# Las empresas deberían cambiar Windows por el escritorio de Linux

*Tiene perfecto sentido tanto para las empresas como para los entusiastas. Pregúntale a GitLab.*

Por Steven J. Vaughan-Nichols originalmente publicado en idioma inglés en:

`https://www.theregister.com/2022/08/10/opinion_column_drop_windows_for_linux/`

**OPINIÓN.** He estado predicando el evangelio del escritorio (GNU) Linux durante más años de los que algunos de ustedes han estado vivos. Sin embargo, a menos que argumente que el escritorio de Linux incluye teléfonos inteligentes Android y computadoras portátiles ChromeOS, no habrá un año del escritorio de Linux.

Pero debería haberlo. Por ejemplo, como GitLab reveló recientemente en su documento de incorporación para empleados, los empleados pueden ejecutar MacOS y Linux en sus escritorios. ¿Pero Windows? ¡Olvídalo!

**¿Por qué?** GitLab explicó: "Debido al dominio de Microsoft Windows en los sistemas operativos de escritorio, Windows es la plataforma más atacada por *spyware*, virus y *ransomware*".

De hecho, es. Pero el lío de seguridad de Windows nunca ha sido solo porque Windows es más popular. **Yo diría que Windows es inseguro por diseño.**

Windows de hoy todavía se basa en una base de sistema operativo de PC independiente. Nunca tuvo la intención de funcionar en un mundo en red. Por lo tanto, los agujeros de seguridad que existían en la época de **Windows for Workgroups**, 1991, todavía están con nosotros hoy en 2022 y Windows 11.

La mayoría de estos problemas se deben a que Windows tiene comunicaciones entre procesos (IPC) que mueven información de un programa a otro, que no tienen seguridad en su diseño. Windows y sus aplicaciones se basan en estos procedimientos para realizar el trabajo. A lo largo de los años, han incluido bibliotecas de vínculos dinámicos (DLL), extensión de control (OCX) de vinculación e incrustación de objetos (OLE) y ActiveX. No importa cómo se llamen, hacen el mismo trabajo y lo hacen sin tener en cuenta la seguridad.

Para colmo de males, los formatos de datos de Microsoft pueden contener macros de programación. Es por eso que los formatos de Microsoft Office se usan comúnmente para transmitir *malware*. Microsoft finalmente compró una pista de que deberían bloquear Office para que no ejecute macros de forma predeterminada. Quiero decir, esto solo ha sido un gran agujero de seguridad desde que Melissa causó estragos en el mundo de Windows en 1999.

¿Pero adivina que? Demostrando que Microsoft aún no sabe cómo solucionar este problema fundamental de seguridad, el equipo de la sede central de Redmond ha revertido el bloqueo de macros de Office. ¿Por qué? Porque la gente usa esos IPC para hacer el trabajo. Al tener que elegir entre la seguridad y hacer que las aplicaciones funcionen como se espera, Microsoft a menudo elige el *statu quo* inseguro.

Para empeorar las cosas, otro problema con la ascendencia de usuario único de Windows es que el usuario predeterminado de Windows con demasiada frecuencia debe ejecutarse como el administrador de PC todopoderoso. Esto significa, por supuesto, que cuando el malware entra, y lo hará, estropea todo y cualquier cosa en la PC de un usuario.

No todas las versiones de Microsoft son igualmente horribles. Como señalan GitLab y otros, Windows Home Edition es notoriamente difícil de proteger.

Ahora, podría preguntarse, pero ¿Cuál empresa usa Windows Home para trabajar? Los baratos sí. Y, si su gente está trabajando desde casa con sus propias PC, como muchos en estos días, es casi seguro que no estén ejecutando Windows 10 Pro o Windows 10 Enterprise E5. E, incluso si su empresa está reembolsando a sus empleados remotos, ¿Cuál cree usted que comprarán? Como GitLab sabe a su pesar, normalmente comprarán una computadora portátil precargada con Windows Home Edition.

Entonces, en cambio, GitLab exige que sus empleados usen MacOS o una computadora portátil Dell Linux. Como fanático desde hace mucho tiempo de las computadoras portátiles Linux para desarrolladores XPS 13 de Dell, eso funciona para mí. Ahora, no es necesario que ejecute Ubuntu, que es el sistema operativo Dell XPS 13 predeterminado, ya que Dell también es compatible con la estación de trabajo Red Hat Enterprise Linux (RHEL), también un buen sistema operativo de escritorio. O puede optar por Arch Linux, o FreeBSD, o lo que sea, siempre que se actualice y admita activamente.

Pero, lamento decirlo, GitLab no lo admitirá con su escritorio Linux. Tendrás que hacerlo tú mismo. Maldita sea.

Yo y muchos otros usuarios de Linux podemos hacer eso, pero no todos pueden. Entiendo por qué

GitLab lo hace de esta manera. Apoyar a los usuarios finales es costoso. Estoy seguro de que la mayoría de sus usuarios trabajan con Mac.

Pero, digamos que no te has decidido por las Mac, que son, después de todo, caras. Digamos que todavía estás usando Windows. Esa es una apuesta segura. Pero si realmente quieres seguridad y estabilidad, Linux es tu mejor opción. Así que eche usted un vistazo a lo que está pagando por las licencias de Windows, el soporte y sus intentos, a menudo inútiles, de asegurarlo. Luego, mire lo que costaría usar una distribución de Linux compatible con empresas, como RHEL Workstation, Canonical Ubuntu Desktop for the Enterprise o SUSE Linux Enterprise Desktop (SLED).

Lo más probable es que sea más barato optar por Linux. Y no importa cómo resulten los números, puedo garantizarle que será mucho más seguro.

---

*Tiene perfecto sentido tanto para las empresas como para los entusiastas. Pregúntale a GitLab.*

Por Steven J. Vaughan-Nichols originalmente publicado en idioma inglés en:

`https://www.theregister.com/2022/08/10/opinion_column_drop_windows_for_linux/`