UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

UNIDAD DE POSGRADO

MAESTRÍA EN CONECTIVIDAD Y REDES DE ORDENADORES

Tesis previa la obtención del Grado Académico de Magíster en Conectividad y Redes de Ordenadores

TEMA:

"SEGURIDAD INFORMÁTICA Y MÉTODOS DE PROTECCIÓN EN INFRAESTRUCTURAS TECNOLÓGICAS Y SU INCIDENCIA EN LA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO, AÑO 2015". DISEÑO DE UNA INFRAESTRUCTURA TECNOLÓGICA SEGURA.

AUTOR:

ING. GEOVANNY VEGA VILLACÍS

DIRECTOR:

Ing. JORGE MURILLO OVIEDO, MSc.

QUEVEDO – LOS RÍOS – ECUADOR

2015

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

UNIDAD DE POSGRADO

MAESTRÍA EN CONECTIVIDAD Y REDES DE ORDENADORES

Tesis previa la obtención del Grado Académico de Magíster en Conectividad y Redes de Ordenadores

TEMA:

"SEGURIDAD INFORMÁTICA Y MÉTODOS DE PROTECCIÓN EN INFRAESTRUCTURAS TECNOLÓGICAS Y SU INCIDENCIA EN LA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO, AÑO 2015". DISEÑO DE UNA INFRAESTRUCTURA TECNOLÓGICA SEGURA.

AUTOR:

ING. GEOVANNY VEGA VILLACÍS

DIRECTOR:

Ing. JORGE MURILLO OVIEDO, MSc.

QUEVEDO – LOS RÍOS – ECUADOR

2015

CERTIFICACIÓN

Ing. Jorge Murillo Oviedo, Msc**.** Director de la Tesis, previo a la obtención del Título Académico de Magíster en Conectividad y Redes de Ordenadores

C E R T I F I C A

Que el Ing. Geovanny Eduardo Vega Villacís, ha cumplido con la elaboración de la tesis titulado: **"SEGURIDAD INFORMÁTICA Y MÉTODOS DE PROTECCIÓN EN INFRAESTRUCTURAS TECNOLÓGICAS Y SU INCIDENCIA EN LA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO, AÑO 2015". DISEÑO DE UNA INFRAESTRUCTURA TECNOLÓGICA SEGURA.**

El mismo que está apto para la presentación y sustentación respectiva.

Ing. Jorge Murillo Oviedo, Msc.

DOCENTE - DIRECTOR

AUTORÍA

Yo, GEOVANNY EDUARDO VEGA VILLACÍS. Egresado de la segunda promoción de la Maestría en Conectividad y Redes de Ordenadores, declaro que el trabajo de tesis titulada: **"SEGURIDAD INFORMÁTICA Y MÉTODOS DE PROTECCIÓN EN INFRAESTRUCTURAS TECNOLÓGICAS Y SU INCIDENCIA EN LA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO, AÑO 2015". DISEÑO DE UNA INFRAESTRUCTURA TECNOLÓGICA SEGURA,** aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo el derecho de propiedad intelectual correspondiente de este trabajo a la Universidad Técnica Estatal de Quevedo, según lo establecido por la ley de propiedad intelectual, por su reglamento, y por la normativa institucional vigente.

_____

Ing. Geovanny Vega Villacís

DEDICATORIA

La presente tesis está dedicado a cada uno de los lectores portavoces de estas ideas, fruto trabajo abnegado con el cariño de mi familia, mi esposa Diana y mi hijo Pablo. La bendición de mi Dios y la guía espiritual de mi ángel celestial, mi Madre Mariana.

Geovanny

AGRADECIMIENTO

Agradezco de forma muy sentida a cada uno de las personas que apoyaron a plasmar estas ideas, hacerlas realidad: Mi Director de Tesis, a mi esposa Diana y mi hijo Pablo. A mi familia: Papá Marcelo, mis hermanos Santiago y Marcela.

A la Universidad Técnica Estatal de Quevedo y sus profesores, guías y tutores de nuestra profesionalización.

Geovanny

PRÓLOGO

En este trabajo de tesis sobre Seguridad Informática en Infraestructuras Tecnológicas, usted encontrará la información actualizada sobre metodologías, técnicas y sistemas de defensa informática para determinar las vulnerabilidades y amenazas que se puede presentar en redes de infraestructura.

Además una propuesta de diseño de infraestructura para la Universidad Técnica de Babahoyo y como incide la seguridad informática y los métodos de protección en la intranet de la institución.

Esperando que este trabajo de investigación sea lo más productivo para quien lo analice y sea referente de estudio con consejos sencillos y prácticos.

…….. (f)

RESUMEN EJECUTIVO

Hoy en día para la mayor parte de empresas, instituciones o cualquier tipo de organización, el recurso más importante a considerar es la información. No muy apartada a esta realidad, vive la Universidad Técnica de Babahoyo la misma que cuenta con una intranet en la que se desarrolla la mayor parte de actividades y se genera información de índole jurídica, administrativa, académica, etc. Razón por la cual la presente investigación plantea el siguiente problema a resolver: *¿Cómo incide una adecuada topología en el diseño de infraestructuras tecnológicas seguras y métodos de protección en la Universidad Técnica de Babahoyo?*

Para hacer frente a esta problemática, se ha trazado varios objetivos de estudio: Identificar los niveles de vulnerabilidad y amenazas que exhibe la intranet, usar adecuadamente paradigmas en materia de seguridad informática, como el modelo de *Defensa en Profundidad* para determinar estadísticamente las irregularidades existentes, y finalmente efectuar un diseño de infraestructura segura para la intranet de la Universidad Técnica de Babahoyo.

Los métodos y técnica de investigación que se emplearon fueron: Inductivo-deductivo, Hipotético-deductivo y el analítico-sintético, que permitieron evaluar los objetivos de investigación y validar la siguiente hipótesis: *"Los sistemas de seguridad informática y los métodos de protección en infraestructuras tecnológicas, inciden favorablemente en la intranet de la Universidad Técnica de Babahoyo."* Cuyos resultados obtenidos a través de encuestas y entrevistas a usuarios, administradores, docentes y autoridades de la institución demostraron que existe un 77% de errores en la red y sus servicios, tales como: Internet, acceso de usuarios registrados, seguridad a nivel de equipos, programas e interconectividad.

Finalmente se obtuvo como propuesta un diseño que mejorará las seguridades dentro de la red universitaria, permitirá la ejecución de un portal cautivo para asegurar el ingreso solo de personal registrado a la intranet, creación de cuentas de usuario encriptadas, aseguramiento de la red ante ataques de malwares y virus con un monitoreo de red; con el empleo del sistema Open Source Zentyal de Linux Ubuntu.

SUMMARY

Today, for most companies, institutions or any organization, the most important thing to consider is the information resource. Not far away this reality, living the Technical University of Babahoyo that it has an intranet where most activities take place and information is generated legal, administrative, academic, etc. Why this research raises the following problem to solve: *How adequate topology affects the design of secure technological infrastructure and protection methods at the Technical University of Babahoyo?*

To address this issue, it has set several objectives of study: Identify the levels of vulnerability and threats that displays the intranet, properly use paradigms in information security, such as defense in depth model to statistically determine the irregularities, and finally make a safe design for the intranet of the Technical University of Babahoyo infrastructure.

The methods and research techniques used were: Inductive-deductive and hypothetical-deductive, analytic-synthetic that allowed evaluate the research objectives and validate the following hypothesis: *"The security system and infrastructure protection methods technology, favorable impact on the intranet of the Technical University of Babahoyo."* The results obtained through surveys and interviews with users, administrators, teachers and authorities of the institution demonstrated that there is a 77% error in the network and services, such as Internet access registered level security hardware, software and interconnectivity users.

Finally it obtained as proposed a design that will improve securities within the university network, will allow the implementation of a captive portal to ensure the entry only registered staff intranet, account creation encrypted user, securing the network against attacks malwares and viruses with network monitoring; with the use of Open Source Zentyal Linux system Ubuntu.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

GLOSARIO DE TÉRMINOS

AES *Advanced Encryption Standard*

AH *Authentication Header*

ARP *Address Resolution Protocol*

CA *Certificate Authority* (Autoridad de Certificación)

CRL *Lista de Certificados Revocados*

DES *Data Encryption Standard*

ESP *Encapsulating Security Payload*

GNU *General Public License*

GnuPG *GNU Privacy Guard*

IDEA *International Data Encryption*

Algorithm **IANA** *Internet Assigned Number*

Authority. **IETF** *Internet Engineering Task*

IKE *Internet Key Exchange*

IP *Internet Protocol*

IPv6 *Internet Protocol* versión 6

ISECOM *Institute For Security And Open Methodologies*

LDAP *Lightweight Directory Access Protocol*

MAC *Message Authentication Code*

MD5 *Message Digest 5*

OSSTMM *Open Source Security Testing Methodology Manual*

PKCS	*Public Key Common Standards*
PKI	*Public Key Infrastructure*
PGP	*Pretty Good Privacy*
RSA	Rivest Shamir y Adleman, algoritmo.
RPV	*Red Privada Virtual*
SA	*Security Association*
SASL	*Simple Authentication and Security Layer*
SCEP	*Simple Certificate Enrollment Protocol*
SHA-1	*Secure Hash Algorithm*
TDES	3DES
TLS	Transport Layer Security
UTB	Universidad Técnica de Babahoyo

INTRODUCCIÓN

Con el desarrollo de la industrialización que forma parte de la actividad humana a partir de la mitad de siglo XVIII y que se consolidó con el desarrollo comercial en los inicios del siglo XIX, uno de los aspectos que siempre ha estado presente es el poder de la información; mismo que ha permitido el crecimiento acelerado de empresas, mano de obra y demanda de productos. En la actualidad tanto las empresas como los usuarios guardan gran cantidad de información en sus ordenadores e incluso en el caso de los usuarios domésticos almacenan gran cantidad de archivos, recuerdos, entre otros en sus computadores.

Esto ha conllevado a una dependencia en la que no todos son ventajas; es así, que hace unos veinte años atrás, podemos pensar que la pérdida de conectividad de Internet[1] o el mal funcionamiento de un sistema resultaba algo molesto; hoy en día la pérdida de conectividad e información significa que una empresa o institución quede prácticamente inoperante. Y a medida en que las organizaciones confían en la tecnología para hacer negocios, compartir información y transferencia de archivos, empiezan aparecer otras personas no tan bien intencionadas que ven la oportunidad para cometer acciones ilícitas y obtener un mayor beneficio.

En los sistemas informáticos es muy importante el volumen de información confidencial que se maneja; al hablar de pérdidas por revelamiento de información confidencial pueden ser numerosas y a partir de esta consideración las empresas e instituciones invierten recursos al implementar redes seguras. No muy ajena a esta realidad la Universidad Técnica de Babahoyo, presenta inconvenientes de seguridad informática en su infraestructura tanto al interior de la red como hacia la salida a la WAN.

[1] *Internet*.- Red de redes de arquitectura abierta con un protocolo de extremo a extremo fiable que permita una comunicación efectiva.
Ref: http://www.internetsociety.org/es/breve-historia-de-internet#Proving

La presente investigación plantea identificar los problemas, vulnerabilidades, amenazas y siniestros que puedan manifestarse en la Intranet de la Institución llegando a exponer información muy sensible y poner en alto riesgo la actividad jurídica, académica y financiera de la Universidad. Específicamente, se aborda el tema de la Seguridad Informática y los métodos para poder mitigar los riesgos que puedan alterar el orden funcional de las redes LAN e Intranets privadas y las vulnerabilidades al extender las comunicaciones hacia el Internet.

La estructura del trabajo de investigación a presentar se organiza de la siguiente manera: CAPÍTULO PRIMERO, se refiere al *Marco Contextual de la Investigación* que engloba la contextualización y ubicación del problema objeto de estudio, la situación actual problemática a ser inquirida, la enunciación del problema y sub-problemas; así como su delimitación, justificación, objetivos y cambios esperados.

El SEGUNDO CAPÍTULO abarca el *Marco Teórico de la Investigación*, donde se detalla las diferentes posturas teóricas de autores, científicos e ingenieros que aportan a la SEGURIDAD INFORMÁTICA en infraestructuras tecnológicas; se conceptualizan términos, definiciones, enunciados y posturas que ayuden a plantear perspectivas y aportes propias de la investigación y permitan resolver el problema objeto de estudio; apegados al marco legal del estado y de educación superior.

Seguidamente se identifica que *Metodología de la Investigación* plasmada en el CAPÍTULO TERCERO, es la que se emplea para desarrollar el presente trabajo de grado, teniendo que identificar los tipos y métodos de utilizados en la investigación, elaboración metodológica y construcción del marco teórico; elegir los medios de recolección de información empírica para su descripción, análisis e interpretación de los resultados obtenidos y llegar a la construcción del informe de investigación.

De los datos e información obtenida en el capítulo anterior, el CAPÍTULO CUARTO aborda el *Análisis e Interpretación de los resultados en relación a la Hipótesis de Investigación*. En este apartado se enuncia la Hipótesis a ser

verificada y su cumplimiento para la presente investigación, a partir de su ubicación y descripción de la información empírica obtenida; posteriormente dicha información será discutida y analizada en relación a la hipótesis en base a modelos cuantitativos (estadísticos), cualitativos (conclusiones) y su respectiva comprobación, finalizando con las conclusiones parciales.

Una vez concluida la investigación respectiva, se plasman los resultados obtenidos a través, de las *Conclusiones y Recomendaciones* que conforman el CAPÍTULO QUINTO; mismas que permitirán conllevar hacia una propuesta para la Universidad Técnica de Babahoyo, producto de la adecuada investigación desarrollada.

Finalmente se concluye con el CAPÍTULO SEXTO, en el desarrollo de la *Propuesta Alternativa,* la que cuenta con el tratamiento de los siguientes puntos: Título de la Propuesta, Justificación basada en las conclusiones de la investigación, Fundamentación ampliada y pertinente al objeto de estudio y su problemática a resolver, Objetivos que deben desarrollarse, Importancia, Ubicación sectorial y Física, Factibilidad y Desarrollo de la propuesta, Impacto, Evaluación.

CAPÍTULO I

MARCO CONTEXTUAL DE LA INVESTIGACIÓN

1.1. Ubicación y Contextualización de la Problemática.

Al enhebrar sobre Seguridad Informática en empresas e instituciones establecidas aquí en nuestro país, es hacer historia sobre los esfuerzos hace más o menos treinta años atrás; donde se comenzó a investigar y ofrecer servicios informáticos de la época para proteger el recurso más vital hasta hoy por hoy, que es la Información.

A medida en que las personas, empresas e instituciones se apegan al ritmo de la tecnología ya sea para almacenar, difundir y gestionar datos, información, recursos y servicios; invirtiendo tiempo, dinero y esfuerzos existe la amenaza de que la misma sea interceptada[2] y manipulada por personas ajenas a la organización con la finalidad de perjudicar y tomar ventaja.

No muy ajena a esta realidad la Universidad Técnica de Babahoyo como una Institución de Educación Superior, que oferta carreras acordes a las necesidades locales, regional y nacional; parte de sus objetivos es emplear métodos y medios tecnológicos que apoyen eficientemente la difusión de oportuna de la información; así mismo, gestionar la correcta información entre docentes y estudiantes con integridad, disponibilidad y fiabilidad de los datos haciendo uso de tecnología innovadora de acceso múltiple y globalizante.

Por tal motivo se considera un especial tratamiento la seguridad en los sistemas informáticos, ya que es muy importante resguardar el volumen de información confidencial que se maneja; las pérdidas por concepto de revelación de información confidencial pueden ser numerosas y a partir de esta consideración, la institución dedicará esfuerzos y recursos a implementar una red segura para atender dichas vulnerabilidades y problemas que se puedan presentar.

[2] *Interceptar.*- Refiérase a detener algo en su camino; interrumpir una vía de comunicación; o apoderarse de algo antes de que llegue a su destino. (RAE, 2012)
Ref: http://definicion.de/intercepcion/#ixzz3YIhQWqk2

La investigación se desarrollará en el perímetro que conforma la Universidad Técnica de Babahoyo, misma que se encuentra situada en el cantón Babahoyo con coordenadas, *"1°48'13.1" Latitud Sur y 79°32'15.0" de Longitud occidental"*[3], dentro de una zona subtropical. Está limitada: Al Norte: los cantones Baba, Puebloviejo y Urdaneta. Al Sur: la provincia del Guayas. Al Este: Montalvo, y la provincia de Bolívar.

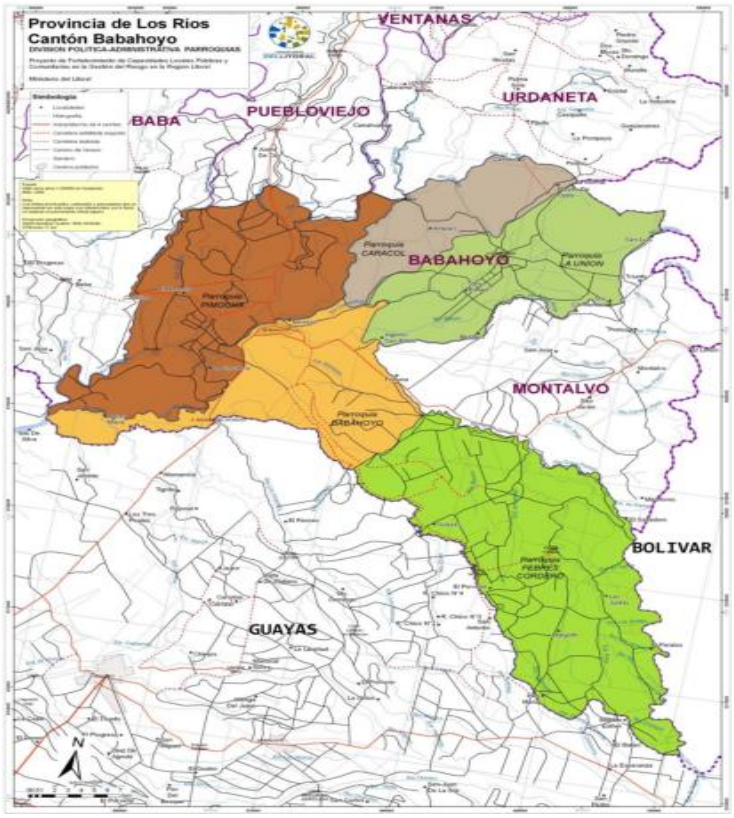


Figura 1. División Política-Administrativa Cantón Babahoyo, Prov. de los Ríos
Fuente: *Plan de Contingencia ante Inundaciones – Cantón Babahoyo* (Gobierno Provincial de los Rios, 2011)

1.2. Situación actual de la problemática

La seguridad informática en redes de computadoras ha pasado de una simple preocupación de unos cuantos encargados a una difícil tarea conjunta con los directivos de la empresa u organización. A cada momento crece el número de empresas que computariza su trabajo de oficina y se van haciendo más dependiente de las nuevas tecnologías.

[3] *GOOGLE MAPS*, https://www.google.com.ec/maps/@-1.8062648,-79.5156956,14z?hl=es-419

A nivel mundial, las empresas tales como las entidades financieras invierten esfuerzos y recursos en implementar y actualizar sus sistemas de seguridad y defensa informática, para ello se establece sólida y firmemente políticas, protocolos, plataformas, servicios, y aplicaciones de seguridad.

> La empresa IBM Co.: "presenta el z13, un sistema informático más potente y seguro de la historia. Se trata del primer sistema capaz de procesar 2.500 millones de transacciones al día para responder a los retos de la nueva economía móvil. Es el primer servidor mainframe con tecnologías analíticas integradas que ofrece información en tiempo real 17 veces más rápido y con menor costo que cualquier otro sistema del mercado. IBM ha diseñado el z13 para un seguimiento en tiempo real y garantizar esta capacidad como característica utilizada para la detección del fraude en el 100 por ciento de transacciones de negocio de cualquier cliente." (IBM Co. Sala de Prensa, 2015)

Cuando se analiza el tema de seguridad informática a nivel nacional, es exhibir el trabajo de más de treinta años de empresas que se han posicionado y han ofertado soluciones en esta área de la informática. Existen también trabajos de investigación realizadas en diferentes Instituciones de Educación Superior que se relacionan con el tema de interés a citar.

> Proyecto de Tesis: "DESARROLLO DEL MANUAL DE SEGURIDADES INFORMÁTICAS DE LA ARMADA DEL ECUADOR misma que generará una propuesta de un Manual de Seguridades Informáticas basado en los lineamientos generales sobre Seguridad Informática citados en la Norma ISO 17799:2000. Lo que implica que, por ser una Institución militar se necesita de una concientización y planteamiento de políticas que salvaguarden la confidencialidad de sus activos informáticos, verificando así la consistencia de los sistemas de información y de control, la eficiencia y efectividad de los programas y operaciones, y el cumplimiento de los reglamentos y normas

> prescriptas. Como resultado se realiza un análisis de la situación actual de su entorno informático permitiendo determinar el nivel de riesgos que enfrentan sus activos y a que factores se encuentran expuestos, para así generar políticas enmarcadas dentro de las normas Institucionales y principalmente tratando de conseguir la confidencialidad, integridad, disponibilidad, autenticidad y el no-repudio de sus datos." (LLERENA FUENMAYOR, 2006)

Al indagar localmente proyectos que se apeguen a la temática de estudio para la Universidad Técnica de Babahoyo, se confirma que no existen proyectos desarrollados que cumplan con ésta especialidad o área de investigación; así como también, no hay proyectos que se hayan implementado en el perímetro de acción de la propuesta a desarrollar.

Existe una gran variedad de estándares de protocolos que implementan en alguna medida seguridad en redes, también se cuenta con numerosas herramientas y aplicaciones para estos fines. Diseñar una intranet segura solo puede ser posible a través de un análisis detallado entre los distintos protocolos, herramientas y aplicaciones, además del funcionamiento de los principales servicios y sus vulnerabilidades.

El principal problema encontrado al interior de la UTB (Universidad Técnica de Babahoyo) y su infraestructura informática es precisamente la falta de estándares, políticas y organización en los centros de datos de sus diferentes unidades, laboratorios, equipos de cómputo de las oficinas administrativas. Se observó defectuosas instalaciones eléctricas y medios de transmisión deficientes. Fallas en los equipos de telecomunicación, antenas y repetidores. Carencia de configuración en sistemas de seguridad física y lógica de la infraestructura universitaria y sus centros de datos anexos; precisando de tal manera una exigua arquitectura de red SEGURA que sea capaz de cifrar las comunicaciones de manera que la información no pueda ser alterada o accedida por personal no autorizado.

Para la solución de este problema surgen las siguientes interrogantes:

- ¿Qué servicios queremos proteger y cuáles son las principales vulnerabilidades de estos servicios?
- ¿Qué protocolos nos brindan seguridad?
- ¿Qué arquitectura y aplicaciones ayudarán a complementar la seguridad para estos servicios?

1.3. Problemas de investigación

¿Cómo incide una adecuada topología en el diseño de infraestructuras tecnológicas seguras y métodos de protección en la Universidad Técnica de Babahoyo?

(Ver ANEXO I, Árbol de Problemas)

1.3.1. Problemas Derivados

P1: ¿Cómo afecta las vulnerabilidades, amenazas y riesgos tecnológicos expuestos a nivel de usuario en la intranet de la Universidad Técnica de Babahoyo?

P2: ¿Cuáles son las debilidades y amenazas que exhibe la intranet universitaria en el tráfico de paquetes al usar técnicas de monitoreo de red?

P3: ¿De qué manera una metodología en seguridad informática en el diseño de una infraestructura tecnológica fortalece la integridad de la intranet de la Universidad Técnica de Babahoyo?

1.4. Delimitación del problema

CAMPO: Ciencias de la Ingeniería

ÁREA: Redes y Telecomunicaciones.

ASPECTO: Seguridad Informática

SECTOR: Universidad Técnica de Babahoyo, ubicada en el cantón Babahoyo provincia de Los Ríos. Tomando como

referentes al personal académico, administrativo y autoridades, en el año 2015.

TEMA: **"SEGURIDAD INFORMÁTICA Y MÉTODOS DE PROTECCIÓN EN INFRAESTRUCTURAS TECNOLÓGICAS Y SU INCIDENCIA EN LA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO, AÑO 2015".**

PROBLEMA: ¿Cómo incide una adecuada topología en el diseño de infraestructuras tecnológicas seguras y métodos de protección en la Universidad Técnica de Babahoyo?

1.5. Justificación

Con la masificación de los servicios telemáticos y el auge del Internet ha hecho que los ordenadores y las redes se conviertan en elementos esenciales de desarrollo. Las empresas e instituciones buscan tecnologías con mayor calidad de prestación, seguridad y robustez incrementando la integridad de sus infraestructuras, la protección y confidencialidad de sus datos.

No muy apartado a esta realidad viven actualmente las instituciones de educación superior y específicamente la Universidad Técnica de Babahoyo (UTB), la cual cuenta con una red de alta velocidad integrada a la red de universidades; que al compartir información y recursos entre instituciones, docentes, estudiantes y otros usuarios al sistema, necesitan que su infraestructura sea lo más robusta, transparente y segura posible.

Actualmente la infraestructura de la UTB, no cuenta con una red efectiva segura y protegida contra amenazas y ataques perpetrados al interior como hacia fuera de su red. Es imperioso ejecutar políticas y estándares de seguridad informática en el manejo de equipos, programas e información.

Un 80 % de la institución no cuenta con un adecuado control de acceso a la red dejando enlaces desprotegidos y con acceso libre; existe redundancia de enlaces inalámbricos que se interceptan unos a otros. Los equipos de comunicación se encuentran sobredimensionados y mal configurados que no actúan efectivamente sobre la seguridad y protección que deben brindar. La seguridad física y lógica de la red depende de un solo equipo hardware para el control de puertos.

Ante ésta situación, la siguiente propuesta fundamentada en la seguridad y protección de redes efectuará un cambio sustancial desde la adopción de políticas y normas que regulen las actividades de conectividad, la consolidación de una infraestructura robusta y segura, y la protección y confidencialidad de información.

Para lograr tal propósito se analizará la plataforma Microsoft y Linux como sistemas de soporte, gestión y dominio. Se hará uso de arquitecturas para autenticación de usuarios, basadas en Linux. Se emplearán métodos de cifrado para creación de cuentas y enlaces inalámbricos.

Finalmente para la protección, control y acceso de puertos, aplicaciones y usuarios, se hará uso del firewall en producción, SOPHOS[4]; mismo que actualmente está instalado a una capacidad inferior del 40%, con una propuesta alternativa de configuración.

1.6. Cambios esperados con la investigación

Con la presente investigación, se espera alcanzar los niveles más altos de seguridad y protección de los datos, recursos, conectividad e información que viven los usuarios de la red universitaria; minorando las vulnerabilidades y niveles de riesgo presentes.

[4] *SOPHOS*.- Ofrece seguridad con una compatibilidad amplia de plataformas para proteger todos los servidores de su organización.
Ref: https://www.sophos.com/es-es/products/server-security.aspx

Mejorar el servicio a los usuarios al interior de la intranet universitaria, el mismo que sea constante, rápido, estable y portable desde cualquier punto.

Que se conviva con una política de seguridad informática y se institucionalice la normalización de las tareas de redes y conectividad. El empleo de protocolos de red, aplicaciones e infraestructura segura.

1.7. Objetivos

1.7.1. Objetivo General

Analizar la incidencia de una topología acorde en el diseño de infraestructuras tecnológicas seguras y métodos de protección en la Universidad Técnica de Babahoyo.

1.7.2. Objetivos Específicos

- Identificar las vulnerabilidades, amenazas y niveles de riesgos tecnológicos a nivel de usuario que inciden en la intranet de la Universidad Técnica de Babahoyo.

- Analizar el tráfico de paquetes a través de técnicas de monitoreo de red para la comprobación de las debilidades y amenazas en la intranet universitaria.

- Determinar una metodología en Seguridad Informática favorable en el diseño de una infraestructura tecnológica para fortalecer la integridad de la intranet de la Universidad Técnica de Babahoyo.

CAPÍTULO II

MARCO TEÓRICO

2.1. Fundamentación teórica

La seguridad informática para poder ser estudiada, analizada y empleada en diversos escenarios, se necesita apelar a sus inicios y poder entender cómo ha evolucionado esta temática de estudio.

2.1.1. Reseña Histórica de la Seguridad Informática

Se puede citar que la seguridad de la información tiene sus inicios alrededor de los **500 años a.c.**, con el apogeo del pensamiento filosófico de los griegos y la época romana, donde ya se empleaban instrumentos para cifrar mensajes en cintas de cuero empleando unos cilindros y enviados desde el emperador a sus subordinados para que sean leídos usando solo cilindros del mismo diámetro.

Años más tarde, aproximadamente en el **año de 1970 d.c.,** cuando recién se cristalizaba un nuevo sistema de comunicación que ahora se la conoce como Internet; en tiempos de la guerra fría entre EE.UU. y la UNIÓN SOVIÉTICA, se desarrollaron protocolos de comunicación capaces de transmitir en forma cifrada para no poder ser interceptados y que eran solo de uso militar, conocido como ARPANET. De igual manera sería en esta década que se publicó el primer algoritmo de cifrado público (DES).

Pero con el desarrollo del Internet y su auge crecimiento, sería en el **año de 1980** que se concibió formalmente el concepto de seguridad informática fundamentando sus bases, Jame P. Anderson escribe un documento titulado *Computer Security Threat Monitoring and Surveillance***.** Lo más interesante de este documento es que James Anderson da una definición de los principales agentes de las amenazas informáticas. Las organizaciones que utilizaban redes informáticas empezaron a comprender la necesidad de dotar los sistemas computacionales de medidas de seguridad informática. (INCIBE, 2015)

Sería en **junio de 1985** que en los Estados Unidos de Norteamérica, se propagaría **ELK CLONER,** el Primer Virus para computadores personales, concretamente para los sistemas Apple II. Creado por un estudiante, el virus infectaba el sistema operativo, se copiaba en los discos flexibles y desplegaba uno o dos versos de un poema. El virus no tuvo mucha notoriedad ni provocó grandes preocupaciones, sin embargo, pocos se dieron cuenta de que iniciaría una generación de cyber criminales y, en paralelo una industria de seguridad de la información.

PAKISTANI BRAIN (**1988**): el primer virus que infectó equipos PC de IBM y fue escrito por dos hermanos de Pakistán. Este fue el primer virus que recibió amplia cobertura de los medios, aunque los virus ya se conocían en la ciencia ficción. El Gusano **MORRIS** (**1988**) fue el primer ejemplar de malware auto replicable que afectó a Internet. El 2 de noviembre de 1988 hizo su aparición el primer gusano (gusano informático) que paralizó Internet.

En **enero de 1994** se adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030), modificando el Acta de 1986. Aquí se contempla la regulación de los virus conceptualizándolos aunque no los limita, sino que contempla otras instrucciones que contaminan otros grupos de programas o bases de datos. Se enfoca en su mayor parte a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras involucradas en delitos interestatales. También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada. Pero sólo es aplicable en casos en los que se verifiquen daños cuyo valor supere el mínimo de mil dólares. (PORTILLO, 2012)

La Cumbre Mundial sobre la Sociedad de la Información (CMSI tuvo lugar en Ginebra acogida por el Gobierno de Suiza, del **10 al 12 de diciembre de 2003**. El objetivo de la cumbre era redactar y propiciar una clara declaración de voluntad política, y tomar medidas concretas para preparar los fundamentos de la Sociedad de la Información para todos, que tenga en cuenta los distintos intereses con principal atención al Fomento de la confianza y seguridad en la utilización de las TIC´s. (PORTILLO, 2012)

Código malicioso para Móviles, desde el hallazgo de CABIR en **junio del 2004**, la primera prueba de concepto para Symbian, periódicamente han sido identificados otros códigos maliciosos similares para sistemas móviles.

1ro Noviembre 2006.- DÍA DE LA SEGURIDAD DE LA INFORMACIÓN. El Día Internacional de Seguridad de la Información (DISI) es uno de los más importantes eventos sobre Seguridad Informática y Sociedad de la Información que se celebran en áreas de la computación e información. (PORTILLO, 2012)

2.1.2. Bases Metodológicas de Seguridad Informática

La seguridad informática como otra área de estudio en el desarrollo de sistemas ha ido perfeccionando, siendo necesario crear nuevas tecnologías para la protección de datos con la misma frecuencia que avanza la tecnología es necesario mejorar los sistemas de protección. Para lograr tal efecto es necesario consolidar bases sólidas que guíen a la ejecución de esta actividad importante. Dichas bases son las metodologías que se utilice para realizar las tareas de seguridad informática y protección de la información, siendo las directrices que fundamenten cada una de las acciones a seguir.

2.1.2.1. Defensa En Profundidad

Considerando que la seguridad informática es una actividad innovadora y evolutiva; existen varias metodologías difundidas a nivel mundial y que promueven a la metodología de **DEFENSA EN PROFUNDIDAD,** para la mayoría de conocidos como uno de los mejores métodos de seguridad informática a aplicar. Esta metodología consiste en apuntar varias medidas de seguridad con el objetivo de proteger un mismo activo. (PORTANTIER, 2013)

Es una técnica que utiliza varias capas de análisis, en que cada una provee un nivel de protección adicional a las demás capas, ejecutando de adentro hacia afuera.

Figura 2. Enfoque en capas para mejorar los controles de seguridad.
Fuente: (PORTANTIER, 2013)

En principio esta metodología se basaba como estrategia militar sin que avance el enemigo, más que proteger. La metodología se sustenta en los paradigmas de proteger, detectar y reaccionar. Esto significa que a más de incorporar mecanismos de protección, se debe estar preparado para recibir ataques e implementar métodos de detección y procedimientos de recuperación y reacción.

2.1.2.2. El Principio KISS

El principio KISS recomienda la implementación de partes sencillas, comprensibles y con errores fáciles de detectar y corregir, evitando las complicaciones innecesarias. El término viene del acrónimo *"Keep It Simple, Stupid",* cuya mejor traducción sería *Mantenlo Simple y Seguro.* La idea detrás de esto es que los sistemas más sencillos y bien implementados tienen más aceptación que sistemas complejos. Siendo más fáciles de administrar y mantener como factor importante para la seguridad, que en muchas ocasiones tienden a caer en una excesiva complejidad, siendo inentendibles y difíciles de sostener.

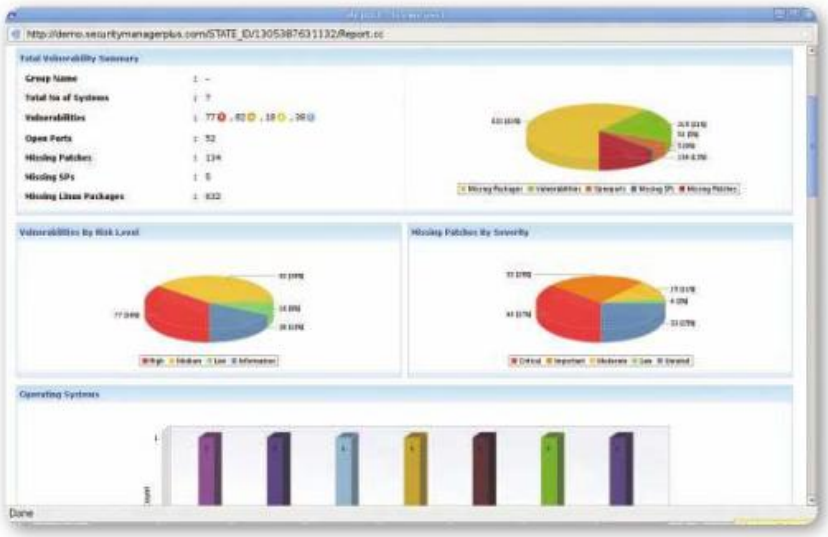


Figura 3. Herramientas que presentan los estados de seguridad para enfocarse en los puntos de mayor atención.
Fuente: (PORTANTIER, 2013)

Esta técnica está relacionado con el **principio de parsimonia,** según el cual indica: *"cuando dos teorías en igualdad de condiciones tienen la misma consecuencia, la más simple tiene la probabilidad de ser más la correcta que la compleja".* (**Navaja de Ockham**).

Este precepto es muy útil cuando se tienen que elegir entre varios controles de seguridad que sean iguales o muy semejantes en cuanto a los beneficios que pueda aportar, pero diferentes en cuanto a diseño y complejidad. Se debe tener presente esto y no caer en lo

que sea más fácil y perder funcionalidad, consistencia y no llegar al objetivo; por lo tanto es necesario e imperioso, hacer un análisis exhaustivo de soluciones posibles y que satisfaga verdaderamente las necesidades.

2.1.2.3. Desde Arriba hacia Abajo

Al igual cuando se construye un edificio es necesario comenzar por los planos del diseño, seguido de las bases y luego con el resto del edificio con cada puerta y ventana en su lugar, en consecuencia los planos representan la parte importante y objetiva de la construcción; así mismo, los objetivos de una organización son los planos de un edificio y deben estar bien definidos desde el principio para que todo el programa de seguridad esté desarrollado en base a ellos.

Muchas veces las empresas comienzan por instalar las infraestructuras tecnológicas y luego considerar las seguridades, realizando diversos parches, bloqueos, etc. Más bien lo correcto es comenzar con una idea más amplia y poco específica de lo que se quiere obtener, posteriormente trabajar en los detalles de las tareas que se va a realizar para alcanzar los objetivos fijados.

El siguiente paso es desarrollar e implementar las guías, estándares y procedimientos que van a soportar las ideas generales escritas inicialmente. A medida que se avanza con el proceso se es más específico, pero siempre con los objetivos en mente hasta llegar a definir cada una de las configuraciones necesarias.

Figura 4. Fases Top-Down para la implementación de técnicas a cumplir en programas de seguridad.
Fuente: (PORTANTIER, 2013)

Es importante trabajar con esta metodología desde un inicio, ya que no permite realizar cambios drásticos ni rediseñar grandes partes de los planes; al principio parecerá que este enfoque conlleva mayor tiempo y trabajo.

Un programa de seguridad debe estar soportado y dirigido por la alta gerencia, para luego ser distribuido hacia abajo en el árbol jerárquico, hasta alcanzar toda la organización, a éste enfoque se lo conoce como **desde arriba hacia abajo** logrando que toda la organización se contagie con los conceptos propuestos y se logre un trabajo cooperativo y armonioso.

"Para efectos del presente trabajo de investigación, resulta ser más apropiada emplear la metodología DEFENSA EN PROFUNDIDAD, ya que consideramos una infraestructura tecnológica ya conformada y en ejecución; pero con las limitaciones, falencias y errores identificados y que pueden ser intervenidos a manera de capas, partiendo desde las más críticas hasta la de menor impacto, comprometiendo al personal adecuado, las herramientas tecnológicas disponibles y las diferentes operaciones que inciden mayormente a la integridad de la seguridad de la red."

2.1.3. Protocolos SSL.

Para establecer una comunicación SSL es necesario que previamente el cliente y el servidor realicen un proceso de reconocimiento mutuo y

de petición de conexión que, al igual que en otros tipos de comunicaciones, recibe el nombre de apretón de manos o handshake, que en este caso está controlado por el Protocolo SSL Handshake, que se encarga de establecer, mantener y finalizar las conexiones SSL. (OPPLIGER, 2014)

El protocolo comienza con el saludo del cliente al servidor, junto con este saludo inicial el cliente envía al servidor información de la versión de SSL que tiene implementada, de los algoritmos de encriptación que soporta, las longitudes de clave máximas que admite para cada uno de ellos y las funciones hash que puede utilizarse, eligiendo las más fuertes. También se le solicita al servidor el envío de su Certificado Digital X.509 v3, con objeto de verificar el cliente la identidad del mismo y recoger su clave pública. A veces el servidor solicita al cliente su Certificado Digital, en el mensaje llamado CertificateRequest. Esto sólo suele ocurrir en SSL cuando los datos a transferir sean especialmente sensibles y precisen la previa autenticación del cliente. (OPPLIGER, 2014)

Si alguna de estas validaciones falla, el navegador del cliente rechazará la comunicación, dándola por finalizada e informando al usuario el motivo del rechazo. Para empezar a transmitir datos cifrados es necesario que cliente y servidor se pongan de acuerdo respecto a la forma común de encapsular los datos que se van a intercambiar, es decir, qué formato de datos se va a usar en la transmisión cifrada. Esto se realiza mediante el protocolo SSL Record (Protocolo de Registro SSL). (OPPLIGER, 2014)

Por último, cuando la transferencia de mensajes ha finalizado y se desea cerrar la comunicación segura, la aplicación cliente (el navegador Web) lanza una ventana de aviso de que se va a cerrar la comunicación SSL, y si es aceptada por el usuario, se sale de la

misma y se regresa a una comunicación normal, finalizando el proceso. SSL Handshake posee además otro subprotocolo específico, denominado Alerta, que se encarga de avisar de los problemas que ocurren durante la conexión, y que pueden llevar a la finalización brusca de la sesión. (OPPLIGER, 2014)

2.1.4. Ventajas de SSL

- *"Es una tecnología rápida, fácil de implementar, barata y cómoda para el usuario, que no tiene que conocer cómo funciona, tan sólo usarla.*
- *Proporciona un canal de comunicaciones seguro entre los servidores Web y los clientes, pero su uso no se limita a este tipo de aplicaciones.*
- *Al encontrarse entre los niveles de transporte y de aplicación, potencialmente SSL puede servir para asegurar otros servicios, como FTP, correo, telnet, etc.*
- *El usuario no necesita realizar ninguna acción especial para invocar el protocolo SSL, basta con seguir un enlace o abrir una página cuya dirección empieza por https://. El navegador se encarga del resto."*

2.1.5. Manejo básico de SSH

El protocolo SSH cuenta con dos versiones, pero se recomienda generalmente el uso de OpenSSH, por su mayor seguridad; es una implementación usada en sistemas Linux como cliente y servidor para el uso de sesiones remotas seguras que ofrecen autenticación, confidencialidad e integridad. (OPPLIGER, 2014)

Este protocolo requiere que los servidores tengan "llaves", las cuales son usadas por los clientes cada vez que se conectan a un servidor para verificar que no fue suplantado. Una llave es un número codificado y cifrado en un archivo. Para la encriptación de llaves, OpenSSH ofrece los algoritmos RSA y DSA. (OPPLIGER, 2014)

2.1.6. IPSec

IPSec es un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública, algoritmos de cifrado, algoritmos de hash y certificados digitales. (TRUJILLO M., 2006)

El protocolo IPSec ha sido diseñado de manera modular, de forma que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Está compuesto por dos protocolos de seguridad: IP Authentication Header (AH) e IP Encapsulating Security Payload (ESP) que proporcionan mecanismos de seguridad para proteger el tráfico IP. Un protocolo de gestión de claves Internet Key Exchange (IKE) que permite a dos nodos negociar las claves y los parámetros necesarios para establecer una conexión. (TRUJILLO M., 2006)

2.1.7. El Protocolo AH

El protocolo AH garantiza la integridad y autenticación de los datagramas IP. Sin embargo no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros. AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar y los datos transportados.

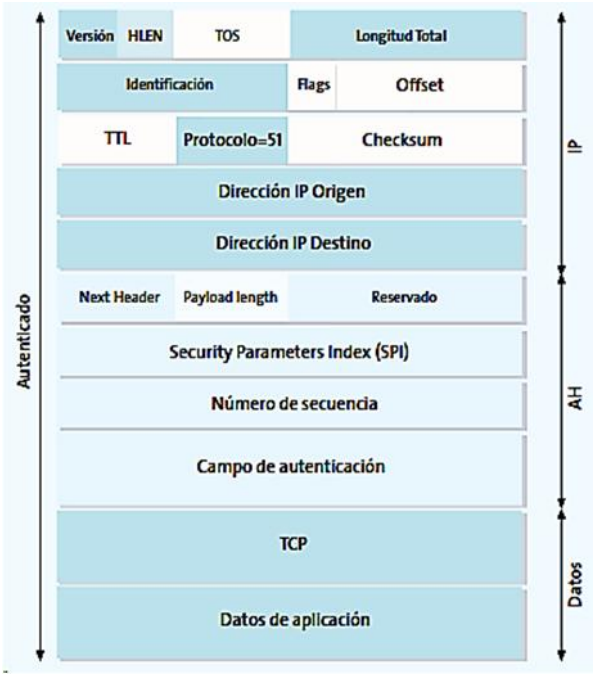
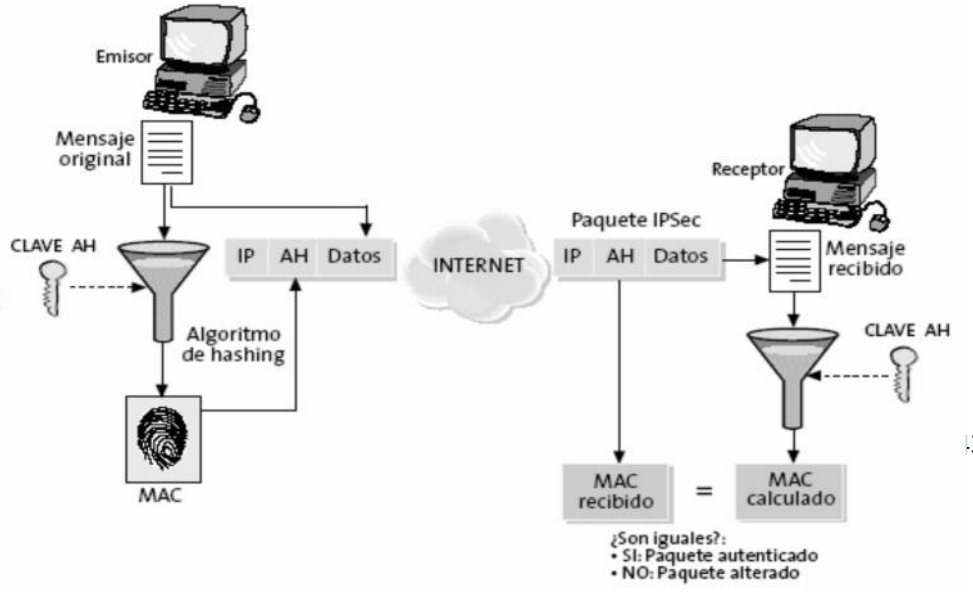


Figura 5. Estructura de un Datagrama AH.
Fuente: (TRUJILLO M., 2006)

El funcionamiento de AH se basa en aplicar una función hash a la combinación de unos datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que denominamos extracto. Dicho extracto tiene la propiedad de ser como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave. (TRUJILLO M., 2006)

"En la figura 6 se muestra el modo en que funciona el protocolo AH. El emisor calcula un extracto del mensaje original, el cual se copia en uno de los campos de la cabecera AH. El paquete se envía a través de la red, repitiéndose en el extremo receptor el cálculo del extracto y comparándolo con el recibido en el paquete, si coinciden es que no ha s i d o m



odificado”

Figura 6. Funcionamiento del Protocolo AH.
Fuente: (TRUJILLO M., 2006)

2.1.8. IKE: El Protocolo de Control

Un concepto esencial en IPSec es el de asociación de seguridad (SA): es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada sentido de la comunicación. El IETF ha definido el protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de las SAs correspondientes. (TRUJILLO M., 2006)

En los estándares IPSec está previsto el uso de un método de autenticación que se basa en utilizar certificados digitales X.509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública.

“*La utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPSec, la PKI (Infraestructura de Clave Pública).”*

2.1.9. Integración de IPSec con una PKI

El uso de una PKI aparece en IPSec como respuesta a la necesidad de un procedimiento para autenticar de forma confiable a un conjunto de nodos que desean comunicarse mediante IPSec, siendo dicho conjunto de nodos muy numeroso. (TRUJILLO M., 2006)

Bajo el nombre de PKI (Infraestructura de Clave Pública) se engloban todos los elementos y procedimientos administrativos que permiten emitir, revocar y, eventualmente, renovar los certificados digitales para una comunidad de usuarios. En el caso de IPSec los sujetos de los certificados son los nodos IPSec, mientras que la función de los certificados es proporcionar un medio confiable para autenticar la identidad de los dispositivos IPSec. (TRUJILLO M., 2006)

Cada uno de los dispositivos IPSec dispondrá de un certificado digital que contendrá su clave pública y la información suficiente para identificar de forma unívoca al dispositivo (tal como su nombre DNS, su dirección IP o su número de serie). Esta asociación entre clave pública e identidad está avalada por la firma de la Autoridad de Certificación (en adelante CA) integrada en la PKI, que da validez al certificado. Se supone que todos los dispositivos IPSec reconocerán como válida la misma CA, para lo cual deberán disponer de una copia del certificado de la propia CA. (TRUJILLO M., 2006)

Los protocolos para la interacción de los dispositivos IPSec con una PKI no están especificados en ninguno de los protocolos de IPSec. Todos los fabricantes utilizan X.509v3 como formato común de los certificados. Sin embargo, el protocolo de comunicaciones, mediante el cual los dispositivos IPSec dialogan con la PKI, no está totalmente estandarizado. En general los nodos IPSec necesitan realizar ciertas operaciones básicas con una PKI: acceder al certificado de la CA, solicitar y descargar un certificado, así como comprobar la validez de un certificado recibido. (TRUJILLO M., 2006)

“En la figura 7 se representan los flujos de comunicación entre una PKI y un nodo IPSec. Inicialmente, cada uno de los nodos genera un par de claves (pública y privada) y envía una petición de certificado a

la CA, en la que incluye información de su identidad y su clave pública. Al mismo tiempo, el nodo descarga el certificado raíz de la CA; a continuación, la CA genera un certificado para el dispositivo IPSec y éste lo recibe. A partir de ese momento el nodo IPSec podrá usar su certificado en una negociación IKE para autenticarse frente a otros dispositivos. Periódicamente los dispositivos IPSec accederán al directorio de la PKI para actualizar la CRL. "

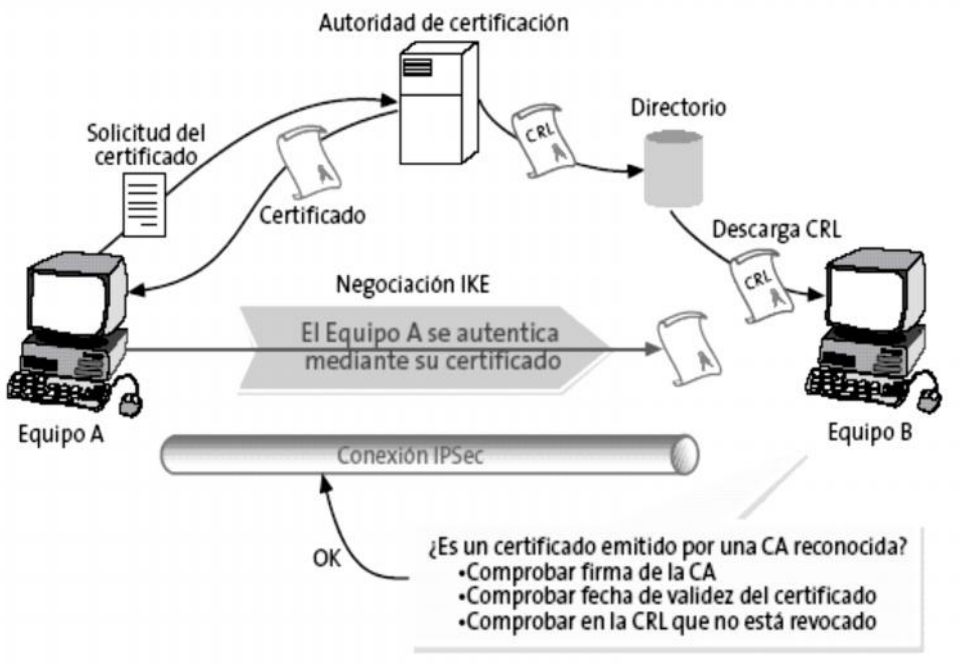


Figura 7. Integración de una PKI con IPSec.
Fuente: (TRUJILLO M., 2006)

2.2. Fundamentación Legal

El presente trabajo de investigación está sustentado por los marcos legales de la Ley orgánica de Telecomunicaciones y de la Ley Orgánica de Educación Superior, mismos a citar en los siguientes párrafos referentes al tema de investigación:

LEY ORGÁNICA DE TELECOMUNICACIONES

Artículo 2.- Ámbito:

La presente Ley se aplicará a todas las actividades de establecimiento, instalación y explotación de redes, uso y explotación del espectro radioeléctrico, servicios de telecomunicaciones y a todas aquellas personas naturales o jurídicas que realicen tales actividades a fin de garantizar el cumplimiento de los derechos y deberes de los prestadores de servicios y usuarios. (ARCOTEL, 2015)

Artículo 3.- Objetivos:

7. Establecer el marco legal para la provisión de los servicios públicos de telecomunicaciones como responsabilidad del Estado Central, con sujeción a los principios constitucionalmente establecidos y a los señalados en la presente Ley y normativa aplicable, así como establecer los mecanismos de delegación de los sectores estratégicos de telecomunicaciones y espectro radioeléctrico. (ARCOTEL, 2015)

17. Establecer los mecanismos de coordinación con organismos y entidades del Estado para atender temas relacionados con el ámbito de las telecomunicaciones en cuanto a seguridad del Estado, emergencias y entrega de información para investigaciones judiciales, dentro del debido proceso. (ARCOTEL, 2015)

Artículo 61.- Competencias del Órgano Rector.- Corresponde a la Institución de Educación Superior:

9. Formular las políticas y planes para la creación, regulación y supervisión de la central de datos de la institución, intercambio de información por medios electrónicos, seguridad en materia de información e informática, así como evaluación de su ejecución. (ARCOTEL, 2015)

Artículo. 76.- Medidas técnicas de seguridad e invulnerabilidad.

Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas

para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente. (ARCOTEL, 2015)

Artículo 78.- Derecho a la intimidad. Para la plena vigencia del derecho a la intimidad, establecido en el artículo 66, numeral 20 de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal. (ARCOTEL, 2015)

1. La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley.

2. La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos.

3. La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.

4. La garantía de que la información suministrada por los clientes, abonados o usuarios no será utilizada para fines comerciales ni de publicidad, ni para cualquier otro fin, salvo que se cuente con el consentimiento previo y autorización expresa de cada cliente, abonado o usuario.

Artículo 80.- Procedimientos de revelación.

Las y los prestadores de servicios implementarán procedimientos internos para atender las solicitudes de acceso a los datos personales de sus abonados, clientes o usuarios por parte de las autoridades legalmente autorizadas. (ARCOTEL, 2015)

LEY ORGÁNICA DE EDUCACIÓN SUPERIOR

CREACIÓN DE UNIVERSIDADES Y ESCUELAS POLITÉCNICAS

Artículo. 109.- Requisitos para la creación de una universidad o escuela politécnica.

Quien promueva la creación de una universidad o escuela politécnica deberá presentar al Consejo de Educación Superior una propuesta técnico–académica, que contenga los siguientes requisitos:
10. Infraestructuras tecnológicas propias y laboratorios especializados. (SENESCYT, 2012)

2.3. Fundamentación Conceptual.

"El crecimiento de Internet unido al auge de la informática ha traído consigo un aumento considerable de piratas informáticos y un incremento extraordinario de los incidentes de seguridad. En la actualidad mantener un sistema seguro resulta una tarea difícil para cualquier profesional de la informática".

2.3.1. Seguridad Informática

La seguridad es un proceso continuo que reduce los riesgos y garantiza que los curiosos no puedan leer, o peor aún, modificar mensajes dirigidos a otros destinatarios. Los problemas de seguridad de las redes pueden dividirse en términos generales en estas áreas interrelacionadas: confidencialidad, autenticación, no repudio y control de integridad. La *confidencialidad* se traduce en mantener la información fuera del alcance de usuarios no autorizados. La *validación de identificación* se encarga de determinar con quien se está hablando antes de revelar información confidencial. El *no repudio* se encarga de garantizar la identidad del usuario de manera que no pueda negar la participación en una transacción en que los mensajes sólo sean modificados por él. (TANENBAUM, 2003)

Otra definiciones de seguridad informática según (INFOSEC Glossary, 2000).- *"Seguridad Informática son las medidas y controles que*

aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican".

En la redes de cómputo se protege todo lo relativo al hardware, el software y los datos. El hardware formado por los elementos físicos del sistema. El software compuesto por los programas lógicos, sistema operativo y aplicaciones. Y los datos que representan la información manejada por el software.

2.3.2. Objetivos de la seguridad informática

Los principales objetivos de la seguridad informática son:

- *Confidencialidad*: consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitido por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información; es decir, que si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación.

- *Disponibilidad:* se define como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento.

- *Integridad:* se dice que es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente.

- *No repudio*: este objetivo garantiza la participación de las partes en una comunicación. En toda comunicación, existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio:

No repudio en origen.- Garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío.

No repudio en destino.- El receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo. (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

Figura 8. Esquema de los objetivos de la seguridad informática.
Fuente: (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

2.3.3. Clasificación de seguridad

Se pueden hacer diversas clasificaciones de la seguridad informática en función de distintos criterios. Según el activo a proteger; es decir, todos los recursos del sistema de información necesarios, distinguiendo entre seguridad física y lógica; en dependencia del momento preciso de actuación, entre seguridad pasiva y activa, según se actúe antes de producirse el percance, minimizando los efectos ocasionados por el mismo. (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

2.3.3.1. Seguridad física y lógica

Se distingue los distintos tipos de seguridad en función del recurso a proteger.

Seguridad física.- La seguridad física es aquella que trata de proteger el hardware (los equipos informáticos, el cableado...) de los posibles desastres naturales (terremotos, tifones...), de incendios, inundaciones, sobrecargas eléctricas, de robos y un sinfín de amenazas más. (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

A continuación se enumera las principales amenazas y los mecanismos para salvaguardar las mismas:

Amenazas	Mecanismos de defensa
Incendios	• El mobiliario de los centros de datos debe ser ignífugo. • Evitar la localización del centro de procesamiento de datos cerca de zonas donde se manejen o almacenen sustancias inflamables o explosivos • Deben existir sistemas anti-incendios, detectores de humo, rociadores de gas, extintores para sofocar el incendio en el menor tiempo posible y así evitar que se propague ocasionado numerosas pérdidas materiales
Inundaciones	• Evitar la ubicación de los centros de datos en las plantas bajas de los edificios para protegerse de la entrada de aguas superficiales. • Impermeabilizar las paredes y techos del CPD. Sellar las puertas para evitar la entrada de agua proveniente de las plantas superiores.
Robos	Proteger los centros de datos mediante puertas con medidas biométricas, cámaras de seguridad; con todas estas medidas pretendemos evitar la entrada de personal no autorizado.
Señales electromagnéticas	• Evitar la ubicación de los centros de datos próximos a lugares con gran radiación de señales electromagnéticas, pues pueden interferir en el correcto funcionamiento de los equipos informáticos y del cableado de red. • En caso de no poder evitar la ubicación en zonas con grandes emisiones de este tipo de señales deberemos proteger el centro frente de dichas emisiones mediante el uso de filtros o de cableado especial, o si es posible, utilizar fibra óptica, que no es sensible a este tipo de interferencias.
Apagones	Para evitar los apagones colocaremos Sistemas de Alimentación Ininterrumpida, UPS, que proporcionan corriente eléctrica durante un periodo de tiempo suficiente
Sobrecargas Eléctricas	Además de proporcionar alimentación, los UPS profesionales incorporan filtros para evitar picos de tensión, es decir, estabilizan la señal eléctrica
Desastres Naturales	Estando en continuo contacto con el Instituto Geográfico Nacional y la Agencia Estatal de Meteorología, organismos que informan sobre los movimientos sísmicos y meteorológicos del país.

Tabla 1. Amenazas y mecanismos de defensa en seguridad Física.
Fuente: (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

Seguridad lógica.- La seguridad lógica complementa a la seguridad física, protegiendo el software de los equipos informáticas, es decir, las aplicaciones y los datos de usuario, de rabos, de pérdida de datos, entrada de virus informáticos, modificaciones no autorizadas de los datos, ataques desde la red, etc. A continuación se enumera las principales amenazas y mecanismos para salvaguardarse de las mismas: (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

Amenazas	Mecanismos de defensa
Robos	• Cifrar la información almacenada en los soportes para que en caso de robo no sea legible. • Utilizar contraseñas para evitar el acceso a lo información. • Sistemas biométricos (uso de huella dactilar, tarjetas identificadoras, caligrafío).
Pérdida de información	• Realizar copias de seguridad para poder restaurar la información perdida. • Uso de sistemas tolerantes a fallos, elección del sistema de ficheros del sistema operativo adecuado. • Uso de conjunto de discos redundantes, protege contra la pérdida de datos y proporciona la recuperación de los datos en tiempo real.
Pérdida de integridad en la información	• Uso de programas de chequeo del equipo, SiSoft Sandra 2000, TuneUp, etc. • Mediante la firma digital en el envío de información a través de mensajes enviados por la red. • Uso de la instrucción del sistema operativo Windows, sfc (system file checker).
Entrada de virus	Uso de antivirus, que evite que se infecten los equipos con programas malintencionados.
Ataques desde la red	• Firewall, autorizando y auditando las conexiones permitidas. • Programas de monitorización • Servidores Proxys, autorizando y auditando las conexiones permitidas.
Modificaciones no autorizadas	• Uso de contraseñas que no permitan el acceso a la información. • Uso de lista s de control de acceso. • Cifrar documentos.

Tabla 2. Amenazas y mecanismos de defensa en seguridad Lógica.
Fuente: (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

2.3.3.2. Seguridad activa y pasiva

Aquí el criterio de clasificación es el momento en el que se ponen en marcha las medidas oportunas de prevención.

Seguridad activa.- La seguridad activa la podemos definir como el conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos. A continuación, se enumera las principales técnicas de seguridad activa: (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

Técnica	¿Qué previene?
Uso de contraseñas	Previene el acceso a recursos por parte de personas no autorizadas.
Listas de control de acceso	Previene el acceso a los Ficheros por parte de personal no autorizado.
Encriptación	Evita que personas sin autorización puedan interpretar la información.
Uso de software de seguridad Informática	Previene de virus informáticos y de entradas indeseadas al sistema informático.
Firmas y certificados digitales	Permite comprobar la procedencia, autenticidad e integridad de los mensajes
Sistemas de Ficheros con tolerancia a fallos	Previene fallos de integridad en caso de apagones de sincronización o comunicación
Cuotas de disco	Previene que ciertos usuarios hagan un uso indebido de la capacidad de disco

Tabla 3. Técnicas de seguridad activa.
Fuente: (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

Seguridad pasiva.- La seguridad pasiva complementa a la seguridad activa y se encarga de minimizar los efectos que haya ocasionado algún percance. A continuación, se enumera las principales técnicas de seguridad pasiva: (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

Técnica	¿Qué previene?
Conjunto de discos redundantes	Podemos restaurar información que no es válida ni consistente.
SAI o UPS	Una vez que la corriente se pierde las baterías del Sal o UPS se ponen en funcionamiento proporcionando la corriente necesaria para el correcto funcionamiento.
Realización de copias de Seguridad	A partir de las copias realizadas, podemos recuperar información en caso de pérdida de datos.

Tabla 4. Técnicas de seguridad pasiva.
Fuente: (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

Elementos que atentan contra la Seguridad Informática

Entre los elementos que atentan contra la seguridad de las redes de cómputo encontramos: programas malignos (amenazas lógicas), catástrofes naturales, acciones humanas, entre otras. Un informe de seguridad de Cisco revela que el 77 por ciento de los trabajadores desconoce las principales amenazas de seguridad, poniendo en peligro los datos de sus compañías. El empleado resulta ser el eslabón más débil de la cadena por falta de conciencia y desconocimiento. Las políticas de seguridad desplegadas, tampoco tienen el rigor necesario. (CASAS, 2014)

2.3.4. Amenazas Lógicas

Las amenazas lógicas son todos los programas que de una forma u otra pueden dañar el sistema informático. Se les conoce con el nombre de malware, bugs o agujeros. Son errores de programación software que pueden comprometer el sistema operativo. A estos errores se les conoce como bugs y los programas que aprovechan de estas vulnerabilidades, exploits; estos últimos son muy peligrosos ya que no se necesita de mucho conocimiento para utilizarlos y comprometer un servidor. (LUDWIN, 2006)

Las herramientas de seguridad también se incluyen dentro del grupo de amenazas lógicas ya que son un arma de doble filo. De la misma manera en que un administrador las usa para detectar y corregir los errores del sistema, un intruso las usa para detectar vulnerabilidades y atacar. Está demostrado que la seguridad de un sistema no puede basarse en el desconocimiento de los problemas por parte de los atacantes, esta política se denomina seguridad mediante oscuridad (Security through obscurity).

Las *BOMBAS LÓGICAS* son partes del código de algún programa que permanecen pasivas hasta que son activadas en determinado momento y ejecutan su tarea destructiva, los detonadores suelen ser presencia o ausencia de un fichero específico, una fecha concreta, una combinación de teclas, y otras variantes.

Los *GUSANOS* son otro de los códigos maliciosos, los cuales son capaces de propagarse y ejecutarse a sí mismos a través de redes aprovechando bugs de los sistemas a los que se conecta y en ocasiones portando virus.

A estos se le unen los *CABALLOS DE TROYA*, los cuales son instrucciones escondidas en programas de manera que este parezca realizar las tareas que el usuario espera de él, pero en realidad ejecuta funciones ocultas que atentan contra la seguridad. Los caballos de Troya ocultan su intención real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente. (VILLALON HUERTA, 2002)

Los *VIRUS* son también secuencias de códigos, estas se insertan en un fichero ejecutable denominado huésped, de manera que cuando se

active el fichero el virus también lo hará, insertándose a sí mismo en otros programas para asegurar su procreación y diseminación.

Las *TÉCNICAS SALAMI* son el robo automatizado de pequeñas cantidades de dinero, lo que la hace difícil de detectar. Este tipo de técnicas se usa normalmente en sistemas bancarios que sustraen céntimos, de miles de cuentas, lo que da en total, miles de dólares. Esta técnica puede ser usada también en sistemas de contabilidad de empresas grandes y medianas asociadas a las nóminas de los trabajadores o a sus movimientos económicos.

2.3.5. Amenazas Naturales

Otra de las amenazas de nuestros sistemas informáticos son precisamente las catástrofes como: terremotos, maremotos, inundaciones por crecidas de ríos cercanos, penetraciones del mar o desbordes de presa, ciclones, descargas eléctricas, incendios y otras.

Las medidas de protección contra estas catástrofes dependen de la probabilidad de ocurrencia, por lo general las empresas no invierten en este tipo de eventos a menos que su ocurrencia sea inminente. En los nodos de comunicaciones se deben tener equipos de protección contra incendios. Aterramiento físico para asegurar el equipamiento de las descargas eléctricas. Copias de seguridad de todo el sistema en medios ópticos y magnéticos que deben estar guardados en otro local donde el peligro a este tipo de eventos sea mínimo.

Todos estos aspectos deben estar incluidos en el plan de contingencia, que son las acciones a tomar en caso de un evento de este tipo.

2.3.6. Ataques Genéricos

Las vulnerabilidades pretenden describir las debilidades y los métodos más comunes que se usan para llevar a cabo ataques a la seguridad. Estos pueden estar motivados por diversos objetivos, incluyendo fraude, extorsión, robo de información confidencial, venganza, acceso no autorizado a un sistema o anulación de un servicio.

2.3.6.1. Ingeniería Social

La ingeniería social es una manipulación verbal que en la mayoría de los casos se lleva a cabo bajo identidad encubierta, ya sea por teléfono o a través de terceras personas y su alcance depende de la creatividad del atacante y de la ingenuidad de la víctima. Para ello el intruso se hacen pasar por el administrador o alguien importante, falseando la dirección de origen de un correo electrónico o mediante el teléfono para que el usuario le facilite su clave o le revele algún tipo de información que pueda necesitar. (MCLURE, 2010)

2.3.6.2. Shoulder Surfing

Es un ataque relacionado con la ingenuidad de los usuarios y consiste en espiarlos físicamente. Esta técnica es muy eficiente con aquellos que escriben sus contraseñas en una pegatina que luego ponen en el monitor, o la escriben en una agenda que olvidan en cualquier lugar. Esta irresponsabilidad es comparable con tener en casa un sistema de seguridad excepcional y al salir dejar la llave bajo la alfombra. (MCLURE, 2010)

2.3.6.3. Basureo (Trashing)

Descuidar el paradero de nuestros borradores de papel donde escribimos contraseñas, recados del teléfono y todo tipo de información, puede resultar peligroso. Una factura arrojada a la basura, donde se encuentren nombres de empleados, direcciones particulares, números de teléfono, puede convertirse en

información valiosa para ser usada en técnicas de ingeniería social. Por estas mismas razones las cintas magnéticas o discos duros no deben ser tirados sin antes destruirlos. También se recomienda cortar o incinerar todos los papeles que no necesiten ser almacenados. (MCLURE, 2010)

2.3.6.4. Huella de Identificación (Footprinting)

El intruso que desea atacar nuestro sistema necesita toda la información posible. Desde el tipo de empresa, el área en que se desarrolla, su solvencia económica, sus clientes, cantidad de empleados, tipos y características de los sistemas implementados (tecnologías de red, sistemas telefónicos), niveles de seguridad física por solo mencionar algunos. Muchos de estos los puede averiguar sencillamente preguntándole a algún trabajador con una excusa justificable o consultando servicios de DNS, páginas Web de la empresa y anuncios publicitarios. Las demás a través de herramientas propias de los sistemas operativos (ping, whois, finger, rusers, nslookup, rcpinfor, telnet, dig, nmap). (MCLURE, 2010)

2.3.6.5. Envenenamiento IP o ARP (Spoofing)

Las relaciones de confianza basada en direcciones IP pueden ser burladas por el spoofing, mediante el cual se suplantada la identidad de la máquina en la que se confía. Los cortafuegos implementan sus reglas basadas en los sockets (número IP y puerto). Si alguien llega a suplantar alguna de las máquinas que nuestro sistema considera confiables, estamos perdidos. El spoofing puede ser IP o ARP, los sistemas operativos de Windows detectan la suplantación de IP, pero las versiones de Linux (Red Hat) no. Cuando el envenenamiento es ARP es más difícil de detectar porque la máquina del intruso funciona de

puente entre las estaciones y no se interrumpe la comunicación. (VILLALON HUERTA, 2002)

Para este tipo de ataque se recomienda la herramienta ARPWatch de Linux que es capaz de detectar cualquier cambio de ARP ocurrido en la subred y emite alarmas en la consola o las envía por correo electrónico.

2.3.6.6. Escaneo de puertos

A partir de las respuestas de los protocolos (TCP o UDP), como resultado de intentos de conexión por determinados puertos, podemos obtener información acerca de los servicios ofrecidos, los sistemas operativos y la versión de la aplicación que brinda el servicio. Una vez conocida la versión de la aplicación, investigamos sus vulnerabilidades. Casi la totalidad de los sistemas de detección de intrusos son capaces de detectar los escaneo de puertos, el cual no llega a ser un ataque pero es sin dudas la antesala. Como Sistema de Detección de Intrusos basado en Red (en adelante NIDS) se recomienda el SNORT, en su versión para Linux. El NIDS debe ser implementado en un punto donde sea capaz de analizar todo el tráfico relativo a las máquinas que desee proteger.

2.3.6.7. Negación de Servicio (DoS)

Los ataques de negación de servicio DoS (Denial of Service) dirigidos contra recursos informáticos, cuyo objetivo es degradar parcial o totalmente los servicios. Pueden estar orientados a una máquina, una red o cualquier aplicación, como un servidor Web, FTP, mail, DNS o cualquier otro. Con el desarrollo de los DoS han aparecido los DDoS o negaciones de servicio distribuido (Distributed Denial of Service), donde el atacante compromete un determinado número de máquinas que en un momento dado

hacen un ataque simultáneo a un objetivo determinado. (HIROAKI, MASAFUMI, & YOUKI, 2003 E86-D(11))

2.3.6.8. Intercepción

El sniffing es una de las técnicas de intercepción más usadas, en la cual el atacante captura en tiempo real los paquetes que viajan por la red a partir de los cuales puede obtener información de servicios, arquitectura de la red, contraseñas, mensajes de correo electrónico y todo tipo de información privada. Otra variante de interceptación la constituyen los keyloggers que son programas capaces de captar las pulsaciones del teclado. Estos son muy usados para el robo de contraseñas, aunque para hacerlo funcionar el atacante tiene que acceder físicamente a la máquina o tener privilegios administrativos.

2.3.7. Amenazas en el desarrollo de sistemas

Durante el desarrollo de aplicaciones los programadores suelen dejar puertas abierta, para depurar fallas con mayor facilidad o simplemente para tener un control permanente sobre el sistema que están desarrollando. Esto puede ser muy importante ya que el sistema siempre sería vulnerable al creador y podría adquirir grandes sumas de dinero por conceptos de mantenimiento. Aunque en la mayoría de los casos las puertas abiertas son causadas por errores de programación. Si dicha vulnerabilidad se descubriera o la existencia de la puerta se llegara a filtrar, cualquier intruso puede hacer uso de ella para violar la integridad de su sistema. Empresas de seguridad a nivel mundial reportan que los ataques a datos confidenciales mediante el uso de puertas abiertas durante el primer semestre del 2014, aumentó en un 113%. (Symantec Corporation, 2015).

Los virus, son más comunes en sistemas Windows que en Linux. Estos inician cada vez que inicia la computadora, para lo cual se

copian en el registro de Windows, se propagan por la red, por correo electrónico, usando vulnerabilidades de los sistemas operativos y puede venir como combinación de gusano, caballo de Troya y otras variantes aprovechando las ventajas de cada uno de ellos, su finalidad puede ser múltiple, desde el robo y destrucción de información, implantación de una puerta trasera o caballo de Troya, negación de servicio distribuido a una página específica en Internet, entre otras variantes. Durante el primer semestre de 2014, las amenazas combinadas aumentaron el 44% comparado con las de la primera mitad de 2013. (Symantec Corporation, 2015)

2.3.8. Protecciones al Sistema

Para proteger nuestro sistema debemos realizar el análisis de las amenazas potenciales que puede sufrir, pérdidas que se podrían generar y probabilidad de ocurrencia. A partir de este análisis hemos de diseñar una política de seguridad que defina reglas y responsabilidades para evitar amenazas y minimizar sus efectos. Los mecanismos de seguridad son los usados para implementar la política, y estos se dividen en tres grandes grupos, prevención, detección y recuperación.

Los mecanismos de prevención prevén la ocurrencia de violaciones a la seguridad. Como es el uso de cifrado en las transmisiones lo cual evita que las comunicaciones sean escuchadas. Los mecanismos de detección son usados para detectar violaciones en la seguridad o intentos de violación, en este grupo se encuentran los sistemas de auditoría, sistemas de detección de intrusos.

Los mecanismos de recuperación, que son aplicables cuando ocurre algún evento que haya generado la pérdida de información sensible, ejemplos de estos mecanismos son las copias de seguridad o hardware redundante. En este punto, las técnicas de análisis forense,

nos ayudan a averiguar la forma y el alcance de la violación, lo que nos permite prevenir ataques posteriores. Los mecanismos de prevención y detección son los más importantes, ya que si están bien concebidos, será menos probable que necesitemos usar el tercero. (LUCENA LÓPEZ, 2010)

2.3.9. Sistemas de identificación. Criptografía

Desde el principio de la historia del hombre surge la necesidad de garantizar la confidencialidad de la información, por eso se han desarrollado diversas técnicas de enmascaramiento u ocultación de la información, siendo en la actualidad uno de los principales objetivos que persigue la seguridad informática.

2.3.9.1. Importancia de la Criptografía

Según Jorge Ramiro Aguirre profesor titular en el Departamento de Lenguajes, Proyectos y Sistemas Informáticos de la Universidad Politécnica de Madrid “Criptografía es la Rama inicial de las Matemáticas y en la actualidad, de la Informática y la Telemática, que hace uso de métodos y técnicas con el objetivo principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves.” (AGUIRRE JORGE, 2003)

Esto da lugar a diferentes tipos de criptosistemas que permiten asegurar cuatro aspectos fundamentales de la seguridad informática: confidencialidad, integridad, disponibilidad y no repudio.”

2.3.9.2. Clasificación de la criptografía tradicional

Una clasificación tradicional de los métodos de criptografía son:

- *Sistemas de transposición*: como indica su nombre consiste en descolocar el orden de las letras, sílabas o conjunto de letras. En función del número de

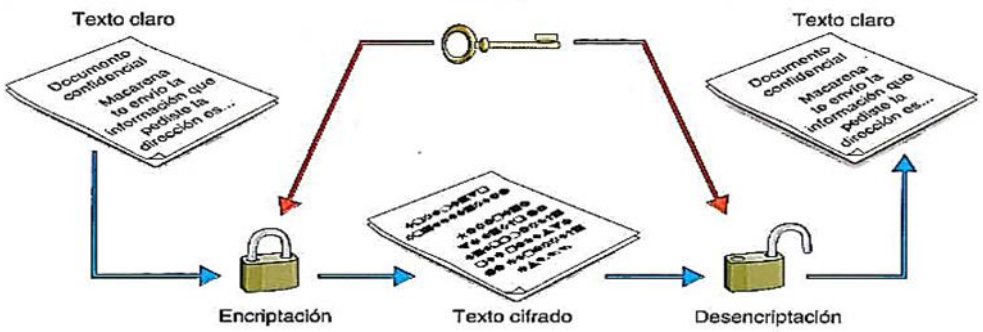
transposiciones podemos clasificar los sistemas de transposición en: Sistemas de transposición simples: cuando el texto en claro solo es sometido a una transposición. Sistemas de transposición doble o múltiple, cuando se realiza una segunda transposición sobre texto que ya había sido cifrado mediante transposición simple. Con este método se consigue una mayor seguridad.

- *Sistemas de sustitución*: como su nombre indica se reemplazan algunas letras del alfabeto por otras o por un conjunto de ellas según el método. Según el tipo de sustitución se clasifica en: Literal, se sustituyen letras por letras. Numéricas, se sustituyen por números. Esteganográfica, se sustituyen por signos o se oculta el mensaje tras una imagen, sonido, etc.

2.3.9.3. Criptografía simétrica

Este método se basa en un secreto compartido entre la entidad que cifra el mensaje y la que lo quiere descifrar, es decir, utiliza la misma clave en el proceso de cifrado que en el de descifrado.

Si analizamos los métodos utilizados para salvaguardar la confidencialidad de los mensajes desde los primeros tiempos de la criptografía hasta mediados de los setenta (prácticamente hasta nuestros días), veremos que solo se hacía uso de métodos simétricos, que exigían necesariamente que el emisor y el receptor se pusieran previamente de acuerdo en la clave que iban a utilizar. El método de Vi genere es un claro ejemplo de lo dicho.



F i g u r

a 9. Cifrado con clave privada.
Fuente: (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

Este método tiene dos desventajas: *la primera*, como se puede deducir de lo explicado, es la que conlleva el intercambio de claves, ya que si las personas se conocen y están físicamente en contacto es más o menos fácil comunicarse la clave.

La segunda desventaja es la cantidad de claves que una persona debe memorizar; supongamos que se intercambia información confidencial con cincuenta personas diferentes, con cada una de ellas utiliza una clave distinta y cada cierto tiempo modifica dichas claves por seguridad. (AGUIRRE JORGE, 2003)

2.3.9.4. Criptografía asimétrica.

Consiste en que cada una de las partes involucradas en una comunicación segura tiene una pareja de claves. Una de ellas, pública, que deberá intercambiar con cada una de las entidades con las que quiera comunicarse mensajes secretos, y otra de ellas privada, y que por tanto, jamás debe comunicar a nadie; sin que exista ninguna vulnerabilidad en las comunicaciones, porque con ella nunca podría un intruso descifrar el mensaje.

Para cifrar un mensaje, el emisor utilizará la clave pública del receptor, y a su vez, el receptor descifrará este mensaje haciendo uso de su clave privada. Como se puede ver, se han solventado las desventajas de la criptografía de clave privada. Como es lógico pensar, estas claves se generan a la vez y se encuentran r

ionadas matemáticamente entre sí mediante funciones de un solo sentido; resulta prácticamente imposible descubrir la clave privada a partir de la pública. (LUCENA LÓPEZ, 2010)

Figura 10. Cifrado con clave pública.
Fuente: (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

2.3.9.5. Criptografía híbrida

La desventaja de la criptografía de clave pública es la lentitud del proceso de cifrado y descifrado, que obedece tanto a la complejidad de los métodos utilizados como a la longitud de las claves. Otra de las desventajas es el mayor tamaño de la información cifrada con clave pública frente al tamaño de la misma cuando se cifra con clave privada.

Todo esto nos hace pensar que lo ideal sería utilizar criptografía de clave privada para intercambiar mensajes, pues estos son más pequeños y además el proceso es rápido, y utilizar criptografía de clave pública para el intercambio de las claves privadas. (LUCENA LÓPEZ, 2010)

2.3.10. Algoritmos

Los algoritmos son los métodos que se utilizan para transformar el texto claro en el texto cifrado. El algoritmo consiste en sustituir cada letra del texto sin cifrar por otra letra del mismo alfabeto que se encuentra situada en el orden del diccionario N puestos por delante.
N es el valor de la clave, que como podemos ver junto con el algoritmo y determinará exactamente la letra que sustituirá a la original.

Como podemos imaginar, hoy en día se utilizan diferentes algoritmos, algunos válidos para criptografía de clave privada y otras para criptografía de clave pública. DES, 3DES, RC4, IDEA Y AES son

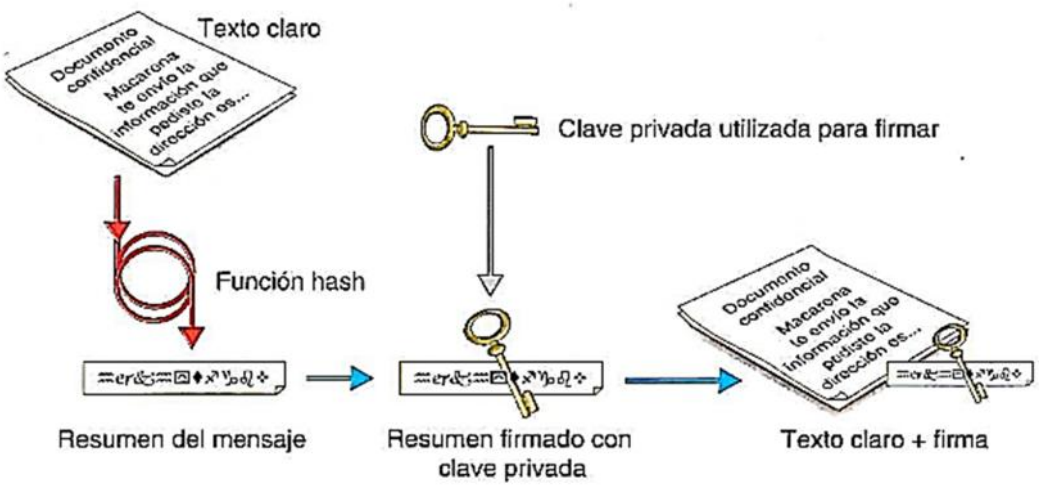
nombres de algoritmos de clave privada y DH, EIGamal, RSA de clave pública, entre otros. (LUCENA LÓPEZ, 2010)

2.3.11. Firma digital

La firma digital viene a sustituir a la manuscrita en el mundo de [a informática. Es decir, si firmamos de forma digital un documenta, [e estaremos dando veracidad y como sucede con la firma manuscrita, no podremos decir que no lo hemos firmado nosotras; por lo tanto, seremos responsables de lo que en él se diga. (LUCENA LÓPEZ, 2010)

La descripción del mecanismo de firma electrónica es el siguiente:

- Se calcula un valor resumen del documento, utilizando algún algoritmo como el SHA.
- Este valor resumen se cifra utilizando la clave privada de nuestra pareja de claves pública-privada (sí, has leído bien, resulta que no sólo se puede cifrar con la clave pública, también algunos algoritmos de cifrado asimétrico permiten cifrar con la clave privada, en especial los que se utilizan para firma digital. Esto permite asegurar que la única persona que ha podido firmar el documenta soy yo, el único que conoce la clave privada).
- El resultado de este valor es el que se conoce como firma digital del documento.



Esquema del proceso de firma digital.
Fuente: (SEOANE, SAIZ, FERNÁNDEZ, & FERNÁNDEZ , 2013)

2.3.12. Certificados Digitales

Los Certificados Digitales, documentos electrónicos basados en la criptografía de clave pública y en el sistema de firmas digitales, garantizan con toda confianza el vínculo existente entre una persona, entidad o Servidor Web con una pareja de claves correspondientes a un sistema criptográfico de clave pública. (MORENO, 2003)

El certificado digital contiene datos identificativos de una persona o entidad y la llave pública de la misma; haciéndose responsable de la autenticidad de los datos que figuran en el certificado de otra persona o entidad de confianza, denominada Autoridad Certificadora (AC). (MORENO, 2003)

Las principales Autoridades Certificadoras actuales son Verisign (filial de RSA Data Security Inc.) y Thawte. Estas entidades atestiguan que la persona portadora de ese documento es quien dice ser. El formato de los certificados digitales es estándar, siendo X.509 v3 el recomendado por la Unión Internacional de Comunicaciones y el que está en vigor en la actualidad. (MORENO, 2003)

2.3.12.1. Tipos de Certificados

Dependiendo del uso que se vaya a dar al certificado y de qué persona o entidad lo solicita, las Autoridades Certificadoras han dividido los certificados en varios tipos. Desde el punto de vista de la finalidad, los certificados electrónicos se dividen en: (MORENO, 2003)

1. Certificados SSL para cliente: usados para identificar y autenticar a clientes ante servidores en comunicaciones mediante el protocolo Secure Socket Layer (SSL), y se expiden normalmente a una persona física. (MORENO, 2003)

2. Certificados SSL para servidor: usados para identificar a un servidor ante un cliente en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden generalmente a nombre de la empresa propietaria del servidor seguro o del servicio que éste va a ofrecer, vinculando también el dominio por el que se debe acceder al servidor. La presencia de éste certificado es condición imprescindible para establecer comunicaciones seguras SSL. (MORENO, 2003)

3. Certificados S/MIME: usados para servicios de correo electrónico firmado y cifrado, que se expiden generalmente a una persona física. El mensaje lo firma digitalmente el remitente, lo que proporciona Autenticación, Integridad y No Rechazo. También se puede cifrar el mensaje con la llave pública del destinatario, lo que proporciona confidencialidad al envío. (MORENO, 2003)

4. Certificados de firma de objetos: usados para identificar al autor de ficheros o porciones de código en cualquier lenguaje de programación que se deba ejecutar en red (Java, JavaScript, CGI, etc.). Cuando un código de éste tipo pueda resultar peligroso para el sistema del usuario, el navegador lanza un aviso de alerta, en el que figurará si existe certificado que avale al código, con lo que el usuario puede elegir si confía en el autor, dejando que se ejecute el código, o si por el contrario no confía en él, con lo que el código será rechazado. (MORENO, 2003)

5. Certificados para AC: identifican a las propias Autoridades Certificadoras, y es usado por el software cliente para determinar si pueden confiar en un certificado cualquiera accediendo al certificado de la AC y comprobando que esta es de confianza. Toda persona o entidad que desee obtener un certificado debe pagar una cuota a las Autoridades de Certificación, cuota que irá en función de la clase del certificado y del uso que se le vaya a dar al mismo. (MORENO, 2003)

2.3.13. SSL (Secure Socket Layer).

Secure Socket Layer, es un protocolo basado en la aplicación conjunta de Criptografía Simétrica, Criptografía Asimétrica, Certificados Digitales y Firmas Digitales. SSL aprovecha de los sistemas simétricos la rapidez de la operación, y de los sistemas asimétricos la seguridad para el intercambio de claves simétricas, consiguiendo con ello resolver el problema de la confidencialidad en la transmisión de datos. (MORENO, 2003)

SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socket, de forma transparente al usuario y a las aplicaciones que lo usan. Es el estándar de comunicación seguro en los navegadores Web. Garantiza la identidad del servidor Web mediante el Certificado Digital correspondiente, del que se comprueba su validez antes de iniciar el intercambio de datos sensibles (Autenticación), mientras que de la seguridad de la integridad de los datos intercambiados se ocupa la Firma Digital mediante funciones hash y la comprobación de resúmenes de todos los datos enviados y recibidos. (MORENO, 2003)

Desde el punto de vista de su implementación en los modelos de referencia OSI y TCP/IP, SSL se encuentra situado entre la capa de Aplicación y la capa de Transporte, sustituyendo los socket del sistema operativo, lo que hace que sea independiente de la aplicación que lo utilice y generalmente se implementa en el puerto 443. Su versión más actual es la 3.0. que usa los algoritmos simétricos de encriptación DES, TRIPLE DES, RC2, RC4 e IDEA, el asimétrico RSA, la función hash MD5 y el algoritmo de firma SHA-1. Los algoritmos, longitudes de clave y funciones hash de resumen usados en SSL dependen del nivel de seguridad que se busque y se soporte. (MORENO, 2003)

2.3.14. SSH (Secure Socket Hash)

El protocolo SSH es usado para acceder a máquinas a través de una red, de forma similar a como se hacía con telnet. La diferencia principal es que SSH usa técnicas de cifrado para que ningún atacante pueda descubrir las contraseñas ni espiar el desarrollo de la sesión.

Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura y gestionar claves RSA. Este protocolo es muy usado para la administración de servidores Unix y para el intercambio seguro de ficheros entre Unix y Windows. (STANGER, 2001)

2.3.15. Protocolos y mecanismos de seguridad

La seguridad informática es un tema muy amplio, por lo que nos vamos a centrar en algunos protocolos y mecanismos de seguridad. Los demás que se consideren importantes y por cuestiones de tiempo no hayan sido tratados en este capítulo quedarán para futuras investigaciones o continuación de este mismo trabajo. Entre los protocolos no tratados se encuentran IPv6, TLS, y SASL por solo mencionar algunos.

2.3.15.1. IPSec

IPSec es un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública, algoritmos de cifrado, algoritmos de hash y certificados digitales. (TSUKAMOTO, 2002)

El protocolo IPSec ha sido diseñado de manera modular, de forma que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Está compuesto por dos protocolos de seguridad: IP Authentication Header (AH) e IP Encapsulating Security Payload (ESP) que proporcionan mecanismos de seguridad para proteger el tráfico

IP. Un protocolo de gestión de claves Internet Key Exchange (IKE) que permite a dos nodos negociar las claves y los parámetros necesarios para establecer una conexión. (DORASWAMY, 2013)

2.3.15.2. Kerberos

Uno de los sistemas de autentificación más importante lo constituye Kerberos, el cual fue creado en el MIT (Massachussetts Institute of Technology) en 1983 con el proyecto Athena. Su nombre se debe al perro de tres cabezas que en la mitología griega vigila la puerta de la entrada al reino de Hades. (VILLALON HUERTA, 2002)

El uso de kerberos se produce principalmente en el inicio de sesión y en el acceso a otros servidores de aplicación. Una vez que un cliente está autenticado o bien se asume que todos sus mensajes son confiables, o si se desea mayor seguridad se puede elegir trabajar con mensajes seguros (autenticados) o privados (autenticados y cifrados). Kerberos se puede implementar en un servidor que se ejecute en una máquina segura, mediante un conjunto de bibliotecas que se utilizan tanto en los clientes como en las aplicaciones; se trata de un sistema de autentificación altamente seguro que puede ser usado en sistemas de alta disponibilidad. (VILLALON HUERTA, 2002)

2.3.15.3. Arquitectura de Kerberos

Un servidor Kerberos se denomina KDC (Kerberos Distribution Center), y provee de dos servicios fundamentales: el de autenticación (AS, Autentication Service) y el de ticket (TGS, Ticket Granting Service). El AS tiene como función autenticar inicialmente a los clientes y proporcionarles un ticket para comunicarse con el TGS. El Servidor de Ticket, proporciona a los

clientes las credenciales necesarias para comunicarse con un servidor final que es quien realmente ofrece el servicio. El servidor Kerberos posee una base de datos de sus clientes (usuarios o programas) con sus respectivas claves privadas, conocidas únicamente por dicho servidor y por el cliente al que pertenece. (VILLALON HUERTA, 2002)

La arquitectura Kerberos se basa en tres objetos de seguridad: Clave de Sesión, Ticket y Autenticador:

- La Clave de Sesión es una clave secreta generada por Kerberos y entregada a un cliente para uso con un servidor durante una sesión; no es obligatorio utilizarla en toda la comunicación con el servidor, solo si el servidor lo requiere (porque los datos son confidenciales) o si el servidor es un servidor de autenticación. Se suele denominar a esta clave K_{CS}, para la comunicación entre un cliente C y un servidor S. Las claves de sesión se utilizan para minimizar el uso de las claves secretas de los diferentes agentes: estas últimas son válidas durante mucho tiempo, por lo que es conveniente para minimizar ataques utilizarlas lo menos posible.
- El Ticket es un testigo entregado a un cliente para solicitar los servicios de un servidor; garantiza que el cliente ha sido autenticado recientemente.
- El Autenticador es un testigo construido por el cliente y enviado a un servidor para probar su identidad y la actualidad de la comunicación; solo puede ser utilizado una a la vez. Este autenticador contiene, cifrado con la clave de la sesión, el nombre del cliente y un sello de tiempo (timestamp). (VILLALON HUERTA, 2002)

2.3.15.4. Consideraciones al emplear Kerberos

Uno de las principales consideraciones de Kerberos es que cualquier programa que lo utilice ha de ser modificado siguiendo un proceso denominado kerberización. Otro problema y esta vez

relacionado con la seguridad es la gran centralización del sistema. Para un correcto funcionamiento se ha de disponer en todo momento del servidor Kerberos, de forma que si la máquina que lo alberga falla, la red se torna inutilizable. (TANENBAUM, 2003)

Otro asunto de seguridad es el uso de sellos de tiempo como prueba de frescura en Kerberos. Esto obliga a que todas las máquinas que ejecutan servicios autenticados mantengan sus relojes sincronizados y el empleo de servicios NTP (protocolos de red para sincronización de tiempo). (TANENBAUM, 2003)

CAPÍTULO III

METODOLOGÍA DE INVESTIGACIÓN

3.1. Métodos y técnicas utilizados en la investigación

Uno de los problemas más complejos que debe enfrentar cualquier investigador, es sin lugar a dudas elegir el tipo de investigación y la gran cantidad de métodos, técnicas e instrumentos que existen; las cuales forman parte de un número ilimitado de paradigmas, posturas epistemológicas y escuelas filosóficas, cuyo volumen y diversidad desconciertan. Para tal efecto se ha considerado los siguientes métodos y tipos de investigación; así como, herramientas y técnicas para el objeto de estudio:

3.1.1. Método inductivo-deductivo.-

Para el presente tema de estudio se analiza las diferentes partes y elementos que conforman un sistema de seguridad y su impacto en las redes; identificando las amenazas y vulnerabilidades que afectan a una infraestructura informática hasta obtener una plataforma segura y sostenible. Este método de inferencia se basa en la lógica y estudia hechos particulares, que van desde la descomposición hasta la construcción.

El método inductivo-deductivo está enmarcado dentro de la investigación descriptiva, misma que se guía a través de las preguntas de investigación para explicar la hipótesis de estudio; y que se formulan a nivel descriptivo para probar dicha hipótesis. La investigación descriptiva se soporta principalmente técnicas como la encuesta, la entrevista, la observación y la revisión documental

3.1.2. Método hipotético-deductivo.-

Una vez definida las diferentes preguntas directrices de investigación, se plantea la siguiente hipótesis a ser comprobada: "*Los sistemas de seguridad informática y los métodos de protección en infraestructuras tecnológicas inciden favorablemente en la intranet de la Universidad Técnica de Babahoyo"*; y del que se busca

afirmar o falsear tal hipótesis a través de la información recolectada, procesada, e interpretada ejerciendo acción directa sobre el objeto de estudio donde se deduce de ellas conclusiones que deben confrontarse con los hechos.

Este método por excelencia forma parte de la investigación experimental que se caracteriza ya que actúa conscientemente sobre los objetivos del estudio que identifica los efectos, amenazas y vulnerabilidades de la intranet universitaria; analiza e interpreta las irregularidades en seguridad informática existente en la intranet y diseña una solución de infraestructura segura, de la situación problemática para determinar los mecanismos necesarios para probar la hipótesis.

3.1.3. Método analítico-sintético.-

Estudia los hechos, partiendo de la descomposición del objeto de estudio en partes para estudiarlas en forma individual y luego integrarlas para analizarlas de manera holística e integral. Para el siguiente trabajo de investigación el estudio analítico se centra en diferentes problemas que presenta la infraestructura informática de la Universidad Técnica de Babahoyo, los mismos que han sido identificados a través de las siguientes preguntas directrices:

P1: ¿Cómo afecta las vulnerabilidades, amenazas y riesgos tecnológicos expuestos a nivel de usuario en la intranet de la Universidad Técnica de Babahoyo?

P2: ¿Cuáles son las debilidades y amenazas que exhibe la intranet universitaria en el tráfico de paquetes al usar técnicas de monitoreo de red?

P3: ¿De qué manera una metodología en seguridad informática en el diseño de una infraestructura tecnológica fortalece la integridad de la intranet de la Universidad Técnica de Babahoyo?

3.2. Técnicas de Investigación

Estos procedimientos permitirán facilitar la recolección de información de manera inmediata según el tipo de investigación y métodos a emplear; y como tal existen tantas técnicas como problemas susceptibles de ser investigados.

Para efectos de la investigación se hará uso en el empleo de técnicas de recolección de información PRIMARIA, ya que al ser focalizado el ámbito de estudio y su problemática es necesario levantar información de primera mano, utilizando técnicas especializadas en este tipo de recolección de datos, tales como: OBSERVACIÓN (Estructurado o Participante), ENTREVISTA Y ENCUESTA (cuestionario).

3.2.1. La Observación.- Para el presente trabajo, se analiza la situación de *La Seguridad Informática en la Infraestructura de la Universidad Técnica de Babahoyo*, captando y anotando lo que acontece en el entorno, describiendo los problemas, amenazas y posibles vulnerabilidades en la intranet universitaria, pero puede ser susceptible a las limitaciones propias de los sentidos, por lo que se recomienda que sea:

1) Estructurado.- Se considera los aspectos a observarse, escogiendo lo que es más importante; para el presente trabajo, es necesario captar los diferentes ataques, vulnerabilidades y perpetraciones que sufre la intranet de la UTB. Observar los diferentes estados de seguridad y evaluar la calidad de las comunicaciones.
2) Participante.- Interviene el criterio del personal que labora entorno a la informática de la institución o directamente el investigador para recoger información, garantizando la objetividad que se pretende dar a la información recogida.

3.2.2. La Entrevista.- En esta conversación se averigua datos específicos sobre el estado, la integridad, la seguridad y las medidas de

protección de la red universitaria; cuya información es requerida en la investigación. Se seleccionó al personal de informática de la institución y a su director, Ing. Iván Ruíz Parrales; estableciendo previamente con el entrevistado los objetivos, tiempo y la utilización de tales resultados.

3.2.3. La Encuesta o Cuestionario.- Tiene la ventaja de formular preguntas a los usuarios, siendo los más afectados de la calidad de servicio de la intranet y las escasas seguridades que presta, los cuales se os identifica en: personal administrativo, docentes y autoridades de la Universidad; quienes proporcionan información del entorno y su contexto donde se presenta la problemática de estudio, y en los que el anonimato constituye una ventaja ya que no puede personalizarse las respuestas.

Su desventaja está en la garantía de su aplicación, porque al requerir la intervención de muchas personas no se puede asegurar que estos cumplan con el cometido, que la información sea la que se necesita; otra limitación proviene de la posible falsedad de las respuestas o cuando no se completa el cuestionario.

3.3. Construcción Metodológica del objeto de investigación

Partiendo en el presente trabajo de investigación desde la conceptualización del problema: *¿Cómo incide la escasa Seguridad Informática y métodos de protección en la intranet de la Universidad Técnica de Babahoyo?* Se analiza la imperativa necesidad de conducir a la intranet universitaria hacia una infraestructura segura, robusta, y protegida a las diferentes amenazas que comprometan la información sensible de dicha institución.

Actualmente la infraestructura de la UTB no cuenta con una red efectiva, segura y protegida contra amenazas y ataques. Es imperioso ejecutar inmediatamente políticas y establecer normas tanto de conectividad y uso

de equipos; configurar accesos de usuarios a la red, proteger los protocolos de comunicación como sus puertos y asegurar las aplicaciones y principalmente la información.

La siguiente propuesta se fundamenta en las metodologías tanto descriptiva, analítica y cuasi-experimental; que mediante la observación, la recopilación de información empírica, recolección de información de los involucrados y usuarios; así como, encuestas a los administradores y jefes departamentales, se podrá obtener una muy cercana veracidad de la situación actual misma que será cotejada con la propuesta de mejora y viabilidad.

Las encuestas y cuestionarios están diseñados en formato de preguntas de opción múltiple y opinión de criterios. Los instrumentos de recolección de datos empíricos para el caso de estudio son elaborados en base al planteamiento del problema, los objetivos planteados, e indicadores; mismos que se plantean a través de un formulario de observación para la investigación en SITU.

Finalmente las encuestas están dirigidas hacia los usuarios, docentes y administradores de los data center de cada facultad; mientras que, las encuestas y cuestionarios son conducentes a la dirección general de sistemas de la universidad y sus operadores.

Con la recolección de los datos anteriormente citados se elaborará el análisis de la investigación y se validará la hipótesis a ser contrastada con la presente propuesta: *Diseño de una infraestructura tecnológica segura aplicando métodos de protección para fortalecer la integridad en la intranet de la Universidad Técnica de Babahoyo*

.

3.4. Elaboración del Marco Teórico

El desarrollo de la presente investigación se constituye en forma general en los siguientes componentes:

- El problema y sus componentes.
- Marco teórico
- Metodología
- Propuesta

El problema planteado en el **CAPÍTULO I**, se lo elaboró en base a la experiencia propia vivida como usuario de la red universitaria, como testigo fiel de las quejas tanto de otros docentes, administradores y autoridades de la UTB; identificando los diversos sub-problemas derivados del problema general, que tienen que ver con la falta de accesos a la red, escasa o casi nula seguridad en las comunicaciones, falta de políticas y normas y la protección misma a los ataques y penetraciones malware no controladas.

El marco teórico **CAPÍTULO II** fue elaborado en base a los diferentes conceptos de seguridad, modelos de protección, normas a seguir como política institucional de seguridad, protocolos eficientes de redes seguras, control de usuarios y cuentas, sistemas de encriptación, entre otros. Adicionalmente se estudió algunas posturas teóricas y modelos de seguridad a seguir de diversos autores, observando las leyes que regulan los sistemas de telecomunicación y al mismo sistema de educación superior.

Para la metodología que es abordada en el **CAPÍTULO III** fueron estructuradas preguntas para determinar en los usuarios, administradores y autoridades, cómo una infraestructura tecnológica segura incide en el desempeño de la intranet universitaria. El planteamiento de la hipótesis en este capítulo es de suma importancia ya que permitirá evaluar la presente investigación y validar la propuesta como producto de mejora ante el problema ya definido.

Para el procesamiento de la información, **CAPÍTULO IV**; se utilizó varias herramientas para el procesamiento de información electrónica, tales como: Google DOCs, Microsoft Excel, Project; mismos que permiten realizar la planificación de las tareas, elaboración de formularios, ingreso de información, tabulación y presentación de resultados en forma de gráficos. Para el análisis estadístico se empleó el método de "*CHI CUADRADO"*, para validar la hipótesis. Esto ayudará a optimizar los recursos, a minimizar los errores y mejorar el análisis, para conllevar hacia las interpretaciones, conclusiones y recomendaciones a tratar en el **CAPÍTULO V**.

Finalmente el diseño de la propuesta se recrea en el **CAPÍTULO VI** sustentada del respectivo análisis de la información contrastada con la hipótesis de investigación, misma que se validará a través de los usuarios y administradores de la red universitaria el diseño de un sistema seguro para la infraestructura tecnológica de la Universidad Técnica de Babahoyo.

3.5. Recolección de la información empírica

Para la recolección de la información, basado en los métodos hipotético-deductivo y analítico-sintético, las herramientas más adecuadas son: Las Encuestas, Entrevistas y Observación de Campo; mismos que fueron realizados al personal que labora en la universidad. Cada pregunta fue realizada aplicando la fórmula de la muestra para la población de usuarios en la red matriz de la Universidad Técnica de Babahoyo; así mismo, las entrevistas y cuestionarios a los administradores de red. Es decir; la población es de 406 usuarios, 10 administradores de red y 4 autoridades. Ver tabla:

Nro.	Descripción	Lugar	Población
1	Usuarios de Red	Campus matriz UTB	406
2	Administradores y Operadores red	Dirección de Sistemas, DataCenter de FAFI, FF.CC.JJ.	10
3	Autoridades	Edif. Administrativo	4

	Inmediatas	FAFI FF.CC.JJ	
		Total	**420**

Tabla 5. Cuadro distribución de la población (universo)
Elaborado por: Geovanny Vega Villacís

3.5.1. Muestra

La muestra constituyen 406 usuarios de red, administradores y operadores de red suman 10 y finalmente se considera la población de 4 autoridades inmediatas, involucradas al objeto de estudio. Total de la población (universo) a considerar, cuatrocientos veinte.

3.5.2. Tamaño de la Muestra

Para el tamaño de la muestra se considera la población total de usuarios de red, **420**. Para el caso de los administradores y operadores se maneja el total de 10 al igual que las autoridades que son 4.

3.5.3. Determinación del Tamaño de la Muestra

La fórmula estadística para el tamaño de la muestra es la aleatoria simple no estratificada, que al emplear permite calcular el tamaño de la muestra simple del universo. Para calcular el tamaño de la muestra suele utilizarse la siguiente fórmula:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

Donde:

n = el tamaño de la muestra.

N = tamaño de la población.

σ = Desviación estándar de la población que, generalmente cuando no se tiene su valor, suele utilizarse un valor constante de 0,5.

Z = Valor obtenido mediante niveles de confianza. Es un valor constante que, si no se tiene su valor, se lo toma en relación al 95% de confianza equivale a 1,96 (como más usual).

e = Límite aceptable de error muestral que, generalmente cuando no se tiene su valor, suele utilizarse un valor que varía entre el 1% (0,01) y 9% (0,09), cuyo valor para la presente investigación es del 8,4% (0,084). (SUAREZ I., 2011)

Hallando el valor de n:

$$n = \frac{420(0{,}5)^2(1{,}96)^2}{(420-1)(0{,}07)^2 + (0{,}5)^2(1{,}96)^2}$$

n = 104 usuarios de red

3.5.4. Banco de Preguntas

- Las preguntas para formular las encuestas a los usuarios de red y autoridades, (*Ver en ANEXO II*). Encuesta a Usuarios.
- Las preguntas para formular las encuestas a los administradores y operadores de RED, (*Ver en ANEXO III*). Encuesta a Administradores.
- El formulario de observación para la recolección empírica de información, *(Ver ANEXO IV)*. Formulario de Observación.

3.6. Descripción de La información

Esta parte de la investigación consiste en procesar los datos (dispersos, desordenados, e individuales) obtenidos de la población objeto de estudio y que tiene como finalidad generar los resultados a partir de los cuales se realizará el análisis de la hipótesis formulada; previa a la definición de las variables o los criterios para ordenar dichos datos.

La información se obtuvo a través de cuestionarios, encuestas, entrevistas y formularios de observación; analizando y determinando las conclusiones y recomendaciones, obtenidas de la hipótesis positiva de la investigación involucrando a los usuarios de red, administradores y operadores de red y las autoridades inmediatas involucradas. Las encuestas para los usuarios

y operadores de red, así como para autoridades pertinentes contienen 10 preguntas; se formula un cuestionario de 12 preguntas para entrevistar a los administradores de la red universitaria. Todos estos instrumentos ayudan a determinar la situación actual de la intranet de la UTB y lo que se espera alcanzar al término de la investigación.

Y finalmente la aplicación del formulario de observación como un método confiable de interpretación, análisis e inferencia del estado de la red universitaria y sus niveles de seguridad, robustez, confiabilidad y operatividad en las circunstancias detectadas en la presente investigación.

3.7. Análisis e interpretación de resultados

El análisis e interpretación de los resultados se a realiza de la siguiente manera:

1) Etapa de preparación: en esta fase, se realizará el reconocimiento del contexto a estudiar. Se analiza la estructura de la red y sus diferentes subredes y se determina los posibles candidatos que nos proporcionarán la información necesaria.

2) Etapa de ejecución: en esta fase aplicamos los instrumentos para recoger la información. Se identifican así mismo las limitaciones y problemas que surjan de la aplicación de los instrumentos. Se ejecuta el formulario de observación en el Departamento de Sistemas de la Universidad y las entrevistas con los administradores de dicha red y jefes inmediatos.

3) Etapa de análisis e interpretación de la información, es decir la tabulación e interpretación de los datos recogidos, mismos que serán analizados por la aplicación MINITAB, y a la formulación de conclusiones y recomendaciones al concluir dicha investigación.

4) Etapa de elaboración de la propuesta*;* se ejecuta los métodos, planes y acciones pertinentes que incidan para validar la hipótesis planteada y que afecten directamente en la variable dependiente.

De esta manera se describe las principales características de los datos obtenidos, información que será validada por un experto en metodología, a fin de que se constate la propuesta de la investigación y así efectuar las correcciones de ser el caso.

3.8. Construcción del Informe de Investigación

Todo documento relacionado con investigación científica debe redactarse y presentarse siguiendo las normas de la metodología de investigación formal determinado por el campo del conocimiento que la institución académica exige, las normas de redacción lingüística (APA), los formatos del documento digital e impreso. Para tal efecto los principales aspectos a considerar en las distintas fases del trabajo de investigación son los siguientes:

a) *Establecer contacto con la población objeto de estudio.*- Para identificar el problema de investigación fue necesario observar, estudiar y establecer las necesidades que imperan en el entorno de las comunicaciones e infraestructura de la Universidad Técnica de Babahoyo. Para esto se estable la detección de las carencias y necesidades de información, mismas que fueron detectadas inicialmente acudiendo a las fuentes primarias: Usuarios de RED, Docentes y Operadores administrativos.

b) *Aplicar los Instrumentos y recolección de información.*- La identificación de las necesidades se logró mediante la aplicación de las actividades que se señalan a continuación y que permitieron recolectar toda la información necesaria para el diseño de los materiales:
   - Consulta de documentos
   - Encuestas
   - Aplicación y análisis de cuestionarios

c) *Elaborar el marco teórico formal de la investigación.*- Dada la importancia del marco teórico se elabora un marco teórico preliminar,

durante la propia investigación, siendo necesario reforzar mucho más sobre el tema objeto de investigación, el cual responda a temas de: Configuración de los Sistemas en Seguridad Informática, Diseño de Protocolos y Configuración de Interfaces de Red, Análisis de la Red Informática contra Intrusos y Malwares, Configuración de Accesos a Usuarios con cuentas Encriptadas, Elevación de Portal Cautivo para acceso a la Intranet Universitaria; detallando un diseño para la ejecución de procedimientos y elaborar un marco teórico de propuesta alternativa, con mayor nivel de rigurosidad propio de la ciencia y que soportará el procesamiento, el análisis, la discusión de los resultados de la investigación, así como las conclusiones de la misma y las recomendaciones que se puedan derivar de éstas.

d) Procesar la información recolectada.- Una vez recolectada la información de estudio hay que procesarla de acuerdo con el enunciado de los objetivos y la redacción de la hipótesis como solución ante las necesidades de un sistema de seguridad en infraestructura. Seguidamente de la Operacionalización de las variables, obteniendo así el cuestionario de preguntas para usuarios de red, operadores, administradores y autoridades de la UTB.

e) *Analizar y discutir los resultados de la información recolectada.-* Luego de procesar la información, es decir; de convertir los datos en resultados del estudio se procede analizar en función del problema de investigación, los objetivos y la hipótesis; empleando el método estadístico denominado **Chi Cuadrado**, mismo que comprueba la relación entre ambas variables (Independiente-Dependiente) y las hipótesis congruentes (H0: Hipótesis Nula y H1: Hipótesis Verificada); con un grado de confianza al 0,05 y dispersión de 2 grados.

f) *Redactar las conclusiones y recomendaciones.-* Incluir conclusiones generales respecto a los resultados del trabajo de campo como del

marco teórico elaborado para fundamentar el estudio o investigación realizada. De igual manera, incluir conclusiones específicas en función del problema de investigación, los objetivos específicos planteados, la hipótesis, los aspectos sobresalientes de los resultados del trabajo de campo y de su relación con los contenidos del marco teórico.

g) *Reporte o informe final de la investigación.*- Para la realización de la propuesta alternativa, se consideró la realización de un diseño que contenga aspectos relevantes en materia de Seguridad Informática, reflejando indicadores actuales de impacto y cómo se pueden minorar a través de una adecuada infraestructura tecnológica.

   Finalmente el proceso de diseño y producción de la propuesta es analizada y evaluada por expertos en materia de la institución y aprobación de viabilidad, con la finalidad de garantizar un producto de calidad que satisfaga las necesidades de los actores involucrados logrando con esto el cumplimiento de los objetivos inicialmente planteados.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS EN RELACIÓN CON LA HIPÓTESIS DE INTERVENCIÓN

4.1. Enunciado de la hipótesis

"Los sistemas de seguridad informática y los métodos de protección en infraestructuras tecnológicas, inciden favorablemente en la intranet de la Universidad Técnica de Babahoyo."

4.2. Ubicación y descripción de la información empírica pertinente a la hipótesis

VARIABLES	DIMENSIONES	INDICADORES	INSTRUMENTOS
Variable Independiente: Seguridad Informática y Métodos de Protección en Infraestructuras de Cómputo.	• Estudio de la seguridad informática. • Métodos de protección y mitigación de Riesgos.	• Metodología. • Conceptos de Operación. • Elementos de configuración. • Parámetros de calidad y validación.	• Argumentos • Ítems • Cuestionarios • Comparaciones y Descripciones
Variable Dependiente: Incidencia en la intranet de la Universidad Técnica de Babahoyo.	• Políticas y Estándares de Seguridad Informática • Adopción de protocolos y sistemas seguros. • Confidencialidad de datos y autentificación de usuarios. • Infraestructura segura, robusta y confidencial.	•Reglamentos y Políticas. •Cantidad de usuarios autentificados. •Cantidad de procesos y datos transmitidos sin errores. •Cantidad de intercepción a ataques por virus y malwares. •Velocidad de transmisión y Ancho de banda útil para las comunicaciones.	• Test´s • Observación • Encuestas • Entrevistas • Cuestionarios

Tabla 6. Operacionalización de Variables
Elaborado por: Geovanny Vega Villacís

4.3. Encuestas a usuarios para identificar las vulnerabilidades y amenazas que inciden en la Intranet de la UTB.

4.3.1. Encuesta para Autoridades, Docentes y Empleados

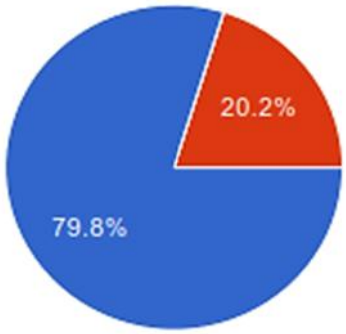
1) La información con la que trabaja en su computador es importante y confidencial para la universidad?

Tabla 7. Respuestas pregunta Nro. 1

Indicador	Valor	Porcentaje
SI	79	79,8%
NO	20	20,2%

Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 1. Respuestas pregunta Nro. 1



Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

En la pregunta Nro. 1 se evidencia que un 79,8 % de usuarios de la red trabajan con información importante y confidencial para la UTB y un 20,2 % no tienen, siendo un valor muy significativo.

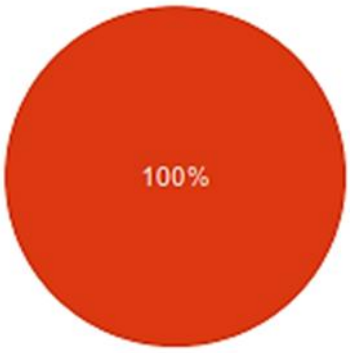
2) Usted como usuario de la red universitaria, trabaja en base a normas y reglamentos en políticas de seguridad informática?

Tabla 8. Respuestas pregunta Nro. 2

Indicador	Valor	Porcentaje
SI	0	0%
NO	100	100%

Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 2. Respuestas pregunta Nro. 2



Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Para la pregunta Nro. 2 el total de encuestados (usuarios de red) que representa el 100%, afirman NO seguir una política de seguridad, ya que la misma NO existe.

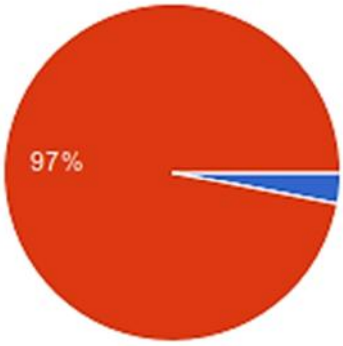
3) Usted para hacer uso de su equipo informático, le han asignado alguna cuenta de usuario y contraseña?

Tabla 9. Respuestas pregunta Nro. 3

Indicador	Valor	Porcentaje
SI	3	3%
NO	97	97%

Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 3. Respuestas pregunta Nro. 3.



Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

En la pregunta Nro. 3 el 97 % de usuarios de red NO le han asignado cuenta de usuario y contraseña para acceder a su equipo, ya que no lo usan; solo el 3% de usuarios SI tienen configurado sus equipos para tal efecto.

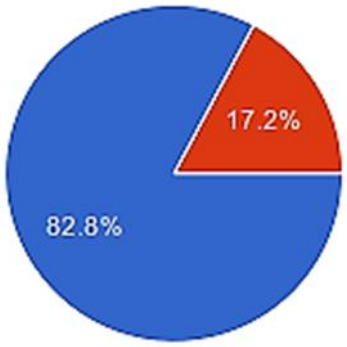
4) Es necesario que su equipo informático esté conectado a la red institucional para poder realizar su actividad laboral?

Tabla 10. Respuestas pregunta Nro. 4

Indicador	Valor	Porcentaje
SI	82	82.8%
NO	17	17,2%

Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 4. Respuestas pregunta Nro. 4



Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Para la pregunta Nro. 4 el 82,8 % de los usuarios SI tienen que estar sus computadores conectados a la red de la universidad, solo un 17,2% trabajan fuera de la red.

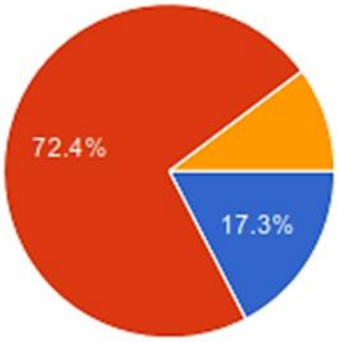
5) Si sus repuestas anteriores fueron afirmativas, en qué medida hace uso de sus cuentas asignadas?

Tabla 11. Respuestas pregunta Nro. 5

Indicador	Valor	Porcentaje
Siempre	17	17,3%
Casi siempre	71	72,4%
Rara vez	10	10,3%
Nunca	0	0%

Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 5. Respuestas pregunta Nro. 5



Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

En la pregunta Nro. 5 un 72,4% casi siempre hacen uso de sus cuentas de usuario asignado, el 17,3% se manifiesta que siempre lo hacen, y un 10,3% lo hacen rara vez. En consecuencia la mayor parte de usuario si hacen uso de sus cuentas, mientras que la minoría aún no lo usan con frecuencia.

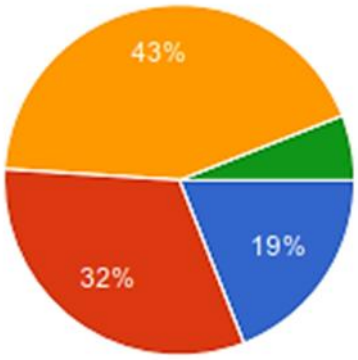
6) Su equipo informático ha tenido ataques de virus?

Tabla 12. Respuestas pregunta Nro. 6

Indicador	Valor	Porcentaje
Siempre	19	19%
Casi siempre	43	43%
Rara vez	32	32%
Nunca	6	6%

Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 6. Respuestas pregunta Nro. 6



Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

En la pregunta Nro. 6, un 43% de usuarios casi siempre tienen ataques de virus, un 32% rara vez y el 19% de usuarios siempre padecen de ataques de virus; teniendo apenas un 6% nunca han sufrido de ataques siendo la minoría. En consecuencia tenemos ataques frecuentes de virus y malwares en la red e internet.

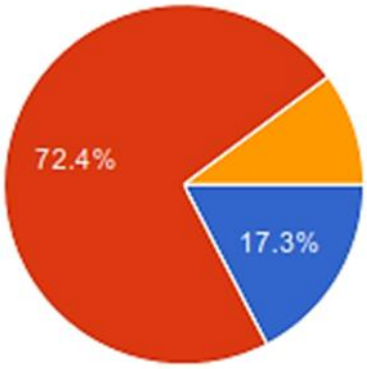
7) En qué medida el antivirus instalado en su equipo de cómputo de la universidad, notifica que se ha actualizado correctamente?

Tabla 13. Respuestas pregunta Nro. 7

Indicador	Valor	Porcentaje
Siempre	17	17,3%
Casi siempre	71	72,4%
Rara vez	10	10,3%
Nunca	0	0%

Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 7. Respuestas pregunta Nro. 7



Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Para la pregunta Nro. 7 indican un 72,4% de usuarios, que casi siempre el antivirus se actualiza; el 17,3% indican que siempre lo hace y un 10,3% rara vez. Por consiguiente es un indicar significativo a considerar para adoptar medidas de prevención y seguridad.

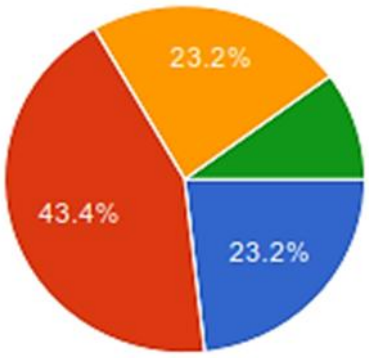
8) ¿En qué medida han afectado la presencia de virus en su equipo informático y en especial han alterado la información (archivos) almacenada?

Tabla 14. Respuestas pregunta Nro. 8

Indicador	Valor	Porcentaje
Muy afectado e Irrecuperable	23	23,2%
Afectado pero Recuperable	43	43,4%
Poco Afectado	23	23,2%
Totalmente Controlado	10	10,2%

Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 8. Respuestas pregunta Nro. 8



Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

En la pregunta Nro. 8. Los usuarios indican en un 43,4% que han sido afectados por virus/malwares, pero si han podido recuperarse; mientras que un 23,2% indican no haber podido recuperarse de un ataque de virus y al igual que otro 23,2% han sido atacados por virus pero no han sufrido consecuencia alguna y tan solo un 10,2% se manifiesta que su equipo está totalmente controlado. Siendo en ocasiones la mayor parte de usuarios que han sufrido fallas en sus equipos por la presencia de virus y/o malwares y no han podido recuperarse del daño.

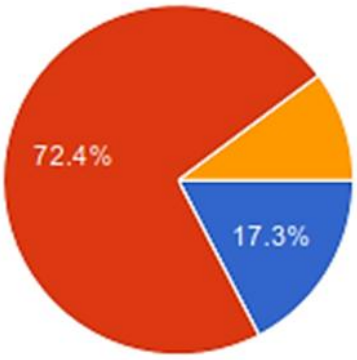
9) Cuando hace uso del internet con qué frecuencia se le aparecen ventanas emergentes en el navegador que afectan a su equipo?

Tabla 15. Respuestas pregunta Nro. 9

Indicador	Valor	Porcentaje
Siempre	17	17,3%
Casi siempre	71	72,4%
Rara vez	10	10,3%
Nunca	0	0%

Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 9. Respuestas pregunta Nro. 9



Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

La pregunta Nro. 8. Un 72,4% indican que casi siempre hay presencia de ventanas emergentes, el 17,3% se manifiesta que siempre, y un 10,3% rara vez. En consecuencia solo pocos usuarios expresan estar conformes con el servicio y la manera de prevenir la presencia de Windows Pop-up´s.

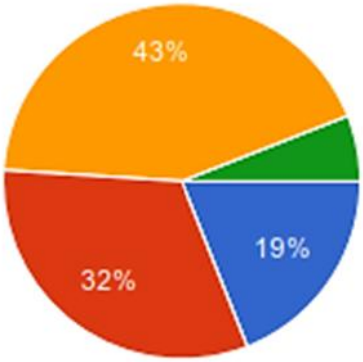
10) Cuando abre sus correos electrónicos en qué medida le han llegado correos basura o correos de desconocidos?

Tabla 16. Respuestas pregunta Nro. 10

Indicador	Valor	Porcentaje
Siempre	19	19%
Casi siempre	32	32%
Rara vez	43	43%
Nunca	6	6%

Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 10. Respuestas pregunta Nro. 10



Fuente: Usuarios de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Para la pregunta Nro. 9, solo un 43 % de usuarios rara vez se le a presentado correos basura, un 32% casi siempre y el 19% siempre les llegan correos basura y desconocidos; teniendo apenas un 6% que nunca ha tenido estos tipos de correos. En consecuencia tenemos un servicio de correo que no está del todo seguro.

4.3.2. Conclusiones Parciales. Usuarios de RED.

No existe una política institucional de seguridad informática que normen las actividades de los usuarios de red; existen pocos usuarios que tienen cuentas registradas en la red (nombre usuario y password) la mayor parte no cuentan con ello, teniendo en efecto una debilidad de protección y seguridad.

La mayor parte de usuarios conviven con algún tipo de virus y/o malwares que afectan el equipo informático y aún más la información con la que trabajan. Los antivirus instalados se encuentran desactualizados e incluso deshabilitados.

Las actividades que comúnmente ejecutan los usuarios de red se ven entorpecidos con intromisiones de ciertos winpopups o ventanas emergentes que se presentan al usar internet. Los correos de igual forma llegan algún tipo de correo basura o propaganda no deseada.

Prueba de Chi-Cuadrado en Usuarios de RED

Variable	Varianza / Rango
Variable I: Servicios de Seguridad y Métodos de Protección en infraestructuras tecnológicas	10 indicadores de Varianza
Variable D: Incidencia en la Intranet de la UTB.	Rango con 4 opciones: *1. Siempre* *2. Casi Siempre* *3. Rara vez* *4. Nunca*

Aplicando las tabulaciones efectuadas a los 10 indicadores que inciden sobre la seguridad y protección de la red al trabajo realizado por las autoridades, docentes y empleados de la UTB, se observa el siguiente comportamiento empleando el programa MINITAB para Test de Chi-Cuadrado. (*Ver pantalla completa, ANEXO V*)

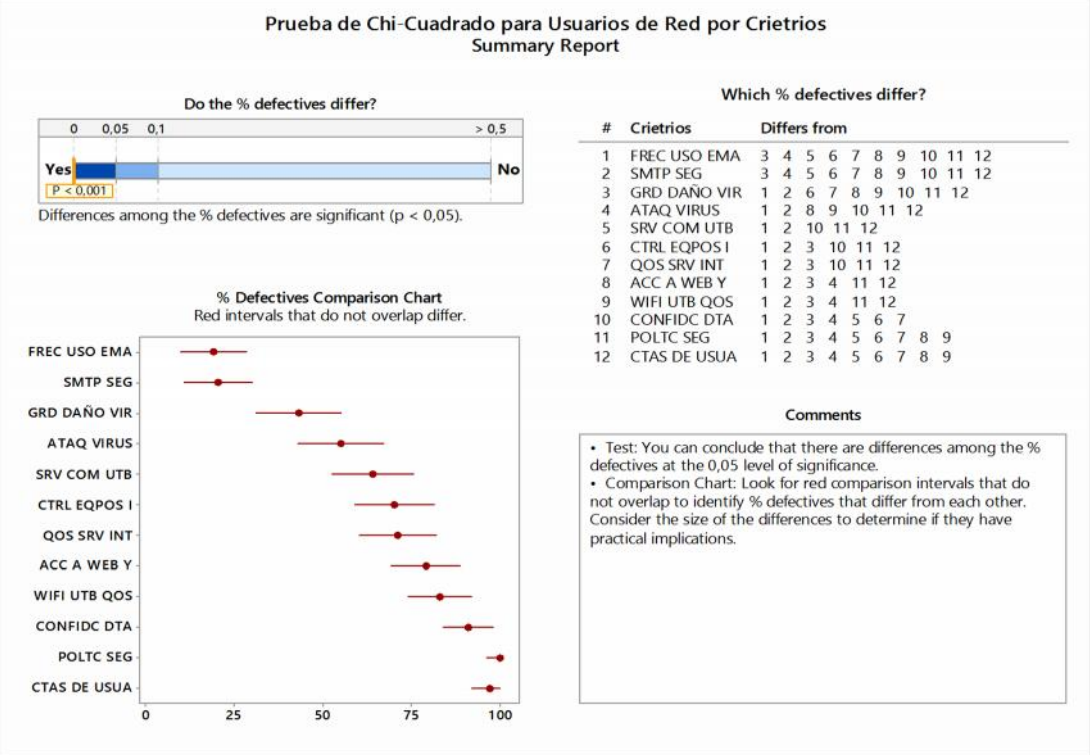


Figura 12. Reporte MINITAB (Chi-Cuadrado), para encuestas a Usuarios de Red.
Elaborado por: Geovanny Vega Villacís

Comentario.- Según el comentario del test aplicando Chi-Cuadrado con MINITAB concluye que:

- Test: Se puede concluir que existen diferencias entre las criterios medidos% en el nivel de significación 0,05.
- Tabla Comparativa: Encuentra intervalos de comparación rojas que no se superponen para identificar% de criterios medidos NO alcanzados que se diferencian unos de otros. Considere el tamaño de las diferencias para determinar si tienen implicaciones prácticas.

"Por consiguiente se NO se aprueba la H0 (Hipótesis Nula), en el que indica que no existe ninguna afectación con la seguridad informática. Como consecuencia al obtener un grado de incidencia menor a 0,05 se aprueba que SI existe incidencia en la seguridad de la intranet de la UTB y puede ser mejorada. "

4.3.3. Encuestas a Administradores RED y Operadores de RED.

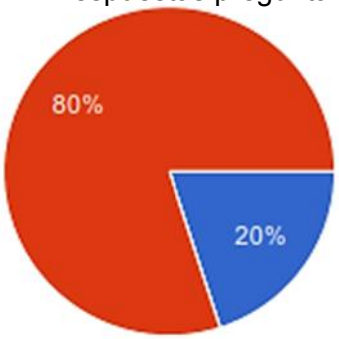
1) ¿Posee un Reglamento vigente y ejecutado al interior del campo universitario?

Tabla 17. Respuestas pregunta Nro. 1

Indicador	Valor	Porcentaje
SI	2	20%
NO	8	80%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 11. Respuestas pregunta Nro. 1



Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

En la pregunta Nro. 1 un 80% indican no tener un reglamento en política de seguridad informática, mientras que un 20% si lo tienen. En consecuencia no se ejecutan políticas en seguridad informática.

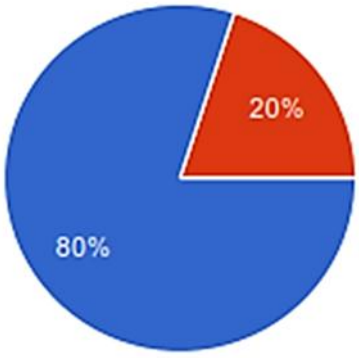
2) **En caso de haber respondido SI; ¿Cuál es el nivel a manera general el compromiso alcanzado por las unidades institucionales?**

Tabla 18. Respuestas pregunta Nro. 2

Indicador	Valor	Porcentaje
Poco satisfactorio	4	80%
Algo satisfactorio	1	20%
Muy satisfactorio	0	0%
Completamente satisfactorio	0	0%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 12. Respuestas pregunta Nro. 2



Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Para la pregunta Nro. 2 el 97 % de usuarios de red NO le han asignado cuenta de usuario y contraseña para acceder a su equipo, ya que no es necesario; solo el 3% de usuarios SI tienen configurado sus equipos para tal efecto.

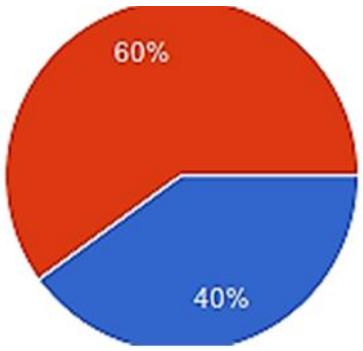
3) **¿Los lineamientos de las políticas se enmarcan en los estándares y normalizaciones de seguridad informática?**

Tabla 19. Respuestas pregunta Nro. 3

Indicador	Valor	Porcentaje
SI	4	40%
NO	6	60%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 13. Respuestas pregunta Nro. 3.



Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

En la pregunta Nro. 3 el 60 % de los administradores y operadores indican que no se enmarcan los lineamientos en políticas de seguridad informática; mientras que un 40% indican que SI se enmarcan dichos lineamientos.

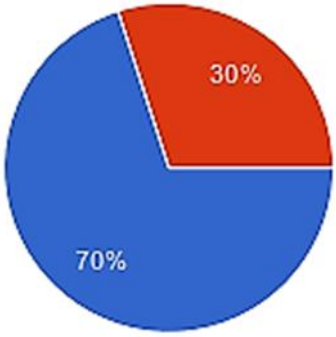
4) **¿Los sistemas hardware de infraestructura institucional están configurados y protegidos en criterios de seguridad informática, en qué medida?**

Tabla 20. Respuestas pregunta Nro. 4

Indicador	Valor	Porcentaje
Poco satisfactorio	7	70%
Algo satisfactorio	3	30%
Muy satisfactorio	0	0%
Completamente satisfactorio	0	0%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 14. Respuestas pregunta Nro. 4



Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

En la pregunta Nro. 4, un 70% de administradores de red y operadores, indican que los equipos están poco configurados a nivel de seguridad, mientras que un 30% indican que si tienen algo más configurados. Por consiguiente existe una deficiencia en la configuración de los equipos en criterios de seguridad y protección.

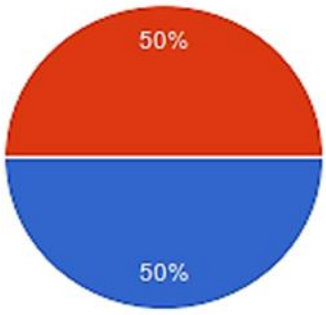
5) ¿Existe un software especial que gestione la seguridad informática de la red, equipos, sistemas y aplicaciones?

Tabla 21. Respuestas pregunta Nro. 5

Indicador	Valor	Porcentaje
SI	5	50%
NO	5	50%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 15. Respuestas pregunta Nro. 5



Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

En la pregunta Nro. 5, la mitad de administradores y operadores de red (50%) emplea algún tipo software que gestione la seguridad y protección de la red; mientras que el otro 50% no lo emplea o desconocen.

6) ¿Existe un hardware especial que gestione la seguridad informática de la red, equipos, sistemas y aplicaciones?

Tabla 22. Respuestas pregunta Nro. 6

Indicador	Valor	Porcentaje
SI	100	100%
NO	0	0%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 16. Respuestas pregunta Nro. 6

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

En la pregunta Nro. 6, se refleja que el 100% de administradores y operadores de red, confían en la gestión realizada por un equipo HW en criterios de seguridad y protección de la red; dicho equipo es un firewall licenciado, marca SOPHOS.

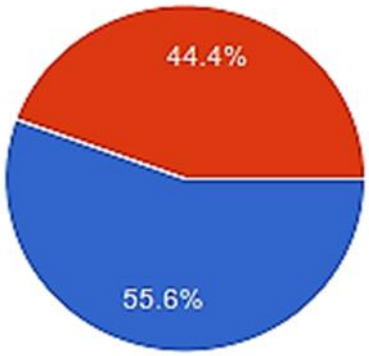
7) ¿Los usuarios de la red e infraestructura informática cuentan con identificación, permisos y contraseñas de acceso?

Tabla 23. Respuestas pregunta Nro. 7

Indicador	Valor	Porcentaje
SI	5	55,6%
NO	4	44,4%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 17. Respuestas pregunta Nro. 7



Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Para la pregunta Nro. 7 indican un 55,6% de administradores de red que si han configurado cuentas para usuarios, mientras el 44,6% no lo han hecho. En consecuencia existe falta de control de accesos y seguridades al ingreso de personal no autorizado.

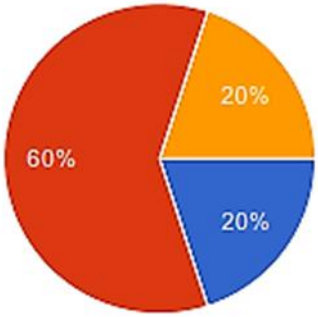
8) ¿Existe un control y seguimiento de usuarios autentificados en la red universitaria?

Tabla 24. Respuestas pregunta Nro. 8

Indicador	Valor	Porcentaje
Ningún control	2	20%
Poco control	6	60%
Muy controlado	2	20%
Completamente controlado	0	0%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 18. Respuestas pregunta Nro. 8



Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

La pregunta Nro. 8. Un 60% de administradores de red indican tener las cuentas de usuario y sus configuraciones poco controladas y seguras, mientras que un 20% no lo han hecho y el otro 20% lo han realizado mayormente controlado. En conclusión NO hay configuraciones controladas y seguras para cuentas de usuarios de la red universitaria, solo una pequeña parte lo tienen.

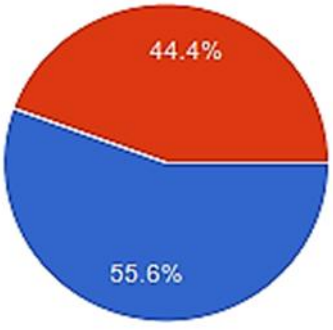
9) ¿Cuentan con alguna aplicación que monitoree la cantidad de penetraciones, ataques mal intencionados y errores en la red?

Tabla 25. Respuestas pregunta Nro. 9

Indicador	Valor	Porcentaje
SI	5	55.6%
NO	4	44.4%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 19. Respuestas pregunta Nro. 9



Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Para la pregunta Nro. 9, un 55,6% manifiesta que si tienen una aplicación para monitorear y controlar la red en criterios de seguridad, ataques y perpetraciones; mientras que el otro 44,4% no lo tiene configurado. Por tal razón se deduce que la red no está totalmente monitoreada y supervisada, dejando todo este ejercicio al departamento de informática de la institución.

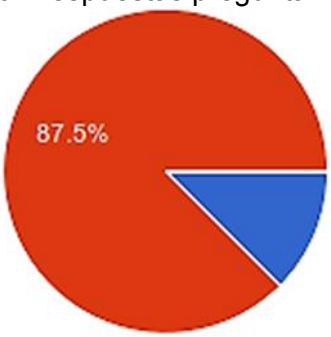
10) Deser positiva la respuesta anterior, ¿En qué medida el contol y s eguimiento de ataques y penetraciones en la red universitaria es ej ecutada?

Tabla 26. Respuestas pregunta Nro. 10

Indicador	Valor	Porcentaje
Poco satisfactorio	1	12.5
Algo satisfactorio	7	87.5%
Muy satisfactorio	0	0%
Completamente satisfactorio	0	0%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 20. Respuestas pregunta Nro. 10



Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

En la pregunta Nro. 10. Un 87,5% manifiesta que algo de satisfacción existe en controlar la red, ya que igual no todos los puntos están monitoreados, controlados y protegidos; mientras que el 12,5% expresa su inconformidad al ejercer esta actividad.

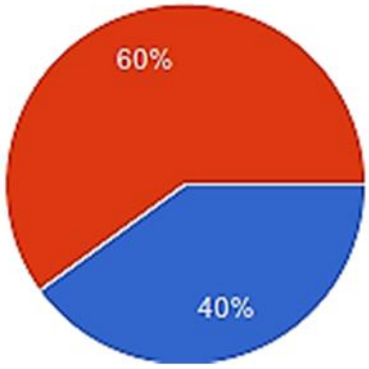
11) ¿La calidad de los servicios y prestaciones de las comunicaciones ante los usuarios, la velocidad de transmisión y las capacidades de ancho de banda?

Tabla 27. Respuestas pregunta Nro. 11

Indicador	Valor	Porcentaje
Poco satisfactorio	4	40%
Algo satisfactorio	6	60%
Muy satisfactorio	0	0%
Completamente satisfactorio	0	0%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 21. Respuestas pregunta Nro. 11



Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Para la pregunta Nro. 11, un 60% manifiesta su algo de satisfacción de la calidad de las comunicaciones y la red, mientras que el 40% se manifiestan con poca satisfacción de la red. En consecuencia se tiene parcialmente la conformidad brindando el servicio de las comunicaciones de red.

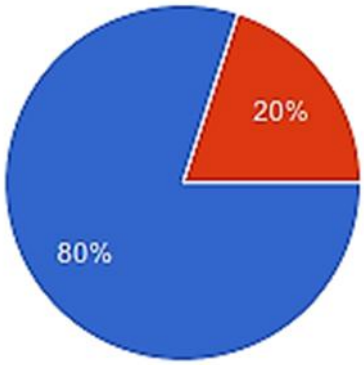
12) ¿La calidad de las conexiones inalámbricas y control de accesos e interbloqueos son?

Tabla 28. Respuestas pregunta Nro. 12

Indicador	Valor	Porcentaje
Poco satisfactorio	8	80%
Algo satisfactorio	2	20%
Muy satisfactorio	0	0%
Completamente satisfactorio	0	0%

Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Gráfico 22. Respuestas pregunta Nro. 12



Fuente: Administradores y operadores de la red
Elaborado por: Geovanny Vega Villacís, Ing.

Para la pregunta Nro. 12, los administradores y operadores de red manifiestan un 80% como poca satisfacción en las redes inalámbricas, mientras que un 20% indican estar algo mejor satisfechos. En consecuencia la mayoría de administradores expresan su inconformidad con las comunicaciones inalámbricas.

4.3.4. Conclusiones Parciales. Administradores de RED.

Se puede evidenciar la falta de procedimientos de seguridad informática debido a que no se ha institucionalizado un plan de seguridad informática que regule las políticas al interior de la red universitaria, ocasionando que no estén normalizados las conectividades de la intranet.

No existe control de acceso de usuarios ni gestor de cuentas para usuarios en la intranet, ya que no hay un controlador de dominio implementado en toda la red universitaria; no están configuradas adecuadamente las diferentes subredes de cada unidad académica.
Carencia de herramientas que ayuden a controlar y supervisar los equipos informáticos por presencia de malwares y virus; fallas en el monitoreo de los equipos informáticos y de red por pérdida de señal o por obstrucción e interferencia.

No existe una adecuada administración de la infraestructura y solo se confía en el trabajo del firewall de hardware SOPHOS para la interceptación de intrusos y control de accesos, el mismo que se encuentra parcialmente operativo por falta de actualización.

Prueba de Chi-Cuadrado en Administradores y Operadores de RED

Variable	Varianza / Rango
Variable I: Servicios de Seguridad y Métodos de Protección en infraestructuras tecnológicas	12 indicadores de Varianza
Variable D: Incidencia en la Intranet de la UTB.	Rango con 4 opciones: *1. No existe* *2. Poca Ocurrencia* *3. Mucha Ocurrencia* *4. Total Ocurrencia*

Aplicando las tabulaciones efectuadas a los 12 indicadores que inciden sobre la seguridad y protección de la red al trabajo realizado por personal administrativo, docente y empleados de la UTB, se observa el siguiente comportamiento empleando el programa MINITAB para Test de Chi-Cuadrado. (*Ver pantalla completa, ANEXO VI*)

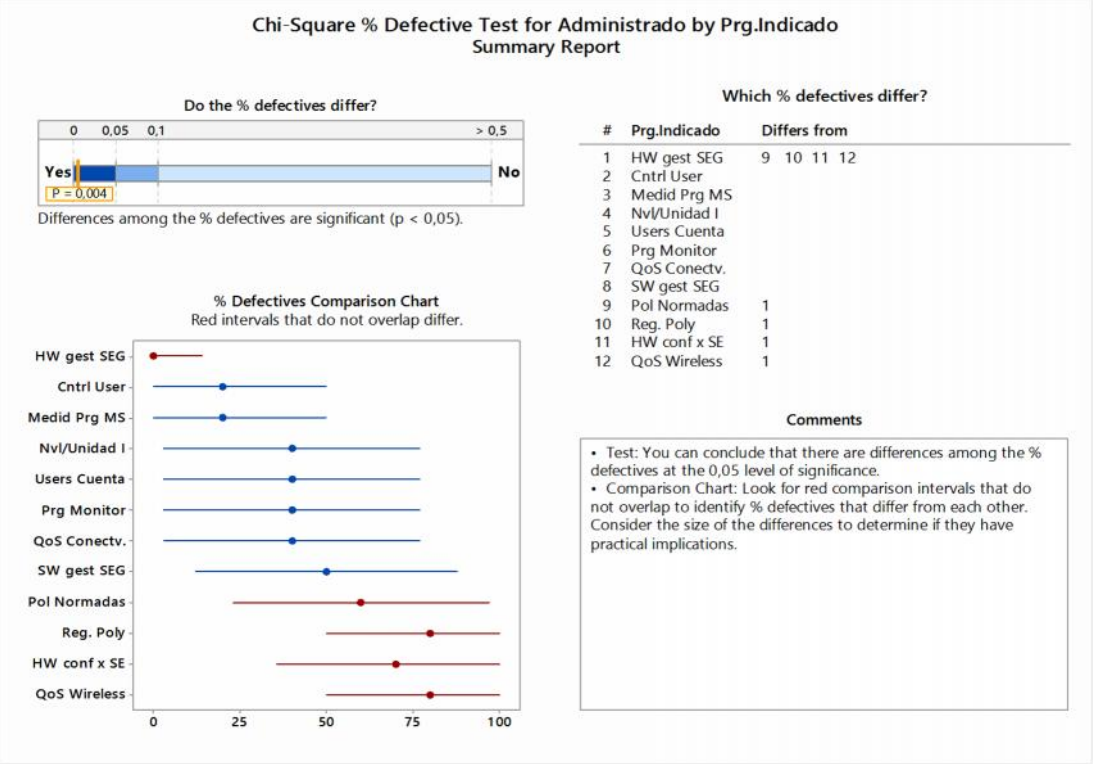


Figura 13. Reporte MINITAB (Chi-Cuadrado), encuestas a Administradores Red.
Elaborado por: Geovanny Vega Villacís

Comentario.- Según el comentario del test aplicando Chi-Cuadrado con MINITAB concluye que:

- Test: Se puede concluir que existen diferencias entre las criterios medidos% en el nivel de significación 0,05.
- Tabla Comparativa: Encuentra intervalos de comparación rojas que no se superponen para identificar% de criterios medidos NO alcanzados que se diferencian unos de otros. Considere el tamaño de las diferencias para determinar si tienen implicaciones prácticas.

"Por consiguiente se NO se aprueba la H0 (Hipótesis Nula), en el que indica que no existe ninguna afectación con la seguridad informática. Como consecuencia al obtener un grado de incidencia menor a 0,05 se aprueba que SI existe incidencia en la seguridad de la intranet de la UTB y puede ser mejorada."

4.4. Análisis del Tráfico de Paquetes para comprobar las vulnerabilidades y amenazas presentes en la intranet de la UTB.

Para proceder con la comprobación de las vulnerabilidades y amenazas que sufre la intranet de la universidad, se desarrolla el siguiente cuestionario de observación de campo y pruebas en SITU.

Tabla 29. Respuestas al formulario de Observación de Campo

Niveles de cumplimiento criterios de red UTB	**GRADO ALCANZADO**				**OBSERVACIONES** 4 = Muy Satisfactorio 3 = Satisfactorio 2 = Poco Satisfactorio 1 = Nada Satisfactorio
	1	**2**	**3**	**4**	
1. Existe personal calificado en Seguridad Informática.			**X**		• Único profesional en redes. • Poca experiencia. • Maneja varias plataformas y equipos.
2. Posee equipos acordes a controlar y supervisar las seguridades informáticas.		**X**			• Único firewall basado en HW para la gestión del tráfico INPUT y OUTPUT. • Equipo licenciado y limitado por falta de renovación.
3. Las conexiones en la institución están enmarcadas a las políticas de seguridad.		**X**			• No existe normativa vigente para las comunicaciones y seguridad informática. • Escasa aplicación de estándares para las comunicaciones.
4. Los sistemas software están correctamente configurados y protegidos a ataques maliciosos.			**X**		• Masificación de antivirus en equipos personales. • Activación predeterminada del firewall de windows.
5. Existe HW especial que supervise, controle y gestione la seguridad informática.			**X**		• Falta configuración del firewall SOPHOS, controlar puertos y aplicaciones. Reglas y ACLs. • Equipo bloqueado por falta de licenciamiento.
6. Coexiste un conjunto de protocolos de red y de aplicación alineadas a nivel de seguridad.	**X**				• Falta configuración de protocolos seguros y normalización de aplicaciones de red. • No existe seguridad de cuentas y accesos de usuarios de red.
7. Existe un portal cautivo que administra el acceso de usuarios a la red.	**X**				• Falta la implementación de portal cautivo para el acceso a la intranet universitaria.

8. El nivel de seguridad está determinado por el Proveedor de Servicio Internet.		X			• NO el proveedor brinda seguridad hasta la entrada al SOPHOS.
9. Calidad de Monitoreo de ataques y perpetraciones maliciosas		X			• Aplicación de utilitarios NO licenciados y limitados.
10. Nivel de Control de ataques e intercepciones maliciosas en la red		X			• Aplicación de utilitarios NO licenciados y limitados.
11. Control de errores y perdidas de información, conectividad y retardos en la transmisión		X			• Persiste errores de conectividad y servicios de red, especialmente wifi.

Fuente: Infraestructura Informática UTB
Elaborado por: Geovanny Vega Villacís, Ing.

Para proceder a las pruebas de testeo en primer lugar se debe identificar la puerta de enlace que permite la Entrada/Salida de paquetes a la intranet universitaria; para ello se ubica la dirección privada y pública del GATEWAY que permite tal tarea siendo en el caso de la UTB, el firewall SOPHOS. Esto se procede realizando una simple consulta de traza y se logra establecer que la IP privada está en el segmento 192.168.0.0/28; mientras que la IP pública asignada es: 181.198.25.129/26. (*Ver figura 14)*

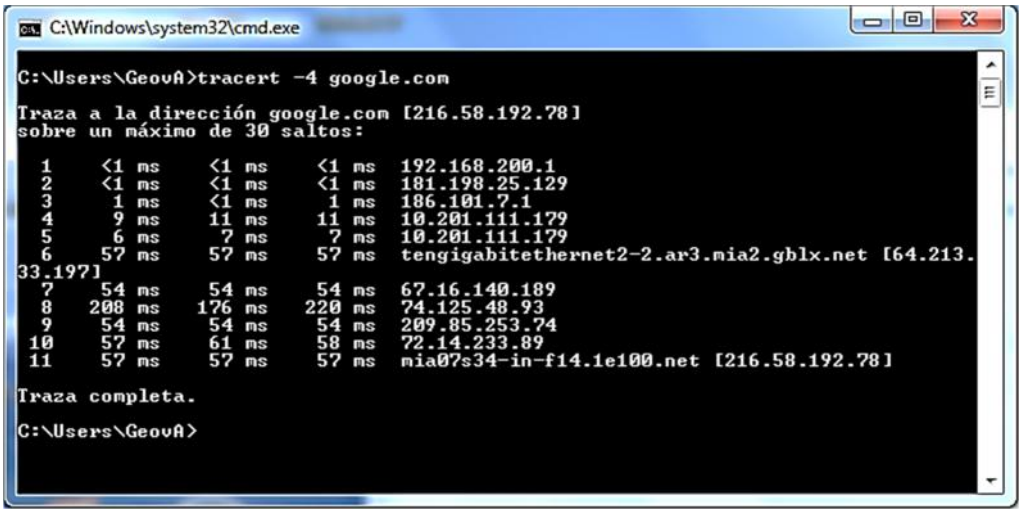


Figura 14. Traza completa identificando equipo Proxy de Salida.
Elaborado por: Ing. *Geovanny Vega Villacís*

1) Traza completa conexión directa al proxy de salida SOPHOS (192.168.200.1) OUTPUT y FORWARD a la red 192.168.19.0
2) Traza completa describe la entrada del proxy SOPHOS (181.198.25.129) INPUT.
3) Usando http://whatismyip.com se obtiene la IP PUBLICA, UTB: (181.198.25.129/26)

4.4.1. Pantallas capturadas durante el análisis de seguridad con inyección de paquetes, malwares y puertos no controlados

Para llevar a efecto la encuesta y responder las preguntas se ejecutó programas testeadores de red e inyectores de paquetes para analizar los tipos, tamaños y calidad de los paquetes.

Se empleó los siguientes programas: *nemesis 1.4, SmartSniff, ZenMap GUI,* del que se obtuvieron los siguientes datos y gráficas correspondientes al firewall SOPHOS que gestiona el tráfico de entrada y salida de la red universitaria.

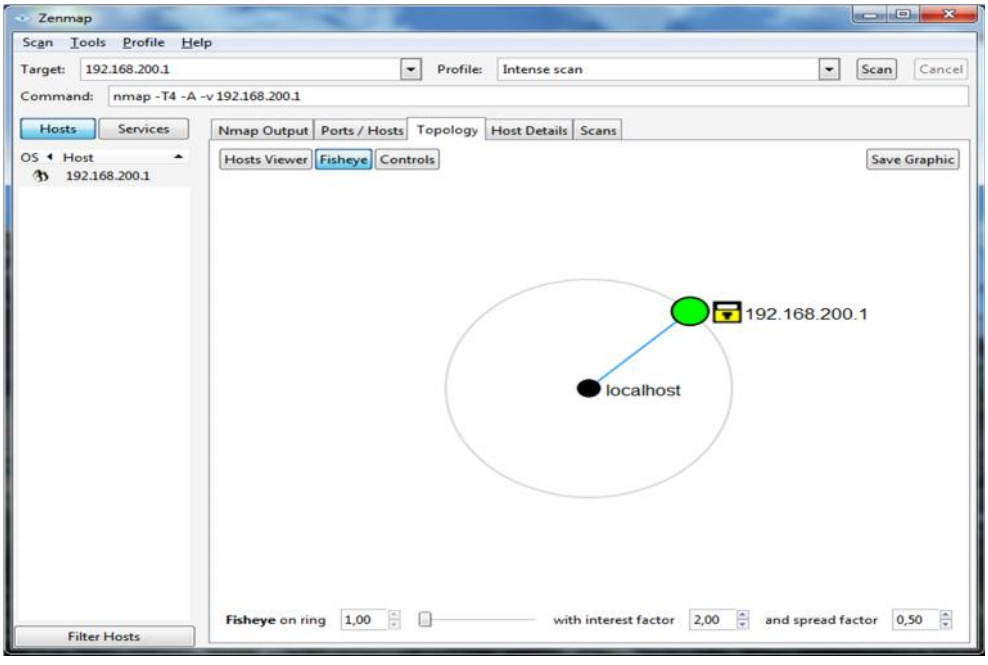


Figura 15. Testeo a la entrada del Firewall SOPHOS. ZenMap 6.4
Elaborado por: Ing. *Geovanny Vega Villacís*

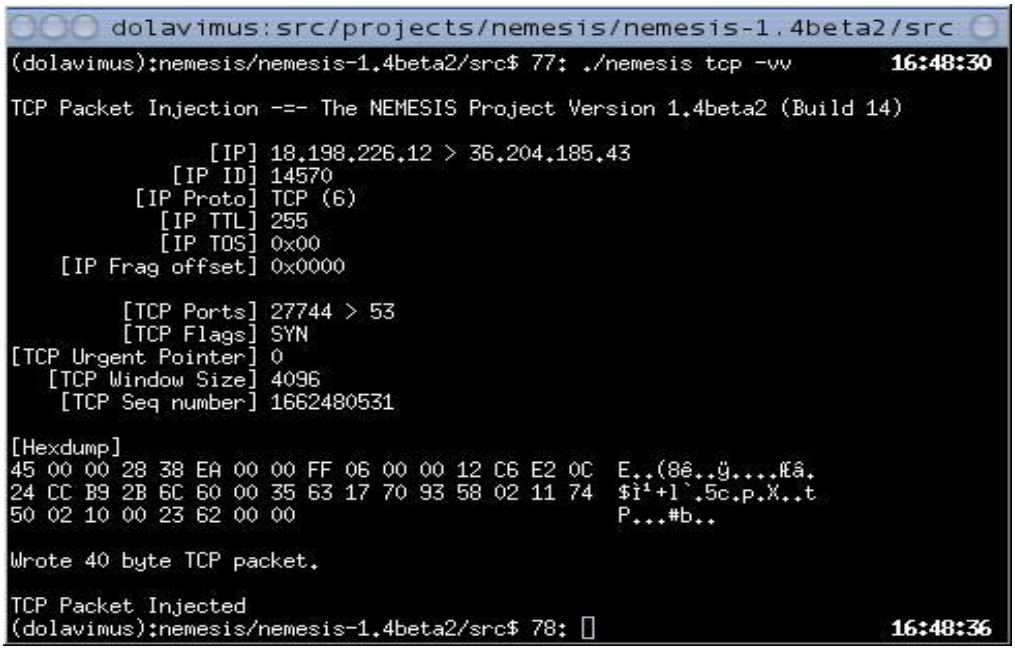


Figura 16. Inyección de Paquetes a la IP (18.198.226.12). Nemesis 1,4
Elaborado por: Ing. *Geovanny Vega Villacís*

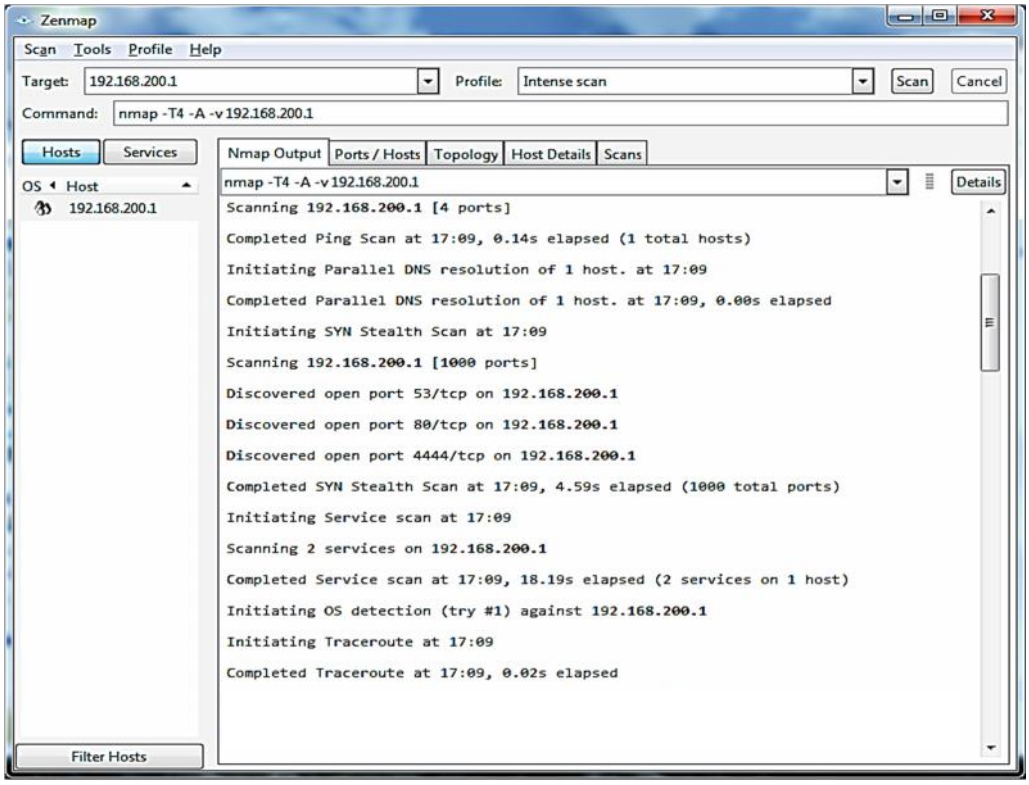


Figura 17. Prueba de Ataques y Perpetraciones a la RED-UTB. ZenMap 6.4
Elaborado por: Ing. *Geovanny Vega Villacís*

La figura 17, visualiza el reporte del análisis de ataques y perpetraciones de paquetes de prueba desde una IP pública 18.198.226.12, usando el programa nemesis 1,4. (Ver archivo completo ANEXO VII)

Los resultados obtenidos son:

- 36 paquetes peligrosos de 2044 enviados,
- 4 puertos no controlados y cerrados por el firewall SOPHOS
- No hay control de paquetes por http, no existe aplicaciones.
- No existen puertos seguros controlados para https, ftps, etc.
- No hay resolución de nombres a direcciones IP's privadas establecidas.
- Ausencia de DNS, no existe control de dominio

4.4.2. Conclusiones Parciales

En consecuencia, de las pruebas realizadas por observación y análisis se concluye que la red de la Universidad Técnica de Babahoyo, está parcialmente protegida y asegurada, dependiendo totalmente de la gestión que realice el FIREWALL SOPHOS, mismo que está bloqueado por la falta de licenciamiento; ocasionando, no poder ser configurado adecuadamente, no hay un software óptimo que optimice el monitoreo, control y gestión de seguridad de la red.

No hay control de dominio, ni un gestor de cuentas de usuario con capacidad de encriptación y cifrado, como Kerberos. Todo el servicio se relega al proveedor de internet y a la plataforma Google para la administración de correos institucional.

4.5. Análisis Comparativo de Bases Metodológicas a ejecutar según datos recolectados e interpretados.

Para proceder a comparar las diferentes bases metodológicas estudiadas: *Defensa en profundidad, Principio de KISS y Desde Arriba hacia Abajo*, se sustentarán en función de la norma internacional para la Gestión de la Seguridad de la Información, **ISO/IEC 2700X**, siendo un marco de trabajo a seguir cuyo objetivo es proporcionar un conjunto de buenas prácticas para la gestión de Seguridad Informática. (LOPEZ NEIRA & RUIZ SPOHR, 2014)

La norma ISO 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044. Para fines de la presente investigación se analizará en resumen ítems claves de los contenidos en las normas ISO 27001, ISO 27002, ISO 27005, ISO 27006 e ISO 27033. Cabe indicar que algunas normas a saber no son de libre difusión sino que han de ser adquiridas. (LOPEZ NEIRA & RUIZ SPOHR, 2014)

ISO 27001.- Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.

- *Objeto y campo de aplicación:* se especifica el objetivo, la aplicación y el tratamiento de exclusiones.
- *Sistema de gestión de la seguridad de la información:* cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma.
- *Responsabilidad de la dirección:* en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.
- *Auditorías internas del SGSI:* cómo realizar las auditorías internas de control y cumplimiento.
- *Revisión del SGSI por la dirección:* cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.

- *Mejora del SGSI:* mejora continua, acciones correctivas y acciones preventivas. (LOPEZ NEIRA & RUIZ SPOHR, 2014)

ISO 27002.- Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

- *Campo de aplicación:* se especifica el objetivo de la norma.
- *Estructura del estándar:* descripción de la estructura de la norma.
- *Evaluación y tratamiento del riesgo:* indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- *Política de seguridad:* documento de política de seguridad y su gestión.
- *Aspectos organizativos de la seguridad de la información:* organización interna; terceros.
- *Gestión de activos:* responsabilidad sobre los activos; clasificación de la información.
- *Seguridad ligada a los recursos humanos:* antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.
- *Seguridad física y ambiental:* áreas seguras; seguridad de los equipos.
- *Gestión de comunicaciones y operaciones:* responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.
- *Control de acceso:* requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.

- *Gestión de incidentes de seguridad de la información:* notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras. (LOPEZ NEIRA & RUIZ SPOHR, 2014)

ISO 27005.- Esta norma establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

- *Fundamentos del proceso de gestión de riesgos.*
- *Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.*
- *Evaluación de los riesgos.*
- *Tratamiento de los riesgos.*
- *Monitorización y revisión de los riesgos.* (LOPEZ NEIRA & RUIZ SPOHR, 2014)

ISO 27006.- Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

- *Campo de aplicación:* a quién aplica este estándar.
- *Requisitos generales:* aspectos generales que deben cumplir las entidades de certificación de SGSIs.
- *Requisitos estructurales:* estructura organizativa que deben tener las entidades de certificación de SGSIs.
- *Requisitos en cuanto a recursos.*
- *Requisitos de información.*
- Requisitos del proceso. (LOPEZ NEIRA & RUIZ SPOHR, 2014)

ISO 27033.- Esta norma da una visión general de seguridad de la red y de los conceptos asociados. Explica las definiciones relacionadas y aporta

orientación de la gestión de la seguridad de la red. Se destina a la gestión de la seguridad, aplicaciones de servicios y/o redes, seguridad de los dispositivos de red y a la seguridad de información que se pasa mediante enlaces de comunicaciones.

- *Gestión de seguridad de redes.*
- *Arquitectura de seguridad de redes.*
- *Escenarios de redes de referencia.*
- *Aseguramiento de las comunicaciones entre redes mediante Gateway.*
- *Acceso remoto*.
- *Aseguramiento de comunicaciones en redes mediante VPNs*.
- *Diseño e implementación de seguridad en redes.* (LOPEZ NEIRA & RUIZ SPOHR, 2014)

A continuación se desarrolla un marco comparativo entre las diferentes bases metodológicas en seguridad informática estudiadas y que se aplican a la investigación realizada tomando como puntos de referencia a controlar, los ítems de cada norma ISO antes detallada; para determinar cuál metodología es la más acorde y que atiende a las necesidades de la presente investigación. *(Ver Tabla 30. Matriz Comparativa de Bases Metodológicas en Seguridad Informática)*

NORMAS ISO/IEC 27000 / BASES METODOLÓGICAS		DEFENSA EN PROFUNDIDAD	PRINCIPIO DE KISS	DESDE ARRIBA HACIA ABAJO
27001	Objeto y campo de aplicación	X	X	X
	Sistema Gestión de Seguridad de la Información	X		X
	Responsabilidad de la dirección	X	X	X
	Auditorías internas del SGSI			X
	Revisión del SGSI por la dirección	X	X	X
	Mejora del SGSI	X		
27002	Campo de aplicación	X	X	X
	Estructura del estándar	X	X	X
	Evaluación y tratamiento del riesgo	X	X	
	Política de seguridad	X		X
	Aspectos Organizativos Seguridad de Información	X	X	X
	Gestión de activos			X
	Seguridad ligada a los recursos humanos	X		
	Seguridad física y ambiental	X		X
	Gestión de comunicaciones y operaciones	X	X	X
	Control de acceso	X	X	
	Gestión Incidentes de la Seguridad Información	X	X	X
27005	Fundamentos del proceso de gestión de riesgos	X	X	X
	Indicaciones en riesgos de Seguridad Información	X		X
	Evaluación de los riesgos	X		
	Tratamiento de los riesgos	X		
	Monitorización y revisión de los riesgos	X	X	
27006	Campo de aplicación	X		X
	Requisitos generales	X	X	X
	Requisitos estructurales	X		X
	Requisitos en cuanto a recursos	X		X
	Requisitos de información	X	X	X
	Requisitos del proceso	X	X	X
27033	Gestión de seguridad de redes	X	X	X
	Arquitectura de seguridad de redes	X		X
	Escenarios de redes de referencia	X		X
	Aseguramiento Comunicaciones con Gateway	X	X	X
	Acceso remoto	X	X	X
	Aseguramiento Comunicaciones mediante VPNs	X	X	
	Diseño e implementación de seguridad en redes	X		X
OTROS	Tiempo más corto para Operar	X	X	
	Uso necesario de presupuesto financiamiento	X		
	Cumplimiento objetivos del negocio	X		X

Tabla 30. Matriz Comparativa Bases Metodológicas en Seguridad Informática
Elaborado por: Geovanny Vega Villacís, Ing.

Finalmente al observar la Matriz Comparativa de Bases Metodológicas en Seguridad Informática, apegadas a las normas ISO 27000; en su mayoría cumple satisfactoriamente la metodología DEFENSA EN PROFUNDIDAD misma a ser adoptada como paradigma en el desarrollo de la propuesta alternativa.

4.6. Discusión y comprobación de la hipótesis en relación a la información obtenida.

Para llevar a efecto la comprobación de la hipótesis es necesario configurar un escenario de prueba donde se evidencie a través de un prototipo de laboratorio, que los diferentes problemas encontrados en materia de seguridad informática en la intranet de la Universidad Técnica de Babahoyo, son minimizados y controlados a nivel de vulnerabilidad, amenazas y debilidades empleando un adecuado sistema de protección y seguridad informática.

Al igual que en las primeras pruebas realizadas, en primer lugar se debe identificar la puerta de enlace que permite la Entrada/Salida de paquetes a la intranet universitaria, la IP del PROXY y del Sistema de Defensa y Monitoreo. Ver figura:

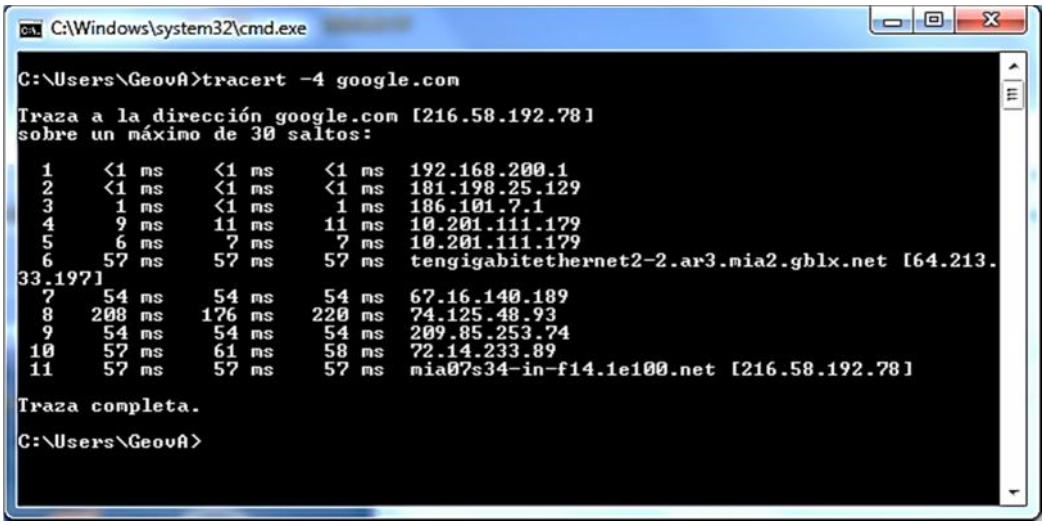


Figura 18. Traza completa identificando Proxy de Defensa.
Elaborado por: Ing. *Geovanny Vega Villacís*

1) Traza completa conexión al proxy de salida SOPHOS (192.168.200.1) OUTPUT y FORWARD a la red 192.168.29.2
2) Traza hacia el PROXY de DEFENSA (192.168.70.1) OUTPUT y FORWARD a la red 192.168.29.2
3) Traza completa describe la entrada del proxy SOPHOS (181.198.25.129) INPUT.
4) Usando http://whatismyip.com se obtiene la IP PUBLICA, UTB: (181.198.25.129/26)

Seguidamente se ejecutó programas testeadores de red e inyectores de paquetes para analizar los tipos, tamaños y calidad de los paquetes, empleando un sistema de protección y detección de intrusos, un sistema de control de puertos y aplicaciones y sistema de monitoreo.

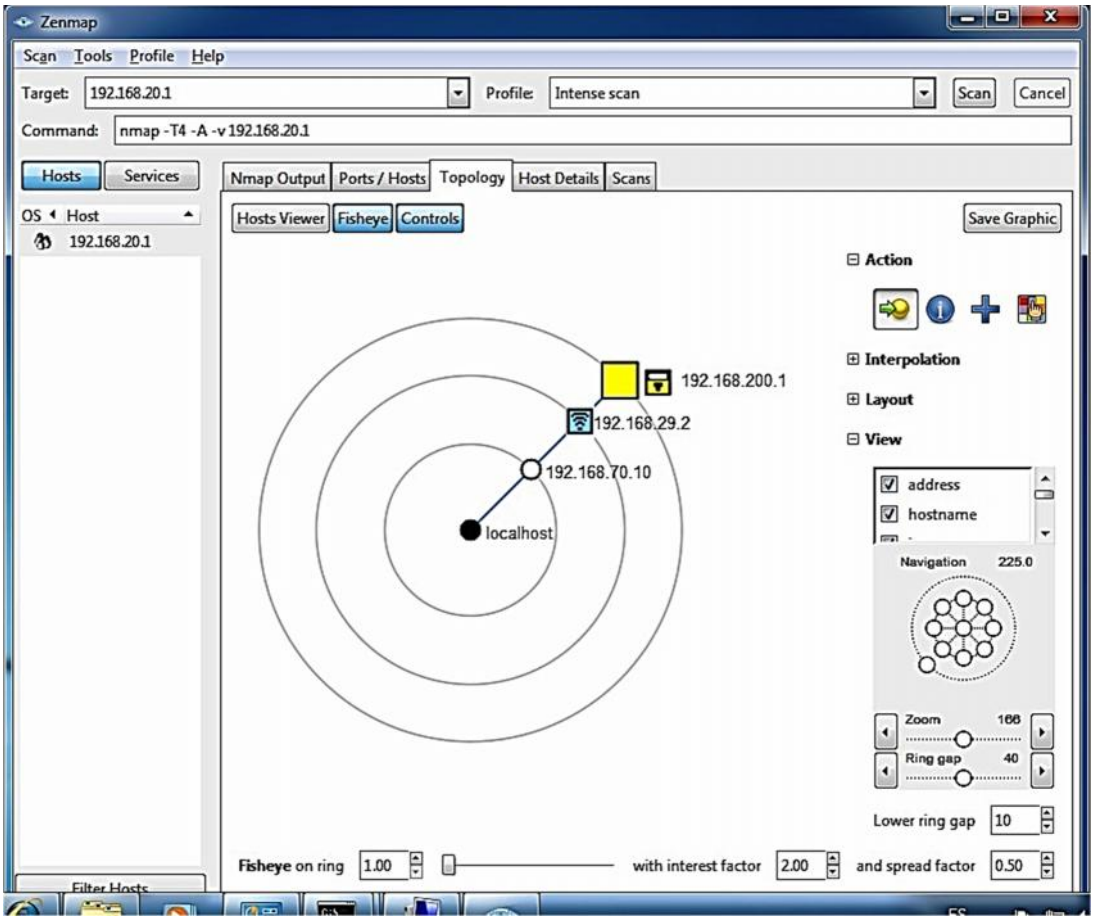


Figura 19. Testeo a la entrada/salida Proxy Seguro y SOPHOS
Elaborado por: Ing. *Geovanny Vega Villacís*

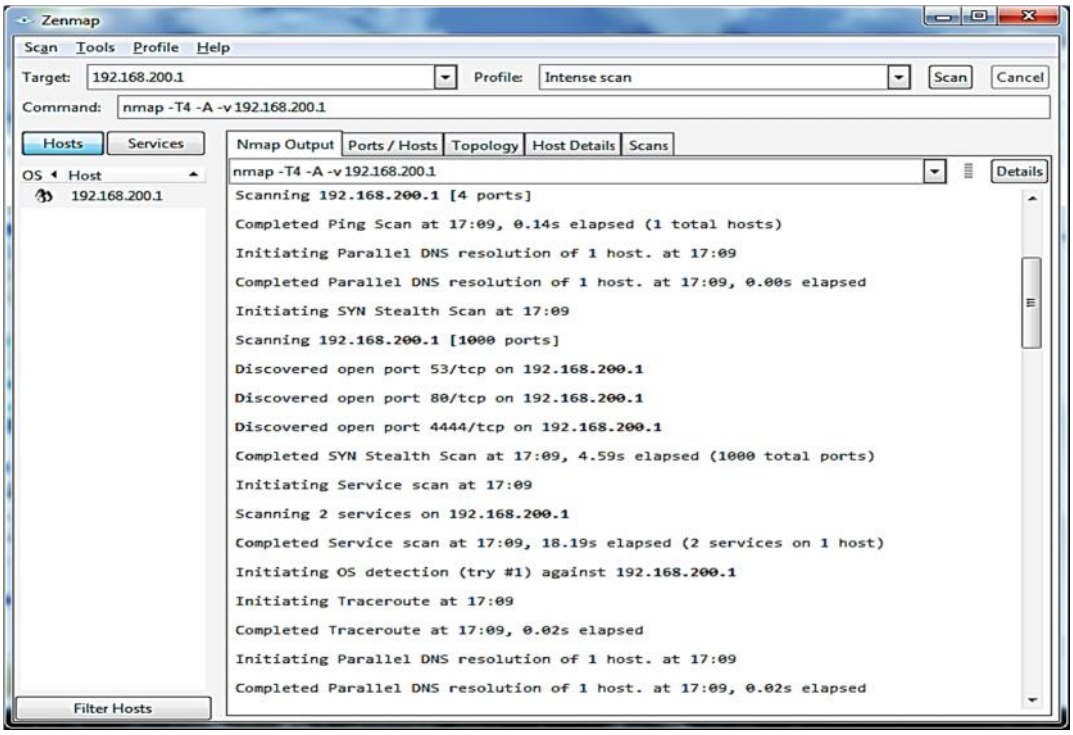


Figura 20. Prueba de Ataques y Perpetraciones a la RED-UTB. PROTEGIDA
Elaborado por: Ing. *Geovanny Vega Villacís*

La figura 20, visualiza el reporte del análisis de ataques y perpetraciones de paquetes de prueba desde una IP pública 18.198.226.12, usando el programa nemesis 1,4.

Los resultados obtenidos son:

- 44 paquetes peligrosos de 2512 enviados,
- 0 puertos no controlados por PROXY de DEFENSA y 4 cerrados por el firewall SOPHOS.
- Existe control de paquetes por http, QoS.
- Existen configurados puertos seguros controlados para https, ftps, etc.

- Hay resolución de nombres a direcciones IP's privadas establecidas.

- Existe configuración de cuentas de acceso por usuario.

- Existe un portal de acceso con permisos delegados para acceder al internet.

- Control total de Dominio y configurado correctamente el servicio DNS para resolución de nombres.

En conclusión una vez terminada las pruebas de laboratorio, ejecutado los diferentes test de observación y completado el formulario de Observación de Campo, se puede evidenciar que*: "Los sistemas de seguridad informática y los métodos de protección en infraestructuras tecnológicas, SI inciden favorablemente en la intranet de la Universidad Técnica de Babahoyo"*

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Una vez concluida la investigación y el análisis de las diferentes vulnerabilidades y amenazas que tiene la red de la Universidad Técnica de Babahoyo, se determinó que existe debilidades e incongruencias en las configuraciones de la red; tal es el caso que no todos los puertos de red están controlados, no existe un monitoreo pormenorizado por segmentos aplicados a cada una de las subredes, no hay un software específico que gestione las actividades de seguridad informática. Falta de procedimientos en seguridad informática y normalización de las comunicaciones.

- Concluida la recolección de información a los diferentes usuarios de red de las unidades académicas, se pudo evidenciar la falta de procedimientos de seguridad en sus equipos informáticos, la carencia de herramientas que ayuden a controlar y supervisarlos, presencia de malwares y ataques constante de virus, fallas en las comunicaciones por pérdida de señal o por obstrucción e interferencia, sea el caso de las redes inalámbricas.

- Con respecto a la información brindada por el personal que administra y opera las redes, se llegó a la conclusión en la falta de procedimientos en seguridad y reglamentados a seguir; así mismo la carencia de herramientas que ayuden a controlar y supervisar los equipos informáticos por presencia de malwares y virus, errores al momento de configurar las comunicaciones por falta de personal adecuado y pertinente, ocasionando pérdida de señal u obstrucción e interferencia entre redes wireless. No existe una adecuada administración de infraestructura y solo se confía en el trabajo que realiza el firewall de hardware SOPHOS para la interceptación de intrusos y control de accesos.

- De las pruebas realizadas por observación y análisis se concluye que la red de la Universidad Técnica de Babahoyo, está parcialmente protegida y asegurada, dependiendo del FIREWALL SOPHOS, mismo que está bloqueado por la falta de licenciamiento y ocasiona que no se lo pueda configurar adecuadamente. No existe un software óptimo que optimice el monitoreo, control y gestión de seguridad de la red.

- No hay control de dominio, ni un gestor de cuentas de usuario con capacidad de encriptación y cifrado para un adecuado control de accesos. Todo el servicio se relega al proveedor de internet y a la plataforma Google para la administración de correos institucional.

- Según lo establece las normas ISO 27000 como marco de trabajo a seguir en actividades de Seguridad Informática, se justificó al comparar varias metodologías a seguir, que en su mayoría cumple satisfactoriamente la metodología DEFENSA EN PROFUNDIDAD misma a ser adoptada como paradigma en el desarrollo de la propuesta alternativa.

5.2. Recomendaciones

- Se recomienda establecer una política aprobada por las autoridades pertinentes en materia de seguridad informática y telecomunicaciones que normen las actividades lícitas tanto para los administradores y operadores de red; usuarios de red (autoridades, personal docente, y administrativo) y hasta los mismos estudiantes al ser parte integral de la intranet universitaria.

- Adquisición de equipos adecuados e implementación de sistemas que articulen una infraestructura tecnológica acorde a las normas y estándares de computo, configurando un Dominio de Red para toda la universidad, segmentando oportunamente a cada una de sus unidades académicas para su propia administración de red y acceso a la WAN; implementación de un portal cautivo para el ingreso de usuarios a la intranet universitaria.

- Configuración de cuentas de usuario basados en una arquitectura jerárquica (*Active Directory*) con encriptación y cifrado de los datos empleando el modelo KERBEROS, elevando la mayor de las seguridades y estableciendo los correspondientes permisos según el tipo de grupo de usuarios a pertenecer.

- Adquirir la licencia respectiva para mejorar las configuraciones de puertos y aplicación basadas en las reglas y ACLs propias del firewall SOPHOS, y

- En especial considerar como tema central del objeto de estudio de la presente investigación; el diseño de una propuesta como alternativa a atender la realidad que aqueja a las telecomunicaciones y seguridades que enfrenta la red de la Universidad Técnica de Babahoyo.

CAPÍTULO VI

PROPUESTA ALTERNATIVA

6.1. Título de la Propuesta

"Diseño de una infraestructura tecnológica segura aplicando el método de Defensa en Profundidad basada en el Sistema Zentyal para fortalecer la intranet de la Universidad Técnica de Babahoyo"

6.2. Justificación

De la realidad eminente que vive la intranet de la Universidad Técnica de Babahoyo y tras de un análisis detallado de las diferentes vulnerabilidades y amenazas que afectan la red universitaria; identificando la existencia de debilidades e incongruencias en las configuraciones de red, un escaso monitoreo pormenorizado a cada una de las subredes, al no existir un software específico que gestione las actividades de seguridad informática, y la falta de procedimientos en seguridad y normalización de las comunicaciones; con llevan a ejecutar medidas correctivas inmediatas para un óptimo desempeño.

No existe dentro de la universidad políticas y normativas que permitan a los diferentes usuarios de la red, actuar en base a procedimientos de seguridad en sus equipos informáticos y la información misma; la carencia de herramientas que ayuden a los administradores a controlarlos y supervisarlos; no existe medidas de defensa ante presencia de malwares y ataques constante de virus, se encuentran con un 38.9% de usuarios afectados. Se convive con fallas en las comunicaciones por pérdida de señal o por obstrucción e interferencia siendo el caso de las redes inalámbricas, con un 82% de errores.

Es necesario configurar adecuadamente el firewall en producción, SOPHOS, mismo que opera a un 40% de su capacidad, ya que no se ha renovado su licencia y su gestión de defensa, monitoreo y control se centra en algunos puertos y aplicaciones, siendo permisivo en otros tipos dejando espacios vulnerables para ataques y perpetraciones.

Se sugiere la implementación de un sistema software de defensa en seguridad informática, con capacidades de administrar y gestionar dominios de red, que se espera llegar atender en forma óptima y reducir las fallas hasta un 85%. Cuentas de usuario encriptadas, mismas que tiene que llegar a su totalidad de usuario con un 98% mínimo de cobertura; aplicación de portal cautivo para el acceso de usuarios al internet e intranet, monitoreo y control de puertos, aplicaciones con defensa ante ataques y perpetraciones de virus y malewares.

Como propuesta para la intranet de la Universidad Técnica de Babahoyo, se presenta el diseño de una infraestructura segura utilizando con las capacidades antes mencionadas y empleando para ello un Sistema *OpenSource* que trabaja sobre plataforma Linux, denominado ZENTYAL y que convive con los sistemas Windows de Microsoft, permitiendo que desde una misma plataforma, facilitar la administración de los servicios.

6.3. Fundamentación

Para llevar a efecto el resultado de la investigación, la metodología a adoptar para el diseño de la propuesta de una infraestructura tecnológica segura, se empleará el método de **DEFENSA EN PROFUNDIDAD,** el mismo que será analizada en la intranet de la Universidad Técnica de Babahoyo, considerando según FABIÁN PORTANTIER, lo siguiente:

> Es una técnica que utiliza varias capas de análisis, en que cada una provee un nivel de protección adicional a las demás capas, ejecutando de adentro hacia afuera Ninguna medida de seguridad puede ser perfecta por lo que es mucho más conveniente tener varias medidas, donde cada una cumpla eficientemente su papel.
>
> La metodología se sustenta en los paradigmas de proteger, detectar y reaccionar. Esto significa que a más de incorporar mecanismos de protección, se debe estar preparado para recibir ataques e implementar métodos de detección y procedimientos de recuperación y reacción.

Es muy importante balancear el propósito de las contramedidas entre los tres elementos primarios de una organización: Personas, Tecnología y Operaciones:

- Personas.- Alcanzar un nivel óptimo de seguridad, comienza con el compromiso de la alta gerencia basados con claro entendimiento de las amenazas. Este debe ser seguido por la creación de políticas y procedimientos, precisión de roles y responsabilidades, asignación de recursos y capacitación. Además es necesario implementar medidas de seguridad físicas y control de personal, monitorizando zonas críticas.
- Tecnología.- Parar asegurar que la tecnología es la adecuada, se debe establecer políticas y procedimientos para adquisición de tecnología; precisando mecanismos de seguridad entre las amenazas y sus objetivos, incluyendo sistemas de protección y detección.
- Operaciones.- Se enfoca en las operaciones necesarias para sostener la seguridad de la organización en las tareas cotidianas, incluye las siguientes medidas: mantener una política clara de seguridad, documentar todos los cambios efectuados en la infraestructura, realizar análisis de seguridad periódicos e implementar métodos de recuperación. (PORTANTIER, 2013)

En el caso de la intranet de la Universidad Técnica de Babahoyo, según éste método en DEFENSA EN PROFUNDIDAD, se procede a realizar el siguiente análisis como posible mejora para atender cada una de las debilidades y vulnerabilidades que presenta la red, como se manifiesta en la presente investigación:

Propuesta para la Intranet de la Universidad Técnica de Babahoyo

La Universidad Técnica de Babahoyo cuenta con una intranet de alrededor de 620 computadoras repartidas entre el edificio central administrativo, las 4 facultades y sus centros de datos, de los diversos departamentos y centros de desarrollo.

Como aspecto general cuenta con una intranet de tipo FastEthernet 1000BaseT para los laboratorios, oficinas administrativas, unidades de desarrollo; ósea, las áreas de trabajo y conexión horizontal. Mientras que las interconexiones física entre las distintas facultades y unidades departamentales se lo realiza a través de una FastEthernet 1000BaseFX, un backbone de fibra óptica multimodo 62.5/125 con topología estrella; según la Figura 18, se aprecian las distancias de fibra óptica y la ubicación física de las áreas. Para la conexión con la facultad de agronomía (FACIAG) se lo realiza con un enlace de microonda.

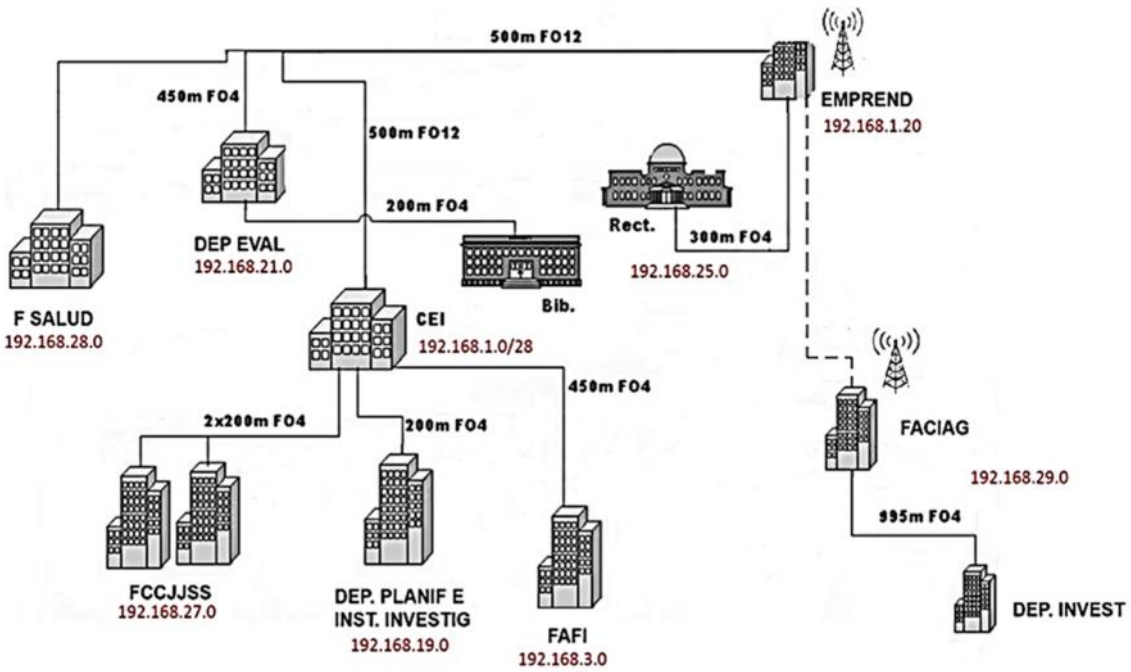


Figura 21. BackBone de la Intranet de la UTB
Fuente: Departamento de Informática

La Universidad asume la dirección de clase C para redes de tipo privadas 192.168.0.0 con mascara de subred 255.255.255.0 para lo cual se realiza la división del tercer byte en subredes, quedando disponibles 255 subredes de 255 hosts cada una. Estas subredes se asignan aleatoriamente entre las diferentes subredes, y las que cuenten con más de 254 máquinas o que por sus condiciones de estructura física no son suficientes en una subred, se le asignaran dos. En estos momentos se encuentran disponible un

número considerable de subredes para uso posterior y futuras ampliaciones.

El dominio asignado por el proveedor para la resolución de nombres es **utb.edu.ec**, del cual se derivan varios espacios de nombre relativos a los diferentes dominios en Windows 2008 Server que existen en su interior. Estos están asignados a las distintas unidades académicas y departamentales, a mencionar los siguientes ejemplos:

fafi.utb.edu.ec	*Facultad de Administración Finanzas e Informática*
fcje.utb.edu.ec	*Facultad Ciencias Jurídicas y Sociales*
fccss.utb.edu.ec	*Facultad Ciencias de la Salud*
faciag.utb.edu.ec	*Facultad Ciencias Agropecuarias*
rectorado.utb.edu.ec	*Rectorado*

En principio cada unidad es totalmente responsable de su sistema informático y conectividad; se proporciona de manera distribuida desde el departamento de Informática, los servicios de correo electrónico, FTP, WEB, bases de datos, y demás aplicaciones en dependencia de las necesidades. De la misma forma se manejaban los usuarios, los grupos de distribución, computadoras, impresoras y políticas de seguridad.

En ese momento no existe ningún tipo de relación de confianza entre unidades de cada facultad y no existían políticas de integración. Esta estructura tenía sobradas deficiencias de manera que es necesario una reestructuración desde el punto de vista lógico. Para lo cual se necesita coordinar esfuerzos para levantar una plataforma robusta, confiable y segura, y a la vez no sea muy costosa apelando al código libre.

Con este objetivo fue creado un controlador de dominio basado en Linux, a través de Zentyal 3,6 con compatibilidad e integración a Microsoft Windows 2008 bajo el espacio de nombre **utb.edu.ec** el cual agrupa como dominio padre a los dominios existentes de cada unidad académica,

estableciéndose entre ellos relaciones de confianza con el objetivo de comenzar la integración y homogenización de los sistemas informáticos.

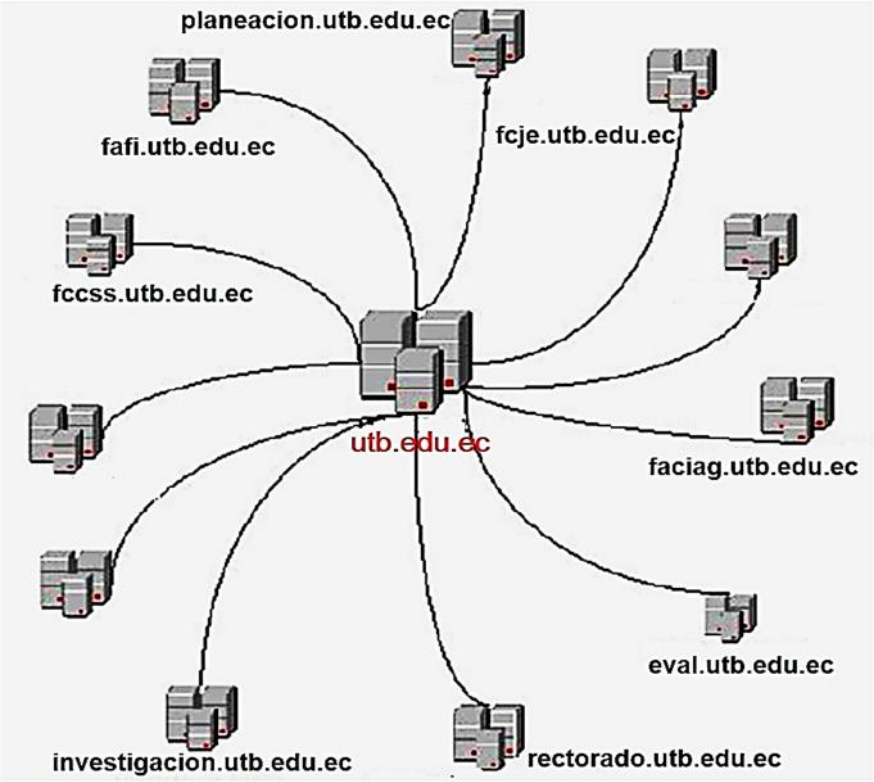


Figura 22. Dominios de la Intranet de la UTB
Fuente: Departamento de Informática

Bajo esta nueva estructura la operatividad se centraliza con el servidor DC (Controlador de Dominio) basado en Linux, Zentyal. Las aplicaciones en el dominio **utb.edu.ec** y el firewall de comunicaciones (SOPHOS) que cuentan con respaldo eléctrico ininterrumpido UPS y condiciones excepcionales de hardware. Por consiguiente se centraliza las aplicaciones de Correo Electrónico, Acceso a Internet, Servidor de ficheros (FTP), Servidor de Bases de Datos (Sistema de Académicos, Moodle, etc.), Portal Cautivo y Servidor de Monitoreo y Control (Nagios).

Las cuentas de usuarios aún se encuentran en cada una de las unidades académicas pero serán migradas hacia el dominio **utb.edu.ec** con el objetivo de lograr una mayor estabilidad. El resto de los dominios no van a desaparecer; ahí seguirán las cuentas de las máquinas, impresoras, y

demás objetos, con el objetivo de que cada dependencia, aplique sus propias políticas de seguridad.

De tal forma se cumple con el objetivo de la metodología ir ejecutando las diferentes tareas de seguridad en cada una de sus unidades o CAPAS internas hacia las más externas, asegurando los datos, las aplicaciones, los equipos y la red considerando las vulnerabilidades y amenazas con sus respectivas correcciones y adecuaciones en sistemas, protocolos, equipos y plataformas de seguridad.

Disponibilidad de conexión a Internet

El acceso de la Intranet hacia la red pública (Internet), se da a través de dos equipos desde un servidor proxy con Linux y el SOPHOS firewall en hardware (DMZ). *(VER ANEXO VIII)*

Zentyal 3,6 basado en Ubuntu Server, están montados los servicios de DNS primario y secundario (Named); Servicio de Proxy (Squid), para el acceso a Internet; Proxy Inverso (Squid). Transporte alterno al gmail de correo entrante y saliente (Sendmail) y servicio portal cautivo. Estos servidores se les conocen con el nombre de servidores reales ya que cuentan con una numeración de IP real para Internet.

Como estos son los equipos que llevan todo el peso de la comunicación de la Intranet con el mundo; se propone para asegurar su disponibilidad un esquema de servidores redundantes; con un total de cuatro máquinas, todos los servicios estarían duplicados como se observa en la *Figura Nro. 20.*

Esta solución se brinda con el objetivo de reducir al mínimo el tiempo de recuperación en caso de que falle algún servicio o sea necesario que cualquiera de estos servidores salga de operación por actualización del

sistema o para análisis forense porque se vio comprometida su seguridad e integridad.

Los servicios redundantes solamente estarían configurados, pero no activados, entrarían en operación solamente si es necesario por las razones antes expuestas y se realizaría de forma manual. Los servidores dedicados son administrados con protocolo SSH desde las máquinas de administración del nodo central. *(VER ANEXO IX).*

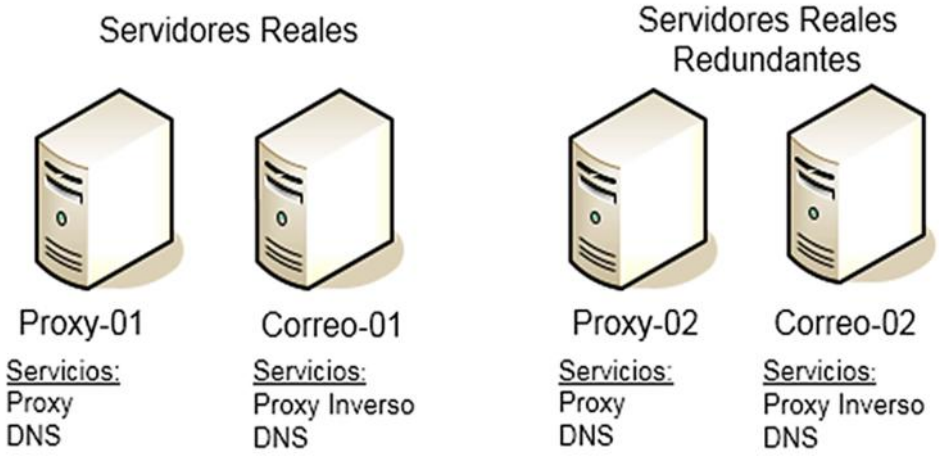


Figura 23. Servidores Redundantes de la UTB
Fuente: Departamento de Informática

Consideraciones de Seguridad en la Intranet UTB

Las estaciones del nodo central integradas por los servidores del dominio **utb.edu.ec**, los servidores reales y las máquinas de administración, pudieran estar en una subred independiente con el objetivo de limitar el dominio de colisiones y brindarles un nivel de seguridad superior, para evitar configurar una Zona Demilitarizada (DMZ).

Esta solución DMZ aunque parezca sensata no es práctica, el tráfico que viaja hacia estos servidores es originado en casi la totalidad de las estaciones de la Intranet, por lo que se crearía un cuello de botella y un deterioro considerable del servicio, que nunca va a ser justificado con los niveles de seguridad brindados. Esta solución se recomienda para redes

más pequeñas, ya que con ella se logra tener un control estricto del tráfico que viaja hacia los servidores.

Los niveles de seguridad en esta situación serán ofrecidos por el firewall de Hardware SOPHOS, el cual puede hacer filtro de paquetes por puertos esta variante es mucho más eficiente puesto que no se afecta para nada el ancho de banda. Este dispositivo tiene además la facilidad de puerto en espejo, mediante el cual el tráfico proveniente de puertos concretos puede ir a parar a un puerto específico en el cual se analizaría el comportamiento del flujo de paquetes con un sistema de detección de intrusos. Este IDS no tendría que analizar todos los paquetes de la subred, sino de los servidores más importantes.

Copias de Seguridad

Como parte de los mecanismos de recuperación, se propone un sistema de copias de seguridad a partir de discos duros. Para guardar los backups de los sistemas operativos de los servidores Windows y la configuración de los servicios ofrecidos en el servidor Zentyal Linux. También se recomienda un sistema de respaldo de hardware, los discos duros que almacenan la parte de la información sensible sean duplicados en RAID 5 - SAS. Además de hacerle copias a los buzones de correo electrónico ofrecido el espacio de G-Mail.

Sistemas de Autentificación en la Intranet de UTB

Los sistemas operativos basados en Windows NT usan como sistema de autentificación LM y NTLM (NT LanManager) incluyendo Windows 2008 Server; y los Windows XP, 7 soportan LM, NTLM y Kerberos.

Para el caso de la red universitaria y sus subredes el controlador de dominio yace en el servidor Zentyal de Linux, el mismo que soporta también dichos tipos de autentificación y en sentido especial aprovecha las potencialidades de KERBEROS. De esta forma y conociendo que el cliente

y servidor negocian el protocolo de autentificación, escogiendo, de todos los que soportan el más fuerte, podremos concluir que los clientes con Windows XP, 7 o superior se autentificarán usando Kerberos, pero los clientes inferiores a Windows 2000 usarán LM o NTLM.

Para una mejor administración de unidades organizacionales, equipos, grupos de usuarios y cuentas se puede integrar las bondades del Protocolo Ligero/Simplificado de Acceso a Directorios (LDAP) que es utilizado sea por la plataforma Microsoft o Linux.

Por esta razón es importante establecer políticas de seguridad; lo cual evitará que por falta de conocimiento o algunas veces hasta por maldad se produzcan problemas ocasionados por las mismas personas. Este es un proceso administrativo apoyado desde la gerencia para que estas medidas tengan el peso necesario.

Figura 24. Componentes a proteger en una infraestructura tecnológica
Fuente: (VANEGAS C, 2013)

Sistema Zentyal 3.6

Es una herramienta que permite gestionar todos servicios de red a través de una sola aplicación; puede actuar como Gateway, Servidor de

seguridad (UTM), Servidor de infraestructura de red, Servidor de comunicaciones y Servidor de Aplicaciones.

Zentyal es un servidor Linux desarrollado en código abierto y que se basa en la distribución Ubuntu Server 10.04 y que proporciona una forma sencilla de configurar un servidor GNU\Linux, para que actúen como Gateway, servidor DNS, DHCP, firewall, backup, servidor VoIP, samba, correo, proxy, etc. Este servidor fue creado con el objetivo de facilitar la administración de los servicios de una infraestructura informática robusta. (NAVARRO, 2014)

Una característica interesante es que puede actuar como controlador de dominio Active Directory y además, puede sincronizarse con otros Active Directory de Microsoft Windows Server, por medio de protocolo LDAP. Se desarrolló con el objetivo de acercar Linux a las pymes y permitirles aprovechar todo su potencial como servidor de infraestructura en código abierto a los productos de Microsoft para infraestructura TIC en pymes. (NAVARRO, 2014)

6.4. Objetivos

6.4.1. Objetivo General

Diseñar una infraestructura tecnológica segura aplicando el método de Defensa en Profundidad basada en el sistema Zentyal para fortalecer la intranet de la Universidad Técnica de Babahoyo.

6.4.2. Objetivos Específicos

- Identificar las necesidades informáticas y la configuración actual de la red y sub-redes de la Universidad Técnica e Babahoyo.

- Identificar las vulnerabilidades y amenazas que tiene la red actualmente, en criterios de seguridad informática para determinar los puntos más críticos a ser atendidos.

- Medir y Testear la red en diferentes puntos, tanto por cable e inalámbricamente para evidenciar los puntos en conflicto, ruptura e interferencia.

- Diseñar un prototipo empleando Zentyal 3,6 de Ubuntu para mejorar los servicios de conectividad, acceso, protección y seguridad; así como también el uso de un portal cautivo.

6.5. Importancia

Una vez demostrado durante el proceso de investigación de campo, que existe una deficiente gestión en seguridad informática en la intranet de la Universidad Técnica de Babahoyo, considerando los aspectos más relevantes en materia se toma como referente los siguientes indicadores:

- Un 69% de usuarios de red desaprueban la gestión informática actual ya que presentan varios inconvenientes desde conectividad, control, seguridad, disponibilidad, entre otros.
- La gestión informática realizada por el mismo personal administrativo y operadores de red, aprueban un 37,5 % una eficiente gestión.
- Mientras que de los datos obtenidos de la misma observación de campo para la investigación, un nivel poco satisfactorio ha alcanzado la red, encontrando múltiples falencias posibles de ser mejoradas.

En tal virtud se presenta la siguiente propuesta de diseño de infraestructura tecnológica segura y ligera, a la vez con capacidades robustas de un servidor integral pero sin licenciamiento en código libre, basada en plataforma Linux. Empleando para tal efecto el sistema Zentyal 3,6 de x86 o en 64 bits para ser usado sobre virtualización.

Teniendo como premisa que es un sistema que se integra muy bien con la plataforma Microsoft sea en sistemas Windows 7, XP, Vista, y otros; ya que

emplea los mismos protocolos de directorio y dominio soportados por LDAP y encriptación con KERBEROS.

6.6. Ubicación sectorial y Física

La propuesta ha de diseñarse en los predios de la Universidad Técnica de Babahoyo y específicamente en el departamento de sistemas informáticos (TICs) de la institución, contando con el apoyo del personal y jefe inmediato.

6.7. Factibilidad

6.7.1. Factibilidad Legal.-

La propuesta alternativa es factible porque está amparada por los siguientes reglamentos vigentes, tanto para la Ley Orgánica de Telecomunicaciones como para la Ley Orgánica de Educación Superior LOES:

En la **Ley Orgánica de Telecomunicaciones** en su **Artículo 3.** Objetivos:

17. Establecer los mecanismos de coordinación con organismos y entidades del Estado para atender temas relacionados con el ámbito de las telecomunicaciones en cuanto a seguridad del Estado, emergencias y entrega de información para investigaciones judiciales, dentro del debido proceso.

En la misma Ley, **Artículo 61.-** Es competencias del Órgano Rector.- Corresponde a la Institución de Educación Superior:

9. Formular las políticas y planes para la creación, regulación y supervisión de la central de datos de la institución, intercambio de información por medios electrónicos, seguridad en materia de información e informática, así como evaluación de su ejecución.

En la **Ley Orgánica de Educación Superior**, de la *CREACIÓN DE UNIVERSIDADES Y ESCUELAS POLITÉCNICAS* en su **Artículo.**

109.- Requisitos para la creación de una universidad o escuela politécnica.

Quien promueva la creación de una universidad o escuela politécnica deberá presentar al Consejo de Educación Superior una propuesta técnico–académica, que contenga los siguientes requisitos:
10. Infraestructuras tecnológicas propias y laboratorios especializados.

6.7.2. Factibilidad de Gestión.-

La gestión de la propuesta es de vital importancia, porque se requiere de una gestión eficiente para hacer posible que los beneficiarios reciban el diseño de la infraestructura tecnológica con éxito.

En cuanto a los recursos a necesitar son los siguientes:

- Laboratorio con conexión a la red UTB y con permisos para efectuar pruebas.
- Equipo informático que soporte los requerimientos mínimos de Zentyal 3,6 en capacidad de procesamiento, memoria y almacenamiento.
- Software de virtualización y para pruebas como cliente Windows (Windows 7)
- Software de testeo de red e inyección de paquetes, Ethreal, Nemesis, Zenmap.
- Personal especializado en el área para configuración de equipos, testeo, pruebas y aportes de conocimiento.

6.7.3. Factibilidad Institucional.-

Es la institución que cuenta como los recursos, materiales y personal que apoyen de manera decidida a conllevar el ejercicio de la propuesta; adicionalmente los rubros son significativos ya que se está trabajando con aplicaciones OpenSource, en las mismas instalaciones y hay disponibilidad de equipos, materiales y herramientas.

6.7.4. Factibilidad Técnica.-

La presente propuesta es totalmente factible desde el punto de vista técnico ya que el escenario que presta la institución, cuenta con todas las instalaciones, herramientas e insumos disponibles para poder ejecutar el diseño que se propone.

Adicionalmente con todo lo expuesto en la investigación, sobra decir la necesidad imperiosa de mejorar la seguridad informática en la intranet universitaria, siendo un proyecto viable a corto plazo.

6.7.5. Factibilidad Social.-

La propuesta es factible a nivel social porque es preciso puntualizar, en los aspectos que se fundamentan la investigación que van acordes a resolver un problema de sentido social, ya que la universidad compuesta de docentes, personal administrativo, autoridades y los estudiantes mismos, viven situaciones incomodas al interior de plantel.

No hay condiciones favorables para la difusión, entrega y adquisición de información rápida y oportuna. En ocasiones la información que se genera fruto del trabajo de cada uno de los usuarios se pone en juego y puede llegar dañarse o peor aún perderse, lo que genera un malestar social.

6.8. Desarrollo de la propuesta

6.8.1. Instalación y Configuración de Zentyal

Se comienza instalando Zentyal con la configuración inicial: Idioma: español, territorio: Ecuador, luego esperar a que se carguen los componentes. (NAVARRO, 2014).

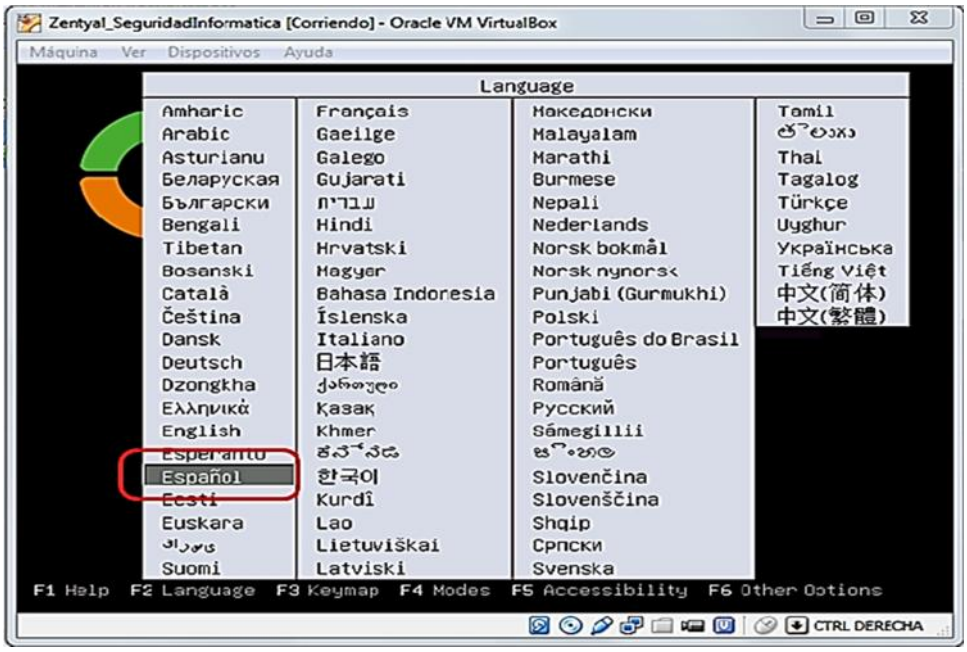


Figura 25. Página inicial instalador de Zentyal
Fuente: (NAVARRO, 2014)

Luego, se configura los parámetros de la tarjeta de red y las configuraciones de red.

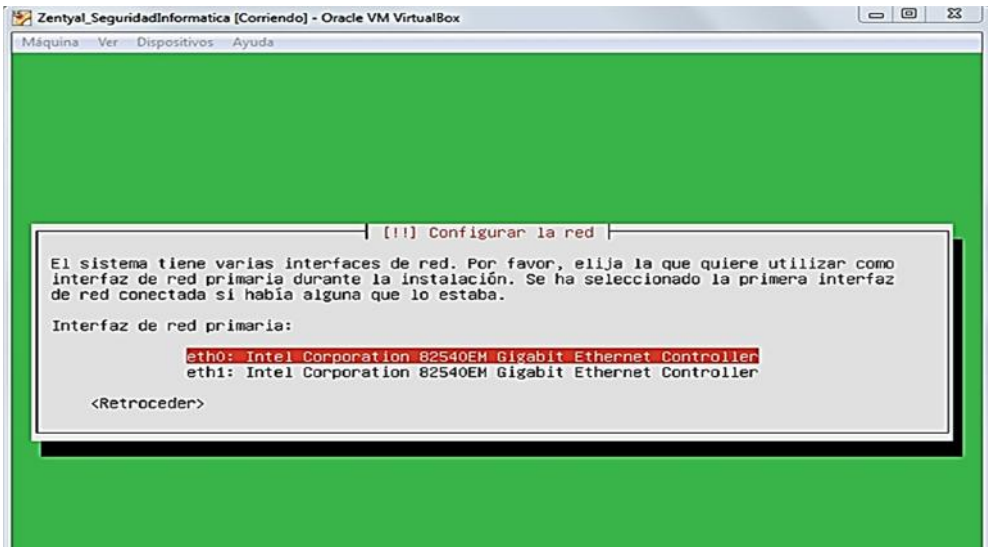
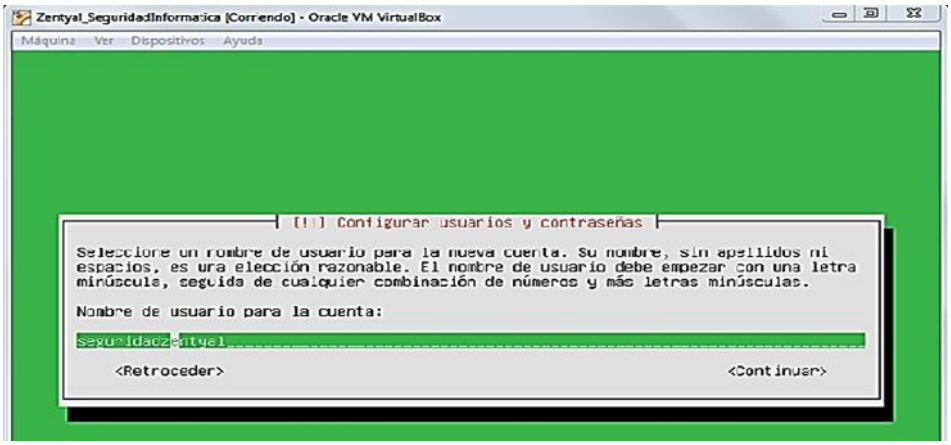


Figura 26. Configuración de tarjetas y parámetros de red Zentyal

Fuente: (NAVARRO, 2014)

Seguidamente se crea una cuenta de usuario y una contraseña.



Contraseña

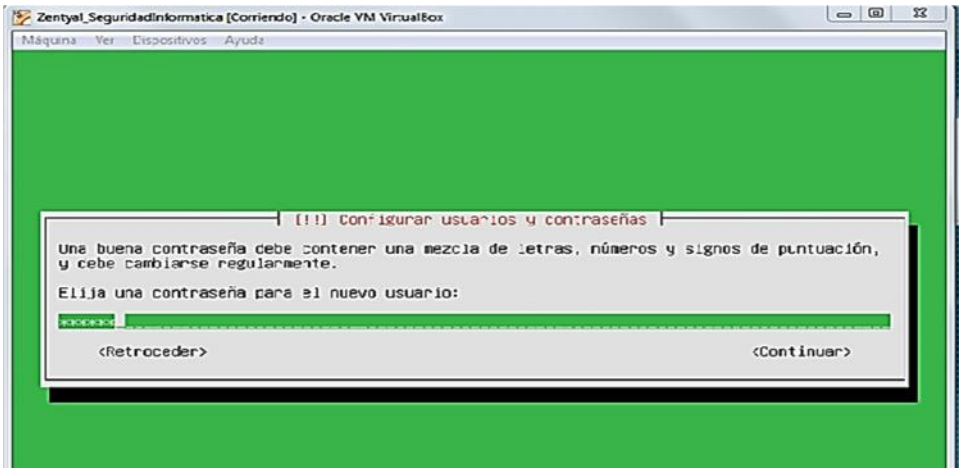


Figura 27. Configuración de cuenta de usuario (User y Password)
Fuente: (NAVARRO, 2014)

Una vez concluida la instalación de Zentyal, el equipo debe reiniciarse e ingresar con la pantalla principal de Zentyal

Figura 28. Reinicio de Zentyal y subida de servicios
Fuente: (NAVARRO, 2014)

Se observa cómo se inicia la carga del sistema y se instalan paquetes adicionales, hay que esperar unos minutos.

Figura 29. Ventana inicial de entrada a Zentyal
Fuente: (NAVARRO, 2014)

Se inicia sesión con el nombre de cuenta y contraseña previamente creadas en la instalación

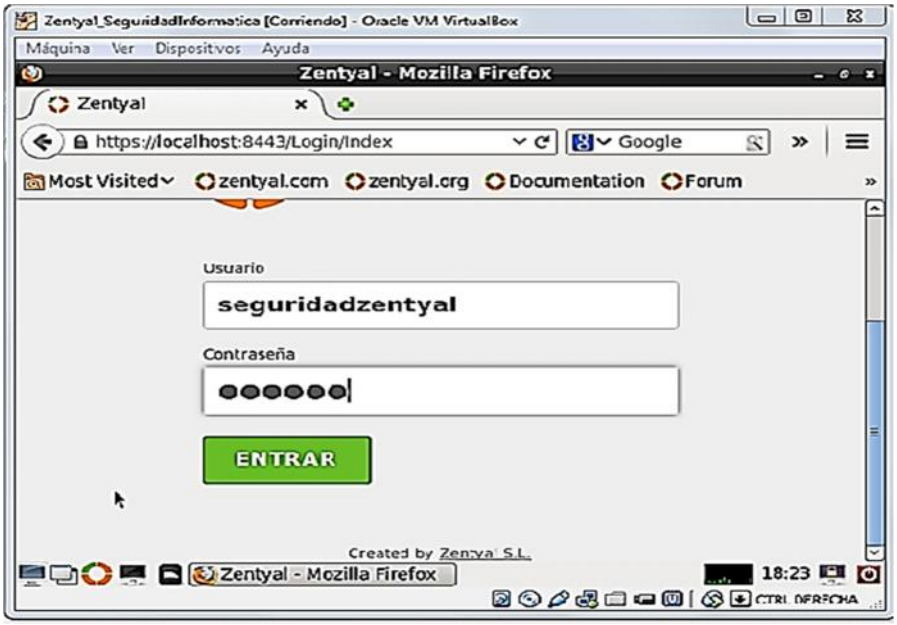


Figura 30. Ventana inicio sesión de Usuario Zentyal
Fuente: (NAVARRO, 2014)

La configuración inicial se la realiza la primera vez que se ingresa al sistema con el usuario y contraseña que son generadas durante el proceso de instalación de Zentyal. En la misma interfaz web de autenticación se presentará un asistente. (VANEGAS C, 2013)

Figura 31. Configuración de Zentyal – Selección de paquetes
Fuente: (VANEGAS C, 2013)

Como paso inicial de configuración, Zentyal permite escoger las funcionalidades que se desean agregar al sistema original. Al momento de seleccionar alguno de los roles que se encuentran en la parte superior se despliegan los paquetes que se pueden instalar y

configurar. Estos roles son: Gateway, Infraestructura, Oficina y Comunicaciones.

- Gateway: su función principal es la de actuar como puerta de enlace con accesos seguros a Internet, protegiendo las redes locales contra ataques externos. Además permite conexiones seguras entre redes locales con redes externas a través de enlaces de internet.
- Infraestructura: este rol se encarga proveer herramientas para la gestión de la infraestructura de la red. Entre ellos se incluyen DNS, DHCP, HTTP.
- Oficina: este rol tiene como finalidad administrar los recursos compartidos que posee la red, sean estos usuarios, grupos, impresoras, ficheros, etc.
- Comunicaciones: este rol provee herramientas para gestionar las comunicaciones dentro de la empresa, entre los que se encuentran los servicios de mensajería, correo electrónico y servicios similares como voz IP. (VANEGAS C, 2013)

6.8.2. Configuración del Servidor Zentyal

La configuración del servidor principal del centro consiste en realizar los cambios necesarios en el mismo para que proporcione acceso a Internet con balanceo de carga entre dos puntos de acceso, los servicios básicos de red y los niveles de seguridad requeridos. (BERMEJO S, 2012)

Acceso a Internet y balanceo de carga

Para tener acceso a Internet desde la red local lo primero que hay que configurar son las interfaces de red.

Figura 32. Configuración Interfaces de Red
Fuente: (BERMEJO S, 2012)

A continuación se configuran las puertas de enlace. Con más peso, la predeterminada ADSL Dinámica.

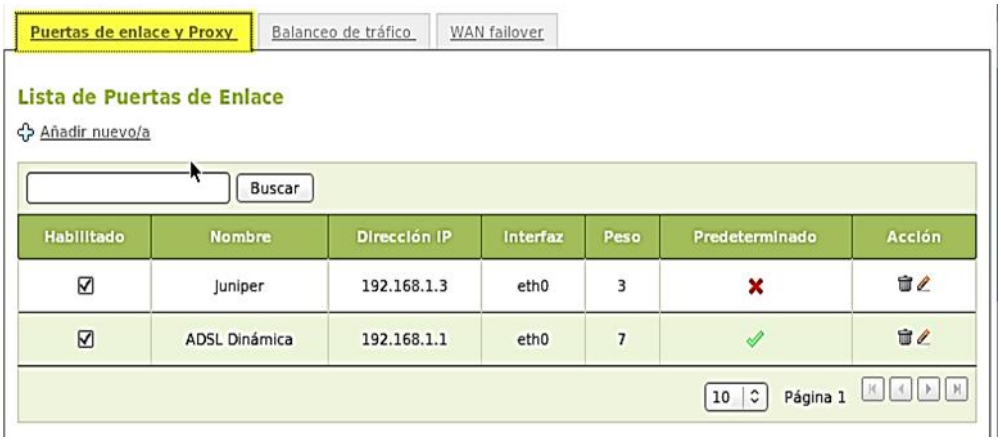


Figura 33. Configuración de las Puertas de Enlace
Fuente: (BERMEJO S, 2012)

Servicio DNS

La configuración de DNS Zentyal se basa en el servicio bind. Se añadió a ZentySrv como primer servidor DNS y en segundo lugar las DNS de google. (BERMEJO S, 2012)

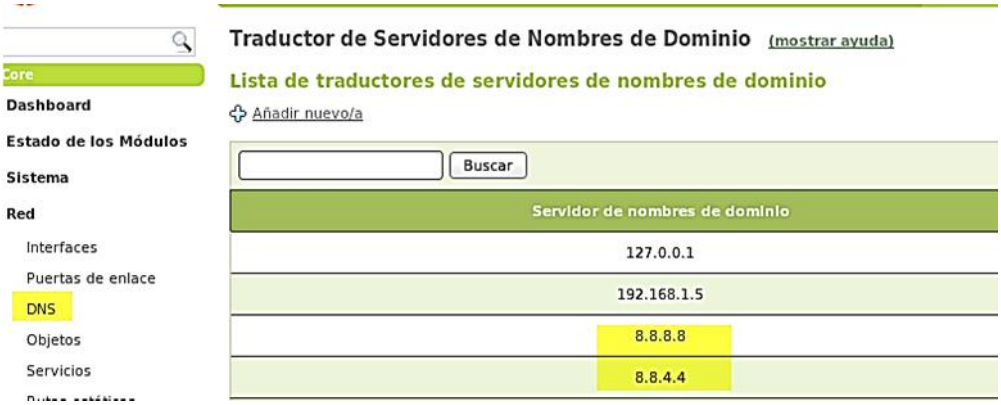


Figura 34. Instalación de Servicio de DNS - Zentyal
Fuente: (BERMEJO S, 2012)

Se habilitó la caché de DNS transparente desde la opción DNS del módulo infraestructura una vez habilitado el módulo DNS. Se mantiene el nombre elegido para la universidad del dominio local, **utb.edu.ec**. Se añadieron los dominios y subdominios solicitados. (BERMEJO S, 2012)

Figura 35. Configuración del DNS
Fuente: (BERMEJO S, 2012)

Servicio DHCP

La configuración de DHCP lleva implícito la configuración en este caso de cinco interfaces, eth0, VLAN33, VLAN34, VLA35 y VLA36

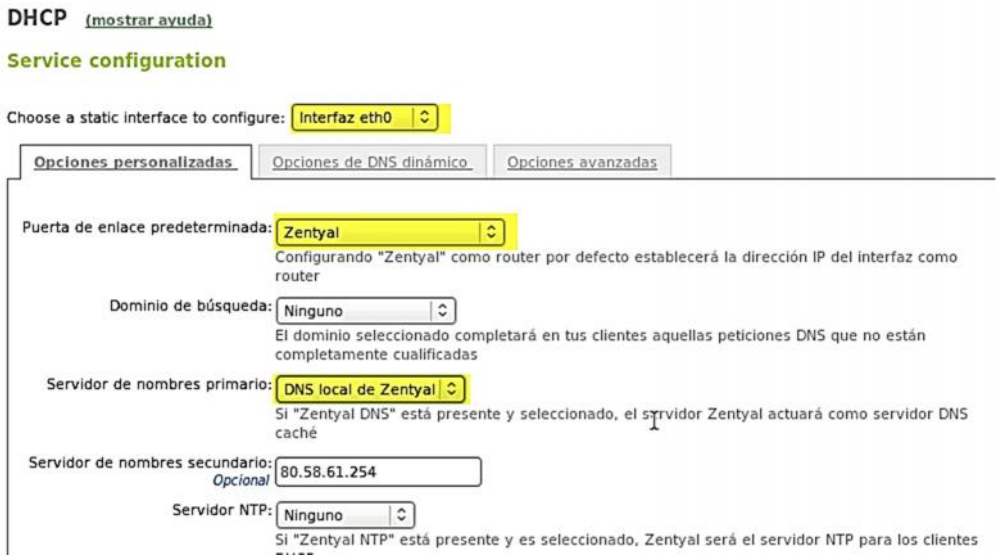


Figura 36. Configuración del DHCP
Fuente: (BERMEJO S, 2012)

Servicio PROXY

Un proxy es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud. (NAVARRO, 2014)

Servidor HTTP

Este tipo de servidor opera en la Capa de aplicación de TCP/IP. El puerto de comunicación de entrada debe ser 80/http según IANA.1Aunque generalmente suelen utilizar otros puertos de comunicación como el 3128, 8080 o el 8085. (NAVARRO, 2014)

Servidor HTTPS

Este tipo de servidor opera en la Capa de aplicación de TCP/IP. A diferencia de un Servidor HTTP, funciona bajo tecnologías de cifrado

como SSL/TLS que proporcionan mayor seguridad y anonimato. El puerto utilizado varía, aunque debe ser 443/https. (NAVARRO, 2014)

Para la configuración del proxy en zentyal seguimos los siguientes pasos.

1. primero escogemos la opción de proxy http la seleccionamos y le damos clic en instalar

2 Se dirige a la configuración del proxy chuleamos la opción que dice proxy transparente escribimos el puerto.

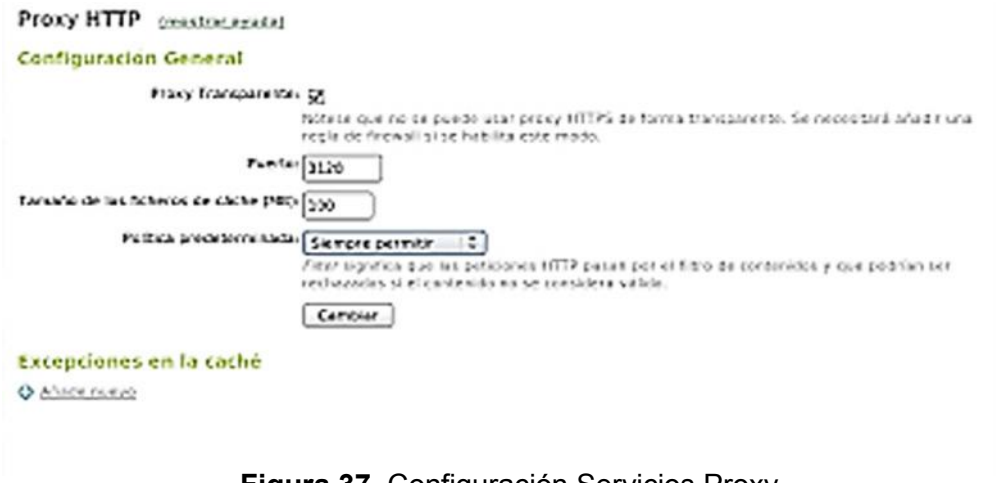


Figura 37. Configuración Servicios Proxy
Fuente: (NAVARRO, 2014)

PORTAL CAUTIVO

1. Se realiza la instalación de los módulos y paquetes necesarios para su configuración: Bandwidth Monitor, Captive Portal, DNS service, Firewall, UserCorner, User and Computers y Web Server.

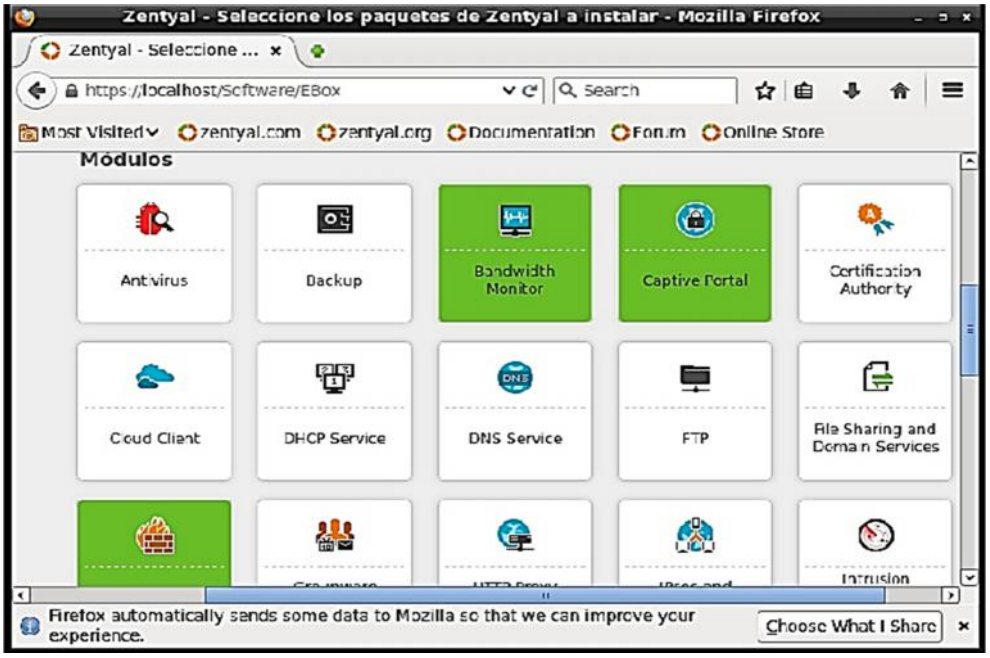


Figura 38. Instalación de Zentyal – Selección de paquetes Portal Cautivo
Fuente: (VANEGAS C, 2013)

2. Se habilita las opciones que se instalamos anteriormente y guardamos los cambios.

3. Vamos a portal cautivo, buscando en el menú la opción y nos muestra las siguientes opciones, primero realizamos la configuración para que sea 1 día, pero esto es independiente a la necesidad. Después guardamos los cambios:

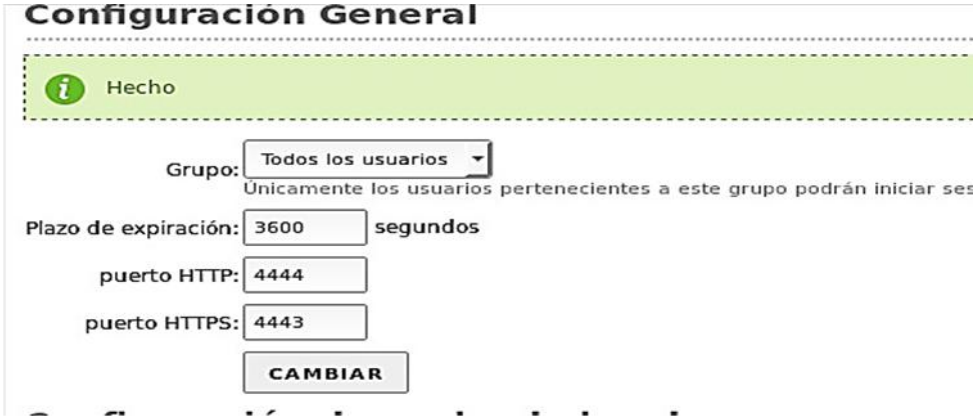


Figura 39. Configuración de Zentyal – Portal Cautivo
Fuente: (VANEGAS C, 2013)

6.9. Impacto

El impacto que concebirá la aplicación de la presente propuesta al ser adoptada por las autoridades de la Universidad Técnica de Babahoyo, será favorable ya que se mejorará en todos los aspectos mencionados en la investigación, donde se presentan fallas, errores o hay escaseo por la falta de procedimientos.

En lo que tiene que ver con la exactitud de la herramienta, se puede observar que cada una de las funciones que tiene Zentyal va siempre enfocada a la solución de un problema o a la ejecución de un proceso específico al servicio de infraestructura ausente en cada unidad académica o administrativa y por consiguiente de toda la red universitaria; es por esta razón que esta característica es bien cumplida por la herramienta (VANEGAS C, 2013)

Como se puede observar en la siguiente *Figura Nro. 34* las funciones apuntan a procesos específicos, cada uno de los roles se dividen en procesos más pequeños. Cada uno afecta directamente a una parte de la red, por ejemplo: Proxy, Cortafuegos, Usuarios, Webmail, etc. (VANEGAS C, 2013)

Figura 40. Funciones Instaladas de Zentyal
Fuente: (VANEGAS C, 2013)

Entonces en base a este análisis, su exactitud es alta con respecto a las funcionalidades que realiza la herramienta, según se detalla en la siguiente tabla:

REFERENCIA	SI	NO	VALOR
Funciones para procesos específicos	X		3,33%
Grupos o roles bien definidos	X		3,33%
Subprocesos bien definidos	X		3,33%
		TOTAL	**100%**

Tabla 31. Configuración de Zentyal – Portal Cautivo
Fuente: (VANEGAS C, 2013)

Para corroborar los criterios mencionados y que validen que, Zentyal como herramienta OpenSource es viable y rentable para la implementación de una infraestructura tecnológica segura, se puede acudir a las evaluaciones realizadas al prototipo como propuesta de diseño y obtener las mediciones necesarias que la validen.

6.10. Evaluación

La evaluación del prototipo como diseño de una infraestructura tecnológica segura para la UTB, es la fase más significativa del proyecto ya que el sistema será evaluado antes de que entre a producción; es decir opera en un entorno simulado, con usuarios reales.

En el caso del proyecto con Zentyal, el entorno simulado es el mismo en el que se realiza las actividades más críticas de la red de la universidad y las cuales presentan errores considerables, también se realiza pruebas parciales de validación con respecto a las diferentes unidades académicas y administrativas. Los usuarios son docentes, personal administrativo y operadores de red. (VANEGAS C, 2013)

En el caso del diseño de red empleando Zentyal, se realizan tres tipos de pruebas exhaustivas:

Pruebas de funcionalidad:

Junto con el personal involucrado en el proyecto (profesores técnicos de informática, personal de administración y operadores), para probar los casos más típicos de configuración de las tarjetas de red y acceso a Internet, así como de accesibilidad o no a otros puntos de la red.

Prueba de tolerancia a fallos:

Para comprobar que se mantiene el acceso a Internet aunque uno de los routers o servidores según sea el caso, no preste servicio.

Pruebas de carga:

Para valorar los límites reales del sistema. Una vez que el sistema comienza su ciclo de explotación, estas pruebas se realizan directamente con los usuarios finales a medida que van haciendo uso del mismo

6.11. Instructivo de Funcionamiento

La presente propuesta lo que entregará en un diseño de infraestructura tecnológica segura para que pueda ser adoptada en la intranet de la Universidad Técnica de Babahoyo; por consiguiente, no existe un producto totalmente terminado para su implementación y ejecución, que trae consigo la elaboración de un manual de funciones o también llamado manual de usuario.

REFERENCIAS BIBLIOGRÁFICAS

- AGUIRRE JORGE, R. (2003). *Curso de Seguridad Informática y Criptografía.* Madrid: Universidad Politécnica de Madrid España.
- ARCOTEL, A. d. (2015). *LEY ORGANICA DE TELECOMUNICACIONES.* Quito: Registro Oficial Suplemento 439.
- BENALCÁZAR Z., J. (2008). *Bases Jurídicas y Técnicas para un Proyecto de Creación de notarias digitales para migrantes".* http://repositorio.iaen.edu.ec/bitstream/24000/400/1/IAEN-M031-2008: Instituto de Altos Estudios Nacionales.
- BERMEJO S, G. (2012). *Gestión de la red de un IES con Zentyal.* San Francisco: Creative Commons.
- CASAS, A. (30 de octubre de 2014). *Revista Digital CSO Computerworld.* Recuperado el 15 de abril de 2015, de CSO Computerworld: http://cso.computerworld.es/seguridad-en-cifras
- DORASWAMY, N. (2013). *IPSec: The new Security Standard for the Internet.* (2nd Edition ed.). Upper Saddle River, NJ.: Prentice-Hall.
- GARCIA M., W., & VARGAS J., A. (2005). *Estudio Técnico para la Implementación de una Autoridad Certificadora para el CTT-ESPE CECAI .* Sangolqui: ESCUELA POLITECNICA DEL EJÉRCITO.
- Gobierno Provincial de los Rios. (2011). *Plan de Contingencia ante Inundaciones del Cantón Babahoyo.* Babahoyo: GADPLR.
- HIROAKI, H., MASAFUMI, & YOUKI, K. (2003 E86-D(11)). A Layer-2 Extension to Hash-Based IP Traceback. *IEICE Transactions on Communications*, 2325-2333.
- IBM Co. Sala de Prensa. (16 de Enero de 2015). *IBM - Sala de Prensa.* Recuperado el 20 de abril de 2015, de IBM presenta el z13, el sistema informático más potente y seguro de la historia.: http://www-03.ibm.com/press/es/es/pressrelease/45866.wss

- INCIBE. (11 de 03 de 2015). *Instituto Nacional de Ciberseguridad.* Obtenido de: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/seguridad_desde_inicio

- LLERENA FUENMAYOR, M. A. (2006). *DESARROLLO DEL MANUAL DE SEGURIDADES INFORMÁTICAS DE LA ARMADA DEL ECUADOR.* ESPOL. Sangolquí: ESPOL.

- LOPEZ NEIRA, A., & RUIZ SPOHR, J. (12 de Noviembre de 2014). *ISO 27000.es.* Obtenido de: http://www.iso27000.es/download/doc_iso27000_all.pdf

- LUCENA LÓPEZ, M. J. (2010). *Criptografía y Seguridad en computadores.* Jaén: Universidad de Jaén.

- LUDWIN, M. (2006). *The Little Black Book of Computer Virus.* Arizona, American: Eagle publications, Inc.

- MCLURE, S. (2010). *Hackers 6: secretos y soluciones para seguridad de redes* (Sexta ed.). México DF.: McGraw – Hill.

- MORENO, L. (14 de noviembre de 2008). *Transacciones seguras (III)*. Obtenido de: http://usuaris.tinet.cat/acl/html_web/seguridad/ssl/ssl_3.html

- NAVARRO, A. &. (2014). *FIREWALL ZENTYAL.* Cúcuta: Universidad Francisco De Paula Santander.

- OPPLIGER, R. (2014). SSL and TLS Theory and Practice. En R. OPPLIGER, *SSL and TLS Theory and Practice* (págs. 94-116). Norwood: Artech House.

- PORTANTIER, F. (2013). *Gestión de la Seguridad Informática.* Buenos Aires: Fox Andina.

- PORTILLO, S. (06 de Septiembre de 2012). *Prezi - Historia de la seguridad informatica.* Obtenido de Historia de la seguridad informatica: https://prezi.com/vnbaj88nuq0p/historia-de-la-seguridad-informatica/

- SENESCYT, S. N. (2012). *LEY ORGANIZA DE EDUCACION SUPERIOR.* Quito: Registro Oficial Suplemento.

- SEOANE, C., SAIZ, A., FERNÁNDEZ, E., & FERNÁNDEZ , L. (2013). *Seguridad informática.* Madrid: McGraw-Hill.

- STANGER, J. &. (2001). *Hack Profing Linux.* Rockland, MA.: Syngress Publishing, Inc.

- SUAREZ I., M. (2011). *Monografías.COM.* Obtenido de Cálculo del tamaño de la muestra: http://www.monografias.com/trabajos87/calculo-del-tamano-muestra/calculo-del-tamano-muestra.shtml

- Symantec Corporation. (20 de enero de 2015). *Symantec Internet Security Corporation*. Recuperado el 20 de abril de 2015, de Symantec Internet Security Threat Report: http://www.symantec.com/security_response/publications/threatreport.jsp

- TANENBAUM, A. S. (2003). *Redes de Computadoras* (Cuarta Edi. ed.). México DF.: Pearson Educación.

- TRUJILLO M., E. (2006). *Diseño e Implementación de una VPN en una empresa comercializadora utilizando IPSec.* Quito: Escuela Politécnica Nacional.

- TSUKAMOTO, K. (2002). An Experimental Study on IPSec. *IEICE Transactions*, E85-A(1): 175-180.

- VANEGAS C, A. (2013). *Zentyal como herramienta de seguridad y gestión frente a ClearOS, en entornos de red.* Cuenca: Tesis - UNIVERSIDAD DEL AZUAY.

- VILLALON HUERTA, A. (2002). *Seguridad en Unix y Redes.* Valencia: Universidad Politécnica de Valencia.

A N E X O S

ANEXO I

MARCO LÓGICO

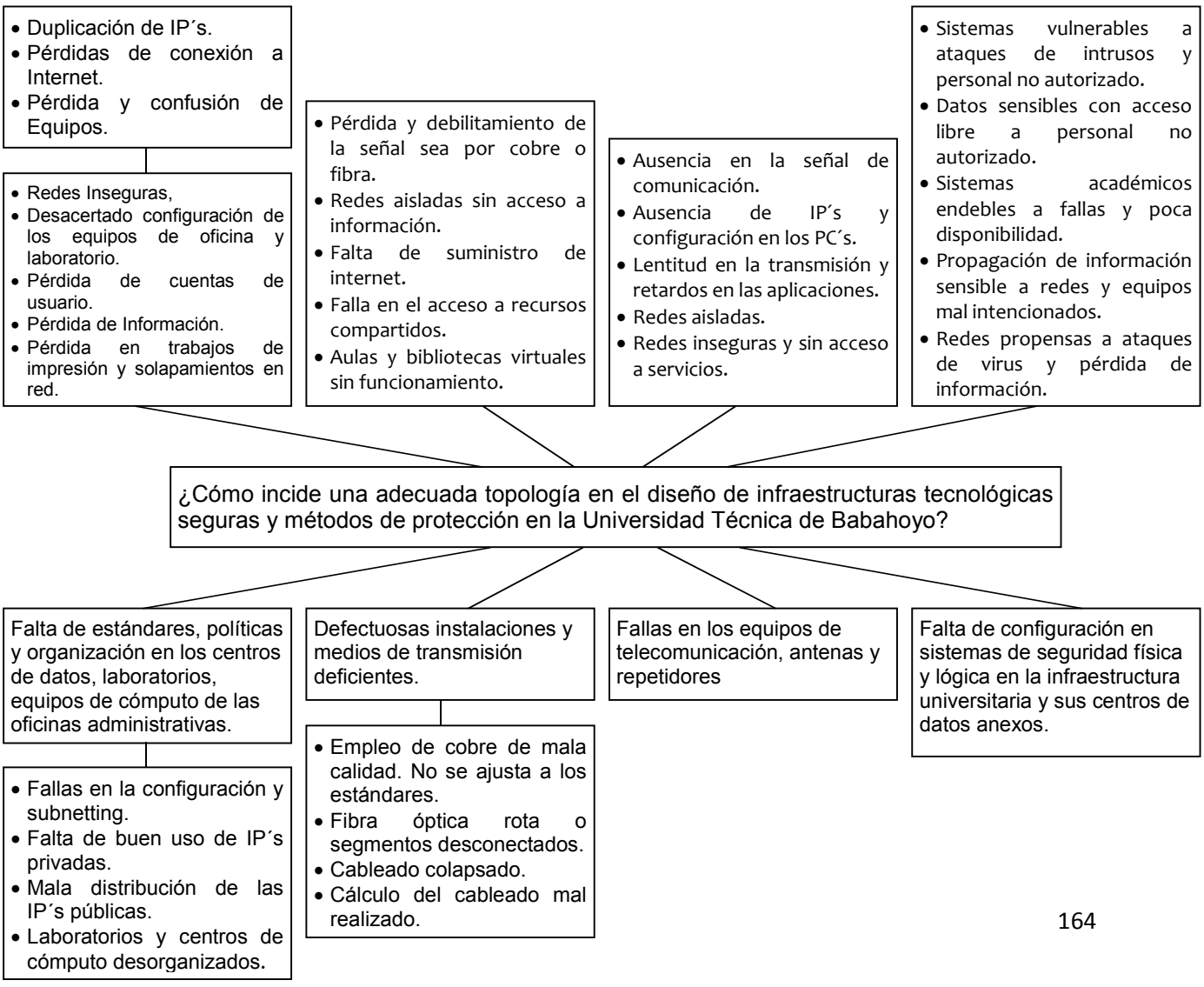
1.1. Formulación del problema:

¿Cómo *incide la escasa Seguridad Informática y métodos de protección en la intranet de la Universidad Técnica de Babahoyo?*

1.2. Análisis de involucrados.

Participantes Directos	Participantes Indirectos	Excluidos	Perjudicados
Centros de datos de Informática de las Facultades y Administración central de la UTB	Equipos de cómputo de: Oficinas administrativas, laboratorios, bibliotecas y aulas virtuales.	Telefonía	Información propicia para: Autoridades, personal administrativo, cuerpo docente y alumnos.

1.3. Árbol de problemas.



1.4. Análisis de Objetivos.

- Definir e implementar estándares y políticas en los centros de cómputo para el diseño y desarrollo de redes seguras, ejecutando una adecuada configuración en los equipos de oficina y laboratorios.

- Organizar adecuadamente los equipos de cómputo y laboratorios, apegados a las normas, políticas y estándares; asegurando la información sensible de la institución.

- Desarrollar instalaciones normalizadas y utilizar medios de comunicación eficientes que cumplan estándares de calidad.

- Mantener en perfecto estado y configuración óptima los equipos de telecomunicación, antenas y repetidores logrando una conectividad eficiente en toda la intranet de la universidad, ejecutando una distribución optima de direcciones IP´s, administración central de los equipos, configuración de seguridades en los equipos y respaldo permanente de información.

- Implementar una adecuada configuración en sistemas de seguridad física y lógica en la infraestructura universitaria y sus centros de datos anexos.

ANEXO II

ENCUESTA A USUARIOS Y AUTORIDADES DE LA RED UNIVERSITARIA

Encuesta con fines de recolección de datos para trabajo de investigación de tesis titulada "SEGURIDAD INFORMATICA Y METODOS DE PROTECCION EN INFRAESTRUCTURAS TECNOLOGICAS Y SU INCIDENCIA EN LA INTRANET DE LA UNIVERSIDAD TECNICA DE BABAHOYO"; previa a la obtención del Grado Académico de Magíster en Conectividad y Redes de Ordenadores de la Universidad Técnica Estatal de Quevedo, Año 2015.

Instrucciones:

Por favor marcar las respuesta que considere la más apropiada a su criterio

BANCO DE PREGUNTAS

1.- La información con la que trabaja en su computador es importante y confidencial para la universidad?

SI NO

2.- Usted como usuario de la red universitaria, trabaja en base a normas y reglamentos en políticas de seguridad informática?

SI NO

3.- Usted para hacer uso de su equipo informático, le han asignado alguna cuenta de usuario y contraseña?

SI NO

4.- Es necesario que su equipo informático esté conectado a la red institucional para poder realizar su actividad laboral?

SI NO

5.- Si sus repuestas anteriores fueron afirmativas, en qué medida hace uso de sus cuentas asignadas?

1) Nunca *2) Rara vez* *3) Casi siempre* *4) Siempre*

6.- Su equipo informático ha tenido ataques de virus?

1) Nunca *2) Rara vez* *3) Casi siempre* *4) Siempre*

7.- En qué medida el antivirus instalado en su equipo de cómputo de la universidad, notifica que se ha actualizado correctamente?

1) Nunca *2) Rara vez* *3) Casi siempre* *4) Siempre*

8.- En qué medida ha afectado dichos virus a su equipo informático y en especial a la información almacenada?

1) Muy afectado e Irrecuperable *2) Afectado y con opción a recuperarse* *3) Poco afectado y sin cambios* *4) Totalmente Controlado*

9.- Usted cuando hace uso del internet con qué frecuencia se le aparecen ventanas emergentes para que ingresen intrusos al equipo o ataques de virus?

1) Nunca *2) Rara vez* *3) Casi siempre* *4) Siempre*

10.- Cuando abre sus correos electrónicos en qué medida le han llegado correos basura o correos de desconocidos?

1) Nunca *2) Rara vez* *3) Casi siempre* *4) Siempre*

ANEXO III

ENCUESTA A ADMINISTRADORES DE LA RED UNIVERSITARIA

Ficha de Observación Científica con fines de obtención de datos para levantamiento de información actual y contra actual en la elaboración de una propuesta de tesis para la Universidad Técnica Estatal de Quevedo, para el grado de Magister en Conectividad y Redes de Ordenadores. Año 2015.

BANCO DE ENCUESTA

1.- ¿Posee un Reglamento vigente y ejecutado al interior del campu Universitario?
SI NO

2.- En caso de haber respondido SI; ¿Cuál es el nivel a manera general el compromiso alcanzado por la unidades institucionales?
1) Poco Satisfactorio *2) Algo Satisfactorio* *3) Muy Satisfactorio* *4) Completamente Satisfactorio*

3.- Los lineamientos de las políticas se enmarcan en los estándares y normalizaciones de seguridad informática?
SI NO

4.- Los sistemas HW de infraestructura institucional están configurados y protegidos en criterios de Seguridad Informática, en qué medida?
1) Poco Satisfactorio *2) Algo Satisfactorio* *3) Muy Satisfactorio* *4) Completamente Satisfactorio*

5.- Existe un software especial que gestione la seguridad informática de la red, equipos, sistemas y aplicaciones?
SI NO

6.- Existe un HW especial que gestione la seguridad informática de la red, equipos, sistemas y aplicaciones?
SI NO

7.- Los usuarios de la red e infraestructura informática cuentan con identifiación, permisos y contraseñas de acceso?
SI NO

8.- Existe un control y seguimiento de usuarios autentificados a la red universitaria
1) Ningún Control *2) Poco Control* *3) Muy Controlado* *4) Completamente Controlado*

9.- Cuentan con alguna aplicación que monitore la cantidad de penetraciones, ataques mal intencionados y errores en la red?
SI NO

10.- De ser positiva la respuesta anterior, ¿En qué medida el control y seguimiento de ataques y penetraciones en la red universitaria es ejecutada?
1) Poco Satisfactorio *2) Algo Satisfactorio* *3) Muy Satisfactorio* *4) Completamente Satisfactorio*

11.- La calidad de los servicios y prestaciones de las comunicaciones ante los usuarios, la velocidad de transmisión y las capacidades de ancho de banda
1) Poco Satisfactorio *2) Algo Satisfactorio* *3) Muy Satisfactorio* *4) Completamente Satisfactorio*

12.- La calidad de las conexiones inalambricas y control de accesos e interbloqueos son:
1) Poco Satisfactorio *2) Algo Satisfactorio* *3) Muy Satisfactorio* *4) Completamente Satisfactorio*

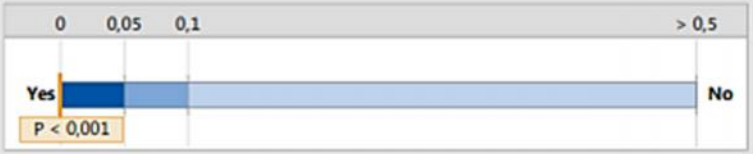
ANEXO IV

FICHA DE OBSERVACIÓN CIENTÍFICA *Ficha de Observación Científica con fines de obtención de datos para levantamiento de información actual y contra actual en la elaboración de una propuesta de tesis para la Universidad Técnica Estatal de Quevedo, para el grado de Magister en Conectividad y Redes de Ordenadores. Año 2015.*					
Nombre del Encargado: Departamento: Función:					
Logro alcanzado en la tarea: Muy Satisfactorio =4 Satisfactorio =3 Poco Satisfactorio =2 Nada Satisfactorio =1	**GRADO DE DESARROLLA ALCANZADO** **1**	**2**	**3**	**4**	**OBSERVACIONES**
Criterios a Evaluar en el DATA CENTER					
12. Existe un Plan de Seguridad Informática Institucional.					
13. Existe personal calificado en Seguridad Informática.					
14. Existen políticas de Seguridad Informática.					
15. Posee equipos acordes a controlar y supervisar las seguridades informáticas.					
16. Las conexiones en la institución están enmarcadas a las políticas de seguridad.					
17. Los sistemas software están correctamente configurados y protegidos a ataques maliciosos.					
18. Existe HW especial que supervise, controle y gestione la seguridad informática.					
19. Coexiste un conjunto de protocolos de red y de aplicación alineadas a nivel de seguridad.					
20. La infraestructura institucional cuenta con un control de accesos de usuarios.					
21. Posee la institución un control de servicios centrado en la validación de usuarios.					
22. Existe un portal cautivo que administra el acceso de usuarios a la red.					
23. El nivel de seguridad está determinado por el Proveedor de Servicio Internet.					
24. Control de ataques e intercepciones maliciosas en la red					
25. Control de errores y perdidas de información, conectividad y retardos en la transmisión					

PRUEBA DE Chi-Square % Defective - ENCUESTA A USUARIOS by PREGUNTAS

Summary Report

Do the % defectives differ?



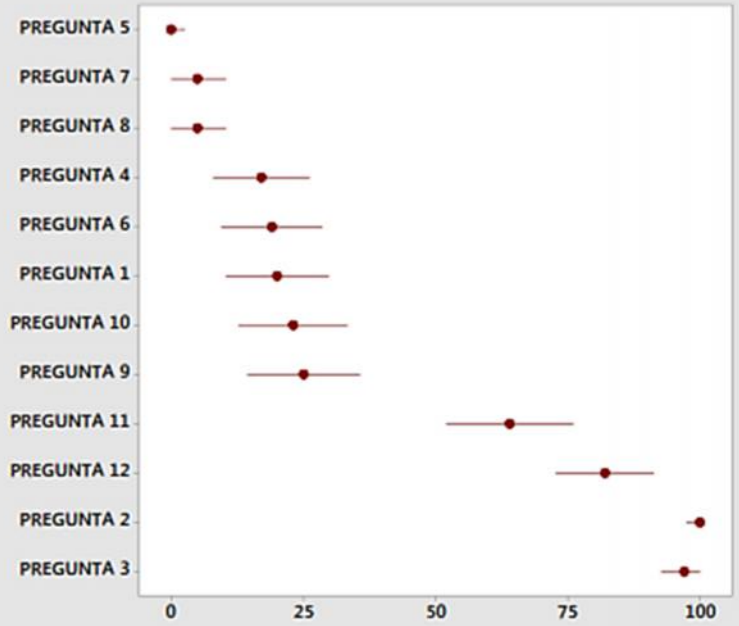
Differences among the % defectives are significant (p < 0,05).

Which % defectives differ?

#	PREGUNTAS	Differs from
1	PREGUNTA 5	4 5 6 7 8 9 10 11 12
2	PREGUNTA 7	7 8 9 10 11 12
3	PREGUNTA 8	7 8 9 10 11 12
4	PREGUNTA 4	1 9 10 11 12
5	PREGUNTA 6	1 9 10 11 12
6	PREGUNTA 1	1 9 10 11 12
7	PREGUNTA 10	1 2 3 9 10 11 12
8	PREGUNTA 9	1 2 3 9 10 11 12
9	PREGUNTA 11	1 2 3 4 5 6 7 8 11 12
10	PREGUNTA 12	1 2 3 4 5 6 7 8 11 12
11	PREGUNTA 2	1 2 3 4 5 6 7 8 9 10
12	PREGUNTA 3	1 2 3 4 5 6 7 8 9 10

% Defectives Comparison Chart

Red intervals that do not overlap differ.



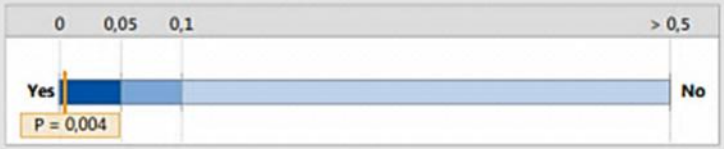
Comments

- Test: You can conclude that there are differences among the % defectives at the 0,05 level of significance.
- Comparison Chart: Look for red comparison intervals that do not overlap to identify % defectives that differ from each other. Consider the size of the differences to determine if they have practical implications.

Prueba de Chi-Cuadrado para Administradores por Criterios

Summary Report

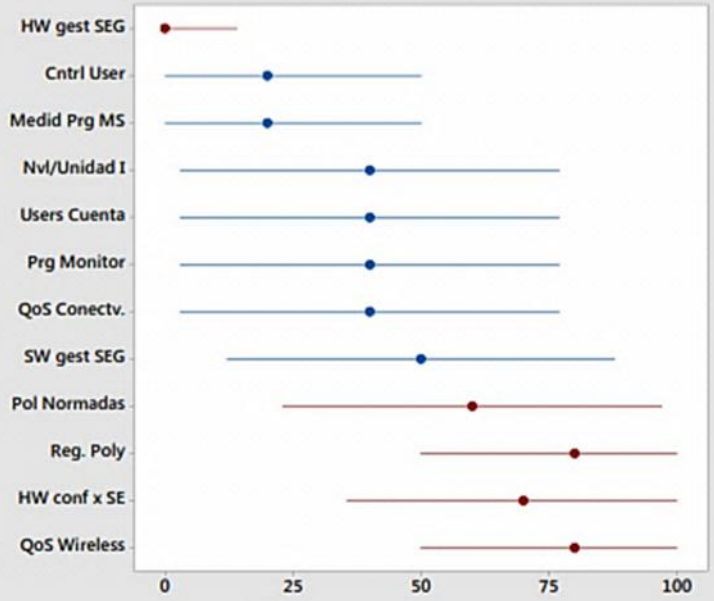
Do the % defectives differ?



Differences among the % defectives are significant (p < 0,05).

% Defectives Comparison Chart

Red intervals that do not overlap differ.



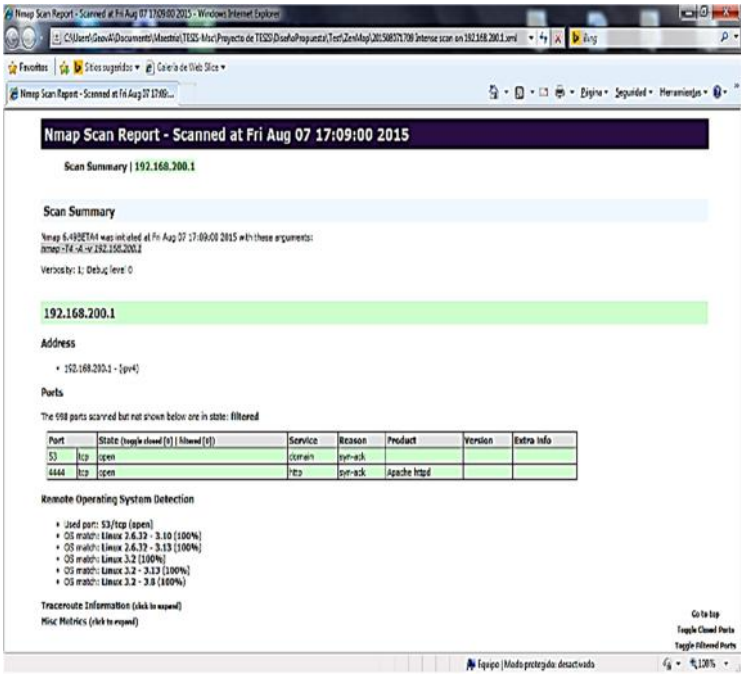
Which % defectives differ?

#	Prg.Indicado	Differs from
1	HW gest SEG	9 10 11 12
2	Cntrl User	
3	Medid Prg MS	
4	Nvl/Unidad I	
5	Users Cuenta	
6	Prg Monitor	
7	QoS Conectv.	
8	SW gest SEG	
9	Pol Normadas	1
10	Reg. Poly	1
11	HW conf x SE	1
12	QoS Wireless	1

Comments

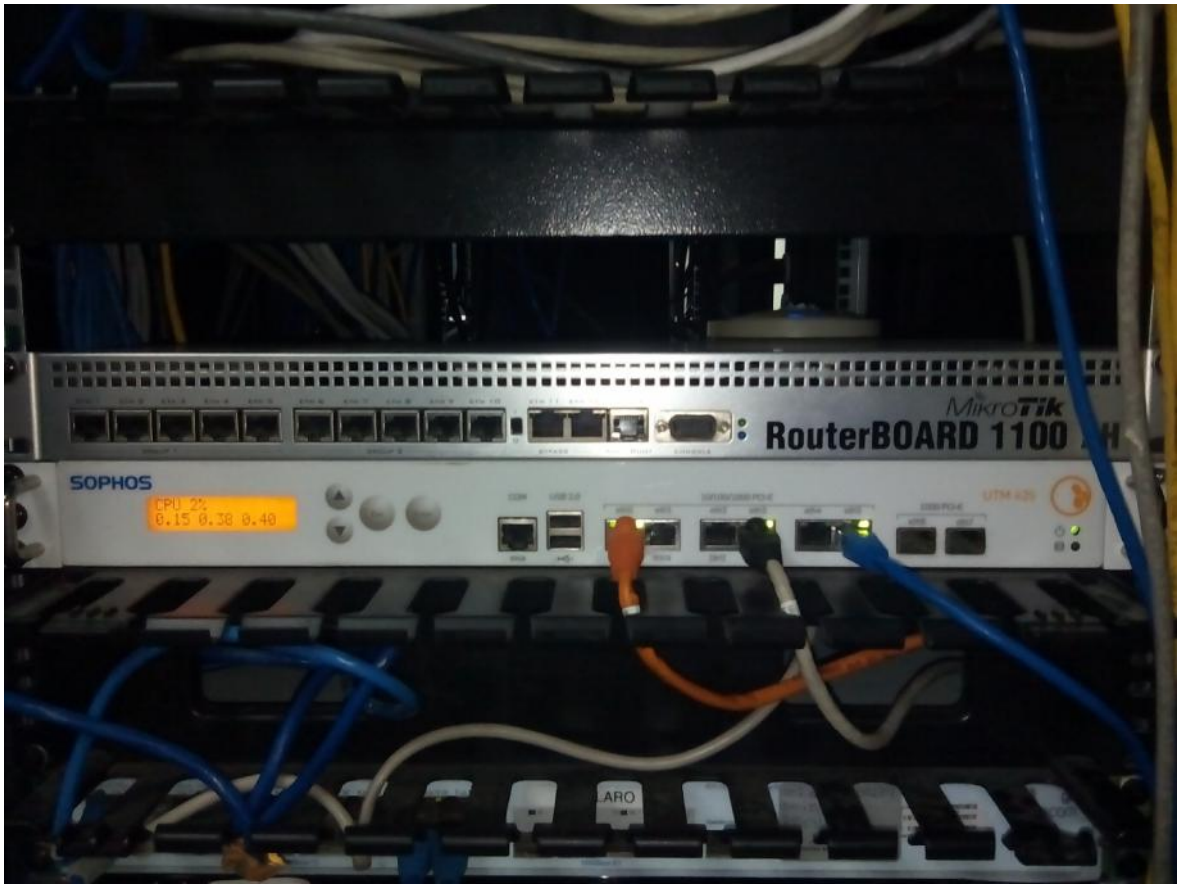
- Test: You can conclude that there are differences among the % defectives at the 0,05 level of significance.
- Comparison Chart: Look for red comparison intervals that do not overlap to identify % defectives that differ from each other. Consider the size of the differences to determine if they have practical implications.

ANEXO VII



Starting Nmap 6.49BETA4 (https://nmap.org) at 2015-08-07 17:08 Hora est. PacÃ-fico, SudamÃ©rica
NSE: Loaded 122 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:09
Completed NSE at 17:09, 0.00s elapsed
Initiating NSE at 17:09
Completed NSE at 17:09, 0.00s elapsed
Initiating Ping Scan at 17:09
Scanning 192.168.200.1 [4 ports]
Completed Ping Scan at 17:09, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:09
Completed Parallel DNS resolution of 1 host. at 17:09, 0.00s elapsed
Initiating SYN Stealth Scan at 17:09
Scanning 192.168.200.1 [1000 ports]
Discovered open port 53/tcp on 192.168.200.1
Discovered open port 4444/tcp on 192.168.200.1
Completed SYN Stealth Scan at 17:09, 4.59s elapsed (1000 total ports)
Initiating Service scan at 17:09
Scanning 2 services on 192.168.200.1
Completed Service scan at 17:09, 18.19s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.200.1
Initiating Traceroute at 17:09
Completed Traceroute at 17:09, 0.02s elapsed
Initiating Parallel DNS resolution of 1 host. at 17:09
Completed Parallel DNS resolution of 1 host. at 17:09, 0.02s elapsed
NSE: Script scanning 192.168.200.1.
Initiating NSE at 17:09
Completed NSE at 17:09, 18.91s elapsed
Initiating NSE at 17:09
Completed NSE at 17:09, 0.00s elapsed
Nmap scan report for 192.168.200.1
Host is up (0.0039s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
53/tcp   open domain
4444/tcp open ssl/http Apache httpd
| http-cisco-anyconnect:
|_ ERROR: Not a Cisco ASA or unsupported version
|_http-favicon: Unknown favicon MD5: 41776FD18CB6FDADF3C2262A81AC0242
|_http-methods: No Allow or Public header in OPTIONS response (status code 500)
|_http-server-header: Apache
|_http-title: WebAdmin
| ssl-cert: Subject: commonName=asdemo.utb.edu.ec/organizationName=UTB/countryName=ec
| Issuer: commonName=UTB WebAdmin CA/organizationName=UTB/countryName=ec
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2012-06-04T20:26:07
| Not valid after: 2038-01-01T00:00:01
| MD5:   a066 5c98 d681 7f07 52d4 e26f 2d2f 31fd
|_SHA-1: 4c8c b18d 0725 8733 abc6 9473 9316 82a2 6488 4076
|_ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10, Linux 2.6.32 - 3.13, Linux 3.2, Linux 3.2 - 3.13, Linux 3.2 - 3.8
Uptime guess: 93.198 days (since Wed May 06 12:25:17 2015)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: All zeros
TRACEROUTE (using port 53/tcp)
HOP RTT   ADDRESS
1   4.00 ms 192.168.200.1
NSE: Script Post-scanning.
Initiating NSE at 17:09
Completed NSE at 17:09, 0.00s elapsed
Initiating NSE at 17:09
Completed NSE at 17:09, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.16 seconds
Raw packets sent: 2044 (91.990KB) | Rcvd: 36 (3.100KB)

ANEXO VIII



FIREWALL SOPHOS

ANEXO IX

GRANJA DE SERVIDORES

CERTIFICACIÓN

Quevedo, Octubre 16, 2015

Ing. M.Sc. Jorge Patricio Murillo Oviedo, en calidad de Director de la Tesis: **"SEGURIDAD INFORMÁTICA Y MÉTODOS DE PROTECCIÓN EN INFRAESTRUCTURAS TECNOLÓGICAS Y SU INCIDENCIA EN LA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO, AÑO 2015". DISEÑO DE UNA INFRAESTRUCTURA TECNOLÓGICA SEGURA"**, *de la autoría del Ing.* Geovanny Eduardo Vega Villacís, Posgradista de la maestría en Conectividad y Redes de Ordenadores de la Unidad de Posgrado, certifico que ha cumplido con las correcciones pertinentes, y su tesis ha sido ingresada la tesis al **sistema URKUND** para determinar el porcentaje de similitud existente con otras fuentes. La evaluación realizada en el sistema Urkund determinó en su informe que existe un 8% de similitud.

Atentamente,

Ing. Jorge Murillo Oviedo, M.Sc.
Director de Tesis