GUÍA

¿CÓMO CUIDAR TUS DATOS?

ECUADOR Chequea
PERIODISMO CON RIGOR

ChequeaLab

Guía para proteger tu información personal y moverte con más seguridad en internet

Cada vez que usamos una red social, una aplicación, una página web o una plataforma de compras, dejamos rastros de información sobre quiénes somos, qué hacemos y cómo nos movemos en el entorno digital.

Algunos de estos datos parecen simples, pero juntos pueden revelar mucho sobre una persona.

Por eso, cuidar los datos personales no es solo un tema técnico: **también es una forma de proteger la privacidad, la seguridad y el control sobre la propia información.**

Este manual explica por qué tus datos importan, cómo pueden exponerse y qué hábitos pueden ayudarte a cuidarlos mejor.

¿Qué son tus datos y por qué importan?

Tus datos personales son informaciones que dicen algo sobre ti.

Pueden incluir tu nombre, número de teléfono, correo electrónico, dirección, documento de identidad, fecha de nacimiento, ubicación, fotos, contraseñas, cuentas bancarias o incluso los hábitos que dejas al navegar por internet.

Algunos datos parecen inofensivos por separado, pero al combinarse pueden servir para identificarte, rastrearte o intentar manipularte.

Cuidar estos datos importa porque permiten acceder a aspectos sensibles de tu vida. Si caen en manos equivocadas, pueden usarse para suplantar tu identidad, entrar a tus cuentas, intentar estafarte o construir perfiles sobre ti sin que lo sepas.

¿Cómo se exponen los datos?

Muchas veces los datos se exponen sin que una persona lo note. Puede ocurrir al aceptar permisos innecesarios en una aplicación, al publicar demasiada información en redes sociales, al usar contraseñas débiles o repetidas, o al hacer clic en enlaces poco confiables.

También puede pasar cuando compartimos documentos, fotos o capturas de pantalla sin revisar qué información contienen.

En otros casos, la exposición ocurre por descuido, por desconocimiento o porque un servicio digital recopila más información de la que imaginamos.

Por eso, cuidar los datos no depende solo de evitar grandes errores, sino también de prestar atención a decisiones cotidianas que parecen pequeñas.

¿Por qué es importante protegerlos?

Proteger los datos personales ayuda a reducir riesgos. Cuando una persona cuida mejor su información, tiene más control sobre quién puede acceder a ella y para qué podría usarse.

Eso no solo disminuye la posibilidad de fraude o robo de cuentas, sino que también protege la privacidad en un entorno donde muchas plataformas recopilan y comparten datos constantemente.

La protección de datos también tiene que ver con la autonomía. Mientras menos expuesta esté tu información, menos fácil será que otros la usen para engañarte, vigilarte o presionarte.

¿Cómo se aprovechan tus datos?

A veces no te piden todo de una vez

Una idea importante es que la información personal no siempre se obtiene en un solo paso. A veces, una persona comparte pequeños datos en distintos lugares sin pensar que, al combinarse, pueden revelar mucho más de lo que parece.

Un nombre en un sitio, una foto en otro, una fecha de cumpleaños en otra plataforma y un número de teléfono en un formulario pueden ser suficientes para construir un perfil que luego se utilice en una estafa o en una suplantación de identidad.

Por eso, proteger los datos no significa únicamente cuidar la información más sensible. También implica prestar atención a esos detalles cotidianos que parecen insignificantes, pero que, al reunirse, pueden volverse muy valiosos.

La confianza también puede usarse en tu contra

Muchas veces, los datos se obtienen mediante mensajes que aparentan ser normales. Una llamada, un correo electrónico o un enlace pueden presentarse como algo legítimo y aprovechar la confianza de la persona para obtener información.

En algunos casos, quien engaña ni siquiera necesita hackear una cuenta; basta con convencer a la víctima de que entregue voluntariamente un dato, una contraseña o un código.

Esto ocurre porque los engaños digitales suelen imitar situaciones reales. Por eso es fundamental verificar la información antes de responder, incluso cuando el mensaje parece provenir de una empresa, una institución o alguien conocido.

Tus datos también pueden circular sin que lo notes

En internet, muchas plataformas recopilan información sobre lo que haces: qué buscas, qué compras, cuánto tiempo pasas viendo un contenido, desde dónde te conectas o cuáles son tus intereses.

Las plataformas que usamos a diario recopilan este tipo de información. Por ejemplo:

Redes sociales: Facebook, Instagram, TikTok, X

Motores de búsqueda: Google Search, Bing

Plataformas de video: YouTube

Comercio electrónico: Amazon, Mercado Libre

Streaming: Netflix, Spotify

Navegación y mapas: Google Maps, Waze

Parte de estos datos se utiliza para personalizar servicios o mostrar publicidad, pero también puede hacer que otros sepan más sobre ti de lo que imaginas.

Comprender esto no significa dejar de usar internet, sino utilizarlo con mayor criterio. Reconocer que tus datos tienen valor te ayuda a prestar más atención a lo que aceptas, compartes y autorizas.

¿Qué puedes hacer?

Compartir menos también protege más

Uno de los hábitos más útiles para proteger los datos personales es pensar antes de publicar o completar formularios. No todas las plataformas necesitan conocer toda tu información. Antes de compartir un dato, conviene preguntarse si realmente es necesario.
Esa pausa ayuda a reducir la exposición innecesaria y a mantener un mayor control sobre la privacidad.

En redes sociales, por ejemplo, no siempre es necesario mostrar información como la dirección, el número de teléfono, las rutinas diarias o documentos personales. Cuanto menos expuestos estén estos datos, más difícil será que alguien los utilice de manera indebida.

Crear contraseñas más seguras

Las contraseñas siguen siendo una barrera fundamental para proteger las cuentas. Utilizar claves largas, difíciles de adivinar y diferentes para cada servicio reduce significativamente muchos riesgos.

Cuando una misma contraseña se repite en varios sitios, un solo incidente puede abrir la puerta a múltiples cuentas al mismo tiempo.

También es importante no compartir contraseñas a través de mensajes y activar, siempre que sea posible, pasos adicionales de seguridad al iniciar sesión. Estas medidas no eliminan todos los riesgos, pero sí dificultan considerablemente el acceso no autorizado.

En Ecuador Chequea recomendamos que una contraseña segura tenga varias características: que sea larga (idealmente más de 12 caracteres), que combine letras mayúsculas y minúsculas, números y símbolos, y que no incluya información personal fácil de adivinar como nombres, fechas de nacimiento o palabras comunes.

Por ejemplo, una contraseña como **"Casa123"** es débil, mientras que una como **"C4s@Azul!2026"** es más robusta.

Otra buena práctica es utilizar frases largas fáciles de recordar pero difíciles de adivinar (como combinaciones de palabras sin relación entre sí) y evitar reutilizar la misma clave en distintos servicios. De esta manera, se refuerza la seguridad y se reduce el impacto en caso de que una cuenta sea comprometida.

Revisar permisos y configuraciones

Muchas aplicaciones y plataformas solicitan acceso a la cámara, el micrófono, la ubicación, los contactos o los archivos del dispositivo. En algunos casos, estos permisos son necesarios para que funcionen correctamente, pero en otros no lo son. Revisarlos con atención permite decidir qué información estás dispuesto a compartir y cuál prefieres mantener privada.

También es útil revisar las configuraciones de privacidad en redes sociales, correos electrónicos y aplicaciones. Ajustar quién puede ver tu contenido, quién puede escribirte o quién puede acceder a tus datos puede ayudarte a reducir la exposición.

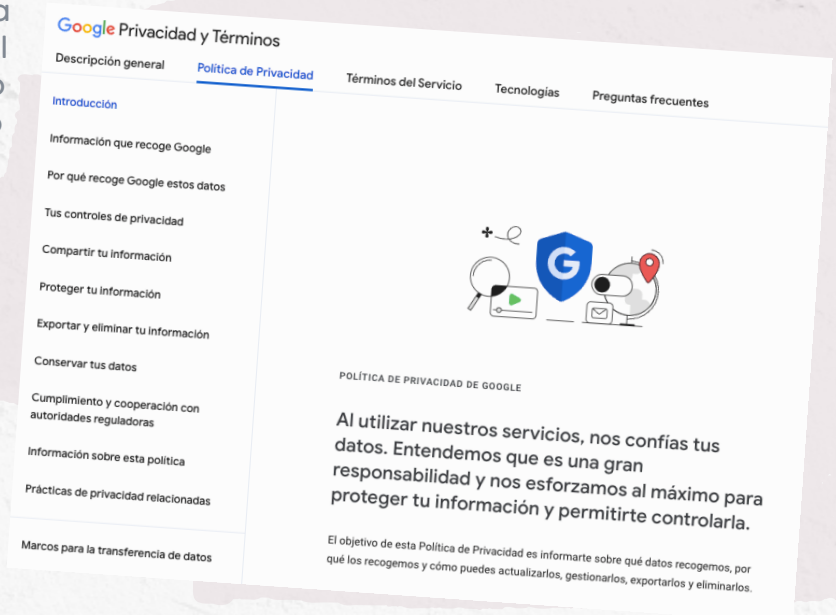
En Ecuador Chequea recomendamos además revisar periódicamente estos permisos desde el propio dispositivo o navegador.

En teléfonos, puedes ir a la sección de "Configuración" o "Ajustes" y luego a "Privacidad" o "Permisos", donde verás qué aplicaciones tienen acceso a la cámara, micrófono o ubicación, y podrás activarlos o desactivarlos según corresponda.

En navegadores web como Google Chrome, Mozilla Firefox o Safari, también es posible revisar qué sitios tienen permisos especiales.

Generalmente, esto se encuentra en la configuración del navegador, en apartados como "Privacidad y seguridad" o "Configuración de sitios", donde puedes ver y modificar accesos a cámara, micrófono, ubicación o notificaciones.

Realizar estas revisiones de forma regular ayuda a mantener un mayor control sobre tus datos y a evitar accesos innecesarios o que ya no recuerdas haber autorizado.



Verificar antes de abrir enlaces o descargar archivos

Muchos problemas de seguridad comienzan con un solo clic. Un enlace sospechoso o un archivo inesperado puede abrir la puerta a engaños, robo de información o acceso no autorizado a cuentas.

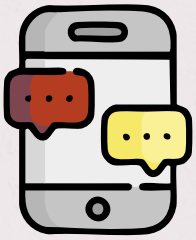
Por eso, antes de abrir algo que llega por mensaje, correo electrónico o red social, conviene verificar quién lo envía, si el contexto tiene sentido y si existe otra forma de confirmar que es legítimo.

No todos los archivos son peligrosos, pero abrirlos sin revisarlos primero aumenta el riesgo. La prevención, muchas veces, empieza con una decisión tan simple como no hacer clic de inmediato.

Señales de alerta

Te piden más información de la necesaria

Una señal de alerta aparece cuando una página, una aplicación o una persona solicita datos que no parecen necesarios para el trámite o servicio que ofrece. Si una plataforma pide acceso a información que no guarda relación con su función, conviene detenerse y revisar con más atención antes de aceptar.

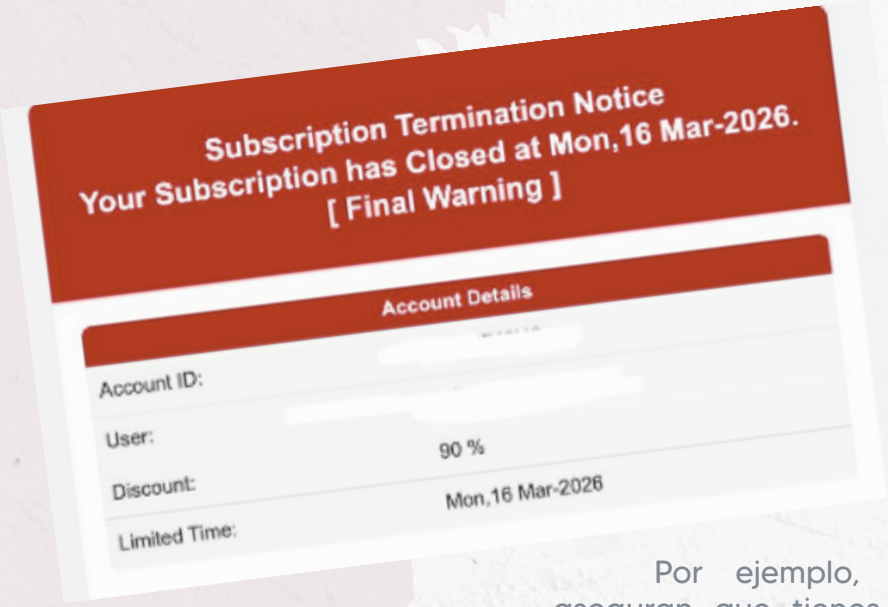


Compartiste algo sin pensar en quién podía verlo

Otra alerta frecuente es publicar o enviar información sin revisar el alcance. A veces una foto, una captura o un comentario muestran datos que no estaban pensados para circular, como números, direcciones, nombres completos o ubicaciones. Ese tipo de exposición puede parecer pequeña, pero puede abrir riesgos innecesarios.

Todo parece urgente o improvisado

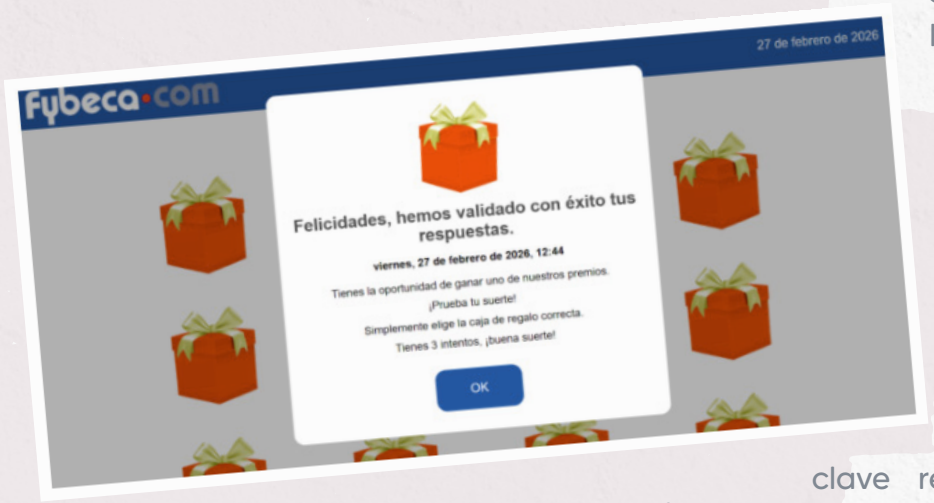
Cuando alguien solicita datos, códigos o accesos con urgencia, sin ofrecer explicaciones claras o a través de canales poco habituales, es recomendable desconfiar.



La urgencia reduce el tiempo para pensar y es una estrategia común en fraudes y engaños digitales. Si algo parece improvisado o excesivamente apresurado, vale la pena verificar la situación antes de responder.

En Ecuador Chequea también advertimos que este tipo de presión es muy común en correos electrónicos fraudulentos.

Por ejemplo, pueden llegar mensajes que aseguran que tienes una deuda pendiente con un banco y que, si no pagas “de inmediato”, tu cuenta será bloqueada.



Otros dicen que ganaste un premio, una lotería o un bono, pero que debes "confirmar tus datos" o hacer un pago previo para recibirlo. También circulan correos que simulan ser de servicios conocidos y alertan sobre un supuesto problema de seguridad para que ingreses tu contraseña.

Aunque estos mensajes pueden parecer reales, es clave revisar el remitente: muchas veces la dirección no coincide con la institución (por ejemplo, incluyen letras extrañas, dominios poco comunes o errores ortográficos). Un banco real no suele escribir desde cuentas genéricas ni pedir información sensible por correo.

Frente a estos casos, recomendamos no hacer clic en enlaces, no descargar archivos adjuntos y no compartir datos personales. En su lugar, es mejor ingresar directamente a la página oficial de la institución o comunicarse por sus canales verificados para confirmar si el mensaje es legítimo.

No sabes qué hará esa plataforma con tu información

Si no está claro para qué se recogerán tus datos, quién tendrá acceso o qué pasará con esa información después, ya existe una razón para ser más cauteloso. Aunque muchas personas aceptan condiciones sin leerlas, detenerse un poco más puede ayudar a tomar decisiones mejor informadas.

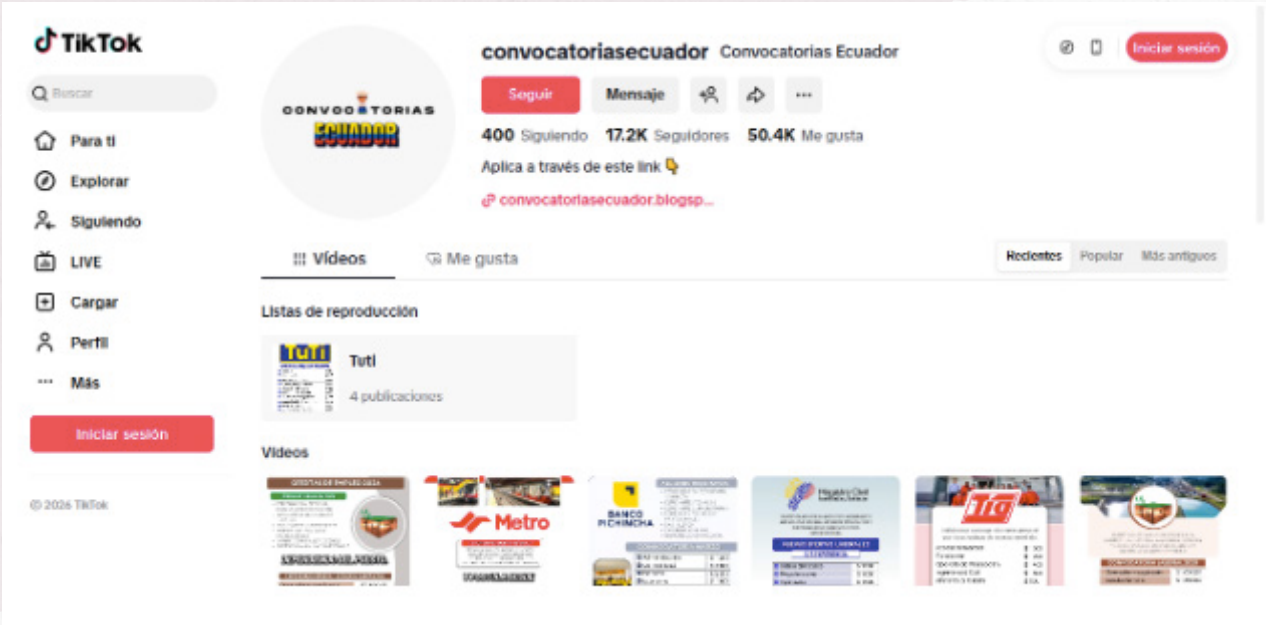
EJEM-PLO

No siempre se trata de grandes ataques: con frecuencia, la pérdida de información ocurre a través de pequeñas acciones cotidianas, como llenar formularios dudosos, dar clic en enlaces no oficiales o reutilizar contraseñas. Enseñar hábitos de cuidado digital ayuda a prevenir riesgos y a mantener la seguridad de nuestros datos.

Ejemplo verificado por Ecuador Chequea

El caso de falsas convocatorias de empleo y créditos en TikTok muestra cómo los contenidos engañosos buscan que la persona haga clic en enlaces no oficiales, dejando información sensible o contactando canales dudosos.

Ecuador Chequea explicó que estos enlaces no correspondían a procesos oficiales de contratación, aunque parecieran auténticos o atractivos.



Este ejemplo conecta directamente con otros casos de estafas digitales: la información que compartimos sin verificar puede ser usada para fraudes, robo de identidad o spam.

Ecuador Chequea recomienda pasos prácticos para mantener la seguridad en línea:

- **Revisar** permisos de privacidad en aplicaciones y redes sociales.
- **Activar** verificación en dos pasos siempre que sea posible.
- **Comprobar** dominios y enlaces antes de completar formularios o ingresar información personal.
- **Evitar** repetir contraseñas en múltiples plataformas.
- **Ser crítico** con la información que compartes: fotos, capturas de pantalla o datos personales pueden ser aprovechados si caen en manos equivocadas.

Herramientas útiles

[Google Security Checkup]

Cuidar tus datos es cuidar tu espacio personal

La información personal forma parte de la vida cotidiana y también de la seguridad de cada persona. Protegerla no significa desaparecer de internet, sino aprender a utilizar las herramientas digitales con mayor atención.

Cada decisión cuenta: lo que se comparte, lo que se acepta, lo que se publica y lo que se responde.

Con pequeños hábitos es posible reducir muchos riesgos y mantener un mayor control sobre la propia información. La protección digital no depende de hacerlo todo perfecto, sino de incorporar prácticas simples que, con el tiempo, marcan una diferencia importante.

Una pregunta útil antes de compartir

Antes de entregar un dato, publicar una imagen o aceptar un permiso, conviene hacerse una pregunta sencilla:

¿realmente es necesario compartir esto y sé quién podrá verlo o usarlo?

Esa pausa puede ayudarte a decidir mejor y a proteger tu privacidad con más criterio.

ECUADOR Chequea
PERIODISMO CON RIGOR

ChequeaLab

EN INTERNET, CUIDAR TUS DATOS TAMBIÉN ES UNA FORMA DE CUIDARTE A TI.

Quito - Ecuador
2026