

**MANUAL DE BUENAS PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN WINDOWS 8.**

**VERSIÓN 1.0**

**RIVERA – HUILA**

**2021**

1



Contenido

INTRODUCCIÓN.............................................................................................................................4 OBJETIVOS......................................................................................................................................5 Objetivo general:..................................................................................................................................5 Objetivos específicos: ..........................................................................................................................5 MARCO TEÓRICO..........................................................................................................................6 Servidor: .................................................................................................................................................6 Modelo OSI:...........................................................................................................................................6 Firewall: ..................................................................................................................................................6 Malware:................................................................................................................................................7 Spam:.....................................................................................................................................................7 Virus: .......................................................................................................................................................7*:....................................................................................................9 Descargas: ........................................................................................................................................9 Servicios de mensajería: ..................................................................................................................9 Software antiguo:.............................................................................................................................9 Malvertising: ......................................................................................................................................9 Qué hacen los virus informáticos....................................................................................................9 ¿Todos los dispositivos son vulnerables a los virus? .....................................................................10 Tipos de virus informáticos.............................................................................................................10 Cómo evitar las amenazas de virus más recientes ....................................................................12* MANUAL .......................................................................................................................................13 Políticas de cuenta:............................................................................................................................13 *Aplicar historial de contraseñas....................................................................................................13 Longitud mínima de contraseña. .................................................................................................14 Duración de bloqueo de la cuenta:............................................................................................16* Políticas locales...................................................................................................................................17 *Etiqueta Integridad de Objetos....................................................................................................17 Generar auditorías de seguridad.................................................................................................20 Crear un archivo de paginación..................................................................................................21 Modificar valores de entorno de Firmware. ...............................................................................*

**INTRODUCCIÓN**

Con la transformación digital y día a día obteniendo nuevos avances tecnológicos navegar en internet se ha convertido un tanto inseguro y posterior a esto se adquiere un miedo a ser víctima de cosas como estafas, secuestros de datos y amenazas y por esta razón se idealiza la necesidad de tener un método o una manera de protección ya sea para realizarse manualmente o preferente automatizado para el público no muy bien ambientado en el ámbito de la informática

Pero las buenas prácticas digitales se deben convertir en un hábito para evitar ser retrógrado con respecto a lo que se conoce en la actualidad y mantenerse actualizado con respecto a los avances que se hacen en el campo de malware y la manera en que estos 3ros atacan y el daño que causan susodichos programas información, para evitar ser infectados y tener problemas legales puesto que a menudo estos métodos no solo se usan con el fin de robar información al azar de una persona y se hace de forma específica a una persona ya sea para suplantar o implantar información y datos para luego dar aviso a las autoridades competentes y que este sea judicializado ya que estos casos son muchísimos visto en casos anteriores, en el que ordenadores incluso empresariales y de parte del sector público se encontraban llenos de videos ilegales de forma ilegal.

4



**OBJETIVOS**

**OBJETIVO GENERAL:**

• Diseñar manual para afianzar la seguridad en informática para el sistema operativo de windows 8.1

**OBJETIVOS ESPECÍFICOS:**

• Diseñar métodos contundentes de buenas prácticas para facilitar la forma con que nos protegemos y evitamos fallos de seguridad o vulnerabilidades que se pueden encontrar en este sistema operativo de windows.

• Concientizar o mentalizar a la comunidad de consumidores de este sistema operativo para que no se vean envueltos en problemas con Malwares.

• Prevención a las amenazas latentes en la red ya que es un sin fin de sitios maliciosos y archivos infectados

**MARCO TEÓRICO**

**WINDOWS 8.1**

El mejor conocido windows 8.1 es un sistema operativo que a diferencia de sus hermanas las versiones 7 y 10 este se encuentra en un equilibrio entre velocidad y rendimiento pero carece de seguridad al igual que la versión posterior windows 7 el cual ya no cuenta con soporte.

**MODELO OSI:**

El Modelo OSI (de las siglas en inglés: Open Systems Interconnection, o sea, “Interconexión de Sistemas Abiertos”), es un modelo de referencia para los protocolos de comunicación de las redes informáticas o redes de

computadores. Fue creado en la década de 1980 por la Organización Internacional de Normalización (ISO).

El Modelo OSI se publicó inicialmente por la Unión Internacional de Telecomunicaciones (UIT) hasta 1983, y desde 1984 también lo ofrece la propia ISO, con estándar. Su función fue estandarizar o serializar las comunicaciones en Internet, dado que en sus inicios ésta era sumamente caótica. (Raffino, Modelo OSI, 2020)

**FIREWALL:**

En informática, y más específicamente en las telecomunicaciones, se entiende por firewall (en inglés) o cortafuegos a un sistema o dispositivo capaz de permitir, limitar, cifrar o decodificar el tráfico de comunicaciones entre un computador (o una red local) y el resto de la Internet, impidiendo que usuarios o sistemas no autorizados tengan acceso.

6



Un firewall puede bien ser de tipo físico o digital, es decir, un aparato o una pieza de software, y en ambos casos constituye apenas un primer paso de defensa en el mundo de las redes informáticas, indispensable pero no suficiente para garantizar la seguridad frente a ataques cibernéticos e intromisiones de terceros. (Raffino, Firewall, 2020).

**MALWARE:**

La palabra malware viene del inglés, y es el resultado de la unión de las palabras malicious software o software malicioso. Por lo tanto, se trata de un tipo de software o de aplicación que tiene como objetivo hacer daño al dispositivo en el que se ha conseguido alojar, instalar o infiltrar, ya sea un ordenador, un teléfono móvil o cualquier otro aparato.

**Tipos de malware:**

**Virus informático**: Un tipo de malware cuyo objetivo es alterar el correcto funcionamiento de un dispositivo. Un virus necesita ser ejecutado por el usuario pensando que es una aplicación legítima, y una vez lo hace, puede replicarse e infectar el equipo. Hay diferentes tipos, desde simples bromas hechas para molestar hasta otros que pueden dañar seriamente tu ordenador borrando o modificando archivos que repercuten directamente en su funcionamiento.

**Gusano informático**: Este malware no necesita de la intervención del usuario ni modificar ningún archivo existente, y también puede replicarse a sí mismo y enviar copias a otros equipos conectados a ese en el que están o que estén en su lista de contactos. Se suelen utilizar para crear botnets, redes de ordenadores zombies que pueden actuar de forma simultánea cuando un operador le da la orden para enviar SPAM de forma masiva, difundir malware o lanzar diferentes tipos de ataques informáticos ataques DDoS o de denegación de servicio.

**Troyano**: Es un malware que va dentro de un programa legítimo o disfrazado de él para introducirse en tu equipo como si usara un Caballo de Troya, de ahí su nombre. Mientras que un virus suele ser destructivo, un troyano trata de pasar desapercibido mientras accede a tu dispositivo con la intención de ejecutar acciones ocultas con las que abrir una puerta trasera para que otros programas maliciosos puedan acceder a él o robar información. Estos no se propagan a sí mismos.

**Spyware**: Un malware que también se instala en tu equipo por sí sólo o mediante la interacción de una segunda aplicación que lo lanza sin que te des cuenta, y suele trabajar a escondidas intentando no ser detectado para recolectar información sobre el usuario u organización dueña de un ordenador de forma no autorizada.

**Adware**: Una aplicación en la frontera del malware, porque no siempre es dañino para el ordenador. Su única misión es la de meterse en tu ordenador y empezar a mostrarte publicidad, ya sea mientras estás navegando por internet, a forma de popup en momentos aleatorios o durante la ejecución de un programa. Para ello, se instala en tu equipo normalmente a través del proceso de instalación de otras aplicaciones, casi como si fuera un troyano pero sin dañarte.

**Ransomware:** Un malware que secuestra los datos de tu ordenador bloqueándolos sólo ellos o todo el equipo, y pidiéndote un rescate económico a cambio de recuperarlos. Este tipo de programas puede acceder a tu ordenador a lomos de un gusano informático u otro tipo de malware, y es importante nunca pagar el rescate para no fomentar su uso y porque no tienes garantías de liberar los datos de tu ordenador.

**Como se infecta el ordenador:**

Cada tipo de malware tiene sus propias técnicas a la hora de infectar tu ordenador. Sin embargo, hay varios métodos comunes que muchos de ellos comparten, y precisamente por eso son a los que más le vas a tener que prestar atención para evitar su instalación.

En primer lugar, ten cuidado con las descargas en Internet. Cuando quieras descargar un programa o aplicación, recurre siempre a las páginas oficiales. Y es que cuando lo bajas de páginas de terceros, puedes acabar con instaladores propios de esas páginas que, en el mejor de los casos, te intentarán meter adware en el ordenador.

Las precauciones las tienes que extremar si buscas descargar programas en redes P2P, sobre todo si buscas cracks para romper las protecciones de seguridad de juegos legítimos para jugar gratis. Estos cracks y las promesas de obtener determinado juego o aplicación gratis ahorrandote mucho dinero son un método de difusión clásico y eterno para muchos tipos de malware, ya que los cracks son siempre programas que tienes que ejecutar.

También has de tener cuidado con los correos electrónicos. Muchas veces, un cibercriminal puede intentar hacerse pasar por una empresa u organización, o incluso por un amigo. Esto lo pueden hacer para llevarte a una página fraudulenta en la que obtener tus credenciales como nombre de usuario y contraseña haciéndote pensar que estás iniciando sesión en la web verdadera, o para que descargues aplicaciones con el malware dentro.

Ten siempre cuidado con cualquier programa gratuito que no descargas de su página oficial o que no conoces. Lo repetimos porque es uno de los métodos más comunes. Y si ya es poco recomendado descargar una aplicación de webs conocidas pero que no sea la oficial del programa, tienes que evitar por todos los medios descargarlos de páginas que no conozcas o de las que nunca hayas oído hablar.

**SPAM:**

El término Spam es un vocablo del inglés que hace referencia al correo basura o mensaje basura de Internet, es decir: mensajes no solicitados, no deseados y/o con remitente desconocido, enviados en grandes cantidades y por lo general con un contenido publicitario. Este término ha dado origen también a la acción del spamming y a sus equivalentes en español como spamear.

El vocablo Spam proviene históricamente de la Segunda Guerra Mundial, cuando a los soldados aliados en el frente les era distribuida masivamente una célebre marca de carne enlatada que llevaba ese nombre (contracción de Spiced Ham, jamón condimentado). (Raffino, Spam, 2020).

*Instale actualizaciones:* Los únicos mensajes emergentes que no debe ignorar son las notificaciones de actualizaciones de su sistema operativo u otros programas. Estas actualizaciones suelen incluir parches de seguridad que tapan vulnerabilidades, por lo que es importante aplicarlas cuanto antes.

*Añada una capa extra de protección:* Por muy bien que se maneje en Internet, los virus pueden acabar colándose. Mejore sus defensas con un antivirus robusto como Avast Free Antivirus, que actúa a modo de red de seguridad que atrapa los virus antes de que se acerquen siquiera a su sistema. (Latto, 2020)

12

**MANUAL**

**POLÍTICAS DE CUENTA:**

**Contar con un Software de Seguridad.**

Para la protección y rendimiento del equipo siempre es recomendable usar un antivirus puesto que este puede lograr una mejora notable en la velocidad del equipo y la seguridad en su uso cotidiano con respecto en el campo de Malware y archivos de 3ros que busquen penetrar nuestra seguridad y comprometer la integridad de archivos o del equipo mismo, para este se recomienda usar el siguiente antivirus **AVIRA ANTIVIRUS GRATIS.**

La protección de seguridad contra malware constituye la segunda capa de protección fundamental para tu computadora o red. Un paquete de software antivirus eficaz es el componente principal de las defensas tecnológicas que todo sistema informático personal y empresarial debe tener.

Una protección antivirus bien diseñada posee varias características. Analiza todo programa nuevo descargado para garantizar que esté libre de malware. Analiza la computadora periódicamente para detectar y eliminar cualquier malware que se haya filtrado. Se actualiza con regularidad para reconocer las amenazas más recientes.

Una protección antivirus eficaz es capaz incluso de reconocer (y advertir sobre) amenazas de malware previamente desconocidas basándose en características técnicas (como el intento de "ocultarse" en una computadora) que son típicas del malware. Además, los productos de software antivirus eficaces detectan y advierten sobre sitios web sospechosos, especialmente aquellos que pueden haber sido diseñados para ataques de "phishing" (una técnica que engaña a los usuarios para que ingresen contraseñas o números de cuenta).

Para terminar, la protección contra el malware debe resultar utilizable. Un producto de software antivirus eficaz debe ser sencillo de descargar e instalar, de manera que no necesites tener un doctorado en ciencias informáticas para usarlo. Busca soluciones de software antivirus que posean las características antes mencionadas y procede a instalarlas.

Una solución segura contra el malware protegerá específicamente tus finanzas. Estas herramientas protegen tu información de cuenta y proporcionan herramientas de administración de contraseñas, de forma que la frustración asociada al olvido de contraseñas no te lleve a pasar por alto este componente esencial de protección.

Ninguna protección es absoluta. Pero una combinación de atención personal y herramientas de protección bien diseñadas garantizarán que tu computadora esté lo más segura posible.

*Método para su instalación:*

**

*Método de instalación:*

*procederemos a ingresar a la web “*[*https://www.avira.com/es/free-antivirus-windows*](https://www.avira.com/es/free-antivirus-windows)*”*

*en la cual encontraremos una descarga directa la cual se podrá realizar de forma fácil y ágil puesto que es una instalación bastante lógica y que cualquier persona puede realizar.*

13



**Sentido Común:**

La forma mas practica de evitar recurrir a un técnico o un especialista para que rescate archivos de nuestro ordenador o intente eliminar el Malware no es nada más ni nada menos que el uso del sentido lógico o sentido común, a dia de hoy en internet rondan muchas webs e incluso personas anónimas que prometen recompensas de forma inmediata si se realiza uso de un enlace o un archivo que en este caso estaría contaminado con dichos Malwares para poder hacer un uso indebido de nuestra privacidad



*Método para concientizar a las personas y abarcar más el ámbito del sentido común:*

*Implementación de charlas o webinarios que permita a la gente poder conocer la forma y metodología con la cual estos piratas cibernéticos son capaces de vulnerar nuestra privacidad.*

15

**Actualización:**

Es recomendable mantener actualizado nuestro sistema operativo puesto que en las actualizaciones que este ofrece hay mejoras en el firewall que evitará que un archivo dañino como un Malware vulneren nuestra privacidad.

*Método para actualizaciones:*

*dirigirse a la barra de tareas y escribir la siguiente linea “Buscar Actualizaciones” y de forma inmediata nos redirigirá a otra ventana en la cual podremos apreciar las actualizaciones aplicadas anteriormente y si hay actualmente alguna disponible.*

**16

*Los links o enlaces que visitamos:*

**

De forma que un enlace puede estar infectado es necesario verificar de forma anticipada que inclusive los correos que recibamos no sean de personas desconocidas o que este se encuentre en spam puesto que al encontrase allí puede que el sistema de seguridad de mail hubiera detectado una amenaza y hubiese enviado allí este correo de rara procedencia o un 3ro que nos envíe un enlace con x o y fines.

*Utilizar una conexión segura:*

Parece sencillo, pero muchos usuarios suelen pasar por alto que al momento de iniciar sesión en un sitio web la conexión sea a través de HTTPS (Hypertext Transfer Protocol Secure). Al acceder a una página web utilizando este protocolo, la comunicación entre el cliente y el servidor viaja cifrada, lo que aumenta la seguridad y minimiza la posibilidad del robo de contraseñas. Al acceder a este tipo de sitios, se puede observar la diferencia entre acceder utilizando HTTPS o sin seguridad a través de HTTP. Es posible configurar una conexión segura en las redes sociales, para que toda la comunicación con el sitio sea cifrada.



*Analizar los archivos adjuntos:*

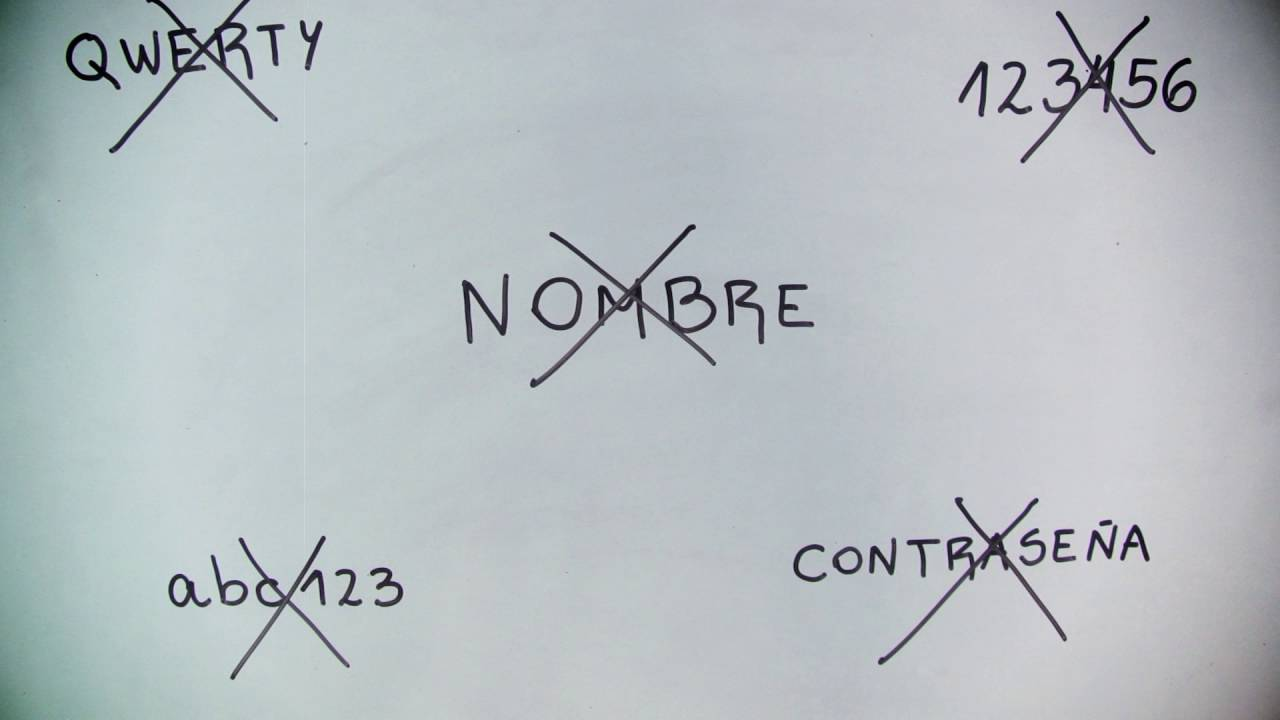
Al enviar y recibir correos electrónicos el usuario debe tomar ciertas consideraciones para evitar infectar su equipo o dispositivo a través de los archivos adjuntos en los correos, ya que en repetidas ocasiones, por una cuestión de tiempo no analizan los archivos adjuntos en los correos con una solución antivirus y de esta manera la seguridad de su información podría verse expuesta.



*Utilizar Contraseñas Fuertes:*

Al crear una cuenta en un sitio web, siempre se deben utilizar claves que sean una combinación de números, letras mayúsculas y minúsculas y de ser posible utilizar caracteres especiales. De esta manera, la posibilidad de que un atacante descubra la contraseña es mínima.

Distintos estudios han demostrado que los usuarios no suelen utilizar contraseñas fuertes para acceder a sus cuentas en Internet, lo que presenta una puerta de entrada para los atacantes. Algunos ejemplos de claves fuertes son “Jos33ntr@”, “C0ntr@z3n@#”, “Jp3t?xi9-”,: “4ApEKzqK” o “L@#nt67nx”



*Cuidar la información en sitios públicos:*

Con el uso masivo de los smartphone, las notebook y tablet, los usuarios suelen conectarse a cual red encuentren disponible, sin tener en cuenta los riesgos que ello puede implicar para su información. Cuando un usuario decide conectarse a una red inalámbrica, desde una cafetería o demás debe prestar atención a la seguridad de la misma y se recomienda no acceder a sitios como la banca electrónica, ya que un atacante podría estar analizando el tráfico de la red y robar su información.

Además de las herramientas tecnológicas, es recomendable que los usuarios sigan las buenas prácticas para navegar por Internet, y de esta manera poder garantizar una mayor protección a sus equipos y a su información.

**

*Detección:*

Una vez conocidas las formas en las que el malware se introduce en los ordenadores, debes saber cómo encontrarlo lo antes posible. Estos son algunos de los síntomas que te pueden ayudar a detectar si tu equipo está afectado por el malware:

Si percibes que el ordenador funciona mal o sufres un bombardeo de publicidad cada vez que abres el navegador, realizar un análisis del antivirus es lo más efectivo para encontrar la procedencia del malware.

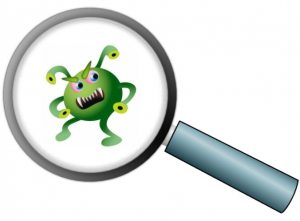
La mayoría de software malicioso ejecuta tareas en segundo plano, consumiendo gran parte de la memoria RAM y haciendo que el rendimiento del ordenador sea más lento de lo habitual.

Si el malware ha dañado el ordenador, es posible que se generen extraños mensajes de error al ejecutar las aplicaciones.

Una actividad inusual en tu correo electrónico o redes sociales, como mensajes que no has enviado, puede ser síntoma de software malicioso en tu ordenador.

El malware puede provocar que aparezcan muchas ventanas emergentes advirtiéndote de que un sistema ha infectado tu ordenador y que debes descargar una aplicación para eliminar el virus.

Hacer un análisis del equipo con un antivirus es lo más efectivo para encontrar archivos maliciosos antes de que se ejecuten y dañen el sistema.

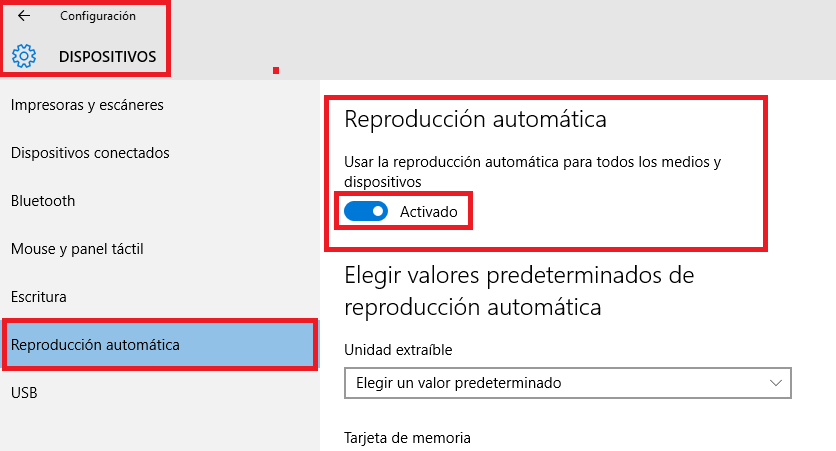
**

*Desactivar la reproducción automática de medios:*

No es necesario si usas Windows 7, ya que de forma predeterminada está deshabilitada en este sistema operativo.

La reproducción automática de medios es una noble y útil posibilidad para el usuario de comenzar a reproducir automáticamente medios que se inserten en la PC de acuerdo con su contenido. Esta característica es aprovechada habilidosamente por el malware para penetrar en el equipo sin tu consentimiento al insertar una memoria flash, un CD, una tarjeta de memoria o cualquier tipo de dispositivo.

Lee la siguiente página y descarga en ella gratis la clave necesaria, solo es necesario dos clics para desactivar o deshabilitar esta opción.

**

*Revisar manualmente el contenido de los USB:*

Revisa todos los archivos que contenga en su interior cualquier memoria flash u otro dispositivo USB conectado al equipo, no confíes nunca, ni le dejes toda la tarea al software antivirus.

• Desconfía de cualquier archivo reciente.

• Desconfía especialmente de cualquier archivo de extensión .EXE

• Desconfía de cualquier archivo que se vea semi-transparente, indica que es un archivo oculto.

• Levanta la alarma si descubres un archivo de nombre AUTORUN.INF, es un acompañante perpetuo de los virus, en él se le indica a Windows y se le ordena, el inicio del ejecutable que contiene el virus. Si tienes la reproducción automática deshabilitada no será funcional, pero sí indica la presencia de malware en el dispositivo.