DECÁLOGO

DE **PROTECCIÓN DE DATOS PERSONALES**

para personas

adultas mayores

inai

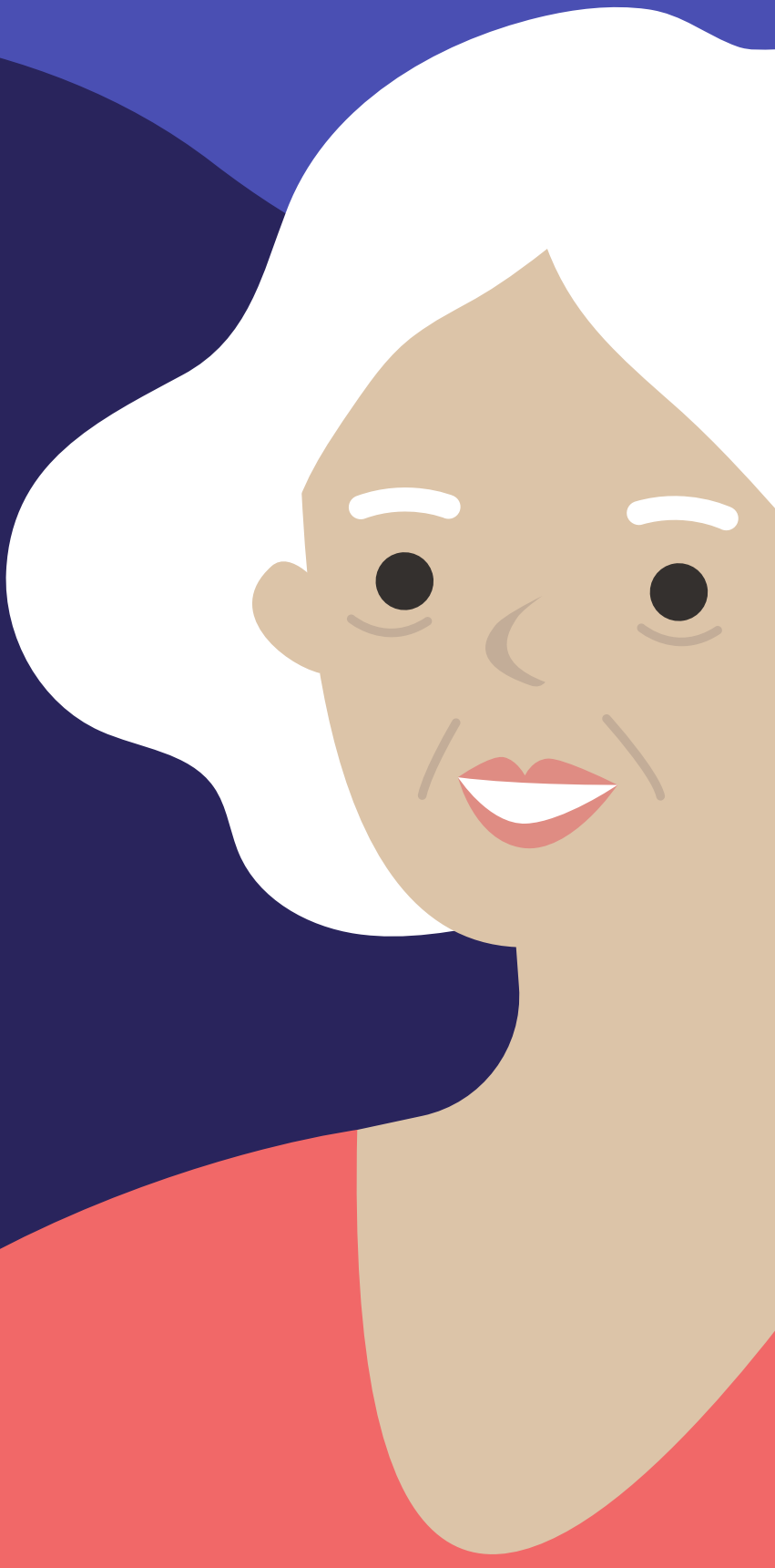
Directorio

Blanca Lilia Ibarra Cadena
Comisionada Presidenta

Adrián Alcalá Méndez
Comisionado

Norma Julieta Del Río Venegas
Comisionada

Josefina Román Vergara
Comisionada



Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Av. Insurgentes Sur 3211,
Col. Insurgentes Cuicuilco,
Alcaldía Coyoacán,
C.P. 04530,
Ciudad de México.

Edición, abril de 2023.

Diseño Gráfico:
María Elena Vargas Zenteno

Índice

Glosario

ADMINISTRADOR DE CONTRASEÑAS	Es un software (programa) que ayuda a las personas usuarias a crear contraseñas seguras, a almacenarlas en una bóveda digital protegida por una única contraseña maestra y luego a recuperarlas cuando sea necesario al iniciar sesión en las cuentas.[1]
ADWARE	Es el nombre que se da a los programas diseñados para mostrar publicidad en tu computadora, redirigir tus solicitudes de búsqueda a sitios web de publicidad y recopilar datos comerciales acerca de ti (como los tipos de sitios web que visitas) para mostrarte avisos personalizados.[2]
ANTIVIRUS	Es un programa que protege su PC, Mac, tableta o teléfono de las amenazas de malware. Estas amenazas cibernéticas pueden presentarse de muchas formas, como adware, spyware, virus, etc. Como pueden dañar su dispositivo o robarle información, es esencial eliminarlas de él.[3]
APLICACIONES	Es un programa informático diseñado como una herramienta para realizar operaciones o funciones específicas. Generalmente, son diseñadas para facilitar ciertas tareas complejas y hacer más sencilla la experiencia informática de las personas.[4]
CARACTERES	Letras, números y signos que puedes utilizar para escribir.
CONTRASEÑAS	Forma de autentificación de un usuario, a través de una clave secreta, para controlar el acceso a algún recurso o herramienta. En caso de que no se proporcione la clave correcta no se permitirá el acceso a dichos elementos.[5]
CUENTA INACTIVA	Cuenta de correo electrónico, de una red social o de cualquier programa informático que no ha sido utilizada por la persona titular durante un período determinado.
DATOS PERSONALES	Los datos personales son cualquier información relativa a una persona física, que la identifica o hace identificable. Es la información que nos describe, que nos da identidad, nos caracteriza y diferencia de otros individuos.

1 Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/protecting-your-data-online-password-manager.

2 Disponible en: https://latam.kaspersky.com/resource-center/threats/adware.

3 Disponible en: https://softwarelab.org/es/que-es-un-antivirus/.

4 Disponible en: https://edu.gcfglobal.org/es/cultura-tecnologica/que-son-las-aplicaciones-o-programas/1/#.

5 Disponible: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf.

DATOS PERSONALES SENSIBLES	Son datos personales que informan sobre los aspectos más íntimos de las personas, y cuyo mal uso pueda provocar discriminaciones o ponerles en grave riesgo, como por ejemplo, el origen racial o étnico; estado de salud (pasado, presente y futuro); información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual.
DIRECCIÓN ELECTRÓNICA	Es el nombre que tienen las página o sitios de internet que se utilizan para localizarlos y acceder a su contenido. Generalmente inician con las letras www.
DISEÑO INTUITIVO	Se centra en la experiencia, se trata de generar un camino de acción sin la necesidad de parar en cada paso para decidir o entender qué hacer. Dirige el camino hacia lo que realmente importa.[6]
DOCUMENTOS ADJUNTOS	Es un documento que se envía junto con un mensaje. Imagina un mensaje escrito en una hoja con un clip que sostiene algunas fotos u otro documento, de esta misma forma puedes enviar archivos adjuntos por correo electrónico.[7]
DOMINIO	Un nombre de dominio (a menudo denominado simplemente dominio) es un nombre fácil de recordar asociado a una dirección [de] Internet. Se trata del nombre único que se muestra después del signo @ en las direcciones de correo y después de www. en las direcciones web.[8]
ENLACE	Texto o imagen resaltado en un documento electrónico que, mediante un clic, permite acceder a información adicional en un mismo o distinto servidor.[9]
ERA DIGITAL	La Era Digital, *Digital Age*, o Sociedad de la Información, es un período en la historia que se considera desde la creación de los dispositivos digitales, asociada a la Revolución Digital (desde la transición de las tecnologías analógicas a las tecnologías digitales, en un período que abarca las décadas del 50 al 70) y se extiende hasta la actualidad. Esta Era supone el uso de las tecnologías de la Información, la expansión de los medios de comunicación, la transformación digital en los sistemas educativos y en la toma de decisiones, la explosión de las redes sociales y un proceso mutuo de enseñanza-aprendizaje de las nuevas formas de la cultura digital a lo largo de la vida.[10]

6 Disponible en: https://www.logorapid.com/branded/diseno-web-intuitivo-como-convertir-tu-website-mas-interactivo/#:~:text=Un%20dise%C3%B1o%20intuitivo%20se%20centra,hacia%20lo%20que%20realmente%20importa.

7 Disponible en: https://edu.gcfglobal.org/es/crear-un-correo-electronico/que-es-un-archivo-adjunto/1/.

8 Disponible en: https://support.google.com/a/answer/2573637?hl=es#:~:text=Un%20nombre%20de%20dominio%20(a,en%20las%20direcciones%20web.

9 Disponible en: https://dle.rae.es/enlace.

10 Disponible en: https://www.edx.org/es/aprende/era-digital.

HISTORIAL DE NAVEGACIÓN O EXPLORACIÓN	Tu historial de exploración o navegación es la información de las páginas de internet que una persona usuaria visita mientras navega por Internet. Entre la información almacenada, se encuentran los formularios y contraseñas que se utilizan para acceder a las páginas de internet.
MALWARE	Es un término que abarca cualquier tipo de *software* (programa) malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. Los delincuentes cibernéticos generalmente lo usan para extraer datos que pueden utilizar como chantaje hacia las víctimas para obtener ganancias financieras. Dichos datos pueden variar desde datos financieros, hasta registros de atención médica, correos electrónicos personales y contraseñas. La variedad de información que puede verse comprometida se ha vuelto ilimitada.[11]
NAVEGAR	Desplazarse a través de una red o de un sistema informático.[12]
PERSONAS CIBERDELINCUENTES	Un ciberdelincuente, también conocido como hacker, es una persona cuyo conocimiento informático le permite realizar acciones delictivas en Internet.[13]
SERVIDOR	Unidad informática que proporciona diversos servicios a computadoras conectadas con ella a través de una red.[14]
SISTEMA INFORMÁTICO	Es el conjunto de partes interrelacionadas, hardware, software y de recurso humano que permite almacenar y procesar información.[15]
SISTEMA OPERATIVO	Es un conjunto de programas que permite manejar la memoria, disco, medios de almacenamiento de información y los diferentes [...] recursos de nuestra computadora, como son el teclado, el mouse, la impresora [...], entre otros.[16]
SITIO WEB O PÁGINA DE INTERNET	Es un conjunto de archivos electrónicos y páginas web referentes a un tema en particular, incluyendo una página inicial de bienvenida generalmente denominada página de inicio o *home page*, a los cuales se puede acceder a través de un nombre de dominio y dirección en Internet específicos.[17]

11 Disponible en: https://www.mcafee.com/es-mx/antivirus/malware.html.

12 Disponible en: https://dle.rae.es/navegar.

13 Disponible en: https://www.universidadviu.com/ec/actualidad/nuestros-expertos/ciberdelincuente-una-nueva-alerta-para-nuestra-seguridad.

14 Disponible en: https://dle.rae.es/servidor.

15 Disponible en: https://sites.google.com/site/pcpi1213informaticamario/home/modulos/2-mantenimiento/1-mantenimiento-de-sistemas-informaticos/1-concepto-de-sistema-informatico.

16 Disponible en: https://desarrollarinclusion.cilsa.org/tecnologia-inclusiva/que-es-un-sistema-operativo/.

17 Disponible en: https://upanama.educativa.org/archivos/repositorio/6000/6126/html/3_qu_es_.htm.

SOFTWARE	Son los programas informáticos que hacen posible la ejecución de tareas específicas dentro de un computador. Por ejemplo, los sistemas operativos, aplicaciones, navegadores web, juegos o programas.[18]
SPYWARE	Software diseñado para recopilar datos de un ordenador u otro dispositivo y reenviarlos a un tercero sin el conocimiento o consentimiento del usuario. Esto a menudo incluye la recopilación de datos confidenciales (como contraseñas, números PIN y números de tarjetas de crédito) [...].[19]
TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)	Son los recursos y herramientas que se utilizan para el proceso, administración y distribución de la información a través de elementos tecnológicos, como: ordenadores, teléfonos, televisores, etc.[20]
VIRTUAL	Que está ubicado o tiene lugar en línea, generalmente a través de internet.[21]
VIRUS INFORMÁTICO	Es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo. Además, está diseñado para propagarse de un equipo a otro.[22]
VULNERACIONES DE DATOS	Pérdida o destrucción no autorizada de los datos personales; el robo, extravío o copia no autorizada de los mismos; su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada.

18 Disponible en: https://edu.gcfglobal.org/es/informatica-basica/que-es-hardware-y-software/1/.

19 Disponible en: https://latam.kaspersky.com/resource-center/threats/spyware.

20 Disponible en: https://www.ulatina.ac.cr/articulos/que-son-las-tic-y-para-que-sirven.

21 Disponible en: https://dle.rae.es/virtual.

22 Disponible en: https://mx.norton.com/blog/malware/what-is-a-computer-virus.

Introducción

En México se considera persona adulta mayor a quien tiene más de 60 años y se refiere a la etapa que suma todas las experiencias de la vida y pasa por la mayoría de las metas familiares, profesionales y sociales. Pero también marca el inicio de una etapa donde las personas presentan condiciones de vulnerabilidad física, social y económica.

De acuerdo con el Instituto Nacional de Estadística y Geografía (INEGI), "para el segundo trimestre de 2022 se estimó que en México residían 17 958 707 personas de 60 años y más (adultas mayores). Lo anterior representa 14 % de la población total del país." De hecho, Julio Alfonso Santaella Castell, quien se desempeñó como presidente de la Junta de Gobierno del INEGI de 2015 a 2021, destacó que "como producto del envejecimiento que está ocurriendo en el país, ahora hay proporcionalmente menos personas jóvenes y proporcionalmente más personas de edades mayores", lo cual, es importante destacar, no es privativo de México.

En los últimos años ha incrementado la cantidad de personas usuarias de Internet, teléfono móvil y otras tecnologías de la comunicación en personas que tienen 55 años o más. Esto, debido a que en la actualidad ha aumentado la diversidad de productos y servicios que se han innovado ejemplo de ello son las modalidades de pagos digitales con la finalidad de evitar las largas filas en sucursales (banco, luz, teléfono, etcétera). Estos servicios e infinidad de productos han evolucionado a formas de actualización denominadas "modernas" gracias al avance de las Tecnologías de la Información y Comunicación (TIC) pues, en conjunto con el Internet, juegan un papel muy importante en la sociedad.

Según el "18º Estudio sobre los Hábitos de los usuarios de Internet en México 2022", el 10.5% de las personas usuarias de Internet tiene una edad entre 55 o más años, cifra que ha ido creciendo en los últimos años.

El uso del Internet hoy en día es capaz de disminuir en gran parte, la imposibilidad de realizar acciones cotidianas por la falta de movilidad, ya que cada vez más servicios son ofrecidos en línea, permitiendo que las personas adultas mayores puedan realizarlos sin moverse de casa. Como ejemplos destaca la posibilidad de comprar artículos, solicitar asistencia médica, contratar un viaje, pedir un documento a una determinada institución, alquilar una película, visitar un museo o una exposición, etcétera.

Por otro lado, para las personas adultas mayores, el uso del teléfono móvil e Internet, juegan un rol importante para la calidad de su envejecimiento ya que les permite interactuar y comunicarse con otros entornos, acceder a información, aumentar su nivel de autoestima, ayudar a la superación del miedo a la soledad y al aislamiento de sus familiares, fomentar las relaciones intergeneracionales, entre otras.

En el caso específico del aislamiento social derivado de la pandemia por la COVID-19, por mencionar un ejemplo, ha quedado demostrado que el uso de las TIC es indispensable para obtener servicios que, normalmente, se realizarían de manera presencial, incluyendo aquellos que, para otorgarse, requieren del registro de datos personales y datos personales sensibles. Es así como las personas adultas mayores han tenido que recurrir a las tecnologías para demandar, vía electrónica, servicios de salud como la vacuna contra la COVID-19, insumos y medicamentos, así como para obtener recursos económicos para subsistir. Por lo general, y como consecuencia de la brecha digital, la mayoría de las personas adultas mayores desconocen los riesgos a los que quedan expuestos sus datos personales que son tratados mediante computadoras, teléfonos inteligentes o cualquier otro dispositivo electrónico.

En este mismo contexto, se ha advertido que las personas adultas mayores se sienten incómodas al usar internet para agendar una cita para una prueba de COVID-19 o para vacunarse, lo cual se debe, en gran medida, al desconocimiento de las TIC y a las preocupaciones por los riesgos inherentes a su uso.

Por lo anterior, resulta necesario que las familias y personas más allegadas a las personas adultas mayores mantengan una comunicación constante para asesorarlos sobre las TIC y la protección de datos personales, de manera que estén conscientes de sus beneficios, pero sobre todo de los riesgos que conlleva su utilización, especialmente cuando se ven involucrados datos personales. Por ejemplo, una persona de menor edad puede leerles los avisos de privacidad antes de que proporcionen sus datos personales o ayudarles a configurar sus dispositivos electrónicos para que cuenten con las medidas de seguridad más robustas. También se puede apoyarlas guardando sus contraseñas para acceder a dispositivos, redes sociales y correos electrónicos y ayudándoles a cambiarlas con cierta periodicidad. En el caso del correo electrónico, por mencionar un último ejemplo, se puede tener acceso a sus cuentas para ayudarles a eliminar aquellos mensajes maliciosos o que provienen de fuentes no confiables.

No cabe duda de que las TIC han mejorado la calidad y condiciones de vida de la sociedad en general. No obstante, aunado a sus bondades, su desarrollo lleva implícitos retos para la privacidad y la protección de datos personales, derivado del uso intensivo que se le da a la información personal a través de herramientas tecnológicas como el Internet, redes sociales, teléfonos celulares inteligentes (smartphones), conversaciones en línea, entre otros.

Si bien es cierto que destacan las ventajas y facilidades que aporta el uso del Internet y las nuevas tecnologías a las personas adultas mayores, también debe considerarse el impacto respecto a su privacidad y la protección de sus datos personales.

Las personas adultas mayores, al igual que el resto de la sociedad, deben: estar al tanto del momento en que les sea requerido cualquier tipo de dato personal; conocer en qué términos y condiciones se desarrollará el tratamiento de esos datos; quién los usará, para qué y durante cuánto tiempo; o si serán compartidos con terceros. Sobre todo, deben estar al tanto de los posibles usos que pueden generarse con posterioridad debido al uso de información captada por los dispositivos.

Dicho esto, resulta preciso que las personas adultas mayores conozcan los principales riesgos a su privacidad derivados del mal uso de sus datos personales, tales como:

- **Usurpación de identidad** para obtener beneficios que les corresponden por ser personas adultas mayores.
- **Divulgación no autorizada de sus datos personales**, como correos electrónicos y números de teléfono, para fines de mercadeo y venta de productos dirigidos a las personas adultas mayores.
- **Uso indebido de datos personales**, como la información financiera, para acceder a las cuentas bancarias, incluyendo la Pensión Universal para Personas Adultas Mayores.

Pero también es fundamental que tengan a la mano un documento con un lenguaje sencillo que les proporcione recomendaciones generales, pero con una explicación detallada, que les permita reducir considerablemente la posibilidad de ser víctimas de vulneraciones de datos y de delitos conexos como el fraude y la usurpación de identidad.

Estos argumentos subyacen a la idea del INAI de presentar este Decálogo que, sin duda, será muy útil para contribuir al logro de uno de sus objetivos: contribuir a la consolidación de una cultura de privacidad y protección de datos personales en México.

Objetivo general

Presentar **diez recomendaciones dirigidas a las personas adultas mayores** para ayudarles a disminuir el riesgo de ser víctimas de vulneraciones de datos, así como de delitos conexos como fraudes y usurpación de identidad.

DECÁLOGO

1

Solicita apoyo de personas de confianza cuando necesites realizar algún trámite en físico o de manera virtual

Actualmente es posible realizar casi cualquier trámite de manera digital, y desafortunadamente las personas adultas mayores enfrentan diferentes obstáculos con la implementación de la tecnología para hacer sus trámites personales. Es por lo que, normalmente recurren a alguna persona para pedir ayuda; sin embargo, es fundamental que se trate de alguien de confianza ya que tratarán sus datos personales.

Así que, si **necesitas ayuda para realizar algún trámite físico o por internet**, es importante que sigas las siguientes recomendaciones:

Identifica a las personas de confianza: busca personas en tu entorno que puedan ayudarte con los trámites, como familiares, amigas y amigos, vecinas y vecinos, etcétera. Asegúrate que sean personas de tu absoluta confianza porque manejarán tu información personal.

Explica tus necesidades: comunica claramente cuál es el trámite que necesitas realizar y qué tipo de ayuda necesitas. Es importante ser específico y asegurarse de que la otra persona entienda lo que requieres.

Proporciona la información necesaria: si la persona de confianza necesita información adicional para poder ayudarte, asegúrate de proporcionarla. Si se trata de un trámite en línea, es probable que necesiten acceso a tu correo electrónico, contraseña u otra información personal. Verifica que la información que compartes sea correcta.

Asegúrate de conocer el trámite que vas a realizar: Si se trata de un trámite importante, infórmate sobre el el procedimiento para realizarlo de manera correcta y, de este modo, proporcionar la información personal que resulte necesaria. Se sugiere comunicarse con una entidad oficial para verificar que todo se está realizando correctamente.

En resumen, al solicitar apoyo de personas de confianza para realizar trámites en físico o de manera virtual, es importante identificar a las personas adecuadas, comunicar claramente tus necesidades y planificar el proceso de manera efectiva. Además, asegúrate de que se esté realizando de manera legal.

DECÁLOGO

2

Utiliza contraseñas difíciles para proteger tus dispositivos electrónicos, redes sociales y correos electrónicos

Actualmente es necesaria la creación de contraseñas difíciles y seguras, pues es esencial para poder proteger tus dispositivos electrónicos, el acceso a tus redes sociales y correos electrónicos. Una contraseña segura puede prevenir la exposición no autorizada de tu información personal y reducir el riesgo de un fraude en línea o de cualquier otro delito derivado de una vulneración de datos.

Al ser tu contraseña uno de los datos más importante que tienes que conservar para poder acceder a tus servicios en línea te presentamos las siguientes recomendaciones para generar una contraseña segura, pero que también sea fácil de recordar.

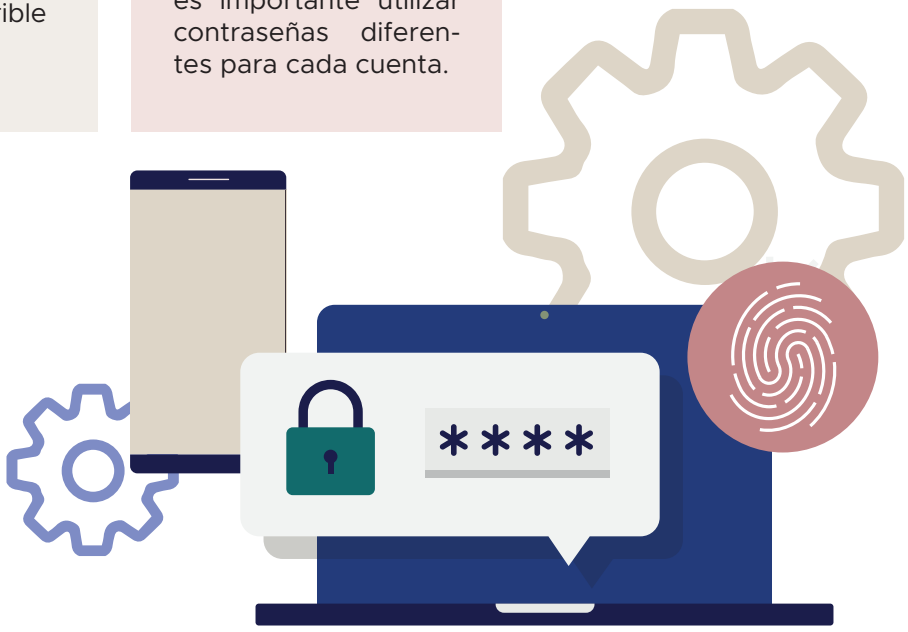
Utiliza una combinación de letras mayúsculas y minúsculas, números y símbolos: una contraseña que contenga una mezcla de estos elementos es más difícil de adivinar y más resistente a los ataques de ciberdelincuentes.

Evita palabras comunes o frases simples: las contraseñas que contienen palabras comunes o frases simples son más fáciles de adivinar. En su lugar, utilizar palabras que no están en el diccionario, abreviaturas o combinaciones de palabras puede reducir enormemente el riesgo de que alguna persona la adivine y utilice. Sin embargo, ya que una contraseña compleja es más fácil de olvidar también podrías recurrir a palabras especiales como el nombre de tu mascota o tu ciudad natal, pero agregando números, combinación de mayúsculas y minúsculas. Quizás de esta manera sea más sencillo recordarla.

Digamos que tienes un perro que se llama “Demóstenes”. Siguiendo lo referido en el párrafo anterior, cambiaríamos la letra “e” por “3” y la “o” por un “0” y al final le agregamos el símbolo de porcentaje, quedando así “**D3m0st3n3s%**”. Este ejemplo es una contraseña segura con 11 caracteres.

Mantén una longitud adecuada: una contraseña larga es más difícil de adivinar o deducir que una contraseña corta. Se recomienda que la contraseña tenga al menos 8 caracteres o, de ser preferible más de 12.

Evita utilizar la misma contraseña en diferentes cuentas: si una contraseña es descubierta por un atacante, todas las cuentas que comparten esa contraseña estarán en riesgo. Por lo tanto, es importante utilizar contraseñas diferentes para cada cuenta.



Utiliza un administrador de contraseñas: puedes utilizar un administrador de contraseñas para almacenar y generar contraseñas seguras. Esto te ayudará a recordar las contraseñas y a mantener su seguridad en línea. En la actualidad hay diferentes gestores que te pueden ayudar, como los instalados en los dispositivos Apple o Samsung. En este caso, solo debes aceptar su uso con tu huella dactilar, reconocimiento facial o tecleando una sola contraseña.

Al seguir estos pasos puedes crear contraseñas seguras que te ayuden a proteger tus dispositivos electrónicos, redes sociales y correos electrónicos de posibles ataques y amenazas en línea.

DECÁLOGO

3

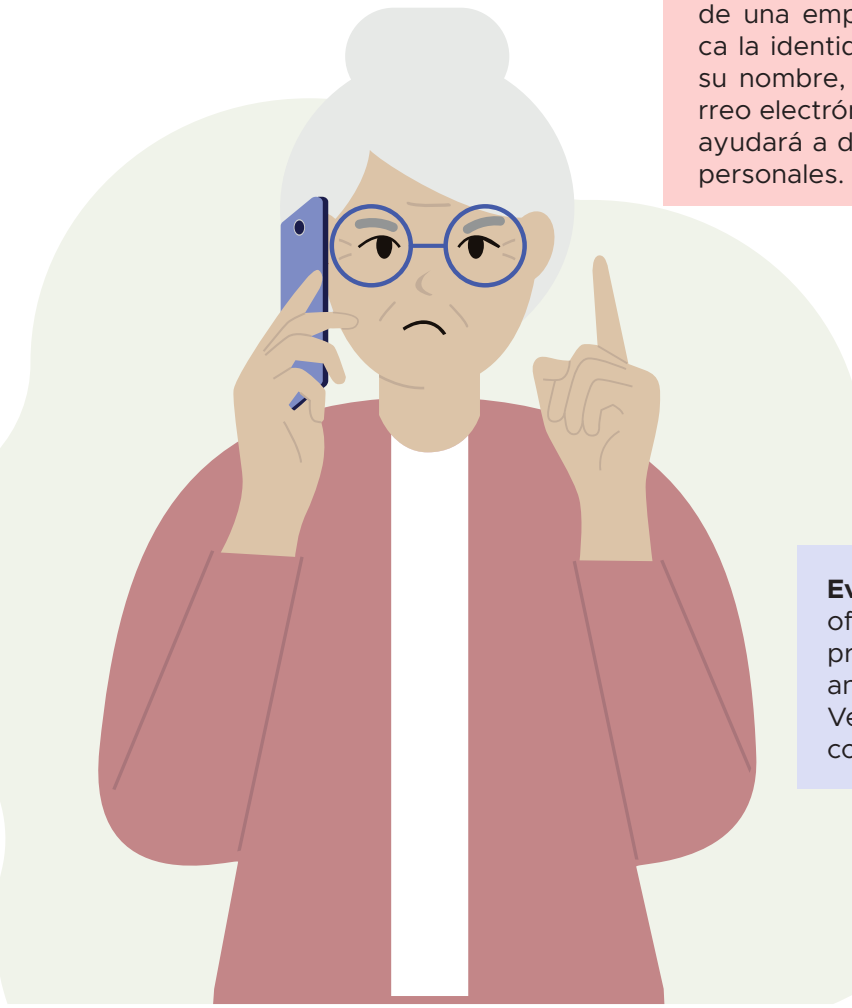
Evita proporcionar tus datos personales a través de llamadas telefónicas

La delincuencia ha evolucionado constantemente, buscando en todo momento aprovecharse del desconocimiento de los nuevos sistemas digitales. Es así como resulta importante que te protejas de posibles estafas telefónicas en las que te solicitan información personal, la cual se puede utilizar posteriormente para vaciar tus cuentas bancarias o incluso usurpar tu identidad.

Es importante que **no proporciones tus datos personales a través de estas llamadas telefónicas**, hechas por ciberdelincuentes, por lo que aquí te dejamos unas recomendaciones que podrán ayudarte a identificar y denunciar estas llamadas.

Evita responder llamadas de números desconocidos: si recibes una llamada de un número que no reconoces, no respondas. Si es importante, dejarán un mensaje y podrás decidir si es necesario regresar la llamada.

Recuerda no compartir información personal: si recibes una llamada en la que te solicitan información personal, haz caso omiso. No compartas información de identificación personal, como números de Seguridad Social, números de tarjetas de crédito o información bancaria.



Verifica la fuente de la llamada: si la llamada es de una empresa o agencia gubernamental, verifica la identidad de la persona que llama. Pregunta su nombre, número de teléfono, dirección de correo electrónico y de qué organización son. Esto te ayudará a decidir si es seguro compartir tus datos personales.

Desconfía de las llamadas de emergencia: ten cuidado con las llamadas que informan emergencias o situaciones de crisis. Quienes delinquen o estafan pueden utilizar estas llamadas para tratar de obtener información personal, aprovechándose de los nervios y el miedo que generan este tipo de situaciones.

Evita aceptar ofertas inesperadas: si te ofrecen algo que no esperabas, como un premio o un descuento, piensa dos veces antes de proporcionar información personal. Verifica la autenticidad de la oferta antes de compartir tus datos.

Cuelga y llama a la entidad: si tienes alguna duda sobre la autenticidad de una llamada, cuelga y llama a la entidad o empresa directamente para verificar la información.

Estos consejos te pueden ayudar a que no seas víctima de la ciberdelincuencia y a protegerte de posibles estafas telefónicas.

DECÁLOGO

4

Dedica unos minutos para leer el aviso de privacidad antes de proporcionar cualquier dato personal

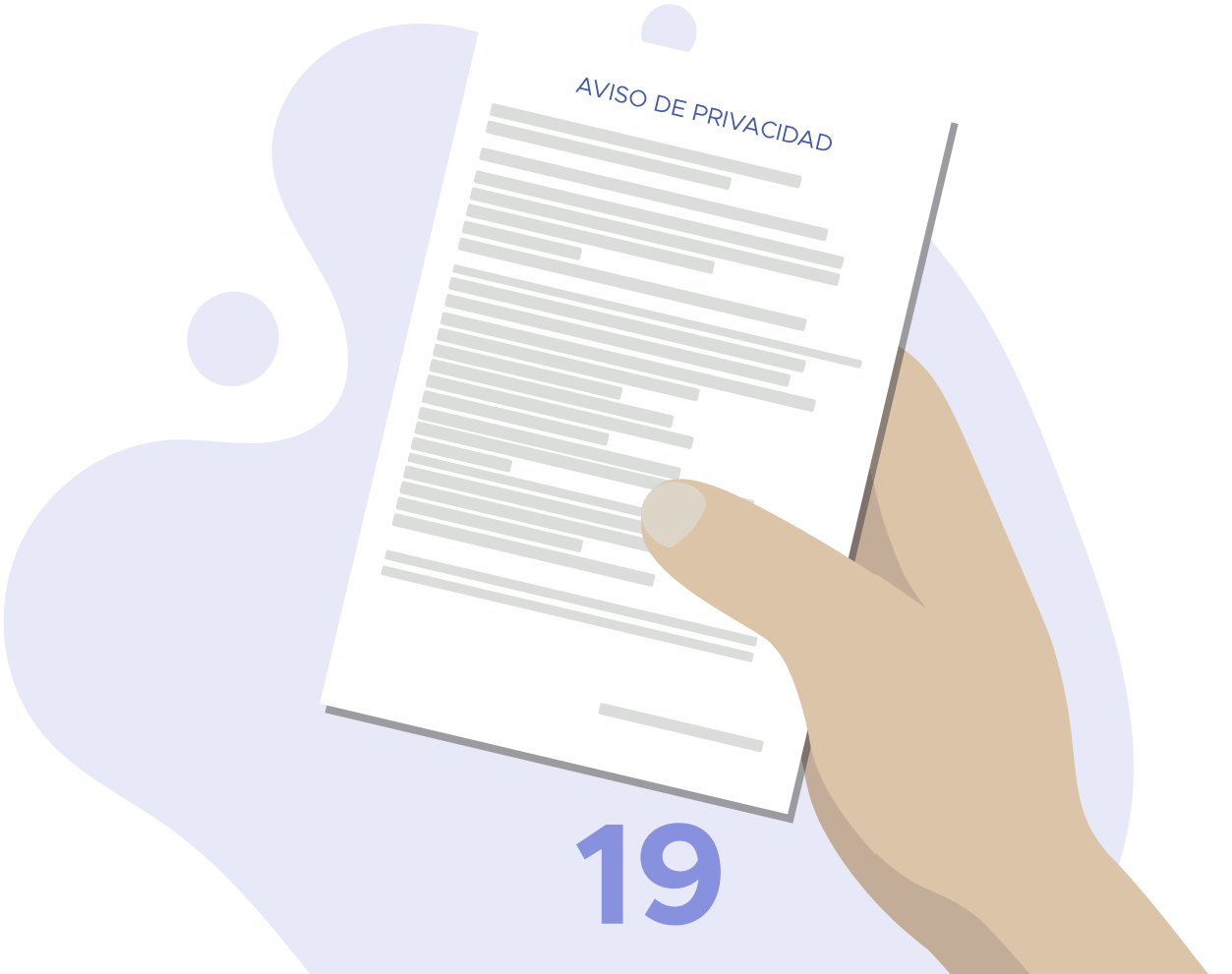
En la era digital actual es común que se soliciten datos personales en línea para diversos fines, desde registrarse en un sitio web hasta realizar compras en línea. Por eso es esencial que las personas usuarias se tomen unos minutos para leer el aviso de privacidad antes de proporcionar cualquier información personal. En caso de que afrontes alguna dificultad con la lectura sería conveniente que le pidas ayuda a alguien de confianza, sobre todo porque al leer el aviso correspondiente podrás conocer qué datos personales te solicitan y para qué serán utilizados.

¿Qué es un Aviso de privacidad?

Un aviso de privacidad es un documento legal que describe cómo se recopilan, utilizan, comparten y protegen los datos personales que proporcionarás a la empresa o sitio web. Es importante leerlo porque brinda información sobre cómo se manejarán tus datos y cómo se utilizarán. Además, contiene información sobre los derechos que puedes ejercer en relación con tus datos personales, como la posibilidad de solicitar que estos se eliminen.

Al leer el aviso de privacidad, puedes tomar una decisión informada sobre si deseas compartir tus datos personales y si estás de acuerdo con las prácticas de privacidad del sitio web o empresa en cuestión. Algunas personas usuarias pueden optar por no proporcionar sus datos personales en absoluto, mientras que otros pueden sentirse cómodos compartiendo cierta información.

En resumen, dedicar unos minutos para leer el aviso de privacidad antes de proporcionar cualquier dato personal es una práctica importante para proteger tu privacidad en línea y tomar decisiones informadas sobre el uso de tus datos.



A continuación, te compartimos algunos pasos útiles que te podrían ayudar a comprender el aviso de privacidad:

Leer el aviso de privacidad en un lugar tranquilo: encuentra un lugar tranquilo y sin distracciones para leer el aviso de privacidad o solicítale a una persona de confianza que te lo lea. Asegúrate de tener suficiente tiempo para hacerlo detenidamente.

Identificar la información clave: busca los aspectos más importantes del aviso de privacidad. Por ejemplo, quién recopila los datos, qué tipo de información se recopila, con quién se comparte la información y cómo se utiliza.

Entender los términos y condiciones: es posible que haya términos y condiciones en el aviso de privacidad que no te resulten familiares. Tómate el tiempo para leer y comprender estos términos. Si no estás seguro, busca definiciones o consulta a una amiga o amigo o familiar que pueda ayudarte.

Conocer tus derechos: asegúrate de conocer tus derechos en relación con tus datos personales. Por ejemplo, el derecho a solicitar que estos se eliminen o el derecho a acceder a la información que tienen sobre ti.
Para más información sobre los derechos de acceso, rectificación, cancelación y oposición de datos personales, y cómo se pueden ejercer consulta la **Guía para titulares de los datos personales** (Volumen 3).

Preguntar si algo no está claro: si hay algo que no entiendes, no dudes en hacer preguntas. Busca el número de contacto o el correo electrónico de la empresa o sitio web y ponte en contacto con ellos para aclarar cualquier duda.

Tomar una decisión informada: una vez que hayas leído y comprendido el aviso de privacidad, toma una decisión informada sobre si deseas compartir tus datos personales o no. Si tienes alguna preocupación o no estás seguro, es recomendable buscar otra opción o solicitar más información antes de compartir tus datos.

En general, es importante que te tomes el tiempo necesario para leer o que te lean el aviso de privacidad y para comprenderlo antes de compartir tus datos personales en línea. Al seguir estos pasos, puedes tomar decisiones informadas y proteger tu privacidad en línea.

DECÁLOGO

5

Ingresa a páginas de internet oficiales de establecimientos reconocidos

El comercio electrónico se ha convertido en una práctica cada vez más común en México y en todo el mundo. Para las personas adultas mayores, ingresar a páginas de internet oficiales de establecimientos reconocidos puede ser una buena opción para realizar compras en línea de manera segura y confiable.

Al ingresar a páginas de internet oficiales, puedes tener la seguridad de que estás comprando en un sitio web legítimo y reconocido, lo que reduce el riesgo de ser víctimas de estafas o fraudes en línea. Además, estos sitios web suelen ofrecer una amplia gama de productos y servicios, que ayudarán a encontrar lo que necesitas en un solo lugar.

Es importante destacar que muchas páginas de internet oficiales de establecimientos reconocidos ofrecen opciones de accesibilidad, por lo que podrás navegar utilizando un tamaño de letra grande que facilitará tu lectura y una navegación sencilla. Esto te facilitará el proceso de navegación y puedas comprar en línea, de manera segura.

Otra ventaja de ingresar a páginas de internet oficiales de establecimientos reconocidos es la facilidad de pago en línea. Estos sitios web suelen aceptar diferentes formas de pago, como tarjetas de crédito y débito, transferencias bancarias y pagos en efectivo en tiendas de conveniencia, lo que brinda mayor comodidad y flexibilidad al momento de realizar una compra. Aquí te bridamos algunos pasos útiles para ingresar a páginas de internet oficiales de establecimientos reconocidos y realizar compras en línea de manera segura.

- **Identificar tiendas y establecimientos reconocidos:** para ingresar a páginas de internet oficiales, lo primero que debes hacer es identificar tiendas y establecimientos reconocidos. Puedes buscar en línea o pedir recomendaciones a amistades y familiares.

- **Visitar el sitio web oficial:** una vez que hayas identificado el sitio web oficial de la tienda o establecimiento, ingresa asegurándote de que la dirección electrónica sea la correcta.
- **Explorar el sitio web:** una vez en el sitio web, explora los productos y servicios que se ofrecen. Asegúrate de que la tienda tenga una amplia variedad de opciones y de que se adapte a tus necesidades.
- **Verificar la accesibilidad:** asegúrate de que la página web sea fácil de navegar y de que tenga opciones de accesibilidad para personas adultas mayores, como letras grandes y un diseño intuitivo.
- **Comprobar las opciones de pago:** verifica las opciones de pago que se ofrecen, asegurándote de que haya varias opciones disponibles, como tarjetas de crédito y débito, transferencias bancarias y pagos en efectivo en tiendas de conveniencia.
- **Realizar la compra:** una vez que hayas encontrado el producto o servicio que deseas adquirir, sigue las instrucciones para realizar la compra en línea. Asegúrate de ingresar la información correcta, como tu dirección de envío y datos de pago.

En general, es importante que las personas adultas mayores, y en general toda persona usuaria, sean cuidadosas al ingresar a páginas de internet de establecimientos reconocidos para realizar compras en línea de manera segura y confiable. Al seguir estos pasos, puedes tomar decisiones informadas y protegerte de posibles fraudes en línea.

DECÁLOGO

6

Evita abrir correos electrónicos, documentos adjuntos y/o enlaces que te envían personas que no conoces

Desafortunadamente, las personas adultas mayores son a menudo víctimas de fraudes y estafas en línea, y una forma común utilizada por la delincuencia para intentar engañar a las personas usuarias es a través de correos electrónicos, documentos adjuntos y enlaces que envían personas desconocidas. Para disminuir el riesgo de ser víctima de las y los ciberdelincuentes te dejamos unos consejos sencillos que pueden ser de utilidad.

Evita abrir correos electrónicos de personas desconocidas: si recibes un correo electrónico de una persona que no conoces, es mejor no abrirlo y eliminarlo de inmediato. Los correos electrónicos a menudo se disfrazan como mensajes importantes o urgentes, pero en realidad están diseñados para robar información personal o financiera que guardas en tus dispositivos móviles.

No descargues documentos adjuntos de correos electrónicos de personas desconocidas: los documentos adjuntos de correos electrónicos de personas desconocidas frecuentemente contienen virus que pueden dañar tu computadora o dispositivo móvil y facilitar el robo de tu información personal o financiera.

Verifica la dirección de correo electrónico del remitente: si recibes un correo electrónico de una persona que conoces, pero que parece sospechoso, verifica la dirección de correo electrónico del remitente para asegurarte de que sea legítima. En muchas ocasiones se envían correos electrónicos a través de direcciones falsas o similares a las de empresas legítimas o por personas conocidas.

No hagas clic en enlaces sospechosos: si recibes un correo electrónico con un enlace que no conoces, no hagas clic en él. Estos enlaces a menudo te redirigen a sitios web falsos que intentan robar información personal o financiera.

Usa programa (*software*) de seguridad: usa un programa de seguridad o antivirus para proteger tu computadora. También puedes solicitarle a una persona de confianza que te ayude a instalar el programa de seguridad en tu computadora.

Es posible protegerte contras estas estafas siguiendo estas recomendaciones y manteniéndote alerta ante cualquier señal de fraude en línea.

DECÁLOGO

7

Evita proporcionar información personal, financiera o de salud a desconocidos o a través de las redes sociales o llamadas telefónicas

Normalmente las personas adultas mayores son buscadas para ser víctimas de fraudes y estafas en línea, y una forma común en que las y los delincuentes podrían intentar engañarte es a través de redes sociales y llamadas telefónicas.

Por lo que aquí te daremos unos consejos para que no caigas en los engaños de estas personas ciberdelincuentes:

No proporciones información personal, financiera o de salud a desconocidos: si recibes una solicitud de información personal, financiera o de salud de una persona desconocida a través de redes sociales o llamadas telefónicas, no proporciones la información. Las y los delincuentes a menudo utilizan información personal o financiera para usurpar tu identidad o cometer estafas.

No compartas información personal en redes sociales: evita compartir información personal en redes sociales, como tu fecha de nacimiento, número de teléfono o dirección. Las y los delincuentes pueden utilizar esta información de manera indebida.

Verifica la identidad de la persona que solicita información: si alguien te solicita información personal, financiera o de salud a través de redes sociales o llamadas telefónicas, verifica su identidad. Pregunta por su nombre completo, empresa y número de teléfono. Luego, verifica la información a través de una búsqueda en línea o llamando directamente a la empresa a la que supuestamente pertenecen para asegurarte de que sea legítima.

No hagas clic en enlaces sospechosos: si recibes un mensaje con un enlace sospechoso a través de redes sociales o correo electrónico, no hagas clic en él. Estos enlaces desconocidos a menudo te redirigen a sitios web falsos que intentan robar información personal o financiera.

No te dejes presionar: si alguien te presiona para proporcionar información personal, financiera o de salud, es probable que sea un intento de estafa. Tómate el tiempo para verificar la identidad de la persona y la legitimidad de la solicitud antes de proporcionar cualquier información.

En resumen, puedes protegerte contra el robo de información personal, financiera o de salud siguiendo estas recomendaciones y manteniéndote alerta ante cualquier señal de fraude en línea o por teléfono.

DECÁLOGO

8

Elimina de forma segura tus datos personales

Así como es importante conocer a quien le proporcionas tus datos personales, también es importante eliminarlos completamente cuando ya no sean necesarios, sobre todo si deseas proteger tu privacidad en línea.

Te damos unos consejos para eliminar de manera correcta tus datos personales y evitar que alguien más los utilice de forma indebida.

Identifica los datos que deseas eliminar: antes de eliminar cualquier dato personal, identifica aquellos que realmente deseas eliminar y asegúrate que no sean necesarios para ningún propósito legítimo posterior.

Usa herramientas de eliminación de datos: muchos dispositivos cuentan con programas para eliminar datos de forma segura. Estos permiten eliminar tus datos personales y no dejar un rastro de ellos. Te sugerimos que le pidas ayuda a una persona de confianza para que utilice estas herramientas para eliminar tus datos personales.

Rompe los documentos físicos: si tienes documentos físicos que contienen información personal, destrúyelos en muchos pedazos a mano o con tijeras antes de desecharlos.

Elimina cuentas inactivas: si tienes cuentas en línea que ya no utilizas, elimínalas para evitar que tus datos personales queden expuestos. Muchas empresas ofrecen opciones de eliminación de cuentas en sus sitios web.

Revisa tu historial de navegación y elimina los datos: tu historial de navegación en línea puede contener información personal, como nombres de usuario y contraseñas. Por eso es importante revisarlos con cierta periodicidad para eliminar aquella información que no necesitas. Te sugerimos que le pidas ayuda a una persona de confianza para que elimine tu historial de navegación.

Puedes proteger tu privacidad en línea eliminando de forma segura los datos personales. Siguiendo estas recomendaciones, puedes reducir el riesgo de que tu información personal sea utilizada de manera indebida.

DECÁLOGO

9

Tómate un minuto antes de compartir tus datos personales

En la era digital es más fácil que nunca compartir información personal a través de dispositivos móviles con acceso a internet. Sin embargo, esto también puede ser peligroso, especialmente para las personas adultas mayores que pueden no estar familiarizadas con las prácticas de seguridad en línea. Por esta razón, es crucial que te tomes un minuto para pensar lo que vas a publicar o compartir, sobre todo si es información personal.

En primer lugar, recuerda que la información que publiques en línea puede ser vista por cualquier persona en alguna parte del mundo. Por lo tanto, considera si la información que compartes es algo que se pueda saber y que no te cause ningún problema. Debes tener cuidado al compartir información personal, como tu dirección, número de teléfono o información financiera.

Además, es importante que tengas mucho cuidado a la hora de compartir información en las redes sociales. Las redes sociales pueden ser un lugar divertido para interactuar con amistades y familiares, pero también pueden ser un lugar peligroso si no tomas las precauciones adecuadas. Siempre asegúrate de que tu perfil esté configurado para que sea privado y solo compartas información con personas de confianza.

Como te hemos platicado a lo largo de este decálogo, existen las estafas en línea y puedes ser un blanco fácil para las personas estafadoras que buscan robar tu información personal o financiera. Recuerda estar atento a los correos electrónicos o mensajes sospechosos y evitar dar información personal o financiera a menos que estes completamente segura o seguro de que tu información está en las manos correctas.

DECÁLOGO

10

Reporta ante el INAI cualquier uso indebido de tus datos personales

Si tienes sospechas de que tus datos personales han sido utilizados de manera indebida, puedes presentar una queja ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Aquí te decimos que debes hacer para presentar tu queja.

Reúne la información relevante: para presentar una queja, necesitarás reunir previamente la información relevante, como el nombre de la empresa o persona que ha utilizado tus datos personales de manera indebida, la fecha en que ocurrió el incidente y cualquier otra información relevante.

Completa el formulario de queja: completa el formulario de queja, o solicítale a alguien de confianza que lo haga por ti, proporcionando toda la información relevante sobre el uso indebido de tus datos personales.

Envía el formulario de queja: una vez que hayas completado el formulario de queja y adjuntado cualquier documento relevante, envía el formulario al INAI.

Accede al portal del INAI: accede o solicita a una persona de confianza que acceda al sitio web del INAI para buscar la sección de protección de datos personales. Allí encontrarás un formulario para presentar una queja.

Adjunta cualquier documento relevante: si tienes algún documento que respalde tu queja, como un contrato o un correo electrónico, adjúntalo al formulario de queja.

Espera una respuesta: el INAI revisará tu queja y te proporcionará una respuesta en un plazo determinado. Si tu queja es válida, el INAI puede tomar medidas para garantizar que tus datos personales estén protegidos en el futuro.

Presentar una queja ante el INAI es un proceso sencillo. Solamente sigue estos pasos o preséntate directamente en el **Centro de Atención a la Sociedad del INAI** que se encuentra ubicado en: Insurgentes Sur No. 3211 Col. Insurgentes Cuicuilco, Alcaldía Coyoacán, C.P. 04530 en un horario de 09:00 a 18:00 horas de lunes a jueves y de 09:00 a 15:00 horas los viernes, o a través de su cuenta de **Twitter: @cas_inai**.
También ponemos a tu disposición el **Telinai: 800 835 43 24**.


inai
Instituto Nacional de Transparencia, Acceso a la
Información y Protección de Datos Personales