

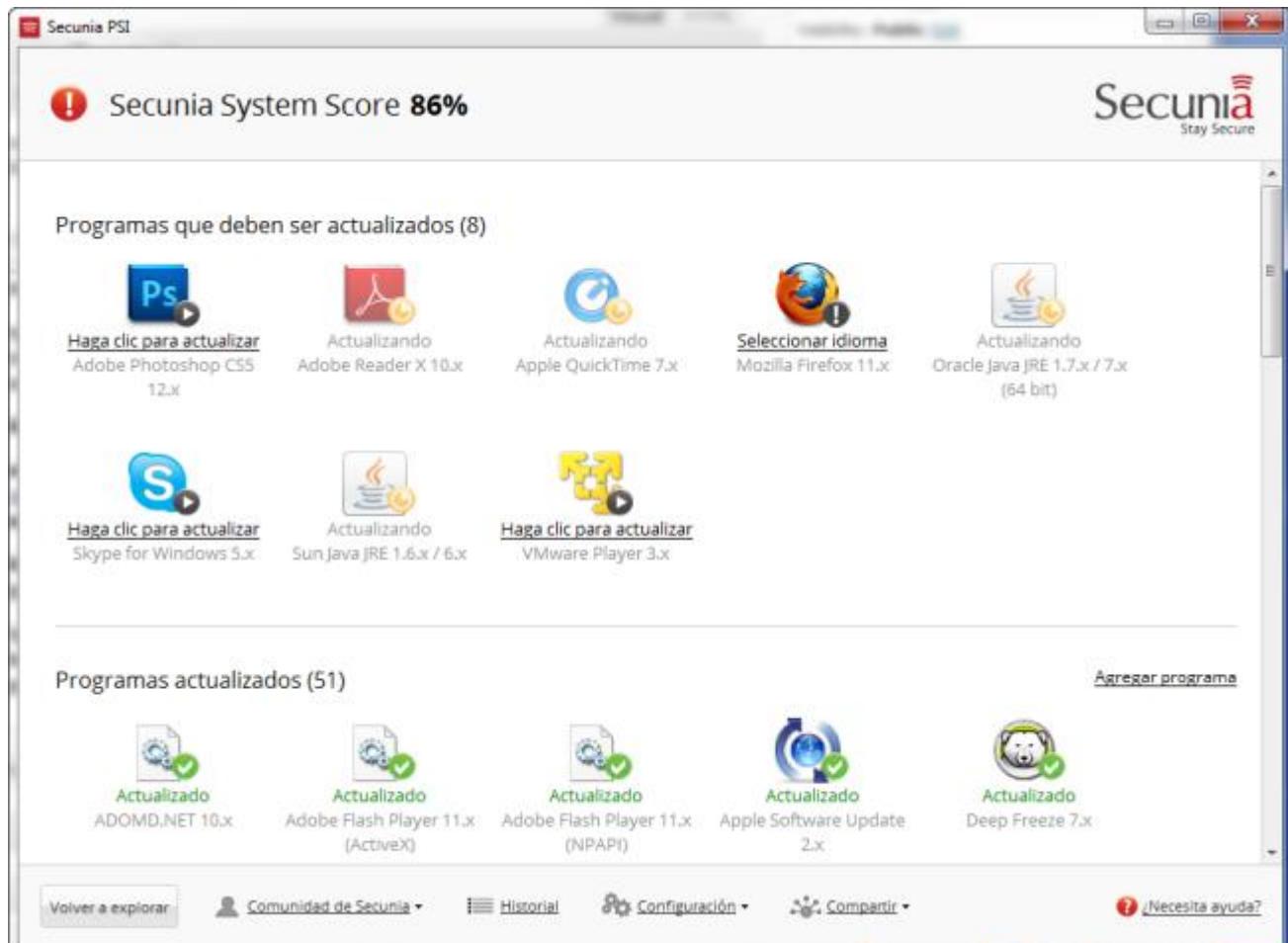
10 consejos de seguridad informática que debes seguir

<http://articulos.softonic.com/10-consejos-de-seguridad-informatica-imprescindibles>

Hay cosas que tu antivirus, por muy bueno que sea, no puede hacer. Te explico qué medidas de seguridad informática necesitas aplicar por tu cuenta.

1. Mantén actualizados los programas

Hay malware que se aprovecha de las [vulnerabilidades en programas famosos](#) para colarse en tu PC sin que el antivirus pueda actuar. Un ejemplo: el [Virus de la Policía](#).



Para evitar sorpresas, debes **mantener actualizados tus programas**. Aplicaciones como [Secunia PSI](#) o [Softonic for Windows](#) te ayudan a conseguirlo.

2. En redes públicas, navega con cifrado

En las redes WiFi públicas, tus datos [pueden ser interceptados](#) de muchas maneras. Navegar desde ellas sin protección es **una imprudencia que se paga muy cara**.



Para defenderte, navega siempre con el [protocolo HTTPS activado](#); con [HTTPS Everywhere](#) es muy fácil. Y para añadir seguridad extra, [te recomiendo usar estas apps](#).

3. Crea usuarios y contraseñas distintos

Casi cada día aparecen [noticias sobre contraseñas robadas](#) en servicios importantes. El riesgo de que entren en tus cuentas una vez atacado un servicio es enorme.

The screenshot shows a software interface titled "dashlane". On the left, there's a sidebar with categories: "PERSONAL DATA" (Contact, IDs, Payment), "INTERNET ACCOUNTS" (Logins and Passwords, Security Dashboard, which is selected), and "INTERNET SHOPPING" (Purchases). Below these are "SHARE" buttons for Facebook and Twitter. The main area is a table with columns: Website, Login, Password, Password strength, # of times Password Used, and Safety Level. The table lists various websites like chartbeat.com, geckoboard.com, mint.com, mixpanel.com, skype.com, etc., with their corresponding logins and password details. A red arrow points to the "Safety Level" column, which includes ratings like "Very unsafe" (with a red circle icon) and "Super safe" (with a green circle icon).

Website	Login	Password	Password strength	# of times Password Used	Safety Level
chartbeat.com	billcrisper	*****	23%	5	Very unsafe
geckoboard.com	bill.crisper@gmail.com	*****	23%	5	Very unsafe
mint.com	bill.crisper@gmail.com	*****	23%	5	Very unsafe
mixpanel.com	billcrisper1@gmail.com	*****	23%	5	Very unsafe
skype.com	billcrisper	*****	23%	5	Very unsafe
@gag.com	bill.crisper@gmail.com	*****	17%	1	Very unsafe
ycombinator.com	billcrisper	*****	23%	1	Very unsafe
live.com	alexis.fogel@hotmail.fr	*****	54%	1	Safe
google.com	billcrisper	*****	72%	1	Super safe
twitter.com	dashlane	*****	77%	1	Super safe
dashlane.com	dashlane\alexis	*****	81%	1	Super safe
yesasia.com	bill.crisper@gmail.com	*****	86%	1	Super safe
google.com	mySpamBill	*****	100%	1	Super safe
lego.com	bill.crisper@gmail.com	*****	100%	1	Super safe
foursquare.com	bill.crisper@gmail.com	*****	100%	1	Super safe
dropbox.com	bill.crisper@gmail.com	*****	100%	1	Super safe
producteev.com	bill.crisper@gmail.com	*****	100%	1	Super safe
buymeacoffee.com	bill.crisper@gmail.com	*****	100%	1	Super safe

[Crea](#)

contraseñas distintas y seguras para todos tus servicios, y usa nombres de usuario diferentes cuando se te dé esa opción. Y usa un gestor de contraseñas como [Dashlane](#).

4. Cambia tus contraseñas a menudo

Las contraseñas envejecen. Y si las vulnera un intruso discreto, puede que tardes mucho en saber si alguien ha accedido a tus archivos y mensajes.

Por muy fuertes que sean tus contraseñas, **cámbialas periódicamente**. Y para añadir un factor de protección adicional, [activa la verificación en dos pasos](#) allá donde puedas.

5. Comprueba las apps autorizadas

"¿Puede la aplicación X leer tus datos de Facebook y Google?". Cuando autorizas una app maligna, el desastre está servido: **spam enviado en tu nombre, robo de datos...**

The screenshot shows a Facebook application settings page for "9GAG". It displays information about the app's access to user data. At the bottom, there is a red arrow pointing to a "Remove app" link.

Use apps, plugins, games and websites on Facebook and elsewhere? On

9GAG Last logged in: August 3 Close

Visibility of app: Public

This app needs:

- Your basic info
- Your email address (algernon@gmail.com)

This app can also:

Post on your behalf This app may post on your behalf, including objects you liked, posts you created and more.

Last data access: No data access recorded Learn more

When to notify you: The app sends you a notification

Legal: Privacy Policy · Terms of Service

[Remove app](#) · Report app

Revocando una aplicación en Facebook

Para prevenir problemas, [controla las apps autorizadas](#) de Google, Facebook, Twitter y otros sitios importantes. Revocar permisos es fácil y rápido.

6. Protege tu red WiFi frente a intrusos

Una red WiFi abierta es un gesto solidario... y peligroso. Un visitante mal intencionado puede intentar [acceder a los datos](#) de tu ordenador. Y entonces [hablamos de intrusos](#).

The screenshot shows the SoftPerfect WiFi Guard application window. The menu bar includes File, View, Help. The toolbar has icons for Scan Now, Settings, Properties, All Devices, and Web-Site. Below the toolbar is a table listing connected devices:

IP address	MAC address	RTT	Name	Info	Vendor
192.168.0.9	08-00-27-28-86-17	0 ms	JOHN-PC	This computer	CADMUS CO...
192.168.0.1	00-8E-F2-76-3C-9D	0 ms		Internet gateway	NETGEAR INC.,
192.168.0.11	18-20-32-B5-31-FF	174 ms			Apple, Inc.
192.168.0.10	04-46-65-70-24-07	---			Murata Manu...
192.168.0.2	BC-AE-C5-20-FC-B9	0 ms	WALLABY-PC		ASUSTek CO...

At the bottom, it says "Idle" and "Next scan at 2:27". The system tray shows "Intel(R) PRO/1000 MT Desktop".

Con [SoftPerfect WiFi Guard](#) puedes ver qué y quién está conectado a tu red WiFi

Revisar la seguridad de tu red WiFi es la mejor manera de evitar sorpresas desagradables. Sigue mis [ocho consejos para reforzar tu red WiFi](#).

7. Controla la privacidad de tus redes

En tus perfiles de Facebook y Google hay un montón de información personal que **puede usarse en tu contra** (por ejemplo, para adivinar contraseñas).

The screenshot shows a Facebook profile page for a user named "Tíobueno Noexistó". The profile picture is a man's face. The bio includes: "Trabajó en Massive Dynamic", "Estudió en Universidad Invisible", "Vive en Pozuelo de Alarcón", and "De Jacksonville". There is a "Muro" (Wall) section with one post from the user: "ola xicassssss" posted "Hace 3 minutos". A note below the post says "A Tíobueno Noexistó le gusta esto."

Cuidado con los [perfils falsos en Facebook](#), podrían ser ladrones de datos...

Rechaza [solicitudes de amistad sospechosas](#) y configura bien la privacidad de Facebook y otras redes sociales. Es una cuestión de privacidad fundamental.

8. Crea usuarios para cada persona

He visto un montón de ordenadores con una sola cuenta para toda la familia. O con varias cuentas, pero desprotegidas. Es un camino seguro hacia el [desastre](#).



Dos usuarios conviven en el mismo PC con Windows 7 ([fuente](#))

Si más de una persona va a usar un PC, crea diferentes cuentas, cada una protegida por una contraseña fuerte u otro sistema de identificación. ¡Y por favor, [bloquea el PC!](#)

9. Desconfía de los archivos que te envían

Uno de los virus más dañinos de los últimos tiempos se propagó a través de Skype: un amigo enviaba un archivo y la gente, **al confiar en su origen**, lo abría. Y kaputt.



¿Vas a abrirlo aunque te lo haya enviado un amigo?

Estés donde estés, **no abras un archivo misterioso por ninguna razón**, ni siquiera si te lo envía un amigo. Pregúntale antes qué es. En la duda, [escanéalo en la web](#).

10. Aprende a ser escéptico

La seguridad es una actitud. Implica desconfiar sanamente de las cosas que ves a diario en Internet, ese mágico mundo de colores... y estafas.

Sé escéptico. En mis guías [Cómo detectar y desmontar bulos](#) y [Qué hacer ante un mail sospechoso](#) te proporciono pautas de sentido común para ser más vigilante.