

www.mexis.net

f X @ in

3 MITOS SOBRE CIBERSEGURIDAD QUE DEBES DEJAR ATRÁS EN 2025





Cada vez que inicia un año, se abre la posibilidad de concretar nuevas metas en diferentes aspectos de nuestra vida. Sin embargo, son muy pocas las personas que establecen un propósito relacionado con el tema de ciberseguridad.

Hoy en día, la ciberseguridad juega un papel importante en la vida de las personas, sobre todo porque el número de ataques sofisticados van en aumento.

Recientemente, expertos revelaron cuáles son los mitos con los que deberías romper este 2025 en relación con la ciberseguridad, con el fin de proteger de manera adecuada tu privacidad e información personal.

¿Cuáles son los mitos de ciberseguridad que no debo creer en 2025?

Según el estudio "Superstición e inseguridad: cómo se relacionan los usuarios con el mundo digital", existen varias supersticiones relacionadas con el mundo de la **ciberseguridad** y que los usuarios no deben creer para evitar ponerse en riesgo.

En el análisis hecho por los expertos, se identificaron **tres mitos** que están impactando de manera negativa la seguridad de los usuarios. Estos son:

"Mis datos bancarios solo pueden ser robados si alguien tienen mis tarjetas físicas". Según el estudio, al menos 20% de los mexicanos cree que los **ciberdelincuentes** no pueden **robar** su **información bancaria** solo con colocar sus tarjetas de crédito o débito en una cartera especial.

Este es un **"mito peligroso"**, ya que 76% de las personas realiza pagos a través del celular, por lo que es importante proteger sus datos financieros desde sus aplicaciones bancarias.

Si estas apps no están bien protegidas, los **ciberdelincuentes** pueden acceder, además de los números de tarjetas, a otros datos sensibles como contraseñas, direcciones físicas y de correo electrónico, así como a nuestro dinero.

Otro de los mitos que no deben creer los usuarios es que **"no pasa nada si doy clic en los enlaces que recibo por SMS, WhatsApp o correos electrónicos"**.

Según la investigación, 30% de los usuarios cree no existe ningún **riesgo**. Sin embargo, es importante considerar que los **ciberdelincuentes** son cada vez más creativos para "engañar a las personas y robar sus **datos personales**".

En este sentido, es importante evitar dar clic en enlaces enviados por remitentes desconocidos o incluso de contactos que no parecen sospechosos.

Finalmente, el tercer mito que no deben creer los usuarios es el de **"tengo control de los datos que comparto en mis redes sociales por lo que mis datos personales están a salvo"**. El estudio revela que 41% de personas en México hace uso de test virales o minijuegos y publica los resultados en sus perfiles sin pensar en las consecuencias.

Muchos de estos juegos requieren permisos para acceder a la cuenta del usuario y **recopilar datos personales** (nombre, ubicación, correo electrónico y contactos).

Por ello, es importante evitar compartir datos con terceros, es decir, evitar usar este tipo de actividades en redes sociales o tomarte el tiempo necesario para leer las políticas de **privacidad** y revisar los permisos que se brindan.

