

10

FORMAS DE USAR DISPOSITIVOS EXTRAÍBLES DE MANERA SEGURA

Las organizaciones adoptan políticas de Bring Your Own Device (**BYOD**) para permitir una mejor flexibilidad en el trabajo para los empleados, pero corren el riesgo de abrir puertas para el malware alojado en USB y las transferencias no autorizadas de archivos. Por tanto, no sorprende que **Ponemon Institute** encontrara que **67%** de los profesionales cree que BYOD ha disminuido su nivel de seguridad. No obstante, hay métodos alternativos para proteger dispositivos de almacenamiento extraíbles o periféricos y usarlos eficientemente y con un mínimo de riesgos. Algunos indicios del uso protegido de dispositivos extraíbles incluyen los siguientes:

1



Definir una política de seguridad de BYOD

Trace e implemente una política para gestionar el uso de memorias USB y otros dispositivos extraíbles, enfocándose en reglas que se deben seguir y en la aprobación de los empleados.

82% de las compañías habilitan activamente BYOD.

Permitir solo dispositivos protegidos

Autorice solo el uso de dispositivos protegidos, como memorias USB con autenticación con huella o protección con contraseña.



2

37% de las amenazas cibernéticas están enfocadas en medios extraíbles.

3



Proteger las memorias USB con contraseñas

Proteja las memorias flash con contraseñas para eliminar las amenazas de intrusos mediante USB y garantice que los datos robados no conlleven una violación.

28% de los ataques cibernéticos en endpoints en 2020 involucraron dispositivos comprometidos o robados.

Controlar el acceso de los usuarios

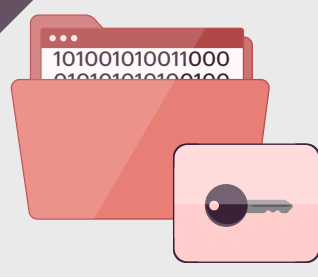
Utilice un **software para la prevención de pérdidas de datos (DLP)** para controlar el nivel de acceso que los usuarios pueden ejercer. Por ejemplo, permita que los usuarios solo lean archivos dentro de memorias USB y bloquee las acciones de modificación o ejecución de aplicaciones.



4

51% de los profesionales sienten que el acceso no autorizado a datos y sistemas es una de las cuatro principales amenazas.

5



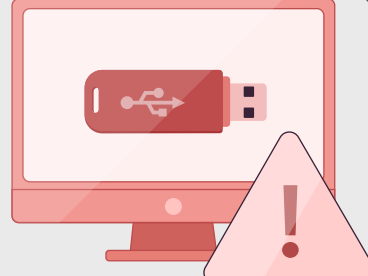
Exigir la codificación de los datos

Solicite a los usuarios codificar los datos almacenados o compartidos mediante dispositivos de almacenamiento extraíbles para disminuir las consecuencias de amenazas o pérdidas. Mantenga varias copias de seguridad de los datos, en la nube y fuera de línea.

56% de las compañías pudieron recuperar los datos desde las copias de seguridad en lugar de pagar rescates.

Bloquear las USB no autorizadas

Permita solo dispositivos USB aceptados o reconocidos por el equipo de seguridad de TI. Bloquee otros dispositivos USB que puedan ser maliciosos, o conectados por usuarios, con una **solución de DLP**.



6

22% de las compañías detectaron malware descargado de dispositivos no gestionados.

7



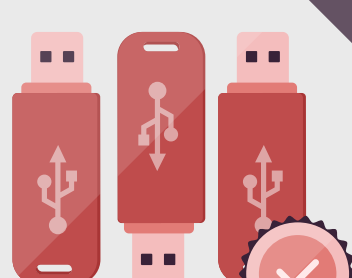
Auditar los eventos de copiado de archivos

Supervise a los usuarios que copiaron archivos sensibles para detener de inmediato una posible violación. Bloquee acciones cuando sea necesario para evitar que los usuarios intenten transferir archivos a dispositivos USB con un **software para prevenir la copia de archivos**.

45% de los empleados han admitido compartir documentos laborales a cuentas personales antes de dejar un trabajo.

Mantener USB oficiales

Use dispositivos provistos por la organización. Garantice que cuando se usen de nuevo los dispositivos estos no contengan ninguno de los archivos previos almacenados o compartidos.



8

82% de las organizaciones no pueden garantizar la detección de amenazas internas desde los dispositivos personales de empleados.

9



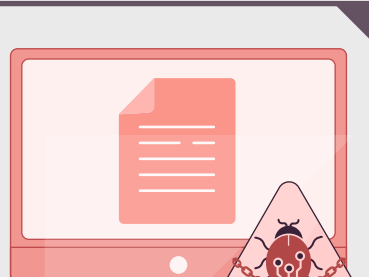
Autorizar a los usuarios correctos

Revise periódicamente los permisos de archivos y revoke los privilegios excesivos otorgados a los usuarios. Gestionar meticulosamente los privilegios de los usuarios disminuye las probabilidades de una filtración o robo de datos por parte de un intruso.

66% de las amenazas internas conlleva el abuso de privilegios para acceder de forma ilegítima a sistemas o datos críticos.

Protegerse contra el malware

Implemente sistemas antivirus y de detección de intrusiones para garantizar que los hackers o intrusos no puedan usar dispositivos no oficiales para infiltrarse en la red.



10

32% de los que respondieron la encuesta expresaron que su mayor preocupación es el riesgo de infección por malware.

ManageEngine DataSecurity Plus

ManageEngine DataSecurity Plus suministra visibilidad y controles seguridad de los datos detallados en una plataforma. Hágase cargo de la seguridad de los endpoints con la ayuda de informes detallados y funciones personalizables para responder ante alertas y así supervisar y controlar:

- 1 Eventos de copiado y pegado de archivos sensibles desencadenados por las acciones de los usuarios.
- 1 Emails salientes, que podrían ser posibles intentos de exfiltración de datos.
- 1 Memorias USB a las que ingresan los usuarios para leer o modificar archivos o ejecutar aplicaciones dentro de las memorias.
- 1 Posibles actividades de carga o descarga de archivos desde navegadores web.
- 1 Actividades de impresión de archivos dentro de su red.
- 1 Eventos de seguridad de archivos, como cambios en la extensión de los archivos, cambios en la lista de control de acceso al sistema o cambios de propiedad.

Descargue una prueba gratuita completamente funcional.

[Descargar ahora](#)

Programe una demo personalizada: support@datasecurityplus.com