HP WOLF SECURITY

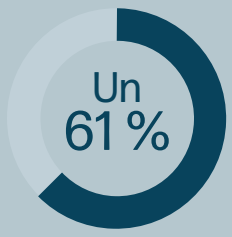
Una nueva era: la protección de los trabajadores híbridos

UN INFORME DE HP WOLF SECURITY

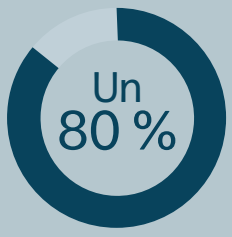
Resumen

Ahora que la mayoría de las organizaciones tiene un programa de trabajo híbrido, ha llegado el momento de evaluar lo que hemos conseguido, así como los desafíos y las oportunidades que se nos presentan.

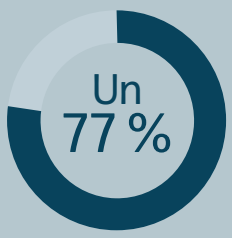
Conforme a los resultados de una encuesta realizada a 984 líderes de IT en Estados Unidos, Reino Unido, Francia, Alemania y Japón:



declara que será aún más difícil proteger a sus empleados híbridos el año que viene.[i]



ha realizado cambios en su estrategia general de ciberseguridad para incluir a los trabajadores híbridos.[i]



coincide en que se acelerarán tanto los ataques cibernéticos como el número de dispositivos de los empleados híbridos.[i]

Sigue leyendo mientras nos sumergimos en los datos y analizamos qué pasos deben adoptar los líderes de IT. Esperamos que este informe te permita, tanto a ti como a tu equipo, comprender los nuevos requisitos del trabajo híbrido y adoptar medidas decisivas.

Desarrollo de una mejor seguridad híbrida

Sección 01

La mejora de la seguridad de los empleados híbridos comienza con una comprensión de todos los riesgos, tanto internos como externos. Sin lugar a duda, estos riesgos se vinculan a los trabajadores remotos y a sus dispositivos.

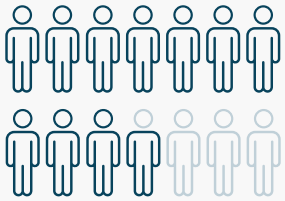
Los encuestados reconocen que existen brechas en lo que respecta a su seguridad. De hecho, es más probable que los líderes de IT detecten más brechas en los empleados híbridos (82 %) que en los empleados de oficina (73 %).[i]

En la encuesta, surgieron dos grandes desafíos que los líderes de IT intentan siempre abordar:

1. LA PROLIFERACIÓN DE DISPOSITIVOS Y SOFTWARE

Un 77 %

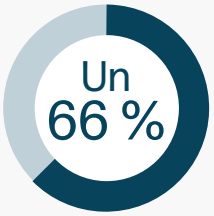
coincide en que los ataques cibernéticos se acelerarán, así como el número de dispositivos.[i]



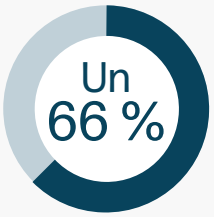
7 de cada **10**

coinciden en que trabajar de forma híbrida aumenta el riesgo de que los empleados pierdan sus dispositivos de trabajo o se los roben.[i]

2. TRABAJADORES FUERA DE LA RED CORPORATIVA



coincide en que el mayor punto débil de la ciberseguridad es la posibilidad de que los empleados híbridos estén en peligro.[i]



declara que es difícil actualizar sus medidas de detección de amenazas (por ejemplo, herramientas EDR y SIEM) para reflejar el comportamiento de los empleados híbridos.[i]

Los líderes han aceptado la realidad del trabajo híbrido en lo que respecta a los dispositivos y ubicaciones de los usuarios, incluso si aún no tienen todas las respuestas. Saben que los dispositivos pueden ser el punto de mira de los ataques y son conscientes de que los trabajadores híbridos fuera de la red corporativa pueden ser la debilidad de los atacantes.

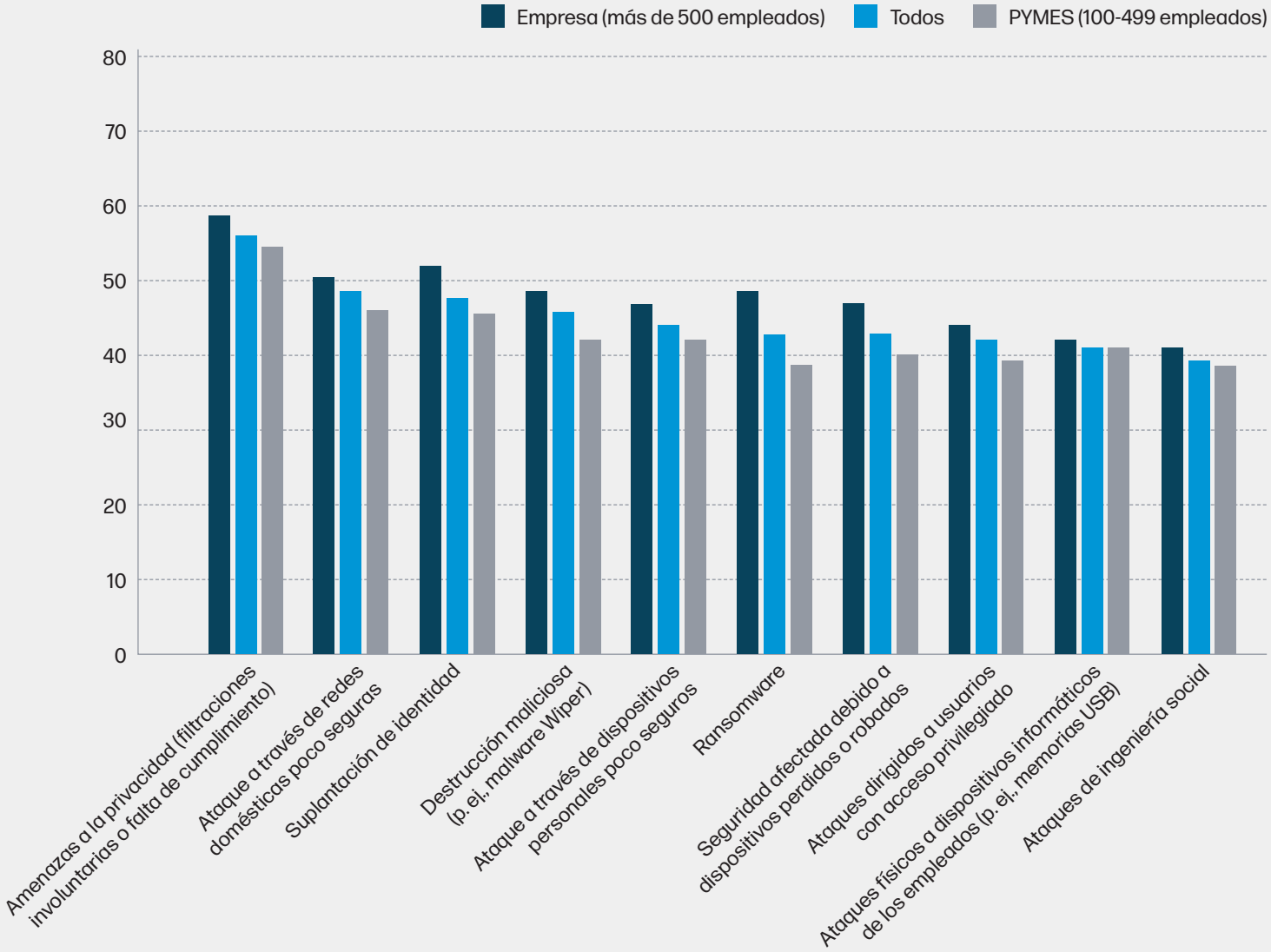
> «Educar a los trabajadores híbridos sobre los riesgos y responsabilidades resulta vital, al igual que lo es la seguridad de los dispositivos. Tecnologías como la microvirtualización son un gran ejemplo. Esta separa las tareas potencialmente peligrosas, como abrir enlaces o archivos adjuntos, del resto del sistema, y garantiza que los atacantes no puedan acceder a datos confidenciales».
>
> Dr. Ian Pratt, director global de seguridad para sistemas personales, HP Inc.

Diversas amenazas con un objetivo común

Además de aceptar los retos organizativos, los líderes son conscientes de la gran variedad de amenazas externas a la seguridad. Y suele coincidir que las más urgentes apuntan de alguna forma a los dispositivos de los empleados.

En lo que respecta a la seguridad en general, las amenazas seleccionadas como motivo de preocupación fueron las siguientes, donde nueve de las diez principales se han relacionado con los dispositivos.

10 AMENAZAS DE SEGURIDAD PRINCIPALES QUE ACTUALMENTE PREOCUPAN A LOS ENCUESTADOS[i]



La importancia del dispositivo

Es evidente que los líderes de IT consideran que las amenazas actuales a los dispositivos son un riesgo continuo y creciente. Las mismas amenazas de dispositivos que actualmente preocupan a los líderes también ocupan un lugar destacado entre las amenazas que se espera que experimentarán sus trabajadores híbridos en los próximos 12 meses. Las más citadas son la suplantación de identidad (33 %), el ransomware (28 %) y los ataques a través de las redes domésticas poco seguras de los empleados (27 %).[i]

Dado que el foco de los ataques se ha alejado de la oficina física y se ha centrado en el usuario final, dondequiera que se encuentre, cualquier solución defensiva también debería centrarse aquí. En la segunda parte de este informe, analizaremos las herramientas que están eligiendo las organizaciones para abordar sus necesidades de seguridad híbrida.

> «La confianza cero es uno de los temas más de moda entre nuestros clientes. Un gran cliente financiero quiere "deshacerse de su red corporativa" por completo. Por ello, observamos un menor enfoque en limitar el acceso a la red y un mayor enfoque en nuevas arquitecturas que permitan la seguridad y la libertad de los trabajadores híbridos».
>
> Alex Thatcher, director de clientes en la nube, HP Inc.

Protección de los trabajadores híbridos en el punto de ataque

Sección 02

Los equipos de IT brindan un servicio de asistencia técnica a una fuerza de trabajo híbrida de éxito. Pero ¿qué tecnologías están implementando para protegerlos de las futuras amenazas híbridas?

En los últimos tres años, los equipos de IT se han convertido en los facilitadores de una fuerza de trabajo productiva, segura y distribuida. El trabajo híbrido se ha convertido en una realidad permanente en muchas organizaciones y a los empleados les encanta el potencial que esto brinda. Sin embargo, todavía queda mucho por hacer.

DIVISIÓN ESTIMADA PROMEDIO DE LA FUERZA LABORAL (USUARIOS DE ORDENADORES)

Siempre trabajan de forma remota[i]: El 23 %

Empleados híbridos[i]: El 36 %

Siempre trabajan en una oficina de la empresa[i]: El 41 %

El 85 % de los empleados está satisfecho trabajando en la oficina, pero también quiere trabajar desde casa al menos dos veces a la semana.[ii]

El 67 % declara que nunca podría haber imaginado ser tan productivo en casa.[iii]

Medidas adoptadas

Después del éxito de la fase de habilitación del trabajo híbrido, el enfoque del departamento de IT consiste en dedicar más recursos e implementar diferentes tácticas para proteger al número creciente de trabajadores híbridos.

- El 82 % declara que ya ha aumentado su presupuesto de ciberseguridad para los trabajadores híbridos.[i]
- El 71 % espera invertir más dinero para la seguridad en general en 2023.[i]
- El 81 % ha implementado un conjunto diferente de herramientas y políticas para proteger a los empleados híbridos.[iv]
- El 80 % ha realizado cambios en su estrategia general de ciberseguridad para dar cabida a los empleados híbridos.[iv]
- El 70 % limita el acceso de los trabajadores remotos a la red corporativa para minimizar el riesgo de una brecha.[iv]

Esta inversión en protección ya está dando sus frutos. En comparación con el año pasado, el 77 % de los líderes de IT coincide en que sus empleados híbridos se están protegiendo mejor de las amenazas de seguridad.[i]

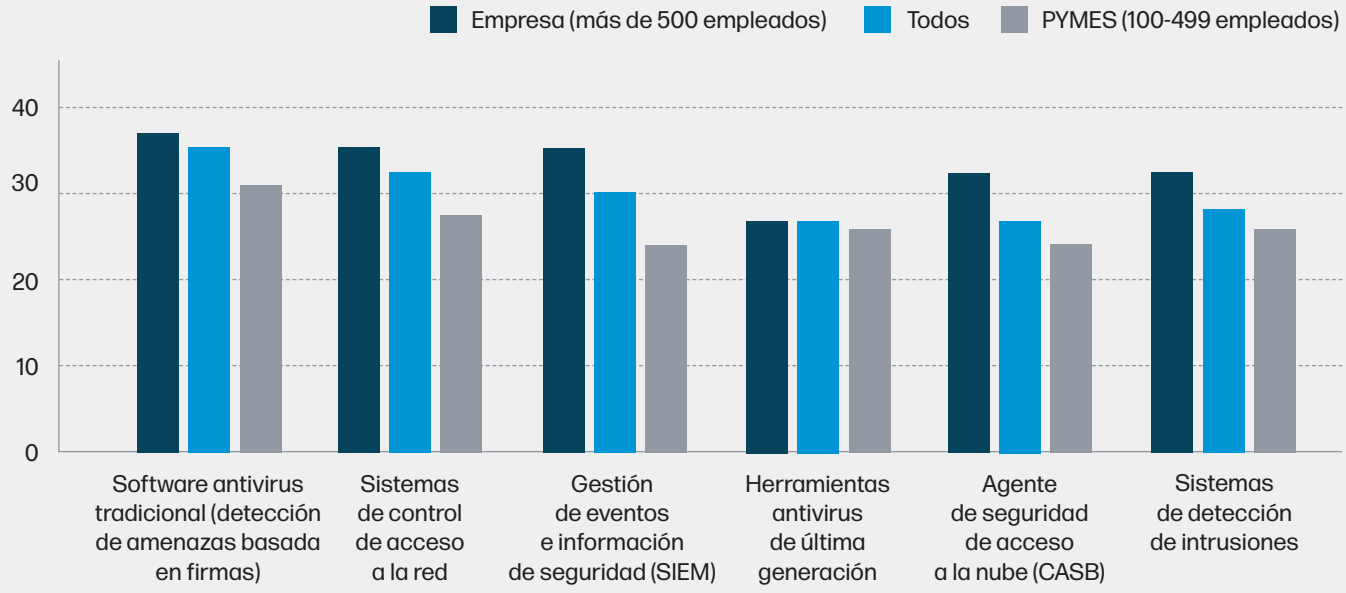
Pero conforme a los retos que los líderes de IT reconocen enseguida, muchos están adoptando medidas adicionales para proteger a sus empleados híbridos.

Implementación de las herramientas adecuadas

La tecnología es lo que realmente facilita el trabajo híbrido, además de desempeñar un papel central como vector de ataque y táctica defensiva. A medida que la fuerza laboral se distribuye cada vez más, la protección del dispositivo (donde ocurren la mayoría de los ataques) debería ser la táctica de defensa principal.

Esto es algo que los líderes de IT están reconociendo. Dos tercios (66 %) de ellos contemplan contemplan la probabilidad de riesgo de los trabajadores híbridos como su mayor punto débil en cuanto a seguridad, por lo que no es de extrañar que muchos de ellos adopten medidas para prevenir y solucionar posibles brechas en el dispositivo.

USO DE HERRAMIENTAS DE CIBERSEGURIDAD ENTRE ORGANIZACIONES DE DISTINTOS TAMAÑOS[i]



Tecnología para proteger a los trabajadores híbridos

Las siguientes tecnologías gozan de una gran popularidad entre los equipos de seguridad. Según algunos estudios, los equipos de IT estaban interesados en aprender más sobre ellas y/o tenían la intención de implementarlas en el futuro.

DISPOSITIVO

Un dispositivo informático remoto conectado a la red que se utiliza generalmente para la interacción del usuario o del entorno (p. ej., un ordenador, una impresora, un móvil o un dispositivo de IoT).

DETECCIÓN Y RESPUESTA DE DISPOSITIVOS (EDR)

Esta tecnología supervisa la actividad del sistema en los dispositivos del usuario, incluidos los ordenadores de sobremesa, ordenadores portátiles y teléfonos móviles, y activa alertas cuando detecta un comportamiento sospechoso. Las soluciones de EDR también pueden adoptar medidas para contener la amenaza y ayudar a los equipos de IT a responder de forma adecuada.

AGENTE DE SEGURIDAD DE ACCESO A LA NUBE (CASB)

Los servicios en la nube son una parte vital de la organización híbrida actual y los CASB facilitan a los equipos de IT la gestión y el control de acceso a los recursos en la nube. Simplifican el acceso de los empleados a los servicios que necesitan, a la vez que restringen el acceso a usuarios no autorizados o malintencionados.

AISLAMIENTO DE APLICACIONES

El aislamiento de aplicaciones protege los dispositivos de amenazas conocidas y desconocidas al aislar las actividades de alto riesgo dentro de los contenedores virtuales temporales. Por ejemplo, suele ser eficaz cuando se trata de proteger a los usuarios que intentan acceder sin querer a contenido malicioso en archivos adjuntos de correo electrónico, enlaces web y descargas de navegadores.

ANTIVIRUS DE ÚLTIMA GENERACIÓN

El software antivirus tradicional se basa en firmas para detectar el malware conocido y ponerlo en cuarentena. El antivirus de última generación utiliza la IA y el aprendizaje automático para identificar comportamientos anómalos en los dispositivos y, de este modo, detener amenazas.

SUPERVISIÓN DE LA INTEGRIDAD DE LOS ARCHIVOS (FIM)

FIM analiza los archivos, sistemas, bases de datos y aplicaciones fundamentales de una organización para verificar si se han modificado, lo cual puede ser una señal de ataque. Si detecta una modificación inesperada, alerta a los equipos de IT para que puedan investigarla.

GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD (SIEM)

Las soluciones SIEM permiten a los equipos de seguridad recopilar datos de diversas fuentes y analizarlos en busca de amenazas de seguridad. Un registro detallado de la información y los eventos también pueden ayudar a gestionar la seguridad (entender dónde asignar los recursos) y demostrar el cumplimiento.

Si bien la mayoría de las tecnologías de la página anterior ya se conocen y se han implementado ampliamente, la tecnología de aislamiento en particular se ha mencionado varias veces en los estudios como una parte importante de las defensas del trabajador híbrido de los encuestados.

Estas herramientas mejoran la resiliencia de una organización al segregar dispositivos, aplicaciones o tareas específicas (como la navegación, el correo electrónico o el procesamiento de textos) de otras partes de la infraestructura de IT. Y los líderes de IT les otorgan cada vez una mayor importancia.

En la actualidad, el 23 % utiliza el aislamiento de aplicaciones para gestionar documentos y enlaces desconocidos y potencialmente dañinos. No obstante, el 32 % tiene la intención de implementar tecnología de aislamiento en los próximos 12 meses y el 76 % lo considera clave para proteger los dispositivos durante el trabajo híbrido.[i]

Las soluciones «silenciosas» prometen

La investigación muestra que los empleados pueden rechazar las medidas de seguridad si se interponen en su camino. Por lo tanto, cualquier protección que los equipos de IT implementen debe ser lo más transparente posible para el usuario final. Según nuestros estudios, el 37 % de los trabajadores de oficina encuestados declara que las políticas y tecnologías de seguridad son demasiado restrictivas, y el 48 % cree que las medidas de seguridad son una pérdida de tiempo.[v]

«El hecho de que los empleados sean conscientes de las mejores prácticas de seguridad es importante, pero la protección incorporada lo es aún más porque el usuario no tiene que pensar en ellas. Sabemos que si la seguridad impide la productividad, los empleados intentarán eludirla. Por consiguiente, cuanto más transparente sea la protección para el usuario, más fructífera será y más fuertes serán las defensas de la empresa».

Robert Masse, miembro de la junta de asesores de seguridad de HP y partner de Deloitte.

Colaboradores del informe

ALEX THATCHER
Director de clientes
en la nube de HP Inc.

DR. IAN PRATT
Director internacional de seguridad
para sistemas personales de HP Inc.

ROBERT MASSE
Miembro de la junta asesora de
seguridad de HP y partner de Deloitte

Acerca de HP Wolf Security

HP Wolf Security forma parte de la cartera de HP de seguridad aplicada por hardware y servicios de seguridad centrados en dispositivos. Se ha diseñado para que las organizaciones puedan proteger los ordenadores, las impresoras y las personas de los depredadores cibernéticos que les rodean.

HP Wolf Security ofrece una protección y resiliencia completas para los dispositivos que comienza a nivel de hardware y se amplía a través del software y los servicios. Visita hp.com/wolf.

Metodología

[i] HP encuestó a 984 líderes de IT en organizaciones híbridas de 100 a 2499 empleados de cinco mercados (Estados Unidos, Reino Unido, Francia, Alemania y Japón) entre julio y agosto de 2022.

El ochenta por ciento de los encuestados son directores o tienen un cargo superior (vicepresidentes y cuerpos directivos). Todos son responsables de los dispositivos, redes, nube o gestión de privacidad, y supervisan un equipo de operaciones de ciberseguridad o hardware y software de IT dentro de su organización.

Las organizaciones híbridas se definen como aquellas que tienen una variedad de empleados que trabajan en la oficina, de forma remota, o una combinación de ambos.

Referencias

[ii] HP, Reino Unido y Estados Unidos, Encuesta de usuarios finales, n=200, julio de 2021.

[iii] HP, Estados Unidos y Reino Unido, n=537 usuarios finales en Estados Unidos y Reino Unido, septiembre de 2020.

[iv] Basado en el porcentaje de encuestados que «están totalmente de acuerdo» o «de acuerdo» con las declaraciones relativas a la protección de los trabajadores híbridos.

[v] HP Wolf Security. (2021). Informe de rebeliones y rechazos de HP Wolf Security. [Online]. Disponible online: https://press.hp.com/content/dam/sites/garage-press/press/press-kits/2021/hp-wolf-security-rebellions-and-rejections/hp-wolf-security-report-rr-final.pdf.

HP Wolf Security for Business requiere Windows 10 u 11 Pro o versiones posteriores, incluye varias funciones de seguridad de HP y se encuentra disponible en productos HP Pro, Elite, TPV retail y estaciones de trabajo. Consulta los datos del producto para conocer las funciones de seguridad que incluye.