# Cómo ‘desintoxicar’ tus datos para lograr seguridad digital

01/01/2020

En la gran mayoría de páginas web, servicios o aplicaciones los usuarios tienen que introducir una serie de datos personales que, de no protegerse adecuadamente, luego deambulan por Internet al alcance de cualquiera.

Por mucho cuidado que se tenga a la hora de proteger los datos personales es prácticamente imposible mantener una seguridad digital completa. Cada vez que se abre una nueva cuenta o perfil en un servicio, datos personales como nombre, correo electrónico o el número de tarjeta de crédito, entre otros, son requeridos.

Aunque se cambie de aplicaciones y páginas webs, aquellas que han sido utilizadas anteriormente siguen teniendo los datos personales de sus usuarios guardados en la Red. Esto hace que los datos no estén seguros y puedan sufrir algún tipo de ataque que exponga sus datos. Por ello, cabe tener en cuenta una serie de pasos para proteger la información personal de la mejor manera posible.

Los primero es hacer una limpieza de aplicaciones. Seguramente en los teléfonos móviles haya aplicaciones que ya no se usan. Estas ‘apps’ no solo ocupan espacio en el dispositivo, sino que recopilan una gran cantidad de información sobre el usuario.

Muchas de estas aplicaciones tienen permiso para acceder a distintas funciones del teléfono que no deberían tener, como el micrófono, la cámara o la ubicación. Además es recomendable también revisar aquellas ‘apps’ que sí utilizamos para ver a qué están accediendo exactamente y si no acaba de convencer, siempre se pueden revocar estos permisos o buscar aplicaciones

alternativas que sean menos invasivas con la privacidad.

Ubicación, contraseñas, redes sociales…
La ubicación del usuario es un tema delicado, pues no hay muchas razones para que el teléfono transmita constantemente la ubicación. Al rastrear los movimientos, esta función recopila información como los recorridos regulares del usuario, dónde trabaja, dónde va a comprar o dónde vive.

Es posible que la función de ubicación no este activa en todos los servicios, pero para asegurarse que dicha información no se quede en la Red, es recomendable desactivar la función en todo el teléfono y solo encenderla cuando sea necesario. Google, por ejemplo, permite gestionar la información de localización que el usuario quiere que guarde -o desactivar esta recopilación de datos-.

El administrador de contraseñas favorece enormemente la higiene cibernética. Uno de los mayores peligros de hoy en día es que la gente utiliza la misma contraseña para todo, haciendo que si alguien la descubre pueda acceder a la mayoría de las cuentas de las que dispone el usuario en servicios como Facebook, Netflix o Amazon.

El administrador de contraseñas se ocupa de administrar todas las contraseñas además de añadir contraseñas seguras encriptadas. Lo único que tiene que hacer el usuario es acordarse de la contraseña maestra que abre esta ‘app’.

Por último hay que limpiar las redes sociales. Estas plataformas son las que más datos personales recogen. Las empresas de redes sociales llegan a crear un perfil bastante preciso recopilando toda la información que tienen de sus usuarios.

Las aplicaciones de redes sociales suelen demandar muchos permisos de acceso a funciones del teléfono -micrófono, agenda, cámara, etc.-. Una forma de minimizarlo es acceder a la plataforma a través de la versión web para móvil.

No obstante, algunas aplicaciones, como las de Facebook, ofrecen en el móvil servicios que en la versión web no tienen, como comprobar los mensajes privados -obliga a instalar Messenger-. Por ello, y para quienes no quieran desintalar estas ‘apps’, es importante actualizar los permisos que tiene la aplicación, como el de rastreo de la actividad en la web, otra de las medidas es cambiar la configuración de privacidad.

Por último es importante no usar una de las cuentas de redes sociales para iniciar sesión en otros sitios, ya que esto proporciona muchísima más información personal de la que las compañías necesitan. Por ello, aunque sea más lento y menos cómodo, conviene crear cuentas separadas para cada servicio, con sus respectivas contraseñas -o recurriendo al gestor de contraseñas antes mencionado-.