Publicado en Latam el 28/03/2023

# [5 pasos para fortalecer la seguridad digital](http://www.notasdeprensa.es)

## Según DigiCert los peligros para las computadoras han aumentado con el tiempo, es por ello que es importante que los usuarios se adapten, se actualicen y recuerden algunos consejos que pueden aplicar tanto a computadoras, portátiles, tabletas y teléfonos inteligentes

 En el mundo digital acelerado de hoy, todos los dispositivos conectados juegan un papel vital en la vida diaria. Ya que ayudan a comunicar, administrar las finanzas, almacenar documentos importantes y mucho más. Sin embargo, nunca ha habido más amenazas a la seguridad digital. A medida que aumentan las conexiones en los países latinoamericanos, aumenta el peligro. Según datos de la empresa de seguridad digital Lookout, las plataformas móviles representan un porcentaje importante de los ataques de phishing en la región. Sus datos muestran que Perú y Argentina son los más susceptibles a ataques de esta naturaleza: 60% y 58% de sus usuarios encontraron algún tipo de phishing en sus dispositivos móviles. Le siguen Colombia, Bahamas y Brasil, con 50%, 44% y 41%. Los datos de la Federación Brasileña de Bancos (Febraban) muestran que Brasil registró un aumento del 80 % en los intentos de ataques de phishing destinados al robo financiero en 2021. "Como los peligros para su computadora han aumentado con el tiempo, es importante que el usuario también se adapte. También hay más dispositivos que nunca, así que recuerde que estos mismos consejos se pueden aplicar a su computadora portátil, tableta y teléfono inteligente", aconseja Dean Coclin, director senior de desarrollo empresarial de DigiCert. Como proveedor líder de confianza digital, DigiCert comprende la importancia de proteger sus activos en línea. Es por eso que la compañía ha  elaborado una guía para ayudar a los usuarios a tomar el control de la seguridad de la computadora. 1. Comenzar con una copia de seguridadAntes de comenzar a limpiar la computadora, es esencial hacer una copia de seguridad de los archivos. De esta manera, el usuario puede asegurarse de que todos sus documentos y fotos importantes estén seguros y protegidos. Hay varias formas de hacer una copia de seguridad de los archivos, que incluyen: Discos duros externos: Un disco duro externo es una forma confiable y rentable de hacer una copia de seguridad de los archivos. Simplemente copiar y pegar los archivos en la unidad externa y está listo. Además, la mayoría de los sistemas operativos de las computadoras permiten copias de seguridad automáticas en discos duros externos, lo que facilita el proceso de copia de seguridad. Servicios en la nube: servicios como Google Drive, Dropbox y OneDrive permiten almacenar los archivos en la nube, lo que facilita el acceso a los datos desde cualquier lugar con conexión a Internet. 2. Eliminar programas y archivos no utilizadosUna vez que el usuario haya realizado una copia de seguridad de sus datos, es hora de comenzar a limpiar la computadora. Los archivos y programas adicionales pueden hacer que el sistema se ralentice y obstruya la memoria del dispositivo. ¿Y cómo se aplica esto a la seguridad de la computadora? Eliminando todos los programas y archivos no utilizados que ocupan espacio valioso en el disco duro. Esto incluye: Correos electrónicos Fotos Archivos basura Archivos duplicados Historial del navegador Aplicaciones y programas antiguos que no están en uso Para eliminar archivos y aplicaciones en un Mac: Hacer clic en el icono de Apple en la parte superior izquierda de la pantalla Hacer clic en Acerca de esta Mac > Almacenamiento > Administrar El usuario verá algunas recomendaciones para ahorrar almacenamiento Para eliminar archivos y aplicaciones en Windows: Configuración > Sistema > Almacenamiento Ordenar por los archivos más grandes Elimina archivos que no se necesitan Configuración > Aplicaciones y características Eliminar las aplicaciones que no se necesitan 3. Actualizar el sistema operativo y softwareActualizar el sistema operativo y software es un paso esencial para mantener la seguridad de las computadoras. Las actualizaciones a menudo contienen parches de seguridad críticos y correcciones de errores que ayudan a proteger la computadora contra malware y otras amenazas cibernéticas. Es primordial asegurarse de buscar actualizaciones regularmente e instalarlas tan pronto como estén disponibles. Idealmente, se debe configurar el software y programas para que se actualicen automáticamente. 4. Utilizar contraseñas seguras y MFAFinalmente, asegurarse de usar contraseñas seguras para todas las cuentas y usar la autenticación multifactor (MFA) cuando se pueda. Una contraseña segura debe tener al menos 12 caracteres, contener una combinación de letras mayúsculas y minúsculas, números y caracteres especiales y no debe usarse para más de una cuenta. Se puede usar un administrador de contraseñas, como 1Password, para ayudarlo a crear y almacenar contraseñas seguras y únicas para todas las cuentas en línea. 5. Consejo extra: evita el phishingIndependientemente de mantener el sistema actualizado y establecer contraseñas seguras, si el usuario es víctima de phishing, la computadora y la  identidad en línea aún pueden verse comprometidas.

**Datos de contacto:**

DigiCert Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/5-pasos-para-fortalecer-la-seguridad-digital\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Telecomunicaciones Programación Software Ciberseguridad Dispositivos móviles



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