



**PREVENIR Y AUTOPROTEGER
LOS DATOS PERSONALES,
ACCIONES INDISPENSABLES
PARA EVITAR LA USURPACIÓN
DE IDENTIDAD: INAI**

Ciudad de México.
3 de agosto de 2022

www.inai.org.mx



- INAI emite recomendaciones para prevenir este delito que preocupa a la población
- Tener cuidado cuando le soliciten información personal por Internet o por teléfono, y estar alerta ante cualquier transacción bancaria inusual, entre los consejos

PREVENIR Y AUTOPROTEGER LOS DATOS PERSONALES, ACCIONES INDISPENSABLES PARA EVITAR LA USURPACIÓN DE IDENTIDAD: INAI

Compartir información sensible en las redes sociales, exponer documentos personales en el automóvil o realizar una transferencia electrónica en una red pública de Internet incrementa significativamente el riesgo de ser víctima de usurpación o robo de identidad, advierte el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Esta práctica implica la obtención y uso no autorizado e ilegal de datos personales, para apropiarse de la identidad de una persona y hacerse pasar por ella frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre.

De acuerdo con la compañía tecnológica [Unisys Security Index](#), la seguridad financiera es la principal preocupación de la población mexicana; 90 por ciento de las personas encuestadas reportó serias preocupaciones por el fraude de tarjetas bancarias, 88 por ciento están muy preocupados por el robo de identidad y 66 por ciento desconfían de los enlaces de los correos electrónicos o mensajes de texto.

En este contexto, la cultura de la prevención y la autoprotección de los datos personales es el camino más eficaz para evitar la usurpación de identidad, por ello, el INAI emite las siguientes recomendaciones para que la sociedad proteja sus datos personales y evite ser víctima de este delito:

1. **Mantener seguros los documentos personales en casa y cuando salga de viaje.** Todos los documentos personales o archivos electrónicos, así como NIP, *password* y claves dinámicas deben conservarse en un lugar seguro, para evitar que personas extrañas tengan acceso a ellos.
2. **Destruir los documentos personales cuando hayan dejado de ser necesarios.** Cerciorarse de destruir perfectamente los documentos que contengan información personal o financiera, o tarjetas de crédito o débito vencidas.
3. **Pensar antes de publicar o compartir información personal.** No compartir ni publicar más de lo necesario y configurar los niveles de privacidad. Nunca enviar claves y NIP por correo electrónico ni compartirlas con nadie.
4. **Proteger la computadora, *smartphone* y *tablet*.** Instalar *software* de seguridad (antivirus) y contraseñas seguras, que no se relacionen con datos personales como fechas de nacimiento, número telefónico o nombres de familiares, y utilizar combinaciones alfanuméricas.
5. **Limitar el número de documentos personales que lleve consigo mismo.** Procurar traer solo aquellos que se vayan a utilizar.
6. **Tener cuidado cuando le soliciten información personal por Internet o por teléfono.** Evita dar datos personales.
7. **Investigar si ha recibido tarjetas de crédito, servicios o artículos que no se hayan solicitado.** Se recomienda estar al pendiente de la correspondencia que haga falta.
8. **Mantenerse alerta ante cualquier transacción bancaria inusual.** Verificar los estados de cuenta y consultar los movimientos para identificar los que no se recuerde haber realizado y revisar el reporte de crédito de manera frecuente.
9. **Procurar tener siempre a la vista la tarjeta de crédito o débito.** Solicite que lo lleven a dónde estén los medios de cobro.
10. **Realizar transacciones seguras.** No utilice equipos públicos para realizar movimientos bancarios o compras por Internet. La información puede quedar grabada en ellos con el uso de un *software* maligno.

En la [Guía para prevenir el robo de identidad](#), edita por el INAI, podrán consultar más información. En caso de ser víctima de este delito, pueden visitar el micrositio del [Identidad Segura](#) donde existe información para saber qué hacer y ante quién acudir.

-o0o-



[VER FOTOGRAFÍA](#)