# Clase 9

## Seguridad Informática

### 9.1 Introducción

La seguridad en los equipos informáticos es algo que a todos los técnicos y usuarios nos inquieta. El constante brote de diversas amenazas a la integridad de nuestra información nos ha obligado a tomar medidas para evitar las amenazas más obvias.

Es importante hacer notar que a pesar de que la mayoría de los usuarios están conscientes de los riesgos a los cuales están expuestos, no conocen a fondo las implicaciones y los alcances en sus actividades financieras y profesionales.

La tecnología digital tiene grandes ventajas, paradójicamente también es de gran fragilidad. La característica fundamental de esta tecnología es su dependencia tanto del proceso de interpretación de datos como de la integridad de los mismos. Cuando alguno de éstos falla, no se puede garantizar que la información se correctamente entregada.

Actualmente existen muchos mecanismos y procedimientos para minimizar los problemas debido a datos erróneos.

No obstante, existen también muchas formas en las que pueden resultar afectados, y dentro de estas, los daños intencionales causados por "software malicioso" o malware.

En esta clase trataremos de dar un pantallazo a esta problemática tan histórica como actual.

### 9.2 El Malware

Uno de los principales enemigos para la seguridad de la información digital es el llamado malware (del inglés malicious software), nombre genérico para referirse a todos aquellos programas que afectan el comportamiento del sistema de cómputo de manera indeseada e inesperada. Éstos pueden tener efectos destructivos, como los virus, o simplemente molestos, como el spam.

Sin embargo, también hay otras clasificaciones para el malware, como spyware, gusano, troyano, etc.

#### 9.2.1 Los virus

Los virus son programas informáticos que dañan parcial o completamente los datos que contiene un sistema de cómputo, están diseñados para reproducirse (copiarse a sí mismos) y distribuirse por el sistema.

Se les llama virus porque su forma de reproducción y propagación guarda ciertas semejanzas con sus equivalentes biológicos: el virus inserta una copia de su código en algún programa o documento que, al ejecutarse o ser leído, provoca su activación.

Los virus suelen ser elaborados por programadores que desean robar información, sabotear sistemas de cómputo, proteger sus propios programas o, incluso, sólo "divertirse".

Los contagios se producen al copiar archivos contaminados de un sistema a otro mediante memorias USB o discos externos, al descargar archivos de Internet e incluso al entrar en ciertos sitios web que piden instalar archivos con la excusa de "configurar el sistema" o asegurando que es necesaria la instalación para alguna funcionalidad de la web.

Algunos síntomas que revelan la posible presencia de virus son:

1. Bloqueo parcial o total de la computadora.

2. Comportamiento anormal de la computadora o programas específicos.

3. Pérdida o alteración injustificada de los archivos de trabajo.

4. Comportamiento anormal de la imagen en pantalla, por ejemplo, la aparición de mensajes de advertencia ajenos al sistema en uso.

5. Cambio inesperado de nuestra página web.

### Origen

El primer virus (considerado como tal) atacó a una máquina IBM Serie 360 y fue llamado Creeper, (ENMS) por su autor, Bob Thomas, en 1971. No estaba diseñado para causar daño sino para comprobar si se podía crear un programa que se moviera entre ordenadores. Este programa emitía periódicamente en la pantalla el mensaje: «I'm a creeper... catch me if you can!» («¡Soy una enredadera... agárrame si puedes!»).

Para eliminar este problema se creó el primer programa antivirus denominado Reaper (cortadora). A partir de los años 80, hasta hoy, el progresivo asentamiento y uso de la informática en hogares, trabajos, establecimientos, ha traído consigo un aumento exponencial del malware, que hoy día se encuentran incluso en dispositivos celulares.

## 9.2.2 Los gusanos

Su objetivo es el mismo que el del virus informático; sin embargo, actúa diferente ya que no necesita ser ejecutado por el usuario ni modificar ningún archivo para infectar tu computadora. Como el virus,

también se replica a sí mismo para expandirse por las redes a las que está conectado el equipo. Así, el gusano intenta obtener las direcciones de otros ordenadores a través, por ejemplo, de tus listas de contactos para enviarles copias e infectarlos también.

Este tipo de malware es difícil de detectar ya que en general no afecta el funcionamiento del equipo, lo que si provoca es que algunas tareas simples sean vuelvan muy lentas. Otra forma de detectarlo es cuando se envían mensajes por correo electrónico o redes sociales sin tu consentimiento.

Respecto a su uso es muy común para crear botnets, es decir redes de ordenadores "zombis" que actúan de forma simultánea cuando el operador le da la orden de enviar spam de forma masiva o realizar ataques como el DDoS (Ataque de denegación de servicio).

Es así que los gusanos pueden ser una gran amenaza en grandes estructuras y afectando el tráfico de nuestra red, creando un sinfín de comunicaciones entre dispositivos que hagan colapsar la red.

La mayoría de los gusanos informáticos conocidos se propagan de una de las formas siguientes:

- Archivos enviados como archivos adjuntos a correos electrónicos.
- A través de un enlace a un recurso web o FTP.
- A través de un enlace enviado en un programa de mensajería instantánea.
- A través de redes de uso compartido de archivos P2P (punto a punto, del inglés "peer-to-peer").
- Algunos gusanos se propagan como paquetes de red que se introducen directamente en la memoria de la computadora para, a continuación, activarse el código del gusano.

## Origen

En la década de 1980, los investigadores buscaban formas de administrar Internet de forma remota, utilizando programas que pudieran distribuirse automáticamente a través de ella.

En Estados Unidos, el 2 de noviembre de 1988, un estudiante de la Universidad de Cornell llamado Robert Morris lanzó un programa experimental de autorreplicación en Internet para averiguar cuántas computadoras estaban conectadas a él. El programa se extendió rápidamente, instalándose en aproximadamente el 10% de las computadoras conectadas.

Morris no tenía intenciones maliciosas, pero un error en su programa hizo que muchas de las computadoras en las que aterrizó el gusano colapsaran. Fue procesado y expulsado de Cornell, pero los gusanos habían alcanzado la mayoría de edad y desde entonces se han convertido en una forma eficaz de atacar sistemas conectados a Internet.

### 9.2.3 Los troyanos

Así como el Caballo de Troya de la Odisea de Homero que fue utilizado para engañar a los troyanos, este tipo de malware se disfraza de archivos legítimos para que una vez que lo ejecutes aproveche las vulnerabilidades de tu equipo y empiece a robar tu información sin que te des cuenta.

A diferencia del virus o gusano informático no se propaga a sí mismo.

Los cibercriminales y hackers pueden utilizar troyanos para tratar de acceder a los sistemas de los usuarios. Generalmente, los usuarios son engañados por alguna forma de ingeniería social para que carguen y ejecuten troyanos en sus sistemas. Una vez activados, los troyanos permiten a los cibercriminales espiarte, robar tu información confidencial y obtener acceso de puerta trasera a tu sistema.

Las acciones llevadas a cabo por los troyanos pueden incluir:

- Eliminar datos
- Bloquear datos
- Modificar datos
- Robar datos
- Interrumpir el funcionamiento de computadoras o redes de computadoras

Hay varias clasificaciones de troyanos, algunas de las más conocidas son:

#### Backdoor

Un troyano backdoor (puerta trasera) ofrece a los usuarios maliciosos control a distancia de la computadora infectada. Permiten que el autor haga cualquier cosa que desee en la computadora infectada, como enviar, recibir, ejecutar y borrar archivos, mostrar datos y reiniciar la computadora.

#### Exploit

Los exploits son programas que contienen datos o códigos que aprovechan una vulnerabilidad del software de aplicaciones que se ejecutan en la computadora.

### Trojan-DDoS

Estos programas realizan ataques DoS (denegación de servicio) contra una dirección web dirigida. Mediante el envío de numerosas solicitudes (desde tu computadora y desde varias otras computadoras infectadas), el ataque puede desbordar la dirección objetivo y provocar una denegación del servicio.

### Trojan-Ransom

Este tipo de troyano puede modificar datos en tu computadora, para alterar su correcto funcionamiento o para que no te deje usar datos específicos. El delincuente solo restaurará tu computadora a su estado de funcionamiento normal o desbloqueará tus datos cuando le hayas pagado el rescate exigido.

### Trojan-Spy

Los programas Trojan-Spy pueden espiar cómo usas tu computadora; por ejemplo, a través del seguimiento de los datos que ingresas con el teclado, de capturas de pantalla o de una lista de las aplicaciones en ejecución.

Dentro de estos tal vez los más temidos son los ramsomware y los keylogger.

El ramsomware encripta todos o la mayoría de los archivos de la PC de una manera que, hasta el momento, no se ha podido desencriptar, haciendo que los archivos sean ilegibles. A continuación, muestra un cartel de este estilo, pidiendo generalmente un rescate en cryptomonedas:

No es recomendable pagar el rescate pues en general los delincuentes no cumplen con la desencriptación. En este caso nuestros archivos, lamentablemente, se consideran perdidos.

Por su parte, un keylogger es una aplicación encargada de almacenar en un archivo todo lo que el usuario ingrese por el teclado (capturadores de teclado). Luego envían esta información a través de la red. Son utilizados por muchos delincuentes para robar contraseñas e información de los equipos en los que están instalados.

### Origen

El término troyano se utilizó por primera vez en 1974 en un reporte sobre el análisis de vulnerabilidades en sistemas de computadoras realizado por la Fuerza Aérea de Estados Unidos, pero el término se volvió popular en la década de 1980 y ya a finales de esa década pueden identificarse los primeros troyanos, los cuales comenzaron a masificarse a principios de la década de 1990 con Internet.

## 9.2.4 El Spyware

El spyware o software espía es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento. Este software malicioso se instala por sí solo o mediante una segunda aplicación, actúan a escondidas tratando de no dejar rastro para que no te des cuenta y sigas actuando con como si nada pasará.

Así, el spyware monitoriza y recopila datos sobre las acciones realizadas en un equipo, el contenido del disco rígido, las aplicaciones instaladas o del historial de Internet. Además, también puede instalar otras aplicaciones.

Normalmente, este malware envía información a sus servidores, en función a los hábitos de navegación del usuario. También, recogen datos acerca de las webs que se navegan y la información que se solicita en esos sitios, así como direcciones IP y URL que se visitan. Esta información es explotada para propósitos de mercadotecnia, y muchas veces es el origen de otra plaga como el SPAM, ya que pueden encarar publicidad personalizada hacia el usuario afectado. Con esta información, además es posible crear perfiles estadísticos de los hábitos de los usuarios.

Muchas veces el spyware suele mezclarse con aplicaciones útiles y que cumplen una función al usuario, además de auto ofrecer su descarga en muchos sitios reconocidos.

En este punto podemos ver que varios tipos de malware se “solapan” en su clasificación, pues un spyware podría considerarse un troyano si es que viene escondido, o bien un keylogger porque espiaría el teclado. Sin embargo, el principal objetivo del spyware es enviar esa información a empresas de publicidad de internet para comercializar con nuestros datos.

## Origen

Las referencias públicas al término “spyware” datan de finales de 1996. En 1999, se utilizó en un comunicado de prensa de la industria informática con la misma definición que la empleada en la actualidad. El término consiguió un éxito inmediato en los medios de comunicación y entre su público. Poco después, en junio de 2000, se presentó la primera aplicación para hacer frente al spyware.

En la actualidad, en términos generales, el sistema operativo Windows es el objetivo por excelencia de las aplicaciones de spyware, debido a su uso generalizado. Sin embargo, en los últimos años, los creadores de spyware también se han interesado por la plataforma Apple, y, sobre todo, por los dispositivos celulares.

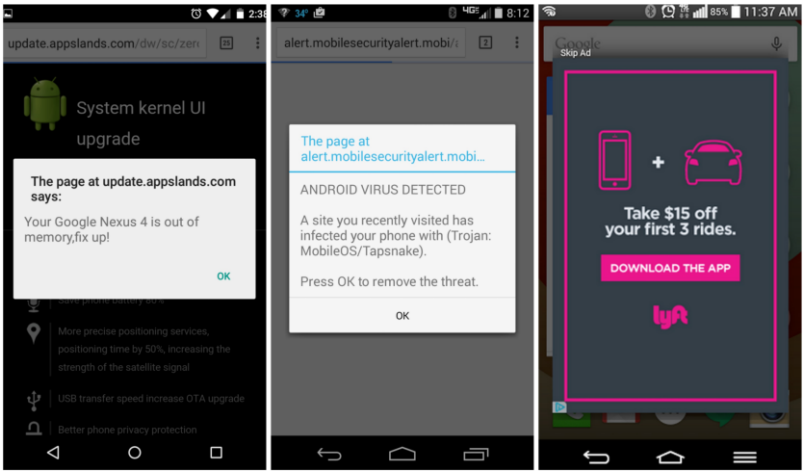
## 9.2.4 El Adware

El adware no tiene la intensión de dañar tu equipo, sino de invadirte de publicidad. Puede presentarse mientras navegas en internet, en forma de popup (pantalla emergente), durante la ejecución de un programa o sustituyendo la publicidad de una página web. Algunos lo consideran un tipo de spyware porque en algunos casos pueden recolectar y enviar datos personales.


Se suele pensar en el malware principalmente es una amenaza para las computadoras de escritorio. Sin embargo, un celular es tan susceptible a los ataques de malware como una computadora de escritorio. De hecho, una parte importante del malware que afecta a Android como plataforma es el adware.

Si tu celular se detiene sin motivo aparente, muestra anuncios no deseados en ubicaciones inusuales y en momentos inusuales, probablemente sea víctima de adware.

En la siguiente imagen vemos ejemplos de adware en Android.




Estos son algunos signos reveladores de tu sistema tiene adware:

- Aparecen anuncios en lugares en los que no deberían.
- La página de inicio de su navegador ha cambiado misteriosamente sin su permiso.
- Algunos de los sitios web que visita con frecuencia no se muestran correctamente.
- Los enlaces redirigen a sitios web diferentes de los que deberían.
- Han aparecido en su explorador, de repente, nuevas barras de herramientas, extensiones o plugins.

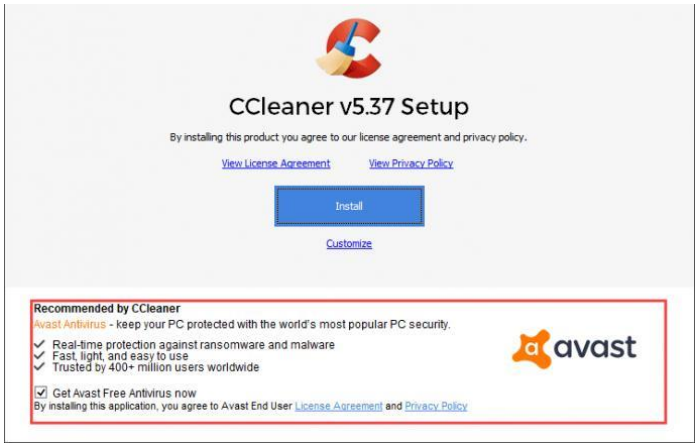
## Cómo infecta el adware

Hoy en día la principal forma de ingreso del adware es cuando instalamos un software que incluye adware en su instalación. El adware puede ser el software mismo o bien un software adicional.

Usted descarga un programa (normalmente freeware o shareware) que instala el adware sin que se dé cuenta y sin su permiso; o bien informando de su instalación, pero de una forma poco clara.

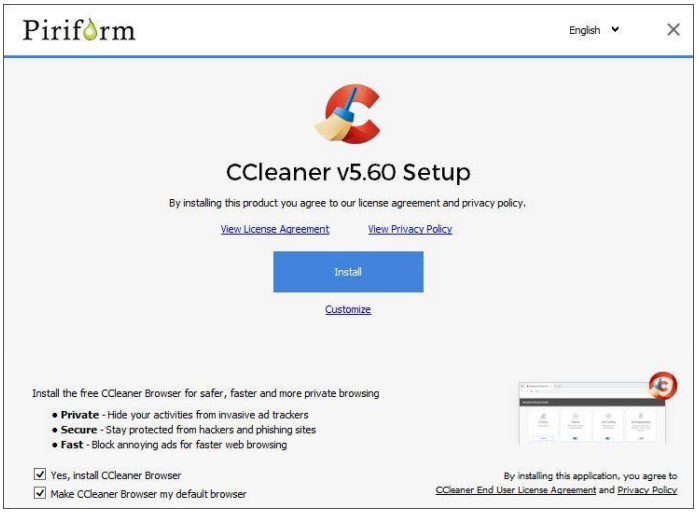
Esto sucede así porque el creador del programa lo ha acordado con el proveedor del adware. ¿Por qué? Porque el beneficio que esta publicidad genera permite que el programa esté disponible de forma gratuita (aunque incluso algunos softwares de pago pueden conllevar una carga de adware).

Un ejemplo de esto es el software CCleaner, en su instalación propone de manera poco clara la instalación por defecto de otro tipo de software.




Vemos que en este caso el software propone por defecto la instalación de un antivirus. El usuario debe destildar, en caso contrario el antivirus también se instalará.

En este caso sucede que el software propone la instalación de un navegador web.




## Origen

En sus inicios, alrededor de 1995, los expertos consideraron que el primer software publicitario o adware formaba parte de una categoría superior: el spyware. Pronto, los profesionales de seguridad comenzaron a diferenciar el adware del spyware como una forma de malware menos dañina. Incluso se consideraba "legítimo", al menos en teoría, pues lo creaban negocios con oficinas y trabajadores reales, para publicitarse.

En la actualidad, el adware está experimentando un resurgimiento: ahora, supone la principal causa de detección de las empresas de antivirus. El motivo de este alto porcentaje es debido a la proliferación de los celulares, que posibilita que el adware se introduzca en todo tipo de aplicaciones móviles.

## 9.3 Software antimalware – Seguridad en Windows

En la actualidad hay multiplicidad de software antimalware, los principales son los antivirus y los antispyware.

Anteriormente era común instalar un antivirus de empresas reconocidas, como Avast, Karspersky o NOD.

Hoy en día podemos asegurar que el antivirus que viene instalado por defecto, como una utilidad del sistema, con Windows 10, es muy efectivo. De hecho, según AVTEST se ubica en la posición decimocuarta entre los mejores antivirus del mundo, incluyendo, por supuesto, antivirus pagos[1].

Vamos a ver algunas de sus funcionalidades principales y que deberíamos tener activadas, en el Windows Defender.

## Windows Defender

Aclaración: No pretendo hacerle publicidad al antivirus ni a Microsoft, simplemente comento los hechos actuales, explicando porque el antivirus de Windows es muy bueno, contrariamente a la creencia popular de que es necesario instalar un antivirus adicional.

Windows Defender es una capa de seguridad que viene integrada en el propio Windows, y que ofrece protección a diferentes niveles.

Tiene, entre otras funciones:

- ✓ Antivirus integrado
- ✓ Firewall
- ✓ Controles parentales
- ✓ Protección para el acceso a la computadora
- ✓ Protección contra archivos peligrosos

El principal protagonista de Windows Defender es su antivirus integrado. Este funciona como la mayoría de antivirus que te puedas encontrar.

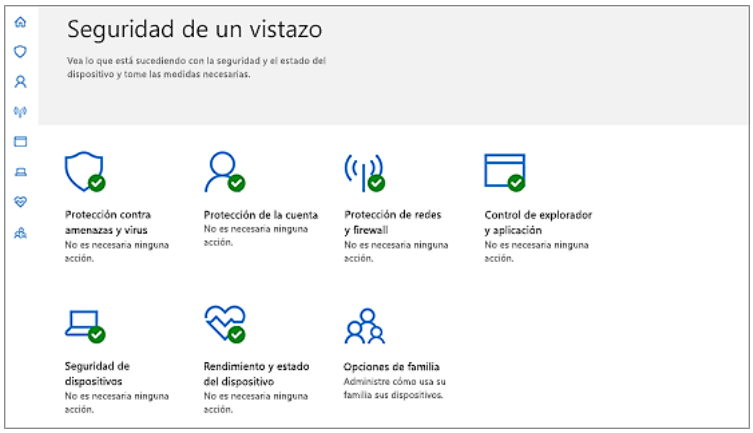
Microsoft suele actualizar su antivirus casi a diario, lo que lo convierte en una competencia muy a tener en cuenta, sobre todo comparándolo con otras alternativas gratuitas que muestran demasiada publicidad o tienen funcionalidades limitadas.

El antivirus de Windows Defender protege de prácticamente todos los peligros convencionales, ofreciendo protección contra virus, malware y spyware. Para esto, Microsoft recoge la información de incidencias de seguridad de todos los ordenadores con Windows, de manera que puede saber los peligros de cada parte del mundo y cuáles están más extendidos.

[1] Test antivirus software for Windows 10 - April 2021 | AV-TEST

## Configuración y explicación de algunas funcionalidades

Haciendo clic en el ícono del escudo en la barra de tareas de Windows accederemos al menú de Windows Defender:

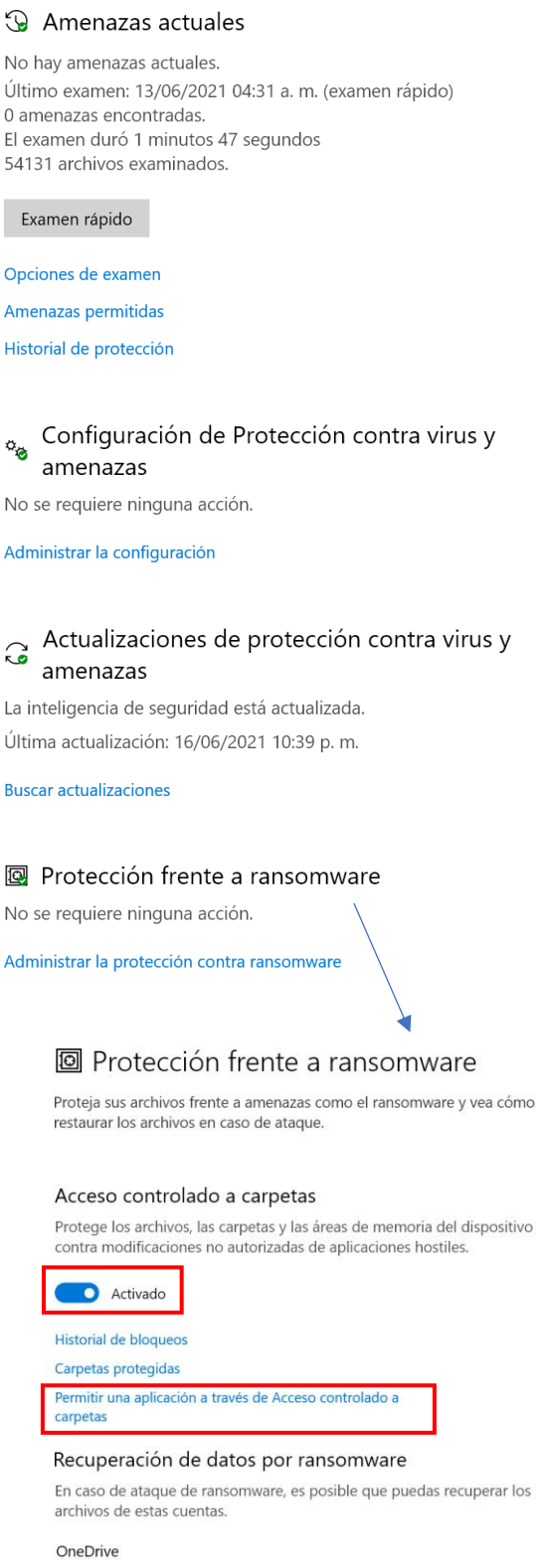



Cliqueando en el ícono del escudo de la izquierda accederemos a las opciones de "protección contra virus y amenazas", es decir, al antivirus.


En ese apartado encontraremos:

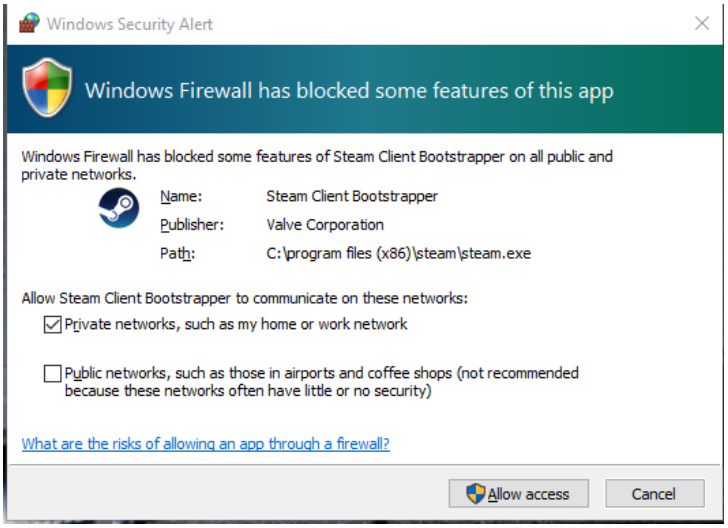
- Las amenazas actuales: nos informará si hay amenazas que requieran nuestra atención y que acciones podremos realizar con ellas.
- La configuración de protección contra virus y amenazas (en donde podremos activar o desactivar el antivirus).
- Las actualizaciones, nos indicará si el antivirus está actualizado.
- La protección frente a ramsomware: es muy recomendable activarla, ya que impide que los archivos, por su propia cuenta, accedan a ubicaciones críticas del sistema, evitando que el ramsomware puede llevar a cabo su objetivo de secuestro de datos. Puede traer como consecuencia que algunos programas presenten problemas por no poder acceder a ubicaciones de

Windows, hay que tener esto en cuenta y habilitar el acceso a esos archivos en la opción "Administrar la protección frente a ramsomware". Hacerlo solo si estamos seguros de que la aplicación a la que le damos acceso es confiable.



También es posible entrar en la opción Firewall y protección de red desde la pantalla principal de Windows Defender. Al hacerlo accederemos a las configuraciones del Firewall, para evitar o permitir que conexiones entrantes accedan a la computadora, o que conexiones salientes accedan a internet.


Generalmente esto se administra por defecto, salvo con aplicaciones nuevas o que Windows no reconozca; en esos casos nos saldrá un cartel consultando si le damos acceso a la aplicación:




El sistema de seguridad también se integra en Microsoft Edge para proteger de webs y descargas maliciosas, y desde su aplicación, accediendo a una configuración online, también se puede configurar el control parental, para controlar la forma y el contenido al que acceden los miembros de la familia.

Por supuesto, hay otros antivirus gratuitos, pero la mayoría tiene funciones limitadas, las cuales se deben activar pagando. Dicho esto, hay funciones que Windows Defender no posee y otros antivirus pagos si, como guardado seguro de contraseñas y cuentas , o navegación con VPN.

En el caso de sistemas Android o iOS, lo recomendable es instalar solamente aplicaciones de las tiendas oficiales de Google o Apple, las

cuales están previamente verificadas. Aunque en muchos casos contienen Adware no dañino (pero si molesto).

### 9.4 Manejo confiable de la información

Además de mantener el antivirus activado y actualizado, veremos brevemente algunas maneras en las cuales podremos mantener nuestra información más segura.

- Al navegar, tener cuidado al descargar e instalar software nuevo, verificar que sea confiable.
- No aceptar instalaciones que automáticamente nos propongan los sitios web, salvo que estemos muy seguros de que son confiables.
- Al instalar un programa, estar atento a cada paso de la instalación y las opciones que propone, en muchos casos instala software adicional no deseado.
- Evitar las páginas de descargas ilegales, sobre todo las páginas que exclusivamente proponen archivos de crackeo para todo tipo de aplicaciones. En muchos casos son malware y bastante peligroso.
- Bajo ningún concepto abrir una aplicación que provenga de una fuente desconocida. Aún si llega en forma de un contacto de correo electrónico/Facebook/WhatsApp conocido, puede ser que el que lo envió sea víctima de malware y la aplicación sea un gusano tratando de replicarse. Consultar a quien lo envió si realmente fue su intención.
- Guardar todos los archivos importantes en un servicio de almacenamiento en la nube (OneDrive, Google Drive, DropBox, etc.). Si bien hay cierto temor a la privacidad de nuestros datos, muchas veces el resguardo seguro de los mismos supera las desventajas.
- Utilizar doble factor de autenticación[2] para todas nuestras contraseñas, al menos para las más importantes
- Hacer copias de seguridad frecuentes de nuestros archivos más importantes y de la imagen del sistema operativo.

[2] Autenticación de múltiples factores - Wikipedia, la enciclopedia libre