



UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2017 – MARZO 2018

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

**ESTUDIO DE AMENAZAS Y VULNERABILIDADES EN LA RED DE COMUNICACIÓN
DE LA FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA**

EGRESADO (A):

ASTRID CANDY LOPEZ BAJAÑA

TUTOR:

ING. ALFONSO JACINTO AGAMA CHICO, MACI

AÑO 2018

INTRODUCCIÓN

Las redes de Datos son cada vez más útiles en toda institución, ya sea Pública o Privada, por los beneficios que aporta a nuestra sociedad. El internet se ha convertido en una herramienta de suma importancia para todo el mundo, porque permite comunicarnos de forma inalámbrica desde cualquier lugar y aporta sustanciales benéficos en la actualidad.

Estas redes de Datos han ido evolucionando con el tiempo y nos brindan cada vez mejores posibilidades de comunicar toda información a alta velocidad de banda ancha, porque permite comunicarse por medio texto, voz, video, etc. En los distintos dispositivos multimedia.

En la Facultad de Administración Finanzas e Informática realice un estudio de amenazas y vulnerabilidades a la red de Datos inalámbrica porque es necesario saber las amenazas a las que puede estar expuesta nuestra red y para ello se realizó algunas pruebas a dicha red con la finalidad de tomar precauciones para no ser presa fácil de algún intruso que quiera robar información o perturbar el buen funcionamiento de la red inalámbrica.

Este documento presenta información real y confiable, que se pudo obtener mediante entrevistas e investigación, con el fin de conocer el estado actual de la red inalámbrica de la FAFI, identificando las vulnerabilidades y las posibles consecuencias que afectan la red. Y por ultimo se expresan las respectivas conclusiones, a partir de los resultados que obtuve al finalizar la respectiva investigación, y las necesarias fuentes bibliográficas que ayudaron a la resolución de este estudio de caso.

DESARROLLO

La universidad técnica de Babahoyo se encuentra ubicada en la Av. Universitaria Km 21/2 Av. Montalvo perteneciente al cantón Babahoyo - Prov. Los Ríos.

La Facultad de Administración Finanzas e Informática, fue creada en Septiembre 22 de 1997, es una Unidad Académica de la Universidad Técnica de Babahoyo, cuyo gobierno se estructura conforme lo determina el vigente Estatuto Universitario, su campo de acción se enmarca en una concepción moderna del que hacer educativo nacional propendiendo la formación de profesionales altamente calificados, a fin de que puedan afrontar con total probidad y eficiencia los retos que imponen el avance y desarrollo de la sociedad moderna.

[...] “Dentro de esta concepción, esta unidad académica provee la fórmula de sistema educativo que profesionalice a entes capaces de planear, dirigir, ejecutar y controlar sistemas administrativos, económicos productivos de salubridad en su radio de acción local, regional y nacional haciendo hincapié fundamentalmente en actividades que constituyen fuentes de riquezas para mejorar las actuales condiciones de vida de nuestra población.” (HISTORICA, 2013).

La seguridad es fundamental para una red de datos inalámbrica funcione correctamente y para ello es necesario establecer políticas de seguridad que ayuden a evitar que personas mal intencionadas roben información dañando la integridad de la red, por eso es necesario asegurar los procesos que realizan para que sean más confiables, así resguardando la información de los datos que se manejan en dicha red.

La presente investigación tiene como finalidad realizar un estudio en la red de datos inalámbrica de la Facultad de Administración Finanzas e Informática, para dar a conocer las vulnerabilidades que existen, así como también verificar a que amenazas está expuesta la red de datos.

Como Línea de Investigación sobre la que se formuló este estudio es Desarrollo de Sistemas de la Información, Comunicación y Emprendimientos Empresariales y Tecnológicos; como sublínea, Procesos de Transmisión de Datos y Telecomunicaciones.

La investigación se planteó mediante la Metodología Cualitativa, por lo que se usó cuestionario de preguntas como instrumento para la ejecución de la entrevista realizada al Administrador y Analista de Redes del departamento de sistemas de la Universidad Técnica de Babahoyo, quien facilitó la recolección de información importante para el desarrollo de este estudio.

Según la investigación realizada al administrador y Analista en redes de la Universidad Técnica Babahoyo, Ing. Holger Paredes Zapata explica que:

La institución no cuenta con una red inalámbrica WIFI que permita la conectividad de uso de datos. Por diversos problemas obtenidos en la misma en ocasiones anteriores, ya que no nos permitía utilizarla para múltiples sesiones, solo para enlaces de radio de dos o tres kilómetros y no proveía una señal inalámbrica de calidad que permita muchas conexiones ya que colapsaba. En la actualidad se encuentra instalada dicha red, pero con equipos obsoletos, esta es la causa de que este deshabilitada de la red inalámbrica.

“En la actualidad el departamento de sistemas deshabilitó la opción DHCP (Protocolo de configuración dinámica de host) por falencias dentro de la red antes mencionadas” (Holger-Zapata,2017).

A raíz de estas falencias en el departamento de sistemas les configuran los routers para los laboratorios y personal administrativo, asignándoles una IP a cada router, con un rango limitado de equipos que puedan hacer uso del internet ya que al hacerlo público se haría lento por la cantidad de usuarios que se conectarían a dicha red, y para que los estudiantes cuenten con este servicio se les permite conectar routers desde los puertos físicos de red que tiene cada

aula proveyéndoles internet inalámbrico, es de este modo que se obtiene internet por medio de (WIFI), hasta que todos podamos contar con el servicio de tener una red inalámbrica de calidad.

Cabe mencionar que la red física tiene acceso permanente a internet y buena señal, ya que estos equipos informáticos si cuentan con un acondicionamiento de aire adecuado y sistema de respaldo de baterías, protegen la red contra ataques externos, y realizan evaluaciones de seguridad interna cada fin de semestre dando mantenimiento a los equipos informáticos.

La institución no participa en la adopción rápida de las nuevas tecnologías, no cuenta con un sistema de prevención para descubrir las instrucciones, equipos de red (Equipos de cómputo, cableado, conexiones a internet) en lugares con acceso restringido, solo cuenta con cambios de equipos que cumplen su ciclo de vida (obsoletos), en la red física.

Dentro de la institución se protegen las maquinas con el antivirus ESET NOD32 Antivirus que ofrece protección contra todo tipo de amenazas y evita que éstas puedan infectar tu ordenador, roben información o se propaguen a otros equipos.

El servidor que utiliza la institución es Linux para lo cual se recomienda utilizar contraseñas largas para mejor seguridad. Las contraseñas en Linux deben tener una longitud mínima de seis caracteres. Teóricamente no hay máximo pero algunos sistemas sólo reconocen los 8 primeros caracteres de la contraseña. No es excesivamente costoso un programa que, de manera aleatoria, trate de adivinar las contraseñas por ello cuanto más larga más tardará en encontrarla. Nunca debe seleccionar como contraseña una palabra del diccionario o una palabra que le identifique fácilmente, como su dirección, su nombre, hijos, número de teléfono, fecha de nacimiento, etc.

La Universidad Técnica Babahoyo, como Institución de Educación Superior maneja información de cada uno de los estudiantes que se han titulado y que ahora son profesionales, de tal manera que, si se llegase al filtrar dicha información, podría perjudicar a dichos

profesionales, y no solo eso, también existen gestiones que realizan internamente las autoridades de la UTB.

Es importante de igual manera realizar auditorías programadas ya que de esta manera se podrán evitar o detectar anomalías en la red de comunicación, y mantener la integridad de los datos que se transmiten en ésta.

Redes de datos

Castillo afirma. [...] “Gracias a la aparición y al éxito de los protocolos de comunicación inalámbrica se ha producido una gran difusión en la utilización de dichas redes, debido fundamentalmente a la interoperabilidad del equipamiento producido por distintos fabricantes. Esto ha promovido que se desarrollen productos de manera veloz, haciendo además que los precios se hayan visto disminuidos gracias al volumen de producción. (Castillo, 2014)

La red de datos se ha convertido en la innovación mas importante de nuestra época ya que permite conectarnos desde cualquier lugar y compartir información.

¿Qué es vulnerabilidad?

Es la disciplina que, con base a políticas y normas internas y externas de una empresa o institución, se encarga de proteger la integridad y seguridad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta. Se considera como vulnerabilidad a cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático. (Baca, 2016)

¿Qué son amenazas?

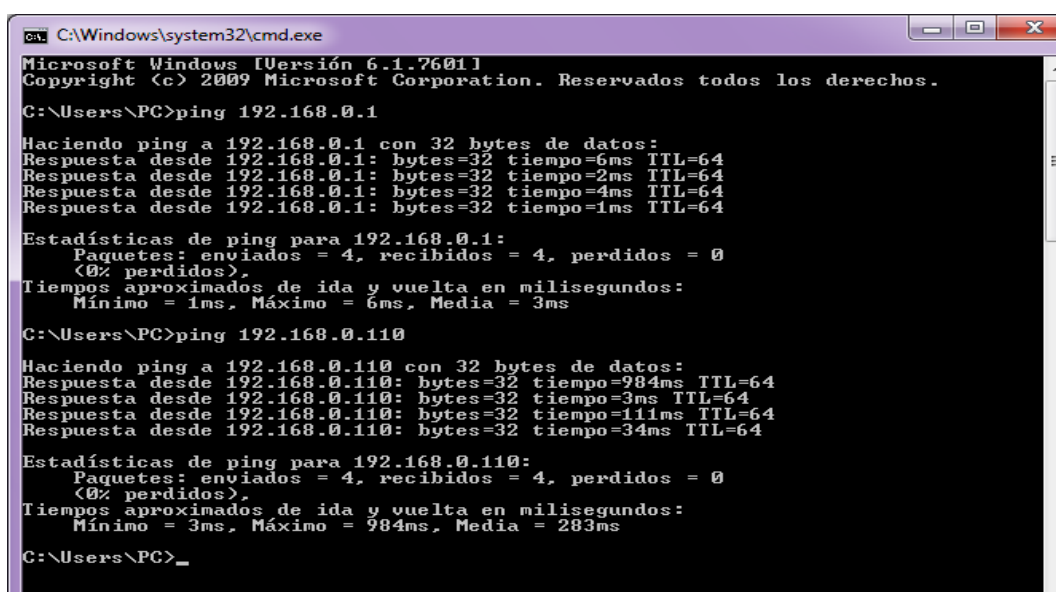
Se entiende por amenazas una condición del entorno de los sistemas, áreas o dispositivos que contienen información importante (persona, equipo, suceso o idea) que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad afectando parte de la información. Una amenaza es un conjunto de hechos y

eventos que pueden ocurrir que pueden provocar efectos perjudiciales a los activos del sistema de información. (CHICANO, 2015).

El personal que administra la seguridad informática de una institución es quienes tienen la responsabilidad de proteger la información que se transmite por medio de una red, dicha red puede tener algunos cambios, por ejemplo, llegar a hacerse más extensa. Y el personal debe estar capacitado para aplicar nuevos métodos necesarios para que la seguridad en esta área sea confiable.

Para realizar el análisis de la red de comunicación inalámbrica de la Facultad de Administración Finanzas e Informática procedí de la siguiente manera:

En primer lugar, realicé un ping para ver si tiene conexión a internet inalámbrica dicha red, la cual dio como resultado que, si se provee internet inalámbrico para laboratorios y personal administrativo ya que el primer ping se lo realicé desde una PC, y el segundo ping se lo realicé a un celular que se encontraba conectado por medio de WIFI, tal como se muestra en la **figura 1**.



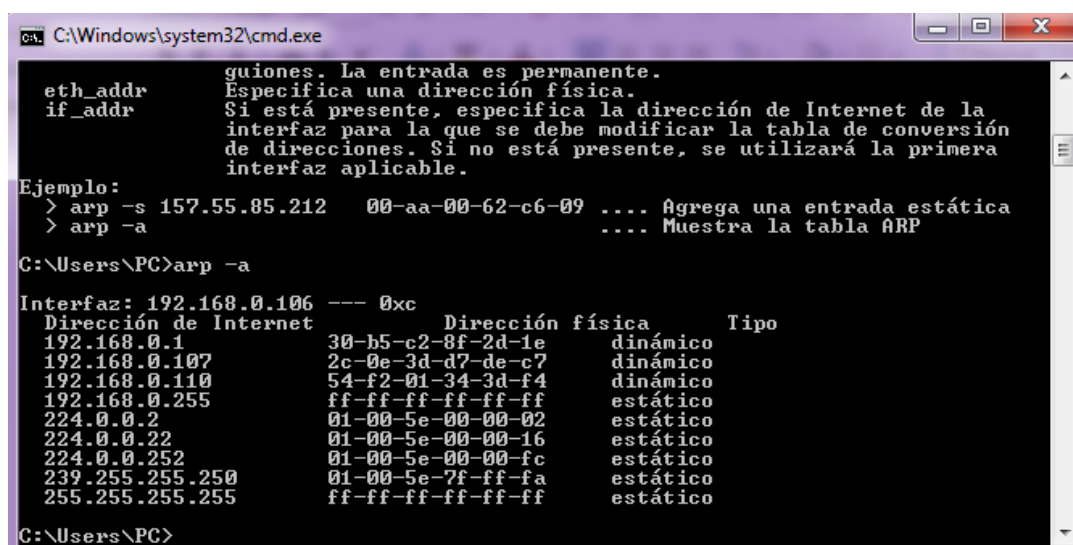
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\PC>ping 192.168.0.1
Haciendo ping a 192.168.0.1 con 32 bytes de datos:
Respuesta desde 192.168.0.1: bytes=32 tiempo=6ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=1ms TTL=64
Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 6ms, Media = 3ms
C:\Users\PC>ping 192.168.0.110
Haciendo ping a 192.168.0.110 con 32 bytes de datos:
Respuesta desde 192.168.0.110: bytes=32 tiempo=984ms TTL=64
Respuesta desde 192.168.0.110: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.0.110: bytes=32 tiempo=111ms TTL=64
Respuesta desde 192.168.0.110: bytes=32 tiempo=34ms TTL=64
Estadísticas de ping para 192.168.0.110:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 3ms, Máximo = 984ms, Media = 283ms
C:\Users\PC>_
```

Figura 1. Ping para verificar la conexión a internet inalámbrico de la Facultad de Administración Finanzas e Informática

Elaborado por: Astrid López.

Luego procedí a realizar un testeo para verificar que direcciones IP tenían cada máquina conectada al segmento de red 168, y cuál de ellas estaban activas, lo que resulto un total 9 máquinas activas con sus respectivas IP, tal como se muestra en la **figura 2**.

[...] “El protocolo **ARP** (*Address Resolution Protocol*, protocolo de resolución de dirección) tiene un papel clave entre los protocolos, porque permite que se conozca la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP.”(Vialfa, 2017)



```

C:\Windows\system32\cmd.exe
eth_addr      guiones. La entrada es permanente.
if_addr       Especifica una dirección física.
               Si está presente, especifica la dirección de Internet de la
               interfaz para la que se debe modificar la tabla de conversión
               de direcciones. Si no está presente, se utilizará la primera
               interfaz aplicable.
Ejemplo:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 ... Agrega una entrada estática
> arp -a      ... Muestra la tabla ARP

C:\Users\PC>arp -a

Interfaz: 192.168.0.106 --- 0xc
Dirección de Internet      Dirección física      Tipo
192.168.0.1                30-b5-c2-8f-2d-1e    dinámico
192.168.0.107              2c-0e-3d-d7-de-c7    dinámico
192.168.0.110              54-f2-01-34-3d-f4    dinámico
192.168.0.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

C:\Users\PC>

```

Figura 2. Escaneo para verificar los equipos conectados en la red de comunicación inalámbrica de la Facultad de Administración Finanzas e Informática.

Elaborado por: Astrid López.

Como última prueba procedí a realizar la comprobación de puertos abiertos, de las que me arrojó el siguiente análisis, para ello hice uso del comando netstat -an para ello podemos evidenciar la cantidad de puertos abiertos en dicho equipo. (Véase en la **figura 3**)

[...] “Gracias a netstat, podremos saber qué puertos tenemos abiertos y el estado en el que se encuentran en este preciso momento. Para poder obtener el listado, bastará con teclear el comando netstat -an desde la consola de comandos de Windows o también llamada **CMD**.” (Guereta, 2015)


```

C:\Windows\system32\cmd.exe
C:\Users\PC>netstat -a

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    0.0.0.0:135           PC-PC:0              LISTENING
TCP    0.0.0.0:445           PC-PC:0              LISTENING
TCP    0.0.0.0:554           PC-PC:0              LISTENING
TCP    0.0.0.0:2869         PC-PC:0              LISTENING
TCP    0.0.0.0:10243        PC-PC:0              LISTENING
TCP    0.0.0.0:49152        PC-PC:0              LISTENING
TCP    0.0.0.0:49153        PC-PC:0              LISTENING
TCP    0.0.0.0:49154        PC-PC:0              LISTENING
TCP    0.0.0.0:49155        PC-PC:0              LISTENING
TCP    0.0.0.0:49156        PC-PC:0              LISTENING
TCP    0.0.0.0:49158        PC-PC:0              LISTENING
TCP    127.0.0.1:30000      PC-PC:0              LISTENING
TCP    192.168.0.106:139    PC-PC:0              LISTENING
TCP    192.168.0.106:2869   192.168.0.1:33      TIME_WAIT
TCP    192.168.0.106:2869   192.168.0.1:34      TIME_WAIT
TCP    192.168.0.106:50440  192.168.0.1:ssdp    TIME_WAIT
TCP    192.168.0.106:50451  192.168.0.1:ssdp    TIME_WAIT
TCP    192.168.0.106:50458  13.107.4.50:http     ESTABLISHED
TCP    192.168.0.106:50465  192.168.0.1:ssdp    TIME_WAIT
TCP    [::]:135             PC-PC:0              LISTENING
TCP    [::]:445             PC-PC:0              LISTENING
TCP    [::]:554             PC-PC:0              LISTENING
TCP    [::]:2869           PC-PC:0              LISTENING
TCP    [::]:10243          PC-PC:0              LISTENING
TCP    [::]:49152          PC-PC:0              LISTENING
TCP    [::]:49153          PC-PC:0              LISTENING
TCP    [::]:49154          PC-PC:0              LISTENING
TCP    [::]:49155          PC-PC:0              LISTENING
TCP    [::]:49156          PC-PC:0              LISTENING
TCP    [::]:49158          PC-PC:0              LISTENING
UDP    0.0.0.0:500          *:.*                 *:.*
UDP    0.0.0.0:4500         *:.*                 *:.*
UDP    0.0.0.0:5004         *:.*                 *:.*
UDP    0.0.0.0:5005         *:.*                 *:.*
UDP    0.0.0.0:5355         *:.*                 *:.*
UDP    127.0.0.1:1900       *:.*                 *:.*
UDP    127.0.0.1:54301     *:.*                 *:.*
UDP    192.168.0.106:137   *:.*                 *:.*
UDP    192.168.0.106:138   *:.*                 *:.*
UDP    192.168.0.106:1900  *:.*                 *:.*
UDP    192.168.0.106:54300 *:.*                 *:.*
UDP    [::]:1500           *:.*                 *:.*
UDP    [::]:4500           *:.*                 *:.*
UDP    [::]:5004           *:.*                 *:.*
UDP    [::]:5005           *:.*                 *:.*
UDP    [::]:5355           *:.*                 *:.*
UDP    [::]:1:1900         *:.*                 *:.*
UDP    [::]:1:54299        *:.*                 *:.*
UDP    [fe80::2dc4:bbf0:14c4:27c9%12]:1900 *:.*
UDP    [fe80::2dc4:bbf0:14c4:27c9%12]:54298 *:.*
C:\Users\PC>

```

Figura 3. Análisis de puertos abiertos desde la consola de comandos de Windows o también llamada CMD.
Elaborado por: Astrid López.

Un puerto abierto en una maquina significa falta de seguridad, ya que, si no tiene virus, o algún programa escuchando en un puerto, no quiere decir que no pueda ser atacado, ya que una persona maliciosa puede enviar paquetes a dicho puerto, y aunque no haya nada allí, si puede hacer daño al recibir varios paquetes podría provocar que se bloquee ya que no podría lidiar con la cantidad de datos.

Existe la posibilidad de instalar programas, ver, cambiar o suprimir datos, o crear nuevas cuentas con privilegios completos. Por esta razón, cualquier acceso a una computadora que se aproveche de esta vulnerabilidad, esto significa un grave riesgo para la seguridad. Así

como para el personal autorizado o los intrusos que pueden acceder por medio de puertos abiertos.

Uno de los puertos más comúnmente rastreados o atacados es el (NetBIOS en Windows NT -- 135 (tcp y udp) que según el análisis de puertos que realice como prueba a la red si se encuentra abierto.

Mientras más puertos de red estén accesibles o abiertos más oportunidad hay de que pueda ser atacado. Por prevención, es de suma importancia conservar los puertos abiertos que ayuden al buen funcionamiento de la red y que no contengan información que pueda ser obtenida por cualquier usuario. Los demás puertos deben ser cerrados.

- Los puertos comprendidos entre el 0 y el 1023 son puertos reservados para usos específicos que se encuentran reglamentados, el sistema operativo los abre para permitir su empleo por diversas aplicaciones mediante los llamados protocolos "Bien conocidos", por ejemplo: HTTP, FTP, TELNET, IRC, POP3, etc.
- Los comprendidos entre 1024 y 49151 son denominados "Registrados" y pueden ser usados por cualquier aplicación.
- Los comprendidos entre los números 49152 y 65535 son denominados "Dinámicos o privados", son los usados por el sistema operativo cuando una aplicación tiene que conectarse a un servidor y le realiza la solicitud de un puerto.

El gestionar direcciones IP se ha convertido en una forma común que emplean los hackers para cubrir sus huellas luego de robar o espiar información confidencial.

Actividades de reconocimiento de sistemas: Estas actividades directamente relacionadas con los ataques informáticos, si bien no se consideran ataques como tales ya que no provocan ningún daño, persiguen obtener información previa sobre las organizaciones y sus redes y sistemas informáticos, realizando para ello un escaneo de puertos para determinar qué

servicios se encuentran activos o bien un reconocimiento de versiones de sistemas operativos y aplicaciones.

Robo de información mediante la interceptación de mensajes: Ataques que tratan de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores como Internet, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.

Introducción en el sistema de “malware” (código malicioso) Entendemos por código malicioso o dañino (“malware”) cualquier programa, documento o mensaje susceptible de causar daños en las redes y sistemas informáticos. Así, dentro de esta definición estarían incluidos los virus, troyanos, gusanos, bombas lógicas.

Las vulnerabilidades identificadas en el estudio realizado a la red de datos se catalogan según su naturaleza.

Vulnerabilidades Naturales

- No cuenta con un Programa de Prevención.
- Equipos informáticos propensos al agua, insuficiencia para soportar terremotos y otros desastres naturales.

Vulnerabilidades Físicas

- Pocas de cámaras de vigilancia en la institución.
- Falta de plan de contingencia para los equipos de red, mismos que no se hallan en lugares seguros.

Vulnerabilidad de Hardware

- No existe un cambio regular de los equipos deteriorados en la red inalámbrica.

- Conservación inadecuada de los equipos de red inalámbrica motivo por el cual se encuentra deshabilitada
- Falta de equipos de contingencia.

Vulnerabilidad de Software

- No cuenta con sistema de protección contra ataques a la red

Vulnerabilidad en la Comunicación

- Bloquear direcciones IP sin usar
- Permitir el acceso a la red solo al tráfico deseado
- Actualización de antivirus regularmente
- Tener una muy buena política de contraseñas
- Limitar la cantidad de ancho de banda de la red

Vulnerabilidad de diseño

- Rediseñar la arquitectura de la red, por falencias antes expuestas, por causa de este tipo de vulnerabilidad la red se expone las diferentes amenazas y mal funcionamiento
- Vulnerabilidad organizacional
- Existen políticas de seguridad dentro de la organización, pero no son correctamente cumplidas.
- Inestabilidad del servicio de internet.

El problema en cuanto a seguridad informática se refiere son los distintos tipos de ataques que existen. Ya que podemos ser atacados de diferentes maneras, por ejemplo, ingresando a páginas que contengan virus, desde nuestra red de forma inalámbrica mediante puertos abiertos o insertando USB a máquinas infectadas.

También existen formas de evitar estos ataques y para ello se necesita tener cierto capital para adquirir instrumentos de defensa para nuestra seguridad de información.

“Para administrar la seguridad informática se debe ser como un portero, con diez delanteros tirando penaltis simultáneamente; y con que nos metan un solo gol, estamos en graves problemas”. Los estándares de seguridad deben ser patrocinados por la alta gerencia, reafirmando así su compromiso con estos temas, tal como lo exige la norma ISO 27001:2005 sobre Sistema de Gestión de Seguridad de la Información. (Adalberto, 2014)

[...] “El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo)”. (Segovia, 2014).

Es importante saber acerca de la seguridad y riesgos que puedan perjudicar el buen funcionamiento de una red en una institución, una de estas vulnerabilidades es el mal uso de contraseñas al formarlas débiles, fáciles de descifrar, para mayor seguridad se debe usar contraseñas muy complejas.

Si se llega a ejecutar dichas amenazas a las que esta expuesta la red de la institución se afectaría al personal administrativo o equipos.

Recordemos los cuatro estándares de la seguridad en internet:

Confidencialidad: Requiere que la información sea accesible únicamente a las entidades autorizadas (confiables).

Autenticación: El usuario es realmente quien dice ser.

Integridad: Requiere que la información sólo sea modificada o borrada por las entidades autorizadas.

No repudio: Ofrece protección frente a un usuario que niega que haya existido una comunicación anterior.

Kali Linux

La característica primordial de Kali Linux es más de 300 herramientas y aplicaciones vinculadas en seguridad informática como:

[...] “Nmap, que permite escanear los puertos de un sistema, el crackeador de contraseñas Jack the Ripper o la suite Aircrack-ng para comprobar la seguridad de las redes inalámbricas.” (Springer, 2016)

Kali Linux es una distribución basada en Debian (Es una comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo basado en software libre). El cual está dirigido a las pruebas de penetración y auditoria de seguridad de la información, tales como pruebas de penetración, análisis forense e Ingeniería inversa es una empresa libre de formación en seguridad de la información, la misma que es completamente gratis y tiene una amplia compatibilidad con dispositivos inalámbricos ya que soporta la mayor cantidad de dispositivos inalámbricos y permite que funcione correctamente una amplia variedad de hardware por lo que es compatible con numerosos USB y otros dispositivos inalámbricos.

A continuación, se dan a conocer mediante un análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas) el estado de la red inalámbrica de la institución.

<p style="text-align: center;">FORTALEZAS</p> <ul style="list-style-type: none"> - Utiliza antivirus (ESET NOD32) - Existencia una persona responsable en el área de las TIC'S. - Existe personal con conocimientos de redes. 	<p style="text-align: center;">OPORTUNIDADES</p> <ul style="list-style-type: none"> - Adaptación nuevas tecnologías dentro de la institución como, por ejemplo, nuevos equipos para hacer funcionar la red inalámbrica (wifi) - Políticas para una adecuada gestión de red. - Capacitaciones en tecnología e infraestructura de red. - Implementación de estándares de calidad y control de los sistemas y equipos.
<p style="text-align: center;">DEBILIDADES</p> <ul style="list-style-type: none"> - Equipos informáticos propensos al agua, insuficiencia para soportar terremotos y otros desastres naturales. - Pocas de cámaras de vigilancia en la institución. - No existe un cambio regular de los equipos deteriorados. - Escasos recurso o poca inversión con respecto a infraestructura de los equipos. 	<p style="text-align: center;">AMENAZAS</p> <ul style="list-style-type: none"> - Carencia de tácticas para gestionar la red. - Falta de equipos de contingencia - Mal diseño a la arquitectura de la red, por falencias antes expuestas, por causa de este tipo de vulnerabilidad la red se expone las diferentes amenazas y mal funcionamiento - No contar con una buena política de contraseñas - Puertos de red abiertos.

Tabla 1: Análisis de FODA

Desarrollado por: Astrid López

CONCLUSIONES

La conservación inapropiada de los equipos de red inalámbrica que se encuentran obsoletos es considerada un punto vulnerable que genera el desgaste en el funcionamiento de dicha red, por lo tanto, es indispensable tomar medidas necesarias para darle solución, ya que es indispensable para la institución, que estos equipos funcionen correctamente ya que son el elemento fundamental para formar una red.

Las vulnerabilidades que se presentaron en el desarrollo este estudio de caso muestran el estado actual de la red y los equipos que la componen, estos resultados demuestran un nivel escaso de seguridad y elevado en vulnerabilidad, a causa de la poca importancia que tiene la red en cuanto a seguridad se refiere, se debe implementar políticas de seguridad dependiendo de cómo se encuentre estructurada la red, de pendiendo de los requerimientos que tenga la Facultad.

Por otra parte, se debe realizar un monitoreo constante a la red, de tal manera que se pueda identificar a tiempo posibles filtraciones de terceros, ya que como se vio en el resultado del escaneo existen puertos abiertos como el 139 y 445 que son usados para realizar ataques a equipos, para ellos es necesario cerrar los puertos que no utilizan y proteger los que por el uso permanecen abiertos.

Es de suma importancia que el personal administrativo de la red aporte con evaluación y control del buen cumplimiento de las nuevas políticas que se creen, de esta forma se dará una mejor solución a los problemas que se presenten.

BIBLIOGRAFÍA

- Adalberto, G. E. (Enero de 2014). <http://www.redicces.org.sv>
- Andres, R. (03 de 04 de 2016). <https://computerhoy.com>
- Ángel, M. M. (12 de Noviembre de 2014). <https://www.welivesecurity.com>
- Gomez, A. (5 de agosto de 2014). *www.edisa.com*. <http://www.edisa.com/>
- Guereta, T. (08 de 04 de 2015). *rootear*. Obtenido de <https://rootear.com>
- HISTORICA, R. (04 de septiembre de 2013). <https://www.utb.edu.ec>. Obtenido de https://www.utb.edu.ec/resena_historica
- Paredes, H. (2013). *Ingeniero de Analista en Redes*. Babahoyo.
- Segovia, J. (12 de 05 de 2014). *ISO 27001*. Obtenido de www.advisera.com
- Selta. (18 de Junio de 2013). <http://www.selta.es>
- Silvana, N. (6 de agosto de 2008). *Vulnerabilidad Infomatica*. Obtenido de <http://www.knowledgeatwharton.com.es>
- Vialfa, C. (20 de 10 de 2017). Obtenido de <https://es.ccm.net/contents/260-el-protocolo-arp>

ANEXOS***CUESTIONARIO DE ENTREVISTA***

1. ¿Tiene conexión permanente a Internet?

Si

No

2. ¿Qué tipo de red utilizan?

3. ¿Cuál son las falencias que tiene dicha red?

4. ¿Qué tipo de señal inalámbrica provee?

Débil

Regular

Buena

Mala

5. ¿Cree que la red inalámbrica brinda las seguridades respectivas para los usuarios?

Si

No

6. ¿Qué tipo de nueva tecnología ha adoptado la institución en los últimos tres años?

7. ¿Cuáles son los métodos de protección que tiene la red inalámbrica para prevenir ataques o infecciones por virus?

Si

No

8. ¿Qué tipos de herramientas utiliza para detectar e identificar los ataques a la seguridad de la red?

Si

No

9. ¿La red dispone de conexión inalámbrica?

Si

No

10. ¿Qué seguridad brinda a los equipos de red de la institución y cada que tiempo se realizan las auditorías de red?

Si

No

11. ¿Realiza la institución evaluaciones de la seguridad del entorno a través de terceros? Y con qué frecuencia se llevan a cabo estas evaluaciones.

Si

Trimestral

No

Semanal

Anual

Semestral

