GUÍA PEDAGÓGICA N° 6

Escuela: **E.P.E.T. N° 1 de Jáchal.** Nivel: **Secundario** Ciclo: **Primero**

Año: **Tercer año** División/es: **1ra; 2da;3ra** Turno: **Mañana y tarde**

Área Curricular: **Informática III**

Docente/s: **Barboza Alejandro, Gómez Iris, Baca María**

Contacto/s: **Baca María (bacamaria98@gmail.com / 2646728631); Barboza, Alejandro Matías (matiasbbz@gmail.com / 2647408990); Gómez, Iris (2645775311 / irisg291@gmail.com)**

Fecha de presentación: **el 26 de agosto del 2020**

Título de la propuesta: **Seguridad Informática – Hardware y Redes**

Contenidos: **Seguridad Informática: seguridad de hardware y seguridad de redes**

Actividades:

1. **Lee comprensivamente la siguiente información**

SEGURIDAD INFORMÁTICA

(Continuación del tema de la guía N°5)

Seguridad de *hardware*

Otro tipo de seguridad informática que debes conocer es el que tiene que ver con el *hardware*, es decir, la parte física de tu equipo. En general, este ámbito se relaciona con ciertos dispositivos y programas que se pueden conectar a un ordenador para hacerlo más seguro, otorgando protección a las computadoras o dispositivos frente a intromisiones o amenazas.

De los tres tipos de seguridad informática (seguridad de hardware, software y de red) que existen, la de hardware es la que hace más difícil que un atacante pueda acceder a tu información; pero al requerir de elementos externos, también puede ser el más caro y el más difícil de instalar. Sin embargo, en el caso de que quieras conseguir una seguridad absoluta, no deja de ser una opción muy interesante.

Algunos de los dispositivos *hardware* más conocidos que pueden aumentar la seguridad de tus equipos informáticos son los ***firewalls de hardware, firewalls de software***.

Por último, otra de las áreas de las que se encarga la seguridad de *hardware* es de detectar y examinar las vulnerabilidades que tiene cada equipo informático. Ningún dispositivo es

perfecto; y por eso, esta rama de la ciberseguridad se encarga de mostrarnos la manera en la que podemos volverlos menos accesibles a cualquier tipo de ataque.

- **Firewall**

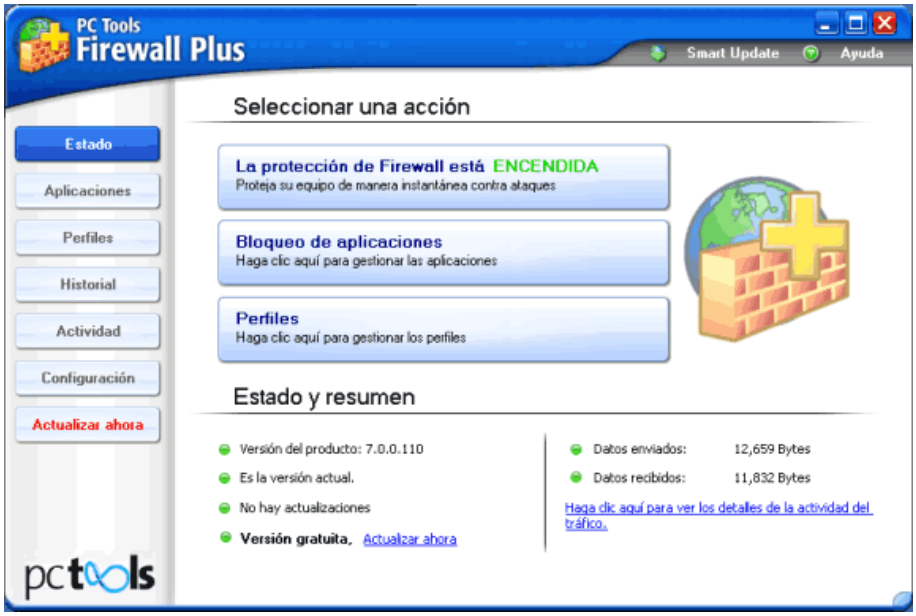
Es un sistema tangible o lógico, que permite proteger nuestra conexión. Es como una barrera, una membrana entre nuestro dispositivo y la red. Su función es **analizar las conexiones** y bloquear aquellas que puedan suponer un riesgo de seguridad por ello se les denomina cortafuegos.

<u>Diferencias entre un Firewall de Software y uno Firewall de Hardware</u>

Es posible tener un **firewall por el hardware** y uno **por el software** activos simultáneamente para lograr una mayor protección.

Cuando hablamos de un **firewall de hardware** nos referimos a un dispositivo físico que puede venir incluido en los dispositivos informáticos a modo de placa o módulo o puede anexarse a nuestro equipo. Su finalidad es bloquear aquellas conexiones que puedan ser peligrosas. Es una manera más de proteger nuestra privacidad y seguridad.

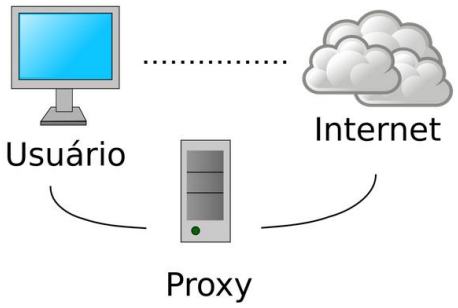
En cambio un **firewall de software** es un programa informático. Existen múltiples opciones que podemos instalar en todo tipo de sistemas operativos y dispositivos.



Si nos preguntamos **cuál es más sencillo de utilizar y para algunos es también más barato** para un usuario medio, se proponen los cortafuegos (o firewall) de software ya que solo necesita instalarlo en su equipo, apenas requiere configuración y actualizaciones esporádica. En cambio, un firewall (o cortafuegos) de hardware requiere de instalación física y una mayor configuración para que el hardware lo reconozca y no genere conflicto. Es para usuarios más expertos, además, su desactualización debe resolverse con un nuevo dispositivo.

Respecto a la **seguridad**, en ambos casos la finalidad es la misma. Sin embargo, hay que decir que el firewall de software va a recibir más actualizaciones y por tanto puede hacer frente a amenazas más actuales.

Un cortafuegos de hardware se sitúa entre el equipo e Internet (servicio). En cambio, un cortafuegos de software se sitúa entre el equipo y la red (otros dispositivos) a la que nos conectamos. Esto hace que, si otros equipos acaban infectados dentro de una red, el software podría proteger al dispositivo.



En **cuanto a la usabilidad**, hay diferencia a tener en cuenta, un firewall de software se instala en el dispositivo. Esto quiere decir que, si tomamos nuestro portátil o móvil y lo llevamos a otro lugar, la protección va a seguir ahí. En cambio, un firewall de hardware lo normal es que esté conectado en el router (dispositivo que amplifica la señal de internet).

Obviamente que es importante pensar que con el avance de la tecnología y los dispositivos electrónico cada vez más se mejorará e innovará en ambas tecnologías de seguridad informática.

Seguridad de Red o Ciberseguridad

El otro campo de la seguridad informática es en el ámbito de las redes de la web, en ello la ciberseguridad es un campo en constante desarrollo, y sus aplicaciones (programas y dispositivos) tienen una importancia fundamental en nuestras vidas. A pesar de poder dividir sus funciones en hardware y software, lo cierto es que estos ámbitos suelen trabajar a la vez para garantizar la máxima protección de nuestros datos y equipos y de la interacción de ello en el tráfico de información en la WEB, para ello se utilizan dispositivos de filtrado llamados proxy.

- **Servidores Proxy**

Con cualquiera de los tipos de Firewall accedimos a cubrirnos en mayor o menor medida de los problemas de seguridad en la conexión. Ahora veremos cómo proteger nuestro equipo informático y nosotros mismo a la hora de navegar por la red.

Para ello nos centraremos en los **proxys**, este es un servidor, un dispositivo y programa que actúa como un intermediario. Se sitúa entre la solicitud que realiza un cliente y otro servidor que da la respuesta. Si queremos acceder desde un móvil a un servidor de Internet donde está alojada una página web, un proxy puede actuar de intermediario.

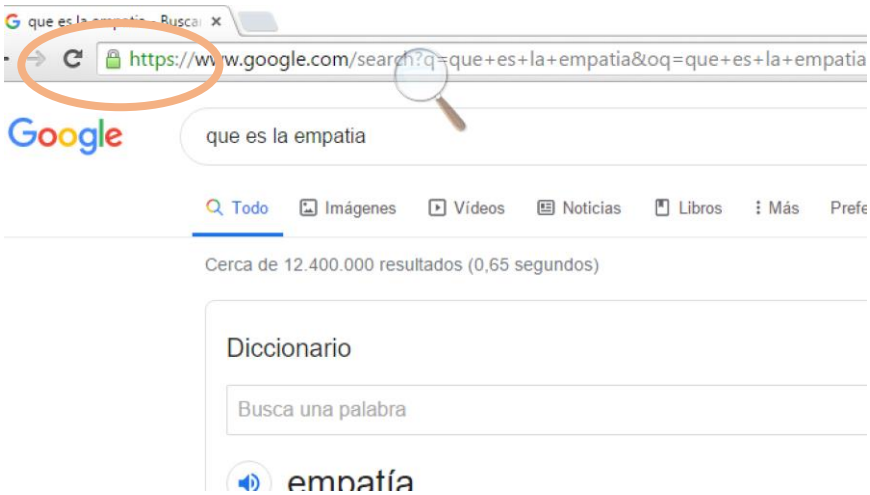
Esto permite ganar más control de acceso, registrar el tráfico o incluso restringir determinados tipos de tráfico. De esta forma podremos mejorar en seguridad y también en rendimiento, así como tener mayor anonimato al acceder a determinados servicios. Básicamente evitar las cookies, acceder a paginas seguras, acceder a contenido controlado, esconder la IP (código que identifica) de nuestra máquina, etc.

Una de las funciones más comunes para lo que los usuarios utilizan los proxys es para **saltarse la restricción geográfica**. Es decir, un proxy puede actuar como intermediarios y hacer que nuestra conexión aparezca en otro lugar. De esta forma podemos acceder a contenido disponible únicamente para un determinado país o poder ver contenido que no esté disponible en el nuestro.

Tipos de proxys existentes

-**Proxy web: s**in duda uno de los servidores proxy más populares y comunes e incorporados a la hora de navegar son precisamente los **web**. Estamos ante una opción en la que los usuarios pueden acceder a través de una página web. Esa web es la que actúa como proxy. Está basado en HTTP y HTTPS son protocolos que permiten que el usuario realice una petición de datos y recursos, como pueden ser documentos y actúa como intermediario para acceder a otros servicios en Internet.

A través de esa página web podremos navegar por otros sitios. Toda esa navegación pasa a través del proxy web que estamos utilizando.



-Proxy caché: otra opción es un servidor **proxy caché**. En este caso este servidor actúa como intermediario entre la red e Internet para cachear contenido. Se utiliza para acelerar el contenido de un sitio al navegar.

Si una persona entra en una página por segunda vez, esa información que está cargando ya puede estar cacheada. De esta forma no necesita descargarla de nuevo y va más rápido. Básicamente genera atajos o una librería lógica, lo que hace que la pagina no se sature y que ante peticiones repetidas de un mismo visitante la descarga sea más rápida porque incorpora accesos más rápidos y reducción de la banda ancha.

-Proxy transparente: en este caso lo que hace el proxy es obtener la petición que hemos dado y darle una redirección sin necesidad de modificar nada previamente, es decir que permite entrar a otras aginas o servidores vedados, pero no oculta la identidad de la máquina, de ahí el nombre que obtiene.

-Proxy NAT: una opción más en cuanto a proxys es el proxy **NAT**. Principalmente se utilizan para enmascarar la identidad de los usuarios. Esconde la verdadera dirección IP para acceder a la red. Cuenta con variadas configuraciones.

En resumen, podemos decir que todos estos proxys, actúan dentro de la conexión de la maquina a las páginas de internet, es por ello que se dice que son intermediarios entre el usuario (dispositivo móvil, computadora, etc.) y un servidor lugar donde se almacenan los contenidos de una página web. Pueden ayudar para mejorar la seguridad y privacidad, así como para obtener diferentes funciones (descriptas en los tipos de proxys) a la hora de navegar por la red, por ejemplo, mayor rapidez de descarga, ocultar el rastro en la web, acceder a contenido prohibido en determinados lugares, ocultar la identificación de la computadora, etc.

2. Explicar con sus propias palabras que significan Seguridad de Hardware y de Redes?

3. En el área de la informática ¿Qué queremos cuidar?

4. Explica de que se trata en general un firewall

5. Explica de que se trata en general un proxy

6. ¿Hay diferencia entre firewall y proxy? Justifica tu respuesta

7. Completa el siguiente cuadro comparativo

Seguridad Informática		
Seguridad de Hardware		
Firewall		
Aspectos a analizar y comparar	**firewall de hardware**	**firewall de software**
• Función que cumple en el equipo informático		
• Instalación y mantenimiento		
• Usabilidad (que abarca en la protección)		
• Reemplazo		
• Accesibilidad económica		

8. Indica que proxys es adecuado para la función solicitada

-Tener en anonimato la IP de mi computadora navegando en la web ……..……

-Acceder y bajar rápidamente a contenidos de páginas WEB ya visitadas ……

9. Elabore en Ítems con los componentes de Seguridad de Hardware, software y redes que pueda identificar las PC de sus casas, Tablet o celular.

Si cuentas con una red de internet domiciliaria, consulta a tu proveedor si tu router cuenta con un dispositivo adicional de seguridad informática, también puedes leer las especificaciones técnicas en el manual de usuario del aparato.