Tabla de contenido

Cómo evitar el ransomware en tu empresa

Este manual esta en construcción y constante actualización... ESTA ES UNA FUENTE Y ESTA ES OTRA FUENTE.

Que es el ransomware ? DEFINICIÓN DE LA WIKIPEDIA

Cómo proteger tus archivos del ransomware con la nueva función del centro de seguridad en Windows 10+

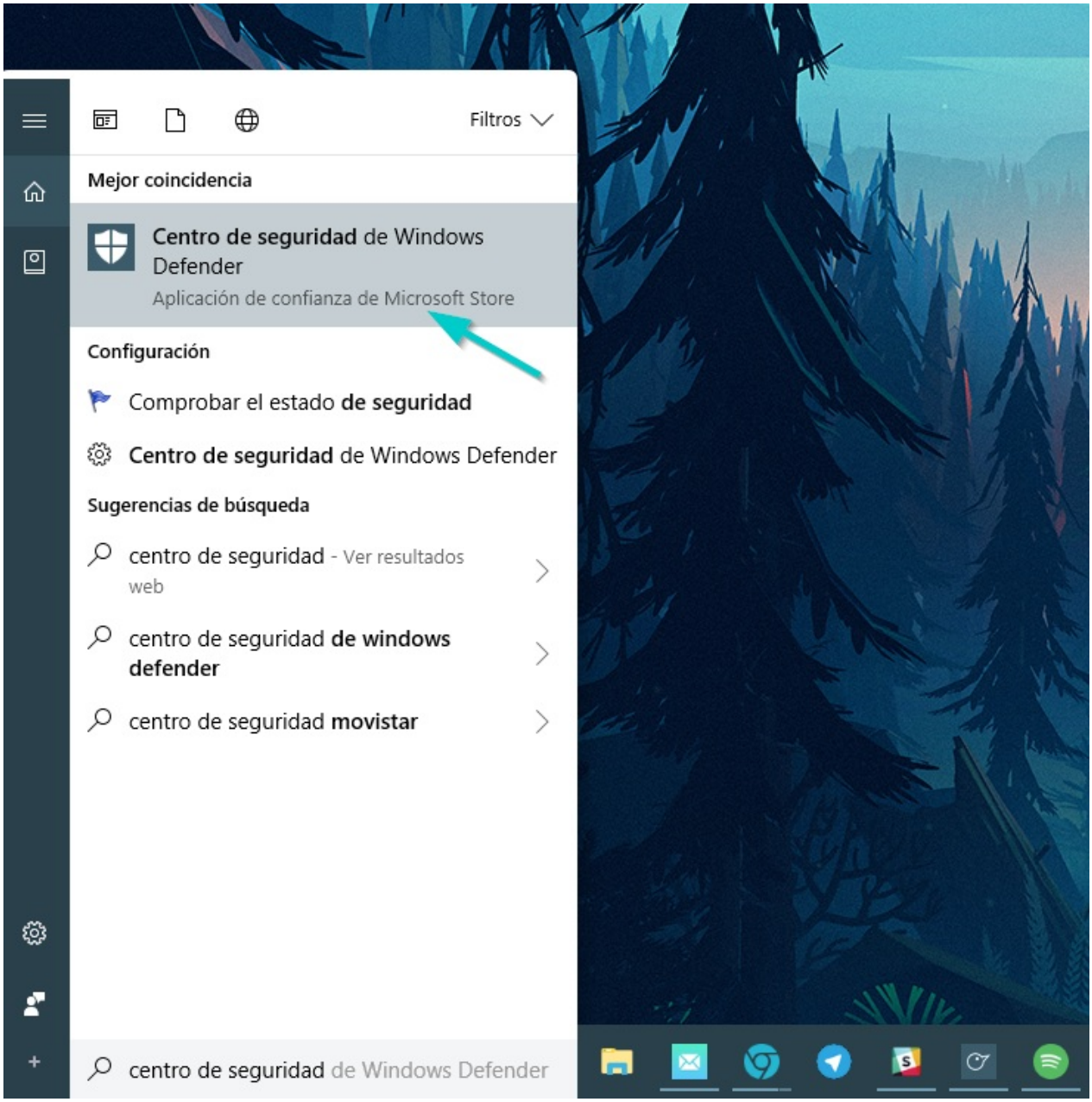
La Fall Creators Update está a punto de cumplir una semana entre nosotros, y aunque no ha estado libre de problemas para algunos usuarios, se trata de una actualización con bastantes novedades interesantes que no se notan a simple vista.

Una de estas tiene que ver con la seguridad. Se trata de una función especial para proteger tus archivos del ransomware controlando el acceso a carpetas. El detalle está en que no se activa por defecto, así que si te interesa disfrutar de ella, te enseñamos cómo usarla.

Siguiendo estos pasos podrás activar la protección contra ransomware de Windows 10. Esto quiere decir que a partir de ahora Windows Defender va a monitorizar los cambios que cualquier aplicación intente realizar en tus carpetas protegidas.

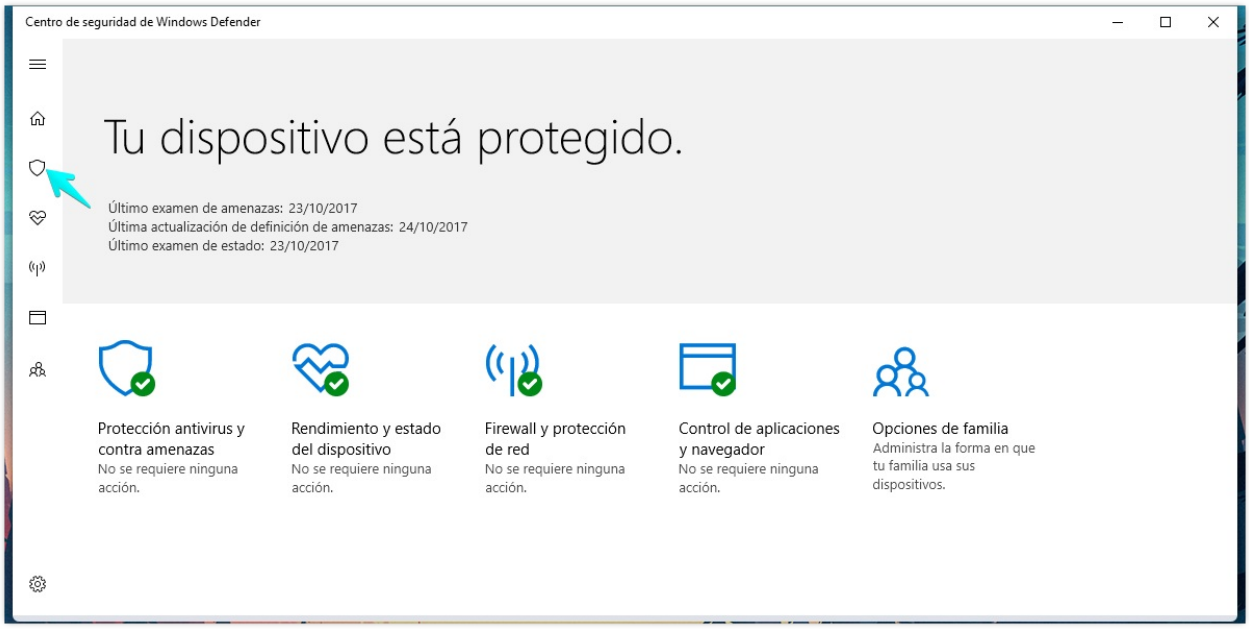
Ya que los ataques de ransomware suelen apoderarse de los archivos del usuario y exigir un rescate para liberarlos, con esta capa de seguridad extra, Windows Defender bloquea completamente el acceso a archivos a software que no sea de confianza, justamente para evitar un secuestro.

Activar la protección contra ransomware en Windows 10

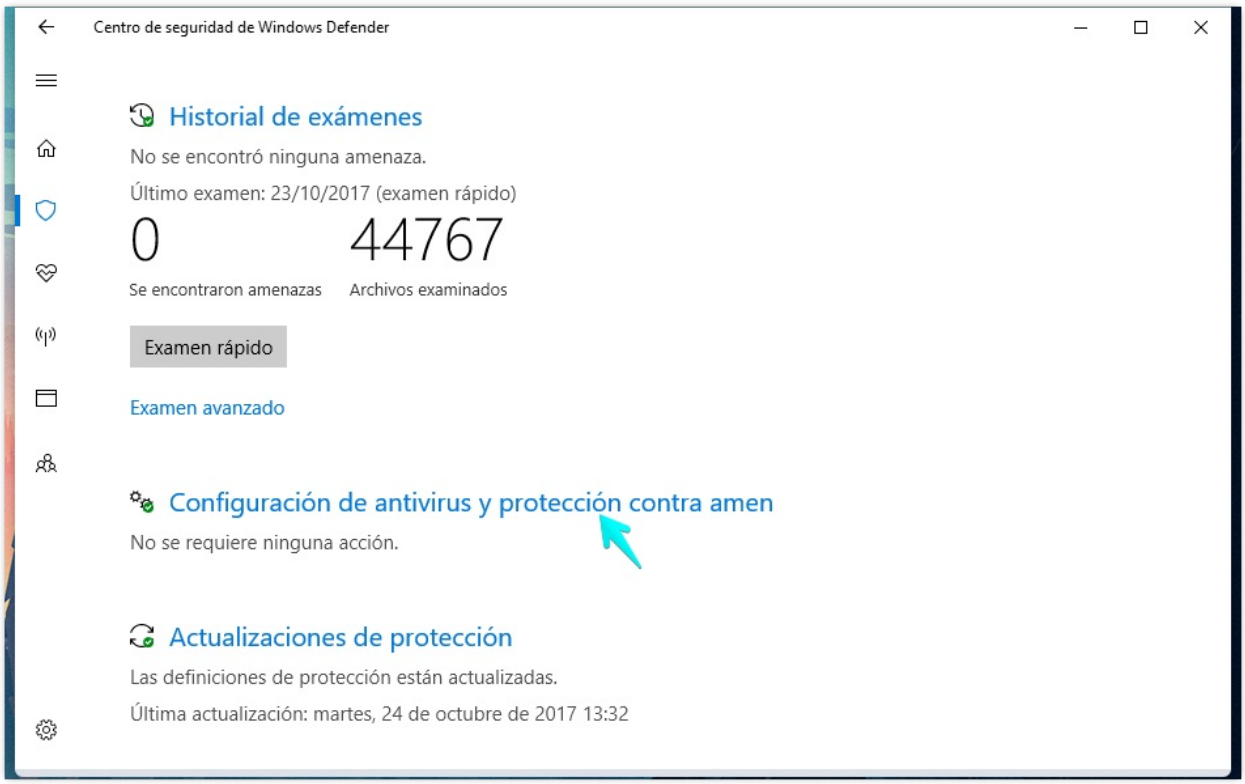


Presiona el botón de inicio, escribe "Centro de seguridad" y elige el primer resultado.

Luego, en la ventana del Centro de Seguridad de Windows Defender haz click en Protección antivirus y contra amenazas, es decir, el icono en forma de escudo a la izquierda.



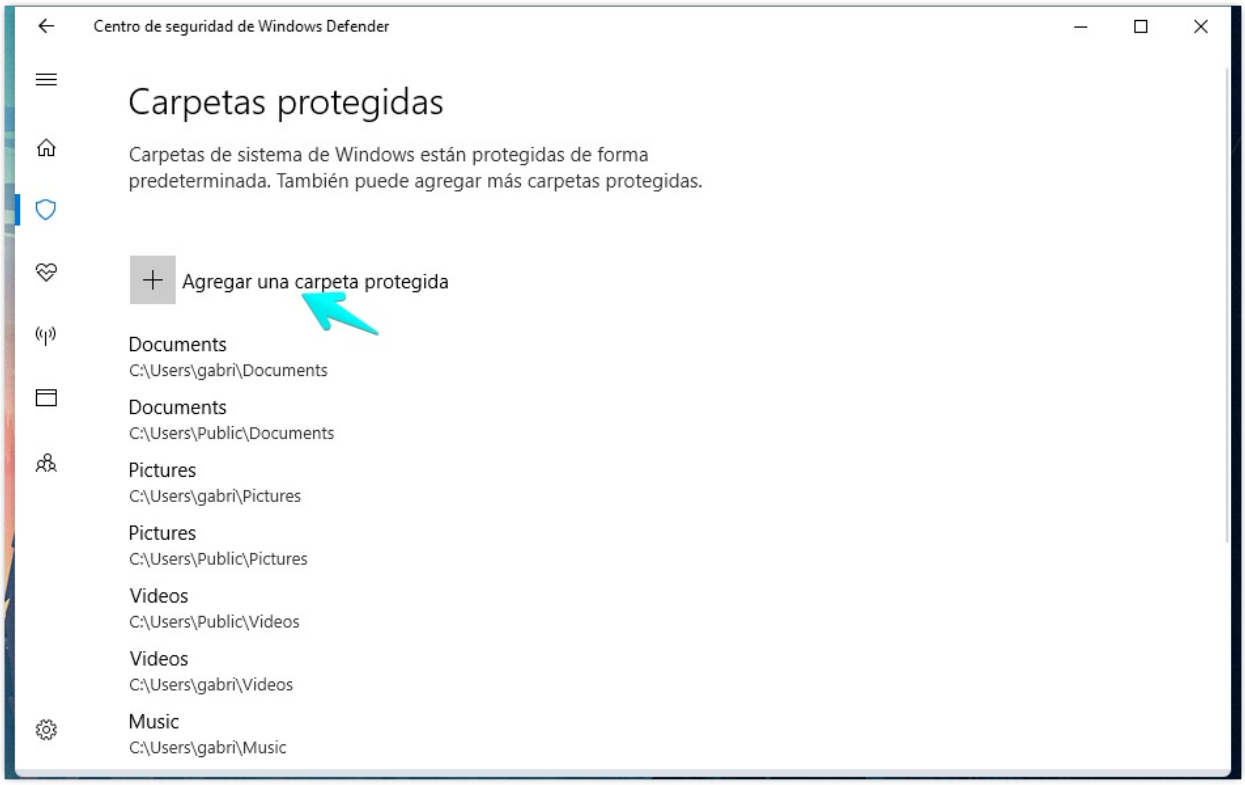
Lo siguiente es hacer click en la opción Configuración de antivirus y protección contra amenazas.



Haz scroll hasta encontrar la opción Controla el acceso a la carpeta y marca la casilla Activado. Esto mostrará una ventana de confirmación para que des permiso a Windows Defender a cambiar la configuración. Dile que sí y listo.

A partir de ahora, si una app intenta cambiar tus archivos protegidos, la app se pondrá en una lista negra y Windows te informará. Por defecto, las carpetas protegidas son: Documentos, Imágenes, Vídeos, Música, Escritorio y Favoritos. También puedes añadir más.

Añadir carpetas protegidas



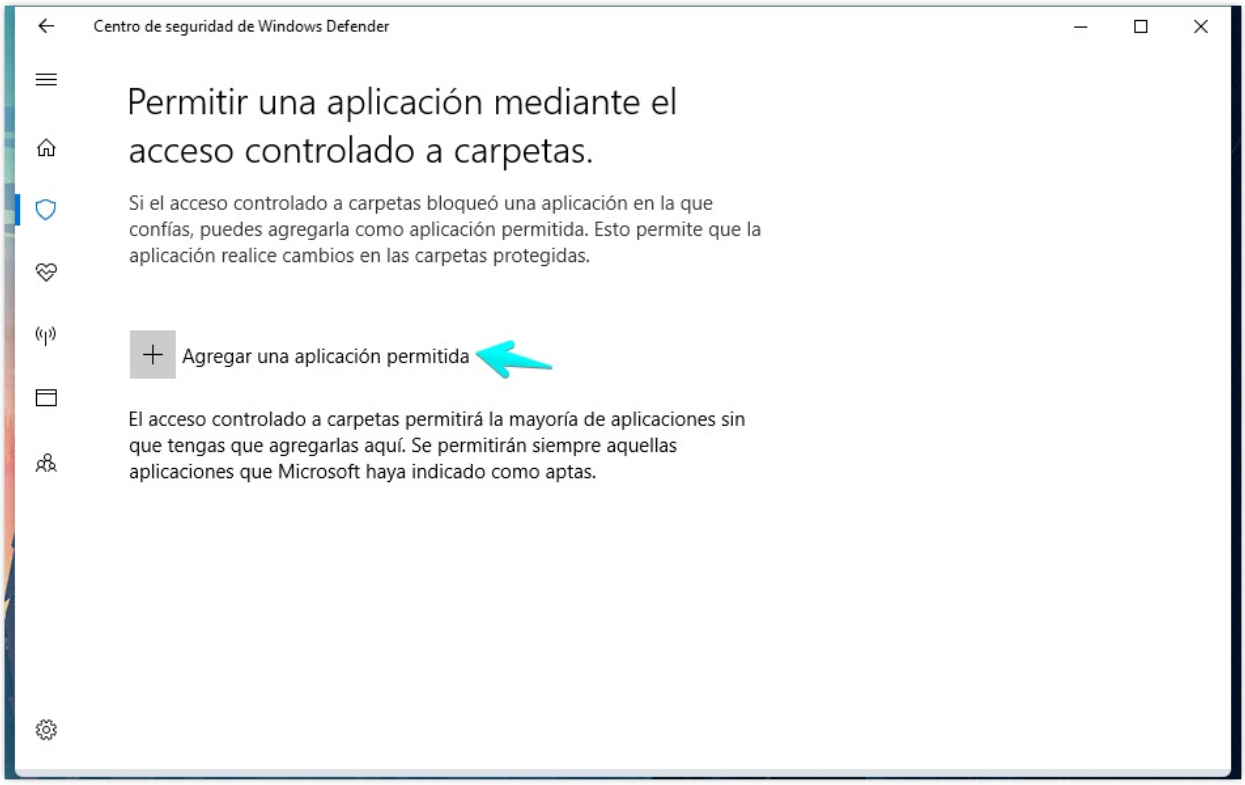
Si haces click en carpetas protegidas debajo del botón de activado en el menú anterior, podrás ver la lista de carpetas (y su su ruta) que actualmente están siendo protegidas por Windows Defender.

Haciendo click en el botón de + para agregar una carpeta protegida podrás seleccionar cualquier carpeta de tu disco o discos de almacenamiento. Eso sí, debes hacerlo una por una.

Permitir el acceso a una app de confianza

El acceso controlado se permitirá a la mayoría de las apps sin que tengas que añadirlas manualmente, si la app ha sido verificada por Microsoft como apta, entonces lo más probable es que no tengas que darle acceso manualmente.

Por ejemplo, no tienes que preocuparte de pronto por tener que añadir Dropbox o Photoshop a la lista de apps que pueden acceder a tus documentos e imágenes. Seguirán teniendo acceso controlado.



Si hay aplicaciones en las que confíes y a las que quieras permitir acceso a tus archivos dentro de las carpetas protegidas, puedes añadir excepciones a la protección contra ransomware.

También si tienes una app a la que el acceso controlado ha añadido a la lista negra y quieres sacarla de ahí, puedes desbloquearla desde aquí.

Solo tienes que hacer click en Permitir que una aplicación acceda a una de las carpetas controladas y luego seleccionar la aplicación desde tu lista de software.

Fuente:genbeta.com

Primer Nivel, el Hardware:

- Deshabilitar y en la mejor medida desmontar de los equipos el hardware plug-in o Dispositivos de entrada como Unidades de DVD, Puertos USB y Lectores de Tarjetas.

Debemos usar un modelo de computación centralizada como un rack con un servidor de estaciones y en cada modulo o consultorio solamente tener una pantalla con un teclado y un mouse conectados al servidor.

Ver en vídeo que es una estación virtualizada

Ver en Mercadolibre un ejemplo

Que ventajas ofrece el modelo de estación virtual ? Que descarta los dispositivos de entrada habituales por donde tus usuarios ingresan el ransomware al sistema.

Que desventaja? Que si el servidor central se cae se queda toda la institución sin sistemas, para este suceso recomendaría tener como contingencia el sistema alojado en la nube (hablare mas adelante de la nube) y habilitar temporalmente el login desde dispositivos del usuario como sus móviles (celulares).

Segundo Nivel el Soporte:

Exigir a sus empresas de soporte técnico licencias pagas del popular TEAM VIEWER que tanto les gusta, ya que es habitual en la region hispana usar un CRACK (con regalitos) para quitar el limite de sesiones de soporte que tiene la versión gratis del popular programa de soporte técnico. O ver que usan versiones realmente libres como el escritorio remoto de windows o el escritorio remoto de chrome.

Tercer Nivel el Antivirus:

Por mas que se defiendan los antivirus gratuitos no son lo mismo que una versión profesional y aunque hoy en día su heurística deje mucho que desear por lo menos algo es algo, y si el software de protección queda inerte ante un ataque 0 day (Dia 0 en wikipedia). Recomiendo combinar el AV tradicional (Norton - https://co.norton.com/) con software extra como el plugin de navegadores adblock (adblockplus) y aun mas importante una suite de spywares como el malwarebytes (malwarebytes).

En este nivel va incluido el monitor o firewall de red, el SO del Servidor y demás...

recomiendo un CentOS 7. Se preguntaran por que recomiendo el CentOS 7, es por que es el SO que tienen en común los centros de datos de la Nube y esta desplegable tipo clic e instale en los racks de los proveedores internacionales como digital ocean.

Cuarto Nivel "EL USUARIO":

Este es el ultimo nivel y lo deje de ultimo por que es el mas
critico y el mas vulnerable.

Aunque si implementaste lo de solo pantalla, teclado y mouse ya descartaste varios posibles flagelos de fuga de información y vas a poder monitorear en la red que comparten mediante sus correos o suben a la nube o descargan, y si se supone que están en el trabajo y deben de usar es solamente el correo corporativo y vas a tener todo el derecho legal de supervisar que navega desde la consola institucional.

Si deseas compartirles WIFI debes separar el proveedor de red abierta del de tu red privada o intranet institucional.

Aparte no sugiero usar conexión wifi hacia los nodos ya que este tipo de conexión es fácilmente interceptable, es mas el usuario va poder obtener la clave fácilmente de una conexión wifi, es mejor conectar los nodos por red cableada. (o tenerlos virtualizados).

Si ya implementaste la red wifi debes asegurarte de que el usuario no tenga acceso a las configuraciones usando herramientas como: Editor del Registro/Abolir todas las restricciones del WinXP

Deshabilitar la ejecución de aplicaciones desconocidas.

Deshabilitar el acceso al panel de control y configuraciones de las conexiones de red

entre otros... (si estaba sobre win XP y si llevo 10 años analizando como hacer mas seguros los sistemas).

Para gestionar la red WIFI de tu empresa te recomiendo PFSENSE puedes descargarlo de: [PDF] Los mejores 30 libros en español de PFSENSE

Si deseas un Servicio Profesional o Asesoria para tu empresa en cuanto a protegerte contra el ransomware contactanos en:

El WhatsApp de Sistemas y Controles:

+573217230780

El correo de Sistemas y Controles:

proyectosweb@sistemasycontroles.net

Nuestra web:

www.sistemasycontroles.net