Firewall PfSense como opción de código abierto para la seguridad de la red informática en centros escolares católicos de Santa Ana

Vidal Enrique Cerritos Magaña
Licenciado en Computación Administrativa Empresarial
Docente investigador. Facultad de Ciencias Empresariales
Universidad Católica de El Salvador, El Salvador
vidal.cerritos@catolica.edu.sv

Fecha de recepción: 19-11-2017 / **Fecha de aceptación:** 04-02-2018

Resumen

La investigación tiene como objetivo indagar sobre las herramientas de seguridad a nivel de hardware y software; y las políticas y prácticas que utilizan los centros escolares católicos del departamento de Santa Ana para mantener la seguridad de la red informática. En la investigación se propone el Firewall Pfsense por ser una herramienta gratuita de código abierto para la seguridad en el acceso en red y que se puede implementar en equipos de bajo costo.

El estudio fue de tipo descriptivo, ya que se analizaron y describieron las características y ventajas del Firewall PfSense. Se utilizó principalmente la encuesta y la entrevista como instrumento para obtener la información relacionada a la seguridad. Se abordó directamente de los encargados del área de informática; también se consultó bibliografía relacionada con el sistema Firewall propuesto y las políticas y prácticas de seguridad recomendadas.

Se encontró que los centros escolares católicos no implementan sistemas dedicados para la seguridad como Firewalls, por requerir altos conocimientos del funcionamiento, de redes informáticas y protocolos de comunicación que implementan las herramientas específicas que se configuren en ellos.

Palabras clave: Centros escolares católicos, políticas y prácticas de seguridad, Firewall Pfsense, herramientas de seguridad informática.

Abstract

The research objective is to investigate about hardware and software safety tools as well as Santa Ana's Catholic Schools policies and practices used to maintain their computer network safety. This research proposes Firewall Pfsense since it is a free and safe open- code tool to network access that can be implemented in low cost equipment.

This was a descriptive research since the characteristics and advantages of Firewall PfSense were analyzed and described. In order to obtain data related to the network safety, researchers used mainly the following tools: a survey and an interview. The staff in charge of the computer network were directly approached. Also, researchers consulted bibliography related to the proposed Firewall system and the recommended safety policies and practices.

Research found that Catholic schools do not implement safety systems such as Firewalls due to the requirement of advanced operation knowledge of computer networks and communication protocols which implement their adjusted specific tools.

Key words: Catholic schools, policies and safety practices, Firewall Pfsense, computer network safety tools.

1. Introducción

El uso de las tecnologías de la información y comunicación (TIC)[1] se han vuelto indispensables para casi todos los ámbitos: laboral, empresarial, escolar, familiar, social, etc. Los beneficios obtenidos de su uso son grandes y contribuyen al desarrollo, pero desgraciadamente hay quienes utilizan las TIC con fines egoístas y dañan de muchas maneras a otros usuarios.

Para Pérez y Merino (2008), la seguridad informática "es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático". Es muy difícil asegurar en un 100% un sistema, aunque se utilicen las técnicas y software más avanzados. Se han dado casos en los que importantes empresas a nivel mundial han sido víctimas de violaciones de seguridad, aun teniendo implementados equipos y sistemas para tal fin en su plataforma de red. Pero al no contar con un sistema de seguridad, los riesgos de ataques o accesos indebidos de los usuarios puede traer problemas mayores.

En el ámbito de la informática, la seguridad es de las áreas que más preocupan a las empresas y a las instituciones. Proteger la red de una empresa o institución es un tema al que debe prestarse atención, ya que están en juego la integridad de los datos, la salud mental de sus miembros, el uso indebido de los recursos y del tiempo. El Firewall se puede considerar como una herramienta importante para establecer reglas que permitan controlar los sistemas informáticos tanto a nivel de hardware como de software.

La seguridad se logra mediante la implementación de un apropiado sistema de controles, que pudieran ser políticas, prácticas, estructuras organizacionales y funciones de software. Las funciones asociadas a la Seguridad informática según Vañó (2016) son las siguientes:

- **Regulación:** capacidad de establecer las normas, preceptos reglamentos y otro tipo de medidas jurídicas que garanticen las bases para lograr un nivel de seguridad adecuado.
- **Prevención:** las acciones que se realizan con el fin de minimizar los riesgos contra los activos informáticos.
- **Detección:** Conocimiento de la materialización de una amenaza contra los activos informáticos.
- **Enfrentamiento:** Acciones de respuesta a un hecho detectado contra los activos informáticos.

Es fundamental saber que recursos de la institución o empresa necesitan protección para así controlar el acceso a la red y a los sistemas y los derechos que deben tener los usuarios a los sistemas de información.

El constante avance tecnológico y las nuevas amenazas que lo acompañan, complican la situación de seguridad informática en los centros

1. El autor también hará referencia a este término dentro del documento mediante su acrónimo.

educativos. Cada día son más las aplicaciones basadas en Web que utilizan los usuarios de los centros de educación, y a las que acceden desde las redes escolares. Esta evolución se debe a las tecnologías Web 2.0, el acceso remoto de usuarios, el aumento del uso de teléfonos inteligentes y al uso de dispositivos propios (el llamado fenómeno BYOD[2], en continuo crecimiento). Los departamentos de Tecnología Informática (TI) de las escuelas deben controlar y ponderar el uso de las aplicaciones productivas y las no productivas e incluso potencialmente peligrosas (Malecki, 2013).

El acceso a la red de Internet ofrece grandes posibilidades para la obtención de información de los usuarios, pero el ser una red abierta, los sistemas pueden sufrir ataques o intrusión de personas ajenas que puede poner en riesgo los sistemas o los datos.

Los alumnos de las instituciones educativas desconocen en su mayoría los riesgos cuando se acceden a sitios inapropiados y descargan aplicaciones que traen consigo, sin que ellos se den cuenta, software malicioso que puede afectar el funcionamiento normal del equipo o robar información personal o del sistema.

Por lo general, los centros escolares católicos que poseen aulas informáticas tienen conexión a Internet, la cual ha sido contratada a un proveedor de servicios, quien como parte del contrato, instala la conexión física (cable de comunicación y aparato de enlace de conexión, comúnmente llamado Modem o Ruteador). Estos componentes son suficientes para que los equipos puedan comunicarse entre ellos y tener acceso a la red de internet.

Dependiendo de los sistemas operativos que utilicen, estos proporcionan herramientas básicas para la seguridad, como Antivirus, Firewall básico y otras herramientas relacionadas. También se instalan softwares adicionales para la seguridad como antispyware, antimalware, etc. Todas estas aplicaciones solucionan en parte el problema de la seguridad, pero hay otro tipo de situaciones que lo complican, como la intrusión externa o la conexión de los usuarios a sitios que atenten contra la moral y que no son controlados por estas herramientas.

El no tener un sistema de seguridad puede poner en riesgo la información personal de los estudiantes, debido a que es común proporcionar datos de usuario para diversos servicios que se utilizan en internet; o cuando se descargan aplicaciones o archivos multimedia de sitios no seguros, también se instalan de forma anónima aplicaciones espías que envían a quienes los proporcionan, datos de los equipos y de los usuarios. Un intruso puede hacer mal uso de estos datos.

Las instituciones educativas como universidades y colegios privados pueden disponer de recursos para adquirir y administrar equipos comerciales, dedicados a la seguridad como un Firewall; pero en la mayoría de centros educa-

2. Bring Your Own Device, entiéndase como "trae tu propio dispositivo", por sus siglas en inglés.

tivos católicos cuyos recursos son limitados, difícilmente podrán adquirir y mantener este tipo de herramientas para la seguridad.

La investigación se enfocó en los centros educativos católicos del departamento de Santa Ana a fin de verificar si disponen de equipos dedicados a la seguridad y políticas o prácticas que contribuyan a mantenerla. Si tales herramientas y normas no se utilizan, proponer un sistema de seguridad a nivel de Software de código abierto (gratuito), que se pueda implementar en uno de los equipos de institución que requiera bajos recursos, considerados para muchos como obsoletos. De esta manera se harán extensivos los beneficios de su implementación, como proyección social, a los centros católicos que no dispongan de tales herramientas para la seguridad informática.

Ante este planteamiento, surgen las preguntas: ¿Utilizan los centros escolares católicos dispositivos o equipos dedicados para controlar el acceso de los usuarios hacia afuera y hacia adentro de la red escolar? ¿Disponen y aplican políticas o medidas de seguridad? ¿Conocen el Firewall Pfsense?

Conceptualización

Los Firewalls son usualmente el primer componente de seguridad de una red. Ellos separan las redes en diferentes niveles de seguridad, utilizando políticas de control de acceso a la red. La función principal de los Firewalls es proteger la red privada local del tráfico de datos no legítimo (Akpah, 2015).

El Firewall está ubicado entre la red de Internet y la red privada. Ellos monitorean todo el tráfico de datos que entra a la red; también pueden prevenir el tráfico de ataques mal intencionados desde Internet: Si una computadora es atacada por un intruso y genera tráfico ilegítimo, el Firewall puede prevenir el ataque y detectar la computadora implicada.

Haciendo una analogía, el Firewall es como un guardia o vigilante que está en la entrada de la casa, institución o comercio que controla quién entra y quién sale; qué es lo que trae consigo o qué es lo que lleva. Si detecta algo sospechoso, procede al registro y previene el ingreso o el egreso de lo sospechoso.

El Firewall controla el tráfico de datos que pasa a través de él con base a reglas definidas por el administrador de la red. Las reglas que definen el tráfico de datos están basadas en las características de los mismos datos: el protocolo de comunicación utilizado, las direcciones IP de origen y de destino, el número o tipo de puerto de comunicación. Las reglas definidas en un Firewall se definen y aplican en las interfaces de red del mismo, en las cuales se permite o se deniega el paso de ciertos tipos de tráfico.

FreeBSD es un sistema operativo para arquitecturas x86 compatibles, derivado de BSD, la versión de UNIX desarrollada en la Universidad de California, Berkeley. FreeBSD es desarrollado y mantenido por un numeroso equipo de personas. En el sitio oficial[3] del sistema operativo se describe que FreeBSD ofrece altas

3. Para mayor información visitar: https://www.freebsd.org/es/

prestaciones en comunicaciones de red, rendimiento, seguridad y compatibilidad, todavía inexistentes en otros sistemas operativos, incluyendo los comerciales de mayor renombre.

PfSense[4] es una distribución personalizada de FreeBSD adaptado para su uso como Firewall[5] y Router[6]. Se caracteriza por ser de código abierto, puede ser instalado en una gran variedad de computadoras, y además cuenta con una interfaz web para su configuración.

El software PfSense incluye características similares a la mayoría de los Firewalls comerciales. También características adicionales que no están disponibles en soluciones de código cerrado comerciales, tales como: Check Point, Cisco PIX, Cisco ASA, Netgear, SonicWALL y otros; este último se ha implementado en la Universidad Católica de El Salvador (Unicaes).

El Firewall Pfsense se implementa de forma nativa en el sistema operativo FreeBSD. Este se deriva directamente del sistema operativo UNIX, del cual también se basan los sistemas operativos populares actuales como Linux, Mac, Solaris y otros. Durante muchos años, FreeBSD ha sido considerado el sistema operativo más seguro del mundo. Otra característica importante es que los requisitos mínimos de instalación y funcionamiento son bajos, por ejemplo: Un equipo con procesador Pentium III con 512 MegaBytes (equipos que fueron lanzados a inicios de siglo).

Para efectos de la investigación se consideró el Firewall Pfsense por ser de código libre, requerir equipos con bajos recursos según los fines del estudio y por las características antes descritas.

2. Metodología

La investigación es de tipo descriptiva, ya que se analizaron y describieron las características y ventajas del Firewall PfSense como opción gratuita para la seguridad informática de los centros escolares católicos del departamento de Santa Ana. Además, se hizo un diagnóstico de las percepciones relativas a la seguridad informática de parte de los encargados de los centros de cómputo, de los directores y de las medidas o políticas utilizadas.

Para la elaboración del marco teórico y la guía propuesta, se consultaron documentos relacionados al tema, procedentes de instituciones educativas de nivel superior que utilizan sistemas dedicados a la seguridad. Se consultaron también documentos de otros organismos que se ocupan de la seguridad informática. Como fuente primaria, se obtuvo información directamente de los encargados de los centros de cómputo y de los directores institucionales de los centros escolares católicos del departamento de Santa Ana.

Debido a que la población objeto de estudio era pequeña, se consideró para la muestra la totalidad de la población. Sin embargo, no todos los centros educativos tenían conexión a Inter-

4. Para mayor información visitar: https://www.pfsense.org/

5. Nombre utilizado para referirse al software que permite controlar el tráfico de datos en una red informática. Puede implementarse como servicio en un sistema operativo o de forma dedicada. La traducción al español es “Cortafuegos”.

6. Dispositivo de red que permite conectar redes, además determina la ruta más corta a los destinos mediante protocolos de enrutamiento. Su traducción al español es “Ruteador”.

net y/ o disponían de centro de cómputo. No se consideraron las instituciones que no impartían clases de informática como las ubicadas en las zonas rurales de del municipio de Texistepeque; y las de difícil acceso por la delincuencia, ubicadas en el municipio de Coatepeque, ambos siempre del departamento de Santa Ana. La población de los centros escolares católicos fue proporcionada por el coordinador diocesano.

Se utilizó principalmente la encuesta como instrumento para obtener la información relevante, destinada a representarla de forma cuantitativa en herramientas electrónicas. También se utilizó la entrevista para obtener información cualitativa de los centros escolares relacionados a la seguridad. Para la tabulación y representación de los datos recolectados, se utilizaron herramientas informáticas como hojas electrónicas de cálculo.

Se contactó con las instituciones que conformaron la muestra para programar cita a través de correo electrónico o vía telefónica. Las que estaban próximas a la zona urbana de Santa Ana, se les visitó directamente.

3. Resultados

De la muestra objeto de estudio, el 60% estuvo concentrado en la ciudad de Santa Ana, el resto se distribuyó en los municipios de mayor población como: Candelaria de La Frontera, Chalchuapa, Coatepeque y Texistepeque.

La información recopilada giró en torno al tema de la seguridad informática, específicamente en la utilización de equipos dedicados a la seguridad (Firewalls), políticas de seguridad, el control de acceso a la red de Internet, conocimiento del Firewalls Pfsense y el filtrado de tráfico de datos hacia adentro y hacia afuera de la red local de los centros escolares.

No todos los centros escolares encuestados incluyen e imparten informática en todos los niveles educativos. El 40% de las instituciones incluyen hasta el nivel de bachillerato, pero el 90% dispone todos los niveles de educación básica (de Primero a Noveno grado). Aunque no a todos los niveles se les imparte informática.

Entre el 70% y 90% de las instituciones estudiadas imparten informática entre Cuarto y Noveno grado. (Ver figura 1).

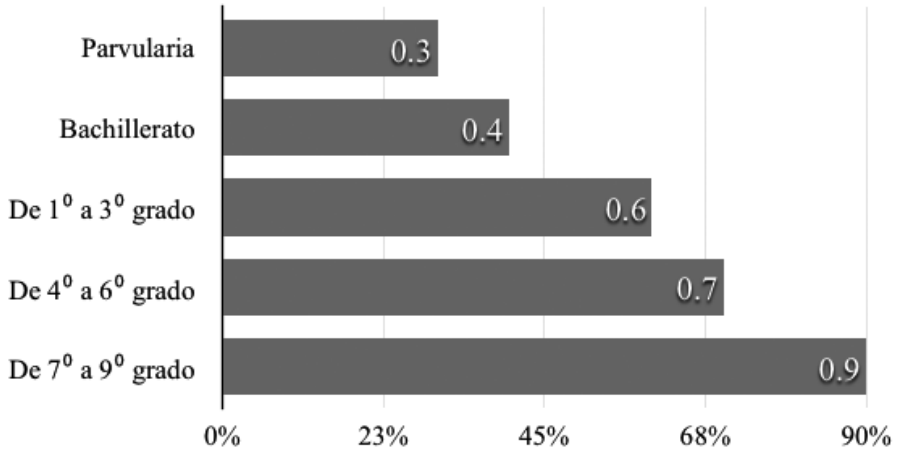

Figura 1. Niveles educativos en los que se imparte Informática dentro de los centros escolares.

El 80% de las instituciones encuestadas tienen instalado el sistema operativo Windows en los equipos del centro de cómputo; de los cuales, el 70% utiliza Windows versión 7, el otro 10% utiliza la versión 8 ó 10 de Windows. Solo un 20% utiliza el sistema operativo Linux de forma exclusiva. Ver figura 2.

El que el 70% de centros escolares utilice el Sistema Windows en las computadoras de los centros de cómputo, implica la necesidad de instalar un antivirus para proteger los datos y las aplicaciones de los mismos. En los sistemas Linux no se requiere antivirus, ya que en estos sistemas no se conoce la existencia de los mismos o que estos causen daños considerables. Sin embargo, el 50% de los equipos que utilizan el Sistema Windows tienen instalado un antivirus en una versión gratuita y un 40% no tiene ningún antivirus.

El hecho que muchas instituciones no tengan implementada una herramienta para la seguridad, facilita la infección por algún tipo de Malware[7] que, al utilizar dispositivos extraíbles en los centros de cómputo y luego introducirlos en los equipos personales, pone en riesgo de infección y en consecuencia, el posible daño de los archivos y datos. Ver figura 3.

La mayoría de las instituciones tienen conexión a Internet (80%); de éstos, el 50% posee más de una conexión, principalmente aquellos que se les agrega el nombre de "Complejo Educativo", que tienen una población estudiantil mayor y que se ubican en la zona urbana de Santa Ana. Un pequeño porcentaje de las mismas consideradas para el estudio, no posee conexión a Internet; sin embargo, imparten clase de informática en el centro de cómputo que poseen. Una de las instituciones estudiadas posee conexión internet, pero ya no dispone de centro de cómputo para impartir las clases, a pesar de estar ubicada en la zona urbana, ser de considerable tamaño y tener varios años de fundación.

Para los centros escolares que no tienen conexión a Internet (20%), el riesgo de infección

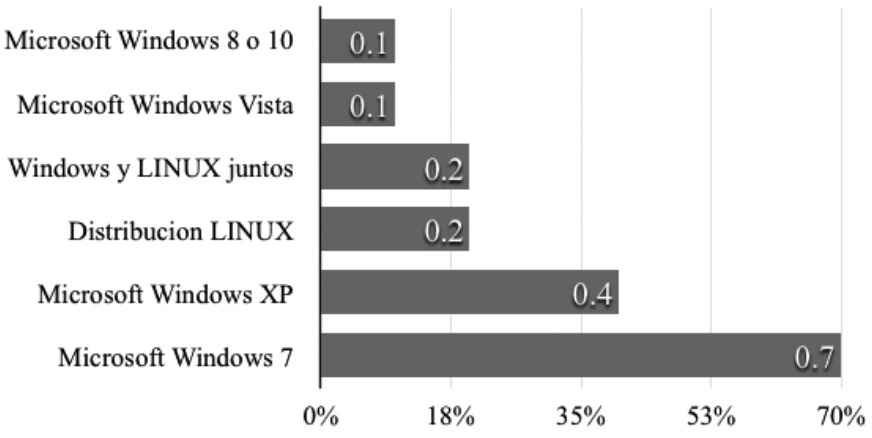

Figura 2. Sistemas operativos que utilizan los equipos de la institución.

7. Programa malicioso o software dañino.

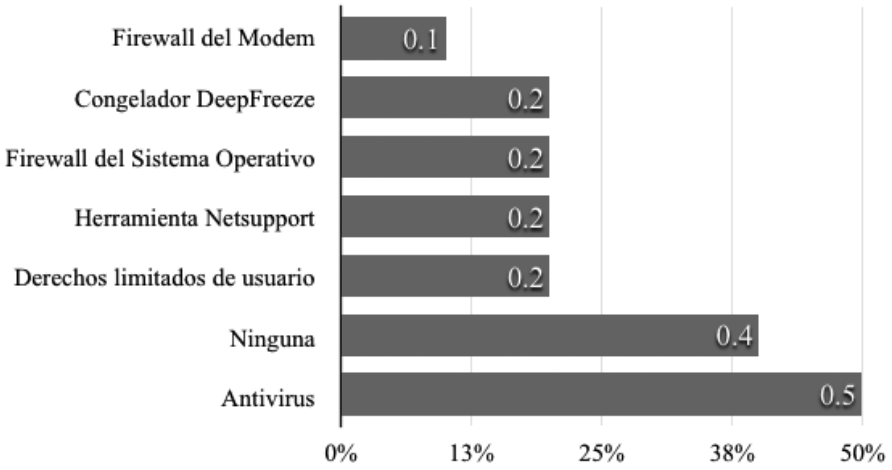

Figura 3. Medidas de seguridad implementadas en los equipos de la institución.

por algún tipo de malware se mantiene debido a que, si no se tiene ninguna herramienta como un antivirus, los equipos podrían infestarse con algún software malicioso, ya que los alumnos utilizan medios extraíbles que podrían estar infestados.

De los centros escolares estudiados, ninguno posee un dispositivo dedicado exclusivamente a la seguridad, es decir, no tienen instalado un Firewall y no tienen conocimiento de Pfsense. Un pequeño porcentaje de centros educativos disponen de una herramienta de software para el sistema Windows llamado NetSupport. Esta herramienta es de pago e incluye opciones para controlar los sitios a los que se conectan los alumnos desde una computadora que actúa como servidor. La desventaja es que el administrador debe investigar primero los sitios que formarían parte de la lista negra[8] o que no son apropiados para los alumnos y luego bloquearlos desde la herramienta.

Para el caso del Firewall dedicado propuesto, es posible configurar un servidor proxy que permite filtrar el tráfico de miles de sitios en diferentes categorías de contenidos preparados y actualizados constantemente por otras organizaciones en Internet. Para este caso se han considerado las listas negras de "Shalla's Blacklists"[7], que son una colección de URL agrupadas en varias categorías. Estas listas negras son gratuitas para uso personal o comercial. Entre las medidas de seguridad básicas adoptadas por los encargados de los centros de cómputo se describen las siguientes:

- A los alumnos no se les proporcionan derechos de administrador para impedir la instalación de aplicaciones no autorizadas y no alterar las configuraciones de los equipos.
- Se revisan los historiales de navegación para controlar los sitios que visitan los estudiantes.

8. Listado de dominios web con contenido considerado no apropiado para los alumnos.

9. Para mayor información visitar: http://www.shallalist.de/

- Se posee algún software que permite bloquear ciertos sitios en Internet. Algunos de ellos les permiten bloquear las redes sociales.
- Se utiliza una herramienta llamada Deep-Freeze, que les permite congelar la configuración del sistema; es decir, si el alumno realiza algún cambio en la configuración del sistema, instala aplicaciones o cualquier actividad que realice en el equipo, no tendrá efecto la próxima vez que se encienda. Una de las desventajas es que cualquier trabajo que realice el estudiante en el equipo se perderá definitivamente una vez se apague.
- Un 60% no utiliza ninguna medida de seguridad para el acceso a Internet.

El 100% de los centros escolares no dispone de un dispositivo dedicado exclusivamente para la seguridad de la red informática. El 90% de las instituciones está de acuerdo en que se implemente en su red local un equipo Firewall dedicado a la seguridad como propuesta gratuita de parte de la Universidad. El 80% dispone de un equipo básico para que se pueda implementar el Firewall propuesto.

4. Discusión

Según comentarios de los encargados de los centros de cómputo, siempre hay alumnos curiosos que acceden a sitios web con contenidos inmorales, sitios que promueven juegos violentos y otros que, sin buscarlos, aparecen como ventanas emergentes en ciertas páginas web, los alumnos se sienten tentados a curiosear tales sitios que van en contra de la filosofía de las instituciones católicas.

Entre las razones por las cuales los centros escolares no implementan sistemas dedicados para la seguridad (Firewall) se mencionan las siguientes:

- Los Firewall basados en Software, como es el caso de PfSense, deben instalarse en un equipo y configurarlo según las necesidades. Esta adaptabilidad es una ventaja, pero la mayor desventaja es que la configuración del mismo requiere conocimientos de cómo funcionan los Firewall, de redes informáticas, protocolos de comunicación y de las herramientas específicas que se configuren en él.
- La mayoría de los Firewall de mayor renombre vienen pre-configurados. Esto es una ventaja importante, ya que solo requieren hacer ciertas adaptaciones y utilizan interfaces de usuario bastante intuitivas. Pero la desventaja es que son muy costosos; difícilmente los pueden adquirir los centros escolares estudiados.
- Al no poder adquirir un equipo para la seguridad, ponen su confianza en las herramientas proporcionadas por los sistemas operativos, antivirus de edición gratuita y otros softwares que remedian en parte el problema de la seguridad.
- El Firewall Pfsense, además de configurar reglas para el control de tráfico en la red,

permite configurar otros servicios de red, algunos de ellos son los siguientes:

a. Servidor Proxy, que es un servidor intermedio que permite a los usuarios realizar conexiones de red indirectas hacia otros servicios de red. En Pfsense se configura el proxy llamado Squid, que es software libre y tiene una variedad de funcionalidades, entre ellas, acelerar un servidor web, guardando en caché peticiones repetidas al servidor DNS y añadir seguridad filtrando el tráfico.

b. Servidor DHCP (Dynamic Host Configuration Protocol), que permite la configuración dinámica de las interfaces de red de los dispositivos que se conectan a la red.

c. Configuración de conexiones VPN (Virtual Private Network) para el acceso seguro hacia la red interna.

d. Monitoreo de la red. Dispone de herramientas que permite observar lo que sucede en la red mediante reportes y gráficas.

Medidas generales básicas de seguridad informática

La seguridad informática es un proceso de administración de los riesgos de los sistemas de información y los componentes integrados, que se apoya en políticas y procedimientos, que tienen como objetivo proteger los activos físicos e intelectuales utilizados en la generación de información.

Aunque la investigación se orienta a la seguridad en las redes informáticas de los centros escolares, esta a su vez forma parte de la seguridad integral de un centro educativo.

El encargado de los centros de cómputo debe definir políticas y prácticas de seguridad informática con la aprobación de la dirección de la institución. Estas políticas deben darse a conocer a los usuarios de la red, que a su vez deben cumplir para evitar sanciones por su incumplimiento.

Prohibiciones en cuanto al uso de los equipos informáticos

Según el Departamento de Educación de Puerto Rico, específicamente en sus Políticas y Procedimientos de Seguridad Informática (agosto 2015), entre las prohibiciones para los usuarios de equipos informáticos para tratar el tema de la seguridad y que puedan adaptarse a los centros escolares católicos de Santa Ana, se mencionan las siguientes:

- Instalar programas o aplicaciones sin la autorización del encargado del centro de cómputo y que sean únicamente para fines educativos.
- Instalar cualquier dispositivo que altere la configuración actual de la red, entiéndase la instalación de: routers, puntos de acceso inalámbricos, switches, impresoras, dispositivos alternos para conexión a Internet como módems USB, entre otros.

- Destruir, alterar, inutilizar o dañar de cualquier otra forma los datos, programas o documentos electrónicos que contienen los equipos de los centros de cómputo.
- Albergar datos personales en las unidades locales de disco de las computadoras de los centros de cómputo, que no sean propios de actividad educativa.
- Intentar obtener derechos o accesos distintos a aquellos que les han sido asignados utilizando medios extraíbles o de cualquier otro.
- Cambiar de posición de cables o dispositivos de red para evitar alteraciones de configuración.
- Intentar distorsionar o falsear los registros (log) de los sistemas de información.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar los recursos informáticos.
- Intentar utilizar las áreas y espacios físicos designados para las telecomunicaciones como almacén o área para guardar materiales ajenos a tal función.

Administrador de seguridad

De acuerdo a esta misma entidad, entre las responsabilidades del administrador de la red, que podrían aplicarse a los centros escolares estudiados son: definir, administrar y mantener las políticas y procedimientos de seguridad y su documentación.

El administrador de red es responsable de:

- Mantener actualizado el documento que describa las políticas, prácticas y procedimientos de seguridad.
- Investigar y documentar cualquier incidente, según sea necesario.
- Mantener a todas las partes informadas de cualquier incidente o situación de seguridad que se presente.
- Establecer los términos razonables de respuesta para detectar, reportar y responder a incidentes de seguridad.
- Divulgar entre los empleados los procedimientos de cómo informar los diferentes tipos de incidentes.
- Desarrollar procedimientos para que los cambios a la seguridad de los sistemas, sean documentados adecuadamente y estén almacenados en medio físico o electrónico de manera segura.
- Coordinar adiestramientos a los empleados sobre los controles de seguridad, requerimientos y beneficios correspondientes.
- Divulgar a todos los empleados los procedimientos de seguridad que les apliquen.

5. Referencias

Buechler, C. M. (2009). *PfSense: The Definitive Guide.* Recuperado de http://cage.owltux.com/ebook/pfsense%20-%20The%20Definitive%20Guide.pdf

Burgos, V. (2014). *PFSense, un poderoso Firewall fácil de usar y gratuito* [Video]. Recuperado de https://www.youtube.com/watch?v=uFL_geKVWsU

Cisco Networking Academy (2017). *Curso: Intro to Cybersecurity-ESP / AD-2017*

España, Junta de Castilla y León (s.f.). *Manual del buen uso de los medios informáticos*. Recuperado de http://www.educa.jcyl.es/ciberacoso/es/plan-prevencion-ciberacoso-navegacion-segura/fomento-buen-uso-medios-informaticos/gestion-seguridad-informatica

España, Junta de Extremadura, Mérida (2015). *Guía para el buen uso educativo de las TIC*. Recuperado de http://enmarchaconlastic.educarex.es/conectadoyseguro/pdf/guia_BPTic.pdf

Estado Libre Asociado de Puerto Rico, Departamento de Educación (7 de agosto de 2015). *Políticas y Procedimientos de Seguridad Informática*. Recuperado de http://www.de.gobierno.pr/files/Politicas_y_procedimientos_de_seguridad_PUBLICADO.pdf

FreeBSD (13 de noviembre de 2013). *¿Qué es FreeBSD?* Recuperado de https://www.freebsd.org/es/about.html

Pujadas, J. (2008). *Seguridad informática en Centros Educativos*. Recuperado de http://www.bellera.cat/josep/pfsense/Valladolid-2008-07-03_v12.pdf

Malecki, F. (29 de enero de 2013). *Lo que debería saber sobre la seguridad en centros educativos.* Computing. Recuperado de http://www.computing.es/seguridad/informes/1065389002501/deberia-saber-seguridad-centros-educativos.1.html

Murillo, R. (21 de agosto de 2015). *PfSense: Instalación y Configuración del Firewall, NAT, DHCP y DNS* [Video]. Recuperado de https://www.youtube.com/watch?v=HR1aTQP6oO8

Organización de Estados Americanos (2015). *Reporte de seguridad cibernética e infraestructura crítica de las Américas.* Trend Micro. Recuperado de https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

Pérez P., J. y Merino, M. (2008). Definición de seguridad informática. *Definicion.de.* Recuperado de https://definicion.de/seguridad-informatica/

Vañó R., F. J. (2016). *Redes seguras en entornos virtualizados* (Tesis de pregrado). Escuela Técnica Superior de Ingeniería Informática, Universitat Politècnica de València, España. Recuperado de http://hdl.handle.net/10251/72043

Williamson, M. (2011). *PfSense 2 Cookbook.* Recuperado de https://the-eye.eu/public/Books/IT%20Various/pfsense_2_cookbook.pdf