UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

MODALIDAD PRESENCIAL

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

Análisis de Vulnerabilidades de la Red LAN de la UTPL

Trabajo de fin de carrera previa a la obtención del título de Ingeniera en Sistemas Informáticos y Computación.

AUTOR.

Srta. Angélica del Cisne Espinosa Otavalo.

DIRECTOR.

Ing. Carlos Gabriel Córdova E.

CO-DIRECTOR

Mgs. María Paula Espinosa V.

LOJA – ECUADOR
2010

CERTIFICACIÓN

Ingeniero.

Carlos Gabriel Córdova E.

DOCENTE INVESTIGADOR DE LA ESCUELA DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

CERTIFICA:

Haber dirigido y supervisado el desarrollo del presente proyecto de tesis con el tema ***"Análisis de Vulnerabilidades de la Red LAN de la UTPL"*** *previo a la obtención del título de* ***INGENIERA EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN****, y una vez que este cumple con todas las exigencias y los requisitos legales establecidos por la Universidad Técnica Particular de Loja, autoriza su presentación para los fines legales pertinentes.*

Loja, Noviembre del 2010

_____

Ing. Carlos G. Córdova E.

DIRECTOR DE TESIS.

CERTIFICACIÓN

Magister.

María Paula Espinosa V.

DOCENTE INVESTIGADOR DE LA ESCUELA DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

CERTIFICA:

Haber dirigido y supervisado el desarrollo del presente proyecto de tesis con el tema ***"Análisis de Vulnerabilidades de la Red LAN de la UTPL"*** *previo a la obtención del título de* ***INGENIERA EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN****, y una vez que este cumple con todas las exigencias y los requisitos legales establecidos por la Universidad Técnica Particular de Loja, autoriza su presentación para los fines legales pertinentes.*

Loja, Noviembre del 2010

_____

Mgs. María Paula Espinosa V.

CO-DIRECTOR DE TESIS.

AUTORÍA

El presente proyecto de tesis con cada una de sus observaciones, análisis, evaluaciones, conclusiones y recomendaciones emitidas, es de absoluta responsabilidad del autor

Además, es necesario indicar que la información de otros autores empleada en el presente trabajo está debidamente especificada en fuentes de referencia y apartados bibliográficos.

.....

Angélica del Cisne Espinosa Otavalo.

CESIÓN DE DERECHOS

Yo, Angélica del Cisne Espinosa Otavalo declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad".

.....

Angélica del Cisne Espinosa Otavalo.

AGRADECIMIENTO

Agradezco primeramente a Dios por darme la oportunidad de la vida.

A mis padres y hermanos por ayudarme incondicionalmente a convertir mi sueño en realidad.

A mis guías Director y Codirector por la paciencia y ayuda brindada para la final culminación de este proyecto de tesis.

A todas las personas del Grupo de Redes y Telecomunicaciones por su colaboración en todo lo que estuvo a su alcance.

A mis amigos, compañeros que compartimos muchos momentos dentro y fuera de las aulas y a todos los demás que me han brindado su amistad y cariño durante todo el tiempo de de mis estudios.

Gracias

Angélica Espinosa.

DEDICATORIA

De todo corazón dedico este trabajo a mis padres y hermanos que son siempre mi sustento y fuente de inspiración para enfrentar los obstáculos de la vida y terminar a cabalidad la tesis.

También a mis familiares, amigos y compañeros que me dieron una mano cuando más lo necesité

A mis tutores de tesis y profesores de aula por haberme impartido sus conocimientos y ser parte de mi formación académica y personal.

Con Amor

Angélica Espinosa.

INDICE DE CONTENIDO

CAPÍTULO 2
ESQUEMA ACTUAL DE SEGURIDAD DE LA UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

CAPÍTULO 3.
ANÁLISIS DE RIESGOS DE LOS SERVICIOS DE LA RED LAN DE LA UTPL DESDE LA PERSPECTIVA DEL USUARIO FINAL.

INDICE DE FIGURAS

CAPITULO 1.

CAPITULO 2.

CAPITULO 3.

CAPITULO 4.

INDICE DE TABLAS

CAPITULO 1.

CAPITULO 2.

CAPITULO 3.

ANEXO I.

ANEXO II.

ANEXO III.

RESUMEN

Este proyecto fin de carrera se orienta al análisis de vulnerabilidades de la red LAN de la UTPL enfocado al usuario final, determinando cuales son los riesgos y amenazas que están expuesto y el impacto en el caso de que estos llegarán a suceder; para llevar a cabo este proceso, se realizó un test de intrusión interno en un entorno de laboratorio de pruebas con la guía de un conjunto de procesos híbridos seleccionados de "Open Source Security Testing Methodology Manual" OSSTMM y de "Operationally Critical Threat, Asset, and Vulnerability Evaluation" OCTAVE.

Del resultado de este test se generó un plan de acción con estrategias de protección preventivas, correctivas y detectivas para mitigar el impacto de los riesgos; la metodología híbrida OSSTMM-OCTAVE que se ajusta al entorno de la Universidad, además un conjunto de políticas de seguridad de la información enfocados al usuario final con normativas mínimas que debería tomar en cuenta con el objetivo de preservar las características de la seguridad de la información que se identifican por la confidencialidad, integridad y disponibilidad.

INTRODUCCIÓN

La Red LAN de la Universidad se ha ido incrementando en su infraestructura física y lógica cada día más, el internet hace unos años atrás fue un lujo, en tanto que ahora se ha convertido en una necesidad para los usuarios finales usándola para un sin número de tareas, pero no todo es transparente y seguro, de tal forma como ha ido incrementando las tecnologías, también las amenazas, las mismas que explotan vulnerabilidades que finalmente se convierten en riesgos potenciales.

El tan solo hecho que los usuarios finales hagan uso de la red LAN por diferentes razones, desde ese momento están corriendo el riesgo de ataques originados por malware, hackers, personas curiosas o en casos por descuido de las personas mismas, pero lo crítico es que hay usuarios que han sido víctimas sin ser consciente de ello, dando como resultado el desconocimiento de las medidas a tomar o el impacto del riesgo que están expuesto.

Pues ahora existen en el mercado herramientas gratuitas o comerciales que permiten realizar un test de intrusión o análisis de vulnerabilidades con el objetivo de prevenir ataques y la apertura de metodologías de ethical hacking.

La estructura de la tesis está conformada por 5 capítulos

Capítulo 1 es el Estado del Arte de la Seguridad en Redes LAN donde se define algunos términos concernientes a la seguridad, las amenazas, la clasificación de los ataques y las vulnerabilidades en los sistemas informáticos, herramientas para la evaluación de vulnerabilidades y riesgos, se menciona algunas mejores prácticas de seguridad y finalmente los proyectos relacionados.

El capítulo 2 denominado Esquema actual de Seguridad de la Universidad Técnica Particular de Loja, señalando la infraestructura de seguridad implementada tanto para la red LAN, Inalámbrica, red WAN, equipos de gestión de seguridad y la tecnología de Voz/IP.

El capítulo 3 es el Análisis de riesgos de los servicios de la red LAN desde la perspectiva del usuario final, pues en este se refleja la aplicabilidad del conjunto de procesos seleccionados de las metodologías OSSTMM[1] y OCTAVE[2], y los resultados arrojados durante el test de penetración en un entorno de pruebas y estrategias de protección.

En el capítulo 4 es de Discusión de Resultados.

Finalmente el capítulo 5 hace mención a las conclusiones, recomendaciones y proyectos futuros que se han logrado obtener por la culminación del proyecto de tesis.

OBJETIVOS.

Objetivo General.

- Indicar el grado de seguridad de exposición actual que enfrentan los usuarios al utilizar la Red LAN.

Objetivos Específicos.

- Evaluar la seguridad del uso de la telefonía sobre IP, seguridad física, seguridad inalámbrica y tecnologías de internet.

[1] Manual de la metodología abierta de testeo de seguridad. Es una metodología para la realización de pruebas de seguridad. Disponible en http://www.isecom.org/osstmm/
[2] Es una metodología para evaluación de riesgos. Disponible en http://www.cert.org/octave/

- Comprobar el nivel de conocimiento o de conciencia de parte de los usuarios en el ámbito de seguridad.
- Determinar el nivel de exposición presente en la red ante ataques de un hacker.
- Comprobar la facilidad con la que un Script Kiddies[3] podría llegar a obtener información sensible y usarla para fines maliciosos aprovechando las brechas de seguridad.
- Determinar la calidad de las claves usadas para el acceso a aplicaciones y otros elementos.
- Evaluar el impacto de los riesgos que está expuesto el usuario final.

RESULTADOS ESPERADOS.

Al finalizar este proyecto de tesis.

- El grupo de Seguridad poseerá conocimiento más a detalle sobre los riesgos que están expuestos los usuarios finales.
- El área de Seguridad de la Información de la universidad tendrá información que le servirá de guía y apoyo para hacer un Ethical Hacking posterior.
- Un informe final detallando los hallazgos encontrados durante el test de intrusión interno, un plan de acción para mitigar los riesgos y políticas de seguridad enfocados al usuario final.
- Verificar que el eslabón débil causante de la ruptura de la cadena de la tecnología de la información es el usuario final, por lo tanto se debe dar una oportuna capacitación y un programa de concientización.

[3] Son personas que utilizan programas sin ningún conocimiento de programación o redes.

"Si no puedes ser fuerte, pero tampoco sabes ser débil, serás derrotado."

Sun Tzu

CAPÍTULO 1.

SEGURIDAD EN REDES LAN.

Resumen.

En este trabajo se describe diferentes criterios de seguridad relevantes que se debe conocer para garantizar una mayor seguridad en el entorno de redes LAN.

Sobre todo los procesos en las organizaciones se han convertido en dependientes de la tecnología y el internet; sin embargo es importante mencionar que así como aumentan los avances tecnológicos cada día, también aumentan las amenazas a la seguridad.

Por lo tanto para mantenerse fuera de estos problemas es necesario conocer las mejores y eficientes soluciones de seguridad que existen, no hay una aplicación que proteja el 100% ante estas dificultades, se plantea diferentes metodologías y buenas prácticas que contrarresten estos efectos.

1.1 Introducción.

La Seguridad actualmente es un aspecto muy importante a considerar en todo tipo de ámbito organizacional, por lo tanto tomar las medidas necesarias es garantizar que los activos estén disponibles en cualquier momento. Cabe recalcar que la información es el elemento más sensible de una entidad, la cual debe ser protegida.

Una red LAN siempre se encuentra bajo constantes ataques y amenazas ocasionadas por circunstancias internas o externas; sin embargo es tiempo de implementar técnicas y/o mecanismos para reducir las vulnerabilidades[4] y riesgos al que está sometido constantemente.

Se debe conocer los aspectos importantes de la seguridad como son: *Confidencialidad, Integridad y Disponibilidad*; definitivamente es imposible alcanzar un 100% de seguridad.

A través de este documento se da un enfoque a un esquema de seguridad para redes LAN[5] en el que se define conceptos introductorios a este tema, cuya estructura está organizada como se detalla a continuación:

En la sección 1.2 se define el término seguridad, que incluye los aspectos de seguridad (sección 1.2.2), tres leyes de seguridad (sección 1.2.3), seguridad física (sección 1.2.4) seguridad lógica (sección 1.2.5), amenazas de la seguridad de la información (sección 1.3). En la sección 1.4 ataques informáticos, a continuación en la sección 1.5 se detalla la seguridad en la red LAN, también en la sección 1.6 se define la seguridad en protocolos de cada capa de la pila TCP/IP; vulnerabilidades, se describen en la sección 1.7, así mismo en la sección 1.8 las herramientas para la evaluación de vulnerabilidades incluyendo las metodologías de test de penetración y análisis de riesgos, sección 1.9 las mejores prácticas y por último en la sección 1.10 proyectos relacionados.

Finalmente este análisis introductorio de terminología conlleva a tener una visión general del tema.

Palabras Claves. Seguridad, Riesgos, red LAN, Políticas. IPv4, IPv6, OSSTMM, OTP, OCTAVE, ISSAF, Vulnerabilidad, Ataques.

[4] Debilidad en un sistema
[5] Red de área local.

1.2 Seguridad.

1.2.1 Definición.

Son las medidas que permiten evitar la realización de acciones no autorizadas que afecten de alguna manera la confidencialidad, autenticidad o integridad de la información y que de la misma forma garanticen el funcionamiento correcto del equipo y la disponibilidad de éste para los usuarios legítimos. [22]

Siempre hay que tener en cuenta que la seguridad comienza y termina con las personas [1] por eso se necesita tiempo, dinero y esfuerzo para conseguirla.

Algunas organizaciones suponen que su información no es vulnerable o interesante para los atacantes, por tal razón no realizan una búsqueda de vulnerabilidades.

1.2.2 Aspectos importantes de la seguridad. [4]

En la seguridad se ha considerado tres aspectos importantes que son:

- *Confidencialidad.* Servicio de seguridad que asegura que la información no pueda estar disponible o ser descubierta por procesos no autorizados.

- *Disponibilidad.* Un sistema seguro debe mantener la información, hardware y software disponible para los usuarios todo el tiempo.

- *Integridad.* Condición de seguridad que garantiza que la información deber ser creada, modificada y borrada sólo por el personal autorizado.

Por lo tanto el objetivo de la seguridad es: preservar cada una de las características mencionadas inicialmente.

En la figura 1.1 muestra la pirámide de los servicios de seguridad.

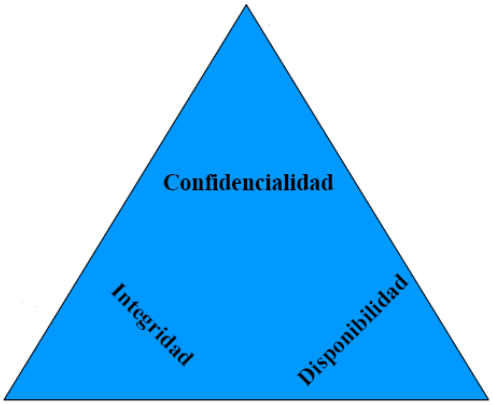

Figura 1.1 **Servicios de la seguridad [7]**

1.2.3 Tres leyes de seguridad [11].

Se define tres leyes de seguridad:

- No existen sistemas absolutamente seguros.
- Para reducir su vulnerabilidad a la mitad se tiene que doblar el gasto en seguridad.
- Típicamente, los intrusos brincan la criptografía[6], no la rompen.

1.2.4 Seguridad Física.

Este aspecto no es tomado muy en cuenta a la hora del diseño de un esquema de redes, sin embargo, es un punto importantísimo ya que permite *"la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial*" [1], es decir la implementación de mecanismos, controles de acceso físico u otros componentes para preservar los sistemas tangibles de la organización.

Las amenazas pueden ser:

- Casos fortuitos o caso mayor (terremotos, inundaciones, tormentas, etc.).
- Intencionados por el hombre (robos, demoliciones, incendios etc.).

[6] Técnica de protección para documentos y datos

1.2.5 Seguridad Lógica.

Consiste en la *"aplicación de barreras y/o procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo*" [4].

Existen muchos controles para la seguridad lógica como se puede evidenciar en la tesis "Seguridad Informática: sus Implicancias e Implementación" pero se ha considerado los siguientes:

- **Roles.**

  Esto se lo realiza controlando a través de la función o rol del usuario que requiere dicho acceso.

- **Controles de acceso.**

  Constituyen en la implementación de controles en cualquier utilitario de red para mantener la integridad de la información y resguardar los datos confidenciales de accesos no autorizados.

- **Autenticación, identificación.**

  La identificación es el momento en que el usuario se da a conocer al sistema y autenticación se refiere a la verificación que realiza el sistema sobre esta identificación.

- **Listas de control de acceso ACL's.**

  Su objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a diferentes condiciones establecidas en los equipos de redes.

- **Limitaciones a los servicios.**

  Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador.

1.3 Amenazas de la seguridad de la información [22].

Las amenazas se dividen en cuatro categorías, que se describen en la tabla 1.1

Tabla 1. 1 **Categorías de las amenazas de seguridad de la información.**

Categoría	Descripción
Interrupción.	Disponibilidad de una parte o total del sistema.
Intercepción.	Confidencialidad.
Modificación.	Ataque contra la integridad.
Fabricación.	Autenticidad.

1.4 Ataques informáticos.

Clasificación de ataques:

- *Ataques pasivos.* Estos ataques se basan en escuchar los datos que son transmitidos pero no en modificarlos.

- *Ataques activos.* Por el contrario de los ataques pasivos estos modifican o alteran la información que ha sido interceptada, con el fin de hacer daño.

A continuación, una lista de algunos ataques informáticos que pueden ser originados por personas internas o externas. [22].

- Actividades de reconocimiento de activos.
- Detección de vulnerabilidades en los sistemas.
- Robo de información.
- Modificación del contenido y secuencia de los mensajes transmitidos.
- Análisis de tráfico.
- Ataques de suplantación de identidad.
- Conexiones no autorizadas.
- Introducción de código malicioso.
- Denegación de servicio.

Según el estudio realizado por CYBSEC [2] demuestra que un 80% de los ataques realizados son internos y el 20% ataques externos. Ver la tabla 1.2 en la cual presenta los porcentajes de ataques internos y externos en los años 2000, 2002, 2005 y 2008 y también apoyándose con un estudio de Seguridad IT realizado por Symantec [18].

Tabla 1. 2 **Porcentaje de Ataques internos y externos por año [2] [18].**

Ataques por año	2000	2002	2005	2008
Externos	**30%**	**25%**	**20%**	**40%**
Internos	**40%**	**70%**	**75%**	**59%**

Y con más claridad se diferencia en la figura 1.2. Por tal razón se ha optado por realizar el test de penetración interno para corroborar con estas afirmaciones.

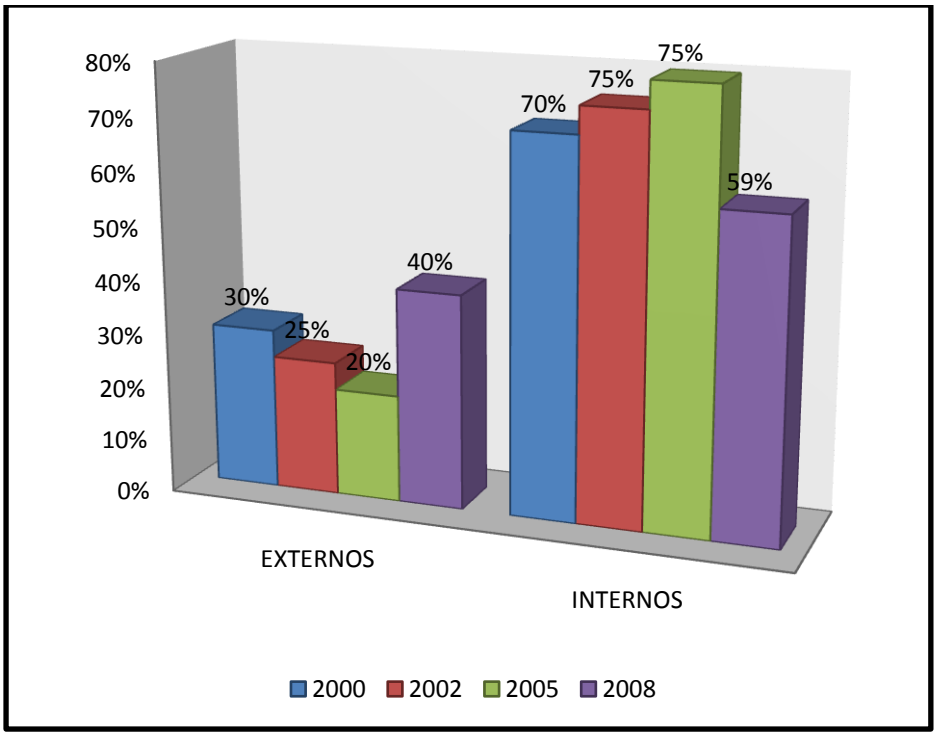

Figura 1. 2 **Porcentaje de los ataques internos y externos.** [2]

Un detalle de las mayores preocupaciones en seguridad informática aparece en la figura 1.3, realizado por ESET en su informe anual del 2009.

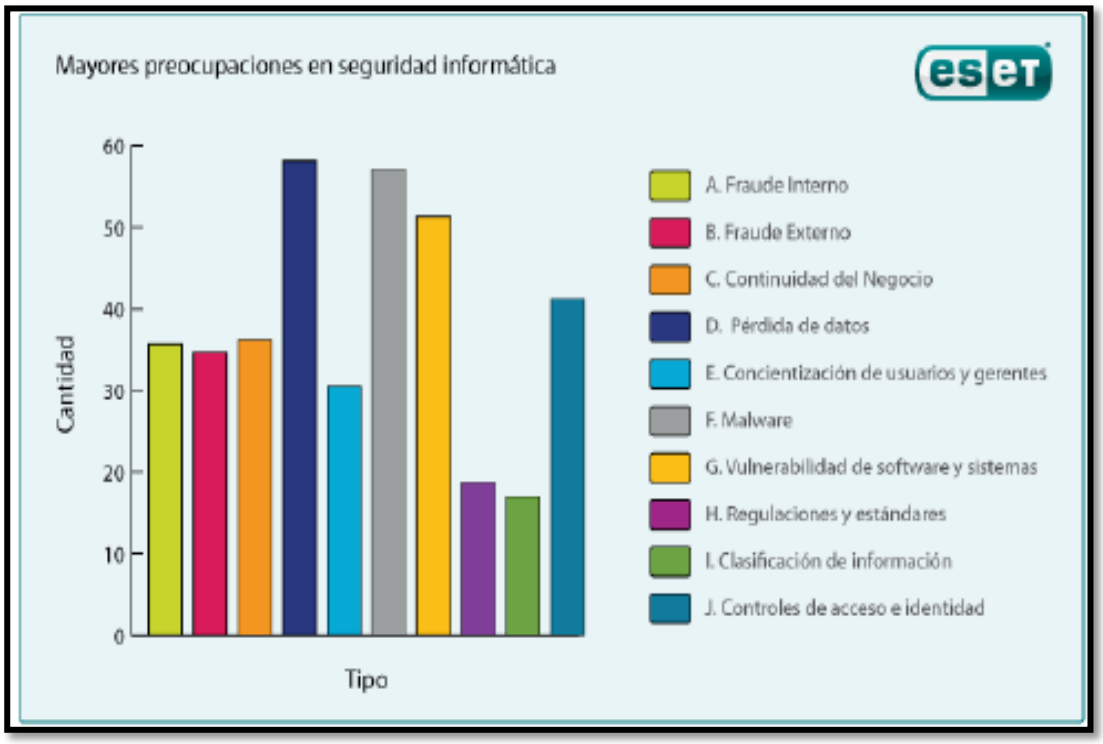

Figura 1. 3 **Mayores preocupaciones en Seguridad Informática. [6]**

Gracias a este informe se determinó cuales son los riesgos más comunes.

Así mismo los servicios internos como externos comparten riesgos comunes tales como:

- Intercepción de las comunicaciones.
- Suplantación de identidad.
- Interrupción de las actividades de los servicios.
- Robo de información.
- Introducción de código malicioso.
- Alteración de la información.

Para comprometer la seguridad de cualquier sistema el atacante debe tener conocimiento de 4 etapas para realizar un test de penetración [12]. Ver figura 1.4.

Figura 1. 4 **Etapas de un test de Penetración.**

Sin embargo, al tener un conocimiento de las etapas, estas forman un triángulo de intrusión como puede apreciarse en la figura 1.5, el atacante para realizar un test de penetración tiene conocimiento de las herramientas, mecanismos, entre otros, como también conoce las oportunidades y el motivo que lo conlleva a llevar a cabo este test de intrusión.

Figura 1. 5 **Triángulo de la intrusión. [22]**

Es indispensable también tener un conocimiento de los modos de hacking ético que se puede hacer según los requerimientos de la organización. [20]

- Ataque local.
- Ataque remoto.
- Ataque con equipo robado.
- Ataque a entradas físicas de la organización.
- Ataque por medio de equipos sin autenticación.
- Ataques de ingeniería social.

En el caso de este proyecto se consideró el modo de Ataque local debido a que este simularía un ataque hecho por el personal interno el cual tiene acceso a la red de la Universidad, tal es el caso de profesores, estudiantes, empleados, entre otros.

1.5 Seguridad en la Red LAN.

La tabla 1.3 demuestra los requisitos mínimos generales de seguridad que debe poseer una red LAN.

Tabla 1. 3 **Requisitos generales para asegurar la red LAN. [1] [4]**

Necesidades	Beneficios
Conocer al detalle las aplicaciones de la red y capacidad para controlarlas.	• Reducción en las inversiones en ancho de banda. • Mejora del rendimiento de la red. • Ahorre de costos. • Disminución de problemas.
Firewall de aplicación.	• Definición de políticas de control y bloqueo a nivel de aplicación, usuario, servicio, etc.
Sistema central de informes.	• Contar con historiales para el seguimiento de incidencias. • Poder escalar a los superiores el conocimiento detallado de la red para toma de decisiones.
Control de flujos no deseados.	• Detección y control de ataques de spam[7], DoS, [8]troyanos[9]. • Conocer que usuarios generan dichos flujos.
Mejorar el rendimiento.	• Controlar el tráfico.
Sistema de alertas.	• Saber lo que pasa en la red en el momento oportuno.

[7] Correo electrónico no solicitado.
[8] Ataque de denegación de servicios.
[9] Programa malicioso.

Por lo tanto, al tener una red LAN sin las medidas adecuadas de seguridad es peligrosa, sin embargo se han mencionado estos requisitos mínimos generales de seguridad para combatir la inseguridad.

La red LAN inalámbrica no es una red diferente que la red cableada, se deben considerar iguales y/o combinar las políticas de seguridad.

1.6 Seguridad en las capas de la pila TCP/IP.

La tabla 1.4 muestra las cuatro capas de la pila de protocolo TCP/IP y algunos elementos de seguridad que se pueden aplicar en cada una de ellas.

Tabla 1. 4 **Seguridad en las capas de la pila de protocolos TCP/IP.**

Capa	Protocolos
Aplicación.	HTTPS, SSH.
Transporte.	TCP, UDP sobre SSL o TLS.
Red.	IPv4, IPv6, IPSEC.
Física + Enlace.	L2TP, Ethernet, PPTP.

1.7 Vulnerabilidades en los Sistemas Informáticos.

1.7.1 Causas de las vulnerabilidades [22].

Según el autor del libro "Enciclopedia de Seguridad Informática" ha considerado diversas causas de las vulnerabilidades según el reporte de ESET, se listan a continuación:

- Debilidad en el diseño de los protocolos utilizados en las redes.
- Errores de programación.
- Configuración inadecuada de los sistemas informáticos.
- Política de seguridad deficiente o inexistente.
- Desconocimiento de las herramientas que facilitan los ataques.
- Existencia de puertas traseras.

- Limitación gubernamental.
- Descuido de los fabricantes.

Debido a estas causas se han originado los siguientes tipos de vulnerabilidades.

- Vulnerabilidades que afectan a equipos
- Vulnerabilidades que afectan a programas y aplicaciones informáticas.

1.7.2 El Factor humano [17] [20].

Según el autor Martin Vila de ISEC[10] , define "la seguridad depende principalmente del factor humano en menor grado del factor tecnológico."

Jorge Arango, Manager Unit Security & ITS de Getronics. "El usuario es el eslabón más débil para evitar fraudes y garantizar la seguridad informática en cualquier organización".

De acuerdo con Luis Gonzalo Acosta, especialista en seguridad de IBM Colombia, "un gran porcentaje de robos a través de transacciones virtuales y acciones irregulares que están ocurriendo con relación a la seguridad informática, es producto del descuido de aquellos usuarios que tienen privilegios de acceso a tareas críticas dentro de las organizaciones".

Para Daniel Rojas, Marketing Manager para Latinoamérica de Symantec, el tema es claro: en el país las aplicaciones y prácticas de seguridad informática que eviten las transacciones fraudulentas no se van a masificar hasta tanto no exista conciencia sobre el real valor (costo vs. beneficio) que implica proteger la información sustancial para el negocio. [17].

Se estima que el 82% de la pérdida de datos sensibles de una compañía la producen los mismos empleados. [20].

Por lo tanto con toda estas afirmaciones se puede decir que el usuario final es el eslabón más débil de la cadena de IT, esto se ha suscitado ya sea por desconocimiento, poca cultura de seguridad o falta de concientización.

[10] Information security INC

1.8 Herramientas para la evaluación de vulnerabilidades y riesgos.

1.8.1 Metodologías de test de penetración[11].

Las metodologías para el test de penetración son:

- OSSTMM
- ISSAF
- OTP

1.8.1.1 OSSTMM (Manual de la metodología abierta de testeo de seguridad) [8].

Es una metodología para realizar un test de penetración, permitiendo evaluar la seguridad cuantificando el nivel de riesgo, además describe qué pasos hacer antes, durante y después de un test de penetración.

Cumple con los estándares ISO[12] 17999-BS7799, es un conjunto de reglas que se refieren el para qué, cómo y por qué del testeo.

Sustentada por ISECOM[13], además está divida en seis secciones en donde cada una está conformada por un conjunto de módulos.

Las secciones que se ha considerado en este trabajo son:

- Seguridad física.
- Seguridad en las comunicaciones.
- Seguridad inalámbrica.
- Seguridad en las tecnologías de la información.

11 Test de Ethical Hacking.
12 Organización Internacional de Estándares. Desarrollado de Estándares.
13 Institute for Security and Open Methodologies.

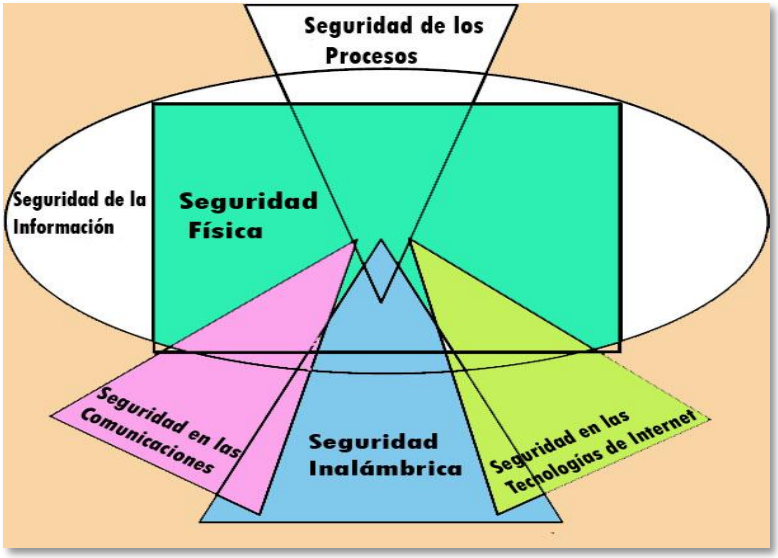

Figura 1. 6 **Mapa de seguridad de la Metodología OSSTMM. [17]**

En la figura 1.6 solo se han pintado las secciones mencionadas anteriormente, se han optado estas cuatro secciones ya que cumplen con lo establecido para la investigación como: testear la red inalámbrica, Voz/IP, red cableada, la robustez de las contraseñas y seguridad física.

También emplea una técnica denominada "Seguridad Perfecta" dentro de la evaluación de riesgos, en donde los analistas pueden realizar una comparación con la Seguridad actual y la seguridad Perfecta.

1.8.1.2 ISSAF (Information systems security assessment framework) [16].

Constituye un framework[14] detallado referente a las prácticas y conceptos relacionados con todas y cada una de las tareas a realizar al conducir un testeo de seguridad.

La información contenida dentro de ISSAF, se encuentra organizada alrededor de lo que se ha dado en llamar "Criterios de Evaluación".

Estos criterios de evaluación a su vez, se componen de los siguientes elementos ver figura 4:

- Una descripción del criterio de evaluación.
- Puntos y objetivos a cubrir.
- Los pre-requisitos para conducir la evaluación.
- El proceso mismo de evaluación.

[14] Es una estructura de soporte.

- El informe de los resultados esperados.
- Las contramedidas y recomendaciones.

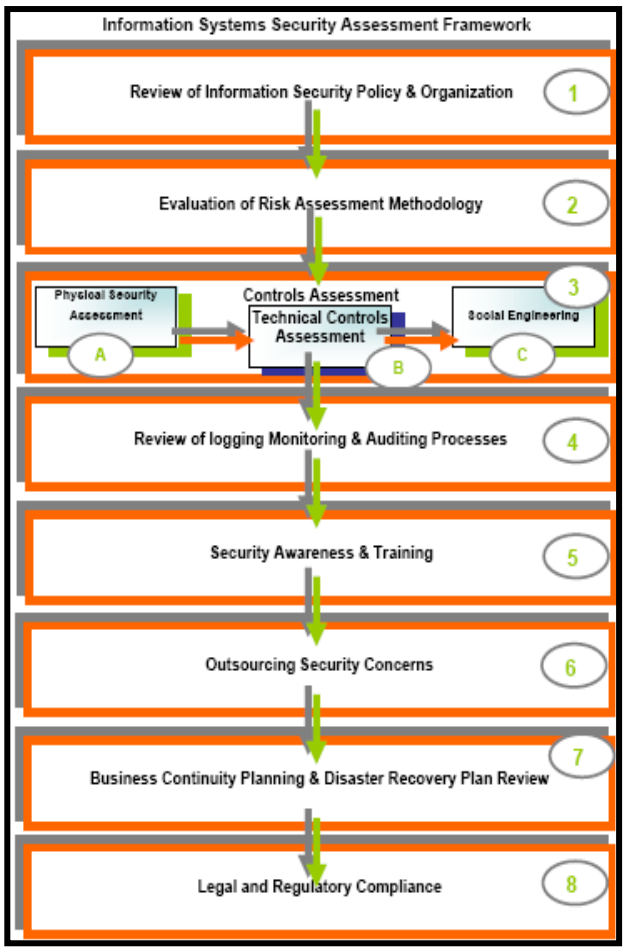

Figura 1. 7 **Elementos del criterio de evaluación de ISSAF** [16].

Esta metodología requiere que el framework se mantenga actualizado con el objetivo que sus partes no se vuelvan obsoletas, no por esto es una desventaja sino más bien un punto para tomar en cuenta. Ver figura 1.7.

1.8.1.3 OTP (OWASP Testing Project) [14].

Es un proyecto de aplicaciones web que está divido en dos partes, la primera parte consta de los siguientes puntos:

- Principios del testeo.
- Explicación de las técnicas de testeo.
- Explicación general acerca del framework de testeo de OWASP.

En la segunda parte se realiza una planificación de todas las técnicas para testear relacionado con el "Ciclo de vida del desarrollo de software" a fin de que el testeo sea al inicio antes que la aplicación esté en producción.

Los elementos incluidos a testear son:

- Personas.
- Procesos y
- Tecnología.

Paso 1 Antes de comenzado el desarrollo.

a) Revisión de políticas y estándares.

b) Desarrollo de un criterio de medidas y métricas.

Paso 2 Durante la definición y el diseño.

a) Revisión de los requerimientos de seguridad.

b) Diseño de revisión de arquitectura.

c) Creación y revisión de modelos UML.[15]

d) Creación y revisión de modelos de amenazas.

Paso 3 Durante el desarrollo.

a) Code Walkthroughs.[16]

b) Revisión de código.

Paso 4 Durante el deployment.[17]

a) Testeo de penetración sobre la aplicación.

b) Testeo sobre la administración y configuración.

Paso 5 Operación y mantenimiento.

a) Revisión operacional.

b) Conducción de chequeos periódicos.

c) Verificación del control de cambio.

[15] Lenguaje unificado de modelado
[16] Técnica de revisión de código
[17] Depuración de código

1.8.2 Herramienta para el análisis de riesgos [2] [13].

Se cuenta con varias herramientas para el análisis de riesgos como:

- OCTAVE.
- MAGERIT.
- CRAMM.
- COBRA.

1.8.2.1 OCTAVE (Amenazas Críticas Operacionales, Activos y Evaluación de Vulnerabilidades). [13].

Maneja los activos de una organización como son las personas, hardware, software, información y sistemas, permitiendo la identificación y evaluación del impacto de dichos riesgos afectando los principios de la seguridad.

Está organizado en tres fases y cada uno se subdivide en varios procesos.

- Fase I. Construir perfiles de amenazas basados en activos.
    - Proceso 1. Identificación de la información a nivel gerencial.
    - Proceso 2. Identificación de la información a nivel operacional.
    - Proceso 3. Identificación de la información al usuario final.
    - Proceso 4. Consolidación de la información y creación de perfiles de amenaza.
- Fase II. Identificar los puntos vulnerables en la infraestructura.
    - Proceso 5. Identificación de componentes claves.
    - Proceso 6. Evaluación de componentes seleccionados.
- Fase III Desarrollo de planes y estrategias de seguridad.
    - Proceso 7. Análisis de riesgos.
    - Proceso 8. Desarrollar estrategias de protección.

La figura 1.8 lista las fases, procesos y subprocesos ya antes mencionados.

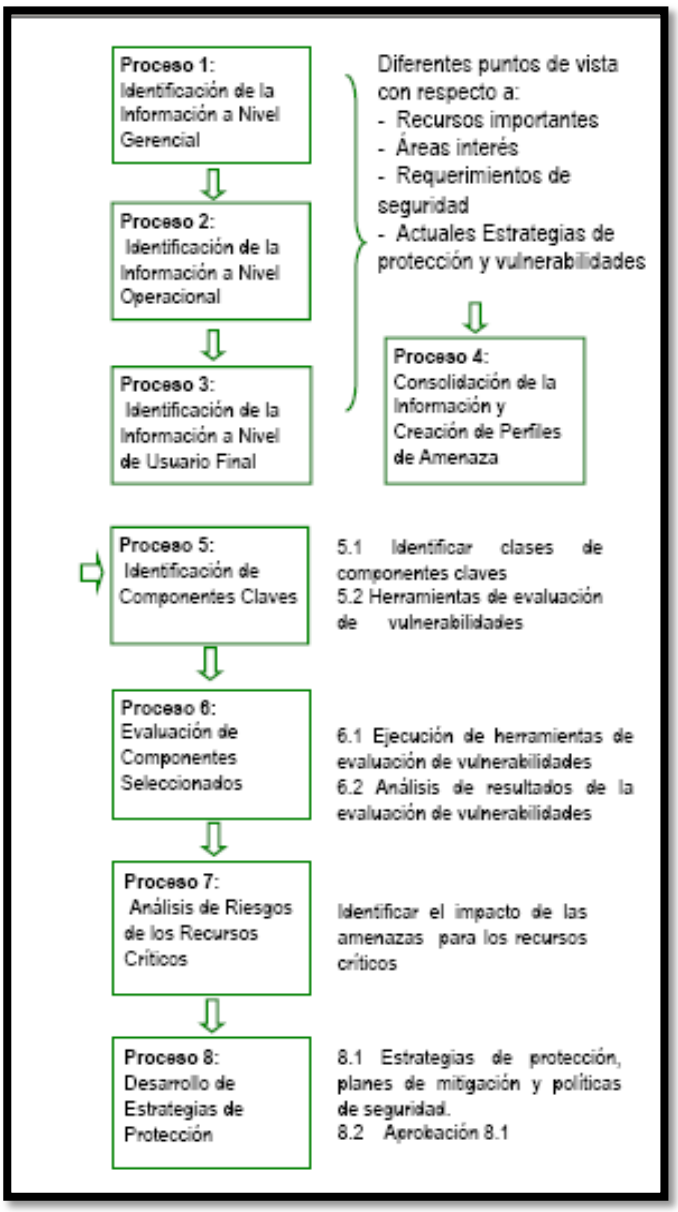

Figura 1. 8 **Procesos de OCTAVE** [13].

1.8.2.2 MAGERIT.

Metodología de análisis y gestión de riesgos de los sistemas de información de las administraciones públicas está compuesta por una serie de guías y una herramienta de apoyo**.**

1.8.2.3 CRAMM.

Risk analysis and Management Method, herramienta para el análisis de riesgos y definición de las buenas prácticas de seguridad.

1.8.2.4 COBRA.

Herramienta comercial definido como un consultor externo ayudando a la toma de decisiones de seguridad.

1.9 Mejores prácticas enfocadas a la seguridad de la información.

A continuación se destacan las mejores prácticas de seguridad para la seguridad de la información:

- Políticas de seguridad.
- Inventarios de activos.
- Norma ISO 27001.
- Aplicar un cuestionario al administrador de la red.
- Fomentar la concientización sobre seguridad de la red LAN.
- Implementar niveles de seguridad informática.
- Utilizar un plan de contingencia.

1.9.1 Políticas de seguridad [3].

Es un documento detallado de cada uno de los procedimientos con el fin de obtener un sistema seguro, confiable para evitar cualquier ataque intencional o causal, así mismo es una descripción de lo que deseemos proteger y porqué.

Las Políticas de seguridad tendrán que basarse en las siguientes características:

- Identificar y seleccionar lo que se debe proteger.
- Establecer niveles de prioridad.
- Saber las consecuencias como tiempo y costo.

- Identificar las amenazas y niveles de vulnerabilidad.
- Realizar un análisis de costos.
- Implementar respuestas a incidentes.

1.9.2 Inventarios de activos [3].

Contar con un inventario de todos los activos que conforman la red LAN es importante, con el objetivo de clasificarlos según su criticidad y desempeño determinando cual sería el impacto si llegaran a fallar.

1.9.3 Norma ISO-27001 [19].

Es un estándar internacional para la administración de la seguridad de la información, estableciendo los requisitos que debe cumplir un Sistema para la Gestión de la Seguridad de la Información **SGSI.**

Es basado en riesgos del negocio para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar seguridad de la información.

Un sistema de gestión incluye varios temas, pero se ha estimado los siguientes:

- Políticas.
- Procedimientos y
- Procesos.

Aplica una **aproximación por procesos** para la gestión de la seguridad de la información enfatizando la importancia de los siguientes aspectos [10].

- Comprensión de los requisitos de seguridad de la organización, necesidad de establecer una política y unos objetivos.
- Implementar controles para gestionar los riesgos en el contexto del negocio.
- Monitorizar el rendimiento del SGSI.
- Mejora continua basada en la medición de los objetivos.

Adopta el modelo **PDCA** (planificar, hacer, comprobar, actuar).

1.9.4 Aplicar un cuestionario al administrador de la red [3].

Un cuestionario contiene un conjunto de preguntas referentes a varios puntos de seguridad de la red LAN, verificando si el administrador de red está cumpliendo con los requisitos mínimos de seguridad.

1.9.5 Fomentar la concientización sobre seguridad de la red LAN [4].

Es importantísimo dar a conocer las políticas establecidas para la seguridad en la red LAN, dirigidas a todas las personas que obtienen un beneficio de los servicios y lo más importante enseñarles el verdadero sentido de la seguridad, realizando campañas de concientización para el correcto uso de las mismas.

1.9.6 Implementar niveles de seguridad informática [4].

Estructurar un estándar que divida diferentes niveles de seguridad clasificando los activos según la criticidad, importancia o riesgos que tiene la red LAN.

Un ejemplo puede ser nombrados de esta forma: Nivel A, Nivel B, Nivel C.

1.9.7 Utilizar un plan de contingencia. [4].

Este documento suministra vías alternas estableciendo controles y políticas para evitar desastres que atenten con la disponibilidad y continuidad de los procesos y poder restablecer el nivel operacional de la red LAN en el menor tiempo.

1.10 Proyectos relacionados.

- ***[Pinzón]*** Pinzón Olmedo Freddy Bolívar. *Identificación de vulnerabilidades, análisis forense y atención a incidentes de seguridad en los servidores de la UTPL*. [15].

  "En este trabajo se desarrolla una metodología para la identificación de vulnerabilidades en los servidores de la UTPL, se determina los niveles de riesgo y así mismo se establece una metodología de análisis forense".

Disponible en: http://www.segu-info.com.ar/tesis/

- **[Loayza]** Loayza *Carlos. Seguridad para la Red Inalámbrica de un Campus Universitario.* [10]

  "Este documento describe los problemas de seguridad en la red inalámbrica de la UTPL y los mecanismos de seguridad que se puede implementar".

Disponible: www.lacnic.net/documentos/lacnicxi/presentaciones/WiFi_UTPL.ppt

- **[Delgado-*Guaichizaca]*** Delgado Reyes Silvia Janeth, Guaichizaca Sarango Laura Amparo. *Análisis de la Influencia de los delitos informáticos e implementación de políticas para su prevención en la red y las plataformas de la Universidad Técnica Particular de Loja.* [5]

  "En esta investigación se realizó un estudio de los delitos informáticos, identificación de los riesgos y la aplicación de una metodología de test de penetración".

Disponible en http://www.utpl.edu.ec/eccblog/wp-content/uploads/2007/04/articulo-tecnico-analisis-de-la-influencia-de-los-delitos-informaticos-e-implementacion-de politicas_silviadelgado.pdf.

- **[Ochoa-Quinde-Uyaguari]** Ochoa José, Magali Quinde, Marieliza Uyaguari, *Evaluación de Amenazas y Vulnerabilidades de Recursos Críticos Operacionales (OCTAVE) a Nivel de usuario Final para la UTPL* [13].

  "Este proyecto de tesis estuvo orientado a evaluar los recursos críticos de la Universidad, utilizando la metodología OCTAVE, obteniendo resultados y en base a ellos se propuso soluciones.

Disponible en: http://www.utpl.edu.ec/eccblog/wp-content/uploads/2007/04/articulo-tecnico-evaluacion-de-amenazas-y-vulnerabilidades-de-recursos-criticos-operacionalesoctave-a-nivel-de-usuario-final-para-la-utpl.pdf.

No debemos depender de la posibilidad de que el enemigo no nos ataque, sino del hecho de que logramos que nuestra posición sea inatacable

Sun Tzu

CAPÍTULO 2.

ESQUEMA ACTUAL DE SEGURIDAD DE LA UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA.

Actualmente la Universidad Técnica Particular de Loja cuenta con un esquema de seguridad que se detalla en la figura 2.1, en donde existen equipos de gestión de seguridad como: firewall, IPS del firewall, IDS del Core, VPN, IME y OSSIM.

La red de la UTPL consta de tres elementos, la red WAN (1), la red LAN (2), y la DMZ[18] (3) en donde se encuentran alojados servidores internos como el proxy, dhcp entre otros.

[18] Zona desmilitarizada donde están ubicados los servidores que tienen conectividad con el exterior.

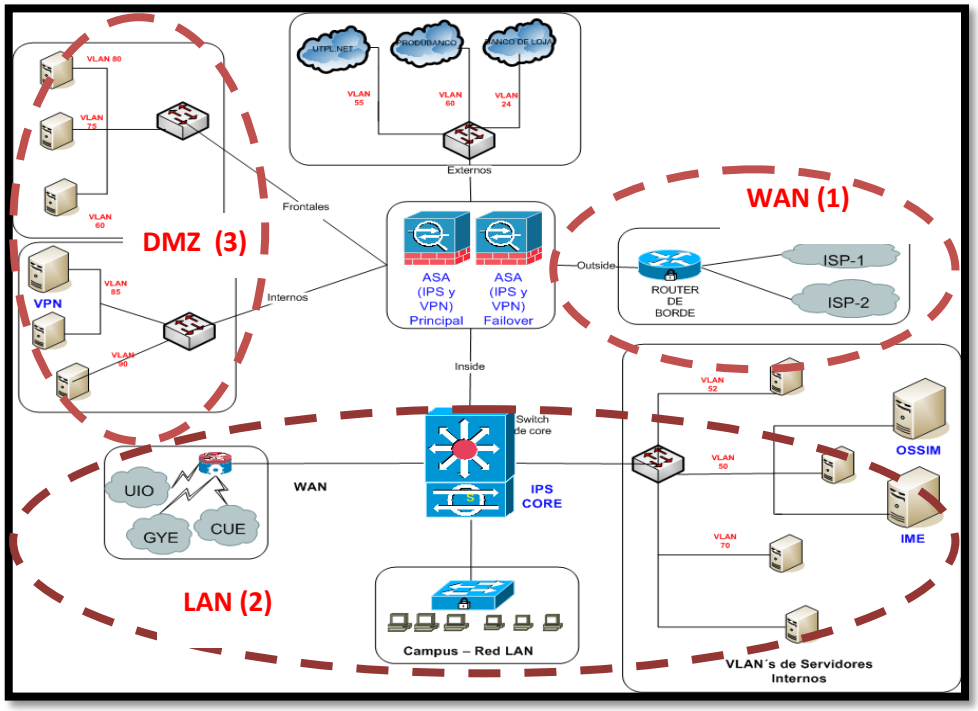

Figura 2. 1 **Esquema de Seguridad de la UTPL**[19]

2.1 Sistema de gestión de seguridad.

2.1.1 Equipos de gestión de seguridad.

Los equipos de seguridad que se han implementado en la UTPL son:

2.1.1.1 Servidor IME.[20]

Tiene la función de almacenar los logs[21] o registros de todos los IPS[22]. Los logs se almacenan en una base de datos mysql[23], realiza también la correlación de eventos enviando una alerta al administrador del equipo informando la alteración del comportamiento, además por medio de este servidor se ingresa a los IPS para verificar el estado y las configuraciones de los mismos.

2.1.1.2 Servidor OSSIM.[24]

OSSIM es un potente componente de seguridad el cual tiene consigo varias herramientas, ver tabla 2.1

[19] Documentación del Grupo de Telecomunicaciones tomado el 27 de Noviembre del 2010.
[20] IPS Management Express.
[21] Archivo creados y administrados de un servidor.
[22] Sistema de Prevención de Intrusos.
[23] Es una base de datos relacional.
[24] Open Source Security Information Management: es una herramienta de monitorización de seguridad.

Tabla 2. 1 **Herramientas de OSSIM.**

Herramienta	Versión	Definición
Nessus	2.2	Escáner de vulnerabilidades.
Osiris	4.2	IDS de red.
Snort	2.7	Monitorea el sistema de archivos de cada servidor.
SYSLOG: [25]	2.0	Las autenticaciones que son realizadas al ASA y Core, se envían al Syslog para almacenarlas.

Principalmente las funciones del OSSIM son:

- Almacenamiento de los registros de los IPS, servidores y el firewall ASA.
- Gestión de vulnerabilidades.

OSSIM cuenta con dos interfaces:

- Interfaz de monitoreo en modo promiscuo para capturar el tráfico de entrada y salida.
- Gestión de vulnerabilidades.

Ventajas.

- Trae consigo varias herramientas.
- Permite obtener reportes para la gestión de vulnerabilidades.

2.1.1.3 Firewall.

Determina que servicios entran y salen estableciendo políticas de acceso desde internet hacia la red interna o viceversa como también de la DMZ mediante ACL's aplicadas hasta la capa de transporte. Permite que el tráfico que entra y sale de los servidores sea analizado por los IPS antes de llegar a su destino.

2.1.1.4 VPN. [26]

Es un canal seguro que permite una extensión de la red LAN sobre una red pública que es el Internet.

[25] Estándar para la transferencia de mensajes de eventos y alertas.
[26] Red Privada Virtual

Se tiene dos tipos de VPN.

- **VPN en el ASA.** Configurada en el ASA para que puedan ingresar a la red interna, destinada para los centros regionales y administradores externos de los servidores, por lo que puede tener acceso a todas las aplicaciones.

- **VPN Físico.** Servidor físico orientado al administrador con acceso interno o externo a través de la web con OpenSSL, la dirección es https://vpn.utpl.edu.ec

Existen 3 perfiles de usuario VPN con diferentes permisos como son:

- VPN-UTPL. General para los administradores.
- VPN-BANCOLOJA, VPN-GUAYAQUIL. Acceso al BAAN de la UTPL.
- VPN-I02 UTPL. Usuarios.

VPN utiliza el protocolo IPSEC [27] y el protocolo SSL.[28]

2.1.1.5. IPS del Firewall, IPS del CORE.

Es un sistema de prevención de intrusos que controla los ataques destinados a los servidores y además incrementar el nivel de seguridad del tráfico entrante y saliente de los servidores.

Políticas: activar firmas. (Actualizan las firmas).

Estos tres IPS, 2 de ellos están ubicados en el firewall ASA y el otro en el Switch de Core.

2.2 Red LAN.

2.2.1 Tipo de modelo de referencia.

El modelo de referencia utilizado es TCP/IP.

[27] Protocolo de Internet seguro
[28] Protocolo de Capa de Transporte para la Conexión Segura

2.2.2 Topología.

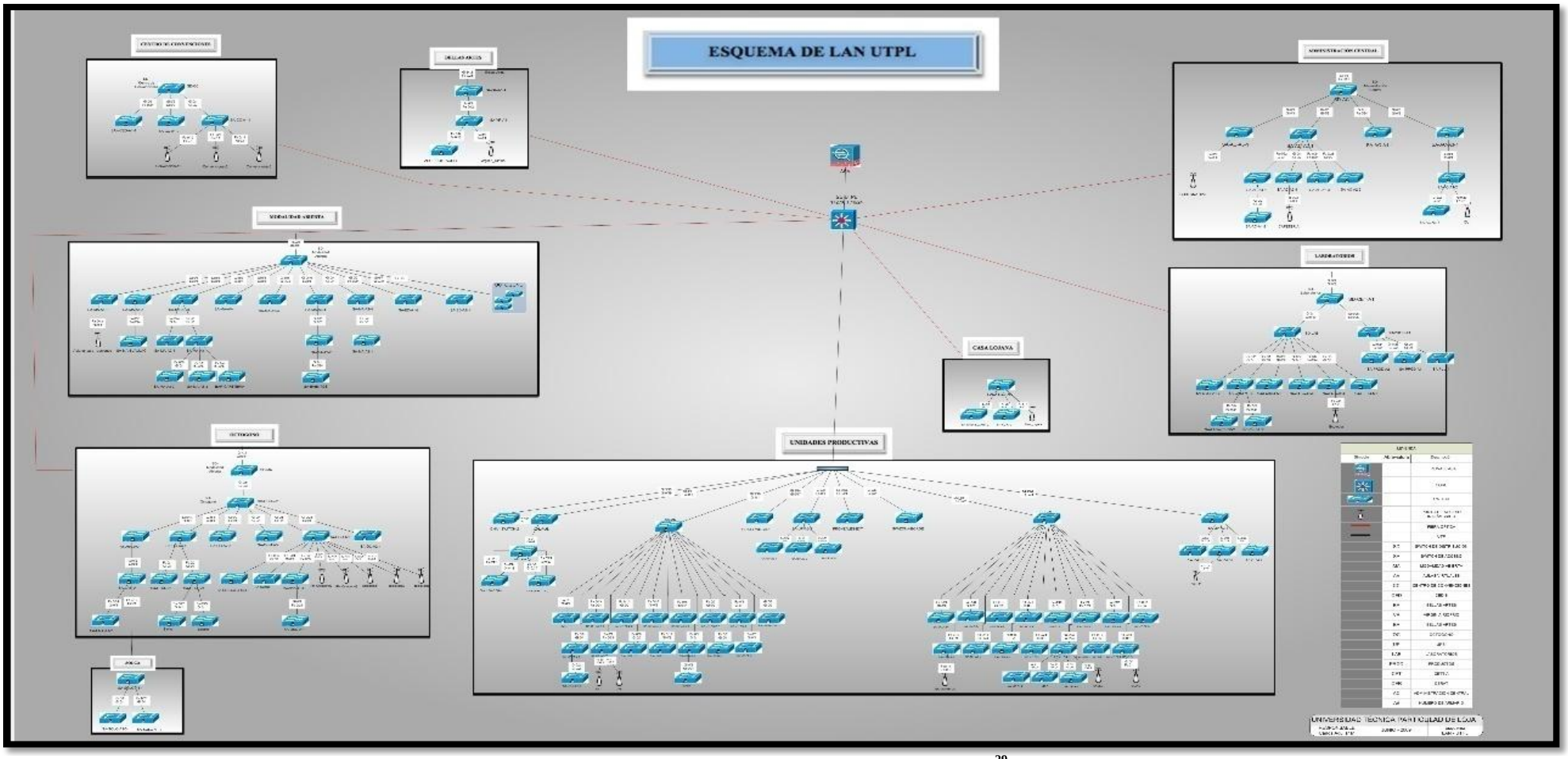

Figura 2. 2 **Diseño de la red LAN de la UTPL [2]** [29]

[29] Figura tomada el 27 de Noviembre del 2010.

Existen varias topologías para la red LAN, la UTPL se caracteriza por utilizar la topología en **estrella** donde cada Switch de distribución está conectado por fibra al nodo central y los switchs de acceso por medio de cable UTP a los de Distribución, demostrado en la figura 2.2.

Esta misma topología en estrella es utilizada en el diseño físico como en el diseño lógico.

2.2.3 Modelo jerárquico.

Modelo jerárquico utilizado es el de 3 capas de CISCO.

- **Core**. Switch Cisco Catalyst 6500
- **Distribució**n. Switch de modelo Cisco Catalyst 3550/3560.
- **Acceso.** Switch 2950/2960.

2.2.4 VLANs.

Por seguridad de la Red LAN está segmentada por VLANs, lo cual se ha realizado de dos maneras:

- Por edificio.
- Por rol de desempeño.

Además se ha definido ACL's a nivel del Switch de Core, que por política se ha establecido bloquear todo tipo de acceso por defecto y habilitar accesos según requerimientos de usuario.

2.2.5 RADIUS[30]

Es un servidor de autenticación remota de los switchs y puntos de acceso tiene las características AAA[31] (Autenticación, Autorización y Registro), almacena información necesaria para la autenticación de los switchs, en los logs se almacenan los accesos al Radius.

Para más detalle de las características de cada uno de los dispositivos que compone la red LAN ver anexo I.

[30] Remote Authentication Dial-In User Server. http://es.wikipedia.org/wiki/RADIUS.
[31] Autenticación, Autorización y Contabilización. http://es.wikipedia.org/wiki/Protocolo_AAA.

2.3 Red Inalámbrica.

La red inalámbrica es muy utilizada ya que proporciona movilidad a los usuarios.

Se ha colocado varios puntos de acceso en diferentes localizaciones de la universidad, cada uno de ellos están configurados según su ubicación.

El método de seguridad implementado en varios access point es WPA[32] y los otros están abiertos. El tipo de cifrado es TKIP.[33]

2.4 Voz/IP

Dada la necesidad de implementar y de utilizar la red para la comunicación de voz se implementó este servicio utilizando Asterisk[34], el mismo que tiene un firewall configurado con ACL's para la administración.

2.5 Políticas y procedimientos de gestión de la seguridad.

2.5.1 Acceso.

- **Acceso de administración.**

  Se cuenta con un servidor Radius el cual permite la autenticación de usuarios de los switchs y puntos de acceso, sin embargo el switch de Core lo realiza localmente.

- **Acceso a la red LAN.**

  Controlar a través de port security en la capa de acceso, tomando en cuenta las direcciones MAC[35] conocidas, diferentes MAC las bloquea. Aunque no todos los switch

[32] (Acceso Protegido WIFI) sistema para proteger las redes inalámbricas. http://wikipedia.or
[33] (Temporal Key Integrity) es un protocolo que mejora el cifrado de datos en redes inalámbricas.
[34] Programa que proporciona funcionalidades de una central telefónica http://es.wikipedia.org/wiki/Asterisk
[35] Control de acceso al medio.

cuentan con esta característica de seguridad por que se ha desactivado o no se ha configurado.

- **Acceso remoto a la administración del router de la red WAN.**

  El acceso remoto a la administración del router de borde es mediante el protocolo SSH.

- **Acceso por VPN a los servicios.**

  Para contar con el servicio de la VPN los usuarios deben enviar la justificación del acceso a la misma a la cuenta de correo electrónico cuentaseguridad@utpl.edu.ec, de esta manera se autoriza o se niega el acceso, el caso de autorizar se entrega un usuario y contraseña teniendo únicamente permiso a los servicios solicitados y a los cuales está autorizado.

- **Acceso remoto a la administración de la Tecnología de VOZ/IP**

  El acceso al servidor Asterisk para la administración es por medio de SSH.

2.5.2 Seguridad de la red LAN.

La política de acceso remota a la administración de los servidores es mediante el protocolo seguro SSH remote desktop por lo cual en el firewall ASA se ha configurado ACL's solo de los equipos o servidores de la DMZ.

2.5.3 Seguridad en el Switch de Core.

En el Core existen niveles de seguridad establecidos desde nivel 0 hasta el 15, pero las utilizadas son:

- **Nivel 14.** Usuario de soporte técnico tiene privilegios de manipulación de ACL's.
- **Nivel 15.** Usuario administrador cuenta con todos los privilegios.

2.5.4 Niveles de autenticación de la WAN.

Se ha determinado dos niveles de autenticación como:

- **Nivel 15**. Administrador posee todos los privilegios.
- **Nivel 10**. Usuarios como proveedores, gestión productiva con privilegios de ver las configuraciones, pruebas de ping y trace router.

2.5.5 Niveles de protección en el Firewall.

Se ha establecido dos niveles de protección.

- **Nivel l00.** Para la parte interna.
- **Nivel 0.** Para la parte externa.

Internamente se maneja una plantilla para la solicitud de permisos, la cual es enviada a la cuenta cuentaseguridad@utpl.edu.ec.

2.5.6 Plan de contingencia.

- ✓ En la red WAN, informalmente se tiene un plan de contingencia, pero no se lo ha documentado, sin embargo tiene enlaces de backup.

- ✓ En la red LAN no se ha definido formalmente un plan de contingencia, pero cuentan con Switchs de acceso y distribución de backup en el caso que fallará un dispositivo de esta naturaleza.

- ✓ No existe un plan de contingencia en el área de seguridades referente a los equipos de gestión de seguridad y además de la sala de servidores ubicada en la UPSI no se tiene una sala de servidores de backup.

- ✓ Con respecto a la red inalámbrica no hay un plan de contingencia documentado, pero en el caso de que un dispositivo activo llegue a tener problemas se cuenta con otros dispositivos alternos.

- ✓ En el momento que fallará el servidor de Asterisk se activa el servidor de backup, pero el servicio de Voz/IP tampoco cuenta con un plan de contingencia documentado.

2.5.7 Respaldos.

- ✓ En la red WAN se realizan copias de seguridad cada 15 días normalmente, o en el caso de que hayan existido cambios importantes como: añadir una nueva ruta, etc.

- ✓ Mientras tanto del switch de Core se realiza copias de seguridad semanalmente del archivo de configuración.

- ✓ En los dispositivos de la red Inalámbrica no hay respaldos ya que no se lo requiere por la facilidad de recuperación de la información de los Puntos de Acceso.

- ✓ Sobre Asterisk[36] se realiza un respaldo de archivo configuración del servidor cada 3 meses.

2.5.8 Documentación.

- ✓ Documentación de los archivos de configuración, como también de los esquemas de la red WAN.

- ✓ En la red LAN se cuenta con la documentación de las configuraciones de los switchs.

- ✓ El OSSIM y el firewall cuentan con un manual de administración mientras tanto los IPS tienen documentación de la configuración de Cisco, así mismo manuales de configuración y de acceso a la VPN.

- ✓ La red inalámbrica y de Voz/IP existe documentación para la administración de los mismos.

[36] Es un programa que proporciona funcionalidades de una central telefónica (PBX). http://es.wikipedia.org/wiki/Asterisk.

2.5.9 Autenticación.

- ✓ Cada uno de estos equipos de gestión de seguridad se autentica localmente en cada servidor. En el proceso de autenticación del firewall ASA y el servidor OSSIM los datos viajan encriptados, al contrario del servidor IME estos viajan en texto plano.

- ✓ En cuanto al servicio de Voz/IP la autenticación se hace localmente, la cual se guarda en un archivo de texto.

2.5.10 Actualizaciones.

- ✓ En algunos de los switchs de acceso se actualizó el IOS para que soporten SSH.

- ✓ En todos los dispositivos de la red WAN hasta el día de hoy no se ha realizado ninguna actualización del IOS por lo que no se lo ha requerido.

- ✓ En el OSSIM se analizan las nuevas aplicaciones o parches existentes, si cumplen con los requisitos de compatibilidad, se aplican las actualizaciones para mejorar la calidad del servicio.

- ✓ Los IPS actualizan las firmas diariamente.

- ✓ Con respecto a la red inalámbrica no se tiene una política de actualización pero cuando se implementan nuevos dispositivos ya cuentan con nuevas actualizaciones.

- ✓ De Voz/IP se ha aplicado un parche de seguridad para el firewall y la versión del Asterisk actual que es la 2.2.12.

- ✓ La información mencionada en las secciones anteriores fue recolectada por medio de entrevistas a los administradores encargadas en la fechas que se realizo la investigación.

- ✓ Además se cuenta con un Manual de Gestión de Seguridad de la Información, la cual se establecen todas las políticas de administración.

"Si algo puede salir mal, saldrá mal."

Ley de Murphy

CAPÍTULO 3

ANÁLISIS DE RIESGOS DE LOS SERVICIOS DE LA RED LAN DE LA UTPL DESDE LA PERSPECTIVA DEL USUARIO FINAL.

3.1 Metodología.

Es primordial considerar la utilización de una metodología para la elaboración de esta tesis por lo tanto las que más se acoplan a las necesidades son dos: OCTAVE [4] y OSSTMM [15] detalladas en el capítulo 1.

3.1.1 Selección de Metodología.

Una vez analizadas las funcionalidades de cada una de las metodologías se ha considerado importante unificar algunos pasos de OSSTMM Y OCTAVE [16] [23]. En un solo grupo de procesos que cumplan con los requerimientos de la tesis.

Por lo tanto de OCTAVE se tomó de la fase I los proceso 3 y 4 de la fase II los procesos 5 y 6; y por último de la fase III los dos procesos 7 y 8; como también de la OSSTMM se escogió 4 secciones, seguridad en las comunicaciones, seguridad inalámbrica, seguridad física y finalmente seguridad en las tecnologías de internet. Como resultado final se obtuvo un solo conjunto de procesos seleccionados como se lista a continuación.

- **Fase I. Construir perfiles de amenazas basados en activos**.

  - Proceso 1. Identificación de la información al usuario final.
  - Proceso 2. Consolidación de la información y creación de perfiles de amenaza.

- **Fase II. Identificar los puntos vulnerables en la infraestructura.**

  - Proceso 3. Identificación de componentes claves.
  - Proceso 4. Evaluación de componentes seleccionados.

    ✓ ***Proceso 4.1 Seguridad en las comunicaciones.***

    - *Subproceso 4.1.2 Testeo de Voz / IP*.

      - Identificar los niveles de control de interceptaciones en las comunicaciones.

    ✓ ***Proceso 4.2 Seguridad inalámbrica.***

    - *Subproceso 4.2.1 Verificación de redes inalámbricas [802.11]*.

      - Evaluar la habilidad de determinar el nivel de control de acceso físico a los puntos de acceso.
      - Evaluar la capacidad de interceptar o interferir las comunicaciones.
      - Determinar si los puntos de acceso son apagados durante los momentos del día en los que no son utilizados.

- ✓ ***Proceso 4.3 Seguridad física.***

  - *Subproceso 4.3.1 Evaluación de controles de acceso.*

    - Enumerar dispositivos o elementos críticos utilizados por el usuario final.
    - Examinar dispositivos y tipos de control de acceso.
    - Determinar el nivel de privacidad en un dispositivo de control de acceso.
    - Determinar las áreas físicas seguras del campus universitario.
    - Examinar los dispositivos de control de acceso en búsqueda de puntos débiles y vulnerabilidades.

- ✓ ***Proceso 4.4 Seguridad en las tecnologías de internet.***

  - *Subproceso 4.4.1 Sondeo de red.*

    - Definición del sistema a sondear.
    - Identificar puertos abiertos.
    - Identificar direcciones IP de las máquinas objetivos.
    - Identificar servicios activos.
    - Tipo de sistema operativo.

  - *Subproceso 4.4.2 Revisión de privacidad.*

    - Cuáles son los sistemas involucrados para la recolección de datos.
    - Listados de cuáles son las técnicas de recolección de datos.
    - Listado de los datos recolectados.
    - Identificar información de empleados, organizaciones o materiales que contienen información privada.

  - *Subproceso 4.4.3 Obtención de documentos.*

    - Recopilar direcciones de e-mail corporativas y personales de las personas claves.

  - *Subproceso 4.4.4 Búsqueda y verificación de vulnerabilidades.*

    - Integrar en las pruebas realizadas los escáneres, herramientas de hacking y exploits utilizados actualmente.

- Medir la organización objetivo utilizando herramientas de escaneo habituales actualmente.
- Identificar todas las vulnerabilidades relativas a las aplicaciones.
- Identificar todas las vulnerabilidades relativas a los sistemas operativos.

▪ *Subproceso 4.4.5 Recursos compartidos.*

- Escaneo de host con recursos compartidos con seguridad activa e inactiva.
- Comprobar contraseñas con fuerza bruta.
- Ingresar a la máquina víctima.

▪ *Subproceso 4.4.6 Re-Ingeniería.*

- Buscar las posibles combinaciones de contraseñas por fuerza bruta en las aplicaciones.
- Reunir información sensible a partir de ataques hombre-en-el-medio.

▪ *Subproceso 4.4.7 Descifrado de contraseña.*

- Obtener usuario y contraseña.
- Usar contraseñas obtenidas o sus variaciones para acceder a sistemas o aplicaciones adicionales.

▪ *Subproceso 4.4.8 Testeo de denegación de servicios.*

- Análisis de la seguridad de las estaciones de trabajo.

- **Fase III. Desarrollo de planes y estrategias de seguridad.**

  - Proceso 5. Análisis de riesgos.
  - Proceso 6. Desarrollar estrategias de protección.

La figura 3.1 presenta cada uno de las fases, así como también, los procesos dichos anteriormente.

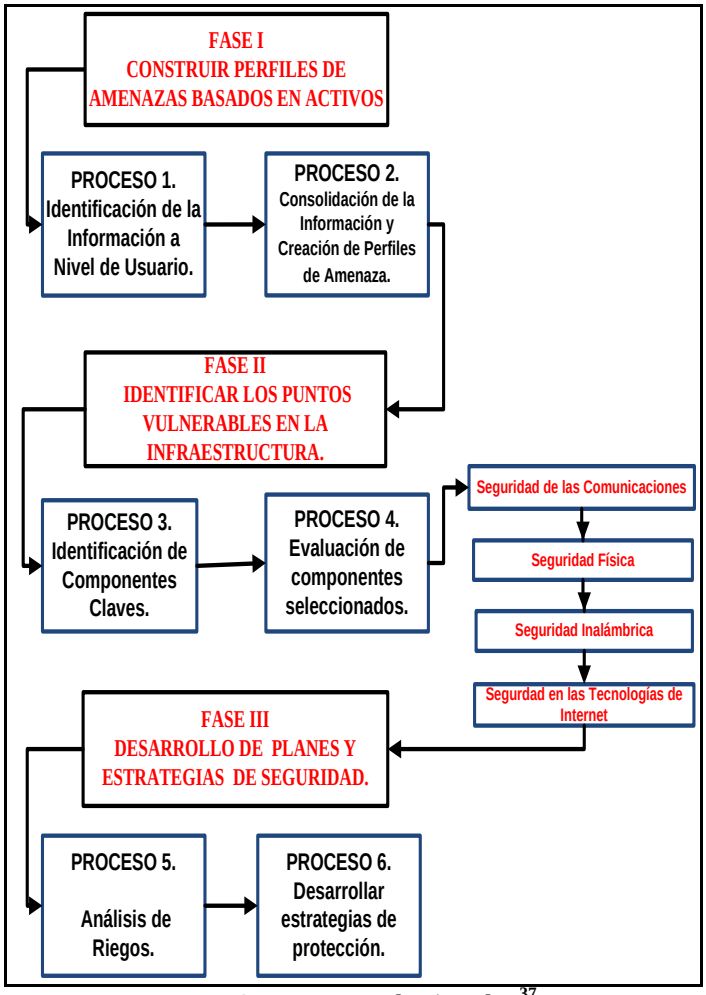

Figura 3. 1 **Procesos seleccionados.**[37]

Y así como también, lo que se debe seguir para un test de penetración. Empezando por la identificación de componentes claves, a continuación con la búsqueda de vulnerabilidades de las secciones de OSSTMM tales como: comunicaciones, física, inalámbrica y tecnologías de Internet.

La siguiente figura muestra un enfoque metodológico acerca de la búsqueda de vulnerabilidades incorporando las secciones de seguridad que se han considerado anteriormente, seguido de la explotación, la respectiva corrección; si la vulnerabilidad no fuese corregida se convertiría en un riesgo potencial y se tendría que buscar mecanismos de protección, caso contrario el desarrollo de la documentación, y es así que esto se volvería un ciclo repetitivo al nuevamente buscar otras vulnerabilidades.

[37] Tomado de OSSTMM y OCTAVE

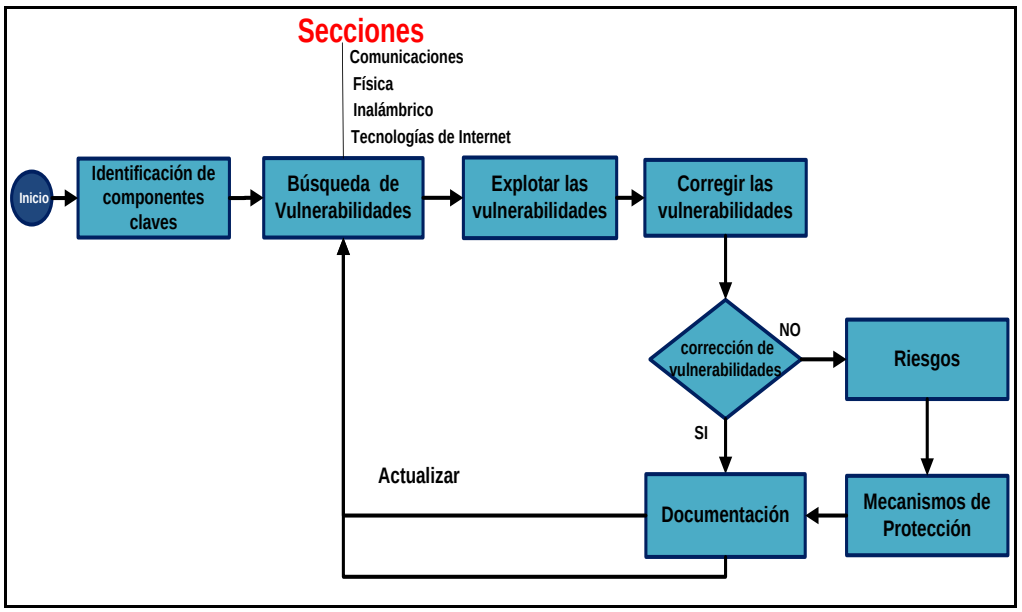

Figura 3. 2 **Enfoque metodológico.**

3.1.2 Aplicación de los procesos.

Luego de haber definido los procesos a utilizar, se desarrollarán de dos maneras: la primera para el proceso de mapeo, descubrimiento y escaneo de: puertos, servicios, sistemas operativos y versiones se lo realizará en los equipos reales del campus de la Universidad, mientras tanto, la explotación de las vulnerabilidades se lo hará en un entorno controlado de laboratorio donde se cuenta con todos los servicios, configuraciones generales en los equipos de la Universidad y configuraciones especificas adicionales en los dispositivos activos de la red para realizar el test de intrusión, todo esto permitirá ahorrar tiempo y esfuerzo en la realización del test, ya que si no se contará con estas configuraciones la intrusión llevaría más tiempo, pero es posible; asimismo se realizó las pruebas tanto en la red cableada como en la red inalámbrica.

El anexo III enseña una plantilla de los procesos seleccionados, en donde la primera columna identifica las fases y la segunda columna los procesos elegidos.

3.2 FASE I. Construir perfiles de amenazas basados en activos.

3.2.1 Proceso 1. Identificación de la información al usuario final [23].

La UTPL tiene diferentes tipos de usuarios tales como:

- Estudiantes.
- Empleados.

- Usuario especial: (autoridades, usuario financiero).
- Profesores.
- Personas externas.

3.2.2 Proceso 2. Consolidación de la información y creación de perfiles de amenaza.

3.2.2.1 Riesgos de los servicios de la red LAN UTPL.

Para realizar este análisis de riesgos que enfrentan los usuarios, se ha clasificado los servicios en dos tipos

- Servicios internos.
- Servicios externos.

La figura 3.3 demuestra los servicios internos y externos, incluyendo el acceso al medio, ya que este también corre riesgos.

Arquitectura de Riesgos	Servicios	
	INTERNOS	EXTERNOS
RIESGOS	Correo electrónico	Redes sociales
	Entorno virtual de aprendizaje[38]	Mensajería instantánea
	Voz/IP[39]	Programas p2p[40]
	Recursos compartidos	Comercio electrónico
	Sistema de Gestión Académica[41]	Búsqueda de información
	Sistema Financiero BAAN[42]	
	Blogs	
	Acceso al Medio Físico (Wireless, LAN)	

Figura 3. 3 **Arquitectura de los riesgos de la red UTPL.**

[38] Sistema de intercambio de información entre el estudiante y el tutor.
[39] Comunicación de la voz a través del protocolo de IP.
[40] Es una red de computadores en la que todos funcionan sin clientes ni servidores http://wwikipedia.org
[41] El sistema de Gestión Académica es utilizado para los procesos académicos de la universidad.
[42] Es un sistema financiero, contable y de facturación de la UTPL.

Los servicios internos son aquellos los que la universidad brinda a la comunidad utepelina en cambio los servicios externos son utilizados por el usuario, pero no son propios de la entidad.

Todos estos son los que hacen uso de los servicios de internet que ofrece la red de la entidad para realizar sus actividades diarias; por eso se ha considerado importante conocer cuales son los riesgos a los que están expuestos, tales como: fraude, robo de información, suplantación de identidades, entre otros comprobando en un ambiente de prueba. En el capítulo 1 sección 1.4 perteneciente a Ataques Informáticos se mencionó los riesgos más comunes de la informática.

En el anexo II están los riesgos de manera detallada en base a los servicios internos o externos.

3.3 FASE II. Identificar los puntos vulnerables en la infraestructura.

3.3.1 Proceso 3. Identificación de componentes claves.

Una vez conocidos los servicios y los riesgos, es imprencindible evaluar los riesgos más importantes, determinando con la ayuda de una tabla el nivel de criticidad de cada uno. En la tabla 3.1, se ha considerado categorizar cualitativamente los nivel de criticidad según el porcentaje de impacto del riesgo como: Alto, Medio y Bajo.

Tabla 3. 1. **Clasificación del nivel de criticidad de los riesgos [16].**

NIVEL DE CRITICIDAD	PORCENTAJE DEL IMPACTO DEL RIESGO
ALTO	81% - 100%
MEDIO	61% - 80%
BAJO	50% - 60%

La forma de determinar el nivel de criticidad de cada uno de los riesgos fue con la ayuda de la tabla anterior considerando el impacto del riesgo en base a la experiencia del personal que administra estos servicios y el porcentaje de probabilidad que ocurra. Cabe recalcar que estos

resultados están enfocados a la continuidad del negocio más no en los servicios. Además estos dependen de la organización y del enfoque que se dé.

La tabla 3.2 presenta la evaluación de los riesgos más comunes y el nivel de criticidad que comparten los servicios.

Tabla 3. 2 **Evaluación de los riesgos.**

RIESGO	NIVEL DE CRITICIDAD
Intercepción de las comunicaciones.	MEDIO
Suplantación de identidad.	ALTO
Robo de información/ robo de usuario y contraseña.	MEDIO
Introducción de código malicioso.	MEDIO
Interrupción de las actividades de los servicios.	ALTO
Alteración de la información.	ALTO

3.3.2 Riesgos seleccionados [10].

Una vez analizados los riesgos y conocer el nivel de criticidad se han seleccionado los siguientes riesgos con el nivel de criticidad ALTO.

- Suplantación de identidad.
- Interrupción de las actividades de los servicios.
- Alteración de la información

En el capítulo 2, se explicó cuál es la situación actual en entorno a la seguridad de la red de la universidad, donde se menciona la utilización de VLANS, como mecanismos de seguridad, es así que se ha determinado realizar el test de penetración en una VLAN que está definida dentro del entorno de pruebas.

3.3.3 Técnicas, Métodos y Herramientas.

3.3.3.1 Herramientas [1]

La siguiente tabla detalla varias herramientas que se utilizó para el test de penetración [12] [25].

Tabla 3. 3 **Herramientas para el test de penetración.**

Herramienta	Descripción	Sitio Oficial
Advanced LAN Scanner	Escanea puertos y recursos compartidos.	http://www.radmin.com/products/utilities/lanscanner.php
Arp –a	Comando para ver las tablas de las direcciones físicas y lógicas.	http://www.halcom5.com/web/kb/comandos/comando_arp.html
Autoscan Network	Herramienta para escanear de los hosts de un segmento de red.	http://autoscan-network.com/
Bactrack	Distribución GNU/LINUX para el test de penetración.	http://www.backtrack-linux.org/
Caín & Abel	Herramienta de recuperación de contraseñas.	http://www.oxid.it/cain.html
Ettercap	Herramienta que funciona como sniffer para auditorias de redes LAN.	http://ettercap.sourceforge.net/
LanSpy	Analizador que permite obtener información de todos los ordenadores conectados en la red LAN.	http://lantricks.com/lanspy/index.php
Medusa	Permite el ataque de fuerza bruta a diferentes servicios.	http://www.rinconinformatico.net/ataque-de-fuerza-bruta-con-diccionario-usando-medusa
Nbtscan	Recopila información escaneando redes en busca de información acerca del NetBIOS.	http://inetcat.net/software/nbtscan.html
Nessus	Herramienta para el análisis de vulnerabilidades.	http://www.nessus.org/nessus/

Nmap	Herramienta para el escaneo de puertos.	http://www.nmap.org/
Netstat	Muestra las conexiones entrantes o salientes de una computadora.	http://www.alcancelibre.org/staticpages/index.php/como-netstat
Ping	Herramienta para comprobar la conexión entre dos equipos.	http://es.wikipedia.org/wiki/Ping
Smb4k	Programa libre que permite examinar y montar recursos compartidos de la red.	http://www.linux-os.com.ar/linuxos/montar-recursos-samba-en-gnulinux/
Wireshark	Herramienta para el escaneo de paquetes.	http://www.wireshark.org/
Xhydra	Herramienta para revisar los recursos compartidos.	http://labs.dragonjar.org/laboratorios-hacking-tecnicas-y-contramedidas-scanning-iii

3.3.4 Proceso 4. Evaluación de componentes seleccionados [14].

3.3.4.1 Proceso 4.1. Seguridad en las comunicaciones.

3.3.4.1.1 Subproceso 4.1.2 Testeo de Voz / IP.

La tecnología de Voz/IP se encuentra instalada y disponible en el campus universitario y algunos de los usuarios la utilizan, es así que el uso del servicio ha ido incrementado y se ha visto la necesidad implementar esta tecnología en el laboratorio para realizar la verificación de las amenazas que se encuentra expuesta.

- ***Identificar los niveles de control de interceptaciones en las comunicaciones.***

  En el laboratorio se realizó la interceptación de las comunicaciones, utilizando ataques de Arp-spoofing, el ataque fue exitoso porque la configuración del switch permitió colocar dos direcciones físicas para una dirección IP y se comprobó la existencia de la vulnerabilidad, por lo tanto la aplicación de Voz/IP debería encapsular la comunicación sobre un protocolo seguro.

3.3.4.2 Proceso 4.2. Seguridad inalámbrica.

3.3.4.2.1 Subproceso 4.2.1 Verificación de redes inalámbricas [802.11].

Para la verificación de la red inalámbrica se utilizó un Punto de Acceso Abierto de prueba, para analizar las vulnerabilidades que se encuentran expuestos los puntos de acceso que están sin autenticación ubicados en algunos lugares del campus universitario.

- ***Evaluar la habilidad de determinar el nivel de control de acceso físico a los puntos de acceso.***

  La mayoría de los Puntos de Acceso están colocados en partes visibles al usuario final, estos no cuentan con una seguridad física que los proteja de robo, daño físico u otras circunstancias ocasionando problemas como: pérdidas económicas, denegación de servicio. etc.

- ***Evaluar la capacidad de interceptar o interferir las comunicaciones.***

  Se puede interceptar las comunicaciones a los usuarios conectados a los puntos de acceso abierto y sin ningún tipo de seguridad, mientras tanto en los puntos de acceso que cuenta con seguridad como WPA es complicado debido que primero se debería romper el sistema de protección del Access Point[43] para tener conexión y luego realizar la interceptación.

- ***Determinar si los puntos de acceso son apagados durante los momentos del día en los que no son utilizados.***

  En este punto se pudo determinar que los Access Point no son apagados durante los momentos que no son utilizados, es así que se ha permanecido conectado al mismo punto de acceso durante todo el día.

[43] Punto de Acceso.

3.3.4.3 Proceso 4.3. Seguridad física.

Otra de las secciones de OSSTMM es la seguridad física, por ende se ha considerado fundamental analizarla, teniendo como apoyo una entrevista realizada al Departamento de Infraestructura de la Universidad sobre los temas incluidos en esta sección, para verificar la entrevista hecha se encuentra en el Anexo V. Los resultados se evalúan en los siguientes puntos:

3.3.4.3.1 Subproceso 4.3.1 Evaluación de controles de acceso.

- ***Enumerar dispositivos o elementos críticos utilizados por el usuario final***

  - Impresoras.
  - Computadoras.
  - Data Centers.
  - Laboratorios.
  - Aulas.
  - Copiadoras.

- ***Examinar dispositivos y tipos de control de acceso.***

  En esta área existen diferentes dispositivos de control de acceso como:

  - Sistema de personal (Guardias).
  - Sistema de circuito cerrado que incluye alarmas y cámaras.

- ***Determinar el nivel de privacidad en un dispositivo de control de acceso.***

  El nivel de privacidad de los controles de acceso es supervisado por los responsables del Departamento de Infraestructura.

- ***Determinar las áreas físicas seguras del campus universitario.***

  Todas las áreas internas del campus universitario se consideran seguras, sin embargo se ha categorizado de dos formas áreas críticas y no tan criticas, las áreas críticas como son:

  - Edificio de la UPSI.
  - Edificio del OCTOGONO.
  - Edificio ADMINISTRACIÓN CENTRAL.

  Y las áreas no tan críticas se puede mencionar algunas como:

  - Aulas.
  - Coliseo.
  - El centro de convenciones.

  Pero cabe mencionar que si estos lugares requieren de seguridad por motivos como: congresos, exposiciones, juegos internos, entre otros se proporciona la seguridad necesaria.

- ***Examinar los dispositivos de control de acceso en búsqueda de puntos débiles y vulnerabilidades.***

  En el caso de robo o pérdida de los dispositivos críticos dentro del campus universitario, el afectado deberá recurrir al departamento de Infraestructura para mencionar lo sucedido, luego de esto el departamento de Infraestructura comunica al Departamento de Seguridad y también a la Policía PJ para las respectivas investigaciones.

  Si el elemento crítico pertenece a los activos fijos de la universidad estos cuentan con un seguro para la remediación del dispositivo, en el caso contrario no se responsabilizan de los daños.

3.3.4.4 Proceso 4.4. Seguridad en las tecnologías de internet.

3.3.4.4.1 Subproceso 4.4.1 Sondeo de red.

- ***Definición del sistema a sondear.***

  En este proceso las herramientas optadas para el sondeo de red fueron: Nmap [22], GFI LANguard Network Scanner y Autoscan Network que se encuentran detalladas en la tabla 3.3 perteneciente a las herramientas para el test de penetración

- ***Identificar puertos abiertos.***

  La tabla 3.4 presenta los puertos más conocidos, los servicios que corren en este y los protocolos correspondientes.

Tabla 3. 4 **Servicios, protocolos y puertos más conocidos [21][44]**

Servicio	Puerto	Protocolo
FTP	21	TCP
SSH	22	TCP
TELNET	23	TCP
SMTP	25	TCP
HTTP	80	TCP
HTTPS	443	TCP
POP3	110	TCP
MSRPC	135	TCP
NETBIOS-SSN	139	TCP
MICROSOFT -DS	445	TCP
TERMINAL SERVER	3389	TCP
VNC	5900	TCP
MY-SQL	3306	TCP
SSDP-UPnP	2869	TCP
KERBEROS	88	TCP

[44] Tomado de la tesis Análisis inicial de la anatomía de un ataque informático a un sistema informático

- ***Identificar servicios activos.***

La figura 3.4 muestra el porcentaje final de todos los escaneos que se ejecutó en los hosts, en donde se identificó los siguientes servicios activos como: el servicio con mayor porcentaje es el NETBIOS, seguido de MICROSOFT-DS, el servicio de MSRPC en tercer lugar, en la siguiente posición es para el servicio de TERMINAL SERVER, a continuación HTTPS, luego HTTP, con un porcentaje del 2% SSH y finalmente con 1% los servicios restantes.

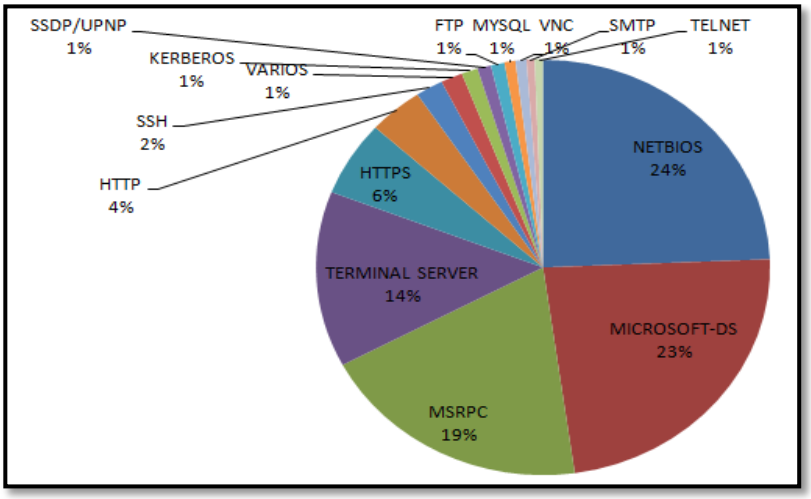

Figura 3.4 **Servicios activos en las maquinas escaneadas.**

- **IPv6/IPv4.**

El escaneo se lo ejecutó tanto para la dirección de IP4 e IPv6 en la red cableada y en la red inalámbrica, por lo que se puede determinar que existen mecanismos de seguridad eficientes y robustos para IPv4 y carentes mecanismos para IPv6.

- ***Tipo de sistema operativo.***

La figura 3.5 muestra que el 90% de los sistemas operativos tiene instalado Windows, mientras que un 7% Linux y el restante 3% Mac OS, luego de haber realizado el escaneó de los hosts activos.

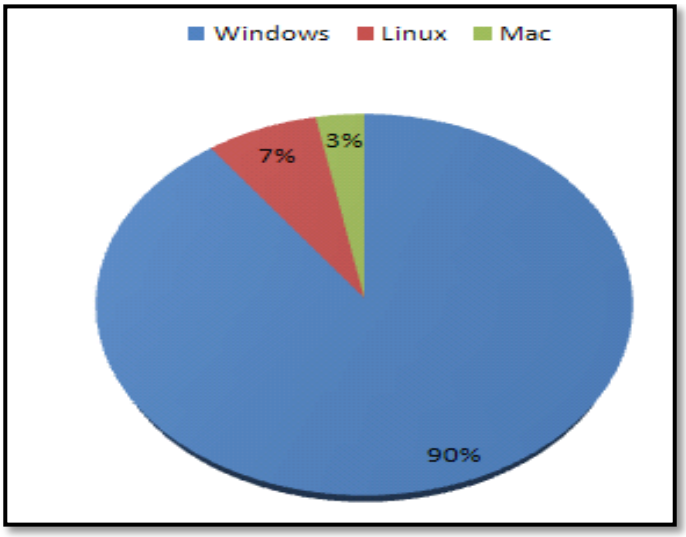

Figura 3.5. **Porcentaje de los sistemas operativos.**

- ***Medir la organización objetivo utilizando herramientas de escaneo habituales actualmente.***

  Las herramientas para el escaneo de la red son:

  - Nmap.
  - Autoscan-Network.
  - Ping.

  Las mismas que se encuentran detalladas en la tabla 3.3 perteneciente a las herramientas para el test de penetración

- ***Identificar todas las vulnerabilidades relativas a los sistemas operativos* [2] [26].**

  Los sistemas operativos utilizados son: Microsoft, Linux y Mac, cada uno de estos presenta vulnerabilidades.

  Windows encabeza la lista del sistema operativo más vulnerable, a continuación Mac OS y GNU/Linux según el reporte de ESET**.** [9]

  Y también en otro estudio realizado se ha reportado lo siguiente:

- Windows XP 55 %
- Windows NT 1.7 %
- Windows Me 6.3 %
- Windows 98 20.8 %
- Windows 95 1 %
- Windows 2003 0.1 %
- Windows 2000 11.5 %
- Linux 0.1%
- Mac OS 1.8 %
- Otros 1.7 % [5].

La mayor parte de las vulnerabilidades son por problemas de seguridad denominados "O Day" [45]

- ***Windows.***

Windows es el sistema operativo universal, es decir el más utilizado por la mayoría de personas, de esta manera se ha convertido en el preferido para ataques. Microsoft proporciona la solución de los mismos con la aplicación de parches, sin embargo mayoría de los usuarios no actualizan su sistema operativo o no instalan los parches sugeridos, ocasionando ser víctimas de ataques. [19].

- Susceptible a ataques de hacking.
- Vulnerable a ataques de virus.
- Agujeros de seguridad en versiones de los sistemas operativos.
- Tiene en su mayoría programas vulnerables que corren en este sistema operativo.
- Se desarrolla mucho software malicioso.

[45] Son problemas de seguridad que no son conocidas o publicadas.

- ***Linux/Unix.***

  - Vulnerabilidad de seguridad en la librería libpng de Solaris.
  - Vulnerabilidad de seguridad en Solaris XScreenSaver.
  - Vulnerable a ataques de hacking.

- ***MAC OS.***

  - Aplicaciones instaladas en Mac que son vulnerables a través de detección de pruebas de concepto (PoC) a través de Ransomware con el objetivo de realizar fraudes.
  - Creación de troyanos con RealBasic lenguaje de programación.
  - Error de Buffer overflow por diferentes aplicaciones como: Google Chrome, Mozilla, OpenBSD [6].
  - Solucionan sus problemas de seguridad en un tiempo considerable.
  - Se tuvo un problema de JRE (Java Runtime Enviromment) que podría ser blanco por los intrusos para ejecutar código con solo ingresar a una página web [17].

Sin embargo estas vulnerabilidades son algunas de las que presenta cada uno de los sistemas operativos.

3.3.4.4.2 Subproceso 4.4.5 Recursos compartidos.

- ***Escaneo host con recursos compartidos con seguridad activa e inactiva.***

El escaneo para verificar recursos compartidos se puede realizar a través de la herramienta SMB4K mencionada en la tabla 3.3 de herramientas.

- ***Comprobar contraseñas con fuerza bruta.***

Los ataques de fuerza bruta son los más utilizados para descifrar contraseñas de diferentes aplicaciones. Existen un sinnúmero de herramientas que se podrían utilizar, a continuación se listan algunas.

- Medusa.
- Xhydra.
- Caín & Abel.

Para más información ver la tabla 3.3 referente a herramientas.

- ***Reunir información sensible a partir de ataques hombre-en-el-medio.***

A través del ataque de hombre en el medio se podría llegar a obtener información sensible.

3.3.4.4.3 Subproceso 4.4.7 Descifrado de contraseña.

Las aplicaciones que se pueden descifrar las contraseñas son aquellas que no utilizan ningún tipo de encriptación y las contraseñas asignadas por parte del usuario son fáciles de descifrar.

3.3.4.4.4 Subproceso 4.4.8 Testeo de denegación de servicios.

- ***Análisis de la seguridad de las estaciones de trabajo.***

Las estaciones de trabajo pueden tener varios métodos de protección, los cuales se demuestra en la figura 3.6, el firewall es una de las tecnologías de seguridad más habilitadas lo que permite bloquear, filtrar y cerrar puertos es decir se puede deshabilitar los servicios que hacen uso de estos puertos, otra solución es compartir recursos con seguridad habilitada y finalmente bloquear los Pings.

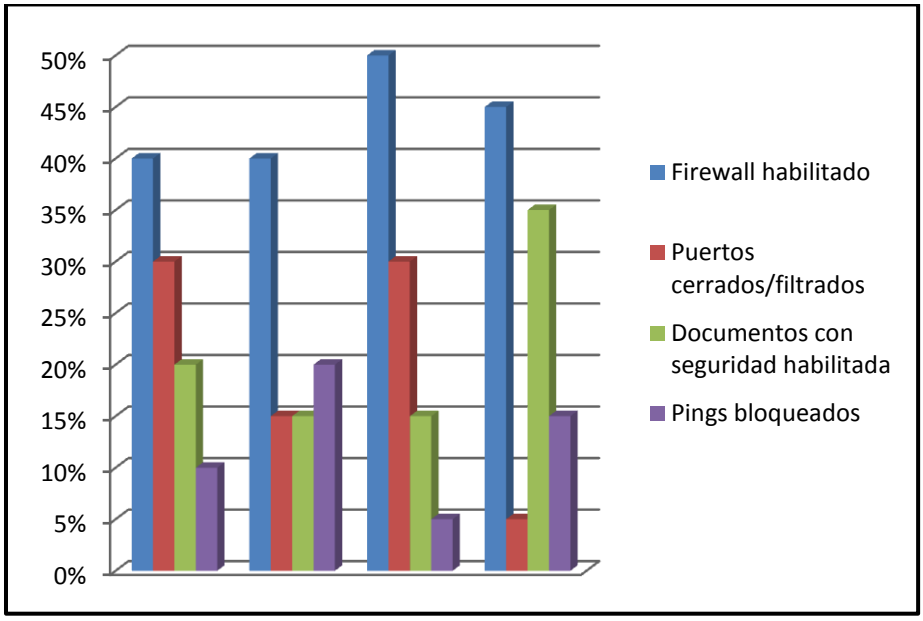

Figura 3. 6. **Seguridad que podría ser habilitada en las estaciones de trabajo.**

3.4 FASE III. Desarrollo de planes y estrategias de seguridad.

3.4.1 Análisis de riesgos.

Es muy difícil considerar la eliminación total de los riesgos, pero implantando contramedidas de seguridad se podrán mitigar y reducir el impacto. De tal forma al encontrarse expuesto a un riesgo, se puede tomar tres alternativas: reducirlo, transferirlo o asumirlo el riesgo. [1]

Las varias pruebas que se realizaron fueron para comprobar el impacto de los riesgos identificados al inicio.

Se determinó que todo los riesgos puede llevarse a cabo de una o de otra manera, al final se puede hacer hincapié de cuáles son los riesgos que tienen mayor probabilidad de ocurrencia. La figura 3.7 demuestra que el riesgo de intercepción de las comunicaciones es el de mayor probabilidad de ocurrencia con un 30%, luego con un 25% el riesgo de robo de datos, con un 20% alteración de la información, mientras tanto el riesgo de Suplantación de Identidad cuenta con un 15%, un 7% concierne al riesgo de Interrupción de las actividades de los servicios y finalmente con 3% la introducción de código malicioso.

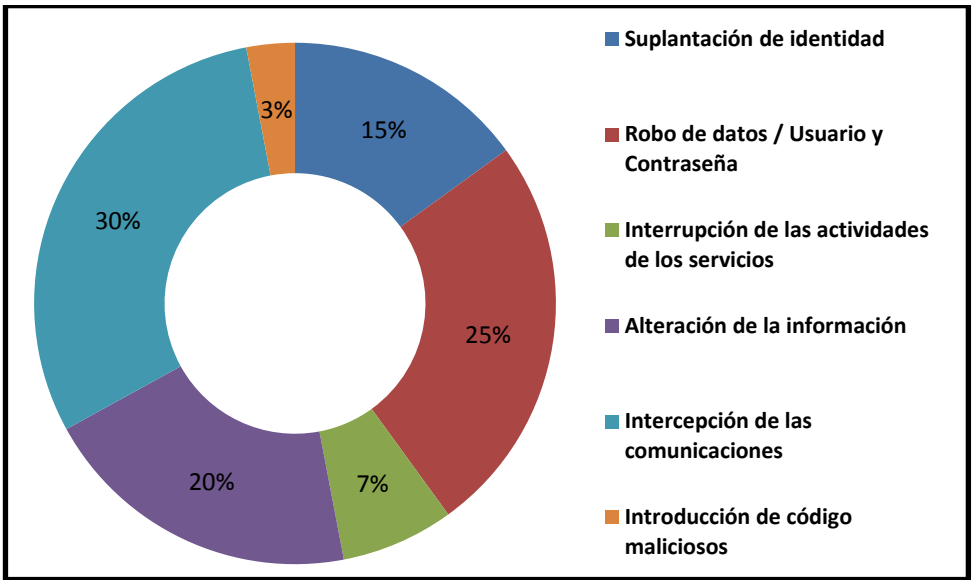

Figura 3. 7 **Probabilidad de ocurrencia de los riesgos.**

Las razones de exposición a estos riesgos y el nivel de criticidad son por varios factores.

- **Protocolo ARP [28].**

  El protocolo ARP no cuenta con autenticación, por lo tanto esta vulnerabilidad permite hacer ataques de hombre en el medio.

- **Intercepción de la las comunicaciones en la Red Inalámbrica.**

  - Como en toda tecnología existen debilidades, es así que ésta también es susceptible a fallos, en la red inalámbrica es muy complicado impedir la intercepción de las comunicaciones, los paquetes son enviados a través de las ondas de radio; en las redes inalámbricas este riesgo es inevitable [1] y ***sobre todo la falta de autenticación de las tramas de administración y control.***

  - Al utilizar los sniffers en las redes inalámbricas no se pueden detectar, ya que los adaptadores configurados se encuentran en modo monitoreo.

  - Ataques de hombre en el medio es otra amenaza pues la red inalámbrica sin autenticación facilita la captura y redirección de sesiones, no se puede detectar la presencia de estaciones adyacentes con la misma dirección MAC o dirección IP.

- **Excesiva confianza o falta de concientización de parte de los usuarios finales.**

  La mayoría de personas no toman en serio los riesgos que se encuentran expuestos al utilizar la red LAN, tampoco toman medidas necesarias de seguridad para evitar ser víctimas de ataques. Y sobre todo no escatiman el impacto al momento que llegara suscitar algunos de estos.

- **No hay presupuesto suficiente destinado a la seguridad informática y falta de de apoyo por parte de las Autoridades.**

  Otro problema es que los directivos no destinan un presupuesto suficiente para la seguridad informática justificando que no es muy necesario y primordial en la actualidad y realmente se llegan a darse cuenta de la necesidad cuando existen daños graves que afectan las características de la seguridad como la confidencialidad, integridad y disponibilidad.

- **Seguridad física.**

  Para el proceso de qué medidas tomar en el caso de pérdida o robo de las computadoras de los estudiantes dentro del campus universitario no se ha difundido formalmente las medidas correctivas.

- **Falta de Políticas enfocadas al usuario final.**

  Es considerable tomar en cuenta este problema de la no existencia de políticas de seguridad enfocada al usuario final.

- **No se lleva un proceso de ethical hacking de forma periódica.**

  Llevar a cabo un proceso de ethical hacking es actuar proactivamente ante ataques, pues el no realizarlo a su debido tiempo, significa no conocer las vulnerabilidades y amenazas que nos asechan.

- **Plan de contingencia inexistente.**

  La falta de un plan de contingencia formal en todas las áreas y las vinculadas con la red LAN es crítica.

- **Recursos compartidos sin seguridad habilitada.**

  En el caso de que se requiera compartir recursos, y que los mismos no cuenten con algún tipo de seguridad, lamentablemente se está corriendo varios riesgos.

- **Vulnerabilidades de los sistemas operativos [3].**

  El manejo de un computador implica instalarle un sistema operativo indiferente de la distribución (Windows, Linux, Mac Os), sin embargo estos presentan ciertas vulnerabilidades cuando no se realizan actualizaciones o no se personalizan las configuraciones por defecto, ya que constantemente se encuentran acechados por amenazas.

3.4.2 Desarrollar estrategias de protección.

Implementar diferentes estrategias de seguridad para la red de la Universidad es importante y necesario, definiendo varias soluciones las cuales incrementen el nivel de confianza, por lo tanto, estas soluciones deberán evitar futuras amenazas que afecten la imagen y reputación de la red LAN de la Universidad. Recalcando que la manipulación no autorizada de la información critica podría llegar a ser invaluable.

Con el objetivo de asegurar la red LAN de la Universidad es necesario implementar estrategias de protecciones como:

- Preventivas.
- Correctivas y
- Detectivas.

La figura 3.8 es la representación gráfica de las estrategias de protección.

Figura 3. 8 **Estrategias de Protección.**

3.4.2.1 Estrategias de protección preventivas.

- **Test de intrusión internos periódicamente.**

  Este tipo de estrategia validaría y se complementaría con todos los esquemas de gestión de seguridad de la información implementada en la Universidad y actuar de forma proactiva ante ataques que los usuarios finales están arriesgados. Debido al cambio de tecnologías y también de la organización en sí.

- **Crear contraseñas robustas y cambiarlas periódicamente [2].**

  Es importante que los programas o personas acepten la creación de contraseñas mínimo de 6 caracteres, que no se han vinculado con el usuario, el número de cédula, o alguno otro para contrarrestar la probabilidad de que se adivine la clave, y también es importante el cambio de las contraseñas por lo mínimo 3 veces al año.

- **Ubicación física del punto de acceso.**

  Ubicar los puntos de accesos expuestos a riesgos en algún lugar seguro, fuera de la vista de los usuarios y además que estén con las respectivas seguridades para la protección contra robos, caídas, etc.

- **Instalar un firewall personal.**

  El tener instalado un firewall en nuestra PC es importante, sobre todo una buena configuración y que se encuentre habilitado.

- **Instalar un antivirus adecuado.**

  Un antivirus eficaz y potente es primordial para evitar estar expuestos a riesgos. Existen actualmente muchos antivirus en el mercado, sin embargo debemos escoger el que se adapte a las necesidades.

- **Defensa en profundidad [18].**

  Que en cada capa de la pila TCP/IP se tenga seguridad robusta, ayudando a protegerse y dificultando la fácil intrusión por parte de procesos o personas mal intencionadas.

- **Implementar soluciones a nivel de host.**

  Una solución es implementar HIPS Protección de intrusos a nivel de hosts, en los equipos de los usuarios.

- **Capacitación a los miembros del equipo de seguridad.**

  Es importantísimo que cada uno de los usuarios que pertenecen al grupo de seguridad contemple un rol y responsabilidades exclusivas sobre la seguridad, todo esto se lleva a través de una capacitación adecuada y oportuna.

- **BCP Plan de Continuidad de Negocio [24].**

  Un plan de continuidad de negocio implica una garantía de superar un desastre con eficiencia y eficacia, tratando de minimizar esfuerzos, tiempo, dinero;

contrarrestando afectar a la continuidad del negocio, de esta manera contar con BCP en la Universidad actualizado e implementado es necesario.

- **Identificación de un plan de seguridad enfocándose al ciclo PDCA. [24]**

  Este plan de seguridad consta de cuatro pasos: Planificar, Hacer, Revisar y Actuar y cada uno de ellos tiene sus principios y acciones a realizarse; es así que esto se vuelve un ciclo repetitivo y un monitoreo continuo.

- **Escaneador de puertos.**

  Esta herramienta permite identificar los puertos abiertos innecesarios, evitando futuros ataques.

- **Respaldo de datos [2].**

  Las copias de seguridad son imprescindibles realizarlas, considerando el tiempo y que respaldar, evitando futuros problemas de pérdida de información o algunos otros riesgos. [18].

3.4.2.2. Estrategias de protección correctivas.

- **Importancia de la implantación de una política de seguridad de la información en la organización.**

  La creciente necesidad de las organizaciones en obtener una certificación tipo ISO 27001, que le permita demostrar que en ellas se aplican correctamente las medidas de seguridad acorde a un norma internacional, y significando por lo tanto un valor añadido.

- **Evitar ataques de envenenamiento de ARP [8] [27].**

  - En el sistema operativo se puede configurar la caché ARP para que sea estática o instalar alguna herramienta para detectar los cambios de la tabla ARP de la computadora, evitando que se actualice la tabla ARP de un rato desde internet de forma sospechosa.

  - En los Switch 3560 de altas prestaciones que traen consigo la forma de configurar la asociación entre Dirección IP-MAC y poder detectar estos ataques [27].

  - Existen herramientas que permiten observar si una tarjeta de red cambio de estado es decir de un estado normal a modo monitoreo.

  - La forma para darse cuenta de que si se está siendo víctima de un ataque de este tipo es observar la caché ARP de las máquinas, revisando si existe dos direcciones IP con la misma dirección MAC.

  - Algunos antivirus traen consigo la manera de detectar ataques, la cual incluye proteger la caché ARP de la computadora.

  - Configuración en los switchs de un Inspector ARP dinámico DAI, se encarga de verificar si el paquete entrante ingresa por un puerto inseguro, comparando en la tabla de asociaciones DHCP, y verifica si la dirección IP está asociada con la dirección MAC correspondiente, en el caso de que la dirección IP no esté asociada descartará el paquete y bloqueará el puerto.

  - Otra solución a estos tipos de ataques es la implementación de IDS/IPS orientada para los usuarios finales, configurando para la detección de ataques de arp-spoofing [27]

  - Para evitar los ataques MIM [46] utilizando ***arp spoofing*** en una red es conveniente configurar en el switch de acceso el port Security y otra solución es ARP WATCH.

[46] Man in the middle (Hombre en el medio). Técnica de ataque que permite interceptar las comunicaciones.

- **Voz/IP. [29].**

  - Encriptación y autenticación del tráfico de la voz en la red.

  - Instalación de un sistema de detección de intrusos o sistema de prevención de intrusos.

- **Realizar un plan de contingencia de los servicios críticos.**

  Este plan de contingencia deberá incluir todos los elementos críticos de la organización tomando en cuenta el impacto en el caso de que llegara a suscitar un problema y conocer cuáles son las alternativas y las estrategias.

- **ISO 27001, 27002 y Sistema de Gestión de la Seguridad de la Información [24].**

  Actualmente la realidad es diferente, implementar estándares de seguridad es ahora una necesidad y se debe hacerlo para proteger los activos críticos de la Organización como los datos que se ha convertido en uno de ellos, comprometiéndose a identificar los riesgos y proporcionar las respectivas soluciones para reducir o desaparecer el impacto del riesgo.

- **Certificados digitales [12].**

  La utilización de certificados para las aplicaciones web es importante y necesaria, debida a la información que se maneja, ya que sin este mecanismo de seguridad la información viaja en texto plano. Es necesario educar a los usuarios finales sobre la importancia de conocer e identificar el origen y la autenticidad de los mismos para no ser víctimas de ataques con certificados digitales falsos.

- **Escaneo de Puertos. [3]**

  En contra del proceso de escaneo de puertos se recomienda:

  - Tener habilitados los puertos necesarios.

- Proteger los puertos que no usemos con aplicaciones de autenticación.
- IDS de hosts.

- **Boletines de seguridad que publican en las páginas web oficiales de los sistemas operativos.**

  Estar pendientes de las expediciones de boletines de seguridad actuales para conocer nuevos parches, programas que soluciones las vulnerabilidades del Sistema Operativo utilizado.

- **Procesos de concientización.**

  Un proceso de concientización de los usuarios finales con una oportuna publicidad, demostraciones, demos, simulacros de los procesos de seguridad física y lógica, para que se encuentren preparados ante ataques de personas maliciosas.

3.4.2.3. Estrategias de protección detectivas.

- **Políticas de seguridad.**

  Establecer políticas de seguridad tanto para la seguridad física y lógica enfocados al usuario final que utiliza la red LAN de la Universidad tanto para la red inalámbrica como la cableada.

- **Herramientas Antisniffing [7].**

  La facilidad de conseguir herramientas para sniffing es fácil, por lo que sería importante considerar el hecho de utilizar herramientas antisniffing para detectar sniffers tales como:

  - Sniffdet Linux.
  - Prodetect Windows.
  - Promise Detect.

- **Siempre estar actualizados.**

  Al tener una cultura de actualización, ya sea del sistema operativo, parches de los programas o herramientas que se está utilizando, reduce el riesgo de enfrentarnos a problemas de seguridad.

- **Recursos compartidos.**

  - Otro tipo de práctica en la seguridad por oscuridad implementada en Windows es desactivar los recursos compartidos de red administrativos (como C$ y Admin$).

  - Otra forma es compartir el recurso y al final del nombre colocar un signo de $ para ocultar y no pueda ser vista por terceras personas.

- **Criptografía [11].**

  Para evitar los ataques de hombre en el medio se debe utilizar un protocolo IPSEC ya que este permite evitarlo ya que cada extremo de la conexión llaves de autentificación protegiendo dicha conexión.

- **Realizar auditorías [20].**

  El hacer auditoría en cierto tiempo ayudaría a mejorar los procesos de seguridad verificando y validando las debilidades existentes de la red LAN de la Universidad.

- **Protegerse de los sniffers [13].**

  Se podría utilizar comandos locales para revisar algún comportamiento anormal, esto se lo puede hacer con el comando ifconfig en Linux. La figura 3.9 muestra que la tarjeta de red se encuentra en modo monitoreo debido a que los sniffers se valen de éste método de escucha.

ifconfig
UP BROADCAST RUNNIG PROMISC MULTICAST MTU: 1500 Metric: 1

Figura 3.9. **Ejemplo del comando ifconfig.**

Se cuenta con un mapa conceptual localizado en el capitulo 4 de Discusión de resultados para mayor información y comprensión de las causas principales de los problemas y las estrategias de protección.

"Por lo tanto, en la guerra, el camino es evitar lo que es fuerte y atacar lo que es débil"

Sun Tzu

CAPÍTULO 4

DISCUSIÓN DE RESULTADOS.

En este capítulo se realiza la discusión de los resultados obtenidos de toda la tesis.

- Para ir disminuyendo o mitigando las vulnerabilidades encontradas durante el desarrollo de esta tesis se debe contar con una gran disponibilidad y unificar esfuerzos para obtener los resultados esperados.
- El considerar todos estos temas de seguridad detallados anteriormente, entender su funcionamiento en la redes LAN, y tener claro lo que se debe proteger es fundamental en una organización.
- Por lo tanto una organización en la mayoría del tiempo está más arriesgada a un ataque interno que a uno externo según los reportes presentados por Symantec y Cybsec, por ello conlleva a una emergente utilización de medidas de seguridad para contrarrestarlas o evitarlas.

- Se cuenta con varias metodologías que se pueden aplicar para un test de penetración, en este caso se han analizado cada una de las características de ellas, optando por la que cumple con las necesidades de la red LAN como: análisis de riesgos, seguridad física, seguridad de las comunicaciones, seguridad en las tecnologías de internet y seguridad inalámbrica.

- Los IDS no controlan el tráfico encriptado y paquetes IPv6[47] por lo que se debería tomar las medidas para resolver estos problemas identificados.

- El manual de gestión de seguridad ya establecido no se ha estipulado las medidas a tomar en el caso de que las personas encargadas de los servidores no cumplan con las políticas ya establecidas.

- El Plan de contingencia en la actualidad es necesario en toda organización, actualmente la información es el activo más importante y crítico, ya que la misma viaja a través de diferentes redes de datos.

- El servicio de Voz/IP implementado en el laboratorio para las pruebas de penetración no garantiza totalmente la seguridad, por lo que la autenticación entre el cliente y el servidor así como las llamadas no viajan encriptados.

- Los puntos de acceso que no cuentan con ningún tipo de cifrado y no están configurados para hacer filtrados de MAC son susceptible a varios ataques como intercepción de las comunicaciones mediante técnicas de hacking.

- Se demostró que el usuario final es el eslabón más débil de la cadena de TI, por ejemplo al presentarse al usuario un certificado digital falso al momento que éste ingresa a una página web con SSL, el usuario lo acepta sin tomar las medidas de seguridad adecuadas, enviando la clave desencriptada. La solución principal para la reducción del riesgo de que un usuario acepte estos certificados es la formación y concientización por parte de los usuarios finales.

[47] Protocolo de Internet Versión 6

- La autenticación que realizan los usuarios para ingresar a aplicaciones web con autenticación no cifrada podría ser vista por un atacante, lo que es crítico e importante la implementación de certificados digitales mediante protocolo SSL para enviar encriptados los datos confidenciales. Y además algunos servicios no controlan el límite de intentos fallidos, pudiendo ser víctimas a un ataque de diccionario.

- La mayoría de los usuarios finales no conocen que puertos o servicios corren en sus máquinas, por eso la mayoría tienen habilitados puertos innecesarios o abiertos sin ningún tipo de restricción, este el caso de configuración por defecto, se debe tomar medidas correctivas por ejemplo de filtrar o instalar una herramienta de escaneo de los servicios habilitados.

- Otro de los puntos débiles del factor humano es al asignar sus contraseñas, la mayoría utiliza contraseñas muy débiles, fáciles de descifrar; la contraseña es la llave de acceso para ingresar a cualquier aplicación. Es así que la robustez de la contraseña determina que tan segura es.

- Los sistemas informáticos utilizan el mecanismo de usuario y contraseña para la autenticación, siendo víctimas de herramientas para descifrar claves, por lo tanto la es importante considerar la creación de contraseñas que contengan caracteres alfanuméricos y especiales.

- La alta disponibilidad de herramientas libres para hacking en el internet son amenazas, ya que hoy en día no se requiere un elevado conocimiento para realizar un ataque a una red puesto que hay herramientas que son fáciles de utilizar automatizando estos procesos, lo cual esto puede ocasionar graves problemas debido al desconocimiento de los efectos del uso, pero lo más importantes es buscar las soluciones para estar protegidos o actuar proactivamente.

- El Mapa conceptual desarrollado es un resumen gráfico del proyecto final de carrera, concibiendo una idea clara y precisa de todo el análisis, desarrollo y soluciones de seguridad sugeridas. Ver figura 4.1.

MAPA CONCEPTUAL.

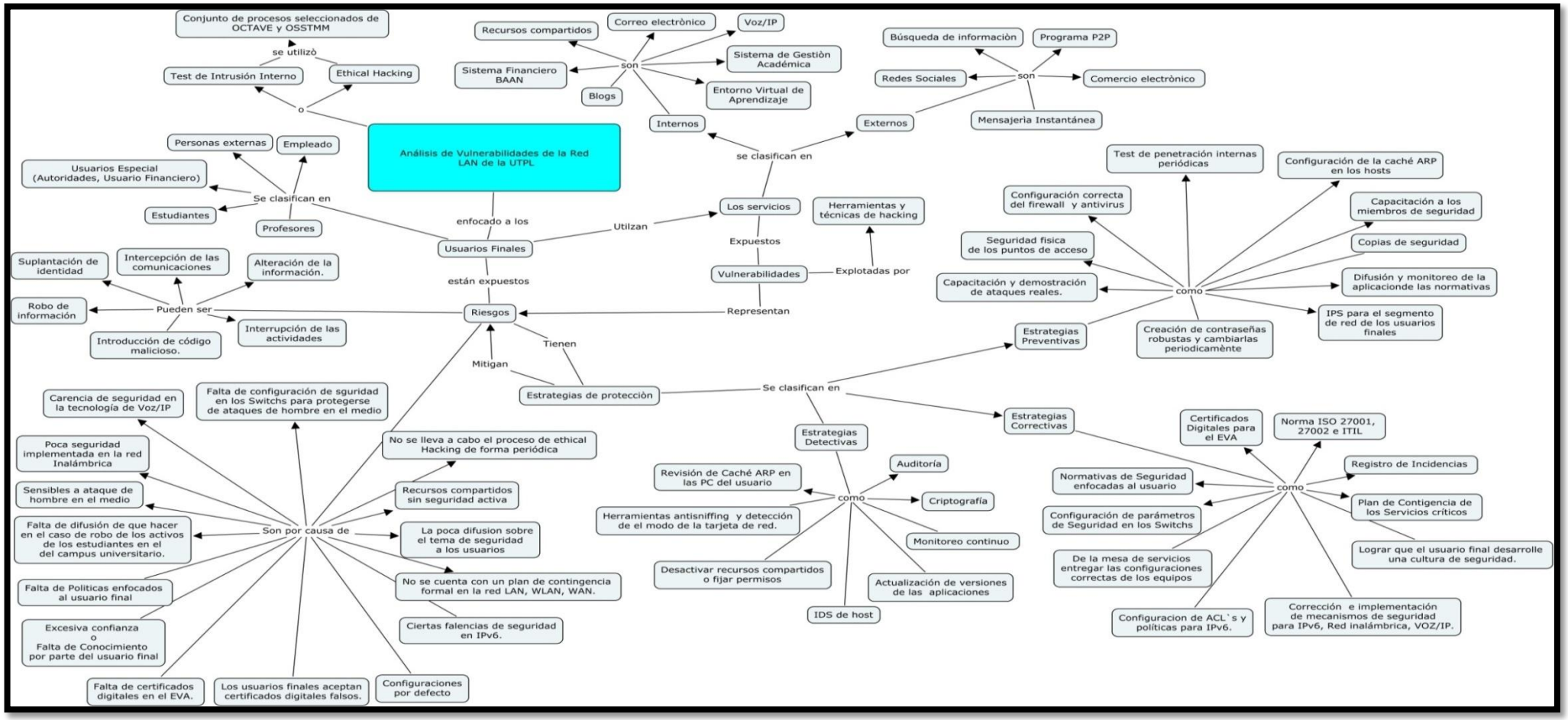

Figura 4.1 **Mapa conceptual**

"Las organizaciones gastan millones de dólares en firewall y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de la seguridad la gente que usa y administra los ordenadores"

Kevin Mitnick

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

Este capítulo está enfocado en contribuir nuevas aportaciones en beneficio al área de Seguridades de la Información de la Universidad Técnica Particular de Loja, y para los usuarios finales con el objetivo de mantener intactas las características de la seguridad.

CONCLUSIONES.

- El conjunto de procesos seleccionados empleados para el test de intrusión fue la unión de algunos secciones de seguridad de la metodología Osstmm y de todas las fases de Octave, las cuales se adoptaron a las necesidades iniciales del proyecto de investigación, proporcionado una guía importante para determinar los pasos a seguir, brindando los ítems de entrada y salida para la culminación exitosa de la tesis.

- Se ha podido cumplir con todos los pasos incluidos en el conjunto de procesos de las dos metodologías durante el periodo abril - agosto, como resultado se presenta un informe final de test de intrusión interno donde se demuestra los hallazgos encontrados,

un plan de acción para mitigar los riesgos y políticas de seguridad enfocadas al usuario final, además en el Anexo V existe un documento de entrega/recepción de los documentos anteriormente descritos al equipo de seguridad de la información de la Universidad.

- Este tipo de proyecto permite actuar de forma proactiva anticipando los hechos que pueden suscitar, analizando el impacto de los riesgos y el nivel de criticidad, además se ha demostrado que no es suficiente la estrategia actual si no la combinación de todo la infraestructura de seguridad con las pruebas de ethical hacking.

- No se puede llegar a tener una seguridad al 100%, pero aplicando algunas de las estrategias de protección se obtendrá una seguridad aceptable de acuerdo a las necesidades de seguridad que se requiere.

- Los servicios internos y externos que manipula el usuario final por medio de la red LAN siempre se encuentran acechados por múltiples riesgos de seguridad, el nivel de criticidad identificado por cada uno de los riesgos fue determinado en base a la continuidad del negocio más no en un cierto servicio, también en la experiencia de las personas que están al contacto de los usuarios finales y por la probabilidad de ocurrencia de los riesgos.

- Es así que la concientización de parte de todos los usuarios finales es crucial y fundamental para mitigar el gran porcentaje de problemas encontrados, siendo el usuario final el principal protagonista, además proporcionar capacitaciones periódicas enfocadas al factor humano con el tema de seguridad de la información con el objetivo de protegerse de los ataques.

- Al tener recursos compartidos sin ningún tipo de restricción podrían ser utilizados por personas ajenas fácilmente para beneficio propio o para hacer un daño y además se podría mencionar que la mayoría de los usuarios tienen servicios comunes habilitados.

- Si el atacante logra obtener la contraseña de cierto sistema informático, podrá acceder, revisar la información, suplantar la identidad, denegar el servicio puede ser en el caso

de algún usuario crítico como: administrador de servidores, sistemas informáticos, casos financieros, académicos, etc. llevando a cabo cualquier intrusión no autorizada.

- Se es necesario que los altos directivos conozcan la realidad latente de la falta de concientización por parte de los usuarios y los problemas que se están ocasionando, con esto se lograría el apoyo de los directivos para desarrollar los procesos de seguridad de manera ágil y oportuna.

- De tal forma que la red cableada como la red inalámbrica puede ser interceptada las comunicaciones, sin embargo la red inalámbrica es más propensa ya que algunos Puntos de Acceso están abiertos, considerar las mismas políticas de utilización y administración para estos dos tipos de redes que son utilizados por los usuarios.

- El conjunto de técnicas, procesos y herramientas utilizadas fue lo más importante para realizar las pruebas de ethical hacking, ayudando a recopilar información y obtención de resultados. La mayoría del software es gratuito y está disponible ampliamente en el internet, siendo una amenaza para la seguridad.

- Los riesgos planificados desde el principio de esta tesis fueron considerados ALTOS, pero en el trayecto y final han sido categorizados de la misma forma, se debe tomar los controles de forma urgente ya que el impacto en el caso de que llegará a suscitar es ALTO, llegando a tener problemas no previstos. Sin embargo la mayoría de estos riesgos de intercepción de las comunicaciones, robo/pérdida de información, suplantación de identidad e interrupción de los servicios son producidos en algunos casos por el factor humano, originados por descuido, robo del equipo portátil, memorias, virus informáticos, recursos compartidos sin protección, entre otros.

- La principal preocupación detectada es que la mayoría de los ataques son suscitados por amenazas internas como el personal interno, reduciendo la hipótesis que el origen son las amenazas externas, no se debería dejar a un lado esta afirmación, al contrario, prestar toda la atención.

RECOMENDACIONES.

- Se recomienda un análisis profundo de los hallazgos encontrados, sobre todo conocer cuál sería el efecto de las estrategias a implementar ya sean estas a corto, mediano o a largo plazo, se debe tomar en cuenta la comodidad ante la seguridad.

- La seguridad es un conjunto de procesos mas no es un producto, es recomendable que se estudie el plan de acción emitido para que sea aplicado por las personas encargadas de la gestión de la seguridad de la información de la Universidad.

- Es primordial utilizar herramientas, técnicas y procedimientos que permitan evitar, detectar o corregir las vulnerabilidades encontradas y actuar de forma proactiva ante ataques informáticos por lo tanto es recomendable que todo los procesos, tecnología y servicios a implementar en la red de LAN, los mismos que sean para el uso de los usuarios finales tengan un proceso de análisis de vulnerabilidades y se recomienda que este tipo de proyecto se haga en un ambiente de pruebas para evitar la interrupción del servicio en producción.

- Debido a los problemas suscitados y encontrados durante este proyecto de tesis, es imprescindible la implementación de un IDS/IPS para todos los segmentos de la red enfocados a los usuarios finales garantizando la seguridad.

- Se recomienda mantenerse informados de las nuevas herramientas de seguridad disponible, de tal forma permite la actualización del plan de acción, debido a que las vulnerabilidades y amenazas cada día aumentan y cambian rápidamente. Gracias a la aplicación de la gestión de la seguridad con el plan de (PLAN-DO-CHECK-ACT). para realizar un monitoreo continuo de la seguridad de la información.

- Sin embargo la implementación de una solución para monitorear al usuario final sería otra solución extrema, permitiría conocer el cumplimiento de las políticas, es el caso del tipo de robustez de contraseñas, parches de las aplicaciones, versiones del sistemas operativos, la actualización del antivirus, entre otras cosas, analizando el nivel de cumplimiento de las mismas.

- Es recomendable la implementación de políticas enfocadas al usuario final que fueron elaborados, es imprescindible utilizar métodos de difusión de las políticas como: prensa escrita o televisiva y lo más difícil es tratar de conocer que el personal está cumpliendo con estas políticas, esto reduciría un gran porcentaje las amenazas que acechan día a día y una respectiva capacitación al factor humano.

- De forma paralela a la aplicación de políticas de seguridad se recomienda el proceso de auditoría de la gestión de la seguridad ya que es fundamental utilizarla, ayudando a verificar de qué forma se están cumpliendo las políticas y revisando si cumplen con las expectativas.

- Se recomienda la implementación de mecanismos de protección y de seguridad para IPv6 y las respectivas políticas de seguridad.

- El recurso humano que integra el grupo de seguridad debe estar constantemente actualizado, capacitado y asesorado, llevar un seguimiento total o un ethical hacking de la seguridad implementada, generando un informe de las vulnerabilidades encontradas y las correcciones correctivas.

- Se debe utilizar mecanismos de autenticación robustos para la administración de servicios críticos u otros servicios definidos por el rol del usuario para establecer los privilegios asignados a ese rol, más no por el método común de asignación de privilegios a la persona que tenga cierta dirección IP, ya que la dirección IP puede ser suplantada.

PROYECTOS FUTUROS.

- Llevar a cabo un proceso de auditoría interna y un control interno a la red LAN de la Universidad.

- Realizar el proceso de ethical hacking enfocado a las aplicaciones desarrolladas por el personal de la Universidad para identificar y analizar vulnerabilidades.

- Implementar el Esquema de Seguridad para IPv6 para toda la red de equipos activos y usuarios finales.

- Que el proceso de la metodología planteada en este proyecto de tesis sea llevada a cabo por el área de la seguridad de la información en los diferentes campos.

- Implementar una Honeynet interna UTPL para analizar tráfico malicioso originado desde la red interna.

- Realizar un software de seguridad que permita automatizar la mayoría de los procesos seleccionados en esta tesis.

REFERENCIAS

Capítulo 1.

[1] ArCERT. (s.f.). ***Manual de Seguridad en Redes*** . Recuperado el 22 de Noviembre de 2009, de Manual de Seguridad en Redes : Disponible ne http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

[2] Ardita C. Julio Lic. ***Jornadas de Seguridad Informática*** recuperado el 30 de Marzo de 2010 CYBSEC. Security Sistems Disponible en: http://www.santacruz.gov.ar/informatica/noticias/seguridad/AR_Santa_Cruz_Presentacion_v2.pdf.

[3] Berenguela Castro, A. A, & Cortes Collado, J. P. (Diciembre de 2006). ***Metodología de medición de Vulnerabilidades en redes de datos de Organizaciones*.** Recuperado el 28 de Octubre de 2009, de http://www.formacionalimentaria.com/documentos/medicion-vulnerabilidades.pdf

[4] Borghello, C. F. (Septiembre de 2001). ***Seguridad Informática sus implicaciones e implementación*.** Recuperado el 28 de Octubre de 2009, Disponible en http://www.segu-info.com.ar/tesis/

[5] Delgado Reyes, Silvia Janeth, Guaichizaca, Sarango Laura Amparo. ***Análisis de la Influencia de los Delitos Informáticos e implementación de Políticas para su prevención en la red y las plataformas de la Universidad Técnica Particular de Loja.*** Recuperado el 24 de Noviembre del 2009. Disponible http://www.utpl.edu.ec/eccblog/wp-content/uploads/2007/04/articulo-tecnico-analisis-de-la-influencia-de-los-delitos-informaticos-e-implementacion-de politicas_silviadelgado.pdf.

[6] ***ESET. (2010). ESET Security Report Latinoamérica***. Recuperado el 16 de Marzo de 2010, de ESET Security Report Latinoamérica. Disponible en http://www.eset-la.com/press/informe/eset_report_security_latinoamerica.pdf

[7] Gómez Cárdenas, R. (20 de Noviembre de 2005). ***Seguridad en redes LAN***. Recuperado el 1 de Diciembre de 2009. Disponible en http://www.criptored.upm.es/guiateoria/gt_m626j.htm

[8] Herzog, P. (s.f.). ***Metodología Abierta de Testeo de Seguridad***. Recuperado el 15 de Noviembre de 2009. Disponible en http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

[9] Hidalgo, R. (2006). ***Uso de IPSEC versus SSL para aplicaciones de internet de la UTPL***. Recuperado el 23 Noviembre del 2010

[10] Loayza *Carlos.* ***Seguridad para la Red Inalámbrica de un Campus Universitario***. *Tomado el 27 de Noviembre del 2010.* Disponible en www.lacnic.net/documentos/lacnicxi/presentaciones/WiFi_UTPL.ppt

[11] López García, M. d. (15 de Junio de 2009). ***Seguridad en los sistemas de información****:* Recuperado el 1 de Diciembre de 2009. Disponible http://delta.cs.cinvestav.mx/~francisco/ssi/PresentacionSeguridad.pdf

[12] Monroy López, D. (Junio de 2009). ***Análisis inicial de la anatomía de un ataque a un sistema informático***. Recuperado el 27 de Noviembre de 2009. Disponible en http://www.segu-info.com.ar/tesis/

[13] Ochoa Roblez, J. M., Quinde España, V. M., & Uyaguari Ojeda, M. (2006). **E*valuación de Amenazas y Vulnerabilidades de Recursos Criticos Operacionales(OCTAVE) a nivel de usuario final para la UTPL.*** Loja. Disponible en http://www.utpl.edu.ec/eccblog/wp-content/uploads/2007/04/articulo-tecnico-evaluacion-de-amenazas-y-vulnerabilidades-de-recursos-criticos-operacionalesoctave-a-nivel-de-usuario-final-para-la-utpl.pdf.

[14] ***Guia de Pruebas OwaspV3.*** (2008). Recuperado el 22 de Noviembre de 2009. Disponible en http://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf

[15] Pinzón Olmedo Freddy Bolívar**.** Junio del (2008***). Identificación de vulnerabilidades, análisis forense y atención a incidentes de seguridad en los servidores de la UTPL***. Recuperado el 22 de Noviembre del 2010. Disponible en http://www.segu-info.com.ar/tesis/

[16] Racciatti, H. M. (2005). ***Metodologías de Testeo de la Seguridad. @RROBA*** (94), 12. http://es.calameo.com/read/000122258ce6a23a6fca2

[17] ***Robos por internet, el factor humano los usuarios son en el talón de Aquiles en la seguridad informática. La 'Ingeniería Social', un arma para cometer ciberdelitos***. (08 de 15 de 2008). Recuperado el 15 de Abril de 2010. Disponible en http://www.dinero.com/edicion-impresa/tecnologia/robos-internet-factor-humano_51219.aspx

[18] Symantec, Applied Research Reporte *Seguridad IT*, Recuperado en Noviembre del 2010**.** Tomado el 6 de Agosto del 2010.

[19] ***Sistema de Gestión de Seguridad Norma ISO-27001***. (s.f.). Recuperado el 27 de Noviembre de 2009. Disponible en http://www.slideshare.net/gugarte/sistema-de-gestion-de-seguridad-it-norma-iso-27001-corpei-presentation

[20] Tirado, J. M. (28 de Enero de 2009). ***El usuario es el eslabón más débil en la cadena de protección*** *IT*. Recuperado el 14 de Abril de 2010. Disponible en http://www.eset-la.com/press/concurso/enemigo-interno.pdf

[21] Verdesoto Gaibor, A. (2007). **Utilización de Hacking Ético para diagnósticar, analizar y mejorar la seguridad Informática en la Intranet de vía celular comunicaciones y representaciones.** Quito. Disponible en http://hdl.handle.net/15000/548.

[22] Vieites, Á. G. (2007). ***Enciclopedia de la Seguridad Informática*** . México : Alfaomega. Tomado el 27 de Noviembre del 2009.

Capítulo 2.

[1] Cabrera, A., Cueva, H., & Espinosa, M. P. (15 de Julio de 2008). ***Manual de Gestión de Seguridad de la Información***. Loja, Ecuador.

[2] ***Manual de Administración de la Red LAN*** del grupo de Telecomunicaciones. Tomado el 27 de Noviembre del 2009.

Capítulo 3.

[1] Aguirre Briones, G. J., Sanclemente Ordóñez, Á. I., & Ureta Arreaga, L. A. (2005). "***Seguridad en redes Inalámbricas***". Guayaquil. Recuperado el 23 de mayo del 2010.

[2] Álvarez Marañón, G., & Pérez García, P. P. ***Seguridad informática para empresas y particulares.*** Mcgraw-hill. Tomado el 5-Agosto-2010

[3] Audea, ***Seguridad de la Información*** Recuperado el 25 de junio del 2010. Disponible en http://www.abogados-lopd.es/wp-content/uploads/2009/11/20100430-%C3%81UDEA-Boletin-de-Vulnerabilidades.pdf

[4] Calvo Orra, A. (2006). ISO 27001. ***Normas y Estándares*** . CERT. (17 de Septiembre de 2008). ***OCTAVE***. Recuperado el 27 de Marzo de 2010, Disponible en http://www.cert.org/octave/

[5] Castellanos Luis ***¿Qué porcentaje de gente usa Mac, Linux, Windows, etc.?*** (2009) .Tomado el 15 de junio del 2010. Disponible en http://tecnologiaaldia.wordpress.com/2009/11/30/%c2%bfque-porcentaje-de-gente-usa-mac-linux-windows-etc/

[6] Corral Torrela, G. (10 de Julio de 2009). **N*ew Challenges in Detection and Manegement of Security of Vulnerabilities in Data Networks*** Tesis Doctoral. Barcelona. tomado el 24 de mayo del 2010.

[7] Detectando sniffers en nuestra red. Redes conmutadas y no conmutadas tomado el 15 de junio del 2010. Disponible en http://www.maestrosdelweb.com/editorial/sniffers.

[8] ***Envenamiento ARP INTECO***. Tomado el 15 de junio del 2010. Disponible en http://www.inteco.es/Seguridad/Observatorio/Actualidad_Observatorio//Noticia_articulo_envenenamiento

[9] ESET. (2010). ***ESET Security Report Latinoamérica***. Recuperado el 16 de Marzo de 2010. Disponible en www.eset-la.com

[10] Farías-Elinos, M., Gómez Velazco, L. E., & Mendoza Díaz, M. C. (s.f.). ***Importancia del Análisis de Riesgo de Seguridad.*** Recuperado el 17 de Abril de 2010. Disponible en http://seguridad.internet2.ulsa.mx/congresos/2003/cudi2/impariesgo.pdf

[11] Forné, J., Melús, J. L., & Soriano, M. (s.f.). ***Criptografía y Seguridad en Comunicaciones***. Recuperado el 28 de Octubre de 2009. Disponible en http://www.govannom.org/seguridad/criptografia/jf_novatica.pdf

[12] Fyodor. (s.f.). *Secctols*. Recuperado el 16 de Abril de 2010, ***Las 75 Herramientas de Seguridad Más Usada.*** Disponible en http://sectools.org/

[13] Gómez Cárdenas, R. (20 de Noviembre de 2005). ***Seguridad en redes LAN***. Recuperado el 1 de Diciembre de 2009. Disponible en http://www.criptored.upm.es/guiateoria/gt_m626j.htm.

[14] Hervalejo Sánchez Alberto. ***Auditorías de Seguridad Informática y la OSSTMM*** (2009). Tomado el 15 de mayo del 2010. Disponible en: http://www.scribd.com/doc/17740680/Auditorias-de-Seguridad-Informatica-y-la-OSSTMM#fullscreen:on

[15] Herzog, P. (s.f.). ***Metodología Abierta de Testeo de Seguridad*** . Recuperado el 15 de Noviembre de 2009. Disponible en http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf OSSTMM 2.1.

[16] Hidalgo, R. (2006). ***Uso de IPSEC versus SSL para aplicaciones de internet de la UTPL***.

[17] Hispasec Sistemas ***¿Cuánto tardan los grandes fabricantes de software en arreglar una vulnerabilidad?*** (Septiembre, 2009). Disponible en http://www.hispasec.com/laboratorio/Hispasec_Estudio_Vulnerabilidades.pdf, tomado el 15 de junio del 2010.

[18] González Tello Mery E ***Diseño del sistema de mejoramiento de seguridad y administración de trafico para el ISP (Internet service provider) "READYNET"*** Recuperado el 22 de Junio de 2010. Disponible en http://bibdigital.epn.edu,ec/bitstream/15000/52/1/CD-0019.pdf.

[19] Hernandez Maximilian Alan (2004) ***Estrategias de seguridad informática***. Tomado el 15 de junio del 2010. Disponible en http://www.desarrolloweb.com/articulos/1592.php

[20] Mieres Jorge(2009) ***Ataques informáticos Debilidades de seguridad comúnmente explotadas***. Disponible en https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf.

[21] Monroy López, D. (Junio de 2009). ***Análisis inicial de la anatomía de un ataque a un sistema informático***. Recuperado el 27 de Noviembre de 2009. Disponible en http://www.segu-info.com.ar/tesis/

[22] Nmap. (s.f.). ***Nmap.*** Recuperado el 13 de Abril de 2010, de Nmap. Disponible en http://nmap.org/

[23] Ochoa Roblez, J. M., Quinde España, V. M., & Uyaguari Ojeda, M. (2006). ***Evaluación de Amenazas y Vulnerabilidades de Recursos Criticos Operacionales(OCTAVE) a nivel de usuario final para la UTPL***. Loja.

[24] Ramió Aguirre Jorge (febrero/junio de 2010) ***Elementos de optimización en la gestión de la seguridad de la información orientada a la continuidad del negocio.*** Recuperado el 13 de Julio del 2010. Disponible en http://www.criptored.upm.es/guiateoria/gt_m001x.htm

[25] *Remoite-**Exploit Bactrack4*.** (s.f.). Recuperado el 13 de Abril de 2010. Disponible en http://www.backtrack-linux.org/?lang=es

[26] Sophos. (2010). ***Security Threat Report 2010***. Recuperado el 19 de Febrero de 2010. Disponible en http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf

[27] Mohamed Al-Hemairy, Saad Amin, Zouheir Trabelsi (2009)
Towards More Sophisticated ARP Spoofing Detection/Prevention Systems in LAN Networks. Tomado el 25 de julio del 2010.

[28] Vila, C. (s.f.). ***El origen de los ataques de la red interna:DEBILIDADES DEL PROTOCOLO ARP***. Recuperado el 15 de Abril de 2010. Disponible en http://www.infosecurityvip.com/newsletter/capacitaciones_abr10.html

ANEXO I

CARACTERISTICAS DE LOS DISPOSITIVOS DE RED DE LA UTPL

Es importante presentar las características de cada uno de los dispositivos que forma la red de la universidad.

- ***Equipos de gestión de seguridad.***

  - **Características del OSSIM.**

Tabla Anexo 1. 1 **Características del OSSIM**

Sistema Operativo	Debian Versión 4.0
Memoria RAM	4 GB
2 Memoria de disco duro	173 GB cada uno.
2 procesadores	Intel XEON 3.6 GHz
Software	OSSIM Versión O.9

  - **Características del firewall ASA.**

Tabla Anexo 1. 2 **Características de Firewall ASA**

Hardware	ASA 5540-k8
Memoria RAM	1 GB
Aplicación	CISCO ADAPTATIVE Security Appliance Versión 7.2
Procesador	Pentium 4 2000 MHz

- **Características del IPS.**

Tabla Anexo 1. 3 **Características del IPS**

IPS del Firewall ASA	
Plataforma	ASA-SS-20
Software	Cisco Intrusión Prevention System Versión 7.0
IPS del Switch CORE	
Plataforma	WS-SVC-IDSM-2

Nota: solo la plataforma cambia entre los IPS.

- ***Equipos de la red LAN***

- **Características del Switch de Core**

Tabla Anexo 1.4 **Características del Switch de Core**

Modelo	Cisco Catalyst 6500
IOS	12.2(8)
Número de Puertos	16 GbitEthernet 8 GBIC
Velocidad de Transmisión de los puertos	10/100/1000MB
Conectores	RJ-45 y Fibra
Soporte de cables	UTP CATG 6
Estándar cumple	IEEE 802.3 1000 BaseLH, 1000 BaseT
Fuente de alimentación	Externa
Capa	3

- **Características del Switch 3550**

Tabla Anexo 1. 5 **Características del Switch 3550**

Modelo	Cisco Catalyst 3550
IOS	12.2(24)SEE4
Número de Puertos	10 Gigabitethernet 2 Gigabit
Velocidad de Transmisión de los puertos	1000MB
Conectores	RJ-45 y FIBRA LX

Soporte de cables	UTP CATG 6 - FIBRA (LX)
Estándar cumple	IEEE 802.3 1000BaseTX, 1000 BaseLX.
Fuente de alimentación	Externa
Capa	2

- **Características del Switch 3560.**

Tabla Anexo 1. 6 **Características del Switch de distribución 3560**

Modelo	Cisco Catalyst 3560
IOS	12.2(35)SE5
Número de Puertos	24 GigabitEthernet 4 GBIC
Velocidad de Transmisión de los puertos	1000MB
Conectores	RJ-45 y FIBRA
Soporte de cables	UTP CATG 6 Y FIBRA (SX)
Estándar cumple	IEEE 802.3 1000 BaseTX, 1000 BaseSX.
Fuente de alimentación	Externa
Capa	2

- **Características del RADIUS**

Tabla Anexo 1. 7 **Características RADIUS**

Procesador	Intel Genuino Pentium 3 733,637 MHz
Memoria RAM	750 MB
Disco Duro	40 GB
Firewall	Local
Sistema Operativo	Centos Versión4.4
Demonio	Radiusd

- **Características Switch Cisco 2950**

Tabla Anexo 1. 8 **Características del Switch de acceso 2950**

Modelo	Cisco Catalyst 2950
IOS	12.1(22)EA9
Número de Puertos	24 Fasethernet
Velocidad de Transmisión de los puertos	10/100MB

Conectores	RJ-45
Soporte de cables	UTP CATG 6
Estándar cumple	IEEE 802.3 10Base-T Ethernet
Fuente de alimentación	Externa
Capa	2

- **Características del Switch 2960.**

Tabla Anexo 1. 9 **Características del Switch de acceso 2960**

Modelo	Cisco Catalyst 2960
IOS	12.2(44)SE6
Número de Puertos	24 FastEthernet 2 Giga
Velocidad de Transmisión de los puertos	10/100/1000MB
Conectores	RJ-45 y fibra
Soporte de cables	UTP CATG 6
Estándar cumple	IEEE 802.3 10Base-T Ethernet
Fuente de alimentación	Externa
Capa	2

ANEXO II

RIESGOS DE LOS SERVICIOS INTERNOS Y EXTERNOS

Los servicios que son utilizados por los usuarios finales se han clasificado de dos maneras:

- Servicios internos.
- Servicios externos.

- **Servicios internos.**

En la tabla 19 esta detallado los diferentes riesgos que están arriesgados los servicios internos que ofrece la universidad.

Tabla Anexo 2. 1 **Riesgos de los servicios internos**

SERVICIOS	RIESGOS
Correo electrónico	• Bloqueo del buzón de correo. • Robo de usuario y contraseña. • Correos infectados. • Pérdida de acceso al correo electrónico. • Correos con programas o antivirus falsos. • Correos cadenas. • Correo basura. • Que los correos se queden encolados. • Compartición de información confidencial. • Filtrado involuntario de información. • Modificación de los correos electrónicos. • Respuesta de servidor inválidas. • Correo no deseados a enlaces malintencionados. • Fraudes.
Eva (Entorno virtual de Aprendizaje)	• Alteración de contenido. • El uso de recursos ajenos. • Divulgación de datos confidenciales. • Sesión abierta o en caché. • Modificación de notas. • Enviar archivos maliciosos. • Adjuntar virus. • Modificar, eliminar tareas. • Robo del usuario y contraseña.
	• Alteración de datos confidenciales. • Eliminación de datos confidenciales.

Sistema de Gestión Académica	• Descifrar la clave y contraseña. Información no sea cifrada. • Indisponibilidad de la información. • Cambiar la clave. • Registrar notas. • Aprobar estudiantes. • Divulgación de la información.
Recursos compartidos.	• Alteración de la información. • Eliminación de la información. • Acceder a los recursos confidenciales. • Crear nuevas cuentas. • Instalar aplicaciones maliciosas. • Bloquear el recurso compartido. • Eliminación del recurso compartido. • Copiar archivos. • Husmear la privacidad. • Instalar programas que permiten acceso no autorizado. • Secuestro de sesiones.
Voz/IP	• Ancho de banda escaso. • Interrupción. • Intercepción de las llamadas. • Desvió de llamadas. • Pérdida de llamadas. • Venta de información. • Fraude. • Virus. • Redirección de llamadas. • reproducción de llamadas. • Secuestro de sesiones.
Acceso al medio con WIRELESS y LAN	• Interceptar las comunicaciones. • Descifrar contraseñas. • Conectarse a redes maliciosas. • Desviar las comunicaciones. • No poder acceder a la red.
Blogs	• Introducción de código malicioso. • Que los sitios se han comprometidos con imágenes, videos obscenos. • Los comentarios sean generados por código malicioso. • Enlaces maliciosos. • Violación a los derechos de autor. • Destrucción de datos.

- **Servicios externos.**

Así mismo como se explicó en los servicios internos también se mencionan los riesgos de los servicios externos.

Tabla Anexo 2. 2 **Riesgos de los servicios externos**

SERVICIOS	RIESGOS
Mensajería instantánea	• Virus. • Robo de usuario y contraseña. • Descargar programas con fines malintencionados. • Plagio de la contraseña. • Transferencia de archivos infectados. • Ingeniería social. • Vínculos a sitios web. • Mensajes con antivirus falsos. • Infectar a la computadora. • Comprometer la computadora.
Redes sociales	• Creación de perfiles falsos sin consentimiento. • Robo del usuario y contraseña. • Alteración de información confidencial. • Secuestro de cuentas de usuario. • Enlaces maliciosos. • Descargar programas, archivos dañinos. • Estafas. • Ataques de código malicioso. • Fraudes. • Pérdida de privacidad de la información. • Infectarse de virus. • Uso inadecuado de la información. • Links maliciosos.
Programas p2p(Emule)	• Software pirata. • Consumo de ancho de banda. • Difamación información confidencial. • Ocupación en el disco duro. • Propagación de troyanos, virus. • Propagación de programas espías. • Instalación de programas no deseados. • Acceder información confidencial. • Conexiones activas a pesar que el usuario se desconecte.
	• Robo de números de tarjeta de crédito. • Desviar los datos.

Comercio electrónico	• Fraudes electrónicos. • Ingresar a enlaces maliciosos. • Robo de usuario y contraseña. • Utilización no autorizada de los recursos. • Pérdida de dinero. • La información no viaje cifrada. • Compras inducidas.
Búsqueda de información	• Enlaces a sitios web maliciosos. • Virus. • Programas maliciosos. • La información quede almacenada en la caché. • Información inapropiada. • Que se indexen documentos confidenciales a través de la web.

ANEXO III

PLANTILLA DE LOS PROCESOS SELECCIONADOS.

La plantilla que está presentada a continuación sirve para llevar a cabo un test de intrusión utilizando la tecnología escogida en el capítulo 3, dividiendo por fases, las mismas que contienen los procesos a seguir.

Tabla Anexo 3. 1 **Plantilla de los procesos seleccionados.**

FASES	PROCESO
1. Construir perfiles de amenazas basado en activos.	P1. Identificación de la información a nivel de usuario.
	P2. Consolidación de la información y creación de perfiles de amenazas basados en activos.
2. Identificar los puntos vulnerables en la infraestructura.	P3. Identificación de componentes claves.
	P4. Evaluación de componentes seleccionados.
3. Desarrollo de planes y estrategias de seguridad.	P5. Análisis de riesgos.
	P6. Desarrollar estrategias de protección.

ANEXO IV

SEGURIDAD FÍSICA

ANEXO V

ACTA DE ENTREGA/RECEPCIÓN DE LOS ENTREGABLES AL EQUIPO DE SEGURIDAD DE LA UTPL

APPÉNDICE A.

GLOSARIO DE TÉRMINOS TÉCNICOS

A

Advanced LAN Scanner. Escanea puertos y recursos compartidos para Windows.

Amenaza. Es un hecho que puede producir un daño.

Antivirus. Programa que evita la intrusión de virus a un sistema.

Arp. Protocolo de resolución de direcciones a nivel de capa de red responsable de encontrar la dirección MAC que corresponde a una dirección IP.

Asterisk. Programa que funciona como una central telefónica es bajo licencia GPL.

Atacante. Persona con conocimientos informáticos que está acechando un sistema.

Ataque. Es un proceso dirigido por un atacante a través de un programa intenta ingresar a un sistema.

Auditoría. Es un estudio que se encarga de analizar e identificar vulnerabilidades.

Autenticación. Es el proceso de establecimiento y verificación de la identidad para realizar una petición.

Autoscan-Network. Herramienta para escanear de los hosts de un segmento de red.

B

Bactrack. Distribución de Linux para realizar un ethical hacking, contiene varias herramientas de hacking.

C

Caín & Abel. Herramienta de recuperación de contraseñas.

Capa de aplicación. Capa superior que maneja aspectos de representación e intercambio de datos que utilizan las aplicaciones.

Capa de enlace de datos. Capa encargada del direccionamiento físico.

Capa Física. Encargada de las conexiones físicas de la computadora hacia la red.

Capa de red. Capa 3 del modelo OSI el objetivo es hacer llegar los datos desde el origen al destino.

Capa de transporte. Esta capa es la encargada de efectuar el transporte de los datos desde el origen hasta el destino.

CERT. (Computer emergency response team) Equipo responsable para manejar los problemas concernientes a la seguridad informática.

Contraseña. Es una clave para la autenticación que tiene información secreta para el acceso.

Cracker. Persona con conocimiento de herramientas de hacking pero con fines maliciosos.

Criptografía. Proceso de transformar un test plano a un texto descifrado.

D

Denegación de Servicio. Es interrumpir el funcionamiento correcto de un servicio.

Diccionario. Se trata de un conjunto de palabras contenidas un archivo.

E

Ettercap. Sniffer para auditorias de redes LAN.

Exploits. Este consiste en aprovechar errores de programación en una aplicación con el objetivo de tomar el control de un sistema o realizar una escalada de privilegios.

F

Firewall. Es un cortafuegos/ software para controlar las comunicaciones denegando o permitiendo.

FTP. (File Transfer Protocol) Protocolo de transferencia de archivos.

Fuerza Bruta. Ataque que utiliza diccionarios para realizar las comparaciones con la clave a buscar.

G

Gateway. Equipos que permiten interconectar computadores

H

Hacker. Individuo con conocimientos informáticos pero no tiene intenciones maliciosos y es apasionado a la seguridad informática

Host. Es una computadora manipulada por los usuarios finales.

HTTP. (HiperText transfer protocol) protocolo perteneciente a la capa de aplicación usada par a las transacciones world wide web.

HTTPS. (HiperText transfer protocol Secure) es un protocolo basado en http, asegurando la transferencia de los datos.

I

IDS. Sistema de detección de intrusos que detecta accesos no autorizados a una red o computador.

Ingeniería Social. Técnica que se aprovecha la ingenuidad de las personas con el objetivo de obtener información.

Internet. Es un conjunto de computadoras conectadas entre sí.

IPS. Sistema de prevención de intrusos que previene accesos no autorizados.

IPSEC. Protocolo Seguro sobre el protocolo IP.

ISP. Proveedor de servicios de internet.

K

Keylogers. Herramienta que captura las teclas pulsadas.

L

LAN. Conexión de varios computadores con una extensión de 200 metros.

LDAP. Protocolo ligero de acceso a directorios permitiendo el acceso a un servicio de directorio ordenado y distribuido.

M

Medusa. Programa que permite el ataque de fuerza bruta a diferentes servicios.

N

Nessus. Herramienta para el análisis de vulnerabilidades.

Netbios. Protocolo que permite el establecimiento y mantenimiento de sesiones de comunicaciones entre computadores.

Nmap. Herramienta para el escaneo de puertos.

P

PC. Computadora personal.

Ping. Comando que prueba el estado de conexión con un equipo.

POP. Protocolo de correo electrónico

Protocolo. Conjunto de reglas que establecen la comunicación entre dos computadoras.

S

SMB. Protocolo de red que permite compartir impresoras y archivos en red.

Smb4k. Programa que permite examinar y montar recursos compartidos de la red.

Smtp. Protocolo simple de transferencia de correo pertenece a la capa de aplicación se lo utiliza para el intercambio de mensajes de correo electrónico.

Sniffers. Programa de captura de las tramas de red.

T

TCP. Protocolo de control de transmisión orientado a la conexión, ofreciendo mecanismos de seguridad en el proceso de comunicación.

TCP/IP. Modelo de descripción de protocolos de red

Telnet. Protocolo que permite la conexión desde un terminal remoto.

Test de Penetración. Es un conjunto de metodologías y técnicas que permitan analizar debilidades de los sistemas informáticos.

U

UDP. Protocolo de datagramas de usuario no orientado a la conexión.

V

Virus. Programa o código malicioso.

VNC. Programa que permite controlar el computador remotamente desde un cliente.

Vulnerabilidad. Es una debilidad presente en cualquier sistema pudiendo ser explotada.

W

WAN. Red de área amplia extendidas sobre una amplia extensión geográfica.

Wireshark. Herramienta para el escaneo de paquetes de red.

X

Xploit. Es un mecanismo que consiste en que la víctima recibe una postal falsa en su correo electrónico que contiene el link de una web falsa.