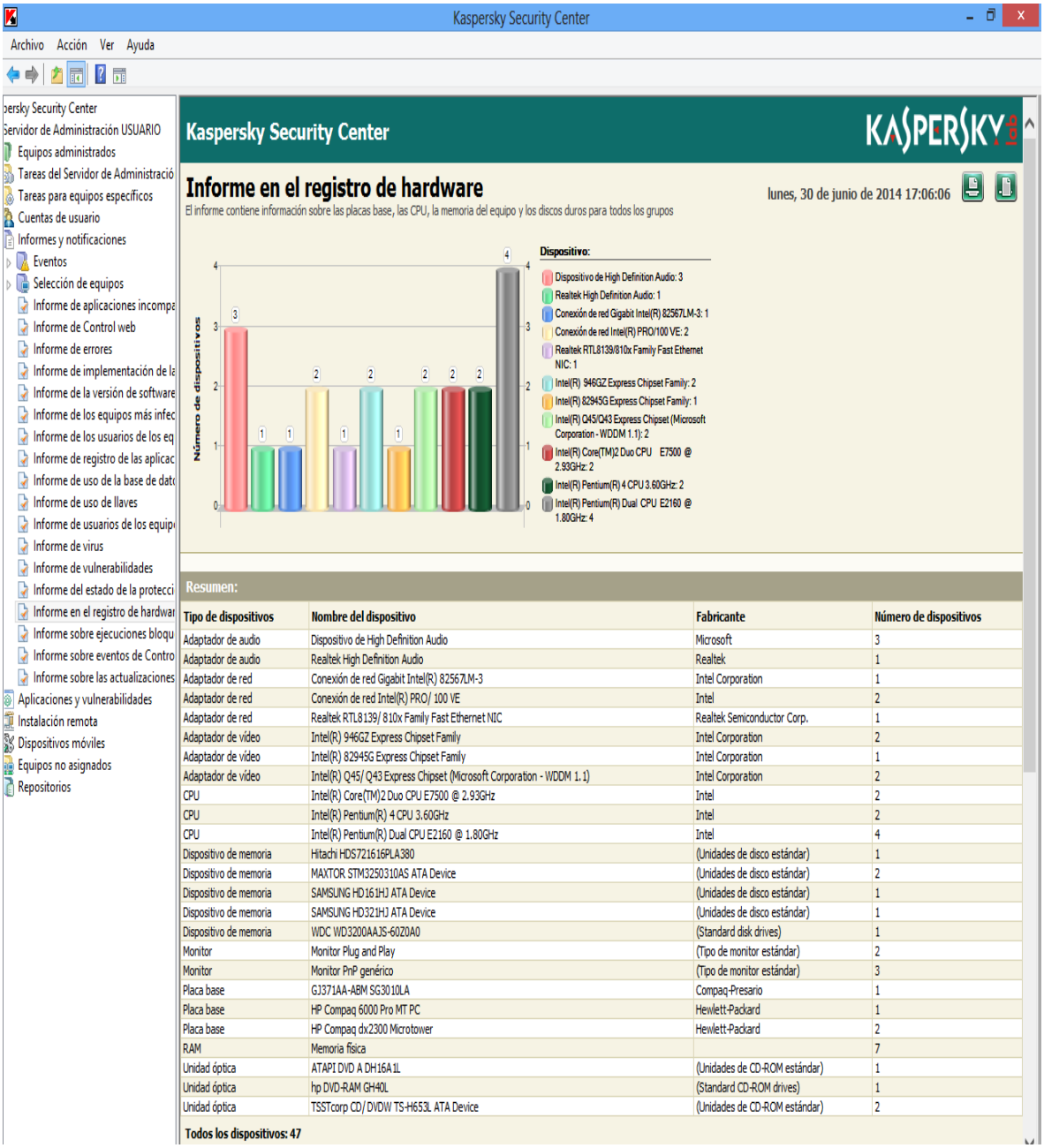


Figura 85: Anexo 28- Informe en el Registro Hardware Kaspersky – Parte1.

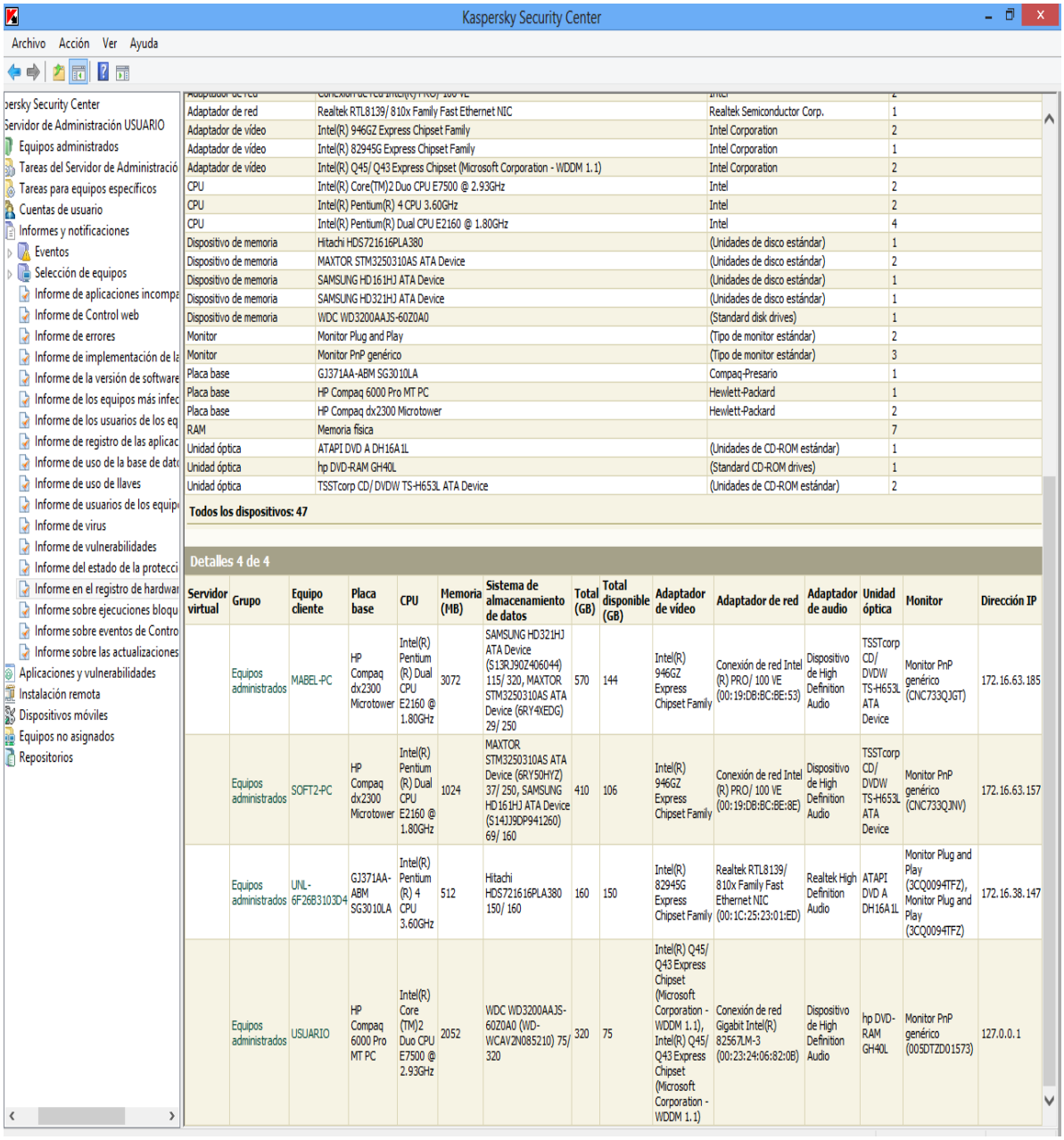


Figura 86: Anexo 28- Informe en el Registro Hardware Kaspersky – Parte2.

Figura 87: Anexo 28- Instalación Remota Kaspersky.

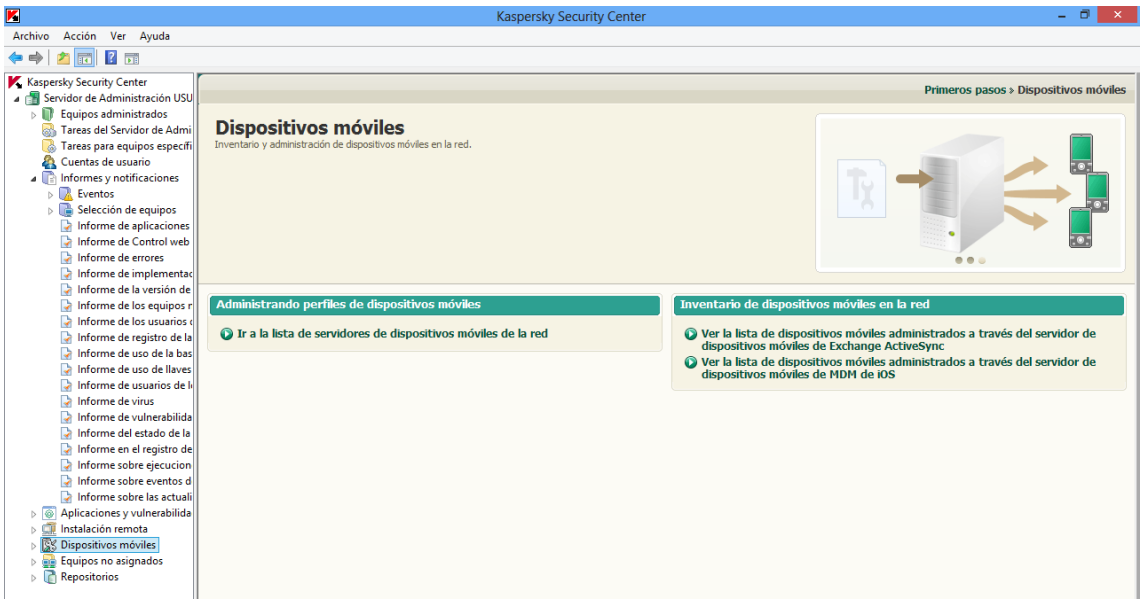


Figura 88: Anexo 28- Dispositivos Móviles Kaspersky.

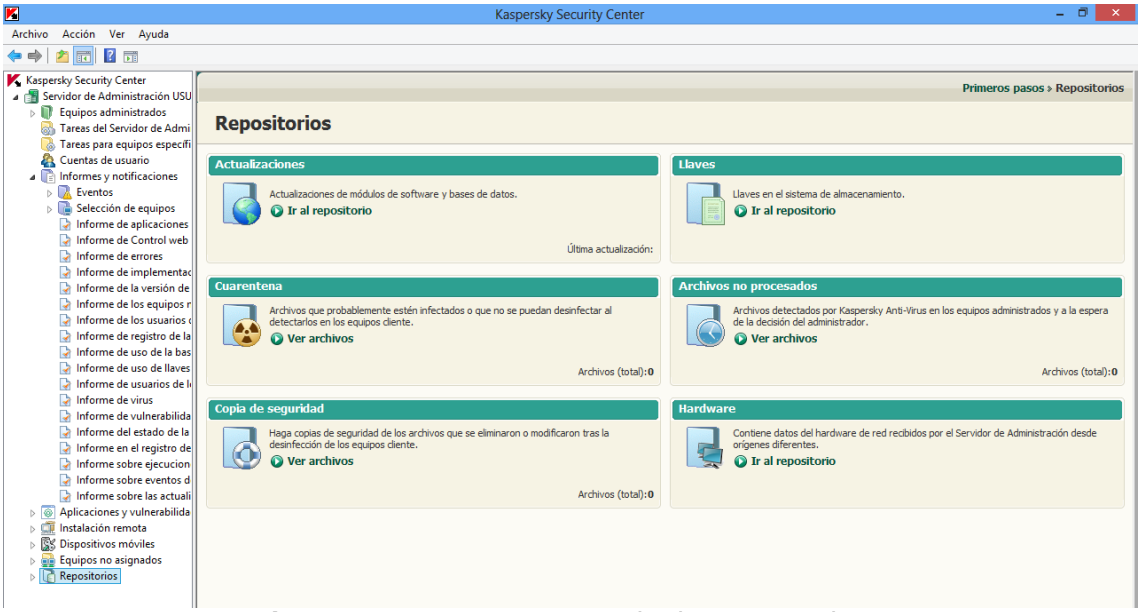


Figura 89: Anexo 28- Repositorios Kaspersky.

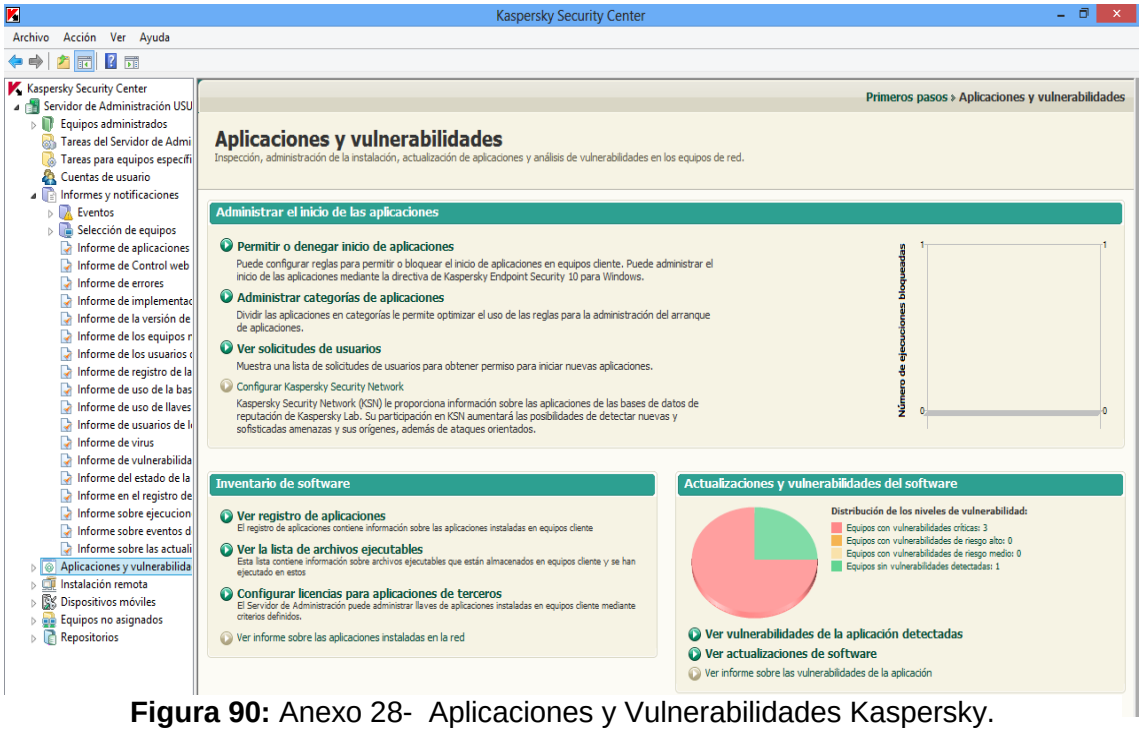


Figura 90: Anexo 28- Aplicaciones y Vulnerabilidades Kaspersky.

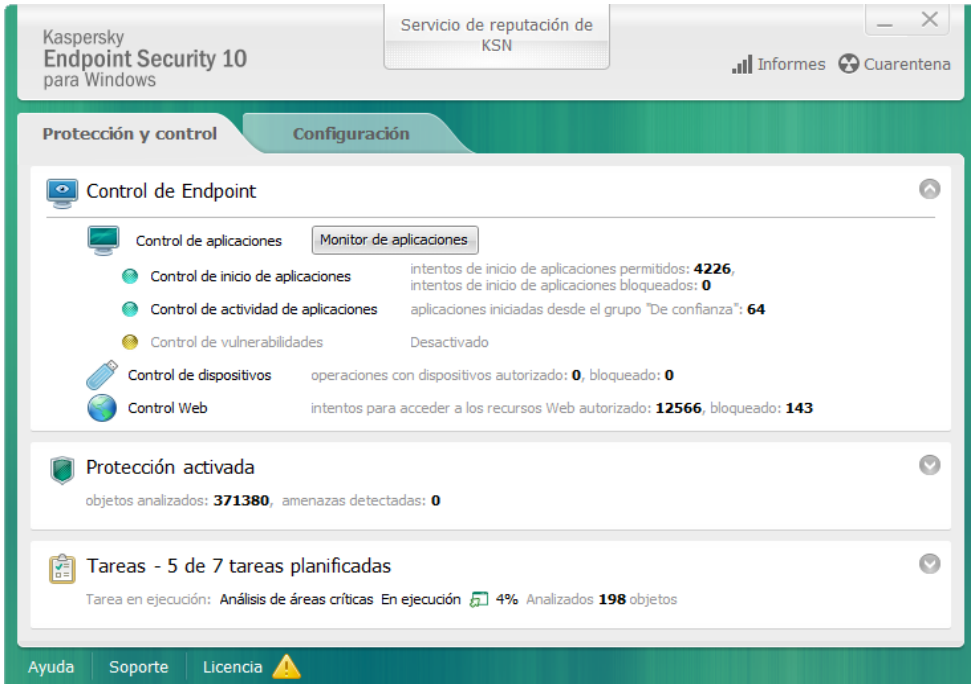


Figura 91: Anexo 28- Interfaz Kaspersky Endpoint Security 10 – Parte1.

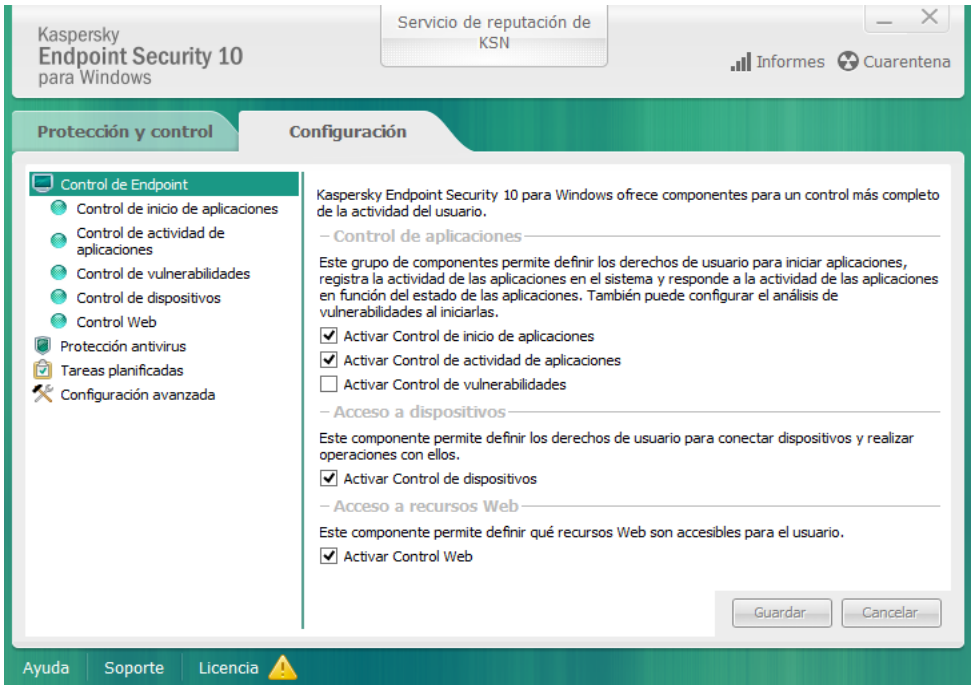


Figura 92: Anexo 28- Interfaz Kaspersky Endpoint Security 10 – Parte2.

29. Políticas Unidad de Telecomunicaciones e Información UTI – Universidad Nacional de Loja

UNIVERSIDAD NACIONAL DE LOJA

POLÍTICAS UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

INTRODUCCIÓN

El presente documento define el conjunto de Políticas de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, que regirán durante el periodo 2012.

Las políticas presentadas en este documento se enmarcan dentro del reglamentación establecido por la Institución, que respecto de estas áreas considera:

La definición de los objetivos, políticas y planes informáticos, deben estar siempre acorde a los objetivos, políticas y planes que la Universidad tenga respecto de su acción como entidad educacional.

Los objetivos, planes y políticas, deberán estar supervisadas y aprobadas por la Dirección de Telecomunicaciones e Información. Todo cambio o alteración debe ser informado y respaldado por las mismas autoridades.

La Unidad de Telecomunicaciones e Información se define como el área de servicios que tiene como clientes todas las áreas de nuestra Universidad Nacional de Loja e incluyendo la MED.

La Unidad de Telecomunicaciones e Información deberá cautelar los bienes muebles e inmuebles de la Universidad que le sean de su competencia, dentro de los cuales se consideran los datos e información que le sean confiados para su protección, administración, operación, revisión, adaptación y en general, toda acción relacionada con las funciones que al departamento le son propias.

Toda acción de incorporación de tecnología y servicios informáticos para la Universidad Nacional de Loja, se debe realizar bajo las normativas establecidas en los procesos de adquisición de equipos y recursos informáticos.

Establecer, de acuerdo a los marcos legales existentes los contratos para cada servicio que lo requiera (Internet.....); los que deberán tener una duración tal que asegure la continuidad y calidad del servicio.

Las políticas institucionales de seguridad informática de la CCSS están basadas en lo establecido en la "Norma ISO/IEC 17799:2000 la cual es un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información", dicha norma ofrece recomendaciones en la gestión de la seguridad de la información, y define la Seguridad de la Información como la preservación de la confidencialidad, integridad y disponibilidad. A continuación se definen dichos conceptos:

1. Confidencialidad: aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.
2. Integridad: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
3. Disponibilidad: aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Este documento contiene una serie de políticas que deberán ser acatadas por los funcionarios, docentes y estudiantes de la Universidad Nacional de Loja.

La Universidad Nacional de Loja tendrá profesionales capacitados y calificados en la Unidad de Telecomunicaciones e Información, en concordancia con la labor y cargo que cada uno desempeñe.

Alcances

La aplicabilidad de estas políticas rige para la Universidad Nacional de Loja en su totalidad y conjunto. Los sistemas, equipos, software, líneas telefónicas y enlaces de comunicación adquiridos o contratados con cualquier finalidad por las diferentes áreas y departamentos, con anterioridad a la fecha de emisión de estas políticas, quedarán igualmente sujetos a ellas y a las auditorías que pudieran realizarse bajo su amparo.

POLITICAS GENERALES

Políticas de Definición

La Unidad de Telecomunicaciones e Información se constituye como Unidad de Servicios Informáticos y Telecomunicaciones para la Universidad Nacional de Loja.

Los usuarios son responsables exclusivos de los datos que manipulen en los ordenadores proporcionados por la Universidad Nacional de Loja y están normados al uso que la Institución establece.

Políticas de prestación de servicios

Los servicios que la Unidad de Telecomunicaciones e Información en sus diferentes secciones son: Mantenimiento Electrónico, Redes y Equipos Informáticos, Telecomunicaciones y Desarrollo de Software.

Los servicios prestados deben, para todos los casos, poseer una métrica de calidad, mediante la cual se midan: tiempos de respuesta, calidades de solución, calidades de satisfacción usuaria, entre otras variables.

La prestación de servicios de las secciones de la Unidad de Telecomunicaciones e Información debe, en todo momento, estar dotado de trazabilidad de procedimientos. Lo anterior implica procesos formales de solicitud de servicios, acción, respuesta y aceptación.

Políticas de administración de recursos

La administración y explotación de los sistemas de información serán realizadas con personal responsable perteneciente a la Universidad Nacional de Loja. Este personal esta conformado por los profesionales que se encargan de la manipulación directa de la información el cual se identificara como Unidad de Telecomunicaciones e Información.

Será responsabilidad de la UTI la administración de los recursos asociados a los sistemas de información y comunicación de la UNL. La responsabilidad por la administración de estos recursos.

La UTI es responsable de la calidad (fidelidad, oportunidad, consistencia y redundancia) de la información de la cual es administrador técnico. Además, deberá definir normas de administración y acceso a la información proporcionada por quienes establezcan los procedimientos de control.

La UTI deberá proveer los mecanismos de protección y control necesarios que aseguren la integridad y privacidad de los datos almacenados en los archivos y bases de datos que tenga en custodia.

La UTI deberá proveer de los mecanismos de respaldo necesarios que aseguren la continuidad operativa ante siniestros que afecten a los archivos y bases de datos que tenga en custodia.

Política de coordinación de actividades

Todo proyecto de modernización o innovación Tecnológicos que se lleve adelante en la Universidad Nacional de Loja que incluya aspectos relacionados con sistemas de información, equipos computacionales, software y transmisión de datos, voz e imágenes, contará con el apoyo logístico y técnico de la UTI.

Políticas de cobertura de los servicios

La UTI procurará extender la cobertura de los servicios de tecnología de información a todas las áreas de la Universidad Nacional de Loja en la medida que ello sea posible y sea del interés de nuestra Institución.

Políticas de Salvaguarda y Confidencialidad

Los funcionarios de la UTI bajo cualquier forma de estructura, se comprometen a salvaguardar de todo riesgo y a guardar la más absoluta reserva y/o confidencialidad sobre toda la información, cualquiera sea su naturaleza, que bajo cualquier medio le sea entregada de parte de la Universidad Nacional de Loja, y que forme parte de los datos, información, procedimientos, conocimientos, comportamientos, actividades, desempeños, funcionamientos, metodologías, rutinas, acciones y en general de toda expresión, en el medio que fuere, que pertenezca a la propiedad exclusiva de la Universidad Nacional de Loja.

Se incluye en este punto, toda información de tipo comercial, financiero, metodológicas, de procesos, de conocimientos propios y adquiridos, experimentales, ya sea su conocimiento de carácter privado o público y que pertenezca a la Universidad Nacional de Loja.

Políticas de Protección de datos y sistemas

El equipo computacional perteneciente a la Universidad Nacional de Loja estará bajo la exclusiva administración de la UTI y por lo tanto queda prohibido al usuario realizar intervenciones no debidas, entre las que se encuentran:

- Manipulación no autorizada.
- Apertura, reemplazo y/o desconexión de componentes.
- Reasignaciones permanentes o temporales sin autorización.
- Instalación de programas, sistemas, módulos y/o archivos externos.
- Empleo de juegos y/o programas con fines no laborales.
- Modifica la configuración de sistemas, programas o dispositivos.
- Desinstalar sistemas, programas, módulos oficiales de la Universidad Nacional de Loja.
- Conexión a redes eléctricas o de Datos no certificadas y o autorizadas

Respecto de lo definido con el fin de proteger las instalaciones, equipos, datos y sistemas de la acción de virus computacionales, será lo estipulado por la UTI lo que permanezca vigente y con prohibición para los usuarios el modificar y/o transgredir las disposiciones establecidas.

Políticas de documentación digital o Impresa

Respecto a la documentación, toda la Unidad de Telecomunicaciones e Información deberá documentar todas sus actividades que realizan en la Institución, en un sistema informático de documentación y el

sistema de registro de solicitudes de los usuarios de la institución, con el fin de medir el trabajo realizado y la eficiencia del servicio brindado.

POLÍTICAS ESPECÍFICAS A LAS SECCIONES DE LA UTI.

POLITICAS DE LA SECCIÓN DE DESARROLLO DE SOSFTWARE

Políticas de proyectos

Los proyectos que la Universidad Nacional de Loja aborde, y que se relacionen con la tecnología de información, deberán estar contemplados en el Plan de Desarrollo la UTI.

El Plan de Desarrollo de la UTI de la Universidad Nacional de Loja, y por lo tanto el plan de desarrollo de sistemas incluido en él, deberán estar autorizados por las autoridades máximas de la Universidad o por la estructura administrativa que sea establecida para tales efectos.

El Plan de Desarrollo deberá ser revisado con una periodicidad mínima de una semana en cuanto a cumplimiento y orientación.

El Plan de Desarrollo de la UTI deberá contemplar, al menos, los siguientes puntos:

- Plan de Sistemas
- Plan de Hardware
- Plan de Software
- Plan de Telecomunicaciones

En los contratos de desarrollo de sistemas, que se convengan con empresas consultoras externas, se incluirá una garantía de cumplimiento de lo convenido contractualmente, por un período de a lo menos un (1) año a contar de su implantación.

Políticas de metodologías de desarrollo

El desarrollo de sistemas se llevará a cabo mediante el uso de técnicas estructuradas de análisis y diseño de sistemas.

Se deberá elaborar, mantener y administrar los datos de la Universidad Nacional de Loja mediante una Base de Datos Institucional.

Las estructuras de almacenamiento de datos de todo sistema de información que se requiera desarrollar, deberán ser diseñadas considerando compatibilidad con la estructura de almacenamiento de la base de datos de la institución.

El diseño de los sistemas de información se orientará a un ambiente cliente-servidor.

La Universidad Nacional de Loja debe poseer un conjunto estructurado de normas y reglas que definan la interfaz que los sistemas presenten al usuario.

Estas reglas deben establecer mecanismos únicos y universales que, establecidos como estándares, se constituyan en el medio de interacción con los datos. Las cuales serán entregadas y aprobadas por el área de desarrollo.

Políticas de demandantes de sistemas

A las diferentes áreas demandantes de sistemas les corresponderá una activa participación en el proceso de desarrollo de sus sistemas, comprometiendo tiempo efectivo de apoyo a las actividades de análisis, modelamiento de datos, diseño administrativo, y puesta en marcha de los sistemas.

Los actuales sistemas en explotación, desarrollados con lenguajes de última generación en un ambiente de Base de Datos Relacional, conforme al modelamiento general de la Universidad Nacional de Loja, se deben certificar por el área de desarrollo.

Políticas de mantención de sistemas

Toda mantención de sistemas, deberá ser dirigida por la UTI de la Universidad Nacional de Loja. Los recursos, plazos y costos que originen las mantenciones de sistemas se regirán por la normativa y procedimientos vigentes al momento de realizarla.

Políticas de explotación de sistemas

La explotación de los sistemas de información residentes en los computadores de la UTI, será de exclusiva responsabilidad de los administradores de los mismos.

La UTI será el organismo encargado de proporcionar o coordinar la capacitación de los usuarios para la incorporación, operación y uso de sistemas de información.

Los funcionarios que tengan equipos, serán responsables de la conservación y buen uso de dicho equipamiento.

Políticas de desarrollo de sistemas y aplicaciones en computadores

Las funciones, procesos, sistemas y aplicaciones que se realicen con los productos de computación, deberán constituirse en parte integral de los sistemas de la Universidad Nacional de Loja, como complemento a los sistemas y/o funciones de ésta y no transformarse en sustitutos de ellos.

La protección, custodia y respaldo de los datos pertenecientes a los sistemas y aplicaciones basados en computadores y que no se tengan en el servidor de la red, serán de responsabilidad exclusiva de sus administradores o usuarios.

La UTI será el organismo encargado de proporcionar apoyo y asesoría técnica a los usuarios para la incorporación y uso de productos estándares de computación que requieran.

POLÍTICAS, NORMAS Y PROCEDIMIENTOS PARA LA ELABORACIÓN DE SISTEMAS

1. Objetivo

Establecer las políticas, normas y procedimientos que permitan homogeneizar el desarrollo de sistemas de información dentro de la Universidad Nacional de Loja.

2. Introducción

El software es el objeto de análisis y estudio de una de las ramas más jóvenes de ingeniería. De hecho, podemos decir que la concepción misma del software, es decir, su naturaleza de construcción y desarrollo es lo que lo hace particularmente distinto. Entre las características fundamentales del software podemos mencionar que su naturaleza es abstracta debido a que su herramienta principal es el manejo de la información. Además el software se desarrolla, no se fabrica como cualquier producto en un sentido clásico; se crea mediante la transformación del poder intelectual y cerebral de los especialistas en el conocimiento.

Consecuentemente, siendo la información uno de los recursos más valiosos de cualquier institución u organización, es de gran importancia contar con sistemas que permitan su uso eficiente, en armonía con todas las áreas. Para garantizar que esto ocurra dentro de la Universidad Nacional de Loja es indispensable contar con políticas, normas y procedimientos que permitan homogeneizar la elaboración de sistemas de información.

3. Políticas para la elaboración de sistemas

La política de calidad se define como las directrices u objetivos generales que tiene la Universidad Nacional de Loja concernientes a la calidad, las cuales son emitidas por la Unidad de Telecomunicaciones e Información.

Objetivo

Establecer un marco de referencia general para garantizar que los sistemas de información que apoyan las tareas sustantivas de una institución o empresa, sean concebidos y desarrollados de una manera tal, que permitan su articulación para una adecuada interacción entre las áreas.

Políticas

- Toda elaboración de sistemas deberá estar orientada a satisfacer las necesidades de manejo de información para las funciones sustantivas de la Universidad Nacional de Loja; es importante concebir el diseño de dichos sistemas de manera que permitan su integración y consolidación en una base de datos.
- Toda elaboración de sistemas, tanto interna como externa, debe cumplir con las normas establecida por la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, El cumplimiento de las normas es un requisito indispensable para considerar un sistema apto para su liberación definitiva.
- Toda elaboración de sistemas, tanto interna como externa de carácter institucional, deberá estar avalada por un informe técnico de la unidad de Telecomunicaciones e Información, este debe normar el uso y aprovechamiento de los recursos informáticos de acuerdo al reglamento interno de la Institución.
- La elaboración de sistemas institucionales debe apegarse a los estándares en cuanto al uso de software. Cuando esto no sea posible, el área usuaria deberá solicitar un dictamen técnico a la dirección de informática de la institución o empresa, justificando plenamente el uso de las herramientas propuestas para el desarrollo.
- Todos los sistemas y sus componentes desarrollados por el personal de la institución son propiedad de la Institución, por lo que la Universidad tendrá los derechos de autor para la utilización de dichos desarrollos en las diferentes áreas que así lo requieran.
- Durante el análisis, desarrollo e implantación de cualquier sistema, el área solicitante deberá participar con la Unidad de Telecomunicaciones e Información.
- Es responsabilidad de la Unidad de Telecomunicaciones e Información, el proporcionar la capacitación y asistencia técnica al personal operativo sobre el correcto uso del Sistema.
- La Unidad de Telecomunicaciones e Información establecerá de manera formal su política de calidad en cuanto a las normas y procedimientos por utilizar, con objeto de que funcione eficazmente el sistema informático de la Institución.
- En la elaboración y diseño de sistemas informáticos internos la Unidad de Telecomunicaciones e Información será la encargada de establecer y mantener un sistema de calidad documentado para asegurar productos conforme a los requerimientos especificados por ella misma, además de alcanzar consistentemente los objetivos de calidad de la institución o empresa. Entre los documentos que se generarán por los desarrolladores, están los manuales de procedimientos, técnicos, de instalación, operativos y de usuario.
- la Unidad de Telecomunicaciones e Información será el encargado de establecer políticas de administración, calidad y control de calidad; así como, la justificación y consistencia de éstas.

Periódicamente tiene la obligación de revisar las políticas establecidas y evaluar los resultados logrados.

Normas para la elaboración de sistemas

Objetivo

Definir la metodología a la que debe someterse todo el personal involucrado en la elaboración de sistemas, con objeto de obtener productos de alta calidad que resulten de fácil mantenimiento para cualquier miembro del equipo de trabajo.

Normas generales

1. Los desarrollos de sistemas, tanto internos como externos, deberán respetar los lineamientos y estándares definidos por la Unidad de Telecomunicaciones e Información para el Desarrollo de Sistemas.
2. La Unidad de Telecomunicaciones e Información y su sección de Desarrollo de Software deberán registrar, ordenar y inventariar: los programas fuentes y ejecutables, documentación técnica, manual de instalación y manual del usuario.
3. Para los desarrollos internos y externos, cualquier área de la institución deberá entregar a la dirección de Telecomunicaciones e Información el original del sistema con su respectiva documentación y todos aquellos elementos que hagan posible su incorporación al Repositorio de Sistemas de la Unidad, conservando una copia.
4. Todos las fases del desarrollo de sistemas deberán estar documentadas.
5. Para aquellos sistemas que se desarrollen con un software no estándar para la institución, será requisito indispensable que cuenten con un módulo de intercambio de información (importación/exportación) a través de múltiples protocolos o servicios (Webservice, LDAP). Por ninguna causa se deberá comenzar la etapa de programación del sistema en general, sin antes tener concluidas las etapas de análisis y diseño. Para el caso en que el sistema por su magnitud se haya dividido en módulos, será válido el comenzar la programación de cada uno de ellos si se cuenta con sus etapas de análisis y diseño concluidas, además de un análisis y diseño preliminar de carácter general del sistema.

Normas para el análisis de sistemas

1. Los desarrollos de sistemas deberán contar con un estudio de factibilidad tecnológica y económica que permita identificar y describir las necesidades del usuario con objeto de justificar la elaboración del sistema.
2. Se deberán establecer los grupos de trabajo encargados para las actividades de diseño de encuestas, entrevistas, recopilación de datos, etc.
3. La fase de análisis de sistemas deberá apegarse a las metodologías de análisis orientados a objetos.

Normas para el diseño de sistemas

1. De existir manuales de procedimientos vigentes en la institución o empresa, todos los grupos de trabajo involucrados en el diseño de sistemas deberán tener conocimiento del contenido de ellos, a fin de reflejarlos en el sistema cuando éstos lo afecten.
2. La fase de diseño de sistemas deberá apegarse a las metodologías de análisis y diseño orientado a objetos.
3. Para los casos en los cuales se efectúe un cambio en el diseño de un sistema, dicho cambio deberá ser documentado previa revisión y justificación, así como aprobación de los responsables para posterior control de la documentación, con el fin de que todas las áreas se enteren del cambio efectuado.

Normas para la programación y documentación de sistemas

1. Todos los programas que integren cualquier sistema deberán estar documentados conforme al Manual de Procedimientos para el Desarrollo de Sistemas.
2. El área usuaria deberá aprobar el manual del usuario previo a la liberación de un sistema. La Unidad de Telecomunicaciones e Información deberá revisar que el manual técnico se apegue a las especificaciones.
3. La Unidad de Telecomunicaciones mantendrá un control de la documentación de los sistemas.
4. La Unidad de Telecomunicaciones tendrá un estricto control de documentación, actualizando los contenidos según el mejoramiento continuo de los sistemas.
5. Todos aquellos códigos que sean objeto de programación, ya sean módulos, programas, pantallas, etc., deberán contener información de quién efectuó la programación y en qué fecha; de ser posible en el mismo software, mediante comentarios y adicionalmente en la documentación por escrito.
6. Después de concluida la programación de una parte del sistema, se deberá registrar en un documento que dicha parte del sistema ha sido concluida, especificar el o los nombre(s) del o los programador(es), así como el tiempo de programación en horas; esto con el fin de establecer un control de calidad del trabajo de los programadores.

Normas para la implantación de sistemas y capacitación

1. Antes de liberar un nuevo sistema, éste deberá ser sometido a pruebas de aceptación definidas por el área solicitante, utilizando para ello datos reales. En el caso de nuevas versiones, será necesario realizar corridas en paralelo para verificar su correcto funcionamiento con respecto a la versión anterior.
2. La capacitación al personal técnico-operativo formará parte fundamental de la liberación de un sistema. Dicha capacitación deberá cubrir todas las necesidades y requerimientos que el área usuaria especifique de común acuerdo con la Unidad de Telecomunicaciones e Información.
3. El proceso de capacitación deberá ser posterior a la aprobación de los manuales: a) técnico, b) de instalación, c) de operación y d) del usuario, que constituirán la guía con la que se lleve a cabo dicho proceso.
4. Los manuales de operación deberán especificar los métodos de manejo que permitan cuidar la integridad, tanto física como lógica de los elementos que conforman el sistema, ya sean datos, información, software, hardware y documentación.
5. Las pruebas de aceptación deberán ser clasificadas en: preliminares, para los casos en que se pruebe el módulo o el programa de manera individual, y totales, cuando se encuentren ensamblados todos los componentes del sistema. Para cada una de estas pruebas, se llevará un control de los resultados obtenidos.
6. Las corridas de prueba que se realicen con el fin de acreditar un sistema como aceptado, deberán efectuarse con una cantidad de datos superior al 50% de la cantidad de datos que el sistema correrá de manera cotidiana, y con el equipo de cómputo en el que se pretende operar sistemáticamente. Para el caso de sistemas que operen en red, también se deberán efectuar pruebas con usuarios concurrentes.
7. Los tipos de datos con los cuales se efectúen las pruebas deberán estar apegados a la realidad, a fin de tomar en cuenta el rango de valores que soportará el sistema y posteriormente realizar una gráfica de rendimiento de cantidad de datos contra el tiempo de procesamiento. En el caso de sistemas para trabajo en red, deberán establecerse elementos que permitan observar objetivamente el desempeño del sistema. Si los resultados de rendimiento del sistema no son aceptables para fines prácticos, se consignará el módulo para su re-trabajo en programación.

Normas para el mantenimiento de sistemas

Los usuarios deberán informar, solicitar cambios en el sistema a unidad de Telecomunicaciones e Información, siempre y cuando se identifiquen y justifiquen plenamente los ajustes y cambios basados en el reglamento y que son necesarios que permitan mejorar el desempeño y cobertura del sistema en cuestión.

Aquellos códigos del sistema que no trabajen de manera óptima con respecto a las necesidades o rendimiento que se pretenda satisfacer, serán dispuestos a un proceso de re-trabajo; en primera instancia a quien realizó la programación, y en último caso a un nuevo equipo de trabajo para programación, esto

considerando un estilo de programación diferente que sea más adecuado a la necesidad a satisfacer. La situación anteriormente descrita debe registrarse en la documentación correspondiente.

Manual de procedimientos para el desarrollo de sistemas (MPDS)

Introducción

El presente Manual de Procedimientos para el Desarrollo de Sistemas (MPDS) está dirigido a las personas directamente relacionadas con el desarrollo de sistemas; como tal, representa una guía para orientar y normar los trabajos y actividades involucradas en el análisis, diseño y desarrollo de los sistemas.

Existen varias metodologías y tecnologías que apoyan el desarrollo de sistemas, la mayoría de éstas identificadas con los métodos de análisis y diseño orientado a Objetos. Este manual de procedimientos está organizado siguiendo los lineamientos de dichos métodos; establece una metodología constituida por una serie de actividades orientadas a regular las acciones de los analistas.

Los procedimientos para el desarrollo de sistemas que se presentan en este manual se encuentran apoyados en las políticas y normas anteriormente descritas.

Objetivo del MPDS

Describir los procedimientos para cada una de las etapas que comprenden el desarrollo de sistemas.

Etapas para el desarrollo de sistemas

Con el fin de contar con un marco conceptual uniforme, se considera el "ciclo de vida de un sistema" constituido por cinco etapas:

1. Análisis
2. Diseño
3. Programación y documentación
4. Implementación (pruebas) y capacitación
5. Mantenimiento

En las siguientes secciones se define el objetivo de cada etapa, se describe en qué consiste y se listan las principales actividades involucradas.

Por último, en la tabla de formas o formatos para la documentación de sistemas se resumen los productos que deben obtenerse en cada una de las etapas de desarrollo, se identifican los responsables de cada una de ellas: área usuaria (U), área de informática (I) y, en caso de existir, empresa responsable del desarrollo (E). Es de gran importancia integrar estos productos en un expediente que permita conocer todas las etapas del ciclo de vida de un sistema, asegurando así su continuidad a través de la independencia del grupo de trabajo que lo desarrolló.

El desarrollo de sistemas se hará según la metodología de desarrollo ágil de sistemas que será aceptado mediante la discusión del grupo de desarrollo para construir un software de calidad, este resultado será descrito en una acta que servirá para todo el desarrollo de software de la Institución.

Para la etapa de programación será seleccionado el lenguaje de programación considerando que sean de Software Libre, el mismo que después de un consenso, de estabilidad, escalabilidad y tenga su plataforma una vigencia de mínimo 10 años.

El Mantenimiento de sistemas permite garantizar la permanencia en operación de un sistema, mejorándolo, adaptándolo a nuevos requerimientos o corrigiendo problemas que sean detectados durante su operación. Este proceso involucra todas las etapas de su desarrollo. Cuando el objetivo es mejorarlo o adaptarlo, el mantenimiento reinicia los trabajos del desarrollo en la etapa de análisis. Cuando se trata de corregir un

problema puede reiniciarse en el análisis, el diseño o la programación, por lo que esta parte del ciclo de vida de un sistema queda sustentada en las secciones anteriores de este manual.

Antes de modificar un sistema debe analizarse cuidadosamente si dicha modificación está justificada; de ser así debe procederse con la misma metodología utilizada durante el desarrollo, para llevar a cabo nuevamente las fases que sean necesarias del análisis, diseño, programación e implantación, poniendo especial atención en dejar una documentación completa y clara de los cambios efectuados, ya que de no hacerlo puede resolverse temporalmente un problema, pero también se contribuye a la rápida degradación del sistema.

POLÍTICAS DE LA SECCIÓN DE MANTENIMIENTO ELECTRÓNICO

Políticas de Mantenimiento Preventivo y Correctivo de los Recursos Informáticos

La Unidad de Telecomunicaciones comunicará el programa de mantenimiento preventivo a las diferentes dependencias de la Universidad Nacional de Loja; informando a los usuarios la fecha de visita de mantenimiento del equipo, con al menos dos días de anticipación.

Antes de llevarse a cabo la actividad de mantenimiento, los usuarios deberán respaldar la información almacenada en la computadora.

Las oficinas deberán programar sus actividades de tal manera que el equipo esté disponible en la fecha programada para el mantenimiento.

El Mantenimiento (mejora ó modificación) de los sistemas de información en operación (En plataforma Base de datos, Web e Intranet), deben estar acorde al Plan estratégico y Plan de Desarrollo Institucional.

Políticas de Servicio de Soporte Técnico

Todas las solicitudes de soporte técnico deberán plantearse a la Unidad de Telecomunicaciones e Información a través del sistema e-tickets quién las recibirá y resolverá oportunamente.

Sólo se atenderán solicitudes que se refieran al software y hardware propiedad de la Universidad Nacional de Loja, es decir que cuenten con el código de bodega correspondiente.

A través de las solicitudes de servicio se cuantificará el servicio prestado y permitirá establecer programas de capacitación y/o adiestramiento enfocados a áreas o temas deficitarios, sustitución de equipo, etc.

Política de mantención de las configuraciones computacionales

Los servicios de mantención técnica de los equipos y de actualización del software básico y programas producto, serán proporcionados por la sección de mantenimiento.

Políticas de respaldos de información

La responsabilidad de la realización de los procedimientos de respaldos corresponde a la sección de Mantenimiento.

Se deberán realizar los siguientes tipos de respaldos sobre equipos informáticos de la Institución:

- Respaldos de disco total.
- Respaldos imagen de disco.
- Respaldos de bases de datos.
- Respaldos Diarios

- Respaldos Semanales.
- Respaldos Mensuales
- Respaldos Semestrales
- Respaldos Anuales

Políticas de estaciones de trabajo

Políticas de adquisición, control y mantención de microcomputadores

Los requerimientos de computadores, ya sea para apoyo de procesos administrativos serán atendidos por la UTI en la siguiente modalidad:

Estación de trabajo: Las estaciones de trabajo serán adquiridas y deberán ser renovados según el período establecido por la Dirección de Recursos Humanos y Servicios Administrativos de la Universidad Nacional de Loja. De este modo se asegurara un nivel tecnológico mínimo, con respecto a lo sugerido por UTI.

Servidores: La UTI cuenta con equipos servidores para procesamiento de datos, que son equipos con tecnología de vanguardia y los cuales anualmente serán chequeados y evaluados para su potenciamiento.

Políticas de administración de equipamiento

Cada equipo con su software será asignado a un usuario (funcionario perteneciente a la Universidad Nacional de Loja), quién será el responsable, para todos los efectos, del uso de dichos recursos.

Por razones de seguridad, se privilegiará la mantención interna de los equipos de computación.

Con relación a los nuevos requerimientos de equipos de computación, éstos serán Adquiridos y/o arrendados a la Empresa que ofrezca la mejor alternativa costo/beneficio y deberán previamente ser autorizados por la Dirección Financiera previo informe técnico de la Unidad de Telecomunicaciones e Información.

Políticas de derechos de autor y propiedad intelectual del software

Se considerarán dos categorías de software que se obtenga por este medio:

1. ***Shareware:*** Es aquel que una persona o entidad física que lo desarrolló ha puesto a disposición del público para un período de prueba, al término del cual el usuario se compromete a pagar un cierto monto si desea seguir utilizándolo; caso contrario deberá eliminarlo de su equipo.
2. ***Freeware:*** Es aquel que la persona o entidad que lo desarrolló ha puesto a disposición del público de manera gratuita, solicitando en ocasiones un donativo para seguir con los trabajos, que el usuario no esta obligado a pagar.

Las licencias que se otorgan con este software determinan las condiciones para su uso, debiendo quedar claro para el usuario a que categoría corresponde el programa obtenido, para proceder conforme al marco que se estipule.

El usuario deberá notificar a la Unidad de Telecomunicaciones información, la existencia de este software, en caso que decida utilizarlo por un período prolongado, incluyendo el nombre, características y funciones del programa, además del motivo para su utilización.

La falta de conocimiento de la existencia de dicho software por parte de la Unidad de Telecomunicaciones e Información será responsabilidad del usuario en caso de la realización de una auditoría informática.

Prohíbase la reproducción o copia no autorizada de los programas computacionales que posee la Universidad Nacional de Loja, así como el uso de programas que no hayan sido adquiridos o autorizados por ésta.

Será responsabilidad de los funcionarios que tengan acceso al uso de equipos, evitar e impedir la reproducción o copia ilegal de programas computacionales, manteniendo un control de los programas en uso.

Los equipos y software de computación estarán destinados exclusivamente a ser utilizados como apoyo a las funciones propias de la Universidad Nacional de Loja y sus unidades.

Política de desarrollo informático

Objetivo:

Esta política tiene como objetivo el disponer de lineamientos que contribuyan a realizar inversiones exitosas en beneficio del desarrollo tecnológico informático institucional.

Los equipos y dispositivos que se adquieran deberán contar con la garantía de línea del fabricante, con el software y documentación técnica correspondiente.

Todos aquellos equipos que son necesarios para el funcionamiento de algún sistema de misión critica deberán contar con un contrato de servicio de soporte, una vez vencida la garantía.

Para la adquisición de computadoras, impresores y servidores se deberá observar que los mismos cubran como mínimo las especificaciones estándar.

Solamente se deben adquirir equipos integrados de fábrica (la totalidad de sus componentes) y cuyas marcas cuente con presencia y permanencia demostradas en el mercado nacional e internacional, y que cuenten con soporte local.

Los dispositivos de almacenamiento así como las interfaces de entrada/salida, deberán estar acordes con el estándar establecido.

Toda mejora de la red informática, sea expansión ó modificación debe estar acorde a las necesidades de la Institución y estándares establecidos.

Para la adquisición de software como: Sistemas Operativos, Bases de Datos, Lenguajes de Programación, Programas Integrados, Antivirus, Correo Electrónico, Control de Proyectos, Diseño Gráfico y Multimedia se deberá observar que los mismos cubran las especificaciones estándares establecidas.

Deberán adquirirse las últimas versiones liberadas de los software seleccionados, y solo en determinados casos bajo situaciones especificas, la Unidad de Telecomunicaciones e Información, podrá recomendar su adquisición en forma distinta.

Todo Software utilizado en la institución debe ser adquirido de forma legal, respetando la ley de Derechos de Autor y Propiedad Intelectual correspondientes.

Los proyectos de desarrollo y/o mantenimiento de sistemas de información de acuerdo a las necesidades de la institución pueden ejecutarse internamente ó a través de la contratación de servicios.

Los sistemas de información desarrollados interna ó externamente deben estar acorde a los estándares establecidos.

Los proyectos de desarrollo informático nacerán como respuesta a la necesidad de cumplimiento de determinados objetivos de la Institución y estarán enmarcados dentro del Plan Estratégico y Plan de Desarrollo Institucional. Por tanto, los proyectos tendrán siempre objetivos y finalidades específicas y hay que considerarlos como las herramientas para el logro de los objetivos institucionales.

Todo Proyecto de desarrollo informático debe iniciar con la etapa de planificación, que nos determina el alcance, etapas, tiempo y recursos necesarios para su ejecución.

El personal informático debe tener una capacitación continua y permanente, para el uso eficiente de los recursos informáticos e implantación de nuevas tecnologías acorde a la necesidades de la Institución.

El personal no informático debe tener una capacitación constante sobre las tecnologías implantadas, para el buen uso y desarrollo de la Institución.

POLÍTICAS DE LA SECCIÓN REDES Y EQUIPOS INFORMÁTICOS

Objetivo.- Regular el uso de los servicios de Redes, Correo Electrónico y el acceso a Internet, para lo cual se emiten los siguientes lineamientos para todo el personal que utilice los recursos de la Red.

Políticas de redes de microcomputadores

La Universidad Nacional de Loja, a través de su Unidad de Telecomunicaciones e Información, orientará la incorporación de redes locales de computadores de plataformas abiertas, en función de satisfacer las necesidades propias de cada unidad y de interconexión con la red Institucional.

La conexión entre redes locales de las diferentes áreas, para permitir el acceso e integración de la información en diferentes ambientes, independiente de su ubicación geográfica, será responsabilidad única y exclusiva de la UTI.

La UTI con su sección de redes Y equipos informáticos supervisará el funcionamiento, uso y mantención de las redes de computadores existentes en la Universidad Nacional de Loja.

Las redes de comunicaciones deberán estar acorde a las normas y estándares aceptados en materias de comunicaciones.

Políticas de enlaces para la transmisión de datos

La UTI será el responsable de estudiar, evaluar y proponer la contratación de enlaces para la transmisión de datos.

Políticas de Estándares Aplicables en la Instalación de Redes de Datos.

Se deberá etiquetar el cableado, las extensiones y los tableros de distribución eléctrica.

Se deberá evitar los cableados sueltos o dispersos, éstos deberán entubarse en el caso de los tendidos horizontales no vistos, en el caso de los tendidos horizontales o verticales vistos deben colocarse canaletas adecuadas.

Para equipos informáticos es recomendable disponer de circuitos alternos y tableros de distribución eléctrica independientes a cualquier otra conexión.

Previo a la instalación de equipos informáticos, es necesario realizar cálculos de la carga eléctrica requerida en la instalación, de los tableros de distribución, así como de los circuitos y conexiones que deben soportar la carga adicional proyectada.

Políticas de uso de la red

La UTI a través de su sección de Redes es el responsable de ofrecer este servicio. Este servicio sólo deberá utilizarse con fines académicos.

Generales :
El servicio de red será proporcionado a todo usuario autorizado que cuenta con una computadora y hace uso de la red. Los usuarios autorizados son:

a. Alumnos activos, profesional, maestría
b. Profesores de cátedra o de planta activos
c. Personal de apoyo activo
d. Departamentos y direcciones.

La UTI a través de su sección de Redes ofrece los siguientes servicios de red:

a. Conectividad a la red local (LAN) con nodos alámbricos e inalámbricos
b. Acceso a Internet
c. Acceso a Servicio ofrecidos por la UNL , siendo estos: Correo electrónico, Bibliotecas Virtuales,
d. Otros

La UTI a través de su sección de Redes se reserva el derecho de bloquear sitios de Internet (si previo aviso) que no cumplan con fines académicos o de investigación.

La UTI a través de su sección de Redes se reserva el derecho de restringir y negar servicio de red (sin previo aviso) en equipos que se detecte algún abuso en el servicio o provocar interrupciones en el servicio por virus y/o gusanos.

La UTI a través de su sección de Redes se reserva el derecho de restringir y negar servicio de red (sin previo aviso) en equipos que se detecte utilizando programas de P2P (Kaza, btorren, imesh, ares y otros) que genere tráfico.

La UTI a través de su sección de Redes restringirá el servicio de red aquellos usuarios que intentan violar la seguridad de cualquier equipo computacional o de red.

No está permitido el uso de la red para juegos recreativos.

No está permitido instalar equipo de red que no sea autorizado por La UTI a través de su sección de Redes

Está prohibido levantar servicios como pueden ser servidores web, ftp, dhcp, dns, irc, de correo o instalar una dirección fija en una máquina.

El usuario que se detecte usando software que invada la privacidad de alumnos, profesores, personal o equipo computacional se le restringirá el servicio de red.

Es responsable el usuario por los sitios que visite en Internet.

El usuario es responsable de la información (audio, video, documentos, etc.) que baje de Internet o Intranet y deberá respetar los derechos de autor. En caso de no hacerlo responderá por el uso la información de la cual no cuente con la licencia o autorización respectiva antes las autoridades que lo requieran

Cada Alumno, profesor o personal de campus universitario, tiene derecho a usar una tarjeta de red alámbrica e inalámbrica siempre y cuando se utilice en el mismo equipo pero no al mismo tiempo por lo que el uso de esta es responsabilidad del usuario.

Los usuarios tiene derecho a utilizar la red siempre y cuando respeten los puntos antes mencionados.

Los usuarios gozan de privacidad de su información, con la excepción de aquellos en los que se detecten acciones que pongan en riesgo la seguridad de la red del campus universitario..

Es responsabilidad del usuario realizar las actualizaciones necesarias a sus sistemas operativos así como las instalaciones críticas de su equipo computacional.

Es responsabilidad del usuario conocer las políticas de uso de la red.

El no tener conocimiento de estas políticas no es justificante para evitar respetarlas.

El usuario que no respete cualquiera de los puntos antes mencionados se le restringirá el servicio de red en el campus de manera temporal hasta que se presente a la UTI para ser revisado su equipo computacional.

Cualquier punto no estipulado en estas políticas queda a juicio de la UTI, al igual que las sanciones correspondientes.

Cualquier punto no contemplado en estas políticas será estudiado y resuelto por la UTI.

Políticas de uso del correo electrónico

Disposiciones Generales

Estas políticas son de carácter general y de cumplimiento obligatorio para todos los alumnos, docentes y empleados que tienen asignada una cuenta de correo en el dominio @unl.edu.ec

La cuenta de correo identifica de manera única a cada usuario y es a través de ella que puede enviar y recibir mensajes de otros alumnos, profesores y empleados de la Universidad Nacional de Loja.

La cuenta se dará de baja en el momento que el alumno, profesor o empleado deje de pertenecer a la Universidad Nacional de Loja.

Si un alumno, profesor o empleado tiene un problema relacionado con su cuenta de correo, deberá tratarlo personalmente, acudiendo a la Unidad de Telecomunicaciones e información de la Universidad Nacional de Loja.

La cuenta de correo electrónico (nombre de usuario y contraseña) se entrega únicamente al titular de la misma, no se puede entregar a través de otra dirección de correo o por teléfono, por motivos de seguridad.

Se asignaran las cuentas por departamento. Las cuentas para Simposios o Grupos Estudiantiles se darán con el visto bueno de la Dirección de la Unidad de Telecomunicaciones e Información.

Obligaciones del Usuario

La cuenta de correo electrónico es personal e intransferible, por lo que queda estrictamente prohibido dar a otros la posibilidad de uso.

El alumno, docente o empleado es completamente responsable de todas las actividades realizadas con su cuenta de correo proporcionada por la UTI.

Una vez que el alumno, docente o empleado haya recibido su cuenta de correo electrónico (nombre de usuario y contraseña), deberá cambiar su contraseña por motivos de seguridad.

El alumno, docente o empleado es responsable de respetar la ley de derechos de autor, no distribuyendo de forma ilegal software licenciado o reproduciendo información sin conocimiento del autor.

El buen uso de su cuenta se entiende por:

- Usar su cuenta con fines académicos y/o investigación.
- Respetar las cuentas de otros usuarios.
- Usar un lenguaje apropiado en sus mensajes.
- No mandar ni contestar cadenas de correo.
- No usar su cuenta para fines comerciales.
- No enviar material obsceno o con intención de intimidar, insultar o acosar.

Es responsabilidad del alumno, docente o empleado depurar continuamente su cuenta para mantener el espacio libre suficiente que garantice la recepción de mensajes.

Es responsabilidad del alumno, docente o empleado respaldar sus archivos de correo. Los mensajes que considere importantes deberá mantenerlos en su equipo personal o en su defecto, en carpetas dentro de su cuenta, cuidando no exceder la cuota permitida.

Está completamente prohibido realizar cualquier abuso de los tipos definidos en el Abuso de Correo Electrónico.

Los alumnos están obligados a reportar cualquier abuso de los tipos definidos en el Abuso de Correo Electrónico a la UTI, para evitar que esto vuelva a suceder al mismo o a otros.

Políticas de uso del servicio de correo electrónico institucional (@unl.edu.ec)

1. Descripción del Servicio

El servicio de correo electrónico institucional con el dominio @unl.edu.ec se lo proporciona a la comunidad universitaria con el objetivo de apoyar las comunicación digital a nivel directivo, departamental, académico, administrativo y estudiantil en la Universidad Nacional de Loja.

El acceso al servicio de correo electrónico de la institución está sujeto a la aceptación de la Política de Uso.

El correo electrónico institucional se encuentra bajo la plataforma educativa de Google Apps for Education, la que proporciona servicios integrados como: Gmail, Google Talk, Google Calendar, Google Drive, Google Sites, Google Groups, Lucidchart, entre otros servicios educativos.

El acceso al correo electrónico se lo realiza por medio del Portal Web Educativo: http://unl.edu.ec, en el banner Correo Electrónico o por medio del enlace directo a la página de ingreso al correo: http://webmail.unl.edu.ec, el servicio se encuentra administrado en la sección de Redes y Equipos Informáticos de la Unidad de Telecomunicaciones e Información.

2. Políticas de uso de las cuentas de correo electrónico institucional (@unl.edu.ec)

Se definen las políticas que cada uno de los miembros de la comunidad universitaria deben de respetar y aceptar:

- Todo docente, personal administrativo, direcciones departamentales y académicas, autoridades, estudiantes, contarán con una cuenta de correo electrónico, la cual deberá ser utilizada y revisada continuamente con fines institucionales.
- Todo oficio, invitación o trámite que no requiera de una firma o sello institucional se lo replicará por medio del correo electrónico.
- Los usuarios son completamente responsables de todas las actividades realizadas con su cuenta de correo electrónico de la institución.
- Como falta grave es facilitar y ofrecer su cuenta de correo electrónico a personas no autorizadas, las cuentas de carácter personal son intransferibles y las cuentas de dependencias son transferibles.
- El servicio de correo electrónico es una herramienta para el intercambio digital de información entre miembros de la comunidad universitaria no es una herramienta de difusión de publicidad, cadenas, entre otros fines.
- No está permitido enviar correos a personas que no desean recibirlo. Si la institución recibe quejas, denuncias o reclamos por estas prácticas se procederá con las sanciones correspondientes de acuerdo al caso.
- Están completamente prohibidas las siguientes actividades:
  - Utilizar el correo electrónico para propósitos comerciales, fines de lucro y actividades ajenas a la comunidad universitaria.
  - Distribuir de manera masiva grandes cantidades de mensajes con contenidos inapropiados para la comunidad universitaria.
- Ya que el servicio es proporcionado por una solución computacional en la nube que lo brinda Google Apps for Education, el usuario podría almacenar los correos en sus ordenadores institucionales o personales por medio de un cliente de correo y así tener acceso a los mismos en cualquier instante.
- Toda información o contenido que sea transmitido por las cuentas de correo de la institución son responsabilidad únicamente del dueño de la cuenta, por lo que dichos contenidos no reflejan las preferencias o ideas de la institución.

3. Datos técnicos y responsables

- La dirección de correo electrónico se compondrá de: nombre.primerapellido@unl.edu.ec, para el sector docente y administrativo; dependencia@unl.edu.ec, para las direcciones departamentales y académicas, [inicialesdenombres][primerapellido][inicialsegundoapellido]@unl.edu.ec, para el sector estudiantil.
- La contraseña que se asigna al crear la cuenta es el número de cédula, le pedirá de manera automático el cambio de misma.
- Las cuentas de correo electrónico son administradas por la Unidad de Telecomunicaciones e Información, en la sección de Redes y Equipos Informáticos.
- Se puede enviar archivos adjuntos por medio de la cuenta de correo electrónico cuyo tamaño total no exceda los 25 Mb.
- Cada cuenta de correo electrónico tienen una capacidad de almacenamiento de 25Gb.
- El uso de API y la compatabilidad facilita la integración de Google Apps con otros sistemas.
- Se cuenta con un certificado de Seguridad ISAE 3402 tipo II lo que permite que los datos privados y seguros de cada una de las cuentas de correo electrónico.
- Cualquier duda o soporte con el correo electrónico se lo puede hacer con envío de un mensaje a la siguiente cuenta institucional: soporte@unl.edu.ec o visitar el sistema de ayuda de escritorio http://soporte.unl.edu.ec para reportar la incidencia.

Facultades de la UTI

La UTI se reserva el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para la seguridad de la UNL y de su comunidad.

La vigencia de las cuentas será definida por la UTI.

Sanciones.

El incumplimiento por parte del alumno, profesor o empleado del buen uso de su cuenta puede ocasionar la suspensión y posterior baja de su cuenta.

Cualquier situación no contemplada dentro de los puntos anteriores será evaluada por la UTI.

Políticas Contraseñas.

La contraseña deberá cambiarse periódicamente (se recomienda cada semestre).

La contraseña no debe ser la misma que el nombre de usuario; se deberán evitar fechas, nombres de familiares o cualquier dato que pueda ser deducido por alguien.

La contraseña debe estar formada por al menos 8 caracteres. Se recomienda que al menos tenga alguno de estos caracteres: una letra mayúscula, dos números y por lo menos un carácter especial (!$%&*()_-+=[]|?/<>).

Políticas de las informaciones contenidas en la Red de Internet:

La Universidad Nacional de Loja no controla, ni es responsable del contenido y veracidad de las informaciones obtenidas o recibidas a través de la red de Internet. La UTI no se hace responsable por la exactitud o calidad de la información obtenida por este medio.

Los usuarios de Internet de la UNL son responsables de reportar inmediatamente a la Unidad de Informática (vía electrónica, telefónica o por escrito) cualquier situación en la red que pueda comprometer la estabilidad o seguridad del servicio de cualquier forma, así como cualquier violación a esta política.

Políticas de Uso de Página WEB

Los usuarios que tienen los derechos para la actualización de la página web, deben realizar los procedimiento conforme el manual de usuario de la página web.

Es responsabilidad del usuario autorizado informar a la Unidad de Informática a la mayor brevedad, algún daño ocasionado a la página web por mala manipulación de la aplicación de administración de la pagina web.

En todo momento, el usuario es el responsable único y final de mantener en secreto las Claves ó Passwords asignadas, con los cuáles tenga acceso a la aplicación de administración de la pagina web.

El responsable del contenido, calidad y actualidad de los datos publicados en la página web es la persona encargada del área, así dicha información sea obtenida e incorporada por sus colaboradores.

La Unidad de Protocolo y Comunicación es el ente encargado y responsable de revisar la redacción de la información que se publica en la página web.

POLÍCAS DE LA SECCIÓN DE TELECOMUNICACIONES

Políticas de uso de sistemas de comunicaciones

Las unidades que, para el mejor desempeño de sus actividades, necesiten utilizar sistemas de radiocomunicaciones podrán hacerlo, ateniéndose a las normativas legales vigentes emanadas de la subsecretaría de Telecomunicaciones y autorizadas por la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

POLÍTICAS PARA EL USO DEL EQUIPO COMPUTACIONAL

El Objetivo de las siguientes políticas es presentar las principales normas para el acceso de los alumnos, docentes y empleados de la UTI, además del comportamiento que han de observar en beneficio de la comunidad universitaria.

Definiciones:

Equipo Computacional. Se considera como equipo computacional a todo aquel equipo de cómputo, audiovisual, accesorio, periférico de telecomunicaciones y relacionado con cualquiera de éstos, que esté instalado en la sala de computadoras, laboratorios de cómputo, aulas tecnológicas, oficinas, administrados por la Unidad de Telecomunicaciones e Información.

Usuarios. Se consideran usuarios de los servicios de cómputo a los alumnos y profesores y empleados activos del campus universitario.

Políticas de uso del equipo computacional.

El equipo computacional deberá utilizarse como herramienta de apoyo para labores académicas y administrativas. Su uso es exclusivo para los alumnos, profesores y empleados activos inscritos en el período académico.

Normas de Comportamiento

El comportamiento de todos los usuarios debe ir a favor de la moral y de las buenas costumbres.

El uso adecuado del equipo computacional será responsabilidad del usuario, por lo que cualquier daño que se haga al equipo o a las instalaciones, será evaluado por la UTI, y si fuere necesario, el usuario se hará acreedor a una sanción y multa que cubra el monto del daño.

El personal de Seguridad y el personal de la UTI está autorizado a pedir al usuario que se retire de la Sala, Laboratorio de Computo especializado, aula teórica u oficina, por jugar, por tener una conducta inapropiada y/o cometer alguna falta expresada en este reglamento, el usuario deberá mostrar respeto y obedecer las indicaciones.

Prohibiciones dentro de la Sala, Laboratorio de Computo especializado, aula u oficina

- Introducir alimentos, bebidas o fumar.
- Desconectar, mover y/o extraer equipo computacional o sus partes.
- Alterar o dañar las etiquetas de identificación del equipo computacional.
- Utilizar grabadoras, radios o equipos de sonido sin audífonos.
- Utilizar los equipos computacionales como máquinas de juegos; esto incluye utilizar software de juegos o el acceso a servicios que impliquen el uso de juegos.
- Utilizar el equipo computacional para desarrollar programas o proyectos ajenos al interés académico de la Universidad.

- Copiar y/o alterar software.
- Utilizar los equipos computacionales para acceder a servicios locales o remotos a los que el usuario no tenga autorización explícita, o en su uso, intentar violar la seguridad de acceso de cualquier equipo computacional.
- Utilizar claves de acceso de otros usuarios, o permitir que otros usuarios utilicen la propia.
- Enviar mensajes a otros usuarios de manera anónima.
- Utilizar una identidad diferente a la propia, ya sea de otro usuario o ficticia, para enviar mensajes vía electrónica.
- Utilizar los equipos como medio de comunicación interactiva.
- Llevar a cabo acciones que puedan interferir con la operación normal de los equipos computacionales.

Sanciones
Las sanciones por infracción a cualquier punto del reglamento son:

Por la primera vez se notificará a su superior y se le suspenderá por un día el acceso a los equipos.
En la segunda ocasión se suspenderá por una semana su cuenta de acceso a equipos y se dará aviso a su superior.

En la tercera ocasión se suspenderá su cuenta de acceso a equipos definitivamente y por igual se dará aviso a su superior.

Bloqueo de equipo.

Políticas de Seguridad Computacional

Políticas de Uso Aceptable

La UTI no es responsable por el contenido de datos ni por el tráfico que en su red circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

Nadie puede ver, copiar, alterar o destruir la información de un usuario sin el consentimiento explícito del afectado.

No se permite el uso de los servicios de la red cuando provoquen una carga excesiva sobre recursos escasos.

Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la UNL y se usarán exclusivamente para actividades académicas relacionadas con la institución.

Todas las cuentas de acceso a los sistemas y recursos de cómputo son personales e intransferibles, se permite su uso única y exclusivamente a los propietarios de las mismas.

Cuando se detecta un uso no aceptable de la red, se cancela la cuenta o se desconecta temporal o permanentemente al usuario involucrado. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

30. Anteproyecto

UNIVERSIDAD NACIONAL DE LOJA

PFC-CIS

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

---

CARRERA DE INGENIERÍA EN SISTEMAS

"Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios"

PROYECTO FIN DE CARRERA

Autor:

- Franklin Mauricio Vega Hidalgo

Tutor:

- Ing. Luis-Antonio Chamba Eras, Mg. Sc.

LOJA-ECUADOR

2013

A. Tema

Modelo de Confianza para Herramientas de Seguridad Informática en Entornos Universitarios.

Índice de Contenidos

B. Problemática

1. Situación Problemática

Ante la presencia del gran avance globalizado que las tecnologías de la información han originado, principalmente por el uso masivo y universal del Internet, como de los servicios involucrados con ellas, la severidad y frecuencia de los ataques informáticos las han transformado en un continuo riesgo, que obliga a las instituciones a crear mecanismos, normas y políticas definitivas para contrarrestar estos ataques, transgresiones y permita la protección de la privacidad, del derecho de autor y de la seguridad informática [1].

Hoy en día existen aproximadamente 90 millones de internautas [2] en América del Sur, sin embargo; gran cantidad de usuarios, administradores o proveedores conectados a la red no tienen un conocimiento claro de las debilidades o vulnerabilidades de seguridad a las que está expuesta su información [3]. Es por ello que más de una ocasión se escoge un mecanismo de seguridad no adecuado para el entorno en donde se va a desempeñar, pudiendo ser que la herramienta seleccionada sea insuficiente para la cantidad de servicios informáticos que brinde el entorno o en caso contrario que la herramienta sea demasiado robusta para su campo de aplicación.

Para ello un mecanismo común por las que optan las instituciones, específicamente de carácter educativo, es la implementación de herramientas de seguridad informática, las mismas que tienen como objetivo central el fortalecimiento de la confidencialidad, integridad y/o disponibilidad de los sistemas informáticos [4]. Las herramientas que por lo general son implementadas aquellas que de quienes se tiene un alto grado de reputación en la Web[1] o una simple recomendación.

[1] Web o World Wide Web (WWW):Red Informática Mundial

Si bien es cierto, las aplicaciones informáticas no son seguras [5], ya que las vulnerabilidades únicamente se pueden contrarrestar desde el momento que se descubren las mismas, para posteriormente poner a prueba la seguridad mediante modelos reducidos de aplicaciones que permitirán valorar su nivel de seguridad. Sin lugar a dudas, como se deduce del principio de Kerckhoffs[2] [6]: "La experiencia es un indicador de seguridad" [5], es decir a través de la experiencia que se adquiere durante la implementación y uso de aplicaciones o mecanismos de seguridad informáticas se podría determinar cuándo es y cuándo no es viable implementar y uso [7].

Partiendo de las premisas antes mencionadas se puede indicar que un modelo informático [7] permite verificar las propiedades de los objetos informáticos [5], dentro de ello sus propiedades [4]. Un rescatable porcentaje de la sociedad informática puede asegurar de la inexistencia de modelos de seguridad [8], pero no es así, la criptografía establece sus bases en varios modelos de este tipo para operar. Sin embargo, estos modelos no tienen el nivel de detalle necesario para asegurar seguridad [5].

En lo que respecta a modelos de confianza, dentro de las Ciencias de la Computación se maneja el término *modelos de confianza y reputación [6],* los mismos que tiene algunos campos de aplicabilidad desde el comercio electrónico hasta los agentes inteligentes [9,10]. Al hablar específicamente de confianza, se hace hincapié a la factibilidad que tiene la aplicación de ciertos objetos del mundo en distintos entornos.

La confianza y reputación que tienen los mecanismos de seguridad informática dentro de los entornos universitarios juega un papel muy importante al momento de elegir uno de ellos para su posterior implementación, puesto que de ello depende su funcionalidad y

[2] Auguste Kerckhoffs

desempeño ante los diversos escenarios que se pueden presentar en estos entornos.

Partiendo de lo antes mencionado, se puede mencionar los siguientes problemas:

- En base a la entrevista y encuesta (Ver Anexo 1 y 2) realizada con el encargado del departamento de redes de la UTI[3] se ha podido corroborar que la institución[4] no cuenta con un departamento dedicado al campo de la seguridad informática, por ende no existe personal dedicado únicamente a explorar esta área para así conocer de mecanismos que ayudarían a mantener sus sistemas protegidos de cualquier tipo de amenaza informática que a la final podrían pasar de ser simples vulnerabilidades a convertirse en riesgos casi inevitables para la pérdida parcial o total de la información que se maneje a nivel institucional. Si bien es cierto el área de seguridad en una institución educativa tiene una gran responsabilidad y siempre tiene como objetivo principal salvaguardar, en este caso, la información que se encuentra en los sistemas informáticos, por tal motivo es necesario buscar la forma de evitar la elección errónea de herramientas de seguridad informática en los entornos universitarios, primeramente identificando los riesgos, requerimientos legales e institucionales, si este es el caso.

- Otro problema radica en la agilidad para la toma de decisiones en cuanto a seguridad informática en la institución o si se la hace de forma ágil se corre el riesgo de no hacerla de forma debida. Los Equipos de Respuesta a Incidentes de Seguridad Informática[5], son una gran ayuda para el área de seguridad informática debido a que, en caso de

[3] Unidad de Telecomunicaciones e Información-UNL
[4] Universidad Nacional de Loja: http://www.unl.edu.ec/
[5] SCIRT-UTPL: http://www.utpl.edu.ec/csirt-utpl/

existir, se encarga de brindar atención, soporte y respuesta a incidentes de seguridad, enfocando también sus servicios en el área de investigación en temas que contribuyan a mejorar la seguridad de los sistemas de la institución [11].

- *La implementación de los mecanismos de seguridad en entornos universitarios se realiza sin respaldarse previamente en algún modelo o estudio oficial [6,9]* que garantice un alto grado de confianza para implementar algún mecanismo de seguridad, debido a que, por lo general, se acostumbra esperar la aparición de alguna vulnerabilidad para actuar sobre la misma. Este es uno de los motivos por el que con el transcurso del tiempo y el avance de la tecnología surgen nuevos riesgos informáticos que ponen en amenaza el activo estratégico de las instituciones, la información.

2. Problema de Investigación

El no contar con un departamento formal dedicado al área de la seguridad informática, es una gran limitante para que la institución se mantenga al margen de los avances, en lo que respecta a mecanismos de seguridad y su correcta elección, así como de los beneficios que pueden traer los mismos, específicamente a la hora de tomar decisiones importantes para el campo informático de la Universidad. El implementar herramientas de seguridad informática que mantengan un alto grado de valor de confianza sería de gran ayuda para implementar mecanismos acordes a las necesidades de la institución.

¿La evaluación de las herramientas de seguridad informática basadas en un modelo de confianza permitirá determinar la factibilidad de implementación de estos mecanismos de seguridad en Entornos Universitarios?

C. Justificación

Los centros de educación superior son el pilar fundamental para la investigación e innovación y conforme a avanzado la tecnología estas instituciones se han visto en la necesidad indagar y hacer uso de ellas en diversos contextos. Un campo importante de aplicabilidad de estas tecnologías es el campo de la seguridad de la información [12], siendo éste el activo estratégico más importante de las organizaciones en general. Es por ello, que han surgido una serie de mecanismos o herramientas de seguridad informática [13], con el único fin de proteger proactivamente la información y los servicios que brindan las Universidades, pero existe un gran dilema a la hora de implementar cualquier de estas herramientas que se encuentran actualmente en apogeo, ya que se carece de un modelo o estándar que nos indique cuándo es y cuándo no aconsejable la implementación de determinada herramienta en entornos universitarios.

Para esto, se propone un modelo de confianza que permita determinar la factibilidad de implementación de estos mecanismos de seguridad en entornos universitarios, basándose en la creación de criterios apegados a los principios fundamentales [14, 15] y a estándares internacionales [16] para la seguridad de la información. De esta forma se puede decir que el presente proyecto aportará de forma significativa a la sociedad científica y tecnológica, otorgándoles criterios de evaluación para los mecanismos de seguridad a implementarse en entornos universitarios, específicamente para nuestra Universidad Nacional de Loja.

De igual manera a través de la evaluación de herramientas ya implementadas en entornos universitarios del país, permite justificar el proyecto académicamente/socialmente puesto que brinda la vinculación de proyectos universitarios y realizar un aporte a los entornos universitarios del país.

Asimismo, podemos decir que el Proyecto Fin de Carrera justifica técnicamente, puesto que se cuenta con herramientas para el análisis de los resultados obtenidos tras las implementaciones de herramientas de seguridad en algunas universidades destacadas del país [17-24], las mismas que han sido tomadas en cuenta como caso de estudio. Puesto que no en todos los casos dichas implementaciones han resultado exitosas, se analizará los motivos para establecer los criterios de evaluación, permitiendo así otorgar un nivel de confianza a las herramientas de seguridad informática.

Por otra parte, el presente proyecto se justifica ambientalmente por el hecho de desvincularse con el ecosistema al momento de realizar las respectivas investigaciones y posterior determinación de criterios para la evaluación de las herramientas de seguridad informática, que se pretendan implementar en los entornos universitarios.

Lógicamente, los gastos que surjan durante el desarrollo del proyecto serán únicamente responsabilidad del postulante, permitiendo así culminar el proyecto satisfactoriamente. Cabe recalcar que durante el presente proyecto se cuenta con el apoyo del docente tutor, Ing. Luis Antonio Chamba Eras, el mismo que maneja la línea de investigación en Modelos de Confianza, permitiendo así mejor desenvolvimiento del tema y mayor aplicabilidad del material investigativo.

Finalizando, el modelo propuesto se pondrá a criterio de la comunidad científica, permitiéndole juzgar el trabajo realizado así como servirá de gran ayuda para futuras investigaciones o proyectos a fines en la rama de modelos de confianza y seguridad informática dentro de nuestra Carrera de Ingeniería en Sistemas y por qué no del país, dando así la oportunidad de que se siga con lo inculcado en las aulas universitarias, la investigación e innovación.

En definitiva, podemos concluir que el proyecto planteado es factible realizar, puesto que justifica en lo tecnológico, técnico, académico, económico y ambiental contando además con los recursos necesarios para el desarrollo y una exitosa finalización del mismo.

D. Objetivos

1. Objetivo General

- Crear un modelo de confianza en base a criterios que permitan determinar la factibilidad de implementación de herramientas de seguridad informática en entornos universitarios.

2. Objetivos Específicos

- Comparar las herramientas de seguridad informática que han sido implementadas actualmente en entornos universitarios.
- Revisar la existencia de estándares que evalúen la confiabilidad en las herramientas de seguridad informática.
- Proponer el modelo de confianza para la implementación de herramientas de seguridad informática.
- Experimentar con el modelo propuesto sobre alguna de las herramientas de seguridad informática previamente estudiadas para evaluar su grado de confianza.

E. Alcance

El presente proyecto fin de carrera llamado “Modelo de Confianza para Herramientas de Seguridad Informática”, tiene como propósito la creación de un modelo de confianza en base a criterios, previamente estudiados y valorados, que permitan determinar la factibilidad de implementación de herramientas de seguridad informática en entornos universitarios, brindando así un gran apoyo a la toma de decisiones en los centros de educación superior de nuestro país, en lo que respecta a la seguridad de la información.

El proyecto antes mencionado se pretende desarrollar durante cuatro fases, en las que se pretende cumplir con los objetivos planteados en su totalidad. El tiempo previsto para la culminación del proyecto es de 8 meses tomando en cuenta la disponibilidad de tiempo del postulante y contados a partir de la aprobación del mismo.

FASE I: Comparar las herramientas de seguridad informática que han sido implementadas actualmente en entornos universitarios.

- Conocer cuáles son las herramientas de seguridad informática más implementadas en entornos universitarios a nivel nacional.
- Determinar un número considerable de herramientas de seguridad informática a ser estudiadas.
- Comparar las herramientas seleccionadas anteriormente, rescatando sus ventajas y desventajas.
- Establecer qué tipo de herramientas de seguridad informáticas han sido las más implementadas en las universidades de nuestro país y porqué.

FASE 2: Revisar la existencia de estándares que evalúen la confiabilidad en las herramientas de seguridad informática.

- Revisar exhaustivamente bibliografía para determinar la existencia de estándares internacionales o apartados de los mismos que brinden pautas para una buena toma de decisiones a la hora de implementar herramientas de seguridad informática.
- Seleccionar los estándares o apartados acordes al tema propuesto.
- Determinar la existencia de modelos de confianza que permitan valorar la confiabilidad a la hora de implementar herramientas de seguridad informática.
- Investigar cómo se realiza la toma de decisiones para implementar herramientas de seguridad informática en entornos universitarios mediante técnicas de recolección de datos (entrevistas, encuestas entre otras) a personal capacitado en temas de seguridad informática.

FASE3: Proponer el modelo de confianza para la implementación de herramientas de seguridad informática.

- Determinar criterios válidos para juzgar la toma de decisiones a la hora de implementar herramientas de seguridad informática
- Contrastar los criterios establecidos con los principios de la seguridad de la información y estándares que cuiden de su cumplimiento para su validez.
- Establecer pesos genéricos para los criterios determinados a la hora de valorar una herramienta de seguridad informática, previa a su implementación.

- Proponer niveles de confianza para la aceptación de la herramienta de seguridad informática al momento de realizar su implementación.

FASE 4: Experimentar con el modelo propuesto sobre algunas de las herramientas de seguridad informática previamente estudiadas para evaluar su grado de confianza.

- Listar un número considerable de herramientas de seguridad informática más implementadas en entornos universitarios en base al estudio previamente realizado.
- Determinar un escenario de experimentación para evaluar el modelo propuesto.
- Evaluar las herramientas seleccionadas mediante el modelo de confianza propuesta.
- Determinar el nivel de confianza de la herramienta de seguridad informática para su posterior implementación en entornos universitarios.
- Proponer a la comunidad científica la evaluación del modelo propuesto.

F. Marco Teórico

1. CAPÍTULO I: SEGURIDAD INFORMÁTICA

1.1. Concepto

Sin lugar a dudas, el término Seguridad Informática es escuchado mayoritariamente únicamente cuando se produce algún problema en equipos o servicios de carácter informáticos. Para ello es importante mencionar que, la Seguridad Informática son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados [12], daños accidentales o mal intencionados que pueden iniciar con una simple vulnerabilidad algún sistema o servicio informático.

1.2. Objetivo de la Seguridad Informática

Si bien es cierto, la seguridad informática tiene como principal objetivo el proteger el activo estratégico más importante que tienen las empresas/instituciones, que es su información, de los riesgos a los que está expuesta.

Es decir, la seguridad informática tiene su enfoque principal en el cumplimiento de sus principios fundamentales, Triangulo CIA (Confidentiality/Confidencialidad, Integrity/Integridad y Availability/Disponibilidad [14].

1.3. Principios Fundamentales de Seguridad

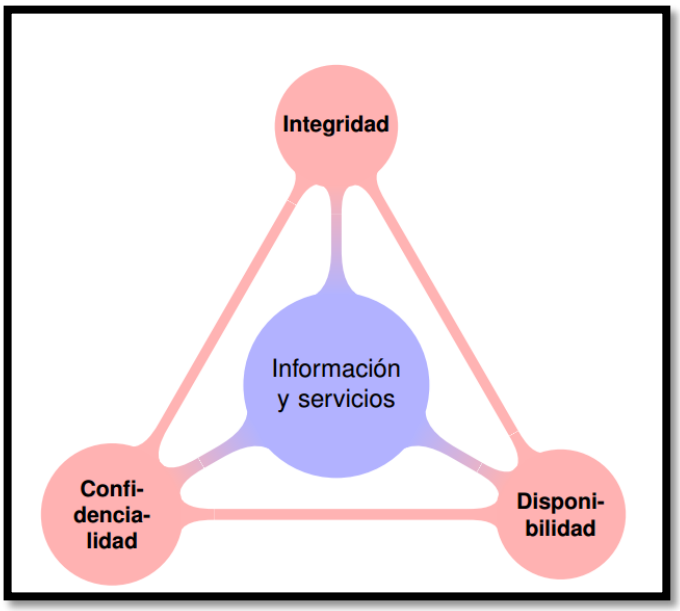


Figura 1 Principios Fundamentales de Seguridad [15]

- **Confidencialidad.** Se puede definir como la prevención de la revelación de la información no autorizada [13, 14, 25]. Esto puede ser el resultado de medidas de seguridad escasas o fugas de información por el personal. La escasez de medidas de seguridad son un ejemplo integro al dar paso al acceso no autorizado a información sensible para la institución.

- **Integridad.** Puede identificarse con la prevención de modificación errónea de información [12, 13, 25]. Los usuarios autorizados son probablemente la causa más grande de los errores, omisiones y alteraciones de información [14]. El almacenar información incorrecta o más bien manipulada por terceros dentro de un sistema puede resultar ser tan malo como perder información valiosa. Cabe mencionar que atacantes maliciosos externos también se destacan como causantes principales a la hora de modificar, eliminar o corromper información de las instituciones.

- **Disponibilidad.** Se define como la prevención de retención no autorizada de información o recursos [14]. Esto no únicamente aplica al personal que retiene información. La información debería estar tan libremente sea posible para los usuarios autorizados, todo bajo sus políticas y normas de la institución.

Existen adicionalmente algunos elementos de la seguridad informática que fortalecen sus principios básicos, entre ellos [25]:

- Control. Se define con el hecho de que solo los usuarios autorizados deciden cuándo y cómo permitir el acceso a la información.

- Autenticidad. Definir que la información requerida es válida y utilizable en tiempo, forma y distribución.

- No Repudio. Evita que cualquier entidad que envió o recibió información, alegue que no lo hizo.

- Auditoria. Determinar qué, cuándo, cómo y quién realiza las acciones sobre el sistema.

La seguridad informática se preocupa de que la información manejada por un computador no sea dañada o alterada, que esté disponible y en condiciones de ser procesada en cualquier momento y se mantenga confidencial [12]. Específicamente la información es y debe ser protegida como el bien más importante para las organizaciones de todo tipo.

2. CAPÍTULO II: MECANISMOS O HERRAMIENTAS DE SEGURIDAD

2.1. Concepto

Un mecanismo de seguridad puede servir para implementar uno o varios servicios de seguridad, al igual que un servicio de seguridad puede ser implementado mediante varios mecanismos [16].

Se puede decir, que un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer los principios fundamentales de esta rama: la confidencialidad, la integridad y/o la disponibilidad de un sistema informático [13]. Permitiéndole así a los sistemas o servicios informáticos contar con mayor nivel de confianza a la hora de operar en su entorno.

Existe una variedad amplia de mecanismos de seguridad informática. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan [13].

Estos mecanismos pueden ser algún dispositivo o herramienta física que permita resguardar un bien, un software o sistema que de igual manera ayude de algún modo a proteger un activo y que no precisamente es algo tangible, o una medida de seguridad que se implemente, por ejemplo las políticas de seguridad.

2.2. Clasificación Según su Función[13]

- Preventivos. Consisten en actuar antes de que un hecho ocurra y su función es detener agentes no deseados. Básicamente se concentran en el monitoreo de la información y de los bienes, registro de las actividades que se realizan en

la organización y control de todos los activos y de quienes acceden a ellos.

- Detectivos. Son aquellos que tienen como objetivo detectar todo aquello que pueda ser una amenaza para los bienes. Se caracterizan por enviar un aviso y registrar la incidencia.

- Correctivos. Este tipo de mecanismos se encargan de reparar los errores cometidos o daños causados una vez que se ha cometido un ataque, o en otras palabras, modifican el estado del sistema de modo que vuelva a su estado original y adecuado.

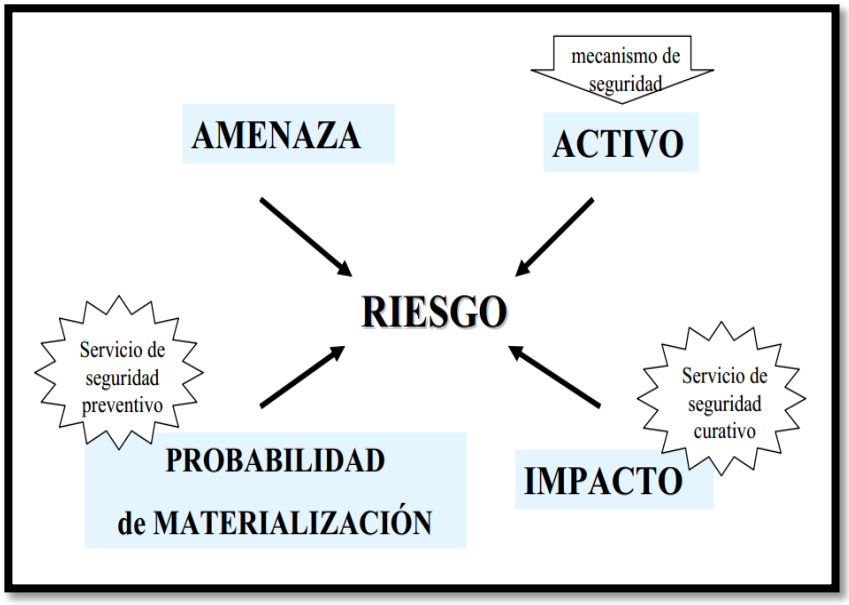


Figura 2 Aplicabilidad de los Mecanismos de Seguridad [26]

2.3. Estándares Internacionales

Dentro de los estándares internacionales relacionados con seguridad informática que se consideran importantes en la actualidad o por su importancia histórica, lo que consolida un

alto grado de confianza en su contenido, se encuentra la norma ISO[6] 17799 [16].

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización [27]. Esta norma tiene como objetivo principal proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre instituciones.

La parte a rescatar y a utilizar para el proyecto es la sección relacionada a Gestión de Comunicaciones y Operaciones, específicamente en el apartado de Control de Cambios Operacionales, en donde nos indica que [28, 29]:

"Se deberían controlar los cambios en los sistemas y recursos de tratamiento de información. Un control inadecuado de dichos cambios es una causa habitual de fallos de seguridad o del sistema. Se deberían implantar responsabilidades y procedimientos formales de gestión para asegurar un control satisfactorio de todos los cambios en los equipos, el software o los procedimientos. Los programas operativos deberían estar sujetos a un control estricto de cambios. Cuando se cambien los programas se debería conservar un registro de auditoria conteniendo toda la información importante. Se deberían integrar, siempre que sea posible, los procedimientos de control de los cambios operacionales y aplicativos. En particular se deberían considerar los siguientes controles y medidas:"

[6] ISO: International Estándar Organization

a) *la identificación y registro de cambios significativos;*
b) *la evaluación del posible impacto de los cambios;*
c) *un procedimiento formal de aprobación de los cambios propuestos;*
d) *la comunicación de los detalles de cambio a todas las personas que corresponda;*
e) *procedimientos que identifiquen las responsabilidades de abortar y recuperar los cambios sin éxito.*

3. CAPÍTULO III: MODELOS DE CONFIANZA

El término confianza puede tener múltiples definiciones que se aplican a diversos entornos. De manera general, se la puede concebir como la medida en la que una persona está confiada y ansiosa de actuar en base a las palabras, las acciones y las decisiones de otros [6, 10].

La confianza en sí, es un concepto abstracto que en la mayoría de las veces es usado indistintamente con términos relacionados como: credibilidad, confiabilidad o lealtad. Aparece un nuevo concepto que va de la mano de la confianza que es la reputación, debido a sus enfoques. En el campo de las Ciencias de la Computación encontramos diferentes modelos de confianza y reputación para variedades de dominio como, entre ellos: comercio electrónico, redes sociales, algoritmos genéticos, correo electrónico, web, comunidades científicas, consumidores y vendedores comerciales, criptografía, etc. Sin embargo, a pesar de la diversidad de las propuestas aún no existe una definición clara de confianza y reputación [10].

Para aclarar conceptos, a continuación se conceptualiza algunos términos que serán de gran ayuda para nuestro proyecto de investigación:

Se considera el término confianza como el nivel de seguridad que se tiene sobre la correcta toma de decisiones a la hora de implementar mecanismos de seguridad en entornos universitarios, los mismos que deben ser evaluados en base a criterios previamente establecidos.
La reputación es la percepción que una persona tiene sobre las intenciones y normas de otra, asicamos la confianza de una persona sobre las capacidades, honestidad y formalidad de otra persona, basada en las recomendaciones de otros [6, 10].

Se considera que la diferencia entre confianza y reputación depende de quien tenga experiencia previa con los mecanismos, es decir, si una persona tiene experiencia directa con un tipo de mecanismo de seguridad informática se puede decir que la persona tiene un valor de confianza para ese mecanismo. Por lo contrario, cuando el mecanismo de seguridad informática ha sido recomendado por otra persona que previamente ha tenido experiencia con esta herramienta, entonces se puede decir que la herramienta tiene un valor de reputación.

3.1. Modelos de Confianza y Reputación

Para refinar un poco más la conceptualización de los modelos de confianza y reputación en vista de que no existe un modelo de este tipo para herramientas/mecanismos de seguridad informática, se realiza una breve descripción de los sistemas que han tenido mayor impacto en la sociedad debido a su amplitud y cobertura, concretamente los sistemas de comercio electrónico y los modelos de confianza basados en agentes, ya que estos han sido el eje principal de los modelos de confianza y reputación [6].

Como es de conocimiento total, los sitios Web[7] de comercio electrónico ofrecen productos y servicios, con la única finalidad de ofrecer un entorno

[7] Web o World Wide Web (WWW):Red Informática Mundial

de confianza en donde los usuarios puedan adquirir sus productos o servicios sin temor a ser engañados. Para ello cada sitio de comercio electrónico implementa diferentes mecanismos que garantizan la confianza del cliente al momento de realizar operaciones [6, 10].

De igual manera, existen otros modelos de confianza y reputación basados en agentes inteligentes. Un sistema basado en agentes o MBA[8] se define como un sistema que busca lograr la cooperación de un conjunto de agentes autónomos para la realización de una tarea. La cooperación depende de las interacciones entre los agentes e incorpora tres elementos: la colaboración, la coordinación y la resolución de conflictos [10]. Es decir, juega un papel importante el grado de confianza que tienen los resultados de cada agente, para generar uno nuevo.

Sin embargo existen modelos de confianza orientados al campo de la seguridad informática, pero si bien es cierto están enfocados al área de la criptografía, los mismos que se basan en Web of Trust[9] , en donde se utilizan técnicas de seguridad informática basadas en la criptografía para estimar valores de confianza y reputación en comunidades virtuales [10].

Por tal motivo, es importante recalcar, que mediante la creación de un modelo de confianza que nos permita determinar cuándo es y cuándo no es factible implementar mecanismos de seguridad informática en entornos universitarios, ya que de esta manera se podrá manejar una toma de decisiones mucho más adecuada en base a una evaluación previa del mecanismo que se pretenda implementar.

[8] MBA: Modelo Basado en Agentes
[9] WOT: Web of Trust

4. CAPÍTULO IV: CASOS DE ÉXITO

4.1. CASO 1: Captura y Análisis de los ataques informáticos que sufren las redes de datos de la ESPOL[10], implantando una Honeynet con miras a mejorar la seguridad informática en redes de datos del Ecuador [17- 19].

Es un hecho que en la actualidad las redes de computadoras son atacadas y vulneradas. Cada año se incrementa la velocidad de propagación, la facilidad de ejecución y el daño que producen estos ataques. Por lo tanto, es muy importante el estudio y la elaboración de estrategias que permitan tener un grado adecuado para protegerse.
Para poder tener una red segura se debe considerar qué se debe proteger y de quién. Luego, definir la política de seguridad adecuada e implementarla.

La seguridad en una red de computadores depende de las vulnerabilidades en el software y hardware en los equipos que la conforman, y de los tipos de ataques internos o externos que sufren.

Se debe conocer las vulnerabilidades del software para poder aplicar medidas que eviten la explotación de las mismas. Así mismo, saber los posibles ataques en los servicios de red para implementar medidas para bloquearlos usando dispositivos de detección y bloqueos de ataques en la red.

Existen mecanismos que sirven de defensa para las redes de computadoras como firewalls, IDS[11], redes privadas virtuales (VPNs), listas de control de acceso, etc. Los problemas con estos mecanismos de seguridad se producen cuando no están correctamente configurados,

[10] Escuela Superior Politécnica del Litoral: http://www.espol.edu.ec/
[11] IDSs: Sistemas de Detección de Intrusos

y pueden dar una falsa sensación de seguridad. Para plantear las reglas correctas en firewalls, IDSs y ACLs[12], es imprescindible que el administrador de la red tenga una visión detallada y realista de los tipos de ataques a los que su red es susceptible. El uso de una de las nuevas tecnologías en mecanismos de seguridad llamada Honeypots permite conocer con detalle los ataques y vulnerabilidades de las redes.

Un honeypot o “tarro de miel”, en el campo de la seguridad en redes de información, se define como un recurso de la red que se encuentra voluntariamente vulnerable para que el atacante pueda examinarla, atacarla.
Directamente no es la solución a ningún problema; su función principal es recoger información importante sobre el atacante que permita prevenir estas incursiones dentro del ámbito de la red real en casos futuros.

Las Honeynets proveen la estrategia de detectar los fallos y mejorar en la defensa cuando se usan en conjunto con otros mecanismos de seguridad. Al recoger información de las intrusiones y estudiarlas podemos conocer nuevas amenazas y herramientas aún no documentadas, determinando así patrones de ataque y los diferentes motivos de los intrusos.

Las Honeynets son una herramienta, y puede ser usada para otros fines, como comprobar y desarrollar la capacidad de respuesta ante cualquier incidente. En las universidades pueden ser usadas para estudiar tipos y patrones de ataque o simplemente para investigar amenazas como función principal.

[12] ACLs: Listas de Control de Acceso

El presente trabajo consiste en implementar un tipo especial de Honeypot denominado “Honeynet”, en las redes de datos en la ESPOL, que nos permitirá capturar y analizar los patrones de ataques a dichas redes.

Luego de haber culminado con el trabajo se pudo constatar el funcionamiento de los dos tipos de Honeynet implementadas (HoneyNet Híbrida y Honeynet Virtual), para ello se citan algunas conclusiones del proyecto:

- El análisis y la implementación de dos arquitecturas distintas de Honeynets nos proporcionó una visión más clara sobre la importancia en el diseño de red. Pudimos experimentar con la posición de los elementos en la Honeynet y notar el cambio que implicaba para la solución.

- En la recolección y el análisis de datos pudimos darnos cuenta de la gran cantidad de traficó de ataque que normalmente circula en una red y tiene como objetivo algún servidor o equipo conectado a la misma, aprendimos la manipulación de archivos de trafico de red y su análisis utilizando herramientas libres como Wireshark[13].
- Una de las características de las honeynets se basa en capturar sólo el tráfico de interés para un análisis forense, facilitando el filtrado de datos. Se capturaron alrededor de 5 G en paquetes de red, una cantidad alta pero, relativamente pequeña si la comparamos con el tráfico normal de una red. Aunque los paquetes recolectados nos exigieron gran capacidad de procesamiento y almacenamiento la tarea se pudo realizar con éxito.

[13] Página Oficial: http://www.wireshark.org/

- La Honeynet de arquitectura híbrida resultó ser extremadamente fácil. Sin embargo, su implementación presentó muchos problemas en los procesos de administración, recolección y análisis.

- La Honeynet de arquitectura virtual, tomó mucho más tiempo en investigación y desarrollo. Esto depende del software de virtualización que se esté utilizando. Resultó muy complicado tenerla por primera vez funcionando pero se facilitaron mucho las tareas de administración, recolección y análisis. Al tener todos los sistemas como máquinas virtuales es posible realizar copias de cada una facilitando las tareas de administración y análisis.

- La Honeynet de arquitectura híbrida presentó un problema en la portabilidad, por el número de elementos físicos que dificultan el traslado, a diferencia de la Honeynet de arquitectura virtual la cual puede ser implementada en una computadora personal.

- Los resultados de los análisis y la gran cantidad de intentos de quebrantar los sistemas ampliaron nuestra perspectiva de la importancia del área de seguridad informática, lo que nos ayudará a mantener sistemas más seguros y aplicaciones que cubran los principales agujeros de seguridad que hemos encontrado.

Criterio: Es importante incursionar en campos en los que la sociedad tecnológica poco lo hace, permitiéndonos así descubrir nuevas tecnologías en cuanto a seguridad informática, las mismas que vienen

con un plus a su funcionalidad en los diversos entornos en los que se desempeña, más aún si estos entornos son universitarios y si estás instituciones como la ESPOL[14] cuentan con una variedad de servicios tanto internos como externos que se ven comprometidos con el cumplimiento de los principios de la seguridad de la información, que tiene como objetivo proteger la misma. El eje principal de todo esto es saber si fue una buena o mala elección de estos mecanismos de seguridad, en este caso se pudo constatar que una de las arquitecturas de Honeynet resultó con muchos problemas que la otra a la hora de recolectar y analizar el tráfico. Por lo tanto, se cree conveniente realizar la elección en base a un modelo y que mejor si el mismo se basa en la confianza establecida por casos de éxitos o experiencia que se ha tenido con estas herramientas y específicamente con la implementación en entornos universitarios.

4.2. CASO 2: Implementación de un Sitema de Detección y Análisis de Intrusiones No Autorizadas Utilizando Honeypots Caso Práctico DESITEL-ESPOCH[15] [20].

A continuación se citan algunos fragmentos del caso de éxito estudiado:
La situación actual de la ESPOCH que centraliza su red en DESITEL en que para la identificación de intrusiones cuenta con un hardware especial con un sistema integrado de firewall, antivirus e IDS la cual protege en tiempo real, filtra contenidos, VPN[16], detección y prevención de intrusos y gestor de tráfico, además tiene las funciones de alertas, apagado de routers y equipos en caso de ataques. Este dispositivo tiene la capacidad de bloquear, filtrar y proteger todo el contenido de la red de la ESPOCH, inmediatamente luego de la entrada de la Wan, el precio de este equipo es muy alto y además se complementa con otro equipo con el que no

[14] Escuela Superior Politécnica del Litoral: http://www.espol.edu.ec/
[15] Escuela Politécnica de Chimborazo: http://www.espoch.edu.ec/
[16] Red Privada Virtual

cuenta el DESITEL llamado FortiAnalizer[17] también tiene un precio elevado, el cual complementa la seguridad de la red. El FortiAnalizer analiza el tráfico de la red a partir de los datos de registro (logs) generados por el FortiGate[18], dando a los administradores una visión global de la red.

Los sistemas de detección de intrusos se han convertido en un componente importante en la caja de herramientas de un buen administrador de seguridad. Algunos aún no lo tienen claro, y piensan que un IDS (Intrusión Detection System) puede ser el remedio que nos lleve a la más absoluta tranquilidad y a una irreal sensación de seguridad, más peligrosa en muchos casos que la inseguridad en sí misma. Un detector de intrusos no es más que una de las medidas de seguridad que necesariamente hay que tornar para proteger una red. Es por ello que se tiene como objetivo reunir información sobre la actividad del intruso. De esta manera seremos capaces de detectar una vulnerabilidad antes de que sea explotada, además de conocer los riesgos a los cuales nuestros sistemas de producción están expuestos. Una de las ventajas de estos sistemas es que proveen de la información necesaria para conocer los riesgos con los cuales contamos en la red. Además de poner de nuestro lado la capacidad de desarrollar seguridad, siendo esto último un punto crucial en la defensa de toda organización o institución.

Como en la actualidad son más frecuentes los ataques que se reciben a través de la red, las técnicas de seguridad y la protección contra ingresos no autorizados han ido creciendo de la misma manera. Es por eso que los Honeypots son una alternativa a este problema los cuales consisten en activar un servidor y llenarlo de archivos tentadores, haciendo que sea difícil, pero no imposible de penetrarlo y sentarse a esperar que

[17] Página Oficial: http://www.fortinet.com/products/fortianalyzer/
[18] Página Oficial: http://www.fortinet.com/products/fortigate/index.html

aparezcan los intrusos. Esto da a los hackers un gran espacio para recorrer mientras el administrador de la red observa cada movimiento que hacen con el fin de mejorar sus sistemas de seguridad, realizar planes de contingencia y de esta forma evitar futuros ataques.

La ESPOCH cuenta con una aceptable protección de la red, más ningún equipo es completamente invulnerable a ataques interiores o exteriores, por ello Los Honeypots y Honeynets, junto a los IDS[19], conforman una herramienta cuando hablamos de seguridad en redes. El Honeypot es un software (programas que simulan uno o más servicios de red diseñados en los puertos de un computador), o conjunto de computadores en una red que actúa y parece como una máquina legítima, pero en realidad está configurado para interactuar con hackers potenciales (cuya intención es atraer a crackers o spammers), a fin de obtener información sobre sus estrategias de ataque. Entre más realista sea la interacción, más tiempo estará ocupado el atacante en máquinas "falsas" y lejos de verdaderos sistemas de producción, simulando ser sistemas vulnerables o débiles a los ataques, para poderlos observar en acción; usualmente está bien aislada del resto de la red, tiene bitácoras extensas (usualmente al nivel de network layer. en una máquina diferente). Los Honeypots, son una herramienta de seguridad diseñada para ser sondeada, atacada y comprometida, que tiene la capacidad de detectar y registrar estas acciones (registrar los intentos de acceso a aquellos puertos que utilizan generalmente los atacantes), pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente de un ataque, además de permitir un examen en profundidad de los atacantes, durante y después del ataque al Honeypot.

La solución que se trata de implementar en DESITEL es complementar los sistemas de seguridad mediante un HoneyPot de código libre el cual

[19] Sistemas de Detección de Intrusos

en caso de que cualquier atacante logre violar la seguridad del FortiGate lo encuentre como el primer y más vulnerable sistema a atacar, quedando dentro logs de registro como pueden ser comandos, scripts, inicios de sesión no autorizados. Rootkits, troyanos backdoors. etc.

Esta valiosa información servirá para detectar las debilidades de los sistemas y combatir futuros ataques utilizando los datos recopilados por el honeypot sin que en el ataque sean afectados los sistemas reales de la institución.

Es por este motivo se ha decidido realizar esta investigación ya que ayudará a la

ESPOCH a evaluar los posibles ataques y vulnerabilidades que tienen sus sistemas.

En la actualidad existen aproximadamente 17 herramientas Honeypots de alta interacción entre comerciales y de código libre, para el siguiente estudio se va a tener en cuenta las tres herramientas OpenSource mejor aplicables al caso.

Se eligió utilizar herramientas OpenSource ya que el gobierno ha adoptado la decisión de trabajar con software libre para instituciones públicas, al trabajar con código abierto el ahorro es significativo ya que no se pagara excesivos costos en las licencias obteniendo también un software de calidad.

La principal limitación para el desarrollo del Sistema de detección de intrusiones es que los Honeypots solo pueden rastrear y capturar actividades que interactúen directamente con ellos. Los Honeypots no podrán capturar ataques a otros sistemas vecinos, al menos que el atacante o la amenaza interactúe con el Honeypot al mismo tiempo.

Tras el planteamiento del proyecto se precede al desarrollo del mismo permitiendo así desarrollarlo prácticamente de la siguiente manera:

Con el siguiente tema de tesis se va a resolver:

- Detección de posibles ataques ya sean externos o internos a través de la red de DESITEL — ESPOCH mediante una máquina señuelo ubicada en la DMZ (zona desmilitarizada) Previamente preparada para recibir ataques.

- Análisis de logs pertenecientes a las intrusiones no autorizadas a los sistemas del Honeypot descartando los falsos positivos utilizando herramientas propias del mismo.

- Evaluación de resultados y vulnerabilidades de los sistemas debido a los ataques realizados a los sistemas de la ESPOCH.

- Realizar planes de contingencia para evitar futuros ataques del mismo tipo. Para realizar lo anteriormente mencionado se propone la implementación de un Honeypot el cual deberá estar ubicado en la DMZ que se encuentra inmediatamente luego del FortiGate para así no afectar a la red LAN de la Politécnica y sus tareas habituales

Luego de haber culminado con el proyecto los investigadores han podido llegar a las siguientes conclusiones:

- Mediante la utilización de parámetros e indicadores se ha logrado ejecutar el análisis comparativo de las herramientas de Administración para la detección de intrusiones en la red, Honeyd. BOF y Specter concluyendo que la herramienta más idónea para implantar la aplicación es Honeyd.

- La instalación e implementación de una herramienta de detección de intrusiones en la red está brindando mayor

seguridad y confiabilidad al usuario al momento de crear sus sistemas operativos virtuales.

- En instalación de las herramientas de detección de intrusiones en la red los honeypots Honeyd, BOF y Specter se puede concluir que la herramienta Honeyd posee un mejor rendimiento en lo referente a instalación.

- Se utilizó la distribución Ubuntu para la instalación del Honeypot Honeyd pues es más fácil de usar y se lo puede utilizar en forma privada, pública o comercial sin tener que pagar.

- Se concluye que la herramienta Honeyd tiene un mayor grado de funcionalidad ya que presenta muchas formas para la generación de sistemas operativos virtuales personalizados, mayor documentación y ayuda que las demás.

- En lo referente al Soporte Técnico oficial en línea se puede concluir que la herramienta Honeyd tiene una extensa información organizada no solo de sus librerías, sino de conceptos teóricos que ayudan a la mejor comprensión del funcionamiento de la herramienta Honeypot.

- Luego de estudiar los conceptos básicos sobre las herramientas de detección de intrusiones en la red se puede concluir que la herramienta Honeypot Honeyd maneja muchos sistemas operativos virtuales que son aplicables en tiempo real e interactúa mejor que las otras herramientas con el intruso.

Criterio: Mientras que se mantenga a la vanguardia de la investigación e innovación todo tipo de experimentación sería de gran ayuda, principalmente para adquirir experiencia. Este es el caso del proyecto antes mencionado en donde se planteó la propuesta de implementación de una de las herramientas de seguridad más actuales con el fin de fortalecer el campo de la seguridad de la información dentro de la ESPOCH, permitiéndoles así darse cuenta, mediante los resultados si la decisión de implementación de este tipo de herramientas fue la más acertada o no.

En este contexto de estudio, se podría concluir que la implementación de este tipo de mecanismos de seguridad resultó favorable, quizás no en su totalidad, debido a su amplia gama de funcionalidad. Pero si brindó pautas para una mejor toma decisiones en futuras implementaciones de estas herramientas de seguridad, como los son las de tipo Honeypot.

4.3. CASO 3: Honeynet como Apoyo a la Investigación de Seguridad de Redes en entornos Universitarios – UTPL[20] [3, 21].

La tecnología honeynet surge como un recurso de seguridad destinado tanto a la investigación como a la protección de una red de datos.

Hoy en día existen aproximadamente 90 millones de internautas en América del Sur, sin embargo; gran cantidad de usuarios, administradores o proveedores conectados a la red no tienen un conocimiento claro de las debilidades o vulnerabilidades de seguridad a las que está expuesta su información.

De acuerdo a un informe presentado por el Computer Security Institute, hasta el 2006 se incrementó el número de ataques y se perdieron cerca

[20] Universidad Técnica Particular de Loja: http://www.utpl.edu.ec/

de 15 millones de dólares únicamente por infección de virus sin considerar las pérdidas ocasionadas por otros tipos de ataques.

A nivel de Latinoamérica países como Brasil, México, Perú, Chile y Argentina cuentan con equipos formales que trabajan en temas de seguridad y que reportan datos estadísticos sobre los comportamientos detectados en cada país. En Ecuador no existe un registro oficial y público sobre el número de incidentes o ataques de seguridad que se presentan. A pesar de que el Proyecto Honeynet[21] capítulo Ecuador ha iniciado su operación no se cuenta con una infraestructura global que integre diversas redes.

Por ello, se ha visto en la tecnología honeynet una herramienta de seguridad valiosa, no solo para aportar a una seguridad proactiva, sino para constituir un potencial recurso de investigación.

Este artículo presenta el proceso que en la Universidad Técnica Particular de Loja, se llevó a cabo para implementar una honeynet, así como los primeros resultados obtenidos una vez analizada la información recolectada, lo que demuestra la importancia y utilidad de implementar esta tecnología.

Uno de los objetivos de una honeynet es recolectar informacion que ayude a identificar el modus operandi de los atacantes, una honeynet proporciona las herramientas y métodos para obtener información sobre ataques reales en internet, lo que permite a los investigadores conocer los patrones de comportamiento de los ataques, los motivos que impulsan a los atacantes y los métodos utilizados para atacar los sistemas, a través de un análisis detallado de los procedimientos y herramientas utilizados.

[21] Honeynet Capítulo Ecuador: http://honeynetecuador.wordpress.com/

Luego de haber culminado el proyecto de la implementación de esta herramienta de última generación se ha podido llegar al planteamiento de las siguientes conclusiones y trabajos futuros:

El comenzar con el Proyecto Honeynet ha generado una diversidad de aspectos poco claros, que difícilmente pudieron ser resueltos en el entorno debido a la inexperiencia en el trabajo con esta tecnología, en el caso del equipo de la UTPL no ha sido sencillo conseguir el apoyo de aquellos grupos cuyas redes están en estado avanzado, sin embargo; se ha logrado el objetivo planteado en el proyecto, que se refleja en contar con un recurso de investigación de los ataques de seguridad, enfocando incluso a la enseñanza.

La implementación de una red trampa en un entorno en producción permite validar la efectividad de este recurso como instrumento de investigación de ataques de seguridad. Los datos recolectados permitieron generar una estadística real de los intentos de acceso a la honeynet y a los diferentes servicios emulados, lo que da inicio a investigaciones detalladas sobre las actividades de la comunidad blackhat en nuestro país. Además los datos recolectados han podido ser contrastados con los datos registrados por los Sistemas de Detección de Intrusos así como Sistemas de Gestión de Seguridad que se tienen operando. Sin embargo; esta primera investigación da lugar a una gran cantidad de inquietudes que deben ser investigadas a profundidad.

Esta primera fase de implementación deja ver la necesidad de afinar varios aspectos de la honeynet, orientados principalmente al monitoreo y mantenimiento, así como la virtualización de nuevos servicios. Estas son las acciones inmediatas a seguir, para luego dirigir los esfuerzos del grupo al análisis detallado de los datos recolectados así como a procesos de análisis forense que permitan concluir precisamente sobre los hallazgos que se registren.

Criterio: Sin lugar a dudas, en este caso la implementación de esta herramienta de seguridad informática fue de gran ayuda, no únicamente para el ámbito de protección proactiva sino también para el ámbito investigativo, ya que da paso a la realización de una serie de investigaciones empleando los datos obtenidos. Así como permite descubrir cosas que podrían pulirse durante una próxima implementación de este mecanismo en las redes de datos de la institución educativa en estudio.

De igual manera el hecho de haber tenido éxito con esta implementación, ha motivado a incluir casi en su totalidad los servicios tanto internos como externos de la Universidad, dando cabida a la realización de los siguientes proyectos:

- Análisis del Tráfico Malicioso en los Servicios Críticos Internos de la UTPL [22].
- Análisis del Tráfico Malicioso de los Servicios Externos de la UTPL [23].

G. Metodología

1. Métodos y Técnicas

En base a lo mencionado en la problemática, en lo que respecta a la carencia de un modelo de confianza que permita evaluar la factibilidad de implementar herramientas de seguridad informática en entornos universitarios, se ve en la necesidad de analizar e investigar en base algunos casos de estudio para tener al menos iniciativas en la determinación de criterios para valorar la confianza en la implementación de mecanismos de seguridad informática en universidades.

Para ello se ha propuesto emplear el método/técnica Estudio por Casos [30-33], el mismo que consiste precisamente en proporcionar una serie de casos que representen situaciones problemáticas diversas de la vida real para que se estudien y analicen [30].De esta manera, se pretende que en base a los resultados obtenidos se puedan generar de soluciones o alternativas a la toma de decisiones [32].

De igual manera, Según Martinez Carazo, el Estudio de Caso es:

> *"Una estrategia de investigación dirigida a comprender las dinámicas presentes en contextos singulares, la cual podría tratarse del estudio de un único caso o de varios casos, combinando distintos métodos para la recogida de evidencia cualitativa y/o cuantitativa con el fin de describir, verificar o generar teoría."[31]*

El empleo de esta técnica está indicado especialmente para diagnosticar y decidir en el entorno de los problemas donde las relaciones humanas juegan un papel importante a la hora de tomar decisiones dentro de las organizaciones.

Alrededor del entorno es donde se aplique esta técnica se puede:

1. Analizar un problema.
2. Determinar un método de análisis.
3. Adquirir agilidad en determinar alternativas o cursos de acción.

4. Tomar decisiones.

Dentro del enfoque del estudio de casos como estrategia didáctica se menciona que se pueden considerar en principio tres modelos, de los cuales se va a emplear el **Modelo Que Busca El Entrenamiento En La Resolución De Situaciones,** en el que se requieren la consideración de un marco teórico y la aplicación de sus prescripciones prácticas a la resolución de determinados problemas, exigen que se atienda la singularidad y complejidad de contextos específicos [30].
En base al modelo seleccionado anteriormente podremos hacer uso de uno de los casos específicos, **Casos Centrados en Generar Propuestas de Toma de Decisiones**, el mismo que permite una mayor vinculación y apego al estudio que se pretende realizar para la determinación de los criterios de confianza para las herramientas de seguridad informática.

Dentro del grupo de casos antes mencionados se pretende el entrenamiento de los investigadores en el estudio de situaciones que requieren la resolución de problemas, de manera que se impliquen en el proceso de toma de decisiones que, desde la opinión de los individuos y/o grupo, sea el más adecuado en la situación estudiada. En el caso del presente proyecto se empleará este grupo de casos con el fin de apropiarnos mayoritariamente del conocimiento relacionado a la implementación de mecanismos de seguridad informática.

A continuación se presenta el proceso operativo requerido en este tipo de casos, se propone el siguiente decálogo:

1. **Discutir** los casos planteados de implementaciones de herramientas de seguridad informática en algunas instituciones situándolos en el entorno universitario del país [17-24].

2. **Analizar** por qué y en base a qué se realizó dichas implementaciones, si es que se tomaron en cuenta las consecuencias que podrían surgir en caso de haber realizado una mala elección.

3. **Identificar** la información adicional en lo que respecta a conocer acerca de más mecanismos de seguridad [16] que podrían implementarse así como acerca de estándares o normas [27] que podrían asegurar mejores resultados de implementación.

4. **Detectar** los puntos fuertes y débiles de las implementaciones en las diversas instituciones de educación superior, así como las interacciones que se producen entre ellos, los roles más significativos, los planteamientos teóricos e ideológicos que entran en juego en los casos de estudio. Finalmente, partiendo de estas consideraciones, enumerar los problemas planteados estableciendo una jerarquía en razón de su importancia y/o urgencia.

5. **Discutir** uno de los problemas o razones que puedan incidir en una mala elección de los mecanismos de seguridad a implementar, describiendo los principales aspectos que se crea preciso llevar a cabo en cada situación para solucionar los que hayan sido seleccionados.

6. **Generar o Plantear** los diversos criterios que se crean convenientes para evaluar la confianza en las implementaciones de herramientas de seguridad informática en los entornos universitarios.

7. **Compaginar** los pros y contras de cada uno de los criterios establecidos para el modelo de confianza propuesto, permitiéndonos así asegurar una eficaz evaluación de las

herramientas con el fin de que presente mayor coherencia con los fines establecidos, sea factible y conlleve el menor número de dificultades y efectos negativos.

8. **Implementar** los criterios establecidos para el modelo de confianza señalando las estrategias y recursos necesarios para llevarla a cabo.

9. **Determinar** el procedimiento con el que se llevará a cabo la evaluación de la decisión adoptada y sus efectos. El mismo que será mediante la puesta a prueba del modelo con alguna de las herramientas de seguridad informática ya estudiadas en fases anteriores.

10. **Reflexionar,** mediante el informe final, sobre los temas teóricos y científicos que plantea el modelo de confianza propuesto para la implementación de herramientas de seguridad informática.

Es importante mencionar, que adicionalmente se hará uso de técnicas para la recolección de información como: cuestionarios, entrevistas, encuestas a personal capacitado en lo que respecta al proyecto, en caso de ser necesario.

H. Cronograma

		Nombre	Duración	Inicio	Fin	Prede	Recursos
1		**Fase 1: Estudio Comparativo de Herramientas de Seguridad Informática.**	**28d**	**14/11/2013**	**23/12/2013**		
2		Conocer cuáles son las herramientas de seguridad informática más impleme	7d	14/11/2013	22/11/2013		Franklin
3		Determinar un número herramientas de seguridad informática a ser estudiada	7d	25/11/2013	03/12/2013	2	Franklin
4		Comparar de las herramientas previamente seleccionadas.	7d	04/12/2013	12/12/2013	3	Franklin
5		Documentar qué tipo de herramientas de seguridad informáticas han sido las	7d	13/12/2013	23/12/2013	4	Franklin,Tutor
6		**Fase 2: Revisión y Selección de Estándares.**	**30d**	**24/12/2013**	**03/02/2014**	**1**	
7		Revisar estándares internacionales para herramientas de seguridad informáti	6d	24/12/2013	31/12/2013	5	Franklin
8		Seleccionar estándares o apartados acordes al tema propuesto.	5d	01/01/2014	07/01/2014	7	Franklin
9		Documentar de la existencia o no de modelos de confianza para herramientas	5d	08/01/2014	14/01/2014	8	Franklin
10		Investigar la forma de tomar de decisiones para implementar herramientas de	14d	15/01/2014	03/02/2014	9	Franklin
11		**Fase 3: Propuesta del modelo de confianza.**	**38d**	**04/02/2014**	**27/03/2014**	**6**	
12		Determinar criterios válidos para juzgar la toma de decisiones al implementar	8d	04/02/2014	13/02/2014	10	Franklin,Tutor
13		Contrastar los criterios establecidos con los principios de la seguridad de la in	10d	14/02/2014	27/02/2014	12	Franklin
14		Establecer pesos genéricos para los criterios determinados del modelo propu	10d	28/02/2014	13/03/2014	13	Franklin,Tutor
15		Proponer niveles de confianza para la aceptación de la herramienta de seguric	10d	14/03/2014	27/03/2014	14	Franklin,Tutor
16		**Fase 3: Experimentación con el Modelo de confianza propuesto.**	**65d**	**28/03/2014**	**26/06/2014**	**11**	
17		Documentar las herramientas de seguridad informática más implementadas e	10d	28/03/2014	10/04/2014	15	Franklin
18		Determinar un escenario de experimentación para evaluar el modelo propuest	7d	11/04/2014	21/04/2014	17	Franklin
19		Evaluar las herramientas con el modelo de confianza propuesto.	20d	22/04/2014	19/05/2014	18	Franklin
20		Determinar el nivel de confianza obtenido por la herramienta de seguridad info	13d	20/05/2014	05/06/2014	19	Franklin
21		Proponer a la comunidad científica el modelo de confianza elaborado.	15d	06/06/2014	26/06/2014	20	Franklin,Tutor

I. Presupuesto y Financiamiento

El presupuesto y financiamiento descrito a continuación contiene los requerimientos humanos, económicos, materiales, técnicos y tecnológicos necesarios para el desarrollo del presente Proyecto Fin de Carrera en base al cronograma elaborado.

El tiempo estimado para el desarrollo del proyecto es de 8 meses, con 20 días hábiles de media al mes y trabajando a razón de 6 horas diarias, se obtiene un total de 960 horas laborables por la postulante.

A continuación se muestran tablas que cubren tanto Talento Humano, Bienes, Servicios e Imprevistos.

- **Talento Humano**

  En lo que respecta al presupuesto de talento humano, se incluye la participación del estudiante postulante (investigador) así como del asesor, cada uno con un precio por hora de $5.00.

  Todo esto tomando en cuenta el tiempo estimado de duración del proyecto y las horas de asesoría por parte del docente.

Equipo Trabajo	Tiempo (Horas)	Precio/ Hora ($)	Valor Total ($)
Investigador	960	5.00	4800.00
Asesor	192	5.00	960.00
SUBTOTAL ($)			5760.00

Tabla 1: Presupuesto Talento Humano.

- **Bienes y Servicios**

  En la sección de bienes y servicios se detalla la utilización de recursos técnicos hardware, como: laptop, impresora, medios de almacenamientos los mismos que se emplearon durante la construcción del proyecto.

RECURSOS TÉCNICOS HARDWARE					
Descripción	**Cant.**	**V. Unitario ($)**	**Tiempo Utilizado (Meses)**	**Precio /Mes($)**	**Valor Total ($)**
Portátil Xtratech	1	1150.00	8	16.00	128.00
Flash Memory 4G	1	10.00	8	0.80	6.40
Impresora	1	100.00	8	3.00	24.00
SUBTOTAL ($)					158.40

Tabla 2: Recursos Hardware.

Dentro de los recursos software se denota los costos de utilización de aplicaciones tanto propietarias como de código libre.

RECURSOS SOFTWARE			
Descripción	**Cant.**	**V. Unitario($)**	**Valor Total ($)**
Sistemas Operativos Windows 8	1	140.00	140.00
Microsoft Project 2010	1	90.00	90.00
Paquete de Ofimática de Microsoft Office 2013 (licencia estudiantes)	1	170.00	170.00
Limesurvey	1	0,00	0,00
SUBTOTAL($):			400.00

Tabla 3: Recursos Software.

A continuación, se detallan los costos unitarios así como los totales de los recursos materiales y los servicios de los que se hará uso para la elaboración del proyecto.

RECURSOS MATERIALES			
Descripción	**Cant.**	**V. Unitario ($)**	**V.Total ($)**
Resma de papel	4	5,00	20,00
Anillados	4	1,50	6,00
Copias	120	0.02	2,40
Cartuchos de Tinta	4	22,00	88,00
CD's	3	0,75	2,25
SERVICIOS			
Transporte	600	0.25	150.00
Comunicaciones	40	1.00	40.00
Internet	960 horas	0.70	672.00
SUBTOTAL ($)			**980,65**

Tabla 4: Recurso Bienes y Servicios.

- **Presupuesto General.**
  Finalmente, se indica en la siguiente tabla la sumatoria de los diversos apartados mencionados anteriormente, permitiendo así un presupuesto general del costo total para el presente proyecto. De igual manera se ha añadido una cantidad relevante por motivos de imprevistos que pudiesen presentarse durante el desarrollo.

PRESUPUESTO TOTAL	
RECURSOS	**SUBTOTALES ($)**
HUMANOS	**5760.00**
TÉCNICOS HARDWARE	**158.40**
SOFTWARE	**400.00**
MATERIALES Y SERVICIOS	**980,65**
IMPREVISTOS	**100,00**
TOTAL ($)	**7399.05**

Tabla 5: Presupuesto General.

J. Bibliografía

[1] Universidad Centro Occidental Lisandro Alvarado, “NORMAS DE SEGURIDAD INFORMÁTICA Y DE TELECOMUNICACIONES”, Disponible en: [http://www.ucla.edu.ve/Telecom/NORMAS_de_seguridad_INF_y_de_telecomunicaciones_UCLA.pdf], Fecha de Consulta: [20/08/2013]

[2] Internet World Stats: Internet Usage Statistics for the Americas, Junio de 2009., Disponible en: [http://www.internetworldstats.com/stats2.htm], Fecha de Consulta: [25/08/2013]

[3] Espinoza, M.P. – Pilco, R. – Montalaván, H., “Honeynet como Apoyo a la Investigación de Seguridad de Redes en entornos Universitarios”, Disponible en: [http://www.docstoc.com/docs/55437009/proyecto-honeynet---UTPL], Fecha de Consulta: [27/08/2013]

[4] Burgos Salazar, J. Campos, P., “MODELO PARA LA SEGURIDAD DE LA INFORMACIÓN EN TIC”, Disponible en: [http://ceur-ws.org/Vol-488/paper13.pdf], Fecha de Consulta: [20/08/2013]

[5] Waissbein, A.-CORE SECURITY TECHNOLOGIES, “Modelos de Seguridad Informática – Software Protection”, Disponible en: [http://www.coresecurity.com/files/attachments/Waissbein_UNR_2004.pdf], Fecha de Consulta: [02/10/2013]

[6] Cortes Argueta, J., “Criptografía- Principio de Kerckhoff”, Disponible en: [http://www.openboxer.260mb.com/asignaturas/criptografia/principioKerckhoff.pdf], Fecha de Consulta: [02/10/2013]

[7] Rodríguez, D. – Rincón, J., “Modelo, Modelar, Modelo del Sistema Viable, Factibilidad y Viabilidad”, Disponible en: [http://www.slideshare.net/toofymen/modelo-informtico], Fecha de Consulta: [02/10/2013]

[8] Vogelmann Martínez, E., “Políticas y Modelos de Seguridad”, Disponible en: [http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonEste.pdf], Fecha de Consulta: [02/10/2013]

[9] Chamba Eras, L.A. Arruarte, A. Elorriaga, J.A. “IMPACTO DE UN FACTOR DE SEGURIDAD DE LA INFORMACIÓN SOBRE OBJETOS DE APRENDIZAJE EN LMS”, Disponible en: [http://dspace.unl.edu.ec:8080/jspui/bitstream/123456789/235/1/A_IMPACTO%20DE%20UN%20FACTOR.pdf], Fecha de Consulta: [25/08/2013]

[10] Chamba Eras, L.A., TESIS: “MODELO DE CONFIANZA PARA OBJETOS DE APRENDIZAJE EN COMUNIDADES DE APRENDIZAJE”, Disponible en: [http://www.ccia-kzaa.ehu.es/s0140-con/es/contenidos/informacion/tesis_master/es_t_master/adjuntos/11lchamba.pdf], Fecha de Consulta: [25/08/2013]

[11] UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA-UTPL, “CSIRT-UTPL”, Disponible en: [http://www.utpl.edu.ec/csirt-utpl/], Fecha de Consulta: [02/09/2013]

[12] Hernández Pinto, M.G. – Naranjo Sánchez, B.A., “Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial”, Disponible en: [www.dspace.espol.edu.ec/bitstream/123456789/15875/2/CICYT.docxwww.dspace.espol.edu.ec/bitstream/123456789/15875/2/CICYT.docx], Fecha de Consulta: [05/10/2013]

[13] Universidad de Sevilla- Departamento de Ciencias de la Computación e Inteligencia Artificial, “Seguridad Informática”, Disponible en: [http://www.cs.us.es/cursos/ai-2003/.../8.-**Seguridad**%20**Informatica**.ppt], Fecha de Consulta: [10/10/2013]

[14] KIT de Repaso para el examen de la Certificación Microsoft Technology Associate: FUNDAMENTOS DE SEGURIDAD, MICROSOFT-EDUTEC-YACHAY, “Principios Fundamentales de Seguridad”, Fecha de Consulta: [08/10/2013]

[15] Hermoso, R. – Vasirani, M. – Universidad Rey Juan Carlos, “Seguridad Informática-Seguridad en Redes”, Disponible en: [http://www.ia.urjc.es/cms/sites/default/files/userfiles/file/SEG-I/2012/introduccion-redes.pdf], Fecha de Consulta: [08/10/2013]

[16] BANCO DE LA REPÚBLICA DE BOGOTÁ, COLOMBIA-DEPARTAMENTO DE SEGURIDAD INFORMÁTICA, “Mecanismos de Seguridad de los Servicios Informáticos”, Disponible en: [http://www.banrep.gov.co/sites/default/files/paginas/Mecanismos_de_Seguridad_Informatica.pdf], Fecha de Consulta: [10/10/2013]

[17] Avilés Monroy, J.I. – Pazmiño Castro, M.R., TESIS: “Captura y Análisis de los Ataques Informáticos que Sufren las Redes de Datos de la ESPOL, Implantando una Honeynet con Miras a Mejorar la Seguridad Informática en Redes de Datos del Ecuador”, Disponible en: [http://www.dspace.espol.edu.ec/handle/123456789/7781], Fecha de Consulta: [09/10/2013]

[18] Avilés Monroy, J.I. – Pazmiño Castro, M.R.- Abad, C., ARTÍCULO: “Captura y Análisis de los Ataques Informáticos que Sufren las Redes de Datos de la ESPOL, Implantando una Honeynet con Miras a Mejorar la Seguridad Informática en Redes de Datos del Ecuador”, Disponible en:

[http://www.dspace.espol.edu.ec/handle/123456789/4203], Fecha de Consulta: [10/10/2013]

[19] Avilés Monroy, J.I. – Pazmiño Castro, M.R.- Abad, C., ARTÍCULO: "Diseño Preliminar de una Honeynet para Estudiar Patrones de Ataques en las Redes de
Datos de la ESPOL", Disponible en: [http://www.dspace.espol.edu.ec/handle/123456789/4784], Fecha de Consulta: [10/10/2013]

[20] Torres García, D.F. –Zambrano Nuñez, P.S., TESIS: "Implementación de un Sistema de Detección y Análisis de Intrusiones No Autorizadas Utilizando Honeypots Caso Práctico DESITEL-ESPOCH", Disponible en: [http://dspace.espoch.edu.ec/handle/123456789/1495], Fecha de Consulta: [10/10/2013]

[21] Espinoza, M.P. – Pilco, R., Montalván, H., PAPER: "Honeynet como Apoyo a la Investigación de Seguridad de Redes en entornos Universitarios", Disponible en: [http://www.docstoc.com/docs/55437009/proyecto-honeynet---UTPL], Fecha de Consulta: [10/10/2013]

[22] Ludeña Ramírez, S.F., TESIS: "Análisis del Tráfico Malicioso en los Servicios Críticos Internos de la UTPL", Disponible en: [http://dspace.utpl.edu.ec/handle/123456789/2190], Fecha de Consulta: [10/10/2013]

[23] Montalván Celi, C.A., TESIS: "Análisis del Tráfico Malicioso de los Servicios Externos de la UTPL", Disponible en: [http://dspace.utpl.edu.ec//jspui/handle/123456789/1424], Fecha de Consulta: [10/10/2013]

[24] Maya, E. – Vinueza, T., PAPER: “Honeynet Virtual Híbrida en el entorno de red de la Universidad Técnica Del Norte de la ciudad de Ibarra”, Disponible en: [http://repositorio.utn.edu.ec/handle/123456789/1058], Fecha de Consulta: 10/10/2013]

[25] López Cámara, L.A. – Universidad Veracruzana, “Objetivo de la Seguridad Informática”, Disponible en:[http://www.uv.mx/personal/llopez/files/2011/09/presentacion.pdf], Fecha de Consulta: [06/10/2013]

[26] Universidad Pontificia de Comillas – Curso de Doctorado en Seguridad de Redes de Ordenadores, “Introducción a la Seguridad Informática”, Disponible en: [http://www.iit.upcomillas.es/palacios/seguridad_dr/tema1_intro.pdf], Fecha de Consulta: [10/10/2013]

[27] Yori, J. – MVA, “Un acercamiento a las mejores prácticas de seguridad de información internacionalmente reconocidas en el estándar ISO 17799:2005- ¿Qué es la Norma ISO 17799?”, Disponible en: http://www.mvausa.com/Colombia/Presentaciones/INTRODUCCION_ISO_17799.pdf], Fecha de Consulta: [09/10/2013]

[28] Bonilla, G., “Seguridad de la Información Norma ISO 17799”, Disponible en: [http://www.ciiasdenic.net/files/doccursos/1196890583_ConferenciaISO17799.pdf], Fecha de Consulta: [05/10/2013]

[29] Enríquez, M.E.- NORMA TÉCNICA PERUANA-NORMA ISO 17799, “EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información”, Disponible en:

http://www.slideshare.net/marieu.enriquez/norma-iso-17799], Fecha de Consulta: [09/10/2013]

[30] Universidad Católica de Temuco, “Estudio de Casos como técnica didáctica”, Disponible en: [http://www.uctemuco.cl/cedid/archivos/apoyo/El%20estudio%20de%20casos%20como%20tecnica%20didactica.pdf], Fecha de Consulta: [10/10/2013]

[31] Universidad de las Américas Puebla, “Estudio de Caso”, Disponible en: [http://www.udlap.mx/intranetWeb/centrodeescritura/files/notascompletas/estudiodeCaso.pdf], Fecha de Consulta: [10/10/2013]

[32] Barrio del Castillo, I. – Jiménez Gonzáles, J. – Padín Moreno, L. – Peral Sánchez, I. – Tarín López, E., Universidad Autónoma de Madrid, “El Estudio de Casos”, Disponible en: [http://www.uam.es/personal_pdi/stmaria/jmurillo/InvestigacionEE/Presentaciones/Est_Casos_doc.pdf], Fecha de Consulta: [10/10/2013]

[33] Soto Ramírez, R., Universidad Nacional Autónoma de México, “Método: Estudio de Casos – Curso: Investigación Cualitativa”, Disponible en: [http://www.paginaspersonales.unam.mx/files/981/estudio_de_caso.pdf], Fecha de Consulta: [10/10/2013]

31. Certificado de Corrección de Estilo y Ortografía

Certificado de Corrección de Estilo y Ortografía

KELVIN HUMBERTO PALADINES TINOCO

LICENCIADO EN CIENCIAS DE LA EDUCACIÒN, ESPECIALIDAD: IDIOMA ESPAÑOL Y LITERATURA

CERTIFICA:

Haber revisado y corregido el ESTILO Y ORTOGRAFÍA del presente trabajo de titulación, bajo el tema "MODELO DE CONFIANZA PARA HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN ENTORNOS UNIVERSITARIOS", previa a la obtención del título de INGENIERO EN SISTEMAS, realizado por el Señor Egresado: **FRANKLIN MAURICIO VEGA HIDALGO**, el que cumple con la reglas establecidas por la RAE, y por el normativo de presentación dispuesto por la carrera de Ingeniería en Sistemas.

Por lo que autorizo su presentación, posterior sustentación y defensa.

Arenillas, 17 de julio del 2014

KELVIN HUMBERTO PALADINES TINOCO

LICENCIADO EN CIENCIAS DE LA EDUCACIÓN

Figura 93: Anexo 31- Certificado de Corrección de Estilo y Ortografía.

32. Licencia Creative Commons

Figura 94: Anexo 32- Licencia Creative Commons.