



RECOMIENDA INAI PROTEGER DISPOSITIVOS MÓVILES PARA EVITAR RIESGOS DE VULNERACIÓN EN INFORMACIÓN ALMACENADA

Ciudad de México.
24 de julio de 2021

www.inai.org.mx



- El Instituto comparte algunos consejos que la población puede poner en práctica para dar seguridad a la información contenida en los equipos con los que se conectan a Internet

RECOMIENDA INAI PROTEGER DISPOSITIVOS MÓVILES PARA EVITAR RIESGOS DE VULNERACIÓN EN INFORMACIÓN ALMACENADA

El aumento en el uso de los dispositivos móviles implica tomar medidas de seguridad para proteger la información de las personas usuarias contenida en esos aparatos que, por estar conectados a Internet, presentan mayor riesgo de ser vulnerados.

Información del 17° [Estudio sobre los Hábitos de los Usuarios de Internet en México](#), 2021, de la Asociación de Internet MX, revela que el *smartphone* es el dispositivo más utilizado por la población, al registrar 92 por ciento de las preferencias, seguido por la computadora con un 45.2 por ciento, y la tableta, con 14.4 por ciento.

Debido a la relevancia que tiene que las personas usuarias comprendan la importancia de proteger sus dispositivos móviles, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) publica los siguientes consejos:

- Evitar hacer transacciones o compras en línea conectado a una red pública. No intercambiar información privada o confidencial, ni conectarse al servicio de banca en línea.
- Extremar precauciones si es necesario conectarse a redes Wifi públicas que permiten a cualquier usuario acceder sin necesidad de identificarse o de una contraseña.
- Utilizar contraseñas fuertes mezclando mayúsculas, minúsculas y números.

- Instalar y actualizar un antivirus para detectar aplicaciones y archivos maliciosos.
- Siempre que un servicio lo proporcione, activar la verificación en dos pasos para añadir mayor seguridad.
- Instalar aplicaciones seguras desde sitios o tiendas oficiales y revisar los permisos de las apps.
- Realizar copias de seguridad en otro soporte para no perder la información almacenada en el dispositivo móvil.
- Utilizar un método de bloqueo de pantalla (código numérico) y cifrar la información para que, si se produce una intrusión, robo o extravío, se dificulte el acceso a la persona que tenga el dispositivo en sus manos.
- Revisar constantemente las aplicaciones que funcionan en segundo plano y que pueden estar haciendo uso de geolocalización (ubicación) a través del GPS.
- Verificar las opciones de configuración de cada red social para tener controlados los principales aspectos de privacidad y seguridad.
- Establecer una contraseña de bloqueo en el smartphone, así se impedirá que lo utilicen sin consentimiento de su propietario.
- Revisar los permisos de alojamiento automático de información en los servicios de la nube.
- Al visitar un sitio, comprobar que realmente es al que se quiere acceder. Poner atención en la URL, preferentemente ésta deberá empezar por *https* y tener el ícono de un candado cerrado.
- Borrar el historial de navegación cuando no se necesite.
- Cerrar siempre la sesión cuando se salga de una página en la que la persona usuaria se haya autenticado con usuario y contraseña, especialmente al usar dispositivos públicos o rentados. Con esta acción se evita que desconocidos que utiliza la computadora o consigan un dispositivo móvil ajeno, accedan a la información personal usando la sesión que quedó abierta.
- Identificar y revisar en los sitios web a los que se accede el aviso de privacidad.
- Si se recibe un mensaje de una red social, banco o cualquier otro servicio conocido, se sugiere no abrirlo, y acceder a su sitio web directamente tecleando la URL desde el navegador.

Para obtener más información sobre la forma de proteger los datos personales y su tratamiento, visitar la página www.inai.org.mx, comunicarse al TEL INAI 800 835 4324 o escribir al correo electrónico atencion@inai.org.mx.

-o0o-



[VER FOTO](#)