compAs
Grupo de capacitación e investigación pedagogica

SEGURIDAD INFORMÁTICA Y MÉTODOS DE PROTECCIÓN EN INFRAESTRUCTURAS TECNOLÓGICAS Y SU INCIDENCIA EN LA INTRANET

Jorge Murillo Oviedo
Geovanny Vega Villacís

SEGURIDAD INFORMÁTICA Y MÉTODOS DE PROTECCIÓN EN INFRAESTRUCTURAS TECNOLÓGICAS Y SU INCIDENCIA EN LA INTRANET

Jorge Murillo Oviedo
Geovanny Vega Villacís

SEGURIDAD INFORMÁTICA Y MÉTODOS DE PROTECCIÓN EN INFRAESTRUCTURAS TECNOLÓGICAS Y SU INCIDENCIA EN LA INTRANET

compÁs
Grupo de capacitación e investigación pedagógica

Título original:
SEGURIDAD INFORMÁTICA Y MÉTODOS
DE PROTECCIÓN EN INFRAESTRUCTURAS
TECNOLÓGICAS Y SU INCIDENCIA
EN LA INTRANET
Primera edición: enero 2020

Publicación derivada del 5to Congreso Multidisciplinario
de Investigación Científica.
Guayaquil-Ecuador

Editado en Guayaquil - Ecuador

ISBN: 978-9942-33-168-7

compÁs
Grupo de capacitación e investigación pedagógica

Cita.
J. Murillo, G. Vega. (2020) SEGURIDAD INFORMÁTICA Y MÉTODOS DE PROTECCIÓN EN INFRAESTRUCTURAS TECNOLÓGICAS Y SU INCIDENCIA EN LA INTRANET, Editorial Grupo Compás, Guayaquil Ecuador, 91 pag

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.

ÍNDICE

PRÓLOGO	2
INTRODUCCIÓN	7
Desde Arriba hacia Abajo	20
Protocolos SSL.	22
Ventajas de SSL	23
Manejo básico de SSH	24
IPSec	24
El Protocolo AH	25
IKE: El Protocolo de Control	26
Integración de IPSec con una PKI	27
Clasificación de seguridad	29
Seguridad física y lógica	30
Seguridad activa y pasiva	33
Elementos que atentan contra la Seguridad Informática	34
Amenazas Lógicas	35
Amenazas Naturales	37
Ataques Genéricos	37
Amenazas en el desarrollo de sistemas	42
Protecciones al Sistema	43
Criptografía simétrica	45
Criptografía asimétrica.	46
Certificados Digitales	50
Tipos de Certificados	50
Arquitectura de Kerberos	55
Consideraciones al emplear Kerberos	57
Conclusiones Parciales. Administradores de RED.	57

Prueba de Chi-Cuadrado en Administradores y Operadores de RED 58

Análisis del Tráfico de Paquetes para comprobar las vulnerabilidades y amenazas presentes en la intranet de la UTB. 59

Pantallas capturadas durante el análisis de seguridad con inyección de paquetes, malwares y puertos no controlados 60

Conclusiones Parciales 62

Análisis Comparativo de Bases Metodológicas a ejecutar según datos recolectados e interpretados. 63

Discusión y comprobación de la hipótesis en relación a la información obtenida. 68

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.

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.

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.

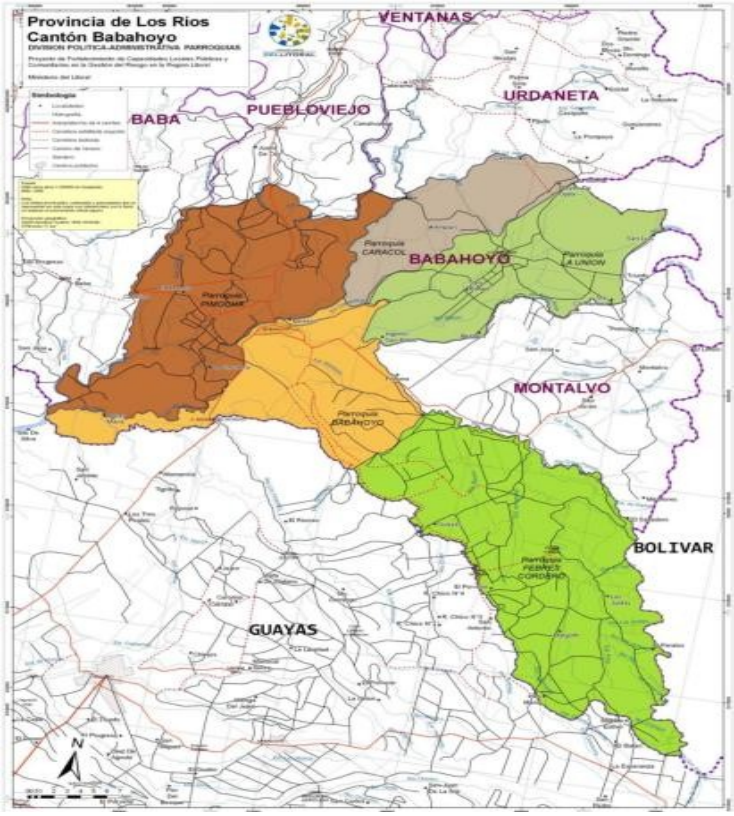
A medida en que las personas, empresas e instituciones se apegan al ritmo de la tecnología ya sea para almacenar, difundir y gestionar datos, información, recursos y servicios; invirtiendo tiempo, dinero y esfuerzos existe la amenaza de que la misma sea interceptada[2] y manipulada por personas ajenas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

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.



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.

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.

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.

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.

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)

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.

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.

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.

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.

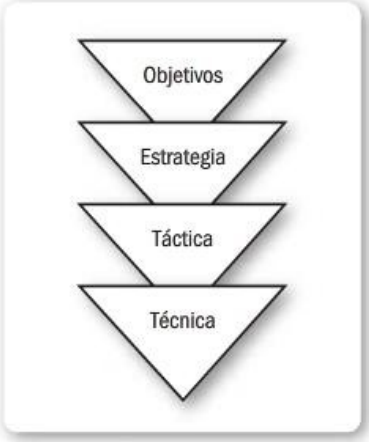
Desde Arriba hacia Abajo

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.



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."

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)

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."*

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)

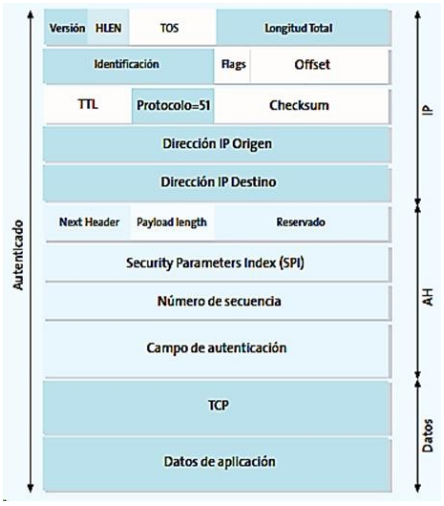
IPSec

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)

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.



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 sido modificado"*

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)*."

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)

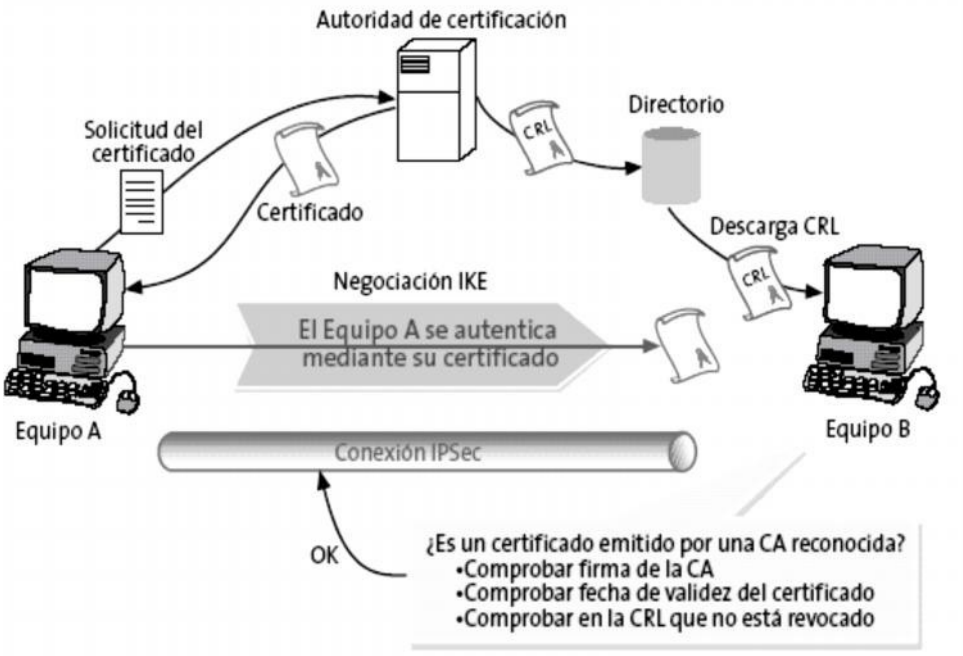
Cada uno de los dispositivos IPSec dispondrá de un certificado digital que contendrá su clave pública y la información suficiente para identificar de forma unívoca al

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. "



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)

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.

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 eviten que se infecten los equipos con malintencionados. programas
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.

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 persona sin autorización pueda 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

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)

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.

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.

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.

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)

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)

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)

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)

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.

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.

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))

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.

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)

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)

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.

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."

Clasificación de la criptografía tradicional

Una clasificación tradicional de los métodos de criptografía son:

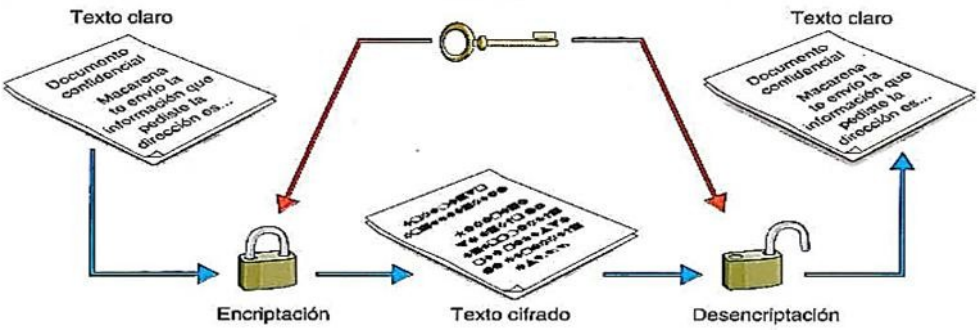
- *Sistemas de transposición*: como indica su nombre consiste en descolocar el orden de las letras, sílabas o conjunto de letras. En función del número de transposiciones podemos clasificar los sistemas de transposición en: Sistemas de transposición simples: cuando el texto en claro solo es sometido 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.

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.



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)

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 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)

r

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)

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.

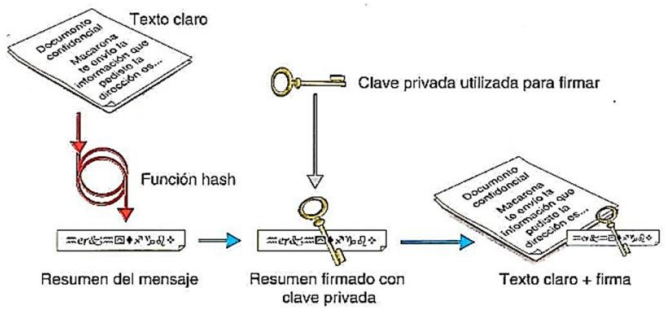
Como podemos imaginar, hoy en día se utilizan diferentes algoritmos, algunos válidos para criptografía de clave privada y otras para criptografía de clave pública. DES, 3DES, RC4, IDEA Y AES son nombres de algoritmos de clave privada y DH, ElGamal, RSA de clave pública, entre otros. (LUCENA LÓPEZ, 2010)

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



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)

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). *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)

2. *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)

3. *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)

4. *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)

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)

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)

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.

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)

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)

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)

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)

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.*

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

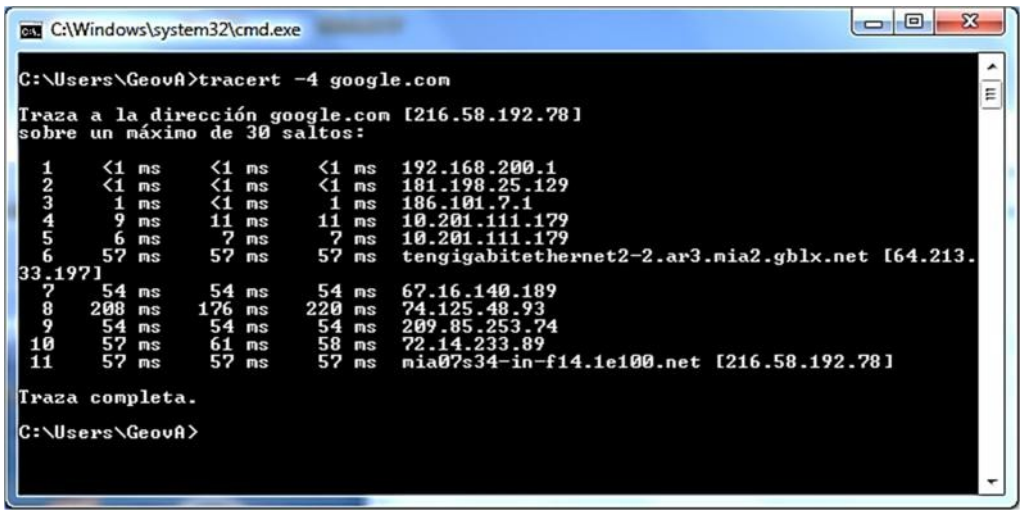
- Test: Se puede concluir que existen diferencias entre las criterios medidos% en el nivel de significación 0,05.
- Tabla Comparativa: Encuentra intervalos de comparación rojas que no se superponen para identificar% de criterios medidos NO alcanzados que se diferencian unos de otros. Considere el tamaño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

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.

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.

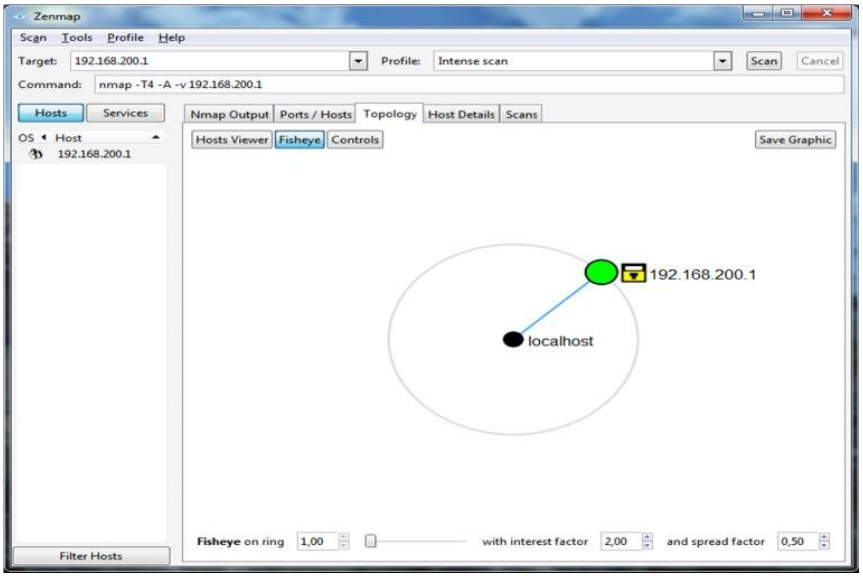
1) Traza completa conexión directa al proxy de salida SOPHOS (192.168.200.1) OUTPUT y FORWARD a la red 192.168.19.0
2) Traza completa describe la entrada del proxy SOPHOS (181.198.25.129) INPUT.
3) Usando http://whatismyip.com se obtiene la IP PUBLICA, UTB: (181.198.25.129/26)

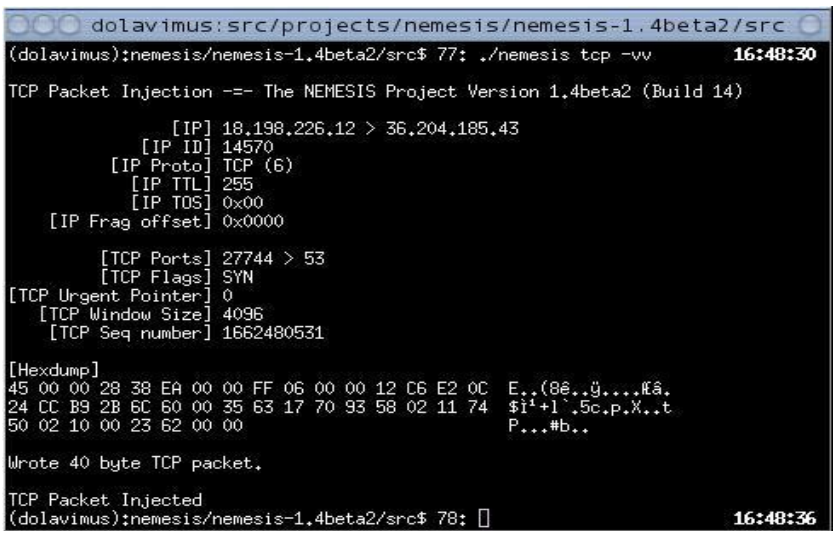
Pantallas capturadas durante el análisis de seguridad con inyección de paquetes, malwares y puertos no controlados

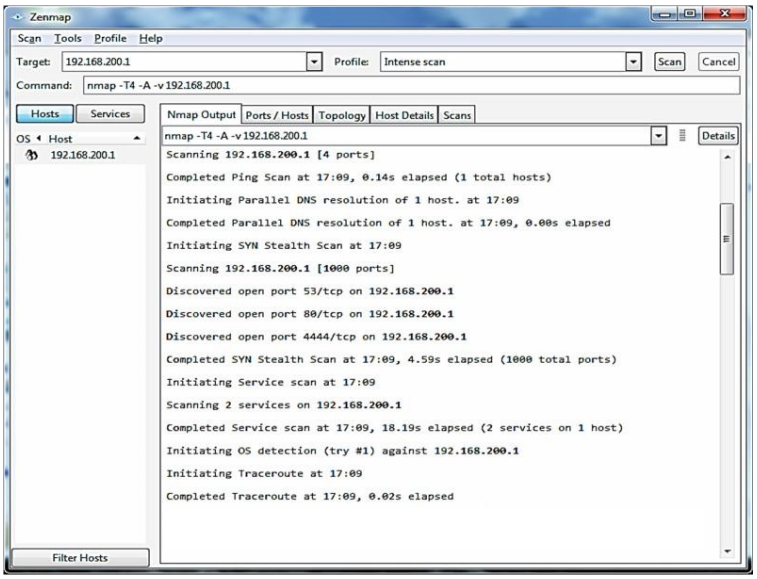
Para llevar a efecto la encuesta y responder las preguntas se ejecutó programas testeadores de red e inyectores de paquetes para analizar los tipos, tamaños y

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.







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

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.

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)*

, 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.

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.

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 laIP 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.

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"*

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.

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_come ntarios/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.

compAS
Grupo de capacitación e investigación pedagógica
@grupocompas.ec
compasacademico@icloud.com

ISBN: 978-9942-33-168-7

@grupocompas.ec
compasacademico@icloud.com

compAs
Grupo de capacitación e investigación pedagógica