Informe Técnico

Mecanismos de seguridad para el sistema operativo Windows

Karen Lucero Roldán Serrato

Concha Zamora Marco Antonio

FEBRERO 2023

Proyecto Interno

ICAT.UNAM
Financiamiento interno

Mecanismos de seguridad para el sistema operativo Windows

Karen Lucero Roldán Serrato, Concha Zamora Marco Antonio

Instituto de Ciencias Aplicadas y Tecnología, Unidad de Cómputo y Telecomunicaciones

Resumen

Existen múltiples peligros mientras utilizamos los equipos de cómputo al estar conectados a internet lo que amenaza la integridad de los dispositivos y la información contenida en ellos. En general depende del sistema con el que opera el dispositivo, es decir, el sistema operativo puede tener vulnerabilidades de seguridad, tales como estar expuestos a infectarse con *software* malicioso informático (como virus, *malware*, *adware*, y etc.). Por lo que es de alta prioridad la contención de dichas vulnerabilidades al realizar la instalación y actualización del sistema operativo. Algunos objetivos de la actualización del *software* informático es evitar el robo, la destrucción, plagio de los datos que alojan las unidades, deterioro del rendimiento o el cifrado de todo el contenido del dispositivo. Para contrarrestar estos riesgos existen mecanismos preventivos que consisten en saber cómo configurar y manejar los sistemas de seguridad, revisiones periódicas en *software* o *hardware* y atender las precauciones que recomiendan los fabricantes y los desarrolladores de *software* para la protección de los equipos. Este trabajo tiene el propósito de presentar una guía de buenas prácticas para informar y lograr difundir entre los usuarios las implementaciones y mecanismos de seguridad en dispositivos con sistema operativo *Windows*.

Índice

Nomenclatura

Símbolo	*Significado*
Amenaza	*Todo aquello que intenta o pretende destruir [López y Quezada, 2006].*
código malicioso	*Programas diseñados para infiltrarse en los sistemas y ocasionar afectaciones en los dispositivos electrónicos (computadoras, tabletas, teléfonos, etcétera), alterando su funcionamiento y poniendo en riesgo la información almacenada en ellos.*
Configurar	*Elegir una serie de opciones y procesos ordenados para lograr optimizar el uso de herramientas de software.*
Firewall	*Dispositivo de seguridad de la red de datos que monitorea el tráfico que entra y sale de la misma.*
Instalar	*Es la ejecución de un programa. Trasladar un programa de cómputo en funcionamiento con el sistema operativo.*
Malware	*Es un software diseñado para causarle daño a los dispositivos. Incluye muchos tipos de programas, como spyware, ransomware, caballos troyanos, rootkits, etc. Se pueden expandir manual o automáticamente (Moes, 2019).*
Microsoft Support	*Plataforma de soporte técnico de Microsoft (M.Support, 2023)*
política de seguridad	*Plan de acción para afrontar riesgos de seguridad. Conjunto de reglas para el mantenimiento de cierto nivel de seguridad (López, Quezada, 2006)*
ransomware	*Es una especie de una tecnología maliciosa diseñada para obtener dinero de una víctima (Kaspersky Lab, 2019).*
Software	*Soporte lógico de un sistema informático, es decir, es la parte no física que hace referencia a un programa o conjunto de programas de cómputo que incluye datos, reglas e instrucciones para poder comunicarse con el ordenador y que hace posible su funcionamiento (CISET, 2023).*
Virus	*Es un software que contiene códigos maliciosos.*
Vulnerabilidad	*Es una debilidad que puede ser explotada para violar la seguridad (López y Quezada, 2006).*
Windows Defender	*Herramienta de seguridad de Windows compatible con versiones 8.1 en adelante (Microsoft, 2023).*
Windows Update	*Módulo de actualizaciones al sistema operativo Windows liberadas por el fabricante (Microsoft, 2023).*

1 Introducción

Entre las principales cualidades de un sistema de información son la disponibilidad, integridad y confidencialidad, por lo que, para poder preservar esa configuración confiable y segura en un dispositivo informático es de gran prioridad atender las recomendaciones de los fabricantes de tecnología. A través del siguiente escrito está contenido los mecanismos de seguridad del sistema operativo *Windows* propuestos por el propio fabricante *Microsoft* para sus diversas versiones.

El presente trabajo tiene como objetivos:

-Investigar las herramientas de seguridad que se pueden implementar en equipos con sistemas operativos *Windows*.

-Proponer los mecanismos y configuraciones mínimas para conservar la protección del equipo a nivel sistema (*software* y *hardware*).

-Crear un documento de referencia para el fortalecimiento de la seguridad en un dispositivo con *Windows* en versiones recientes (*Windows* 10, 11 y algunas versiones anteriores).

El propósito de las plataformas de ayuda y soporte es proveer un medio de ayuda actualizado con el fin de prevenir riesgos a través de las implementaciones de mecanismos de seguridad y funcionalidades del sistema operativo para lograr sistemas seguros. La originalidad del presente trabajo es aportar información relevante y de referencia sobre la seguridad en sistemas operativos *Windows* con una línea de acciones sencilla, clara y oportuna hacia la comunidad del instituto para facilitar su consulta y referencia y así establecer acciones de protección a un equipo con el sistema operativo *Windows*.

1.1 Antecedentes

En el año 2000, la seguridad en el sistema operativo *Windows* dio un gran avance, con el lanzamiento de la herramienta incluida *Microsoft Security Essentials* (Carvajal, 2022). Dicha solución de seguridad hacia el dispositivo ofreció protección eficaz y silenciosa y cuya ejecución es en segundo plano, es decir no hay interrupciones del sistema o de otras aplicaciones mientras está activa la herramienta (Microsoft, 2023). *Microsoft*

Security Essentials incluida en los sistemas operativos *Windows Xp* y *Windows* 7 principalmente. Y las ventajas era una solución en tiempo real de protección contra *software* malicioso tipo Virus con un banco de firmas recolectadas por *Microsoft* (Microsoft, 2023).

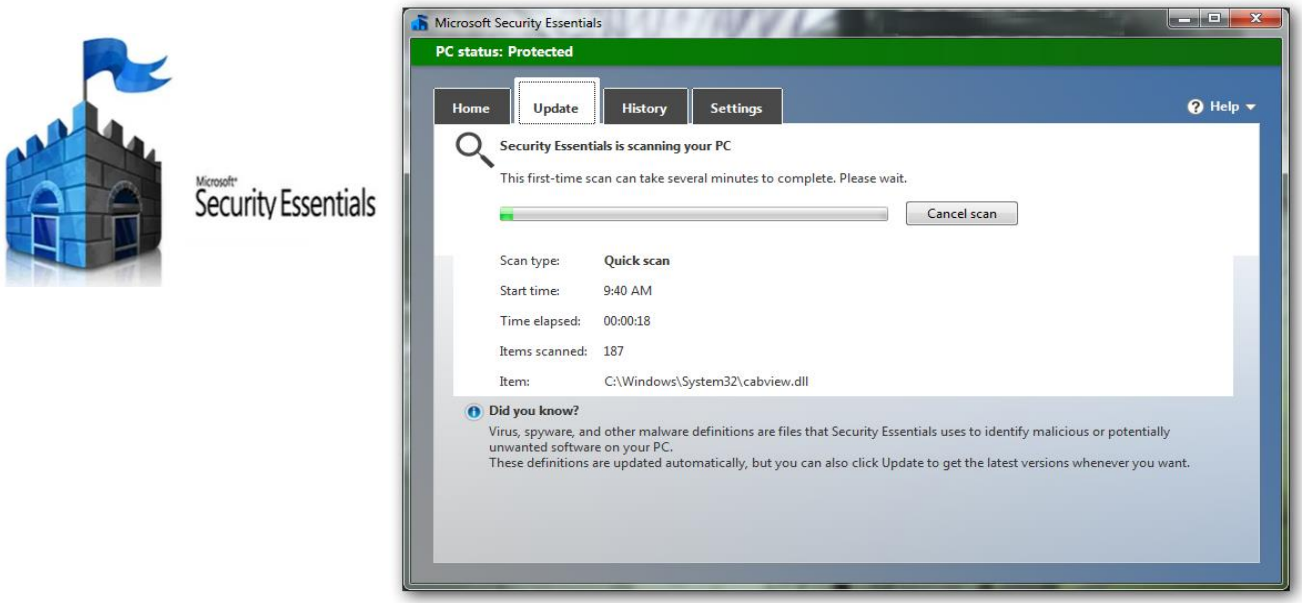

Figura 1. Herramienta de seguridad *Essentials* (Opris, 2018)

La herramienta de seguridad *Microsoft Defender* se integró a los sistemas operativos *Windows Vista*, *Windows* 7 y en adelante como *Windows* 8 y 10; la estructura del *software* es un programa de seguridad tipo antivirus que tiene las funcionalidades de contener amenazas y detección de *software* malicioso en el sistema operativo (Microsoft 2023).
Mientras que para la versión de *Windows* 11 está integrado como un módulo de las medidas de seguridad *Microsoft Mechanics Windows 11,* de acuerdo con la siguiente tabla 1.

Tabla 1. Características *Defender* en *Windows* (Microsoft, 2023)

Medida de seguridad	**Funcionalidad**
Microsoft Defender para punto de conexión	Los clientes de *Windows* se benefician de *Microsoft Defender* para punto de conexión, una funcionalidad de detección y respuesta de puntos de conexión empresariales que ayuda a los equipos de seguridad empresariales a detectar, investigar y responder a amenazas avanzadas. Con datos de eventos enriquecidos e información sobre ataques, *Defender for Endpoint* permite al equipo de seguridad investigar incidentes y realizar acciones de corrección de forma eficaz y eficaz. Defender para punto de conexión también forma parte de *Microsoft 365 Defender*, un conjunto de defensa empresarial unificado previo y posterior a la vulneración que coordina de forma nativa la detección, la prevención, la investigación y la respuesta entre puntos de conexión, identidades, correo electrónico y aplicaciones para proporcionar protección integrada contra ataques sofisticados.

La seguridad de *Windows* por *Microsoft Defender* incluye permisos de hardware, control de aplicaciones, *firewall* local y protección de red, análisis de amenazas y más (Figura 2).

Figura 2. Opciones de configuración en *Defender (Creación propia)*

La aportación de este trabajo es presentar los mecanismos y configuraciones de seguridad basada en las herramientas de protección del sistema operativo *Windows Defender* como una utilería o medio de implementación nativo o dentro del sistema operativo para los equipos y de fácil acceso a los usuarios, que garanticen la confidencialidad, integridad y disponibilidad de la información dentro del equipo de cómputo con sistema operativo *Windows*.

2 Seguridad en sistemas operativos Windows

Las versiones más recientes de *Windows,* de acuerdo con el uso y la configuración de las funcionalidades establecen una serie de opciones al usuario para configurar y robustecer la seguridad de la información alojada en los equipos con esos sistemas operativos. En la página oficial da la pauta el módulo de *Defender* sobre protección y seguridad para *Windows* bajo lo siguiente:

> *Windows 10 y 11 incluyen Seguridad de Windows, que proporciona la protección antivirus más reciente. El dispositivo se protegerá activamente desde el momento en que inicies Windows. Seguridad de Windows examina continuamente en busca de malware (software* ***malintencionado****), virus y amenazas de seguridad. Además de esta protección en tiempo real, las actualizaciones se descargan automáticamente para ayudar a mantener tu dispositivo seguro y protegerlo de amenazas (Microsoft, 2023).*

La forma de acceso a los módulos de protección general es a través del buscador de la barra de tareas introducir la palabra *Defender* y presentar las opciones de configuración para la Seguridad en *Windows* (Figura 3).

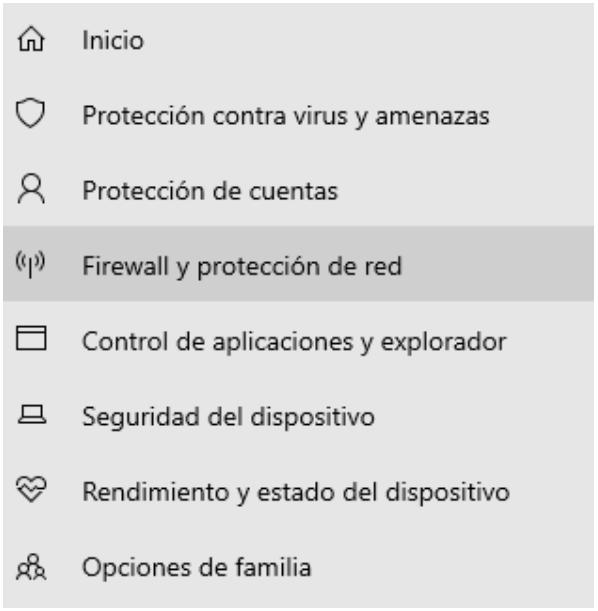

Figura 3. Módulos de seguridad en *Windows* (Creación propia)

A continuación, se presenta de forma detallada las opciones de seguridad en *Windows*.

3 Control sobre permisos de usuarios/administradores

Los permisos por usuario, es el perfil de sesión activa capaz de modificar las características o funcionalidades de acuerdo con los privilegios asociado.
Dichos privilegios se otorgan para ver y modificar la configuración del sistema o ya sea para lograr un acceso remoto al equipo, por lo que, el usuario debe contar con privilegios con todos los privilegios, es decir con los permisos de *Administrador local completos*; mientras que otros permisos como un usuario no puede modificar ni reemplazar la configuración proporcionada por el usuario administrador.

La funcionalidad de acceso remoto al equipo deberá estar asociada al usuario principal (administrador) para minimizar riesgos de usuarios no autorizados al equipo. Existe la opción de notificación cuando haya intento de modificaciones mediante acceso remoto, tal como, activar *Microsoft Defender Antivirus real-time protection*.

Procedimiento para ver o cambiar la lista de acceso remoto protegido:

1. En el dispositivo con *Windows* 10 o *Windows* 11, abrir la aplicación Seguridad de *Windows*.
2. Seleccionar “Protección contra virus y amenazas”.
3. En Protección contra *ransomware*, seleccionar Administrar protección contra *ransomware*.
4. Si el acceso controlado a carpetas está desactivado, deberá activarlo. Seleccionar carpetas protegidas.
5. Realice uno de los siguientes pasos:

- Para agregar una carpeta, seleccione + Agregar una carpeta protegida.
- Para eliminar una carpeta, selecciónela y luego seleccione Eliminar.

4 Protección de actualización (*Windows Update)*

La actualización de los sistemas operativos es un procedimiento periódico cuyas ventajas son las mejoras al sistema operativo y la protección de vulnerabilidades en el *software* por parte del fabricante de *Windows* en la opción *Windows Update*. Mediante la ejecución de módulos o archivos en el sistema, *Microsoft* actualiza automáticamente estos archivos como parte de las actualizaciones de *Windows* (Figura 4). La ruta de acceso a esta línea es en el menú inicio, la búsqueda con *Windows Update*->Buscar actualizaciones, y si las hay disponibles se habilita el botón “Instalar”.

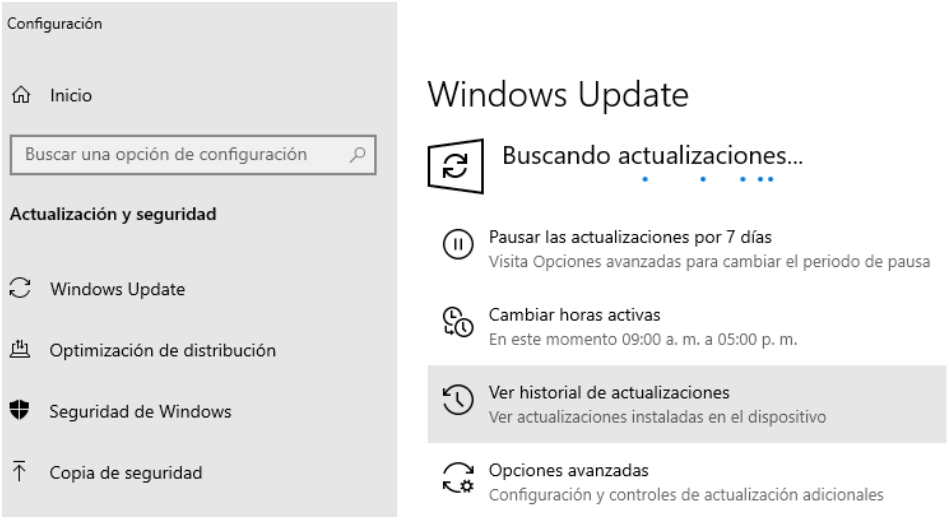

Figura 4. Actualizaciones del sistema

Al concluir la descarga e instalación de actualizaciones al sistema operativo, se deberá realizar run reinicio al equipo, así el sistema marcará un estatus exitoso ¡Todo está actualizado! (Figura 5).

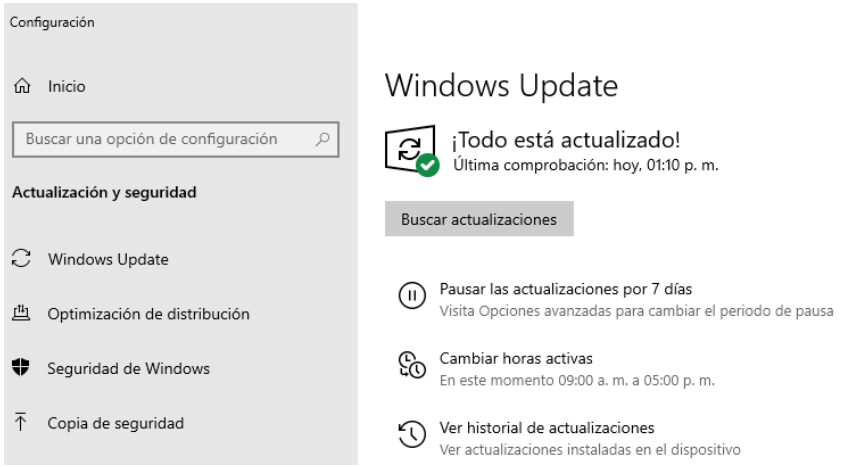

Figura 5. El sistema actualizado

También se valida la actualización de las firmas o de la sección Protección contra virus y amenazas; en Actualizaciones de protección contra virus y amenazas, seleccionar Buscar actualizaciones para garantizar que tiene una protección actualizada y completa por parte del fabricante (Figura 6).

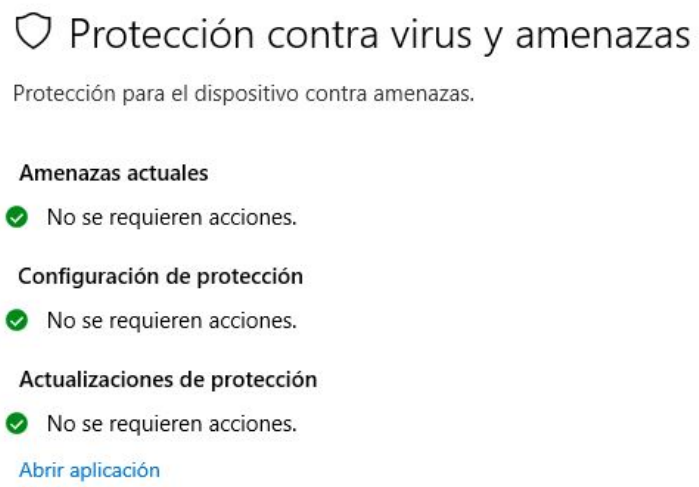

Figura 6. Actualizaciones de protección

5 Protección con firewall

5.1 Firewall

En los sistemas operativos un *firewall* o cortafuegos tienen la capacidad de controlar las entradas/salidas de un sistema a través de sus puertos o servicios del equipo. Es un mecanismo de seguridad que va validando el *ID* de proceso con lo que una aplicación ejecutada en el sistema operativo.

> *Para la mayoría de los equipos, especialmente los portátiles o equipos de escritorio normales, o las redes de inicio, el firewall debe permitir muy poco tráfico de entrada, si los hay. Rara vez hay motivos legítimos para que otros dispositivos necesiten conectarse a su dispositivo, o a la red doméstica, no solicitado.*

Los cortafuegos tienen la función de depurar aquellas peticiones que no cumplan con determinados criterios de seguridad entre la comunicación entre la *PC* y la red, bloqueando probables amenazas a la información, además este módulo es una gran herramienta para el tráfico de información. Algunas desventajas son la protección de aquellas comunicaciones que no pasan a través del sistema, tales como intercambio de archivos e instalación de *software*, para ello se recomienda el uso de un antivirus.

Nota: Desactivar la herramienta cortafuegos/*firewall* puede aumentar el riesgo para su dispositivo o sus datos respecto a la conexión de *internet*. (Windows Security de Microsoft Support, 2022).

En el menú principal del sistema operativo *Windows* se encuentra la protección cortafuegos, *Firewall de Windows Defender* (Figura 7).

Figura 7. Acceso al *Firewall* de *Windows*

Al abrir Opciones Avanzadas (Figura 8), se tiene la opción de configurar en tres secciones de su conexión local perfil de dominio, perfil privado y perfil público; en cada uno de estos perfiles se activan para filtrar las conexiones o intercambios de información o procesos cuando se presenta una conexión a *internet*.

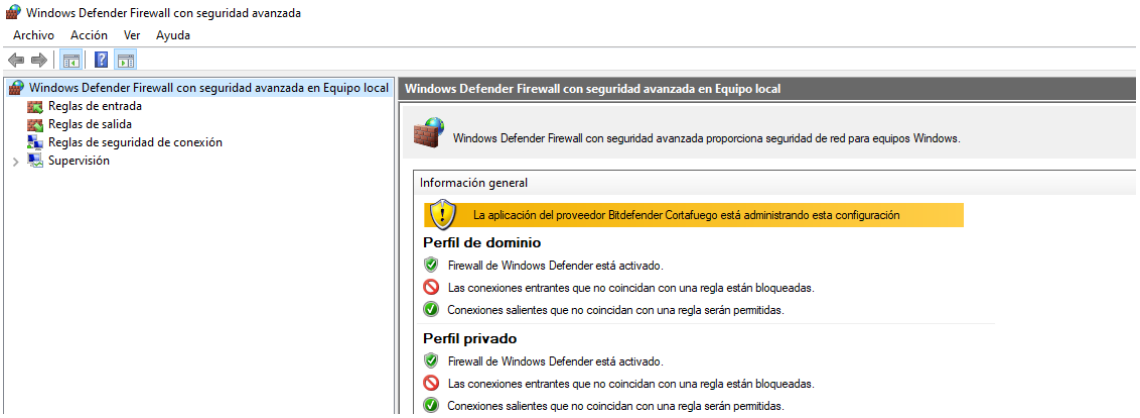

Figura 8. Opciones avanzadas de configuración

Los estatus de la protección sobre *Windows* son dos, “privado” o “público”, la diferencia entre estos son los permisos que tiene otros dispositivos en la misma red para ver o conectarse al dispositivo. Como se mencionó anteriormente, el *firewall* es un auxiliar en el control del tráfico sobre peticiones que entran o salen de la red o del dispositivo; su funcionamiento radica en permitir reglas declaradas sobre puertos y servicios (Seguridad de Windows, 2022).

Recomendaciones de **Microsoft Support** a la protección del sistema:

- Mantener activo el f*irewall*.
- Mantener *software* actualizado.
- Usar el antivirus y mantenlo actualizado.
- Hacer buen uso de tus contraseñas (mínimo de 8 dígitos).
- No abrir archivos sospechosos o dar clic en enlaces sospechosos (pueden aparecer en mensajes, *tweets*, fotos en línea, como archivos adjuntos e incluso en fuentes confiables).

- Usar el navegador con precaución (Evitar visitar páginas con contenido ilícito o no apropiado, algunos de estos pueden instalar *software* malicioso, los *firewalls* y antivirus bien configurados también ayudan a prevenir).
- No consumir o utilizar material ilegal (la mayoría de estos contenidos provienen de páginas no confiables que pueden instalar al mismo tiempo *software* malicioso).
- Evitar usar memorias o unidades de almacenamiento tipo USB u otros dispositivos externos que no sean de uso personal o ajenos (Estos pueden contener código malicioso que se instala automáticamente al conectar esta clase de dispositivos).

6 Configuración de privacidad

La configuración de la privacidad incluye gestionar los permisos sobre los periféricos tales como micrófono, cámara y etc. Así, en el sistema operativo *Windows* 10 y 11 tiene una sección de Privacidad y sobre esta se Activan o Desactivan los permisos de acuerdo con el perfil mínimo por aplicación e incluye el dispositivo (Figura 9).

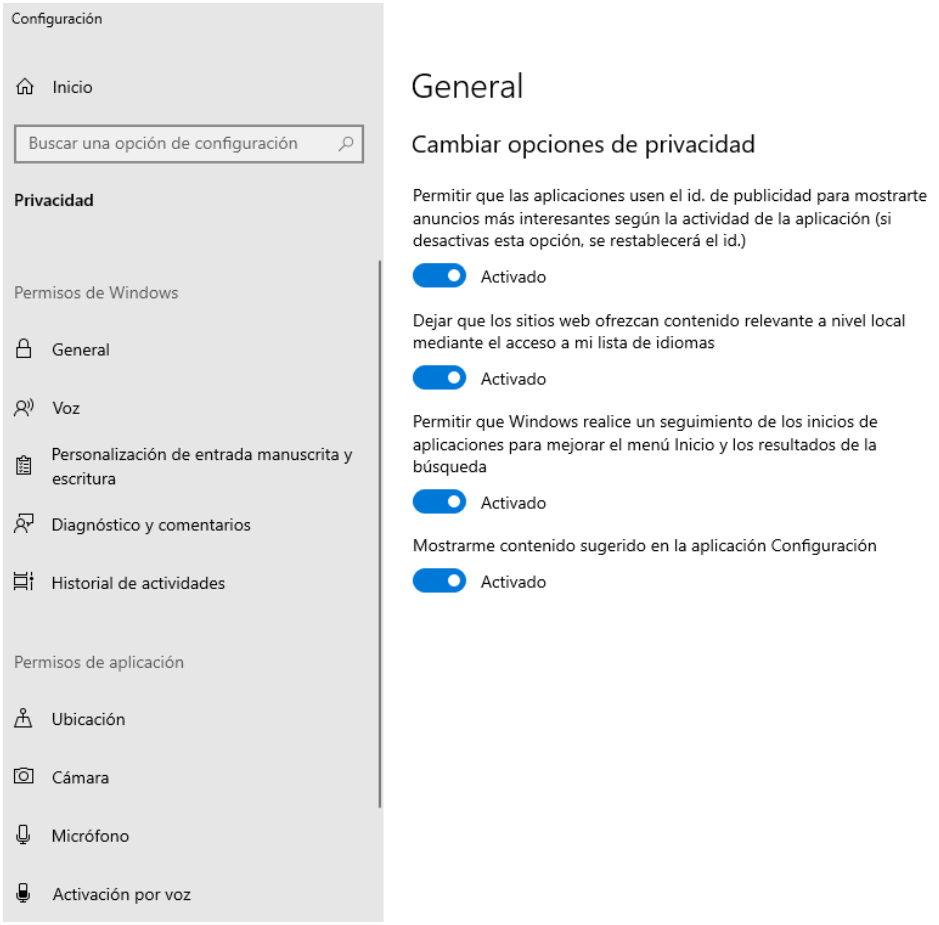

Figura 9. General de privacidad

Existen tres permisos por aplicación los cuales se tienen que gestionar: ubicación, cámara y micrófono; y se activan/desactivan de acuerdo con la aplicación que usa dichos periféricos (Figura 10).

En los permisos de Ubicación se desactivan para disminuir la localización del dispositivo a terceros, otra opción es activar mientras esté en uso la aplicación, es decir de forma manual realizar la activación, solo cuando se requiera (Figura 10).

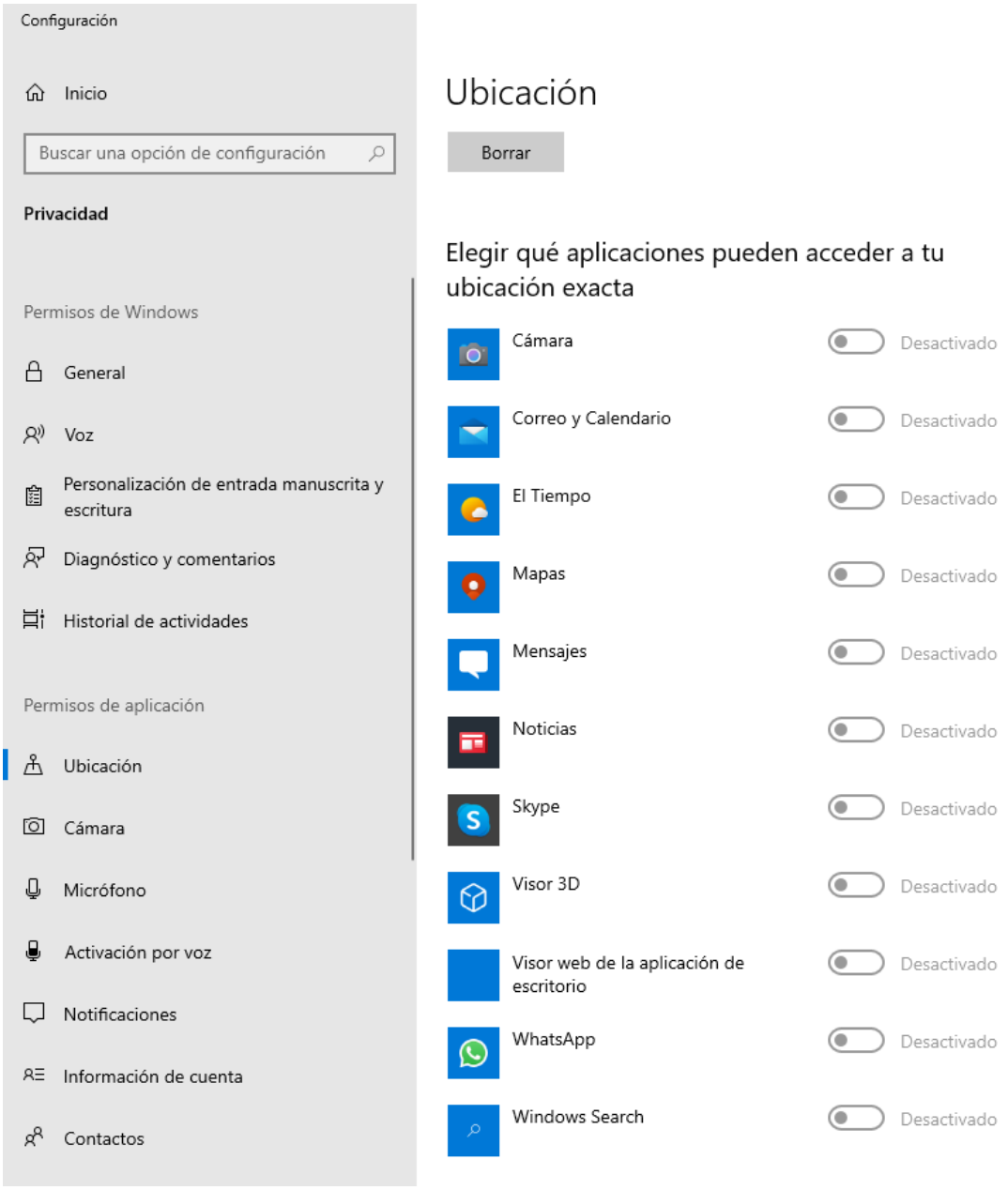

Figura 10. Lista de aplicaciones

Para los permisos de la cámara, es la misma idea de habilitar por aplicación (aplicaciones instaladas desde la *Microsoft Store).* El uso de la cámara o a menos que se active mientras esté en uso (Figura 11). Se activa los permisos desde esta sección, ya que al abrir la aplicación puede verse afectada la cámara si no se habilita en esta sección.

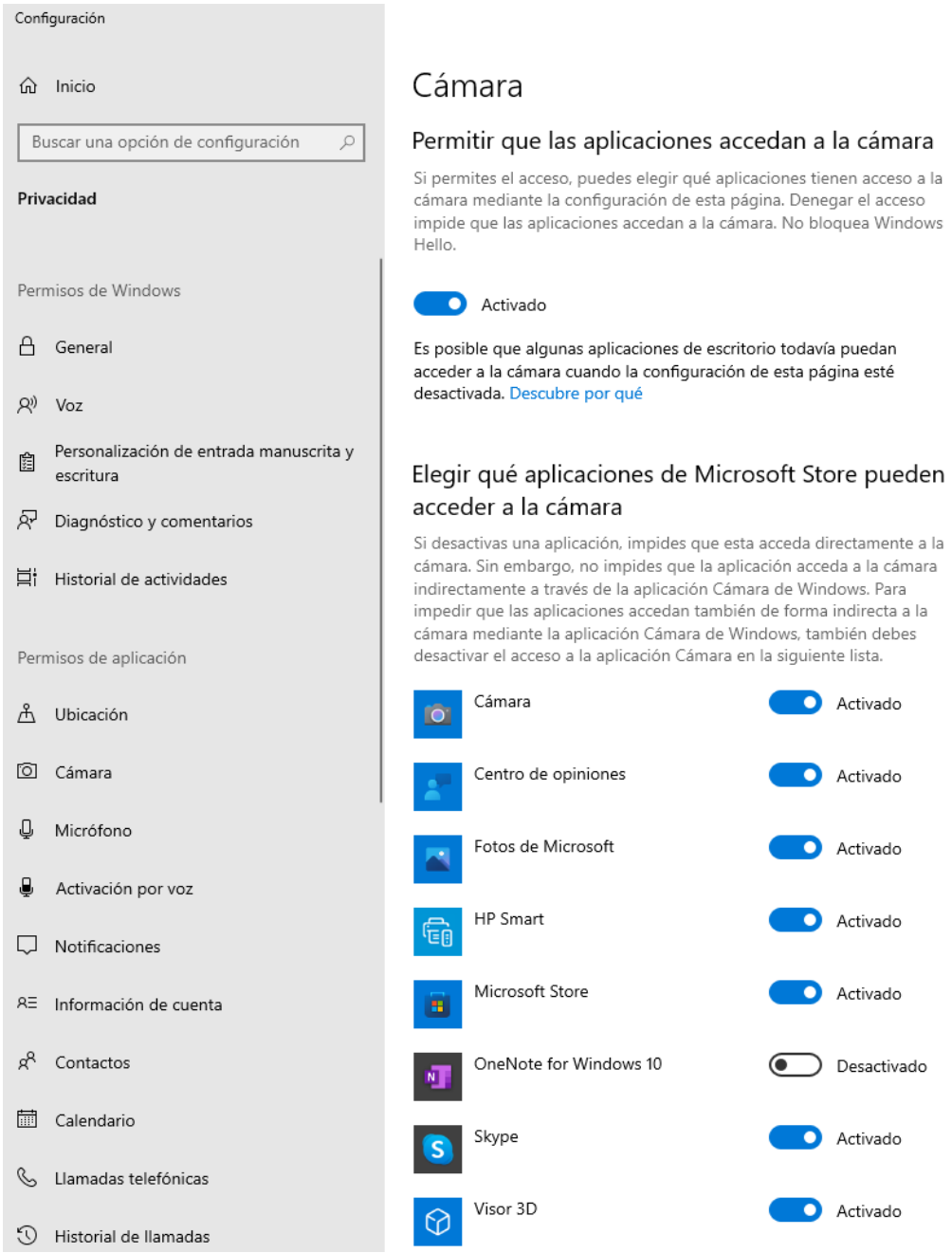

Figura 11. Permisos de aplicación sobre la cámara

Permisos por aplicación en Micrófono, se activan de acuerdo con la lista de aplicaciones que la requieren, es importante que la lista de aplicaciones también proviene de fuentes confiables de descarga como *Microsoft Store* y páginas oficiales de *software*. Se activa los permisos desde esta sección (Figura 12).

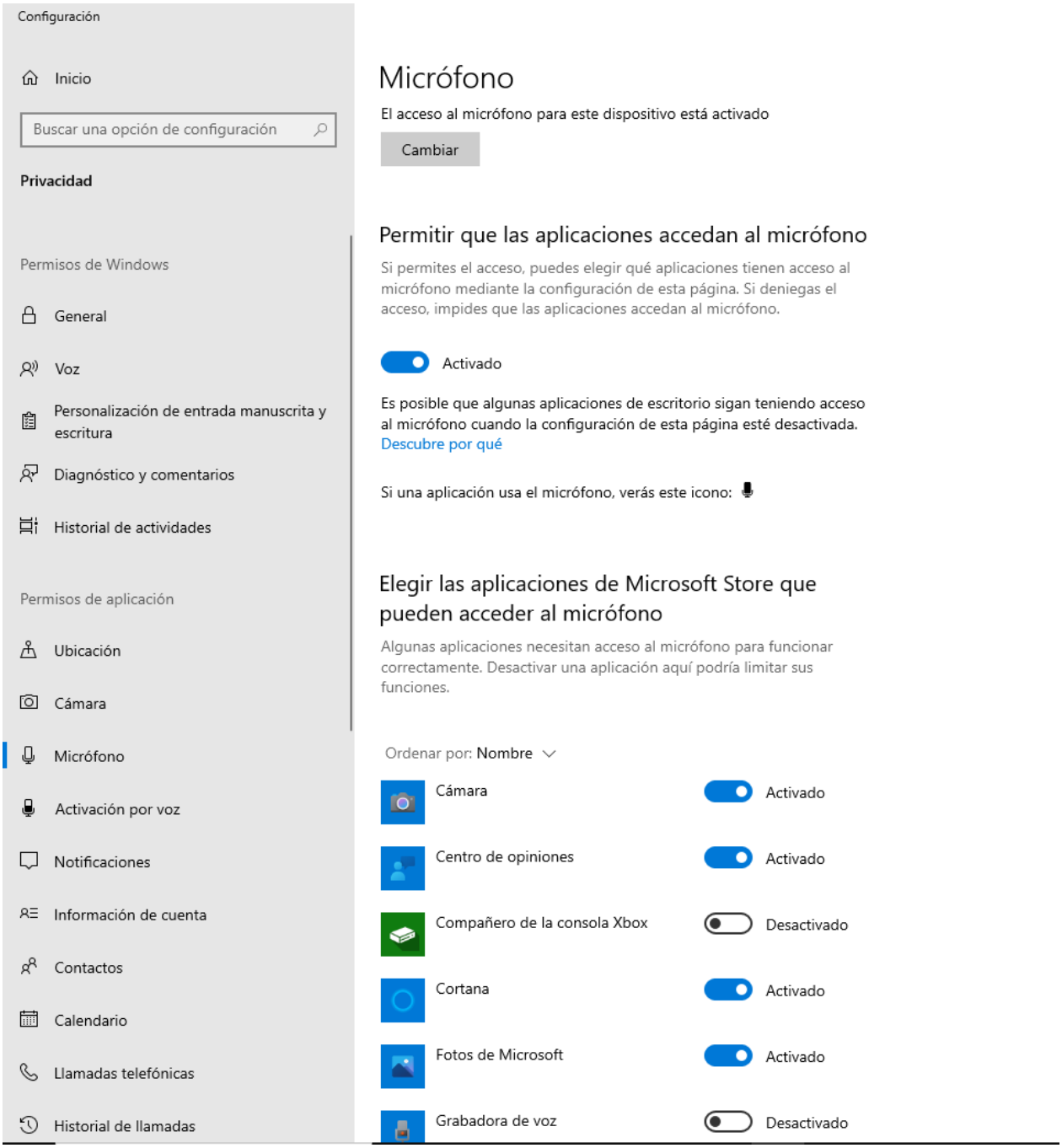

Figura 12. Permisos de aplicación en micrófono

7 Antivirus

Los antivirus son programas cuya función es proteger el sistema de nuestro equipo de amenazas como virus que evolucionan cada día para encontrar nuevas maneras de robar información o perjudicar el funcionamiento de nuestra computadora.

Dependerá del usuario la elección del antivirus que considere apto, en el caso de un antivirus gratuito ofrece la siguiente cobertura:

- Análisis de todos los archivos de la computadora.
- Análisis de correos electrónicos y mensajes instantáneos en busca de virus u otro *malware* (código malicioso por vía navegación *Web*).
- Antivirus en la red para interceptar y bloquear la ejecución de *script* en las páginas de Internet si amenazan la seguridad de tu computadora.
- Medidas contra el *phishing* para bloquear las páginas web que parecen seguras y que terminan robando tus datos.

En el sitio oficial de *software* UNAM (https://www.software.unam.mx/), es el medio de la comunidad para consultar y medio de descarga confiable de *software* para la Universidad Nacional Autónoma de México.

De acuerdo con la sección de Antivirus, se toma como referencia la instalación la protección *Avira Free* Antivirus que está dentro de la lista de opciones a instalar.

La instalación del antivirus es similar al de los demás programas o aplicaciones, siguiendo las instrucciones, dar clic sobre el enlace de la página del proveedor, y en la opción “Descargar”, paso siguiente iniciará la descarga e instalación para la cual solicitará permisos de administrador.

Cuando está instalado el antivirus será necesario realizar el primer “Escaneo inteligente”, el cual analizará todos los directorios de nuestro equipo y enviará un resumen con los hallazgos o resultados que haya encontrado al término de este procedimiento; en caso de encontrar algún mensaje, podremos ajustarlo o configurarlo en la sección “Arreglar problemas”.

Escaneo avanzado

1. Seleccione Inicio > Configuración > Actualización y seguridad > Seguridad de *Windows* y luego Protección contra virus y amenazas.
2. En Amenazas actuales, seleccione Opciones de análisis (o en versiones anteriores de *Windows* 10, en Historial de amenazas, seleccione Ejecutar un nuevo análisis avanzado). (Anexo A. Figura A.8)
3. Seleccione una de las opciones de escaneo:

- Escaneo completo (verifique los archivos y programas que se están ejecutando actualmente en su dispositivo). (Anexo A. Figura A.9)
- Escaneo personalizado (escanear archivos o carpetas específicos)
- Exploración sin conexión de *Microsoft Defender* (ejecuta esta exploración si tu dispositivo ha sido o podría estar infectado por un virus o *malware*). Más información sobre *Microsoft Defender* sin conexión

4. Seleccione Escanear ahora.

Programar un escaneo

1. Seleccione el botón Inicio, escriba programar tareas en el cuadro de búsqueda y, en la lista de resultados, seleccione Programador de tareas.
2. En el panel izquierdo, seleccione la flecha (>) junto a la Biblioteca del programador de tareas para expandir, haga lo mismo con *Microsoft* > *Windows* y luego desplácese hacia abajo y seleccione la carpeta *Windows Defender*.
3. En el panel superior central, seleccione Exploración programada de Windows Defender. (Señale las opciones para ver los nombres completos). (Anexo A. Figura A.10)
4. En el panel Acciones de la derecha, desplácese hacia abajo y luego seleccione Propiedades. (Anexo A. Figura A.11)
5. En la ventana que se abre, seleccione la pestaña Desencadenadores y luego seleccione Nuevo.
6. Establezca su hora y frecuencia preferidas, y luego seleccione Aceptar. (Anexo A. Figura A.12)
7. Revise el programa y seleccione Aceptar.

8 Conclusiones

De acuerdo con el desarrollo del presente trabajo fue creado un documento con las configuraciones básicas de protección y seguridad al equipo, ya que se establecieron una serie de 6 etapas para robustecer la seguridad con sistemas operativos *Windows*, en su módulo *Windows Defender*:

1 Seguridad en sistemas operativos *Windows*

2 Control sobre permisos de usuarios/administradores

3 Protección de actualización (*Windows Update*)

4 Protección con *firewall*

5 Configuración de privacidad

6 Antivirus

En la configuración de seguridad en el sistema operativo *Windows*, en su versión más reciente *Windows* 10 y 11, se detalló un documento técnico y amigable al usuario para robustecer de forma mínima la configuración de la seguridad en el sistema operativo.

Los resultados de este documento son una aportación breve de los procedimientos (paso a paso) sobre los mecanismos de seguridad a nivel *software* para un equipo con sistema operativo *Windows*.

En la actualidad las opciones predeterminadas en la seguridad del equipo *Windows* puede incluir variación de acuerdo con las necesidades y las aplicaciones que el usuario necesite, por lo que es importante tener una referencia general de las configuraciones mínimas y adecuarlas a los perfiles de uso de cada equipo y de cada usuario.

Las ventajas de la referencia del fabricante como *Microsoft* es la actualización de sus *blogs* de Seguridad de *Windows*, ya que actualiza las líneas y los módulos, así como dar una referencia completa de la configuración en el sistema operativo.

En futuro se pretender realizar un documento con los lineamientos de seguridad en el *Internet* de las cosas y en sistemas operativos *GNU/Linux*.

Referencias bibliográficas

Carvajal, C. (2022). Hace 13 años nació el antivirus de Microsoft para Windows: Microsoft Security Essentials [Internet] Disponible desde: https://computerhoy.com/noticias/hace-13-anos-nacio-antivirus-microsoft-windows-microsoft-security-essentials-11323613 [Acceso 16 Febrero 2023]

CISCO (2007). Guía del usuario de Cisco Router and Security Device Manager. Webinar Trendnet: Cómo la calidad de servicio mejora la implementación de la red IP en tus proyectos. [Internet] Disponible desde: https://www.youtube.com/watch?v=on3z5iwnBEU [Acceso 01 Agosto 2021]

CISET [2023]. Software - Concepto y tipos de software https://www.ciset.es/glosario/480-software-concepto-y-tipos

Cunha (2020). Qué es un proxy y para qué sirve. [Internet] Disponible desde: https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/ [Acceso 22 Junio 2021]

Firewall-Firm (2021). Firewall Training in India [Internet] Disponible desde: https://firewall-training.in/ [Acceso 15 Julio 2021].

Google (2021). History of Firewalls [Internet] Disponible desde: https://sites.google.com/site/firewallsfordummies/history-of-firewalls [Acceso 25 de Mayo 2021].

Kaspersky Lab, (2019) Ransomware: definición, prevención y eliminación. [internet], Threats KasperskyLab. Disponible desde: https://latam.kaspersky.com/resource-center/threats/ransomware [Acceso 15 de Noviembre de 2019]

López, B.; Quezada C. (2006) Fundamentos de seguridad informática. 1a. ed. México, UNAM, Facultad de Ingeniería.

Microsoft (2023) Microsoft Security Essentials [Internet] Disponible desde: https://www.microsoft.com/es-mx/download/details.aspx?id=5201 [Acceso 14 Enero 2023]

Microsoft (2023) Micorsoft Defender [Internet] Disponible desde 10 de febrero de 2023 https://learn.microsoft.com/es-es/windows/security/operating-system [Acceso 20 Febrero 2023]

Microsoft D. (2022, June 1). *Protect important folders from ransomware from encrypting your files with controlled folder access*. Microsoft Docs. Retrieved June 16, 2022, from https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide

Microsoft. (n.d.-a). *¿Qué es un firewall?* Retrieved June 16, 2022, from https://support.microsoft.com/es-es/office/-qu%C3%A9-es-un-firewall-6870c88d-69b6-4db4-9cb1-0e4afa7a8603

Microsoft. (n.d.-a). *Firewall & network protection in Windows Security*. Retrieved June 16, 2022, from https://support.microsoft.com/en-us/windows/firewall-network-protection-in-windows-security-aef9838b-d081-fd75-3b1b-e5fa794c003b

Microsoft. (n.d.-a). *Activar o desactivar el Firewall de Microsoft Defender*. Retrieved June 16, 2022, from https://support.microsoft.com/es-es/windows/activar-o-desactivar-el-firewall-de-microsoft-defender-ec0844f7-aebd-0583-67fe-601ecf5d774f

Microsoft. (n.d.-c). *Firewall y protección de red en seguridad de Windows*. Retrieved June 16, 2022, from https://support.microsoft.com/es-es/topic/firewall-y-protecci%C3%B3n-de-red-en-seguridad-de-windows-2385b621-9c5c-4834-9914-c7393f75fa84

S. (2021, October 29). *Best practices for configuring Windows Defender Firewall - Windows security*. Microsoft Docs. Retrieved June 16, 2022, from https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring

Microsoft. (n.d.-g). *Work remotely*. Retrieved June 16, 2022, from https://support.microsoft.com/en-us/windows/keep-your-computer-secure-at-home-c348f24f-a4f0-de5d-9e4a-e0fc156ab221

Microsoft. (n.d.-d). *Protect your devices and Data from Malware*. Retrieved June 16, 2022, from https://support.microsoft.com/en-us/windows/protect-my-pc-from-viruses-b2025ed1-02d5-1e87-ba5f-71999008e026

Microsoft. (n.d.-b). *Device protection in Windows Security*. Retrieved June 16, 2022, from https://support.microsoft.com/en-us/windows/device-protection-in-windows-security-afa11526-de57-b1c5-599f-3a4c6a61c5e2

Microsoft. (n.d.-i). *Turn on device encryption*. Retrieved June 16, 2022, from https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838

Microsoft. (n.d.-e). *Help protect my device with Windows Security*. Retrieved June 16, 2022, from https://support.microsoft.com/en-us/windows/help-protect-my-device-with-windows-security-1a5b8102-c93d-0573-8fd3-b2d33a1e5386

Microsoft. (n.d.-f). *Programar un examen en el Antivirus de Microsoft Defender*. Retrieved June 16, 2022, from https://support.microsoft.com/es-es/topic/programar-un-examen-en-el-antivirus-de-microsoft-defender-54b64e9c-880a-c6b6-2416-0eb330ed5d2d

Microsoft .Support [2023]. Soporte técnico de Microsoft. https://support.microsoft.com/es-es

Moes T. (2019) ¿Qué es malware? La definición y los 5 tipos principales. [internet], SoftwareLab Blog. Disponible desde: https://softwarelab.org/es/que-es-malware/ [Acceso 16 de Noviembre 2019].

Opris E. (2018). Microsoft Security Essentials - MSE. From Softpedia [Internet] Disponible desde https://www.softpedia.com/get/Antivirus/Microsoft-Security-Essentials.shtml [Febrero 2023]

Ostec (2020). Firewall: Historia. [Internet] Disponible desde: https://ostec.blog/es/seguridad-perimetral/firewall/ [Acceso 25 Mayo 2021].

Ryabova, Y. (2021, March 18). *Kaspersky Free: Protección gratuita para tus computadoras*. Kaspersky Daily. Retrieved June 16, 2022, from https://latam.kaspersky.com/blog/free-antivirus/12241/

Valero, C. (2022, June 6). *Ajustes del antivirus Windows Defender para más seguridad*. ADSLZone. Retrieved June 16, 2022, from https://www.adslzone.net/esenciales/windows-10/windows-defender-antivirus/

Wikipedia (2019) Log (informática). [internet], Artículo definición de log. Disponible desde: https://es.wikipedia.org/wiki/Log_(inform%C3%A1tica) [Acceso 19 de Noviembre 2019]

Anexo A. Implementación de mecanismos de seguridad en *Windows* (laboratorio)

Protección de *ransomware*, esta protección aporta un nivel activo en la denegación del acceso sobre información del equipo que tiene activa esta herramienta, en la opción: Seguridad de *Windows*->Protección frente a *ransomware* (en estado encendido/indicador verde), se encuentra activo por *default* (Figura A1).

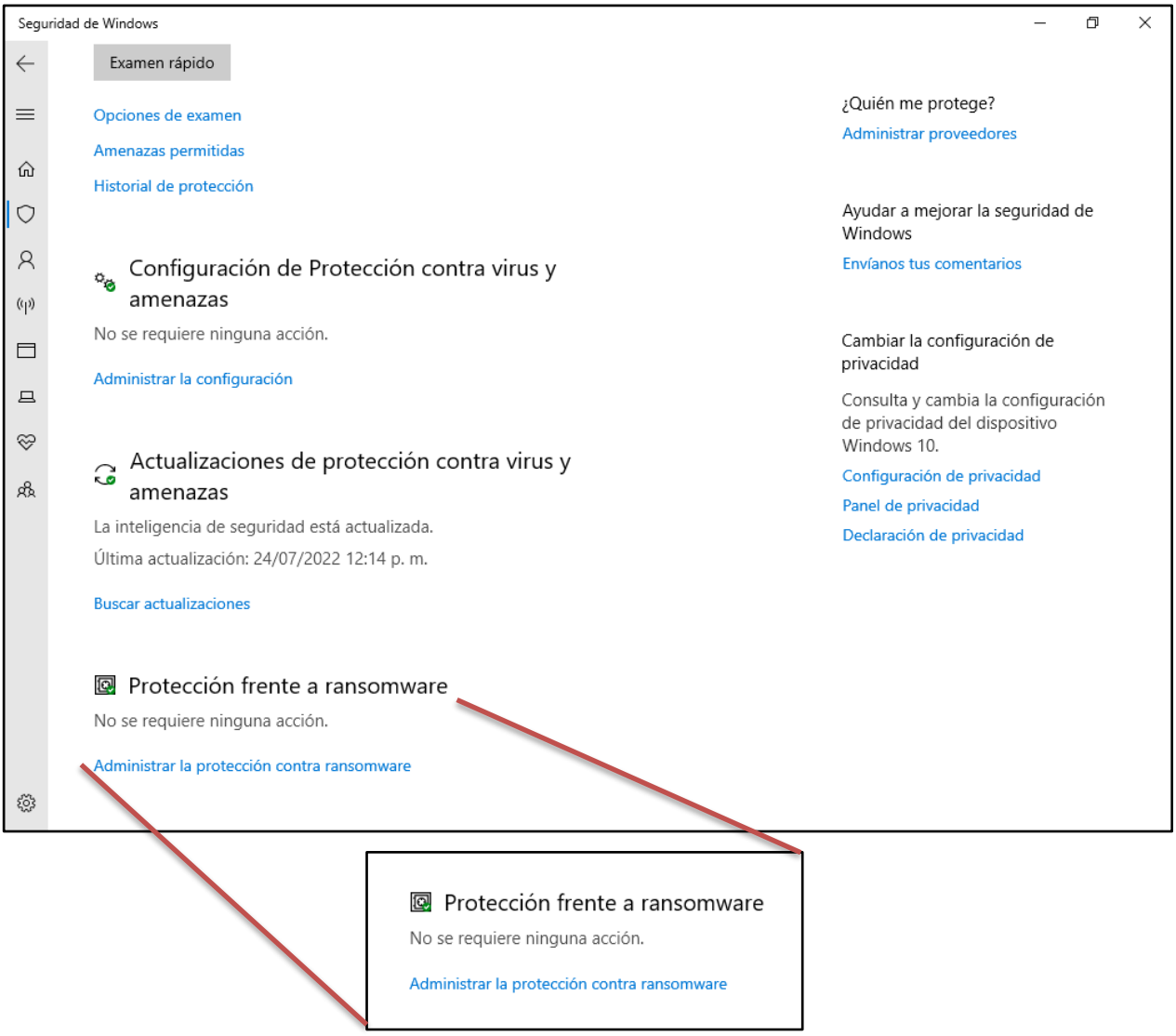

Figura A.1 Activación de mecanismo de protección

El control de acceso a las carpetas nos brinda mayor seguridad contra virus o cualquier agente que pretenda manipular nuestra información. Para seleccionar las carpetas que deseamos proteger, es necesario primero seleccionar el estado de “Activado” en el apartado de “Acceso controlado a carpetas” (Figura A.2).

Figura A.2 Configuración de nivel de protección

Desde “Carpetas protegidas” en Seguridad de *Windows* > Protección contra virus y amenazas > Protección frente a *ransomware* > Acceso controlado a carpetas > Carpetas protegidas, seleccionar agregar o eliminar las carpetas protegidas adicionales (Figura A.3).

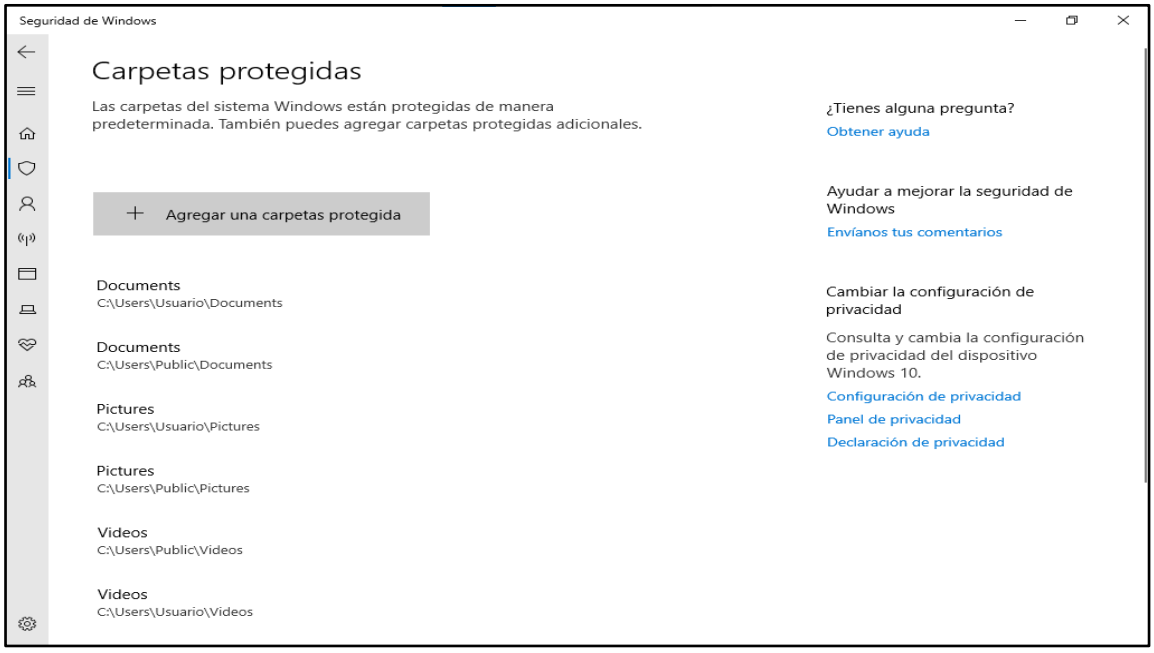

Figura A.3 Personalizar nivel de protección “a nivel archivos”

En la siguiente fase es la protección de virus, en el manejo de archivos es común que en los dispositivos de almacenamiento externos tales como memorias USB, DVD, discos externos y etc., al no hacer uso adecuado de los mismos pueda haber vulnerabilidad de contener virus y programas maliciosos que creen huecos de seguridad en el sistema operativo. Por lo que, se debe considerar la activación del módulo de seguridad. Configuración de protección contra virus y amenazas (Figura A.4). Además, se debe mantener y buscar actualizaciones del módulo de virus y amenazas, desde seguridad de *Windows* (Figura A.4).

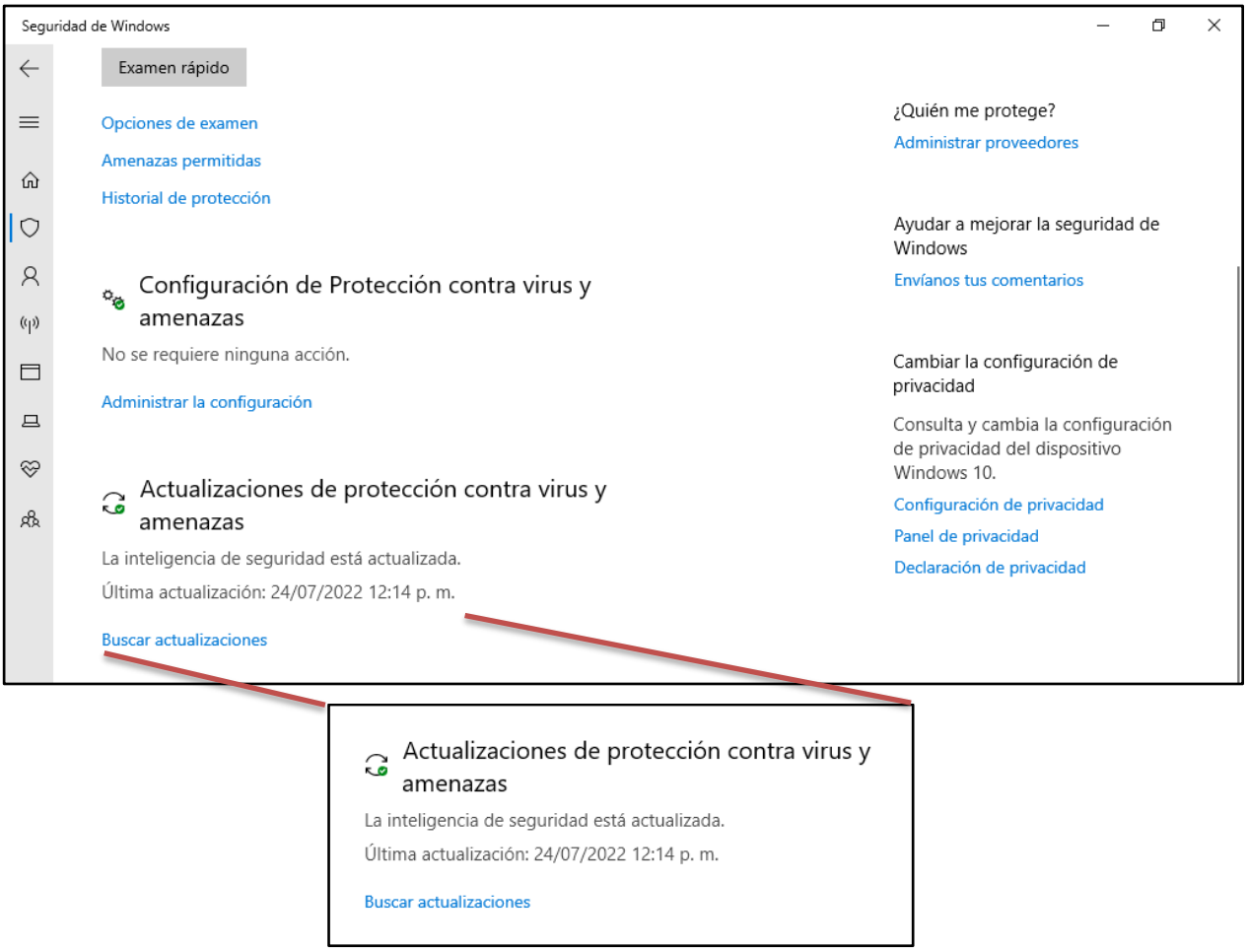

Figura A.4 Actualización de protección contra virus y amenazas

En el módulo Seguridad de *Windows -> Configuración de protección contra virus y amenazas* se administran las funciones relacionadas con la seguridad de nuestro dispositivo a nivel análisis en carpetas o archivos para conocer su nivel de estado (Figura A.5).

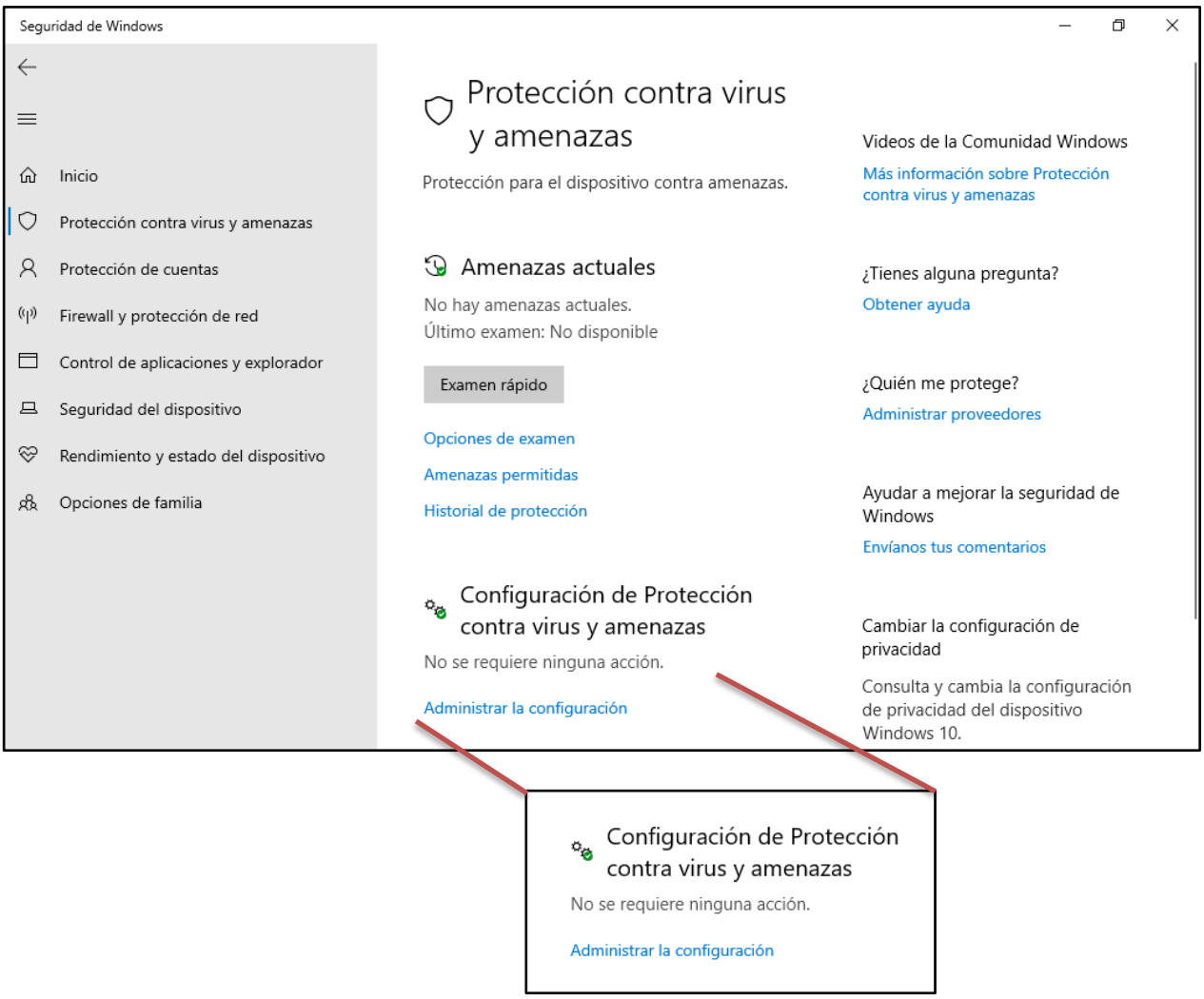

Figura A.5 Administrar la configuración de protección

Protección contra alteraciones o *Tamper Protection* es una de las herramientas que ofrece a *Windows* una función de protección y gestión de cambios críticos relacionados a la seguridad en tiempo real, compatibilidad y configuración del módulo *Microsoft Defense*. Este módulo identifica procesos que contengan datos personales y al tratar de ser modificados por un tercero (tal como un *software* o petición de internet) enviará una alerta en tiempo real mencionando que se ha solicitado cambios a la información personal del equipo; así el usuario gestionará y se conocerá si es un proceso válido o no (Figura A.6).

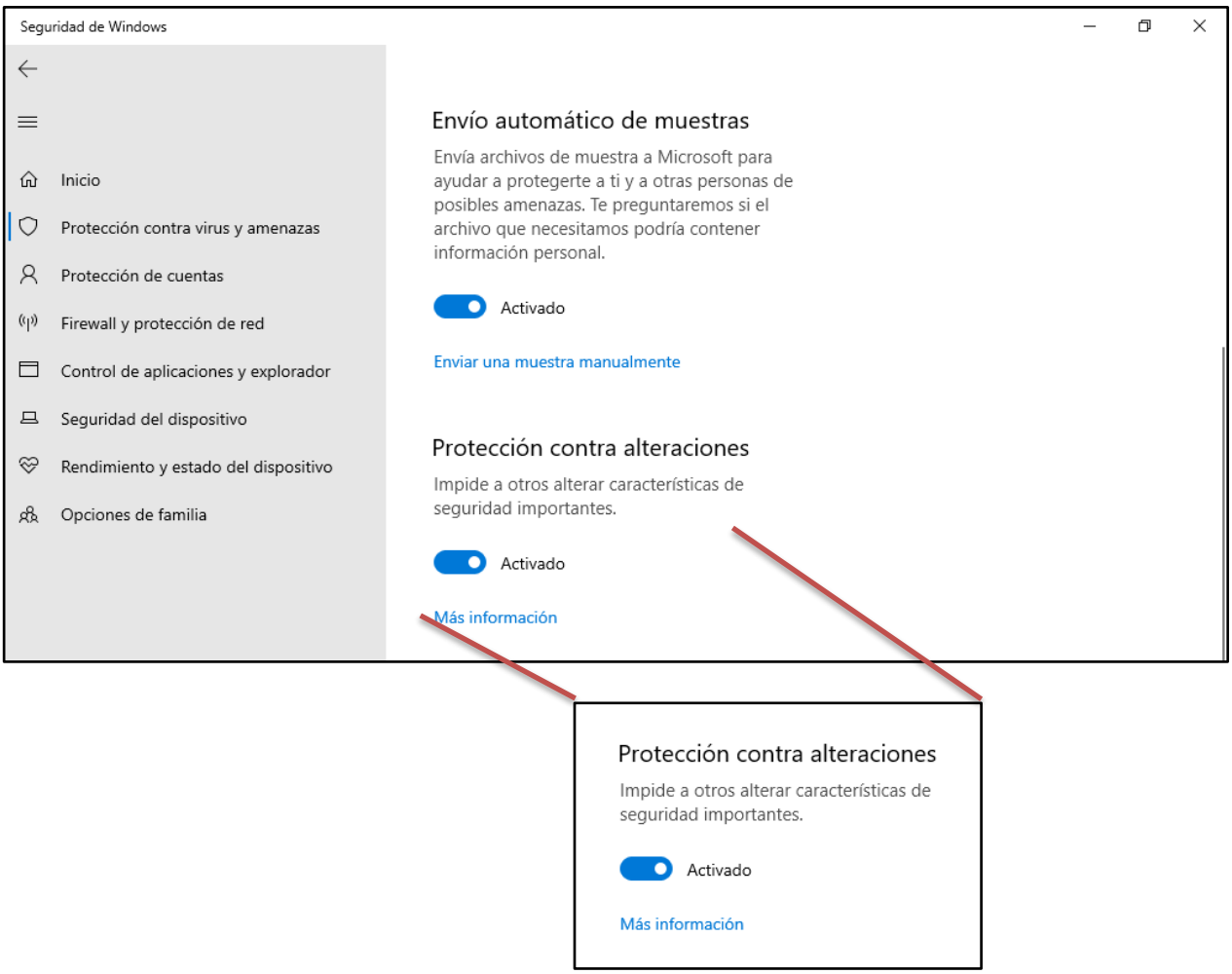

Figura A.6 Activar función de seguridad *(*Protección contra alteraciones)

Realizar un examen rápido permite llevar a cabo un escaneo de nuestros archivos en caso de existir sospecha de que nuestro equipo ha sido infectado, esto lo podemos llevar a cabo desde Seguridad de *Windows* o en la mayoría de los antivirus (Figura A.7).

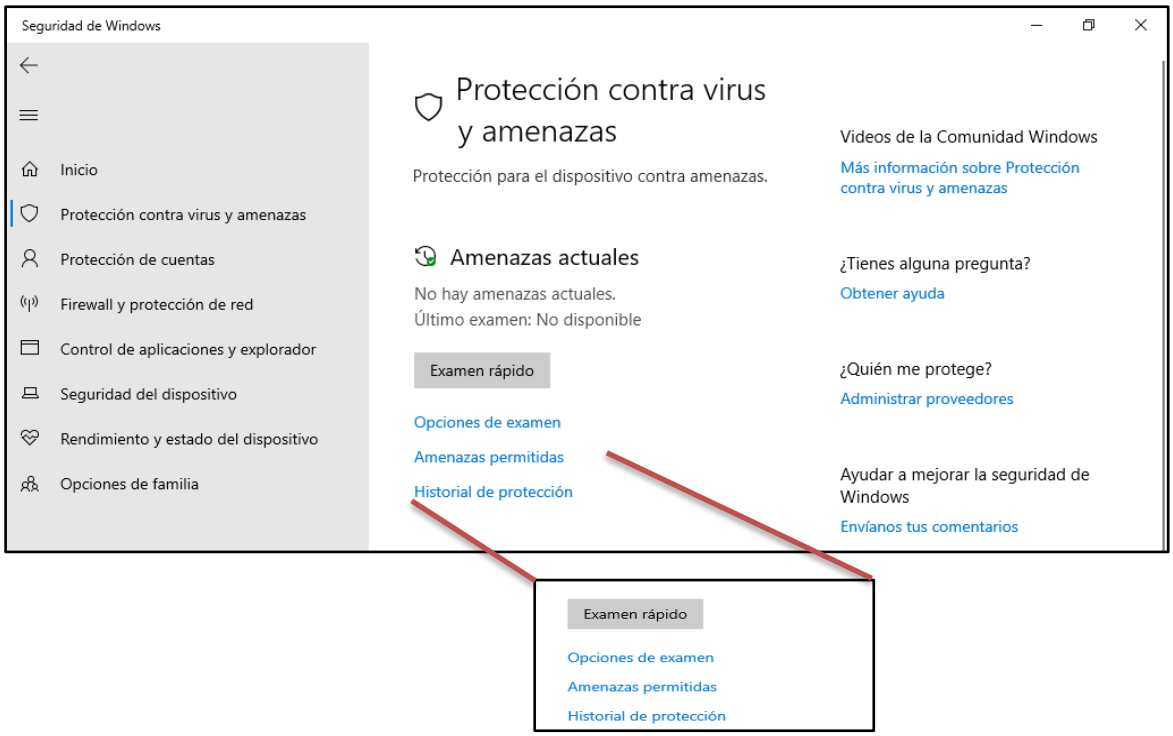

Figura A.7 Examen rápido del sistema de archivos Windows

En el apartado de Opciones de examen se encuentran tipos de exámenes, el examen completo revisa todos los archivos almacenados, que puede tomar más tiempo en el análisis, resulta más completo y efectivo en el proceso de detección de posibles amenazas (Figura A.8).

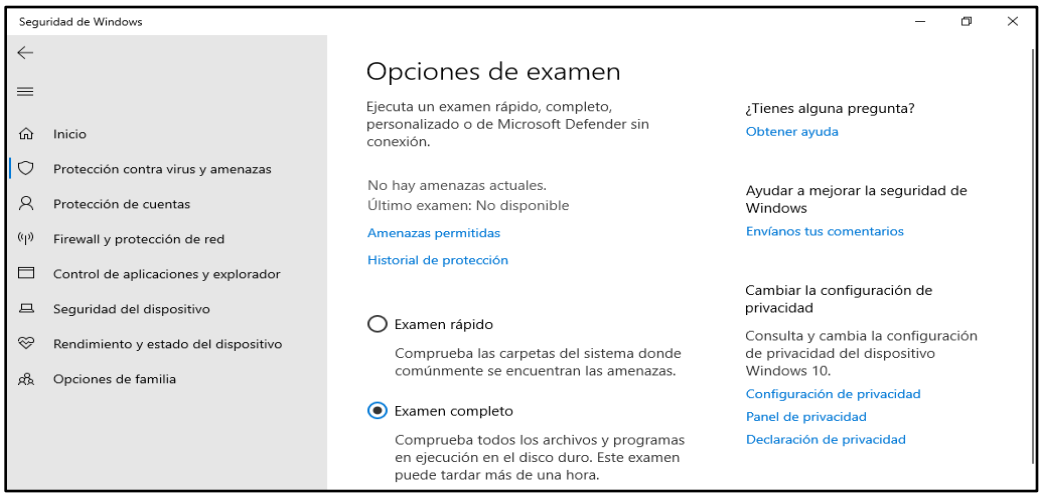

Figura A.8 Examen completo del sistema de archivos en Windows

Protección complementaria (antivirus).

Los antivirus son programas que detectan y eliminan aquellos programas maliciosos que pueden atentar contra el equipo y/o la información. Para explicar el procedimiento de protección mediante Antivirus, se usa como referencia *Avira*, el cual pertenece a la lista de *software* UNAM, avalado y recomendado por DGTIC (Dirección General de Cómputo y de Tecnologías de Información y Comunicación) de la UNAM.

La descarga de *Avira* será la versión compatible al que tiene *Windows* 10, únicamente hay que dar en el clic en la opción *Descargar gratis*, ejecutar o instalar el archivo en el sistema y otorgar permisos necesarios al realizar la configuración de protección basada en este antivirus (Figura A.9).

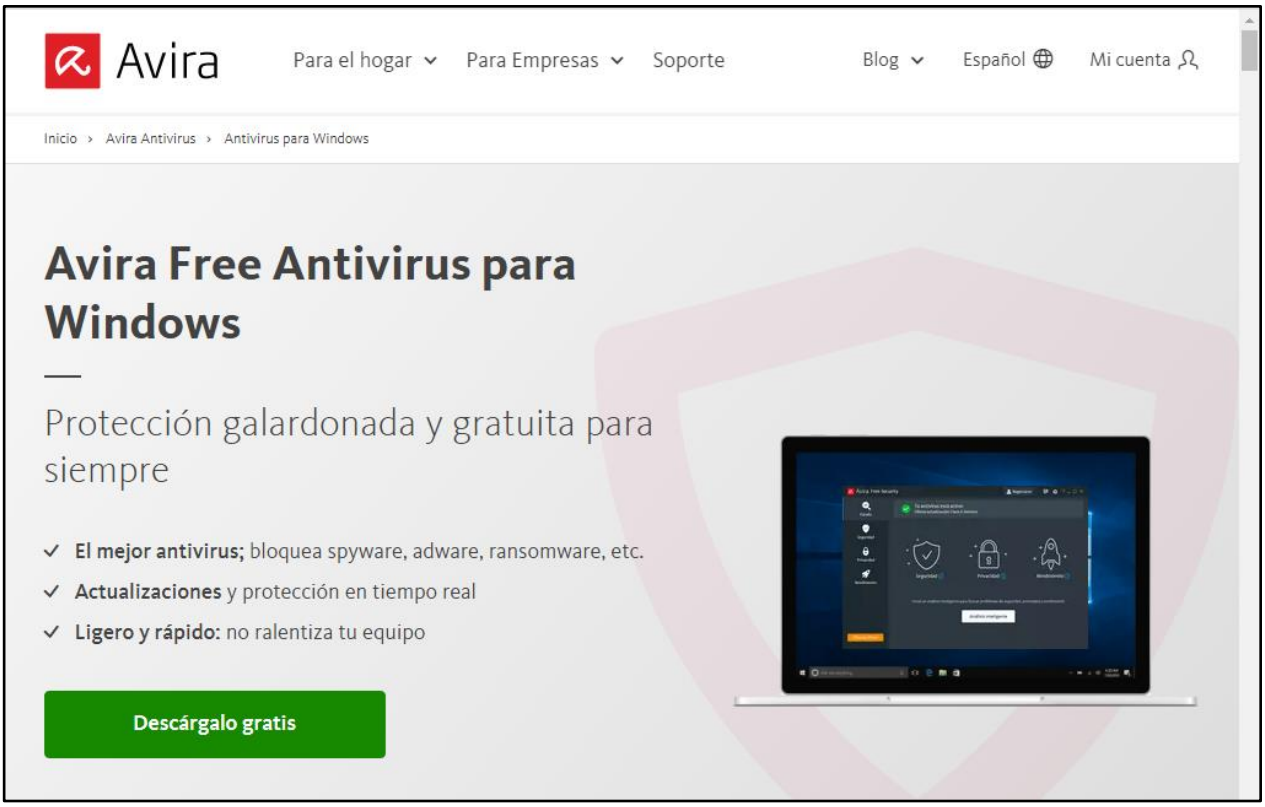

Figura A.9 Página *web* Antivírus *Avira*

Programación de exámenes periódicos automáticos

El programador de tareas es un programa de *Windows* que permite ejecutar funciones específicas de algunos programas, en este caso lo utilizaremos para programar un escaneo en busca de amenazas sobre lo que ofrece la seguridad en *Windows Defender.*

En el panel izquierdo, seleccionar la flecha (>) junto a la Biblioteca del programador de tareas para expandir, aplica lo mismo en la sección *Microsoft* > *Windows* y posterior, se desplegará la opción *Windows Defender* (Figura A. 10).

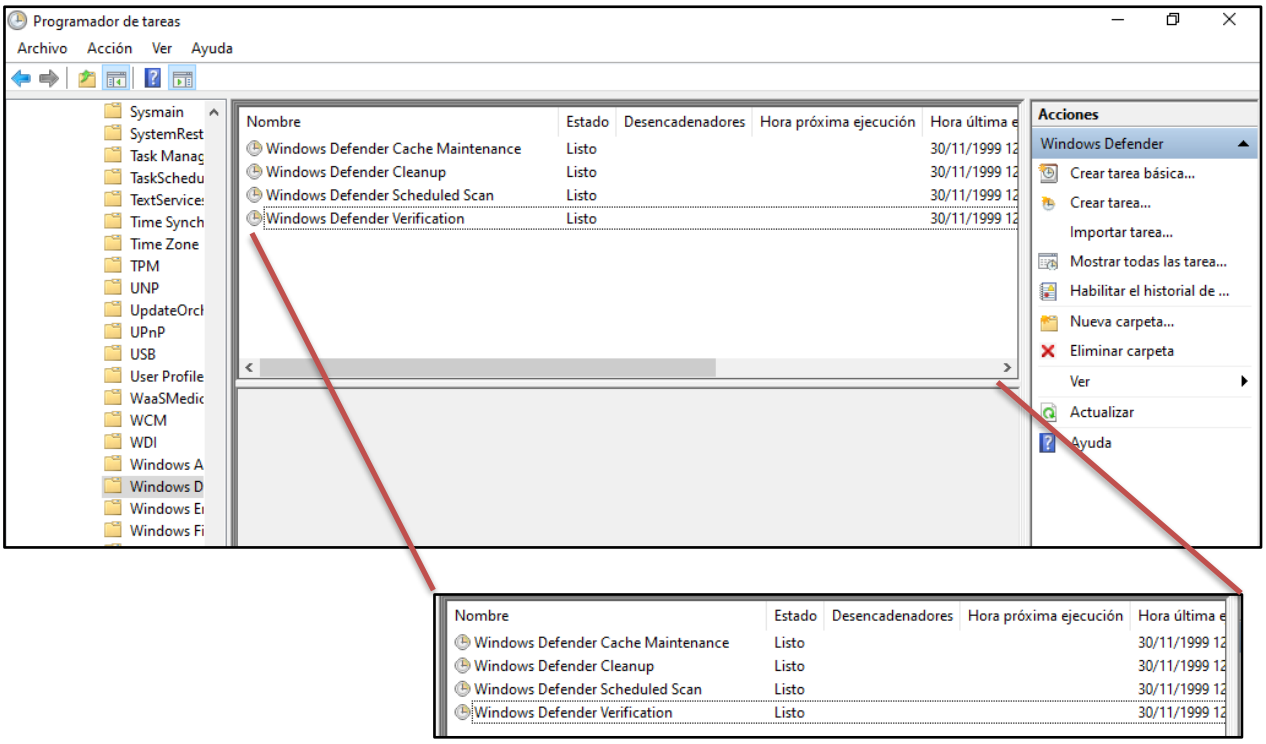

Figura A.10 En el programador de tareas en el módulo *Windows Defender*

De acuerdo con el uso del equipo *Windows*, es decir, ante múltiples de procesos con dispositivos externos o alto uso de sitios de internet, se recomienda realizar un escaneo periódico en busca de vulnerabilidades y amenazas en *Windows Defender*, el menos una vez al mes, estos periodos de análisis de amenazas se recomiendan dejar como una tarea programada en todos los procesos que comienzan con *Windows Defender.*

Cada módulo de Windows Defender se deberá configurar como tarea programada como la imagen A.11, en el submenú derecho, dar clic en Propiedades.

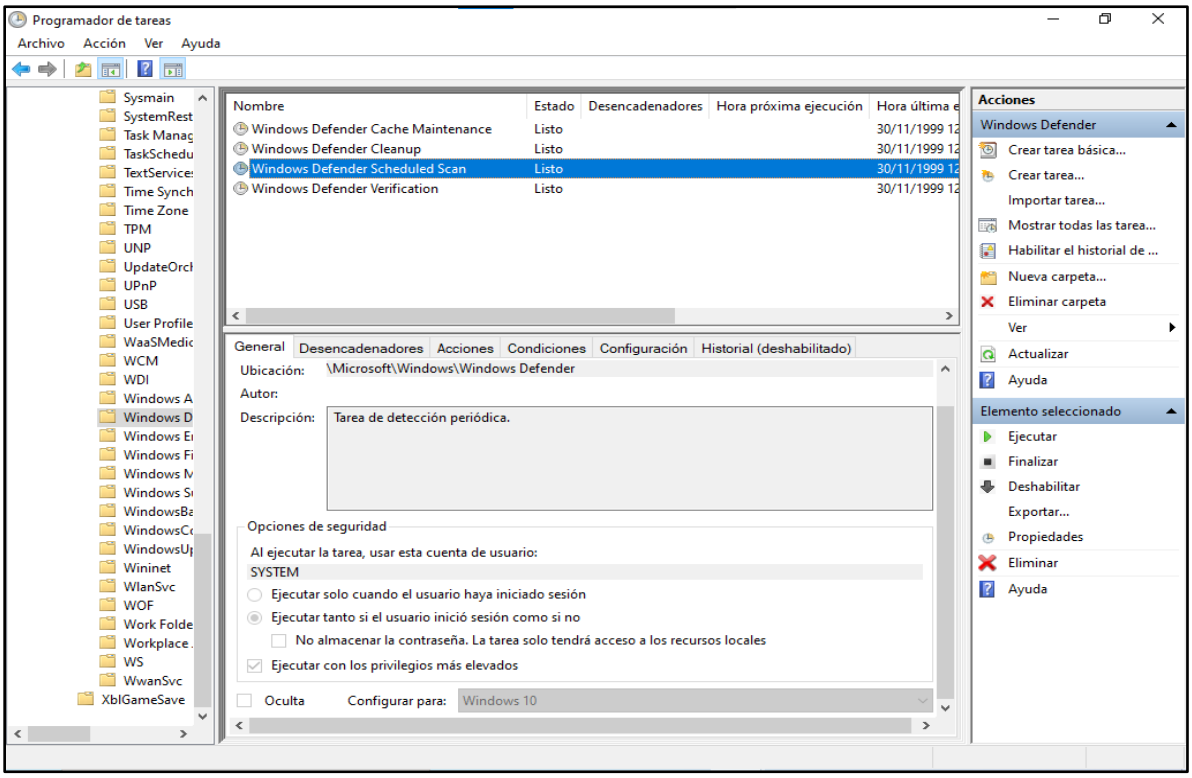

Figura A.11 Configurar el Programación de tareas sobre módulos de *Windows Defender*

En las Propiedades, en la ventana *Nuevo desencadenador*, se selecciona la opción iniciar la tarea “Según la programación” y se configura conforme se requiere que se realice el evento, mes, día y hora, además la opción Habilitar tarea (Figura A.12).

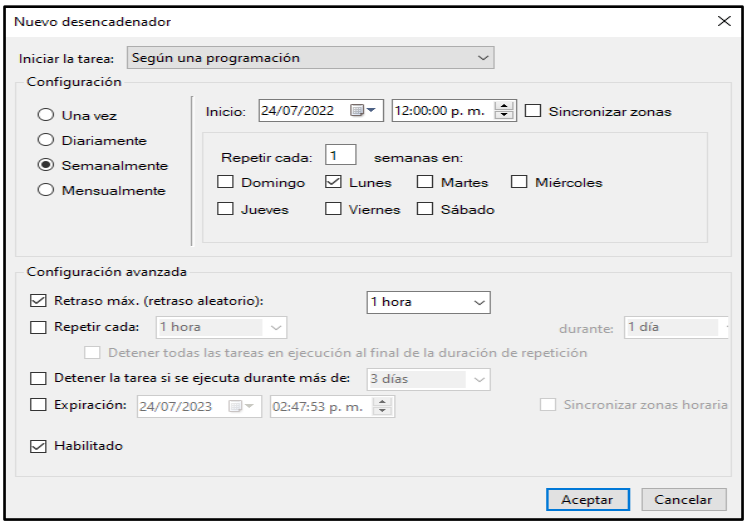

Figura A.12 Configurar Propiedades de tareas

Módulo de Windows Update

En la opción “Buscar actualizaciones”, realizará una búsqueda a través de la conexión de internet con dicho módulo para buscar las últimas actualizaciones sobre *Windows* que el fabricante *Microsoft* ha actualizado para protección de vulnerabilidades a nivel sistema operativo (Figura A.13).

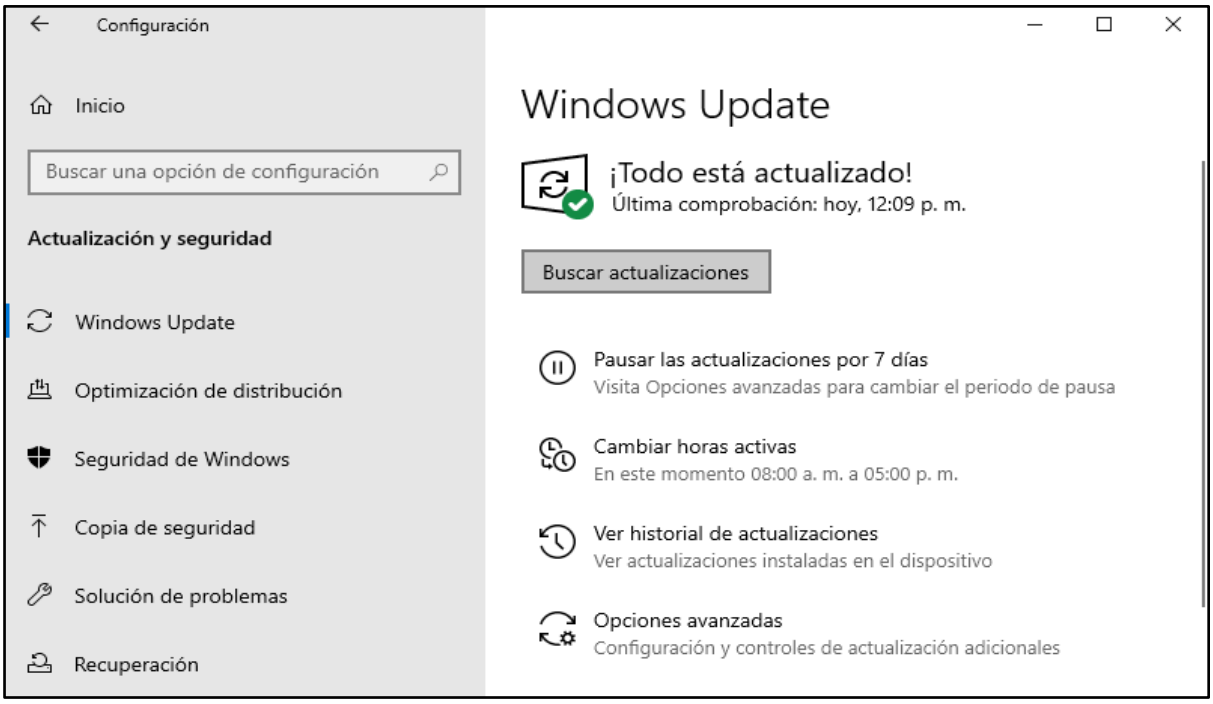

Figura A.13 Versión del sistema operativo actualizado

Nota. Este anexo incluyó acciones con los mecanismos de seguridad aplicados a *Windows* cuyas versiones 8, 8,1, 10 y 11 que pertenecen a *Windows Defender, Windows Update* y otras herramientas de *software* que pueden ser implementadas para la protección de amenazas, vulnerabilidades de nuestro dispositivo y nuestra información sobre sistemas operativos anunciados.