

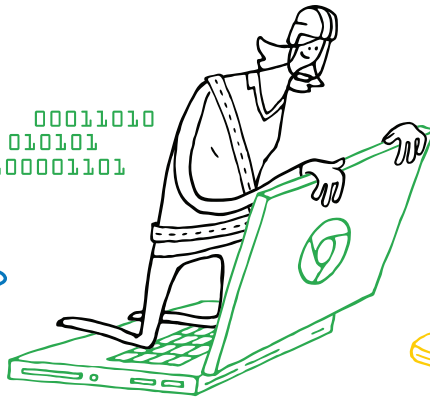


# Está bien saberlo

Una guía para mantenerse  
seguro y protegido en Internet



00011010  
010101  
100001101



Google™



**POLICIA NACIONAL**  
**Mº INTERIOR**





**POLICIA NACIONAL**  
**Mº INTERIOR**

## Contenido

1. Cómo mantenerte seguro y protegido en Internet
2. Cómo puedes proteger a tu familia en Internet
3. Descubre cómo te ayuda Google a protegerte

## ¿De qué va esto?

El objetivo de la guía Está bien saberlo de Google es velar por tu seguridad y la de tus familiares y amigos al navegar por Internet.

Este folleto está diseñado para ofrecerte una serie de sugerencias y de consejos fáciles de recordar y de poner en práctica. Hemos incluido algunas pegatinas con consejos importantes que puedes poner en tu ordenador o en tu portátil como recordatorios útiles.

Para obtener información detallada sobre todos los temas que se tratan en este folleto y sobre otros temas, accede al sitio web de Está bien saberlo:

[www.google.es/goodtoknow](http://www.google.es/goodtoknow)



# 1. Cómo mantenerte seguro y protegido en Internet

Internet ofrece muchas oportunidades para explorar, crear y colaborar. Pero es importante que te mantengas seguro y protegido para aprovechar estas ventajas.

Existen muchos tipos diferentes de delitos informáticos. Un pirata informático puede intentar obtener acceso a información como, por ejemplo, tu contraseña de correo electrónico, tus datos bancarios o tu número de la Seguridad Social.

Es posible que los piratas informáticos también intenten utilizar Internet para engañarte, venderte productos falsos o convencerte para que realices acciones que cuestan dinero. O, al igual que un ladrón roba un coche para darse a la fuga sin importarle quién es el dueño, podrían querer tu ordenador o tu sitio web como herramienta para cometer delitos informáticos.

Tanto si eres un usuario nuevo como si eres un experto en Internet, a continuación te indicamos sugerencias y herramientas útiles para ayudarte a navegar por la Web de forma segura.



POLICIA NACIONAL  
M° INTERIOR

## Protege tus contraseñas

Las contraseñas son la primera línea de defensa contra los piratas informáticos. Es esencial escoger contraseñas seguras diferentes para cada una de tus cuentas importantes y también es una buena práctica actualizar tus contraseñas regularmente. Sigue estas indicaciones para crear contraseñas seguras y mantenerlas protegidas:

1. Utiliza una contraseña exclusiva para cada una de tus cuentas importantes como tu correo electrónico y tu cuenta bancaria online.
2. Utiliza una contraseña larga formada por números, letras y símbolos.
3. Muchos servicios te envían un mensaje a una dirección de correo electrónico de recuperación si necesitas restablecer tu contraseña, así que asegúrate de que la dirección de correo electrónico de recuperación que proporciones esté actualizada y pertenezca a una cuenta a la que sigas accediendo.

Una idea es pensar en una frase que solo sepas tú y relacionarla con un determinado sitio web para recordarla. Para tu correo electrónico, podrías crear una contraseña con las iniciales y los números de "Mis amigos Tomás y Yasmina me envían un correo gracioso cada día". "MaT&Yme1cgcd" es una contraseña con muchas variaciones. Repite el proceso con otros sitios.

MaT&Yme1cgcd





POLICIA NACIONAL  
M° INTERIOR

## Evita el robo de identidad

Del mismo modo que no le darías la llave de tu casa a un ladrón, debes asegurarte de protegerte contra el fraude y el robo de identidad online. Descubre los trucos habituales que utilizan los piratas informáticos para poder protegerte del fraude online y del robo de identidad. A continuación te indicamos algunas sugerencias sencillas.

1. No respondas si ves un correo electrónico sospechoso, un mensaje instantáneo o una página web que solicite tu información financiera o personal.
2. Nunca introduzcas tu contraseña si has accedido a un sitio a través de un enlace incluido en un correo electrónico o en un chat en el que no confías.
3. No envíes tu contraseña a través del correo electrónico ni la compartas con otros usuarios.

Si ves un mensaje de alguien que conoces pero que no parece ser esa persona, puede que un pirata informático haya interceptado su cuenta para intentar que le des dinero o información, así que ten cuidado al responder. Una táctica habitual de estos piratas es solicitar el envío urgente de dinero alegando que están en otro país o que han perdido el teléfono y no pueden recibir llamadas. En el mensaje también pueden pedirte que hagas clic en un enlace para ver una foto, un artículo o un vídeo y dirigirte así a un sitio donde pueden robar tus datos. ¡Piénsalo bien antes de hacer clic!





POLICIA NACIONAL  
M° INTERIOR

## Evita estafas

No, probablemente no hayas ganado la lotería. Ni tampoco puedes ganar tanto dinero trabajando desde casa. Y esa oferta en realidad podría ser demasiado buena para ser verdad.

La Web puede ser un lugar fantástico, pero no todas las personas que acceden a Internet tienen buenas intenciones. A continuación se indican tres formas sencillas de evitar a los estafadores y mantenerse protegido en la Web:

- 1. Ten cuidado con los desconocidos que te ofrecen regalos.** Si alguien te dice que has ganado un premio y te pide que rellenes un formulario con tus datos personales, no sientas la tentación de empezar a rellenarlo. Aunque no hagas clic en el botón de envío, puedes estar enviando tu información a estafadores si empiezas a introducir tus datos en sus formularios.
- 2. Investiga siempre un poco.** Al realizar compras online, busca información sobre el vendedor y ten especial cuidado con los precios sospechosamente bajos tal y como lo harías si fueses a comprar algo en una tienda. Comprueba las ofertas online que parezcan demasiado buenas para ser verdad. Nadie quiere ser engañado para comprar productos falsos.
- 3. Ante la duda, no te arriesgues.** Si tienes un mal presentimiento sobre un anuncio o una oferta, confía en tu instinto. Únicamente haz clic en anuncios o compra productos de sitios que sean seguros y se hayan revisado y en los que confíes.





POLICIA NACIONAL  
M<sup>o</sup> INTERIOR

## Bloquea la pantalla o el dispositivo

No te irías de casa dejando la puerta abierta, ¿verdad? Pues haz lo mismo con los dispositivos que utilices. Cuando termines de usar tu ordenador, portátil o teléfono, bloquea siempre la pantalla.



Para más seguridad, debes establecer el bloqueo automático del dispositivo cuando se suspenda. Esto es especialmente importante para teléfonos y tablets (que puedes dejar por ahí al alcance de personas que no quieras que accedan a tu información) y ordenadores domésticos situados en espacios compartidos.





**POLICIA NACIONAL**  
**M° INTERIOR**

## Utiliza redes seguras

Resulta conveniente ser más precavido al acceder a Internet a través de una red que no conoces o en la que no confías como, por ejemplo, al utilizar la red Wi-Fi gratuita de tu cafetería local. El proveedor de servicios puede controlar todo el tráfico de su red, lo que puede incluir el acceso a tu información personal.

Al conectarte a través de una red Wi-Fi pública, cualquier persona que se encuentre en la zona puede controlar la información que se transmite entre tu ordenador y la zona Wi-Fi si la conexión no está encriptada. Evita realizar actividades importantes, como la banca online o comprar en Internet, cuando utilices redes públicas.

Si utilizas una red Wi-Fi en casa, debes asegurarte de usar una contraseña para proteger el router. Simplemente debes seguir las instrucciones facilitadas por tu proveedor de servicios de Internet o por el fabricante del router para establecer tu propia contraseña para el router en lugar de utilizar la contraseña predeterminada del router, que los piratas informáticos pueden conocer. Si los piratas informáticos pueden acceder a tu router, pueden cambiar la configuración y acceder a tu actividad online.

Por último, también debes asegurarte de proteger tu red Wi-Fi doméstica para añadir un nivel de seguridad adicional y evitar que otras personas la utilicen. Para ello, debes configurar una contraseña para proteger tu red Wi-Fi y, al igual que ocurre con otras contraseñas que seleccionas, debes asegurarte de seleccionar una combinación larga y única de números, letras y símbolos para evitar que otros usuarios puedan averiguar tu contraseña fácilmente. Asimismo, debes seleccionar la opción WPA2 al configurar tu red para obtener una protección más avanzada.







POLICIA NACIONAL  
M° INTERIOR

# Conoce las herramientas de seguridad y privacidad que te ofrece Google

Google te ofrece una amplia variedad de herramientas que pueden ayudarte a mantenerte protegido y mantener la privacidad y seguridad de tu información. A continuación te indicamos algunas de nuestras herramientas más populares que pueden ayudarte a que Google funcione mejor para ti.

## Verificación en dos pasos

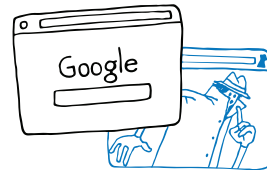
La verificación en dos pasos te ofrece una mayor protección para tu cuenta de Google. Esta herramienta añade un nivel de seguridad adicional, ya que no solo requiere una contraseña, sino también un código de verificación para iniciar sesión en una cuenta de Google. Aunque pirateen, adivinen o roben tu contraseña, los piratas informáticos no podrán iniciar sesión en tu cuenta sin introducir el código de verificación que se envía a tu teléfono móvil. Nuestro sistema de verificación en dos pasos está disponible en más de 50 idiomas y en 175 países.

## Configuración de la cuenta de Google

En la página de configuración de tu cuenta, puedes consultar servicios e información que están asociados a tu cuenta de Google, así como modificar tu configuración de privacidad y seguridad.

## Modo de incógnito

En el modo de incógnito, las páginas que abres y los archivos que descargas no se registran en el historial de descargas o navegación de Chrome. También puedes utilizar esta función en Chrome para Android, ya que Chrome es ahora el navegador predeterminado para los nuevos productos Android, lo que te permite navegar por la Web en tu teléfono o tablet de forma privada.





**POLICIA NACIONAL**  
**M° INTERIOR**

## Panel de control de Google

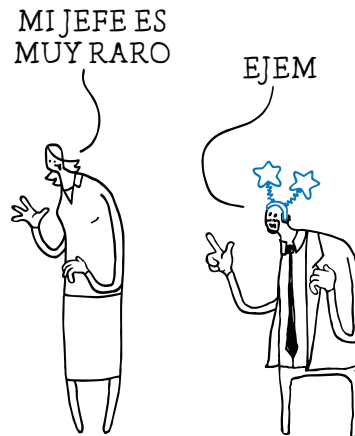
En el Panel de control de Google, puedes ver la información que está almacenada en tu cuenta de Google. Desde una única ubicación central, puedes ver y actualizar fácilmente tu configuración para servicios como Blogger, Calendar, Docs, Gmail, Google+ y muchos más.

## Configuración de anuncios

Los anuncios permiten financiar muchos de los servicios gratuitos online que te encantan y que utilizas todos los días en Internet. La configuración de anuncios de Google te permite saber cómo se seleccionan los anuncios que ves, controlar la información que se utiliza para seleccionarlos y bloquear a anunciantes específicos.

## Círculos de Google+

Los círculos de Google+ te permiten administrar tus contactos y amigos. Puedes incluir a tus amigos en un círculo, a tu familia en otro y a tu jefe en un círculo independiente (tal y como ocurre en la vida real). A continuación, puedes compartir contenido relevante, como publicaciones de Google+, vídeos de YouTube o fichas de empresa locales, con las personas adecuadas en el momento que elijas.





**POLICIA NACIONAL**  
**M° INTERIOR**



## Está bien saberlo. Y tenerlo a mano.

5 consejos para ayudarte  
a proteger tu seguridad online.

Más consejos en  
[www.google.es/goodtoknow](http://www.google.es/goodtoknow)



Evita estafas: no respondas a correos sospechosos, mensajes instantáneos o páginas que soliciten tus datos financieros o personales

Google

[www.google.es/goodtoknow](http://www.google.es/goodtoknow)



Comprueba con frecuencia tu configuración de privacidad y seguridad y elige cómo compartir tu contenido

Google

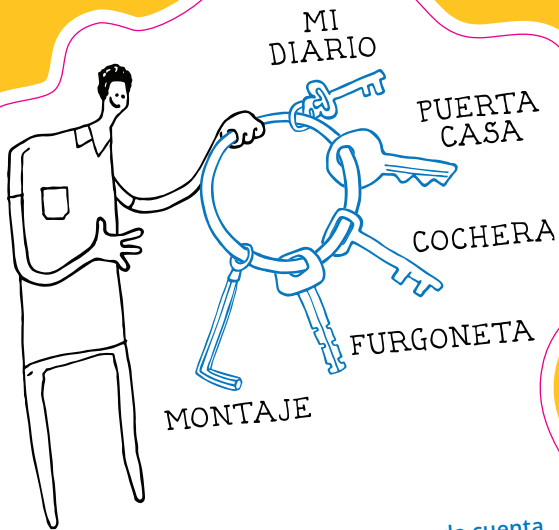
[www.google.es/goodtoknow](http://www.google.es/goodtoknow)



No envíes tu contraseña por correo electrónico ni la compartas

Google

[www.google.es/goodtoknow](http://www.google.es/goodtoknow)



Usa una contraseña exclusiva para cada cuenta importante (p. ej., email y banca online)

Google

[www.google.es/goodtoknow](http://www.google.es/goodtoknow)



Bloquea la pantalla al terminar de usar el ordenador, el portátil o el móvil

Google

[www.google.es/goodtoknow](http://www.google.es/goodtoknow)



**POLICIA NACIONAL**  
**Mº INTERIOR**



## 2. Cómo puedes proteger a tu familia en Internet

Somos conscientes de la importancia que tiene proteger a los jóvenes e instruirlos en el uso de Internet y deseamos ofrecer una experiencia segura a todos los usuarios.

Nuestros objetivos en lo referente a la seguridad familiar son los siguientes:

- Proporcionar a padres y profesores herramientas para ayudarles a elegir el contenido que sus hijos ven en Internet
- Ofrecer sugerencias y consejos a las familias sobre cómo mantenerse protegidos en Internet
- Colaborar con organizaciones (por ejemplo, instituciones benéficas), con otras empresas del sector y con organismos gubernamentales dedicados a la protección de menores



POLICIA NACIONAL  
M° INTERIOR

## Herramientas de seguridad familiar

Hemos integrado herramientas y funciones de control en nuestros productos para que puedas gestionar tu experiencia en Internet.

### Filtro SafeSearch de Google y bloqueo

SafeSearch se ha diseñado para excluir sitios que incluyan contenido sexual explícito y eliminarlos de los resultados de búsqueda. Aunque ningún filtro es eficaz al 100%, SafeSearch evita que aparezca contenido inadecuado o que preferirías que tus hijos no encontraran.

Si te preocupa que otros usuarios puedan cambiar la configuración de SafeSearch sin tu consentimiento, puedes utilizar el bloqueo de SafeSearch para protegerlo con una contraseña. Una vez que SafeSearch se haya bloqueado, aparecerá una página de resultados de búsqueda de Google diferente para indicar que SafeSearch está bloqueado.



Para habilitar el filtro SafeSearch, accede a la página de preferencias de búsqueda:  
**[www.google.es/preferences](http://www.google.es/preferences)**

### Control del contenido subido a YouTube

Es posible que, en algunas ocasiones, prefieras que tus vídeos familiares sean privados o quieras compartirlos únicamente con determinadas personas. Para ello, YouTube te ofrece la posibilidad de clasificar un vídeo como privado o de dejarlo sin clasificar al subirlo.







**POLICIA NACIONAL**  
**M° INTERIOR**

### **Modo de seguridad de YouTube y bloqueo**

El modo de seguridad permite excluir de los resultados de búsqueda de vídeos el contenido para adultos que pueda resultar ofensivo, aun cuando no infrinja las Normas de la comunidad de YouTube. Cuando se activa el modo de seguridad, los vídeos con contenido para adultos o con restricción de edad no se muestran en los resultados de búsqueda.

Para acceder a esta función y activarla, haz clic en el botón de seguridad situado en la parte inferior de cualquier página y activa el modo de seguridad.

### **Filtrado de contenido en Android**

Los desarrolladores que incluyen sus aplicaciones en Google Play deben etiquetarlas según el sistema de clasificación de Google Play, que incluye cuatro niveles: Para todos, Nivel de madurez bajo, Nivel de madurez medio y Nivel de madurez alto. Mediante un código PIN, los usuarios pueden bloquear un ajuste para filtrar aplicaciones en sus dispositivos de modo que solo se puedan ver y descargar las aplicaciones que se consideren adecuadas.

### **Google+**

Hemos incluido en esta aplicación una serie de funciones que te ofrecen transparencia y control sobre los usuarios que acceden a tu información y sobre el tipo de datos que publicas o compartes. Entre estas funciones se incluyen los círculos, que te permiten especificar quién puede ver tus publicaciones, las opciones de notificación, que te permiten especificar quién puede contactar contigo, y las opciones de visibilidad, con las que puedes convertir tu perfil en privado.

### **Blogger**

De forma predeterminada, los blogs de Blogger son totalmente públicos, así que puede leerlos cualquier usuario de Internet. Si quieres que tu blog sea privado, puedes limitar los visitantes del blog invitando únicamente a las personas que quieras que lo vean.





**POLICIA NACIONAL**  
**M° INTERIOR**

## Notificación de contenido inadecuado

Varios productos de Google, como Google+, YouTube y Blogger, te permiten crear, publicar y compartir tu propio contenido. Hemos creado herramientas para que nos informes si encuentras contenido que no debería aparecer en el sitio. A continuación, te ofrecemos una breve guía sobre cómo informar sobre contenido inadecuado en algunos de nuestros productos más populares.

### Google+

Puedes denunciar distintos tipos de contenido inadecuado en Google: puedes informarnos sobre publicaciones, comentarios, vídeos, fotos o perfiles inadecuados para que los revisemos.

### YouTube

Si encuentras en YouTube un vídeo que consideras que infringe las Normas de la comunidad, puedes marcarlo como inadecuado para que nuestro equipo lo revise. Recuerda que puedes utilizar el modo de seguridad de YouTube para excluir contenido que, aun cumpliendo las Normas de la comunidad, prefieres que no aparezca en el sitio.

### Blogger

Los usuarios que leen blogs alojados en Blogger pueden marcar cualquier material que consideren que infringe las políticas de este servicio.

Para obtener información sobre cómo se utilizan estas herramientas, accede a la página [www.google.es/goodtoknow/familysafety/abuse](http://www.google.es/goodtoknow/familysafety/abuse)



### 3. Descubre cómo te ayuda Google a protegerte

Internet es algo realmente extraordinario. Pero al igual que en la vida real, no todo el mundo tiene buenas intenciones. Google se toma muy en serio la privacidad y la seguridad de sus usuarios. Invertimos millones de dólares cada año y disponemos de los expertos en seguridad de datos más importantes del mundo para mantener tu información protegida. Su objetivo es proteger tu seguridad y la de tu información y anticiparse a las acciones de los piratas informáticos.

Google trabaja duro para protegerte de delitos como el robo de identidad, el fraude personal y las estafas de Internet, proteger tu ordenador y hacer de Internet un lugar más seguro. Te proporcionamos las herramientas y los conocimientos necesarios para que tu familia y tú estéis protegidos en Internet. Además, estamos constantemente invirtiendo y mejorando para luchar en tu nombre.



**POLICIA NACIONAL**  
**M° INTERIOR**

## Cómo luchar contra el robo de identidad

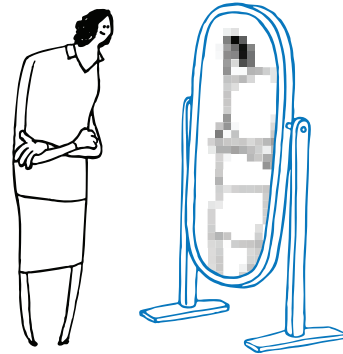
Google utiliza varias tecnologías para protegerte del robo de identidad online y garantizar que tu cuenta de Google se mantenga segura y protegida.

### **Verificación en dos pasos**

La verificación en dos pasos te ofrece una mayor protección para tu cuenta de Google. Esta herramienta añade un nivel de seguridad adicional, ya que no solo requiere una contraseña, sino también un código de verificación para iniciar sesión en una cuenta de Google. Aunque pirateen, adivinen o roben tu contraseña, los piratas informáticos no podrán iniciar sesión en tu cuenta sin introducir el código de verificación que se envía a tu teléfono móvil.

### **Encriptación**

Google toma muchas medidas para mantener tu información personal protegida frente a piratas informáticos y estafadores. De forma predeterminada, encriptamos la conexión de Gmail entre tu ordenador y Google, lo que evita que otras personas accedan a tu actividad de Google. También utilizamos de forma predeterminada este sistema de protección, conocido como encriptación SSL, cuando inicias sesión en Google Drive y en otros muchos servicios.





POLICIA NACIONAL  
M<sup>o</sup> INTERIOR

## Cómo actuar para poder mantener limpios tu ordenador y tu dispositivo

Puedes ayudar a proteger tu ordenador del software malicioso, pero Google también contribuye al mantenimiento de la seguridad de tus datos y dispositivos mediante el trabajo ininterrumpido de cientos de expertos en seguridad.

### Cómo puedes evitar el software malicioso

Al igual que buscamos en la Web los sitios que mejor respondan a las preguntas de los usuarios, también buscamos sitios que parezcan ser perjudiciales para ellos o que puedan incluir software malicioso. Cada día identificamos y marcamos más de 10.000 de esos sitios no seguros y mostramos advertencias en hasta 14 millones de resultados de la Búsqueda de Google y 300.000 descargas, indicando a los usuarios que un determinado sitio web o enlace podría incluir contenido sospechoso.

### Cómo puedes mantener la seguridad de tu dispositivo móvil

Los smartphones que ejecutan el software Android de Google tienen instaladas protecciones similares para reducir el riesgo de daño. Android también requiere que todas las aplicaciones de Google Play Store indiquen el tipo de información que la aplicación quiere recopilar o a la que quiere acceder en tu dispositivo para que puedas decidir si debes confiar o no en la aplicación. También analizamos Google Play de forma automática para bloquear y eliminar aplicaciones perjudiciales y, en el caso de algunos teléfonos Android, el servicio de verificación de aplicaciones de Google busca aplicaciones potencialmente dañinas, independientemente de su procedencia.





POLICIA NACIONAL  
Mº INTERIOR

# Haciendo que Internet sea un sitio más seguro para todos

La protección de los usuarios es una responsabilidad compartida. Todos nos beneficiamos si todo el mundo utiliza las mejores técnicas y tecnologías de seguridad.

## Experiencia y herramientas compartidas

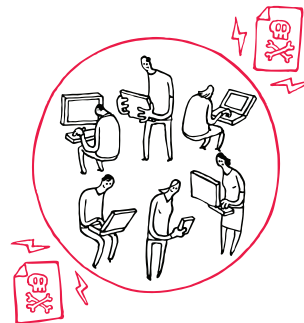
Tu seguridad nos importa, por lo que, independientemente de los servicios o productos que utilizas, compartimos la información sobre los enlaces y sitios inadecuados que detectamos con empresas para que también puedan proteger a sus usuarios. Al trabajar de forma conjunta y ayudarnos mutuamente, toda la Web es mucho más segura.

## Comunicación con usuarios y propietarios de sitios web

A medida que trabajamos para proteger a nuestros usuarios y su información, en ocasiones descubrimos e investigamos patrones de actividad inusuales. Cada día, identificamos y marcamos más de 10.000 sitios no seguros. También enviamos mensajes diariamente a miles de propietarios de sitios web, cuyos sitios creemos que se podrían haber interceptado a través de un ataque, para que puedan limpiarlos.

## Asociación con organizaciones de seguridad

Google forma parte de una serie de organizaciones que trabajan para ayudar a las empresas a mejorar la seguridad de sus usuarios. Por ejemplo, nos hemos asociado con StopBadware.org y hemos ayudado a la organización a hacer que Internet sea un lugar más seguro deteniendo, reduciendo y limpiando sitios web que incluyen software malicioso u otro software dañino.







Google™



**POLICIA NACIONAL**  
**Mº INTERIOR**

Más información sobre cómo mantenerse protegido en Internet en  
[www.google.es/goodtoknow](http://www.google.es/goodtoknow)

