Seguridad de Windows

Transcribed on August 4, 2025 at 2:35 PM by Minutes AI

Speaker 1 (00:07)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la protección de Windows Security, lo que antes era conocido por Windows Defender y lo que viene a ser la solución antimalware que viene instalada por defecto en los sistemas operativos Windows.

Aunque en principio ha sido siempre un tema polémico el que el propio sistema operativo traiga instalado de fábrica un software antimalware o un antivirus, las necesidades para poder defenderse de tanta amenaza de malware y software malicioso y diferentes elementos perjudiciales para el buen funcionamiento de las aplicaciones del sistema operativo, hace que sea muy interesante el tener un software antimalware preinstalado en el propio sistema.

Además, en los últimos años Microsoft ha decidido aplicar mucho esfuerzo en la mejora del software antimalware y tiene muchísimas características que pueden ser muy interesantes, sobre todo en las últimas versiones del sistema operativo como puede ser Windows 10 o Windows 11.

Dentro de las áreas de protección de Windows Security vamos a tener lo que sería la protección contra virus y amenazas, tendríamos la protección de cuentas, vamos a tener también enlaces por ejemplo al firewall de Windows para la protección de red, tendríamos también protección de aplicaciones y de control del navegador, y tendríamos en esta parte la protección contra exploits.

También tendríamos protección del propio dispositivo, esto siempre va a tener que ver con el hardware del dispositivo, que tenga componentes que sean compatibles con esas tecnologías.

Y después vamos a hablar también de la reducción de la superficie de ataque.

Empezamos definiendo las diferentes secciones de protección que tenemos en Windows Security.

Vamos a tener una solución completa que tiene solución para el virus, para poder escanear software malicioso, para poder actualizar la base de firmas para esos escaneos de software malicioso.

Vamos a ver que también tiene enlaces para la protección de cuentas y mejoras para la securización de las identidades del sistema operativo.

También tiene protección en la parte de red y vamos a ver que tiene también protección en la parte de aplicaciones, también en el market de las aplicaciones para hacer descargas más seguras en lo que se refiere a la parte de las aplicaciones y en la parte del funcionamiento del navegador del sistema operativo.

También tiene aplicaciones que se pueden activar en función de la capacidad del hardware para proteger los procesos del microprocesador u otros componentes del sistema operativo o cifrar el disco duro.

Y luego tiene otras características como puede ser el estado de salud o rendimiento del dispositivo o las opciones de control parental que tendríamos en las opciones de familia.

Empezamos hablando un poco de lo que sería la configuración de la protección de amenazas y virus.

Esto sería la parte más conocida de un antivirus o de un software antimalware, en la que nosotros vamos a tener la protección en tiempo real que vamos a tener habilitada y que va a detener ataques en base a una serie de comportamientos malicios que previamente se conoce y también la posibilidad de realizar escaneos periódicos en el sistema operativo y en la parte de almacenamiento de datos de todos los ficheros y archivos del dispositivo en busca de Marwa.

Aparte de esto, nosotros vamos a tener dentro de esta categoría nuevas características como puede ser la protección contra ransomware con lo que se denomina el control de acceso a carpetas, una excelente medida de seguridad que va a permitir que nosotros podamos definir una serie de carpetas a las que no se va a poder acceder, excepto una serie de aplicaciones que previamente nosotros vamos a definir.

Tenemos también dentro de la seguridad de Windows la protección de identidades con la protección de cuentas.

Realmente lo que hace la parte de Windows Security redirige las peticiones a la parte de administración de cuentas, concretamente a la parte de las opciones de inicio de sesión, donde nos va a permitir configurar las diferentes opciones de autenticación.

Y también hay nuevas opciones en Windows 11, como por ejemplo lo que se llama el bloqueo dinámico.

El bloqueo dinámico consiste en que nosotros podemos hacer que se bloquee el dispositivo cuando un determinado elemento que está emparejado mediante Bluetooth se distancia o sale del rango de alcance del portátil, por ejemplo, de la tablet.

Entonces en ese momento, por ejemplo, si yo tengo el portátil que está emparejado con el teléfono, si el teléfono está conectado por Bluetooth y sale del rango del dispositivo, automáticamente me bloquea el dispositivo porque entiende que yo no estoy cerca de ese dispositivo.

Este bloqueo dinámico puede ser administrado en la ruta de configuración de cuentas.

Opciones de inicio de sesión, Configuraciones adicionales, Bloqueo dinámico Tenemos también la posibilidad de configurar opciones en la seguridad de aplicaciones y también en la utilización del servicio web.

Vamos a tener una serie de configuraciones que van a basar las opciones que van a permitir, basadas en un sistema de reputación, con un sistema inteligente para funcionar con el navegador y con el almacén de aplicaciones, con una protección anti phishing y de esta manera se van a bloquear una serie de aplicaciones o una serie de páginas web o una serie de descargas en función de la reputación de un determinado sitio, determinado fabricante o de un determinado stock.

Dentro de esta categoría vamos a tener también la posibilidad de configurar la protección contra exploit.

Y en la protección contra exploit nosotros vamos a tenerla habilitada por defecto en Windows 11 y nos va a proteger contra vulnerabilidades de seguridad y va a mitigar diferentes tipos de ataques.

Y muchas de estas características vienen heredadas o han sido integradas de lo que se conocía como M MT era una herramienta que en versiones posteriores de Windows podíamos descargar para poder hacer configuraciones de protección incluso contra ataques tipo DI.

Pues muchas de estas configuraciones que teníamos integradas en M, que ha sido un software que ha sido ya descatalogado para las últimas versiones de Windows, vienen integradas dentro de Windows 10 y de Windows 11.

Las mitigaciones que nosotros podemos configurar para poder estar en estado encendido, apagado o el balón por defecto.

Y en el caso de algunas configuraciones vamos a poder configurarlas en modo auditoría.

De esta manera vamos a ver si eso está bloqueando algo sin que realmente llegue a bloquearlo, entonces miraremos los registros y mediante esos logs podemos ver si están bloqueando ciertas características o ciertas funciones, aunque nos lleven a bloquearlas y no va a afectar al funcionamiento del dispositivo.

Tenemos también opciones para la propia seguridad del dispositivo, nos van a permitir configurar opciones de seguridad del procesador, de arranque seguro o de cifrado de datos y siempre que todas estas características sean compatibles con el Hábrica, con componentes físico, es decir, el dispositivo que estemos utilizando y van a ayudar a mejorar lo que sería la parte de salud.

Finalmente tenemos otras opciones como por ejemplo reducir la superficie de ataque, como esta tecnología que tenemos en la diapositiva que es AESR, es un conjunto de reglas configurables en Windows PowerShell y que nos van a permitir combatir ataques contra Office, contra ejecuciones de scripts como PowerShell, maliciosos, JavaScript o Visual Basic Script, o contra la parte de correo, bloqueando descargas potencialmente peligrosas o una serie de reglas que van a decidir qué es lo que va a estar permitido y lo que no.

Tenéis más información en la URL de la diapositiva sobre ASR y tenéis un ejemplo de la sintaxis también en la diapositiva de cómo sería la configuración de esas preferencias mediante Windows PowerShell y un enlace a los diferentes comandos o las diferentes opciones de sintaxis que tendríamos para la configuración de ASR a través de Windows PowerShell.

Vamos a ver un poco las diferentes áreas de protección que tenemos en Windows Security y cómo podemos trabajar con ellas.

Estamos en la máquina virtual, nos vamos a las opciones de configuración y dentro de las opciones de configuración nos vamos a la categoría de seguridad y privacidad.

Dentro de esta categoría lo primero que vamos a ver a nivel general es que podemos configurar aquí los diferentes permisos o analizar los diferentes permisos que vamos a tener utilizados en el equipo.

Entonces podemos entrar en la configuración general de privacidad y vamos a ver las opciones que tenemos configuradas.

Tendríamos también en lo que se refiere a la parte, por ejemplo, del análisis de voz o por ejemplo, en el reconocimiento de voz.

Tendríamos también diferentes tipos de configuraciones para la parte de personalización, el histórico de actividad.

Tendríamos aquí la parte de permisos de búsqueda.

Esta es una opción muy interesante porque nosotros podemos configurar aquí qué opciones vamos a tener en la parte de búsqueda y podemos configurar también aquí las diferentes opciones que vamos a permitir si queremos tener una protección de búsqueda que sea moderada, que esté apagada o que sea stream.

Y luego dentro de la parte de las búsquedas de Windows, nosotros también podemos hacer configuraciones y podemos incluso excluir carpetas de la parte de búsqueda de Windows.

Si nos fijamos, por ejemplo, tenemos una serie de carpetas en lo que se refiere a la parte de datos de programa o lo que se refiere a la parte de los archivos de si sistema de Windows o lo que sería la parte de backup, que directamente están excluidos en la parte de indexación cuando nosotros hacemos una búsqueda de Windows.

Todas estas opciones pueden ser muy interesantes para configurar diferentes entornos o diferentes temas de privacidad, sobre todo en lo que se refiere a la parte del funcionamiento del propio sistema operativo.

En lo que se refiere también a la parte de permisos de aplicaciones, vamos a tenerlos aquí disponibles en la parte de localización, cámara, micrófono, Todo esto tiene una vital importancia, sobre todo si tenemos dispositivos que tienen estos elementos integrados, por ejemplo portátil o una tablet o móvil, pues vamos a ver que tiene integrada la cámara, el micrófono, entonces la configuración de todos estos permisos por aplicación puede ser interesante.

Y luego tendríamos las opciones de encuentra mi dispositivo.

Si nosotros tenemos un dispositivo como puede ser una tablet o un teléfono o incluso un portátil, pues podemos activar estas opciones siempre y cuando nosotros estemos trabajando con una cuenta de Microsoft 365 o con una cuenta de la nube que nos permita habilitar este posicionamiento para el control el dispositivo en el caso de que perdamos o que sea sustraído.

Luego si entramos en la parte de Windows Security vamos a ir directamente a aquellos aspectos relacionados específicamente con la seguridad.

Vamos a abrir Windows Security.

Una vez que tenemos abierto Windows Security, en Windows Security nosotros nos vamos a encontrar con una categorización de todas las características de seguridad que podemos implementar de forma centralizada en este panel.

Algunas de estas características son propias de este panel y otras características nos van a llevar a otras consolas de administración diferentes.

Si nos vamos a la parte de protección de virus, nosotros aquí vamos a tener las diferentes opciones relacionadas con lo que sería la parte de administración del software antimarware.

Nos vamos aquí, por ejemplo, a ver las opciones de escaneo, donde podemos iniciar un escaneado del dispositivo.

Luego tendríamos histórico de protección, tendríamos aquellas amenazas que queda queremos permitir una serie de software que puede ser en un momento determinado detectado como malware por ser una herramienta de seguridad informática, por ejemplo, y que nosotros queremos permitir porque la estamos utilizando para una determinada tarea.

En la parte de configuración vamos a poder definir la protección en tiempo real, también la protección cloud y también cómo va a comportarse el software antimalware y si queremos añadir, por ejemplo, una serie de exclusiones a ese software anti malware.

Y luego tendríamos aquí la configuración del acceso a carpetas.

El control de acceso a carpetas es una herramienta que va a funcionar para defendernos del ransomware.

Ransomware es este malware que lo que hace es que nos cifra los datos y luego nos pide un RES para poder recuperar esos datos, para poder descifrarlos.

Entonces nosotros lo que vamos a hacer es proteger una serie de carpetas.

Si vamos a la parte de carpetas protegidas vemos que además está protegida esta configuración mediante el control de puntas de usuario y vamos a tener una serie de carpetas en las que no se va a poder escribir.

Entonces para escribir en esas carpetas tiene que ser una serie de aplicaciones autorizadas.

Evidentemente un malware no va a ser una aplicación autorizada para escribir en la carpeta de documentos, con lo cual no tendría permisos de escritura.

Además nosotros tenemos la posibilidad de añadir carpetas determinadas.

Yo tengo una carpeta con proyectos, pues puedo añadir esa carpeta para que esté protegida por esta tecnología.

Luego lo que podemos hacer también es que podemos permitir que una determinada aplicación tenga la capacidad de poder escribir en esas carpetas.

Es muy lógico que yo en la carpeta de documentación permita por ejemplo que a lo mejor el Excel o que el Word pueda modificar esos archivos.

Entonces vamos a añadir aquí esas aplicaciones y esas aplicaciones sí que van a poder hacer esas modificaciones.

Además otra opción que tenemos disponible es que podemos configurar todos estos datos para que haya una copia inmutable en OneDrive.

Esto lo que va a hacer es que sabemos que aunque nos fallara por algún motivo este sistema, nosotros tendríamos una posibilidad de recuperar los datos con esa copia que tendríamos en la nube.

Lo mismo que acabamos de definir lo tenemos en la parte de abajo de categoría de virus y protección contra amenazas en la parte de protección de Ransomware.

Vamos aquí a la parte de protección de Ransomware.

Dentro de la parte de protección de Ransomware vemos que lo tenemos habilitado y tendríamos aquí la parte de protección de carpetas.

La siguiente característica sería la característica de protección de cuentas.

Pero si nosotros entramos en la característica de protección de cuentas vamos a ver que lo que tendremos aquí es la parte de inicio de sesión de Windows Hero, donde podemos manejar las opciones de inicio de sesión.

Y si nos fijamos, al manejar las opciones de inicio de sesión realmente Windows Security lo que nos lleva es a la parte de cuentas.

Vamos a la parte de cuentas, las opciones de inicio de sesión y dentro de las opciones de inicio de sesión tendríamos aquí también el bloqueo dinámico.

Si damos para atrás volvemos a la parte del mundo Security y si nos vamos a la protección de cuentas y vamos a la parte de configuración del bloqueo dinámico vemos que nuevamente nos vuelve a redirigir a la parte B y inicio de sesión de cuentas y nos vendría aquí a habilitar el bloqueo dinámico.

El bloqueo dinámico es esta nueva característica que lo que va a hacer es que va a emparejar el dispositivo con un dispositivo conectado mediante Bluetooth, puede ser un teléfono y cuando ese dispositivo sale de rango automáticamente puede bloquear el portátil, puede bloquear el dispositivo para que nadie pueda acceder de una forma autorizada a ese dispositivo Entiende que yo me separo del portátil, me he olvidado el portátil o la tablet pero me llevo mi teléfono entonces cuando el teléfono se separa, sale del rango de la tablet o del portátil pues entiende que yo no estoy ahí, entonces bloquea el dispositivo, es una característica que bastante interesante.

Luego tendríamos las opciones de firewall que nos va a pasar un poco lo mismo, las opciones de firewall lo que nos va a llevar es a la protección de red o firewall que hemos visto en vídeos anteriores donde nosotros podremos aquí configurar las diferentes opciones del firewall y tendríamos aquí las características avanzadas del firewall de objetivos.

La siguiente sección que tendríamos disponible sería el control de aplicaciones y dentro de la parte de control de aplicaciones nosotros vamos a tener aquí la posibilidad de configurar una protección basada en reputación.

Si fuéramos aquí a la parte de configuración vamos a ver las diferentes opciones que tenemos disponibles para chequear aplicaciones, archivos, lo que sería un filtro inteligente para el navegador, en este caso para Microsoft Edge, protección anti phishing donde podemos configurar también diferentes opciones y tendríamos también la posibilidad de bloquear aplicaciones, podríamos iniciar esto y podríamos hacer que esto bloqueara aplicaciones o descargas de aplicaciones.

Vemos que muchas de estas características vienen configuradas, configuradas por defecto, entonces Microsoft se ha puesto mucho las pilas con el tema de la seguridad y de esta manera vemos que hay una serie de configuraciones que tenemos disponibles en Windows 11 que ya estarían funcionando.

Luego tendríamos también dentro de esta misma categoría de control de aplicaciones lo que sería la protección de exploits entonces si entramos dentro de la protección de exploit vamos a tener una serie de tecnologías como Control Flowbar, como T, como ASLR que lo que nos va proteger contra diferentes tipos de ejecución de código con la actividad maliciosa de malware o de ataques dirigidos que trata de inyectar código en procesos legítimos y de esta manera nosotros podemos habilitar todas estas características, Vemos que la configuración es encendido, apagado, la configuración por defecto y vemos que muchas de estas configuraciones por defecto son configuraciones que por defecto están encendidas.

Entonces esto lo que nos va a hacer es que nos va a generar un sistema operativo que es mucho más seguro que sistemas operativos o versiones de Windows anterior.

Luego en la parte de configuración de programas vamos a tener aquí diferentes programas y vamos también a poder añadir programas con una configuración específica.

Si yo cualquiera de estos elementos voy a la parte de editar, puedo seleccionar cualquiera de esos programas y puedo seleccionar aquí todas las características de configuración de bloqueos, de integridad de código, bloqueos, características como Control Front, etc.

Y puedo definir todas estas características si quiero que estén encendidas y sobrescriban la configuración que tengo por defecto para el resto del dispositivo, para el resto de programas o para la configuración que tiene por defecto el sistema.

Finalmente tenemos lo que sería la parte de configuración del dispositivo, la configuración de seguridad del dispositivo, que lo que va a hacer es que vamos a tener diferentes tecnologías basadas en partes del hardware del dispositivo.

Aislamiento del Core Nosotros ponemos aquí habilitarlo si es compatible con el sistema.

Veis que lo que hace es verificar la compatibilidad del hardware.

En este caso como estamos en una máquina virtual, puede darse el caso de que el hardware no sea compatible, pero no es compatible porque es una máquina virtual, porque no haya una compatibilidad con el procesador real.

Tendríamos aquí información sobre lo que sería la parte del procesador arranque seguro y después tendríamos aquí la parte de el cifrado de datos, de tal forma que nosotros podríamos entrar en la parte de cifrado de datos y utilizar BitLocker para la parte de cifrado tanto de aquellos volúmenes donde nosotros tengamos datos como aquellos volúmenes de la parte de sistema.

Aparte, cuando nosotros ciframos el volumen de sistema, bitlocker va a proteger también el sistema de arranque para que una serie de archivos que se cargan antes del sistema operativo no se puedan modificar.

Para esto necesitamos compatibilidad con el chip criptográfico o chip TPM del hardware del dispositivo.

Generalmente en los dispositivos modernos suele venir integrado en todos los dispositivos.

Luego tendríamos aquí otras características como sería el historial de protección, las opciones de control parental por ejemplo, o información sobre el estado de salud del dispositivo.

Como hemos podido ver Windows en sus últimas versiones trae integrado un software de protección contra malware y actividad maliciosa que es muy completo, que tiene un amplio abanico de solución para diferentes problemas de malware o de ataques sobre el sistema y que nos va a permitir protegernos contra ransomware, otro tipo de virus, analizar el dispositivo, protección de identidades y de cuentas, protección del navegador, protección contra aplicaciones, protección del propio hardware cifrado, etc.

Con esto llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.