UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2019 – MARZO 2020

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS

Tema:

Analisís de factibilidad de un IDS (sistema de detección de intrusos) en redes para la Cooperativa de Ahorro y Credito San Antonio

EGRESADA:

Nadia Nathaly Arriciaga Dumes

TUTOR:

ING. Alcoser Cantuña Fabian Eduardo

AÑO 2020

INTRODUCCIÓN

Hoy en día la seguridad de la información es un tema de vital importancia para cualquier empresa, compañía o institución pública o privada, el crecimiento de la tecnología, la facilidad para obtener información y el no contar con un sistema de detección de intrusos, obliga a las empresas a tomar medidas de seguridad adicionales y prevenir posibles ataques por personas ajenas a la misma.

Los sistemas de detección de intrusos pertenecen al área aplicada de la seguridad informática encargada de advertir a través de alertas, al administrador de la red, cualquier intento de intrusión, entendiendo como intrusión: la realización de un acto no autorizado como el acceso a un sistema, la ejecución de un programa o ataques a una red de computadoras de área local.

La Cooperativa de ahorro y Crédito "San Antonio" Agencia Vinces se encuentra sujetas a riesgos, vulnerabilidades en su información, ya que manejan grandes cantidades de datos confidenciales de sus clientes y de la propia cooperativa, por tal motivo que se requiere un mayor nivel de seguridad, en los usuarios, en la institución y en la forma de manejar la información a nivel general.

El problema que se presenta dentro de la red informática de la Cooperativa de Ahorro y Crédito San Antonio, es que no está correctamente protegida contra ataques informáticos, de tal manera que pueden causar vulnerabilidad y pérdida de información importante para la institución, además la manipulación de información importante por otros usuarios no autorizados, siendo necesario aplicar una gran cantidad de requisitos de seguridad para la protección de sus recursos.

La metodología de investigación que se utilizó para el desarrollo de este análisis fue la metodología científica utilizando métodos como el método deductivo que se lo utilizo en el

análisis de los procesos de toma de decisiones que se realizan en cuanto a los intrusos para así obtener información acerca de las áreas propensas a ataques por intrusos en la red. El método inductivo parte desde el conocimiento de búsqueda de los intrusos en la red. El método cualitativo se lo utilizará para ver las cualidades el proyecto para poder ser aplicado en la cooperativa de ahorro y crédito "San Antonio". En el método cuantitativo se lo utilizará para las encuestas que serán aplicadas a los usuarios de la institución.

La investigación realizada en la Cooperativa de ahorro y crédito "San Antonio" tiene relación con la línea de investigación del Desarrollo de Sistemas de la Información de la carrera de Ingeniería en Sistemas que pertenece a la Facultad de Administración Finanzas e Informática, debido a que, se trata de identificar los problemas o la situación que existe en la red de la institución.

DESARROLLO

En la actualidad las infraestructuras tecnológicas de las empresas están expuestas a riesgos, debido a que existen muchos tipos de ataques y herramientas que explotan las vulnerabilidades de las empresas. Por tal motivo es necesario prevenir ataques, de manera que se pueda mitigar un IDS, con reglas flexibles, potentes y sencillas, para poder mejorar la seguridad de la información.

El presente estudio se realizó en la Cooperativa de Ahorro y Crédito "San Antonio" que se encuentra ubicada en el cantón Vinces de la Provincia de Los Ríos, la cual no cuenta con herramientas de detección de intrusos en la red para fortalecer su seguridad y no sufrir alguna alteración de la información debido a ataques. Existen diversas herramientas para tener una buena seguridad como pueden ser los firewalls, los antivirus o los IDS.

Sistemas de detección de intrusos

Un IDS es un elemento que monitorea la información que circula por una red de datos e identifica posibles ataques. Cuando surge un ataque, el sistema reaccionará informando al administrador y cerrará las puertas al posible intruso reconfigurando los elementos de la red como los firewalls y los routers. (López, 2009)

La detección de intrusión significa detectar un uso no autorizado o ataque a un sistema de red. Los IDS se diseñan para detectar ciertos ataques o usos no autorizados de sistemas, redes u otros recursos, y desviarlos o impedirlos si es posible. Un IDS se puede considerar como un antivirus para intrusos, ya que los dos tienen una base de datos firmada, hacen comparaciones con las firmas y generan alertas (Toro, 2015, pág. 107).

Seguridad perimetral

La seguridad perimetral es importante para una empresa ya que vigila el perímetro de la red permitiendo niveles de confianza en los usuarios y restringiendo todo aquello que pueda hacer daño en la red.

> La seguridad perimetral trata de solucionar el problema de la seguridad de las redes corporativas. La seguridad perimetral propone la disposición estratégica de los equipos en subredes debidamente protegidas de accesos externos no autorizados mediante cortafuegos. Un cortafuego es un dispositivo que filtra las comunicaciones que entran y salen de una subred, cerrando todos los puertos innecesarios y bloqueando por tanto los servicios no autorizados. (Arroyo, 2016)

Tomando el punto de vista de Arroyo se puede señalar que la seguridad perimetral es una defensa ante ataques en la red la cual tiene como objetivo restringir el paso a los enemigos, limitando el acceso a paquetes confiables que circulan por la red, para así evitar perdida de información indispensable para una empresa.

El firewall tiene como objetivo filtrar las conexiones que ingresan a la red examinando todos los paquetes que se dirigen hacia ella, evitando la propagación de códigos maliciosos e intrusiones en la misma. Un firewall sirve para proteger la red de accesos no autorizados los cuales pueden manejarse a nivel de hardware y software. El IDS y el firewall con herramientas complementarias para evitar riesgos en la información.

Tipo de IDS

Los tipos más importantes de IDS para el campo de seguridad son los IDS basados en Host y los IDS basados en la Red que explicarán a continuación:

IDS basados en Host (HIDS)

Desde el punto de vista de (Botina, 2018) se puede definir que un HIDS "analiza diferentes áreas para determinar el uso incorrecto como acciones maliciosas que se presentan dentro de la red o intrusiones de accesos no autorizados, comparan los registros contra una base de datos interna de particularidades comunes sobre ataques conocidos. (Botina, 2018)

Los IDS basados en host generalmente pueden ser instalados individualmente en equipos corporativos en una red empresarial. De tal manera que:

> Los IDS basados en hosts filtran los registros, los analizan, vuelven a etiquetar los mensajes anómalos con su propia clasificación de severidad y los reúne en su propio registro para que sean analizados por el administrador. Los IDS basados en host también pueden verificar la integridad de los datos de archivos y ejecutables importantes (Vallejo de la Torre, Marcillo Sánchez & Uvidia Vélez, 2018).

Los HIDS suelen instalarse en las maquinas que componen la red, los cuales se basan en la supervisión de las acciones de los usuarios y de los archivos del servidor, analizando la máquina de manera que se pueda detectar situaciones importantes que indiquen que el sistema puede ser atacado por hacker, considerando así la toma medidas de prevención que sean necesarias para proteger el sistema.

IDS basados en la Red (NIDS)

Los NIDS aquéllos que monitorean y analizan los paquetes que circulan en la red para detectar actividades maliciosas que puedan atacar contra un sistema.

> Un IDS basado en la red tiene como función escanear los paquetes de red al nivel del enrutador o host, auditar la información de los paquetes y registrar cualquier paquete sospechoso en un archivo de registros especial con información

extendida. Basándose en estos paquetes sospechosos, un IDS basado en la red puede escanear su propia base de datos de firmas de ataques a la red y asignarles un nivel de severidad para cada paquete (Red Hat Inc, 2005).

Como señalo (Pilataxi, 2019) “Los IDS basados en la red son aptos para el escaneo de numerosas actividades en la red detectando transmisiones sospechosas, son bien aceptos dentro de la industria de seguridad” (Pilataxi, 2019)

Los NIDS no afectan el rendimiento de las computadoras ya que puede situarse en cualquiera de ellas, esto se debe a que utilizan el tráfico de la red.

Métodos del atacante

El ataque de “denegación de servicio” se caracteriza por un explícito intento de los atacantes para evitar que los usuarios legítimos de un servicio realicen uso de este. Los ejemplos incluyen:

- Inundación de una red, evitando así el tráfico de red legítimo.
- Interrumpir un servidor mediante el envío de más solicitudes de lo que posiblemente puede manejar, lo que impide el acceso a un servicio.
- Impedir a una persona en particular el acceso a un servicio.
- Interrumpir el acceso a un servicio específico a una persona.

Herramienta SNORT como alternativa para la Detección de Intrusos

Snort desarrollado por Sourcefire, es un sistema para la prevención y detección de intrusión en la red IDS / IPS su mayor despliegue es debido a la composición de los beneficios de la firma, el protocolo y la inspección de anomalías basado en Snort convirtiéndolo en uno de los IDS de red más populares, actualizados y robustos.

> Snort sirve para el análisis de paquetes y detector de intrusos basados en red, este software flexible ofrece un sinnúmero oportunidades como la capacidad de almacenamiento de sus bitácoras en archivo de texto, en base de datos como MySQL, además se puede ejecutar un motor de detección de ataques y barrido de puertos, Snort permite realizar un registro de todas las alertas que se presentan durante una anomalía, igualmente responde a cualquier suceso previamente definido (Ramirez, 2019).

Según (Ocampo, Castro, & Solarte, 2017) Snort es un "lenguaje muy sencillo ya que contiene reglas flexibles y potentes, su instalación es sencilla ya que tiene una serie de filtros o reglas este programa puede desempeñarse como analizador ya que permite monitorear lo que ocurre en la red" (Ocampo, Castro Bermúdez, & Solarte Martínez, 2017)

Como señaló (Jiménez, 2019) "Snort es una herramienta gratuita con licencia GPL, funciona bajo plataformas Windows y UNIX/Linux. Dispone de una gran cantidad de filtros ya predefinidos, así como actualizaciones constantes ante ataques, vulnerabilidades que vayan siendo detectadas" (Jiménez, 2019)

Retomando el punto de vista de (Ocampo, Castro, & Solarte, 2017) "Cuando se presente un ataque los usuarios tienen la capacidad de crear firmas basadas en las características del ataque de la red, para sí poder informar y beneficiar a todos los usuarios" (Ocampo, Castro Bermúdez, & Solarte Martínez, 2017)

Arquitectura de Snort

La arquitectura de Snort se basa en cinco componentes principales

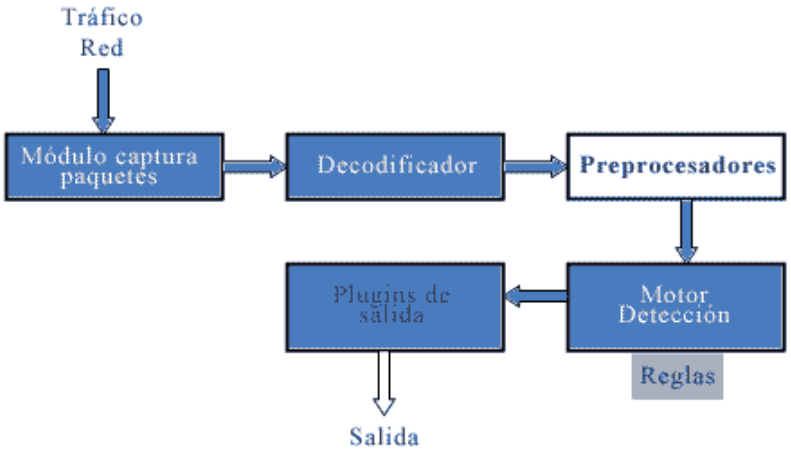

Ilustración 1 Arquitectura de Snort. Fuente: (Sánchez Lorente, 2015)

Decodificador de paquetes (sniffer)

Es el dispositivo que se encarga de capturar los paquetes que viajan por la red. En realidad, se trata de una serie de decodificadores que clasifican el tráfico capturado según de qué protocolo sea, para facilitar su análisis posterior en el Preprocesador. (Olmedo, 2018)

Preprocesador

Recibe los paquetes sin tratar del decodificador. Manipula los paquetes recibidos de forma eficiente para que a continuación se analicen en el motor de detección. De esta manera, el tráfico queda ordenado y se pueden aplicar las reglas para poder identificar un ataque concreto (Sánchez Lorente, 2015).

Según (Sánchez, 2015) “Los procesadores de Snort son en realidad pequeños programas C que toman decisiones para saber qué hacer con un paquete, los cuales se compilan junto a Snort en forma de librería y son muy flexibles” (Sánchez Lorente, 2015)

Motor de detección

Contrasta los datos recibidos del preprocesador con las reglas definidas y emite alertas, si se analizan y observan los paquetes para detectar los ataques según las reglas definidas. Esta parte es muy importante en Snort, ya que debe detectar cualquier indicio de intrusión en un paquete. Si alguna de las reglas coincide con la información capturada, el motor de detección avisa al sistema de notificaciones indicando la regla que ha saltado. (Polvoreda, 2017)

Reglas de detección

Las reglas se agrupan en un conjunto de firmas que categorizan los incidentes. Se leen y se comparan con cada paquete. Se realiza una acción apropiada si un paquete equipara con cualquier regla, como registrar el paquete o generar una alarma. De lo contrario, el paquete se descarta (Sánchez Lorente, 2015).

Sistema de notificaciones

Permite generar ficheros de registro, enviar las alertas por la red o almacenar la información en un gestor de la base de datos. El sistema de notificaciones de Snort utiliza un esquema de plugins para el tratamiento de la información, como también lo hacen el motor de detección y el preprocesador (Sánchez Lorente, 2015).

Caracterización de la empresa

La cooperativa de ahorro y crédito “San Antonio” es una institución de intermediación financiera sólida, rentable, competitiva y solidaria al servicio de la provincia de Los Ríos, con servicios financieros orientados a las necesidades de la comunidad; procesos y sistemas de control adecuados a su gestión, tecnología innovadora y un equipo profesional comprometido con el servicio al socio. (Cooperativa San Antonio, 2016)

La cooperativa de ahorro y crédito “San Antonio” de Vinces cuenta con un personal de 5 personas, este análisis se ha elaborado para saber si los activos y la información de la cooperativa está propensa a riesgo y ser vulnerada por intrusos o usuarios no autorizados que ingresen a la red de dicha empresa.

Se determinó que una de las causas de los problemas que presenta la Cooperativa de ahorro y crédito “San Antonio” se debe a que por el momento no existe ningún tipo de sistema de detección de intrusos, la red de la institución no está adecuadamente protegida ya que cuentan con el firewall que posee Windows por defecto y no tienen una herramienta firewall mediante software o hardware, es muy importante que las empresas por lo menos tengan una herramienta de este tipo ya sea en software o hardware, debido a que un firewall protegerá los equipos conectados a la red de intrusiones, spam, virus y un sinnúmero de ataques a los que están expuestos los equipos.

De acuerdo a lo estudiado y analizado sobre los firewalls una solución a este problema sería que la institución opte por una herramienta firewall mediante hardware ya que todos los paquetes de la empresa pasarían a través de él y así obtener una mejor seguridad, pero la desventaja de obtener dicho hardware será el precio y la dificultad al configúralo, por tal motivo lo factible para la empresa es obtener un firewall mediante software los cuales permiten bloquear aplicaciones sospechosas y se los puede obtener de manera gratuita.

Es importante que la Cooperativa de Ahorro y Crédito tenga como opción la implementación de una herramienta que intente detectar o monitorizar los eventos ocurridos en la red, en busca de intentos de comprometer la seguridad de la información, ya que una de las ventajas que tendrá dicha implementación será generar confianza de los usuarios en la seguridad de la red.

Problemas que presenta la Cooperativa de ahorro y crédito “San Antonio”		
Elemento	**Problema**	**Solución**
Firewall	La institución solo cuenta con el firewall que viene integrado en Windows.	La institución puede obtener un software de firewall como Kaspersky, está disponible para Windows y tiene un costo de $134.95 anual para 5 dispositivos lo que si estaría factible para la institución porque dicha institución solo cuenta con 5 equipos de cómputo. Puede optar por el antivirus TinyWall que es gratuito para no presentar gastos en la institución, aunque no dispone de las mismas prestaciones que el pagado.
Antivirus	La institución cuenta con el antivirus ESET Security.	Puede optar por un mejor antivirus como Norton LifeLock que tiene un precio de $39.99 anual. También existe un antivirus gratuito que es Avast que incluso sin tener que pagar ofrece una protección aceptable.
Contraseñas	Los usuarios de la institución solo unan una condición en sus contraseñas que es que dicha	Los usuarios de la institución deberían de aplicar condiciones para las contraseñas como pueden ser que

	contraseña sea mayor a 8 dígitos, por tal motivo están vulnerables.	tengan letras minúsculas, letras mayúsculas, que incluyan números y caracteres especiales para así tener una contraseña completamente segura.
Sistemas Antispam	La institución no cuenta con sistemas Antispam ya que ocupan espacio innecesario y sobrecarga la red.	Implementación de la herramienta SpamAssassin que es una solución OpenSource muy eficiente que sirve para eliminar correos no deseados con un valor de $48.77 anual. La empresa puede optar por una herramienta 100% gratis como lo es SPAMfighter.
Navegador Web	La institución usa uno de los navegadores más comunes que es el Google Chrome. Ciertos usuarios lo utilizan para navegar en sus redes sociales u otras actividades ajenas a la empresa y mediante estas actividades se pueden presentar problemas de virus ya que la navegación web es la principal entrada de virus.	Se debe hacer uso adecuado de los recursos de la institución, de tal manera que la empresa debe de restringir ciertas paginas para que los usuarios no puedan acceder a ellas y así no presentar problemas de cualquier tipo de ataque o pérdida de información.
IDS	No se cuenta con ningún tipo de IDS y no puede controlas los	La institución debe optar por la implementación de la herramienta IDS

	accesos no autorizados.	Snort. Esta herramienta es muy factible para la institución porque se ejecuta en sistemas operativos como Windows que es el que posee la empresa, además esta herramienta es fácil y sencilla de manejar ya que los usuarios poder personalizar sus propias reglas. Es totalmente gratuito y la empresa no presentara ningún tipo de gasto.

Tabla 1 Problemas que se presentan en la Cooperativa de ahorro y crédito " San Antonio" . Fuente: Autor

Los equipos de la Cooperativa de ahorro y crédito “San Antonio” no tenían activado el firewall por tal motivo se procedió a la activación del mismo para que los equipos no estén propensos a ataques.

Especificaciones de las PC de la Cooperativa de ahorro y crédito “San Antonio”		
Cantidad	**Especificaciones**	**Ubicación**
2	• Procesador Intel Core i5 • Disco Duro SATA de 1TB • Memoria RAM de 8 GB SDRAM DDR3 • Sistema Operativo Windows 10 Pro (32 Bits)	• Atención al Socio • Cajera
3	• Procesador Intel Core	• Jefe de Agencia

	i7-9700, 8 núcleos • Disco Duro SATA de 2TB • Memoria RAM de 16 GB • Sistema Operativo Windows 10 Pro (64 Bits)	• Asesor de Negocios • Asesora de Negocios

Tabla 2 Especificaciones de las PC de la Cooperativa de ahorro y crédito "San Antonio". Fuente: Autor

Población y Muestra

Se ha considerado la siguiente población para la siguiente investigación:

Datos	Cargo	Cantidad
Paredes Rodriguez Darwin Daniel	Jefe de Agencia	1
Huacon Suarez Washington Calixto	Asesor de Negocios	1
Miño Gurumendi Elba Lisbeth	Asesora de Negocios	1
Medrano Suarez Gabriela	Atención al Socio	1
Yela Cervantes Eileen Stephanie	Cajera	1
Total		**5**

Tabla 3 Personal que conforma la Cooperativa de ahorro y crédito "San Antonio" en Vinces. Fuente: Autor

Como la población que se ha considerado es reducida, formará parte del total de la investigación para la realización de una encuesta.

Análisis de factibilidad

A continuación, se procederá a realizar el análisis de factibilidad mediante tres aspectos como lo son la factibilidad técnica, la factibilidad operativa y por último la factibilidad

económica, para poder considerar la posibilidad de implementar un IDS en redes de la cooperativa de ahorro y crédito “San Antonio”.

Factibilidad Técnica

En la actualidad la cooperativa de ahorro y crédito “San Antonio" cuenta con 5 equipos de cómputos asignadas al personal administrativo, estos a su vez están conectados a una LAN. El hardware requerido está dentro de la lista de los dispositivos con los que cuenta la institución, es decir que la institución no requerirá incurrir en gastos para la implementación del Sistema Detector de Intrusos.

Factibilidad Operativa

Desde el punto de vista operativo el Sistema Detector de Intrusos, será de apoyo para la Institución y sus directivos en la realización del uso cotidiano de sus dispositivos dentro de la red en la cooperativa de ahorro y crédito “San Antonio”, puesto que contribuirá en la seguridad interna y externa de la red con la que cuentan como institución.

Este sistema cuenta con una interfaz gráfica de fácil aprendizaje, con un alto nivel de interacción con el usuario, lo que lo convierte en una herramienta de gran utilidad para la institución.

La cooperativa de ahorro y crédito “San Antonio” puede aceptar la implementación de una herramienta de Sistema detector de Intrusos, debido a que esta herramienta le proporciona mayor seguridad y disminuye la ralentización de la red. El administrador del IDS tendrá que ser capacitado.

Factibilidad Económica

Para esta propuesta, en cuanto a costos de software, recursos humanos e insumos la empresa se ahorra ya que la herramienta que se utilizara es Snort la cual distribución de LINUX, que permite su distribución sin ningún costo de licencias.

Conclusión del Análisis de Factibilidad

Demostrado los estudios de factibilidad técnica, operativa y económica se llega a la conclusión que este estudio de factibilidad resulta ser favorable para la institución. Lo que determina su viabilidad. El estudio resulta ser una buena herramienta para la institución, además no implica que la Cooperativa de Ahorro y Crédito "San Antonio" incurra en gastos.

Análisis de la problemática en la Cooperativa de Ahorro y crédito "San Antonio"

La existencia de amenazas que afectan la disponibilidad, integridad y confidencialidad de los datos es real. Es difícil para las organizaciones ecuatorianas poder identificar esas amenazas y adoptar recomendaciones que permitan prevenir, destacar y protegerse de ellas.

La Cooperativa de ahorro y crédito "San Antonio", no está ajena a esta situación, razón por la cual se creyó importante aportar una solución que permita mejorar el nivel de seguridad de la información que la entidad maneja.

Una posible solución para la Cooperativa de ahorro y crédito "San Antonio" puede ser la implementación de una herramienta IDS (Sistema de detección de intrusos) en la red de dicha institución, una metodología de prevención de intrusos basada en normas y metodologías de análisis y gestión de riesgos que servirían de guía para el desarrollo de una metodología adaptada a la problemática en inseguridad que la entidad poseía.

CONCLUSIONES

El análisis se realizó en la Cooperativa de Ahorro y Crédito “San Antonio” ubicada en el cantón Vinces el cual permitió conocer el nivel de riesgo de la información que posee la institución, mediante el cual se concluye que este análisis de un sistema de detección de intrusos en redes es factible ya que así se obtendrá una mejor seguridad en la información en dicha institución.

Una herramienta IDS (Sistema de detección de intrusos) permitirá estar al tanto cuando esté siendo atacada la red, la cual contribuirá información necesaria y valiosa para determinar los ataques. A pesar de que los IDS sean factible para una empresa y que sean de seguridad perimetral, es necesario complementarlo con otros controles de seguridad en el enfoque de seguridad en profundidad como los firewalls.

Un sistema de detección de intrusos como lo es Snort es importante para mejorar la seguridad de una red el cual crea reglas flexibles, potentes y sencillas que las comunicaciones sean seguras. Snort es gratuito y funciona bajo plataformas como Windows y UNIX/Linux esta herramienta permite registrar, alertar y responder ante cualquier anomalía mediante la implementación de un motor de detección de ataques y barridos de puertos.

En la Cooperativa de ahorro y crédito “San Antonio” utilizan los inicios de sesión para acceder a la información, sus claves de inicio de sesión no son muy seguras ya que sus claves solo la única regla que cumplen es que sea mayor de 8 dígitos, además solo hacen cambio de claves cuando ellos deseen cambiarla, no tienen un tiempo definido para cambiar las claves.

Bibliografía

Arroyo, L. P. (2016). *Docplayer.es*. Obtenido de Docplayer.es: https://docplayer.es/14271324-1-objetivos-del-proyecto-4-2-alcance-del-proyecto-6-3-estado-del-arte-8-3-1-sistemas-de-deteccion-de-intrusos-8.html

Botina, J. B. (2018). *Diseño de la arquitectura de seguridad perimetral de la red informática en la industria de licores del valle.* Santiago de Cali: Universidad Autónoma de Occidente.

Cooperativa San Antonio. (2016). *San Antonio Cooperativa de Ahorro y Crédito*. Obtenido de San Antonio Cooperativa de Ahorro y Crédito: http://coopsanantonio.fin.ec/vision.html

Jiménez, J. G. (2019). *CONFIGURACIÓN DE UNA HERRAMIENTA OPEN SOURCE PARA LA DETECCIÓN DE INTRUSOS EN REDES WIFI CASO DE ESTUDIO: SURICATA IDS.* Loja: Universidad Nacional de Loja. Obtenido de http://dspace.unl.edu.ec:9001/jspui/bitstream/123456789/22835/1/Gutierrez%20Jimenez%2C%20Jimena%20Gabriela.pdf

López, J. G. (2009). *Optimización de sistemas de detección de intrusos en red utilizando técnicas computacionales avanzadas.* Editorial Universidad de Almería.

Olmedo, H. C. (2018). *Sistema de desvío de intrusiones de red.* Valladolid: Universidad de Valladolid.

Pilataxi, W. (28 de Enero de 2019). *Scribd.com.* Obtenido de Scribd.com: https://es.scribd.com/document/398389761/Alarma-Antirrobo-o-Hurto

Polvoreda, J. L. (2017). *SISTEMA DE MONITORIZACIÓN DEL IDS SNORT.* Valencia: Universitat Politècnica de València.

Ramirez, C. J. (20 de Mayo de 2019). *Backtrack Academy*. Obtenido de Backtrack Academy: https://backtrackacademy.com/articulo/deteccion-de-intrusos-en-la-red-snort

Toro, J. A. (2015). *Mantenimiento de la infraestructura de la red de comunicaciones.* Elearning, S.L.

Britos, J. D. (2010). *Detección de Intrusiones en redes de datos con captura distribuida y procesamiento estadístico* [Universidad Nacional de La Plata]. http://sedici.unlp.edu.ar/bitstream/handle/10915/4190/Documento_completo.pdf?sequence=1&isAllowed=y

Ocampo, C. A., Castro Bermúdez, Y. V., & Solarte Martínez, G. R. (2017). Sistema de detección de intrusos en redes corporativas Intrusion Detection System in Corporate Networks. *Scientia et Technica Año XXII*, *22*(1), 60–68.

Red Hat Inc. (2005). Red Hat Enterprise Linux 4: Manual de seguridad. *RedHat*, *1.0*, 132. http://web.mit.edu/rhel-doc/4/RH-DOCS/pdf/rhel-rg-es.pdf

Sánchez Lorente, O. (2015). Detección de intrusiones con Snort. *Universitat Oberta de Catalunya*. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43090/6/osanchezloTFM0715memoria.pdf

Vallejo de la Torre, C. A., Marcillo Sánchez, P. M., & Uvidia Vélez, M. V. (2018). SISTEMAS DE PREVENCIÓN DE INTRUSOS (IDS) EN LA GESTIÓN DE LA INFORMACIÓN. In *Centro de Investigación y Desarrollo Profesional (CIDEPRO)*. https://doi.org/10.1017/CBO9781107415324.004

Interpretación de resultados de la encuesta realizada a los usuarios de la Cooperativa de ahorro y crédito "San Antonio"

1.- ¿Dentro de la red de la institución se puede enviar y recibir información de gran importancia con seguridad?

ITEMS	RESULTADOS	%
Si	1	20%
No	4	80%
Total	**5**	**100%**

Tabla 4 Resultado de la pregunta 1 de la encuesta realizada. Fuente: Autor

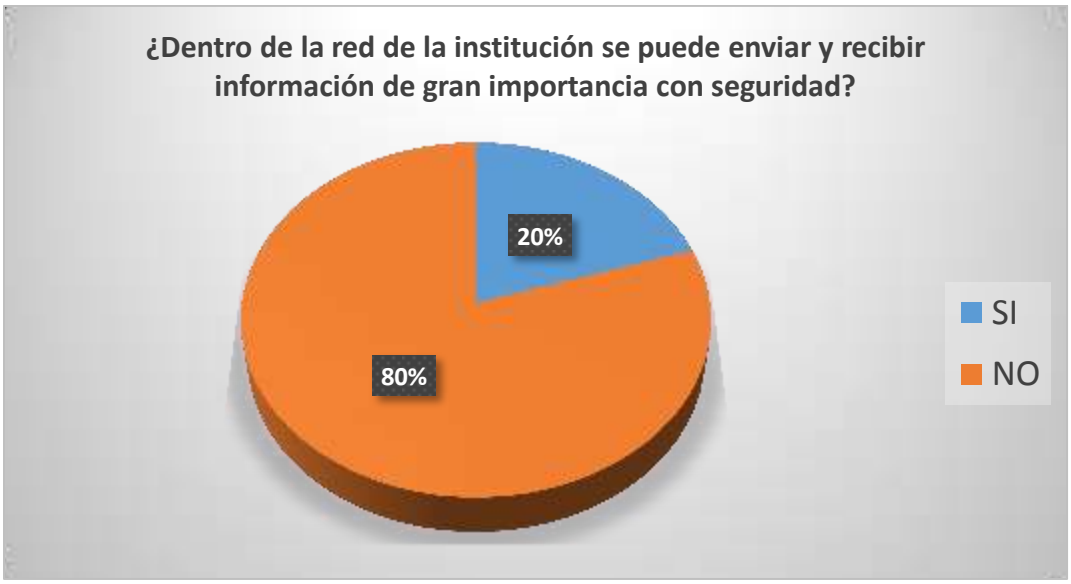

Ilustración 2 Resultado de la pregunta 1 de la encuesta realizada. Fuente: Autor

Análisis: Se evidencia que un 80% de los encuestados no pueden enviar y recibir información de gran importancia con seguridad.

2.- ¿En los procesos de seguridad, se protege su información confidencial?

ITEMS	RESULTADOS	%
Si	2	40%
No	3	60%
Total	**5**	**100%**

Tabla 5 Resultado de la pregunta 2 de la encuesta realizada. Fuente: Autor

Ilustración 3 Resultado de la pregunta 2 de la encuesta realizada. Fuente: Autor

Análisis: De acuerdo con las encuestas realizadas el 60% de los encuestados opino que no se protege su información confidencial y el 40% que si se protege la información.

3.- ¿Cómo califica la velocidad en el acceso a la información interna para realizar su trabajo?

ITEMS	RESULTADOS	%
Muy Bueno	1	20%
Bueno	3	60%
Malo	1	20%
Total	**5**	**100%**

Tabla 6 Resultado de la pregunta 3 de la encuesta realizada. Fuente: Autor

Ilustración 4 Resultado de la pregunta 3 de la encuesta realizada. Fuente: Autor

Análisis: De acuerdo a la encuesta realizada un 20% de los encuestados opinaron que es muy bueno la velocidad en el acceso a la información interna para realizar su trabajo, un 40% opino que es bueno y un 20% que es malo.

4.- ¿Con qué frecuencia considera usted que debería existir un monitoreo permanente dentro

de la red de la institución?

ITEMS	RESULTADOS	%
Semanal	2	40%
Mensual	2	40%
Cada 6 Meses	1	20%
Total	**5**	**100%**

Tabla 7 Resultado de la pregunta 4 de la encuesta realizada. Fuente: Autor

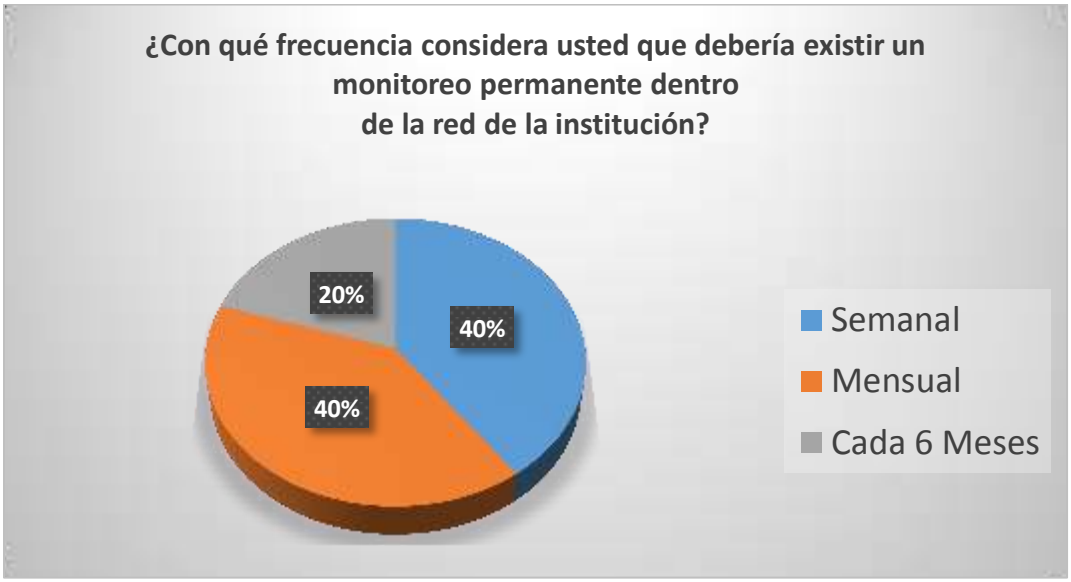

Ilustración 5 Resultado de la pregunta 4 de la encuesta realizada. Fuente: Autor

Análisis: De acuerdo a la encuesta realizada un 40% de los encuestados opinaron que debería existir un monitorio semanal dentro de la red de la institución, un 40% opino que debería ser mensual y un 20% que sea cada 6 meses.

5.- ¿Dentro de la institución usted ha sido víctima de un ataque informático?

ITEMS	RESULTADOS	%
Si	1	20%
No	4	60%
Total	**5**	**100%**

Tabla 8 Resultado de la pregunta 5 de la encuesta realizada. Fuente: Autor

Ilustración 6 Resultado de la pregunta 5 de la encuesta realizada. Fuente: Autor

Análisis: Según la encuesta realizada el 20% de los usuarios ha sido víctima de un ataque informático y un 80% no ha tenido ningún ataque informático.

6.- ¿Para acceder a la información existente en la red, usted utiliza un Usuario y Contraseña?

ITEMS	RESULTADOS	%
Si	5	100%
No	-	0%
Total	**5**	**100%**

Tabla 9 Resultado de la pregunta 6 de la encuesta realizada. Fuente: Autor

Ilustración 7 Resultado de la pregunta 6 de la encuesta realizada. Fuente: Autor

Análisis: De acuerdo a la encuesta realizada el 100% los encuestados utilizan un usuario y contraseña para acceder a la información.

7.- ¿Dentro de la red los usuarios pueden modificar la información sin previa autorización?

ITEMS	RESULTADOS	%
Si	2	40%
No	.3	80%
Total	**5**	**100%**

Tabla 10 Resultado de la pregunta 7 de la encuesta realizada. Fuente: Autor

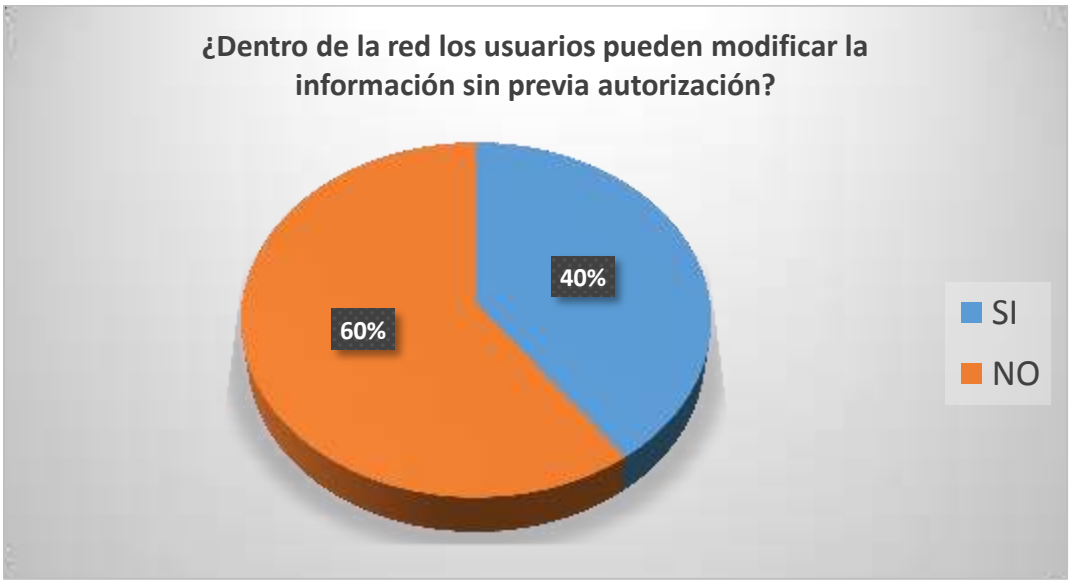

Ilustración 8 Resultado de la pregunta 7 de la encuesta realizada. Fuente: Autor

Análisis: De acuerdo a la información recaudada en su gran mayoría con un 60% los encuestados opinan que tienen negado modificar la información sin previa autorización y un 40% tiene permitido acceder a la información.

8.- ¿Cree usted que es conveniente el bloqueo de usuarios no autorizados dentro de la red para evitar robo de información valiosa?

ITEMS	RESULTADOS	%
Si	4	80%
No	1	20%
Total	**5**	**100%**

Tabla 11 Resultado de la pregunta 8 de la encuesta realizada. Fuente: Autor

Ilustración 9 Resultado de la pregunta 8 de la encuesta realizada. Fuente: Autor

Análisis: Según los resultados otorgado por la encuesta realizada un 80% de los encuestados están de acuerdo con el bloqueo de usuarios no autorizados dentro de la red para evitar robo de información valiosa y un 20% no está de acuerdo.

9.- ¿Considera usted necesario una defensa como una herramienta IDS (sistema de detección de intrusos) para proteger la red?

ITEMS	RESULTADOS	%
Si	5	100%
No	-	0%
Total	**5**	**100%**

Tabla 12 Resultado de la pregunta 9 de la encuesta realizada. Fuente: Autor

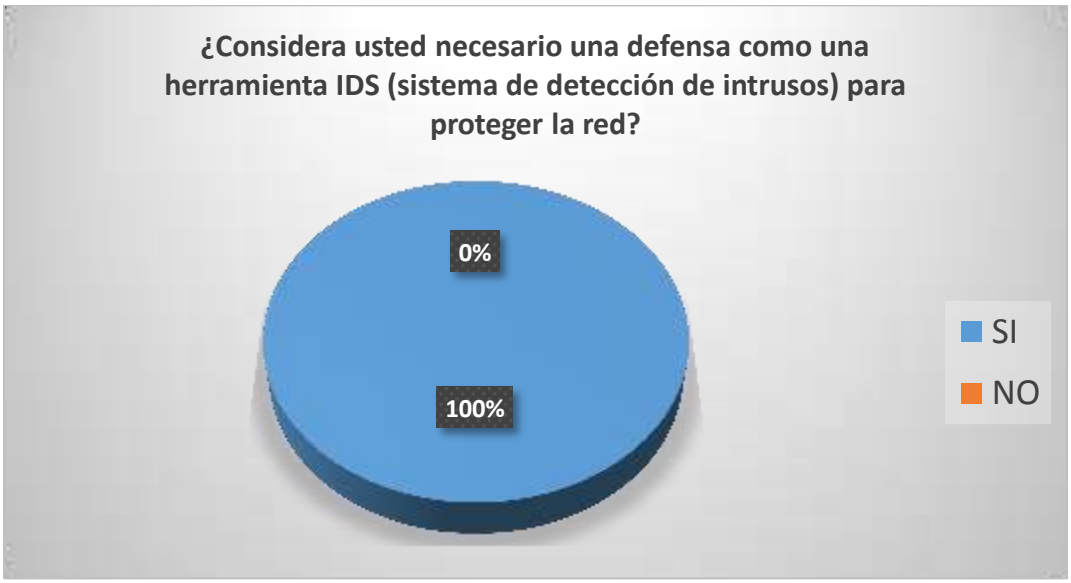

Ilustración 10 Resultado de la pregunta 9 de la encuesta realizada. Fuente: Autor

Análisis: De acuerdo a la encuesta realizada todos los encuestado están de acuerdo en tener una defensa como una herramienta IDS para proteger la información de la red.