[notasdeprensa.jpg](http://www.mexicopress.com.mx)Publicado en Ciudad de México el 04/05/2018

# [8 tips de Avast en el día Mundial de las Contraseñas para mantener la tecnología segura](http://www.notasdeprensa.es)

## Un año después del ciberataque masivo WannaCry, casi un 30% de las computadoras con Windows siguen siendo vulnerables

Con las amenazas cibernéticas, fraudes online y robos de identidad digital en aumento, es ahora más importante que nunca mantener los dispositivos electrónicos y las cuentas en línea tan seguros como sea posible. El día Mundial de las Contraseñas, hoy 3 de mayo, recuerda a las personas estar atentos para hacer que las contraseñas sean más seguras. Sin embargo, el mensaje sobre comprobar contraseñas y cambiarlas regularmente no es suficiente. Cuando se trata de asegurar que el software de los dispositivos esté actualizado con los parches de seguridad más recientes, podría decirse que estamos viendo una `inercia de actualización´ a gran escala. El 12 de mayo de 2018 será un año desde que WannaCry, el ataque de ransomware más grande en la historia, estalló. WannaCry indiscriminadamente afectó a las computadoras de todo el mundo, incluidas aquellas que pertenecían tanto a consumidores, negocios, servicios de salud, como hospitales e inlcuso departamentos de gobierno. A pesar de lo anterior, datos de Avast muestran que el 30% de las computadoras con Windows en México aun se siguen utilizando con la vulnerabilidad establecida un año después. Ya sea tanto con sólidas contraseñas o actualización de sistemas en teléfono móvil, los usuarios deben mejorar al tomar medidas cuando se soliciten y también cuando no, para mantenerse seguros en línea. A continuación, Avast, líder global en productos de seguridad digital, comparte 8 tips para que los usuarios se protejan. Comprobar: El router. Es la puerta de acceso a todos sus dispositivos conectados y podría comprometerlos si la contraseña no es segura. Si un servicio en línea que ha estado utilizando sufrió una violación de datos en el pasado, existe la posibilidad de que la contraseña ya no sea segura, por lo tanto, es primordial el asegurarse de cambiar las contraseñas de todos los dispositivos conectados. Que las actualizaciones de software son realizadas. Asegurarse de que todos los dispositivos conectados a la red doméstica se actualicen, según sea necesario, cuando se emitan los parches de software. Esto incluye cámaras web, juguetes conectados y televisiones inteligentes. Que está instalada una solución antivirus actualizada. Esto detectará y bloqueará malware como ransomware antes de que cause daño. También detectará y removerá amenazas como keylogging, el cual podría rastrear cualquier contraseña que haya creado. Estas amenazas deben recogerse a través de escaneos regulares del software antivirus para ayudar a proteger su dispositivo. Si las contraseñas utilizadas son fáciles de hackear. Elegir una frase memorable o una serie de palabras y agregue caracteres especiales para crear contraseñas únicas y complejas que incluyan números, caracteres y símbolos. Evite combinaciones simples y célebres como usar su nombre, `contraseña´ o `12345´. Cambiar: ¡El parche y los hábitos de actualización! Muchos dispositivos, como computadoras y teléfonos móviles, pueden ejecutar actualizaciones durante la noche por lo cual no hay excusas para “posponer” las actualizaciones hasta el tiempo más conveniente. A menudo las actualizaciones incluyen soluciones a las vulnerabilidades, por lo cual no instalarlas puede ocasionar agujeros de seguridad que los ciberdelincuentes aprovecharán. Las contraseñas de dispositivos y cuentas en línea regularmente. Mucha gente no se da cuenta de que cambiar sus contraseñas de manera regular puede ayudarlos a prevenir los problemas de seguridad más comunes, como fraude cibernético, robo de datos en línea y de identidad, así como hackeo. Cómo guarda las contraseñas. No es recomendable guardar contraseñas en el navegador. Si la computadora es hackeada, entonces los cibercriminales pueden encontrar las contraseñas en el navegador y usarlas para acceder a cuentas en línea. Lo ideal es utilizar un administrador de contraseñas que ayude a crear contraseñas sólidas para todos las cuentas y las almacene de forma segura a través de una contraseña maestra. Cuando se desbloquea, y se haya instalado el complemento del navegador que lo acompaña, la herramienta de administrador de contraseñas autocompletará la información de inicio de sesión siempre que quiera acceder a sus cuentas protegidas. El acceso seguro y utilizar una autentificación de dos pasos para acceder a sitios web si no lo hace actualmente. Por ejemplo, se puede elegir tener un teléfono móvil como segundo nivel de seguridad, de modo que se recibe un código que se tiene que ingresar para verificar las credenciales de acceso. Este paso extra hace más díficil para un tercero acceder a otras cuenta. Avast Software (www.avast.com), líder global en productos de seguridad digital para consumidores y empresas, protege a más de 400 millones de personas en línea. Avast ofrece productos con las marcas Avast y AVG que protegen a los usuarios de amenazas en internet y el escenario de amenazas de Internet de las Cosas que está en constante evolución. La red de detección de amenazas de la empresa está entre las más avanzadas del mundo, y utiliza tecnologías de aprendizaje automático e inteligencia artificial para detectar y detener amenazas en tiempo real. Los productos de seguridad digital Avast para dispositivos móviles, PC o Mac están clasificados como los mejores y certificados por VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs, entre otros. Avast cuenta con el respaldo de CVC Capital Partners y Summit Partners, que son sociedades de inversión de capital privado líderes en el mundo.

**Datos de contacto:**

Flor Carreno

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/8-tips-de-avast-en-el-dia-mundial-de-las](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional E-Commerce Ciberseguridad Ciudad de México Innovación Tecnológica

[notasdeprensa.jpg](http://www.mexicopress.com.mx)

[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)