
# UNIVERSIDAD TÉCNICA DE BABAHOYO

## FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

## PROCESO DE TITULACIÓN

**MAYO – OCTUBRE 2018**

**EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA**

**PRUEBA PRÁCTICA**

**INGENIERÍA EN SISTEMAS**

**PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS**

## TEMA:

**ESTUDIO DE LAS VULNERABILIDADES DEL TRÁFICO DE RED EN EL INFOCENTRO "BARREIRO"**

## EGRESADA:

**JOSELIN TATIANA SAMANIEGO SAMANIEGO**

## TUTOR:

**ING. FREDY MAXIMILIANO JORDÁN CORDONES, MSC**

**AÑO 2018**

# I. INTRODUCCIÓN

Los Infocentros son centros de cómputos que se encuentran al servicio de la ciudadanía por parte del gobierno, a través del ministerio de telecomunicaciones (MINTEL).

En el Infocentro Barreiro se realizan diversos cursos informáticos a todo tipo de persona, por ende, hacen uso de los tics como lo es el internet para poder realizar sus actividades diarias totalmente gratis, el estar disponible para todo público se vuelve altamente vulnerable y podría atacar a los servidores, estos se encuentran a cargo de facilitadores ellos también se encuentran a cargo de las clases de computación.

Los facilitadores obtienen todos los datos personales de los ciudadanos que van a capacitarse, y estos son guardado en el servidor porque al finalizar el curso cada uno recibe su certificado.

La manera que se podría reducir los riesgos de que la información sea extraída mediante la red es implementando normas que resguarden la información.

La norma ISO27001 tiene como propósito un sistema de gestión de la seguridad de la información que permite garantizar que los riegos de seguridad sean conocidos por las organizaciones de manera eficiente, documentada y adaptada a cambios tecnológicos.

La información usada en las TIC es muy relevante para los usuarios, por cuanto ofrecen una herramienta de ayuda a cada una de las organizaciones; a través de las cuales se garantizan la confiabilidad, integridad y disponibilidad de los datos.

Debido a esto se puede determinar que la seguridad informática es uno de los pilares de mayor importancia en la estructura de la organización, porque la filtración o el mal uso de la información causarían perdidas económicas en la organización.

La línea de investigación de este proyecto se encuentra vinculada con los procesos de transmisión de datos y telecomunicaciones porque se realizará un escaneo en la red del Infocentro “Barreiro”.

El siguiente proyecto tiene como objetivo general realizar un estudio de las vulnerabilidades del tráfico de red en el Infocentro “Barreiro”, en la parroquia Barreiro perteneciente al Cantón Babahoyo, el mismo que será desarrollado entre los meses de junio a septiembre del año en curso, una vez realizado el análisis del Infocentro podemos determinar cuáles son las vulnerabilidades que presenta dicha red y sugerir acciones necesarias para la correcta seguridad de la información que se manipula en el Infocentro.

## II. DESARROLLO

En la actualidad la seguridad de la información es un punto clave de análisis, puesto que las condiciones van cambiando a lo largo del tiempo en función de las nuevas tecnologías, lo que ha permitido fijar nuevos horizontes dando como resultado, la aparición de nuevas amenazas tecnológicas que pudieran poner en riesgos los activos. (Karen Andrea Pintado Cuji, 2015)

Nunca antes el hacking y la piratería informática habían sido tan mediáticos. Desde los años 70, los sistemas informáticos se han ido multiplicando y han adquirido más y más importancia, permitiendo acceder cada vez más rápido a la información, multiplicando el intercambio de esta con la democratización y el urge de internet en los hogares (ACISSI, 2015)

Cada una de las organizaciones manejan grandes cantidades de datos los mismo que pueden ser alterados, dañados, robados o infectados por virus lo que provocaría grandes daños en los sistemas operativos, para evitar dichos problemas es mejor contar con equipos informáticos que sean capaces de brindar una mayor seguridad y confiabilidad de los datos.

La seguridad en redes se considera en dos aspectos: física y lógica, en la primera de ellas se debe estar atento y tomar medidas preventivas como son los desastres naturales, inundaciones, terremotos incendios, así como también de las instalaciones eléctricas, etc. En la segunda se debe tener cuidado con aquellas personas que no están autorizadas para el acceso de la información, y es aquí donde entran los piratas de informáticos, un ejemplo de ellos son los hackers, crackers, etc. Que buscan algo que les interesa y después puedan poseerlo, o también para probarse a sí mismos hasta donde pueden llegar, aprovechándose de las vulnerabilidades de la víctima, como por ejemplo de los sistemas operativos o de la ingenuidad de los trabajadores al recibir archivos desconocidos y abrirlos, infectando el sistema por medio de virus u otra especie de herramientas. (Carlos, 2014)

**Amenazas**

Se considera amenaza a cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización. (Vieite, 2014)

| CLASIFICACIÓN DE AMENAZAS | | |
|---|---|---|
| **PERSONAS** | **FÍSICAS** | **LÓGICAS** |
| Ex empleados<br>Hackers<br>Intrusos remunerados | Robos de información<br>Suministro eléctrico<br>Desastres naturales | Perdidas de datos<br>Ataques o intrusos a la red<br>Virus |

**Tabla 1:** Amenazas en una red de datos
**Elaborado por:** Joselin Samaniego

Algunos tipos de ataques

Suplantación de identidad: Una persona o entidad suplanta a otra con fines ilícitos. Por ejemplo, personas que se hacen pasar por otras con el fin de obtener recursos de la red.

Divulgación del contenido: Se produce cuando una persona o entidad se entromete en el destino final de un mensaje para hacer uso de la información interceptada.

Modificación de mensajes: Consiste en modificar el contenido de un mensaje sin que sea posible de ser descubierto.

Denegación del servicio: Esto significa que una persona no pueda operar de forma normal ya que impide el acceso a determinados servicios como podría ser, por ejemplo, el correo electrónico. (Ríos Yáguez, 2014)

Mecanismos que llevan a cabo un ataque informático

Puertas traseras: En ocasiones están son creadas para propósitos maliciosos

Troyanos: Se encuentra bajo la apariencia de un programa o mensaje inofensivo, se introduce un virus en la máquina de los usuarios afectados y de esa manera permite que otra persona tenga el control sobre la computadora.

Virus: Es un programa cuya finalidad es alterar el funcionamiento del equipo sin el consentimiento del usuario.

Gusanos: Los gusanos informáticos se propagan de ordenador a ordenador, pero a diferencia de un virus, tiene la capacidad a propagarse sin la ayuda de una persona. (Gonzàlez, 2014)

**Amenazas más conocidas en la informática**

Morris: Uno de los primeros grandes ataques que se recuerdan. En 1988 apenas había cerca de 60.000 ordenadores con conexión a internet en todo el mundo, pero este gusano infectó a más del 10% de esos usuarios los daños fueron estimados en cerca de 96 millones de dólares. (Otto, 2017)

Troyanos financieros: Los troyanos financieros son piezas de malware que los ciberlincuentes utilizan para monetizar sus actividades. Los ciberlincuentes utilizan sistemas de ataque avanzados orientados a realizar transacciones ocultas y atacar a diferentes bancos. (Juliá, 2018)

Ransomware: Se aprovechó de una vulnerabilidad de la NSA que se filtró, y que llevo 3 meses solucionarla. Sin embargo, tanto usuarios como empresas no fueron capaces de instalar un simple parche de seguridad de Microsoft, gratuito y automático, lo que finalmente terminó en desastre. (Velasco, 2018)

Conficker: aprovecha los medios más potentes y comunes de transmisión de archivos, como puede ser el email o aplicaciones de mensajería tipo WhatsApp. Su principal función es exportar las contraseñas a través de su red. (Nomasvirus, 2018)

Mydoom: Inutilizaba gran parte de las herramientas de seguridad de Windows, con lo que era capaz de moverse a sus anchas por todo el sistema operativo y el ordenador del usuario infectado, este virus generó unos daños cercanos a los 40.000 millones de dólares. (Otto, 2017)

**Vulnerabilidad**

Una vulnerabilidad es cualquier debilidad en el sistema informático que puedan permitir a las amenazas causarle daño y producir perdidas en la organización. (Vieite, 2014).

En la actualidad se contempla que hay ataques intencionados y no intencionado, mismos que las empresas siempre es vulnerable en mayor o menor medida. La primera vulnerabilidad que puede suceder es que los diseñadores del sistema no sean capaces de prever todas las amenazas que existen o que pueden suceder en el futuro. (Baca Urbina , 2016) Los ataques se clasifican en:

Ataques no intencionados: Es cuando perjudica la información, organización sin que ocurra por la acción intencional de alguien. Por ejemplo, un incendio, una inundación, la falla del suministro de energía, errores del usuario.

Ataques intencionados: Estos son los que no son autorizados al sistema, aquí se descubren a los atacantes que acceden sin permiso alguno de la empresa, con el fin de robar información, o alterarla.

**Causas de las vulnerabilidades de los sistemas informáticos**

- Debilidad en el diseño de los protocolos utilizados en las redes.
- Errores de programación.
- Configuración inadecuada de sistemas informáticos.
- Falta de políticas de seguridad.
- Desconocimiento de los usuarios responsables de informática

- Disponibilidad de herramientas que actúen contra los ataques.
- Limitación gubernamental al tamaño de las claves criptográficas y a la utilización de este tipo de tecnologías.
- Existencia de "puertas traseras" en los sistemas
- Falta de capacitación del personal.

Los Infocentros son sitios comunitarios de aportación, en los que se garantiza el acceso a las Tecnologías de la Información y Comunicación (TIC), brindándonos diversos cursos en diversas áreas, para de esa forma poder fortaleza el conocimiento de la ciudadanía.

Brindas diversos servicios como son:

- Los tramites en línea
- Dictan cursos y talleres capaces de fomentar la formación académica
- Espacio para reuniones y asambleas
- Cursos de computación gratis

El Infocentro de Barreiro cuenta con una sala de computo de aproximadamente 10 computadoras, las mismas que son usadas para trabajos educativos, investigaciones entre otras actividades, además que brindan capacitaciones que duran de 3 a 4 meses, esto fortalece el conocimiento de las personas que viven en esta zona, pero aquí se encuentran con problemas en la red lo que genera la caída de internet, inestabilidad en la conexión a internet, lentitud al momento de cargar páginas web y el no poder realizar las actividades que desean los ciudadanos de este sector, el Infocentro cuenta con equipos de cómputo y de redes tales como; routers , swicht, y servidores que poseen instalado un software que permite iniciar con el sistema operativos (Windows o Ubuntu) de acuerdo a las necesidades de las personas.

El problema existente en la red de datos del Infocentro, se especificará en función a la observación y la elaboración de entrevistas al encargado del Infocentro.

Como objetivos específicos tenemos:

- Sensibilizar al encargado del Infocentro la existencia de riesgos en la red.
- Realizar una encuesta al encargado del Infocentro, para determinar el nivel de conocimiento que tiene acerca de la seguridad de la información.
- Ayudar a mantener los riegos en bajo control

El presente caso de estudio hace uso del método inductivo, debido a observar los parámetros de configuración para evaluar la red, con el fin de a llegar a una propuesta que permita ofrecer una guía referencial, con el fin de poder ofrecer un buen servicio a la ciudadanía y tratar de mantener un buen nivel de seguridad de la información que existe en el Infocentro Barreiro.

Existen diversas técnicas para la recolección de información, en el presente estudio tomaremos en cuenta las siguientes:

**Observación:** La cual nos permitió saber la situación actual en que se haya en el Infocentro, ya que uno de los objetivos del presente estudio es conocer los problemas existentes en la red y dar posibles soluciones a dichos inconvenientes.

**Entrevistas:** Ya que nos ofreció tener una mejor perspectiva por cuanto se tiene datos exactos del problema por parte de las personas que laboran y manejan el sistema.

Una vez recopilada la información, se hará uso de herramientas necesarias para el análisis de las vulnerabilidades en la red, así se podrá saber qué tipos de problemas se presenta

en Infocentro y cuáles pueden ser las medidas a tomar por parte del personal que labora en la misma.

Las maquinas del Infocentro Barreiro se las protegen con el antivirus ESET NOD32, que permite mantener una protección contra todo tipo de amenazas y de esa forma poder evitar que se puedan infectar las computadoras o que la información que maneja el Infocentro sea robada.

**Beneficios de realizar un análisis en la red.**

Antes de realizar dicho análisis se solicitó, el permiso respectivo del encargado del Infocentro para de esa forma poder determinar el nivel de vulnerabilidades que existe en la red.

Entre las principales tenemos:

- Identificar los problemas en el menor tiempo posible.
- Reducir los riesgos que pueden generar pérdidas o robo de información y conocer el nivel de vulnerabilidad.
- Ahorrar recursos económicos.
- Mejoras en el Infocentro permitiendo garantizar la confidencialidad, integridad de la información a través de la red.

**Factibilidad operativa:** El análisis de vulnerabilidades que se desarrollará con herramientas encargadas en el monitoreo del tráfico de red, será realizada con la finalidad de incrementar la seguridad en red.

**Factibilidad económica:** No se requiere de altos niveles de recursos económicos, ya que solo se cuenta con el tiempo que debe temer la persona encargada de realizar el análisis, siempre y cuando contando con el permiso adecuado de dicha organización.

Con esto se facilita el análisis de factibilidad ya que nos da a conocer que el proyecto es viable y que la realización del mismo no genera gran inversión económica, por lo cual es factible realizarlo sin ningún impedimento.

## Aplicaciones para el monitoreo de red

Wireshark, permite capturar el tráfico de red además de dar soluciones a los problemas de comunicación, es una herramienta que se ejecuta en diversos sistemas operativos Linux, y Mac OS X, así como en Microsoft Windows y es gratuito a continuación, se presenta las características del programa.

- Software libre
- Importa y exporta paquetes de datos en diferentes formatos
- Disponibles en Linux y Windows
- Utiliza licencia GPL

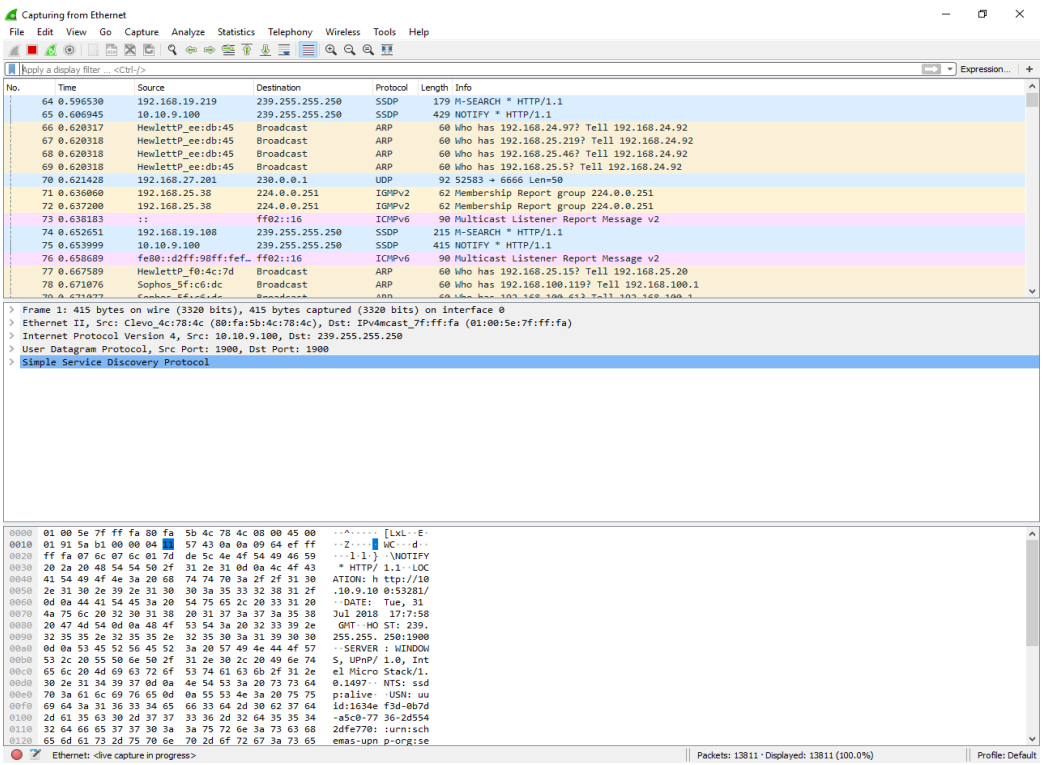



**Figura 1:** Resultado de escaneo en Wireshark
**Elaborado por:** Joselin Samaniego

Las interfaces de datos capturados están compuestas por tres partes: resumen o lista de paquetes, el panel de detalles del paquete y el panel de paquetes de bytes.

Nmap es una herramienta de código abierto para el escaneo de puertos y auditorias de seguridad. La misma permite determinar qué tipos y versiones de sistema operativos utilizada cada host. Originalmente era una herramienta de línea de comandos, pero actualmente incluye también la posibilidad de instalar la herramienta con interfaz gráfico que facilita su uso Zenmap. (Gabriel Diaz Oruta, 2014)

Zenmap, escanea los puertos que se encuentran abiertos y cerrados en esta aplicación nos permite realizar varias clases de escaneo, la figura a presentar realiza un escaneo intenso, características del programa.

- Muestra las computadoras que se encuentran en red
- Identifica los puertos que se encuentran abiertos
- Muestra los servicios que se están ejecutando
- Trabaja bajo comando en Linux y de forma gráfica para Windows

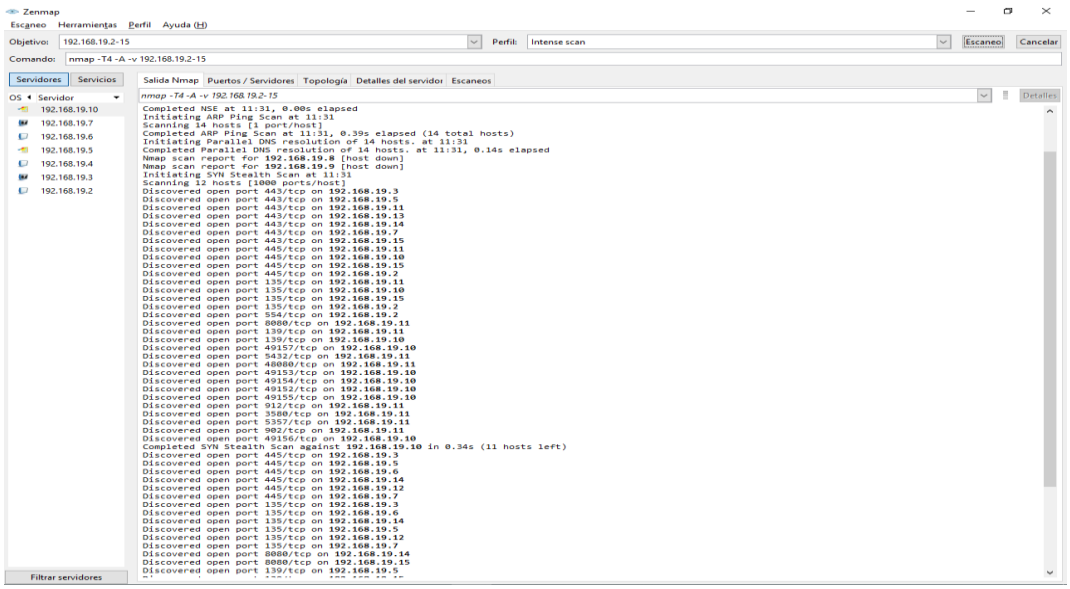



**Figura 2:** Resultado de escaneo en Zenmap
**Elaborado por:** Joselin Samaniego

Entre las dos herramientas utilizadas más practicable es Zenmap ya que Wireshark escanea todos los protocolos existentes en la red y demora al momento de realizar el escaneo y además en más difícil de descifrar la información que transita en la red mientras que la otra herramienta me permite ver con claridad que puertos se encuentran abiertos, que servidores, su sistema operativo.

Los puertos son puertas virtuales las cuales permiten ingresar o salir información, al no contar con una seguridad adecuada podemos encontrarnos vulnerable a que nuestra información sea robada, alterada, manipulada.

Mientras más puertos abiertos se encuentren en la red, más oportunidad hay de ser atacado.

La IANA (Agencia de Asignación de números de internet) los divide en tres categorías como son:

- Una categoría para los protocolos menores de 1024 que se reservan para el sistema operativo y los protocolos más comúnmente utilizados como son el HTTP que utiliza el puerto 80, FTP que utiliza el puerto 21.
- Del 1024 al 49151 llamado “registrados”, estos lo utilizan cualquier aplicación como son las de conexiones remotas con otro ordenador.
- Mayores de 49151 utilizados por el sistema operativo para que una aplicación se conecte al servidor.

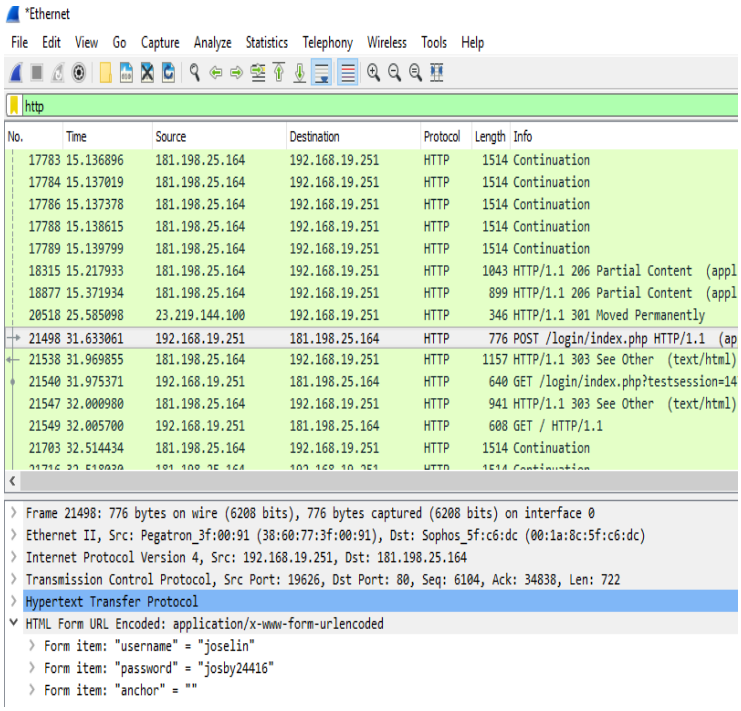



**Figura 3:** Hacking ético con Wireshark, donde obtendremos el usuario y la clave.
**Elaborado por:** Joselin Samaniego

En la Figura 3, nos muestra cómo podemos obtener el usuario y la clave de una persona que navega en la red con facilidad, para evitar este tipo de problemas debemos acceder a páginas webs del tipo HTTPS ya que estas se encuentran protegidas de extremo a extremo que, aunque puedan acceder a nuestros datos estos se encontraran cifrados.

Los problemas de seguridad encontrados en la red son los siguientes:

- Falta de políticas de seguridad, lo que genera al acceso no autorizado en la red
- Falta de conocimiento en el personal encargado del área
- No contar con un programa de protección contra los ataques
- No existe cambio de los equipos que se encuentran deteriorados.

La seguridad afecta a todos los sistemas de información y más hoy en día con el uso de las redes de comunicación especialmente el internar, fuente de muchas cosas buenas y

malas, virus, hackers. Pero la falta de seguridad no es solo culpa de factores externos, sino también viene dada por factores internos como el uso que se hace de los equipos, la falta de formación en la materia acerca de seguridad. (Arantes, 2016)

La seguridad de la información está destinada a la protección de los datos y a tratar de evitar la pérdida y las modificaciones no autorizadas de los mismos. Dicha protección debe garantizar tres requisitos fundamentales. (Carlos Caballero González, 2017) Como son:

**Disponibilidad:** Es cuando el usuario o sistema necesite realizar una consulta.

**Confidencialidad:** Que la información no sea divulgada a personas o entidades no autorizados

**Integridad:** Que la información no sea modificada por personal no autorizado.

El problema de la seguridad informática se da a que puede ser atacada de diferentes formar por ejemplo ingresando a páginas web que contengan virus, o insertando USB a maquinas infectadas, usando contraseñas débiles y pocas seguras, aprovechándose de la vulnerabilidad existente en la red.

## III. CONCLUSIONES

Este estudio de caso servirá de ayuda para determinar el nivel de seguridad que se encuentra el Infocentro Barreiro.

De acuerdo al estudio realizado sugiero que es de suma importancia realizar con frecuencia un monitoreo de red para de esa forma poder identificar a tiempo todo tipo de vulnerabilidad para de esa manera poder evitar daños o perdidas de información que manipule el Infocentro.

La mala configuración de los dispositivos, se debe a que el encargado del Infocentro desconoce acerca de la seguridad informática y por ende el no contar con conocimientos necesario excluye los riesgos al que se enfrenta al no contener una seguridad adecuada.

Se recomienda que el personal encargado del área sea capacitado con más frecuencia acerca de la seguridad informática, para de esa forma poder actuar a tiempo cuando se presente una amenaza, de la misma forma sugiero que se implemente políticas de seguridad para tener un control de acceso a la red, el nivel existente de vulnerabilidad en el tráfico de red no lo considero alto, pero si se encuentra en un nivel moderado el cual tiene que ser atendido para evitar fallos en la red.

**BIBLIOGRAFÍA**

ACISSI. (2015). *Seguridad Informática.* barcelona: Ediciones ENI.

Arantes, S. C. (2016). *Gestion de redes telematicas* . España: ELEARNING S.L.

Baca Urbina , G. (2016). *Introducción a la Seguridad Informática* . México: Ebook.

Carlos Caballero González, . A. (2017). *Salvaguarda y seguridad de los datos.* españa.

Carlos, U. d. (2014). *Seguridad de la Información. Segunda Cohorte del Doctorado en Seguridad Estratégica.*

Gabriel Diaz Oruta, I. A. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES.* Madrid .

Garcia, D. R. (20 de mayo de 2015). *Investigacion wireshark.* Obtenido de https://es.slideshare.net/DulceRomeroGarcia/investigacion-wireshark

Gonzàlez, C. (2 de 10 de 2014). *Virus, Gusanos, Caballos de Troya y Spyware*. Obtenido de Prezi: https://prezi.com/0gtyjv4j7urp/virus-gusanos-caballos-de-troya-y-spyware/

Juliá, S. (2018). *Amenazas a la seguridad informática en 2018.* Obtenido de GADAENETWEB: http://www.gadae.com/blog/amenazas-seguridad-informatica-2018/

Karen Andrea Pintado Cuji, C. L. (04 de 2015). *Diagnostico de las vulnerabilidades informaticas en los sistemas de informacion para proponer soluciones de seguridad a la rectificadora gabriel mosquera S.A* . Obtenido de Universidad Politecnica Salesiana Sede Guayaquil : https://dspace.ups.edu.ec/bitstream/123456789/10349/1/UPS-GT001276.pdf

Nomasvirus. (2018). *LOS VIRUS INFORMÁTICOS ACTUALES MÁS PELIGROSOS 2018.* Obtenido de Nomasvirus : https://nomasvirus.com/2018/02/11/los-virus-informaticos-actuales-mas-peligrosos-2018/

Otto, C. (21 de 05 de 2017). *Los siete virus informáticos más dañinos de la historia*. Obtenido de LaVanguardia:

https://www.lavanguardia.com/tecnologia/20170521/422734535859/virus-informaticos-mas-daninos-historia.html

Ríos Yáguez, J. (2014). *Técnicas y herramientas de análisis de vulnerabilidades de.* Obtenido de http://oa.upm.es/32786/1/TFG_javier_rios_yaguez.pdf

Velasco, R. (2018). *Qué nos deparará 2018 en cuanto a seguridad informática.* Obtenido de RedesZone: https://www.redeszone.net/2018/01/01/seguridad-informatica-2018/

Vieite, Á. G. (2014). *Enciclopedia de la seguridad Informatica 2a Edicion Actualizada.* Obtenido de https://books.google.com.ec/books?id=Bq8-DwAAQBAJ&pg=PT9&lpg=PT9&dq=Pol%C3%ADticas+de+seguridad+deficiente+o+inexistente&source=bl&ots=dwn40h3fhD&sig=dLCtMiZtdOf5rq5yYJrGo9NBE8k&hl=es&sa=X&ved=0ahUKEwjZlYDUt7jcAhVJw1kKHejECHUQ6AEIYDAG#v=onepage&q=Pol%C3%A

**ANEXOS**

1. ¿Utiliza normas para la seguridad de información?

   a) Si
   b) No

2. ¿Cómo considera usted que se encuentra el nivel de seguridad de la red?

   a) Alta
   b) Media
   c) Baja

3. ¿Ha sido usted víctima de robos de información?

   a) Si
   b) No

4. ¿Cómo califica usted la cobertura y la señal wifi?

   a) Buena
   b) Mala
   c) Regular

5. ¿Qué tipo de seguridad poseen las computadoras para evitar robos de información?

   a) Firewall
   b) Software de detección de malware
   c) Antivirus
   d) Ninguna

6. ¿Usted tiene conocimiento acerca de seguridad de información?

a) Si

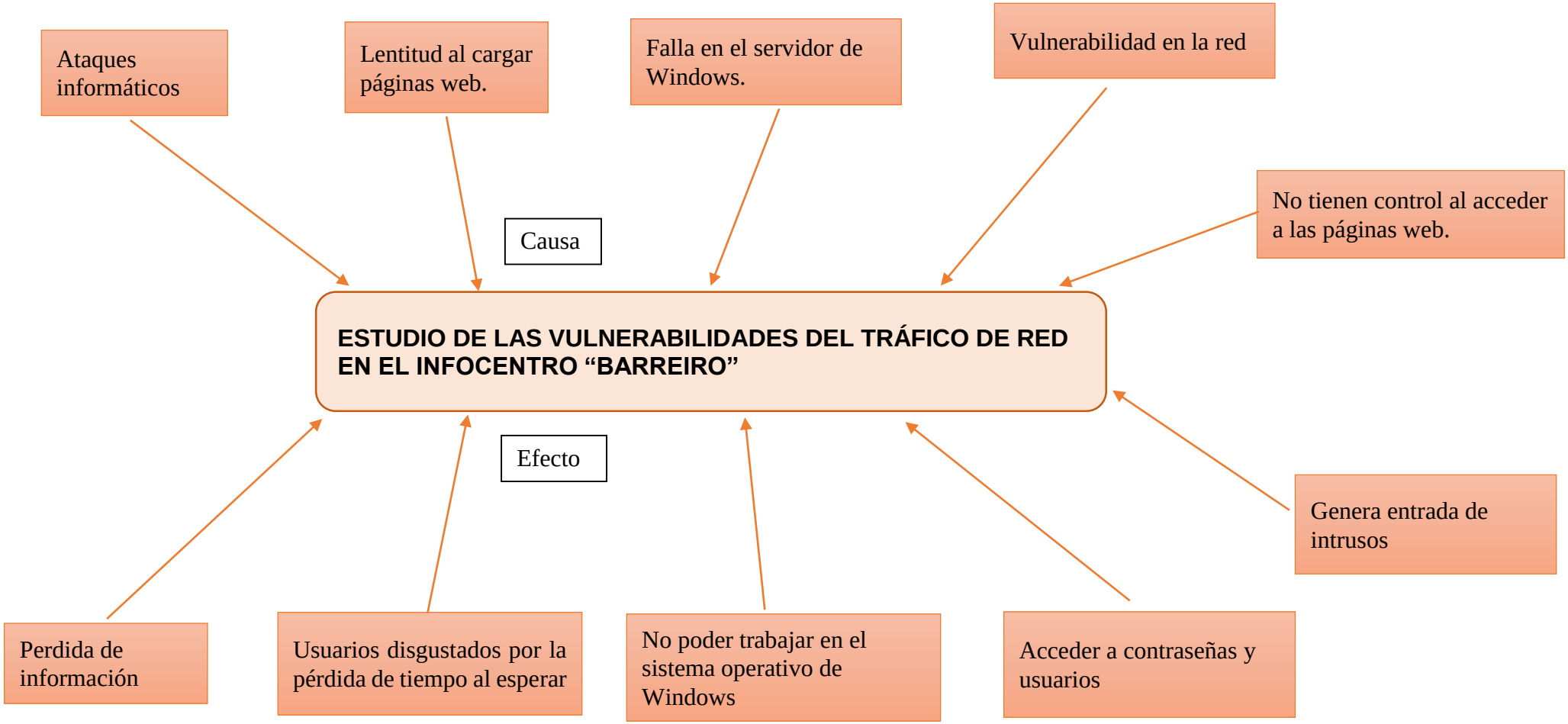
b) No

7. ¿Conoce los riesgos a los que se presentan la organización al no tener las medidas necesarias en lo que respecta a la seguridad de información?

a) Si

b) No

**ÁRBOL DE PROBLEMAS**



| FORTALEZAS | OPORTUNIDADES |
|---|---|
| ✓ Utilizar antivirus<br>✓ Existente de una persona responsable en el área de sistemas<br>✓ Que el personal a cargo tengo conocimiento en redes | ✓ Te permite realizar actividades escolares.<br>✓ Te permite realizar trámites en línea<br>✓ Puedes capacitarte gratuitamente |
| **DEBILIDADES** | **AMENAZAS** |
| ✓ Pedida de información<br>✓ Lentitud a cargar páginas web<br>✓ Dispositivos de comunicación pocos factibles<br>✓ La falta de cambio regular de los equipos que ya no funciona<br>✓ Pocas cámaras de vigilancia | ✓ Manipulación de la información<br>✓ Que los niños puedan acceder fácilmente a las redes sociales sin control alguno<br>✓ Ataques informáticos |

*Tabla 2 Análisis de FODA*
Elaborado por: Joselin Samaniego