9 Seguridad

9.1. Introducción

Cuando hablamos de seguridad en un sistema informático, nos referimos a las tareas necesarias que debemos llevar a cabo para asegurarnos de que los componentes y recursos del equipo se ejecutan y utilizan del modo establecido. Asimismo, seguridad significa que solo las personas autorizadas tengan acceso a los datos incluidos en el sistema y la modificación de los mismos.

Windows 10 presenta numerosas herramientas para mantener nuestro equipo lo más resguardado posible ante amenazas externas y proteger nuestra privacidad. Es por ello que, en este capítulo analizaremos todas las utilidades que nos ofrece Windows 10 Anniversary Update para tratar y paliar en la medida de lo posible todas estas amenazas. Incluimos aquí un elemento que ha mejorado considerablemente en esta nueva versión: Windows Defender. En las siguientes secciones enumeramos otras utilidades que incluye Windows para mantener el equipo seguro. Todas ellas están habilitadas de forma predeterminada, aunque en algunas ocasiones es necesario hacer un seguimiento más detallado para asegurarnos de que todo funciona correctamente.

9.2. Seguridad y mantenimiento

La seguridad en Windows 10 Anniversary Update se gestiona a través de las opciones de Seguridad y mantenimiento que envían las notificaciones necesarias (dependiendo de su configuración) al Centro de actividades. Recuerde que puede

abrirlo haciendo clic en el icono de notificaciones ( ) de la barra de accesos. También encontrará diversas opciones de seguridad y mantenimiento en el nuevo panel Configuración que puede ver en la figura 9.1. En el capítulo cambiaremos del Panel de Control a este panel Configuración dependiendo de la tarea que necesitemos ejecutar.

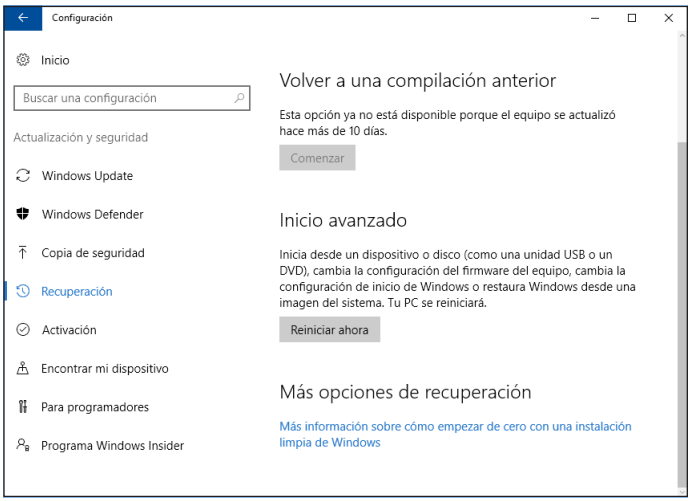

Figura 9.1. Opciones de seguridad en Configuración.

> ***Nota:*** *Recuerde que la forma más fácil de acceder al* Panel de control *es haciendo clic con el botón derecho del ratón sobre* **Inicio** *y seleccionando dicha opción desde el menú contextual.*

Siguiendo la línea que presenta el resto de herramientas de gestión y control del sistema, Seguridad y mantenimiento se encuentra en una ubicación centralizada dentro de Panel de control>Sistema y seguridad>Seguridad y mantenimiento, para controlar las actividades relacionadas con los dos aspectos más importantes para que el equipo se comporte de la forma deseada: la seguridad y el mantenimiento. Como puede ver en la figura 9.2, la ventana está dividida en estas dos categorías, Seguridad y Mantenimiento, las cuales contienen información relativa al estado de distintas utilidades:

- **Seguridad:** Es la primera utilidad disponible. Incluye información y, en ocasiones, acceso a distintas utilidades de seguridad, que pueden variar dependiendo de las

protecciones establecidas en su equipo, además de un vínculo de ayuda para saber la configuración de seguridad más adecuada para su equipo. Estas son las opciones que ofrece al hacer clic en su flecha desplegable:

- Firewall de red.
- Protección antivirus.
- Protección contra spyware y software no deseado.
- Configuración de seguridad de Internet.
- Control de cuentas de usuario.
- Windows SmartScreen.

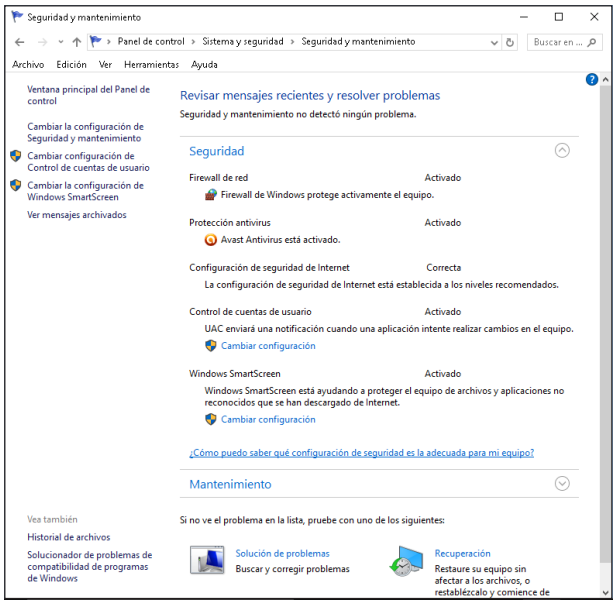

Figura 9.2. Seguridad y mantenimiento en Panel de control.

- **Mantenimiento:** La segunda utilidad incluye información y, en ocasiones, accesos a diversas herramientas de mantenimiento y estas son las opciones que ofrece en su menú de flecha desplegable:
  - **Buscar soluciones para problemas notificados**, que incluye dos enlaces: Buscar soluciones y Ver historial de confiabilidad.
  - **Mantenimiento automático** incluye dos enlaces: Iniciar mantenimiento y Cambiar la configuración de mantenimiento.

- **Grupo Hogar**, con un enlace para Unirse ahora en caso de que se haya configurado uno.
- **Historial de archivos**, con enlaces a Cambiar configuración, Restaurar archivos personales y Ejecutar ahora.
- **Estado de la unidad**, que incluirá los mensajes correspondientes a problemas detectados en el sistema.

A continuación vamos a analizar cada una de las categorías y los elementos que nos ofrecen para ayudarnos a mantener nuestro sistema más seguro.

9.2.1. Seguridad

En la primera categoría de la ventana y es donde se agrupan todos los elementos relacionados con la protección del sistema ante amenazas externas. Más concretamente, administra la configuración del Firewall de Windows, de Windows SmartScreen, del software antivirus y anti spyware, del control de cuentas del usuario, de la cuenta de Microsoft y de la seguridad de Internet.

Si hace clic sobre el botón de flecha desplegable que se muestra al final de la categoría Seguridad, se visualizarán todos los elementos que están agrupados dentro de ella. Ocurre lo mismo al ejecutar la misma acción en la categoría Mantenimiento. Puede replegar ambas categorías haciendo clic de nuevo sobre las flechas.

Firewall de red

La misión de un firewall de red es impedir accesos malintencionados a nuestro equipo desde Internet o de cualquier otra red, por parte de hackers o software malintencionado. Asimismo, un firewall permite controlar el tráfico de redes domésticas, públicas y de trabajo, realizando un seguimiento completamente independiente entre una y otra ubicación, en función de la configuración de red que hayamos definido. El firewall de red debe estar activado y su funcionamiento debe ser correcto. En caso contrario, debemos configurarlo. Existen dos pantallas de configuración: una sencilla y una más avanzada. Para acceder a la pantalla de configuración del Firewall de Windows más sencilla, abra el Panel de control y seleccione Sistema y seguridad>Firewall de Windows. Se abrirá la ventana principal del Firewall de Windows que se muestra en la figura 9.3.

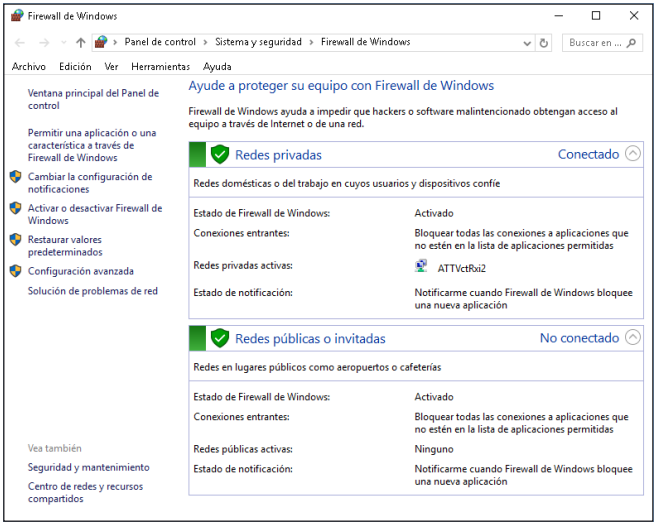

Figura 9.3. Configuración del Firewall de Windows.

En la figura se muestra el estado de configuración de las notificaciones asociadas a las redes que posee el equipo. Una de las ventajas del Firewall de Windows es la posibilidad de configurar niveles de seguridad diferentes según la ubicación de red. En este caso, el firewall está activado para redes privadas, públicas o invitadas, aunque ahora mismo el equipo solo está conectado a una red privada. Desde esta pantalla podremos realizar diversas tareas de configuración:

- **Personalizar configuración del Firewall de Windows:** Es posible establecer qué clase de notificaciones queremos que se visualicen con el Firewall de Windows. Para ello, seleccione la opción Cambiar la configuración de notificaciones situada en el panel izquierdo de la ventana Firewall de Windows y se abrirá la pantalla que se muestra en la figura 9.4.
  En esta pantalla de personalización para cada tipo de red, puede dejar activado el Firewall de Windows, pero a su vez bloquear cualquier intento de conexión desde el exterior. Para ello, seleccione Bloquear todas las conexiones entrantes, incluidas las de la lista de aplicaciones permitidas dentro de las opciones Configuración de red privada y Configuración de red pública Si, además, desea recibir una notificación cada vez que el Firewall de

Windows bloquea un nuevo programa o acceso, marque Notificarme cuando Firewall de Windows bloquee una nueva aplicación.
También podemos desactivar el Firewall de Windows desde esta ubicación. Solo tiene que activar la opción Desactivar Firewall de Windows (no recomendado) y hacer clic en el botón **Aceptar**.

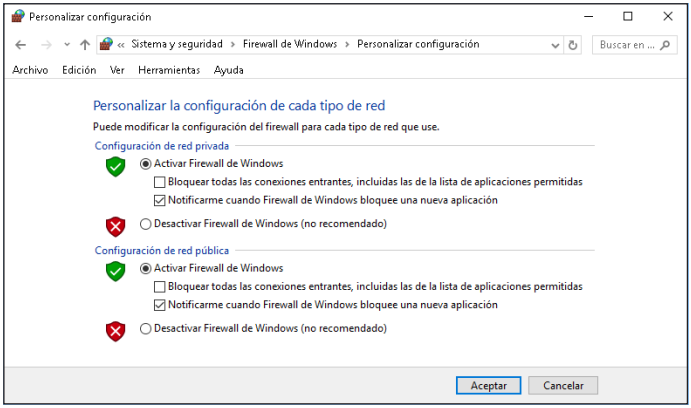

Figura 9.4. Personalizar la configuración del Firewall de Windows.

Advertencia: *Nos es recomendable desactivar el Firewall de Windows, a menos que tenga otro firewall de red instalado en el equipo y desee utilizarlo.*

- **Aplicaciones permitidas:** En ocasiones, necesitamos permitir la conexión de determinadas aplicaciones al equipo y nos gustaría que dicha tarea fuera posible sin tener que desactivar el firewall de red. Por ese motivo, Firewall de Windows nos permite autorizar a determinadas aplicaciones acceder al equipo. Para ello, seleccione la opción Permitir una aplicación o una característica a través de Firewall de Windows del panel izquierdo de la ventana y se abrirá la ventana Aplicaciones permitidas que se muestra en la figura 9.5.

Truco: *Puede acceder a diversas opciones de configuración del Firewall de Windows escribiendo* **firewall** *en el cuadro de búsqueda y seleccionando una de las opciones mostradas en la lista de resultados.*

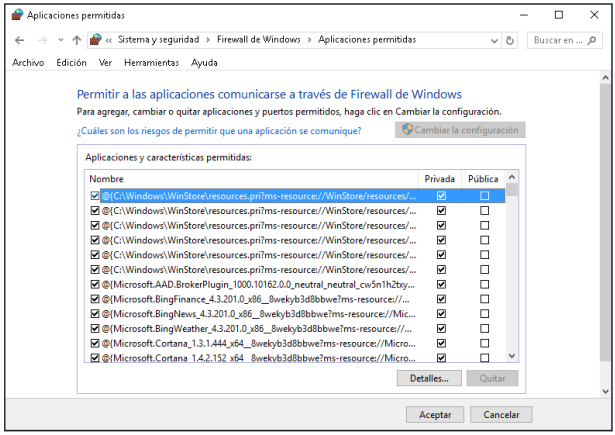

Figura 9.5. Aplicaciones permitidas en el Firewall de Windows.

- **Restaurar valores predeterminados:** Al hacer clic en esta opción del panel izquierdo, podrá restablecer los valores de configuración a su estado original haciendo clic en el botón **Restaurar valores predeterminados** que ofrece la ventana que se abre al hacer clic en el vínculo del mismo nombre.
- **Configuración avanzada:** Seleccione la opción Configuración avanzada para acceder a la consola de Firewall de Windows con seguridad avanzada que se muestra en la figura 9.6, desde donde podrá establecer diferentes reglas de seguridad.
  Desde este panel, podrá establecer directivas para las aplicaciones y programas de entrada y salida y una serie de reglas para personalizar la configuración del firewall. En el panel izquierdo, verá las distintas reglas de entrada, salida y de supervisión con solo hacer clic. Si selecciona la raíz de la consola, tal como muestra la figura anterior, podrá ver en el panel central una serie de utilidades. La primera, Información general, incluye información sobre los perfiles establecidos. Para cambiar cualquiera de estas opciones, haga clic en el enlace Propiedades de Firewall de Windows y establezca la configuración deseada desde el cuadro de diálogo que se abre utilizando cualquiera de los elementos incluidos en sus cuatro fichas: Perfil de dominio, Perfil privado, Perfil público, Configuración IPsec. La segunda, Introducción, incluye una serie de enlaces para crear reglas de seguridad de una conexión,

reglas de entrada para permitir o bloquear conexiones a programas o puertos específicos o supervisar la directiva y actividad del firewall e IPsec actuales. Para ello, haga clic en el enlace correspondiente: Reglas de seguridad de conexión, Reglas de entrada, Reglas de salida y Supervisión. Todos estos enlaces los puede encontrar también en el panel de navegación izquierdo si extiende todos los menús principales. Haga clic en las distintas opciones que le ofrece el cuadro de diálogo para abrir los distintos elementos y configurar la seguridad de acceso de programas a su gusto.

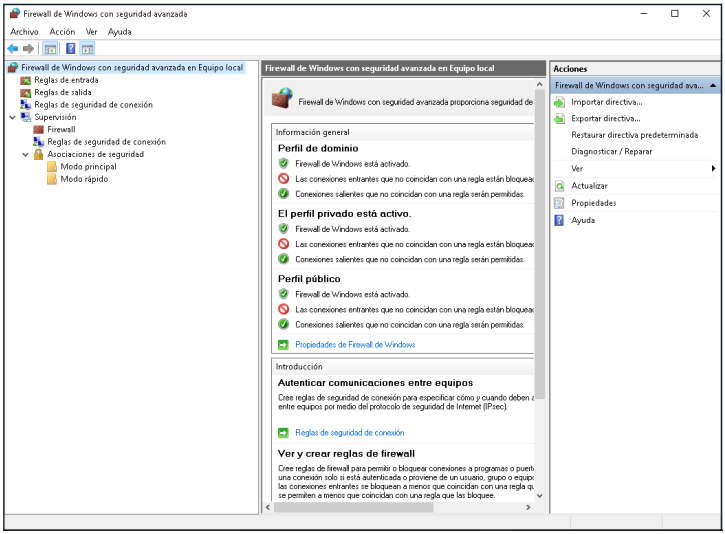

Figura 9.6. Configuración avanzada del Firewall de Windows.

- **Solución de problemas de red:** Al hacer clic en esta opción del panel izquierdo del Firewall de Windows, se abrirá la ventana mostrada en la figura 9.7. Desde este solucionador podrá buscar y corregir problemas de redes e internet, así como de su impresora local haciendo clic en el enlace correspondiente y siguiendo las instrucciones del asistente.

Cambiar la configuración de Seguridad y mantenimiento

Este es uno de los enlaces que se encuentran en el panel izquierdo de Seguridad y mantenimiento. Al hacer clic en él se abre la ventana mostrada en la figura 9.8.

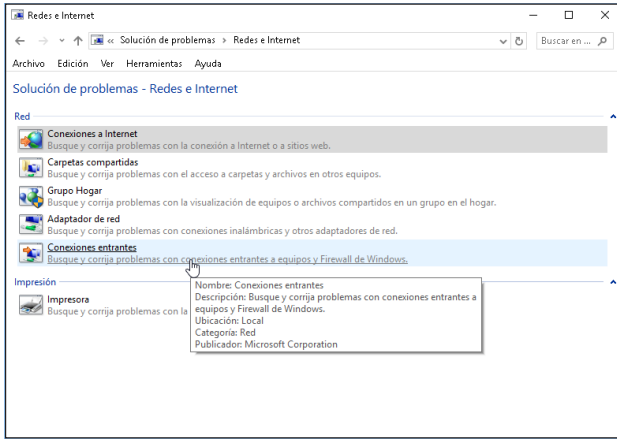

Figura 9.7. Solucionador de problemas de redes.

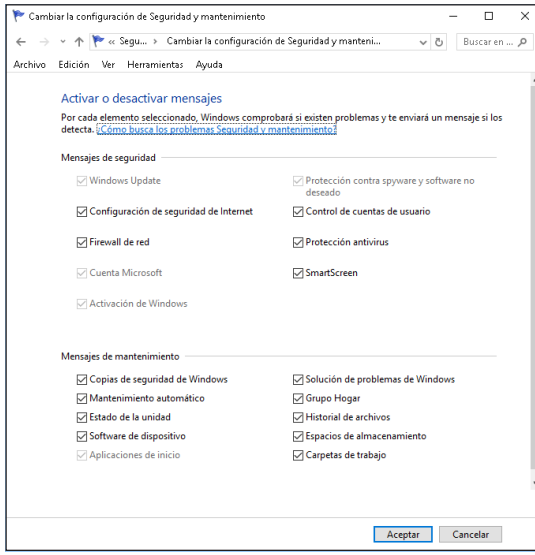

Figura 9.8. Mensajes de seguridad y mantenimiento.

Como puede ver, aquí es donde se configuran los mensajes de seguridad. Estos mensajes se dividen en dos grupos: Mensajes de seguridad y Mensajes de mantenimiento. Para activar o desactivar la aparición de mensajes de este tipo dentro de su sistema, simplemente seleccione o anule la opción de la casilla correspondiente.

Control de cuentas de usuario

Control de cuentas de usuario (UAC) es una utilidad que nos permite controlar nuestro equipo de forma que nos informe con un mensaje cuando un programa lleva a cabo una modificación que requiere permisos de administrador. Podemos establecer automáticamente el nivel de permisos de nuestra cuenta de usuario, ya que UAC ajusta dicho nivel en función de las tareas que lleva a cabo en el equipo. Puede acceder a y cambiar la configuración del UAC haciendo clic en Cambiar configuración dentro del panel de Seguridad y Mantenimiento, para abrir el cuadro de configuración de las cuentas de usuario que puede ver en la figura 9.9.

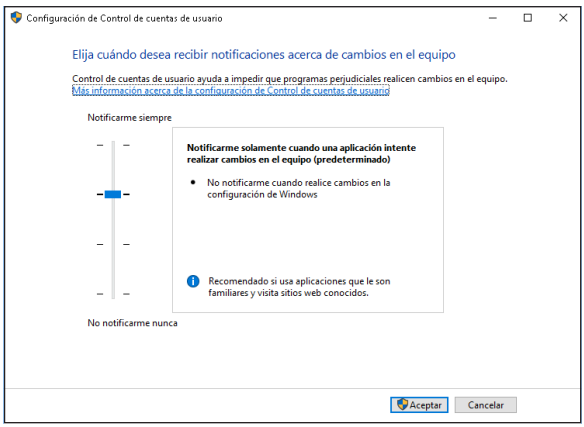

Figura 9.9. Configuración de Control de cuentas de usuario.

En otro capítulo del libro hablamos con detalle sobre las cuentas, pero aquí queremos resaltar que existen cuatro tipos diferentes de cuadros de notificación UAC, los cuales se detallan a continuación, y que se pueden establecer simplemente deslizando la barra deslizadora de esta ventana entre los valores Notificarme siempre y No notificarme nunca:

- **Notificarme siempre cuando:** Le avisa cuando las aplicaciones intentan instalar software o hacer cambios en el equipo, o cuando realiza cambios en la configuración de Windows.
- **Notificarme solamente cuando una aplicación intente realizar cambios en el equipo (predeterminado):** Esta es la configuración predeterminada y solo recibirá notificaciones cuando realice cambios de configuración.

- **Notificarme solo cuando una aplicación intente realizar cambios en el equipo (no atenuar el escritorio):** No recibirá notificaciones cuando realice cambios en la configuración de Windows.
- **No notificarme nunca cuando:** Las aplicaciones intenten instalar software o hacer cambios en el equipo ni cuando se realicen cambios en la configuración de Windows. Esta opción no se recomienda.

Windows SmartScreen

Esta función le ayuda a proteger el equipo de archivos y aplicaciones no reconocidos descargados desde Internet al enviar un mensaje informándole antes de ejecutar archivos o aplicaciones desconocidos. Haga clic en Cambiar configuración en la sección Windows SmartScreen de Seguridad y mantenimiento para abrir la ventana mostrada en la figura 9.10.

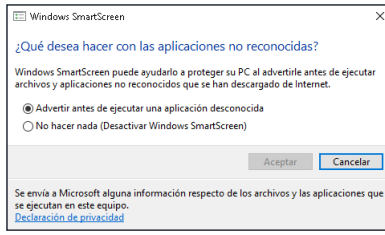

Figura 9. 10. Configuración de Windows SmartScreen.

9.2.2. Mantenimiento

La segunda categoría de Seguridad y mantenimiento agrupa una serie de elementos que ayudan a mantener el equipo en buenas condiciones:

- **Buscar soluciones para los problemas notificados:** Cuando se produce un problema en Windows y el equipo envía un mensaje sobre el problema de software o hardware, esta información se almacena en el Monitor de confiabilidad (véase la figura 9.11).
  El Monitor de confiabilidad le resultará muy útil para saber cuáles son los problemas de hardware y de software del equipo ya que evalúa la estabilidad del sistema en una escala que oscila del 1 (menos estable) al 10 (más estable). Además, puede seleccionar un periodo determinado para revisar problemas específicos en

ese tiempo. Cualquier cambio realizado en el equipo o cualquier problema producido afectará a este índice de estabilidad.

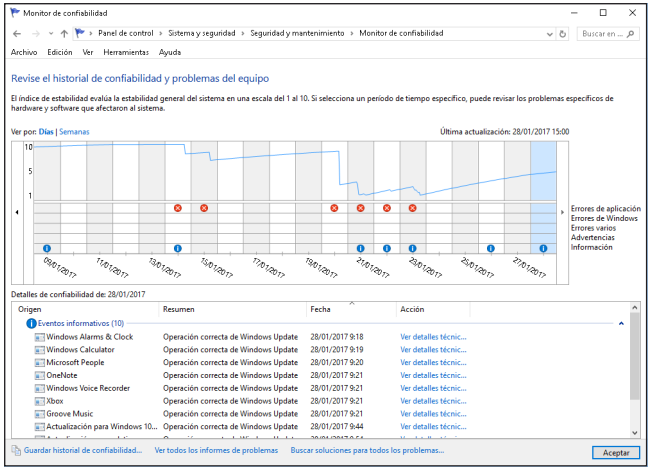

Figura 9. 11. Monitor de confiabilidad.

Para abrirlo, haga clic en el enlace Ver historial de confiabilidad dentro de en Buscar soluciones para los problemas notificados. Este monitor se divide en dos partes: la parte superior presenta de manera gráfica todos los eventos detectados y ordenados según las siguientes categorías: Errores de aplicación, Errores de Windows, Errores varios, Advertencias e Información. En la parte inferior puede ver una tabla de datos ordenada según distintas columnas. Ambas partes están relacionadas ya que, al hacer clic en un elemento del gráfico, podrá ver sus eventos en la parte superior. Desde esta utilidad, podrá realizar principalmente las siguientes tareas:

- Ver los detalles de cualquier evento en la parte inferior del gráfico haciendo clic sobre un determinado elemento en el informe gráfico.
- Ver el índice de estabilidad en un tiempo determinado haciendo clic en Días o Semanas.
- Ver más información sobre un evento haciendo clic en Ver detalles técnicos dentro de la columna Acción.
- Encontrar una solución al problema detectado haciendo clic en Buscar una solución en la columna Acción.

- Guardar un historial con los datos ofrecidos, dentro del enlace Guardar historial de confiabilidad, que abre un cuadro de diálogo para exportar el informe en la ubicación que elija del sistema. Solamente tiene que elegir el lugar donde quiere guardarlo y hacer clic en **Guardar** cuando haya terminado.
- Ver informes de problemas haciendo clic en Ver todos los informes de problemas, que abre la ventana mostrada en la figura 9.12. Esta ventana muestra los informes de problemas desde donde puede buscar una solución, eliminar el informe, ver los detalles técnicos o incluso agrupar el informe por Origen, Resumen, Fecha, Estado o Desagrupar, que le facilitan la presentación de problemas en la pantalla. El botón **Borrar todos los informes de problemas** que se encuentra en la esquina inferior derecha de la pantalla, hace precisamente eso: borra todos los eventos mostrados en el informe.

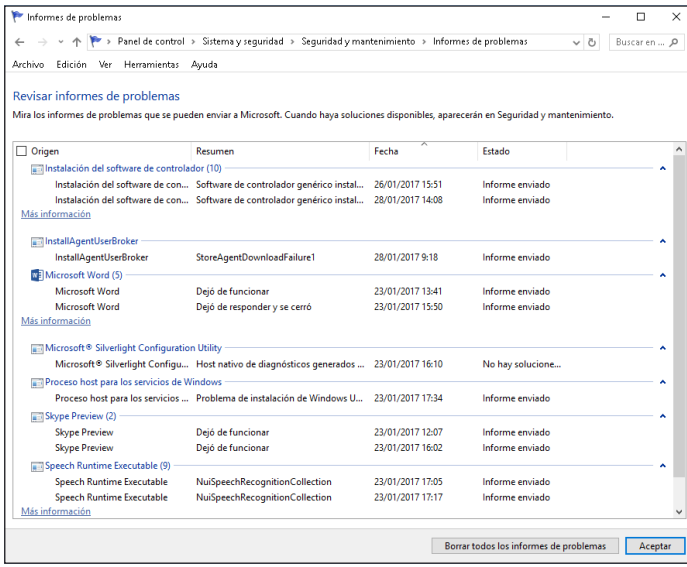

Figura 9. 12. Informes de problemas.

- Puede buscar soluciones para todos los problemas de su equipo haciendo clic en Buscar soluciones para todos los problemas. Se abrirá un asistente

para ayudarle a encontrar soluciones a todos los problemas detectados en el equipo y si no existe ninguna solución, el asistente enviará un mensaje indicándolo.

Nota: *Si no existen soluciones a un problema, aparecerán en* Seguridad y mantenimiento *cuando estén disponibles.*

- **Mantenimiento automático:** Windows programa automáticamente la ejecución de actividades de mantenimiento. Para cambiar esta configuración, tiene que entrar en la opción correspondiente haciendo clic en Cambiar la configuración de mantenimiento (véase la figura 9.13).

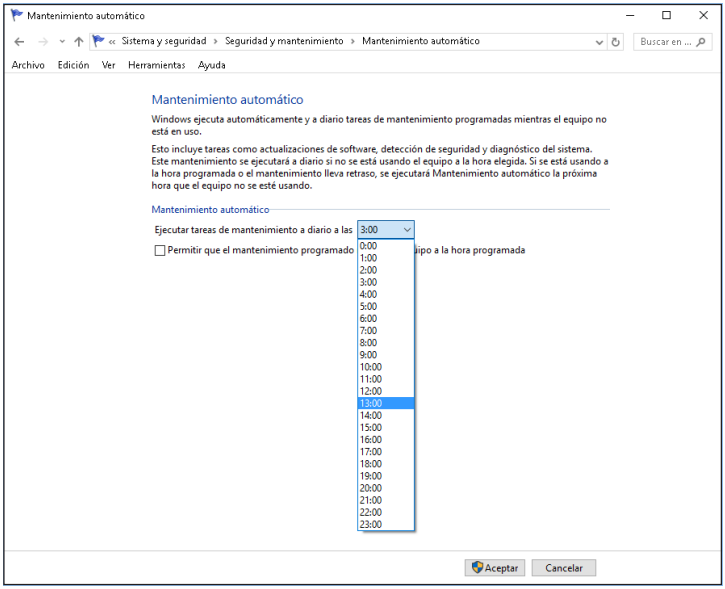

Figura 9. 13. Mantenimiento automático.

Para cambiar la hora en que se ejecutan las tareas y permitir que se reactive el equipo a la hora especificada, seleccione primero una hora desde el menú desplegable de Ejecutar tareas de mantenimiento a diario a las y después, seleccione la casilla Permitir que el mantenimiento programado reactive el equipo a la hora programada. Las tareas de mantenimiento consisten principalmente en realizar actualizaciones de software, detectar problemas

de seguridad, y diagnosticar el sistema. El mantenimiento se realiza automáticamente a la hora que elija. Iniciar mantenimiento empieza a realizar las tareas de mantenimiento y cambia por Detener mantenimiento tras hacer clic en el enlace.

Desde este apartado de tareas de mantenimiento también podremos crear un grupo en el hogar, haciendo clic en el enlace correspondiente, y cuya utilidad trataremos con más detalle en el capítulo dedicado a las redes. También presentada en el capítulo sobre configuración, la opción Historial de archivos nos permite activar y desactivar directamente el historial de nuestros archivos y conocer en qué estado se encuentra.

Las opciones Estado de la unidad y Software de dispositivo nos permiten saber si tenemos que ejecutar alguna acción con respecto a nuestra unidad o el software de nuestro equipo.

En caso contrario, mostrarán mensajes indicando que todo funciona correctamente y que no se requiere ejecutar ninguna acción.

9.3. Windows Defender

Se trata de una aplicación, mejorada en esta nueva versión de sistema operativo, que nos ayuda a evitar el acceso de cualquier tipo de software malware (o malintencionado) al equipo. Estas aplicaciones se conocen comúnmente como software antimalware y, como su nombre indica, tienen la misión de eliminar o evitar la instalación de software malware en el equipo. Un ordenador está continuamente expuesto a amenazas de malware y más aún si está conectado a Internet, algo más que probable. El malware puede llegar a nuestro equipo a través de diversos medios: medios extraíbles, unidades USB, CD o DVD, un mensaje de correo electrónico y especialmente desde Internet, lugar donde se aglomeran incontables aplicaciones con fines de dudosas intenciones (y no tan dudosas). Es por ello que Windows incluye Windows Defender dentro de sus opciones de seguridad. Para abrir su panel de configuración, haga clic en el icono ( ) de la barra de tareas. Se abrirá la ventana mostrada en la figura 9.14.

El panel de configuración de Windows Defender nos ofrece primero distintas opciones de protección que podemos activar o desactivar, así como exclusiones e información sobre su

estado. Desde este panel también podremos acceder a la configuración y ejecución de análisis a través del enlace final del panel y que pasaremos a detallar enseguida.

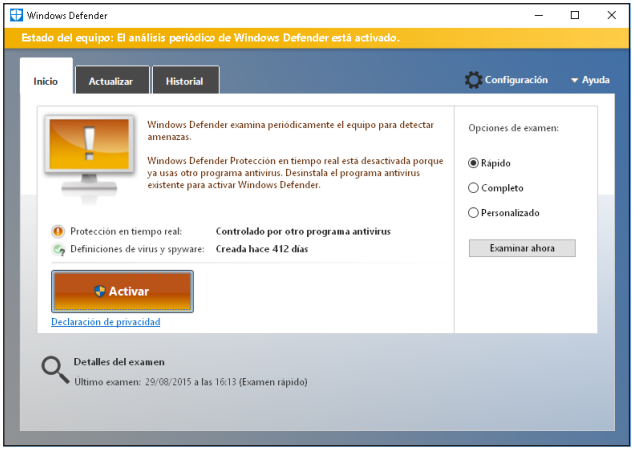

Figura 9.14. Página inicial de Windows Defender.

9.3.1. Modos de protección

Desde el panel de configuración de Windows Defender que podemos abrir desde su página inicial al hacer clic en **Configuración** (esquina superior derecha de la ventana) podremos activar o desactivar las siguientes opciones de protección (véase la figura 9.15):

- **Abrir Windows Defender:** Abre la página inicial de Windows Defender.
- **Examen periódico limitado:** Al activar esta utilidad, el equipo será revisado por Windows Defender de manera periódica para buscar amenazas. Tenga en cuenta que para ver esta opción en el panel de configuración de Windows es necesario tener instalado un antivirus de terceros. En caso contrario, no aparecerá en la ventana.
- **Protección en tiempo real:** Esta utilidad nos ayuda a encontrar malware y a evitar que se instale o se ejecute en nuestro equipo ya que Windows Defender nos avisará cuando haya un intento de instalación o ejecución de spyware o incluso una modificación en algún elemento de configuración de Windows. La utilidad aparecerá

desactivada si tenemos instalado en el equipo un antivirus de terceros ya que será este el que se ocupe de dicha protección.

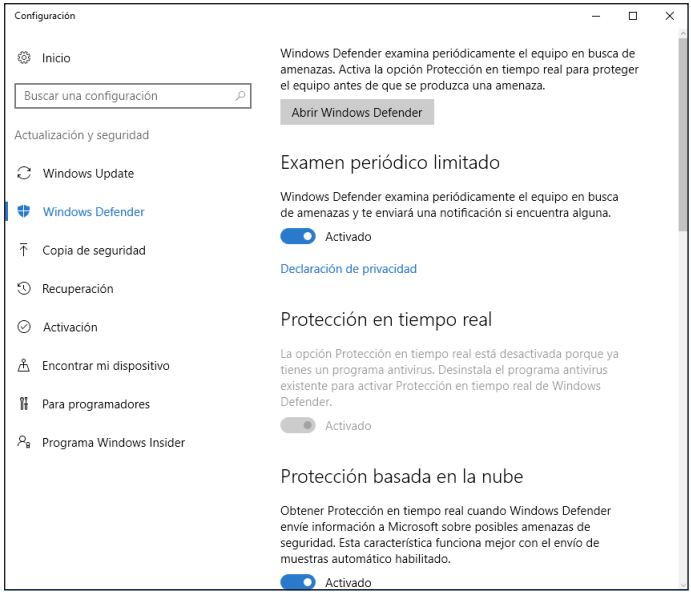

Figura 9.15. Configuración de Windows para Windows Defender.

- **Protección basada en la nube:** Esta utilidad le permite enviar a Microsoft información sobre los problemas de seguridad encontrados.
- **Envío de muestras automático:** Si activa esta opción, se enviará a Microsoft una muestra del malware para obtener información acerca de sus posibles problemas de seguridad y evitarlos a tiempo. Estas dos últimas opciones ayudan a mejorar Windows Defender a medida que se detectan posibles amenazas.
- **Exclusiones:** Puede agregar archivos para excluirlos del examen que ejecuta Windows Defender. Para ello basta con hacer clic en Agregar exclusión y seleccionar la exclusión de un archivo, una carpeta, un tipo de archivo o incluso un proceso. Al hacer clic en el botón correspondiente, se abrirá un cuadro de diálogo desde el que puede realizar su búsqueda.

- **Notificaciones mejoradas:** Al activar la utilidad, recibirá notificaciones que le ayudarán a ver cuál es el estado de su equipo. No obstante, si aparece algún problema que necesite atención inmediata, recibirá una notificación, aunque la utilidad esté desactivada.
- **Declaración de privacidad:** Este enlace abre dicha declaración en línea en el sitio Web de Microsoft.
- **Windows Defender Offline:** Una nueva opción que le puede ayudar a encontrar y eliminar software malintencionado haciendo clic en **Realizar el examen sin conexión**.
- **Información de versión:** Aquí se encuentra toda la información de las versiones del software antimalware.

9.3.2. Aplicación de escritorio de Windows Defender

Volviendo a la aplicación de escritorio de Windows Defender (haga clic en el icono de la barra de herramientas o en **Abrir Windows Defender** dentro del panel **Configuración**, verá que ofrece tres fichas desde donde podrá ejecutar las siguientes acciones.

> ***Nota:*** *También puede abrir el cuadro para usar Windows Defender escribiendo* **windows defender** *en el cuadro de búsqueda y seleccionando* Windows Defender Aplicación de escritorio *de la lista de resultados.*

- **Inicio:** En el panel derecho de esta ficha se encuentra el botón Examinar ahora, y opciones para realizar el examen manual: Rápido, Completo o Personalizado. Además, podrá ver información sobre la protección en tiempo real y si están actualizadas las definiciones y cuándo se realizó el último examen del equipo.
- **Actualizar:** Como puede ver en la figura 9.16, la ficha incluye la utilidad de **Actualizar definiciones**. La efectividad de esta opción depende en gran medida de lo actualizadas que estén sus definiciones (igual que ocurre con un antivirus). Las definiciones son bases de datos con las amenazas conocidas hasta una fecha determinada. Por ejemplo, si las definiciones de Windows Defender de un equipo, no se actualizan desde hace dos meses, significa que todo el software no deseado o spyware que

haya surgido en los últimos dos meses, no está registrado en las definiciones de la aplicación, convirtiendo a nuestro sistema en un blanco fácil para todo ese tipo de software reciente. La actualización de estas definiciones las ejecuta Windows Update automáticamente. Por eso es importante mantener activado Windows Update.

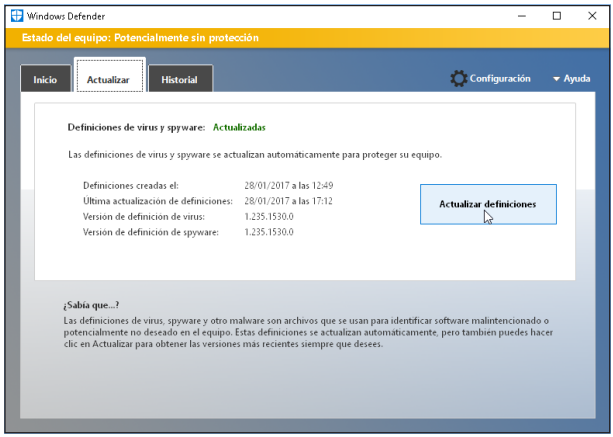

Figura 9.16. Actualizar en Windows Defender.

- **Historial:** En esta ficha podrá acceder al historial de Windows Defender:
  - **Elementos en cuarentena:** Cuando Windows Defender detecta una posible amenaza de spyware, nos ofrece varias posibilidades, entre las que se encuentra la de poner la aplicación en cuarentena. Esta acción impide la ejecución de la aplicación, pero la mantiene en el sistema por si posteriormente descubrimos que se trata de una falsa amenaza y decidimos utilizarla. Haciendo clic sobre esta opción se mostrarán todas las aplicaciones que tenemos en cuarentena.
  - **Elementos permitidos:** En esta lista se incluyen las aplicaciones que Windows Defender ha detectado como posibles amenazas pero que nosotros, como usuarios, hemos tomado la decisión de autorizar en nuestro equipo.
  - **Todos los elementos detectados:** Aquí se incluye una lista con todos los elementos detectados, tanto permitidos como en cuarentena.

Para configurar las opciones de Windows Defender, haga clic **Configuración**, en la esquina superior de la ventana. Se abrirá una ventana ofreciendo los siguientes elementos:

- **Protección en tiempo real:** Seleccionar esta opción para que Windows Defender realice exámenes rutinarios.
- **Archivos y ubicaciones excluidos:** Podrá indicarle a **Windows Defender** cuáles son los archivos y ubicaciones que quiere excluir del examen rutinario.
- **Tipo de archivos excluidos:** Puede escribir una lista de tipos de archivos que desea excluir.
- **Procesos excluidos:** Igual, pero para procesos.
- **Avanzada:** Seleccione o anule la selección de los elementos ofrecidos en esta opción.
- **MAPS:** Desde esta opción podrá elegir si usa o no Microsoft Active Protection Service (MAPS).
- **Administrador:** Desde esta opción podrá activar o desactivar Windows Defender.

9.4. Windows Update

Gracias a las actualizaciones automáticas de Windows ya no hace falta buscar actualizaciones en línea ni preocuparse por la existencia de posibles correcciones importantes para el sistema en el equipo. Windows Update es la opción que instalará automáticamente las actualizaciones importantes en cuanto estén disponibles. También es posible configurar Windows Update para que instale automáticamente las actualizaciones recomendadas o que solo nos avise de que están disponibles. Las actualizaciones opcionales, que incluyen actualizaciones para otros productos de Microsoft, no se instalan automáticamente. Windows Update no agregará aplicaciones al equipo sin pedir permiso ni eliminará nada que haya instalado. Para comprobar la configuración de Windows Update en su equipo, seleccione el vínculo con el mismo nombre que se encuentra en Inicio>Configuración>Windows Update.

Al hacer clic en **Buscar actualizaciones**, el sistema iniciará una búsqueda manual de actualizaciones y mostrará un mensaje indicando si hay alguna disponible o si el dispositivo está actualizado.

El enlace Historial de actualizaciones abre una ventana con una relación de todas las actualizaciones realizadas en el equipo (véase la figura 9.17) y un enlace debajo de cada una

de ellas para ver información más detallada en el sitio Web de Microsoft, además de las opciones disponibles Desinstalar las actualizaciones u Opciones de recuperación.

Dentro de Configuración de actualización podremos elegir entre tres enlaces: Cambiar horas activas, Opciones de reinicio y Opciones avanzadas. Los dos primeros enlaces le ayudan a modificar las horas de actividad del equipo y cambiar la forma de reinicio del equipo cada vez que se instale una actualización que así lo requiera. Al hace clic en el enlace Opciones avanzadas, se abrirá el panel de configuración mostrado en la figura 9.18 que le ofrece la posibilidad de cambiar distintos elementos de configuración y actualización:

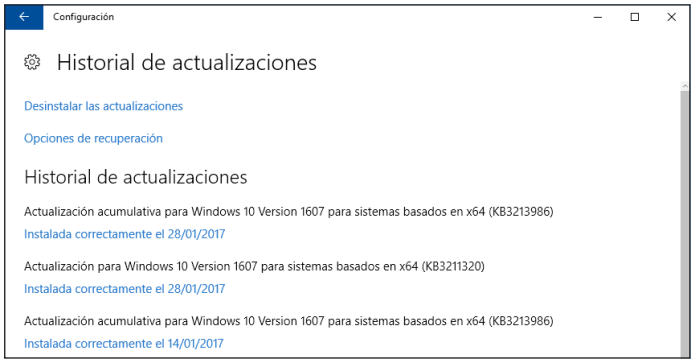

Figura 9.17. Historial de actualizaciones.

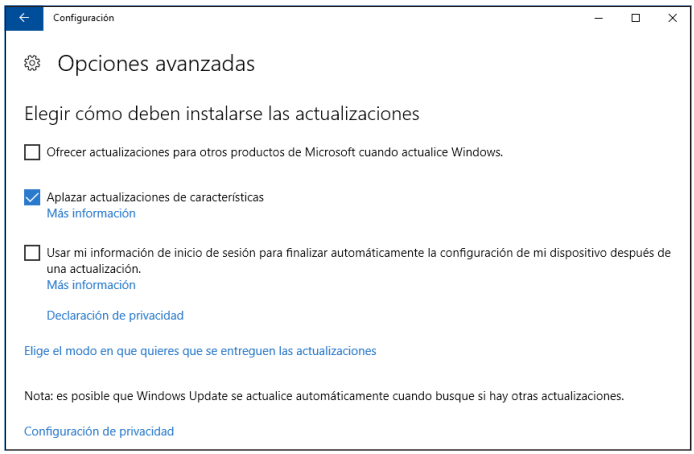

Figura 9.18. Opciones avanzadas de Windows Update.

- **Ofrecer actualizaciones para otros productos de Microsoft cuando se actualice Windows:** Seleccione esta casilla de verificación si quiere ver las actualizaciones para otros productos de Microsoft.
- **Aplazar actualizaciones de características:** Seleccione esta casilla si prefiere aplazar las actualizaciones que estaban programadas para su instalación.
- **Usar mi información de inicio de sesión para finalizar automáticamente la configuración de mi dispositivo después de una actualización:** Esta casilla, cuando está seleccionada, se comportará como indica su título después de una actualización.
- **Elige el modo en que quieres que se entreguen las actualizaciones:** Haga clic en el enlace Elige el modo en que quieres que se entreguen las actualizaciones para elegir entre los ajustes de actualización disponibles dentro de Actualizaciones de más de un lugar. Elija si quiere descargar actualizaciones y aplicaciones de otros ordenadores y seleccione cómo quiere obtener las actualizaciones y luego enviarlas a equipos en una red local o en la red local y en Internet.
- **Configuración de privacidad:** El último enlace abre el panel de configuración Privacidad, mostrando todas las opciones de privacidad disponibles.

9.5. Configuración de seguridad en Internet

Microsoft Edge, el nuevo explorador de Microsoft que presentó en Windows 10 y mejoró con Windows 10 Anniversary Update. En otro capítulo del libro hablaremos sobre este explorador que presume de ser mucho más seguro que Internet Explorer ya que elimina ActiveX y viejas tecnologías y que en esta última versión incluye la posibilidad de descargar extensiones.

En el capítulo mencionado hablaremos de sus opciones de seguridad y, aunque Microsoft Edge sea el explorador predeterminado, sabemos que muchos seguirán prefiriendo usar el conocido Internet Explorer. Por esta razón, en esta sección vamos a hablar de la seguridad para Internet Explorer 11 y su principal configuración de seguridad, dependiendo de las zonas.

Truco: *Puede abrir Internet Explorer desde Microsoft Edge seleccionando* Más acciones>Abrir con Internet Explorer*, o desde el escritorio escribiendo* **internet explorer** *y seleccionando* Internet Explorer *de la lista de resultados.*

La configuración de zonas que podemos aplicar en el explorador Web se categorizan en función de la clasificación del sitio Web que estemos visitando. Estas categorías se denominan zonas y para Internet Explorer son las siguientes:

- **Internet:** Todos los sitios Web se clasifican o en esta zona o en la zona Intranet local, de forma predeterminada. Cuando accedemos a un sitio de la zona Internet se aplica un nivel de seguridad medio-alto que, por ejemplo, impide la descarga de controles ActiveX no firmados y nos pregunta antes de ejecutar los contenidos no reconocidos.

Nota: *Un programa firmado es aquel que posee un certificado de seguridad expedido por una compañía de reconocido prestigio, como por ejemplo VeriSign.*

- **Intranet local:** En esta zona se clasifican todos los sitios alojados en servidores de nuestra Intranet. En este caso se aplica un nivel de seguridad medio-bajo, pues se supone que estos sitios son de confianza.
- **Sitios de confianza:** En esta categoría podemos incluir los sitios que sepamos fehacientemente que son seguros. En ellos se aplicará un nivel de seguridad medio.
- **Sitios restringidos:** Aquí incluiremos los sitios que consideremos no seguros. Podremos seguir visitando estos sitios, pero en ellos se aplicará un nivel de seguridad máximo.

Para configurar las zonas de seguridad, acceda a Internet Explorer 11 y seleccione Herramientas>Opciones de Internet. Por último, haga clic en la ficha Seguridad en el cuadro de diálogo que aparece (véase la figura 9.19).

En la parte superior de este cuadro de diálogo seleccione la zona que desea configurar y, a continuación, haciendo clic en el botón **Sitios**, indique qué sitios desea incluir en ella. Utilice el regulador de la sección Nivel de seguridad para esta zona para elegir uno de los niveles de seguridad predeterminados, o haga clic en el botón **Nivel personalizado** para configurar exactamente qué niveles desea definir en los sitios de confianza.

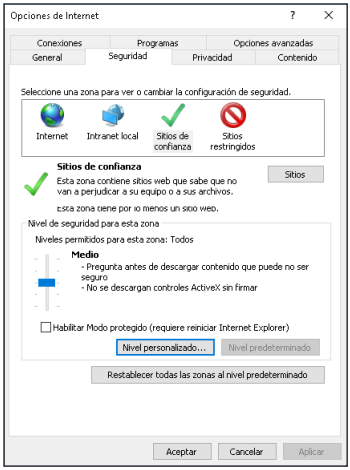

Figura 9.19. Configuración de las zonas de seguridad de Internet Explorer.

9.6. Copias de seguridad y recuperación del equipo

Otras utilidades importantes para poder prevenir y recuperar el equipo si se produce un desastre o se pierde información como, por ejemplo, si el ordenador se infecta con algún virus o cualquier tipo de malware, es la realización de copias de seguridad y la opción de poder restaurarlas si algo sucede. Aunque existen accesos directos desde el nuevo panel Configuración tal como hemos explicado en otro capítulo del libro, es el momento de entrar en una configuración un tanto más avanzada para preparar el equipo para realizar copias de seguridad y su posterior restauración.

9.6.1. Crear una copia de seguridad

Ya sabemos que lo mejor para crear una copia de seguridad es utilizar el Historial de archivos ya que realiza una copia en otra unidad y así podremos restablecer los archivos fácilmente. También hemos hablado en otro capítulo del libro sobre cómo realizar una copia de seguridad desde el nuevo panel Configuración y que Windows 10 Anniversary Update nos permite restablecer el equipo desde otras copias de seguridad

realizadas con Windows 7. Vamos a explicar estos pasos con más detalle para saber con qué opciones cuenta para sus copias de seguridad. Para crear una unidad de recuperación del equipo, siga estos pasos:

1. Introduzca un CD/DVD en el lector óptico o conecte un disco duro externo u otro dispositivo de almacenamiento al equipo.
2. Cierre todas las aplicaciones.
3. Escriba **crear una unidad de recuperación** en el cuadro de búsqueda y seleccione Crear una unidad de recuperación en la lista de resultados.
4. Si se abre un mensaje de control, haga clic en **Sí** para continuar.
5. Haga clic en **Siguiente** en la primera pantalla del asistente.
6. Haga clic en **Siguiente** una vez establecido el destino de la copia de seguridad.

Advertencia: *Al seleccionar un medio externo, todos los datos guardados en el mismo se eliminarán para crear la copia de seguridad.*

Nota: *En el* Historial de archivos *solo se guardan archivos que se encuentran en las bibliotecas, contactos, favoritos y en el escritorio. Para hacer copias de seguridad de archivos o carpetas que están en otra ubicación, debe agregarlos a una de las bibliotecas existentes o crear una nueva biblioteca.*

Para configurar la unidad, dentro del nuevo panel Configuración seleccione Actualización y seguridad>Copia de seguridad. Dentro de Copia de seguridad con Historial de archivos, haga clic en Más opciones y seleccione Ver la configuración avanzada (véase la figura 9.20).

Dentro ya del panel de control, haga clic en **Activar** y siga las instrucciones del asistente.

Si lo prefiere, puede configurar una unidad de reproducción automática haciendo clic en la notificación que se muestra y posteriormente en **Hacer copia de seguridad de los archivos en esta unidad**.

Para configurar una ubicación de red, siga estos pasos:

1. Seleccione el Historial de archivos dentro de Sistema y seguridad del Panel de control.

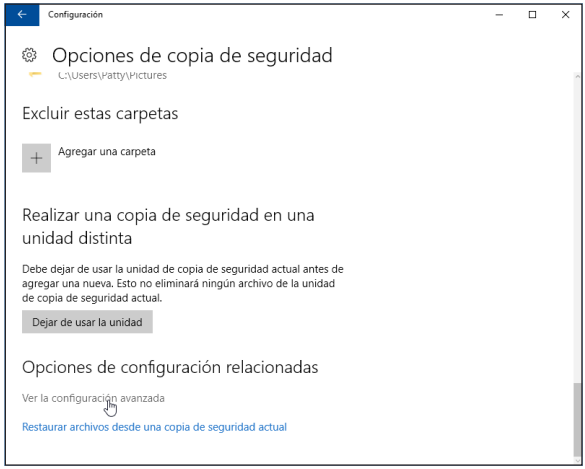

Figura 9.20. Copia de seguridad en Configuración.

2. Haga clic en Seleccionar unidad en el panel izquierdo de la ventana y haga clic en **Agregar ubicación de red** en el cuadro de diálogo mostrado en la figura 9.21.

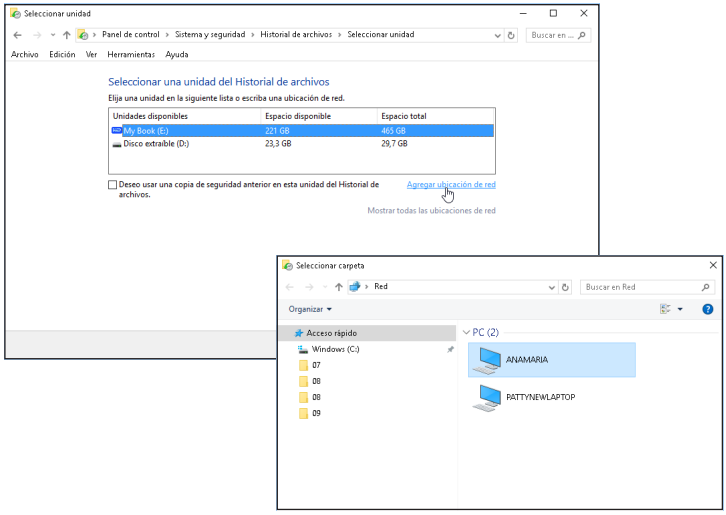

Figura 9.21. Seleccionar unidad de red.

3. Seleccione una carpeta en el cuadro de diálogo de selección y haga clic en **Aceptar**.

El siguiente paso es preparar el equipo para poder restablecerlo en caso de que haya algún problema a partir de las copias de seguridad que hemos realizado. Para ello, haga clic con el botón derecho del ratón sobre **Inicio** y seleccione Panel de control>Sistema y seguridad>Sistema>Cambiar configuración. Posteriormente seleccione la ficha Protección del sistema dentro del cuadro de diálogo Propiedades del sistema (véase la figura 9.22).

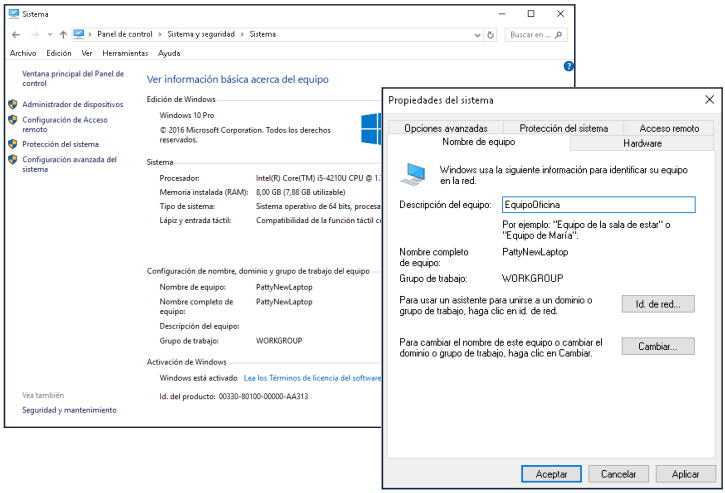

Figura 9.22. Cambiar configuración en Propiedades.

> ***Nota:*** *Recuerde que también puede acceder a este cuadro de diálogo seleccionando* Información del sistema>Cambiar configuración>Protección del sistema *en la sección* Acerca de *del nuevo panel* Configuración *dentro de* Sistema.

En la ficha Protección del sistema, podrá activar la protección de sus unidades. Seleccione la unidad y haga clic en el botón **Configurar** dentro de la sección Configuración de protección. Seleccione Activar protección del sistema y, si lo desea, ajuste el espacio máximo en disco que va a usar esta protección deslizando la barra hasta la opción deseada. Cuando haya terminado, haga clic en **Aplicar**. Siga estos pasos para cada una de las unidades hasta haber activado la protección en todas ellas. Por último, haga clic en **Aceptar** para volver a la ventana anterior.

9.6.2. Restaurar sistema

Para poder restaurar una copia de seguridad del sistema y restablecer así el equipo, tiene que haber ejecutado al menos una vez la copia, tal como hemos indicado anteriormente. Además, necesita crear un punto de restauración para las unidades en las que activó anteriormente la protección. Si no las ha activado, hágalo ahora y después siga estas indicaciones:

1. Haga clic en **Crear** dentro del cuadro de diálogo Propiedades del sistema en la ficha del mismo nombre para crear un punto de restauración.
2. Escriba una descripción del punto de restauración y haga clic en **Crear**. Se creará automáticamente el punto de restauración.
3. Cuando el asistente haya terminado, mostrará un mensaje indicando que el punto de restauración se creó correctamente.
4. Dentro de Propiedades del sistema, haga clic en **Restaurar sistema**. Se abrirá el asistente que le guiará por todo el proceso. Haga clic en **Siguiente**.
5. Ahora seleccione un punto de recuperación como muestra la figura 9.23 y, si lo prefiere, haga clic en **Detectar programas afectados** para ver una lista de los programas que se verán afectados por el restablecimiento. En caso contrario, haga clic en **Siguiente**.

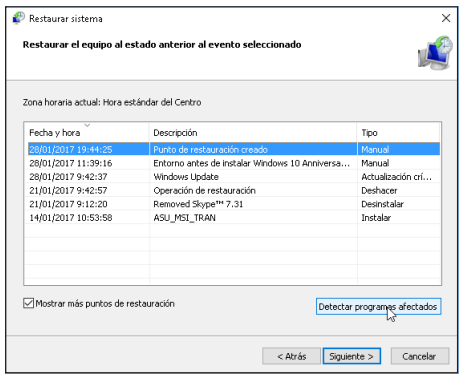

Figura 9.23. Pantalla de restauración.

6. En la pantalla de confirmación del punto de restauración podrá ver información sobre lo que va a pasar cuando restablezca el sistema. Si está de acuerdo con toda la

información proporcionada, haga clic en **Finalizar** para restaurar el sistema. Si desea realizar algún cambio, haga clic en **Atrás** y siga las indicaciones del asistente otra vez.

Si prefiere hacer una restauración desde el Historial de archivos, seleccione Panel de control>Sistema y seguridad>Historial de archivos desde el menú contextual de **Inicio** y haga clic en Restaurar archivos personales en el panel izquierdo para seleccionar el punto de restauración al que desea volver. Posteriormente, solo tendrá que seguir las indicaciones del asistente para recuperar sus archivos.

Si es un usuario avanzado y quiere realizar una copia de seguridad del registro, podrá hacerlo con ayuda del cuadro Ejecutar que puede abrir desde el menú contextual de **Inicio** haciendo clic con el botón derecho del ratón sobre él. Después, siga estos pasos:

1. Dentro del cuadro de texto Abrir, escriba **Regedit** y haga clic en **Aceptar**.
2. Si se abre un mensaje de control de cuentas de usuario, haga clic en **Sí** para seguir adelante. Una vez abierto el Registro de Windows, haga clic en Archivo>Exportar y seleccione dónde desea guardar el archivo con `extensión.reg`. Escriba un nombre de archivo para poder reconocerlo fácilmente en caso de necesitar usarlo para una tarea de restauración.
3. En la parte inferior del cuadro de diálogo Exportar archivo del Registro, seleccione la opción Todo para exportar todo el registro. Haga clic en **Guardar** para almacenar la copia de las claves de su registro en la ubicación indicada (véase la figura 9.24).

Ahora, si por algún motivo las claves de su registro desaparecen, podrá importar este archivo ejecutando Archivo>Importar.

9.7. Problemas de seguridad

Tome nota de algunas situaciones muy comunes, especialmente en los usuarios que empiezan a usar Windows, ya que pueden convertir al equipo en una máquina muy vulnerable y exponerla ante cualquier malware:

- **Borrar archivos "porque no sé lo que es":** Es normal que por motivos de falta de espacio en el disco o simplemente, porque no se sabe por qué está un determinado

archivo en una ubicación concreta, haya usuarios que, sin saber lo que hacen, borran archivos vitales para que el sistema pueda iniciarse. Es mejor que si no sabe bien lo que está haciendo, no elimine ningún archivo. Si le hace falta más espacio, le recomendamos que utilice una unidad de almacenamiento extraíble.

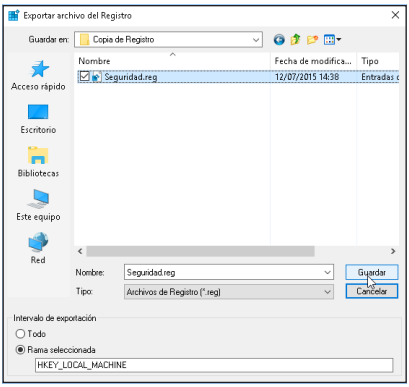

Figura 9.24. Exportar un archivo de registro.

- **Hacer clic en cualquier mensaje sin leer el contenido:** Esta práctica es especialmente peligrosa en el ámbito de Internet, donde con un solo clic, podemos infectar nuestra máquina con algún tipo de software malicioso.
- **Abrir correos de remitentes desconocidos:** Se trata de otra fuente importante de introducir software espía y virus en el equipo.