Consejos para proteger la información personal al llegar a EEUU

Una de las novedades llegadas al panorama estadounidense con la llegada de **Donald Trump al poder es que en las fronteras estadounidenses** o en alguno de sus aeropuertos, las autoridades de **Aduana y Protección Fronteriza** pueden indagar en los dispositivos de los viajeros, buscar entre todos los archivos y hasta conservar su laptop o su celular para una investigación más precisa, en caso de considerarlo necesario, incluso aunque esto no se fundamente en una sospecha.

Por este motivo, el medio The New York Times ha creado un documento en el que ofrece consejos a los viajeros que lleguen a Estados Unidos para evitar que su información personal y privada pueda ser investigada y **SiliconWeek** te hace un resumen de ello.

Una de las cosas más importantes que destacan, para no tener problemas es el de **no mentir a los agentes sobre las contraseñas o las redes sociales** que el viajero utiliza, para no llegar a parecer sospechoso de algo, de acuerdo con Jeremiah Grossman, el jefe de la estrategia de seguridad para **SentinelOne**, una compañía de seguridad computacional. De todos modos, aquellos que quieran arriesgarse a no ceder su contraseña de alguna de sus cuentas es mejor que digan que no la recuerdan a que aleguen que se niegan a hacerlo. O, incluso, algunos expertos recomiendan crear una muy larga y no memorizarla.

Uno de los consejos es el de **comprar un aparato de bajo costo que no contenga información personal** y dejar en casa el equipo costoso donde están descargadas las aplicaciones de redes sociales a las que accede el usuario. Otra idea es la de desconectar el lector de huella digital que viene en algunos dispositivos disponibles en el mercado. **¿La razón?** "Las fuerzas policiales han utilizado con éxito órdenes judiciales para obligar a la gente a desbloquear sus teléfonos con su huella digital. No obstante, gracias a tener el derecho a permanecer callado, podría ser difícil (mas no imposible) que el gobierno federal te fuerce a compartir tu contraseña".

Otros de los consejos son uso de la doble verificación, que aporta una protección extra o la encriptación de los aparatos electrónicos pueden también ser de utilidad para contar con una mayor protección de la información personal guardada en los dispositivos. Otra opción es hacer un respaldo en la nube de los datos y luego borrarlos en el dispositivo.