Nº597 Año XXIII • 2021
Sale viernes sí, viernes no

PRÁCTICA • ACTUAL • QUINCENAL

Computer Hoy

computerhoy.com

Miembro del grupo Computer Bild

ESPECIAL SEGURIDAD

BLINDA TU VIDA DIGITAL

- ✓ **Doble verificació. :** qué es y cómo funciona
- ✓ **Asegura** tus cuentas y datos personales
- ✓ **Protégete** frente a ciberamenazas
- ✓ **Evita** que te espíen y chantajeen
- ✓ **Y mucho más...**

¿Tu móvil te espía?

Antes de vender tu equipo... ¡bórralo bien!

Navega de forma segura

COMPARATIVA

16 Servicios VPN

+ LAS CLAVES PARA CONTRATAR UNA RED PRIVADA VIRTUAL

El enemigo invisible

La clave: a. ticiparse y reaccio. ar a tiempo

¿Por qué es ta. importa. te el cifrado de datos?

¡Viejuno!

YA A LA VENTA

¡NOS GUSTA LO RETRO!

SI TE HAS QUEDADO SIN LOS ANTERIORES, CONSÍGUELOS EN NUESTRO STORE:
store.axelspringer.es/retrogamer

EDITORIAL

Computer Hoy N° 597

CARLOS GOMBAU
Redactor Jefe

EVITA SUSTOS POR EL EXCESO DE CONFIANZA

"Tranquilo, que yo controlo". En 1975, hace ya más de 45 años, que Sam Peltzman enunció su Teoría de Compensación del Riesgo (conocida actualmente como efecto Peltzman) en el artículo 'Los efectos de la regulación de la seguridad del automóvil'. Publicado en el Journal of Political Economy, el profesor de Economía de la University of Chicago Booth School of Business afirmó que, cuanto menor es el riesgo percibido en una situación determinada, menores son las medidas de precaución que tomamos. O, dicho de otra forma, tenemos comportamientos más o menos arriesgados en función de si nos sentimos más o menos protegidos, compensando las medidas de seguridad impuestas tomando conductas más atrevidas de lo normal. El problema es que este sesgo puede ser solo una mera ilusión.

Ese exceso de confianza en las medidas de seguridad que nos hace olvidarnos del riesgo no solo se aplica al mundo del automóvil, como enunció Peltzman –confiamos en elementos como los sistemas de retención, el ABS o el airbag desde hace décadas–. En otros ámbitos, como el deportivo, ocurre lo mismo, con medidas de protección en pruebas de velocidad y/o contacto como el casco en el ciclismo o las hombreras en el fútbol americano. O algo más de andar por casa como la seguridad infantil –tapas de enchufe, topes o esquineras– o actual como la crisis sanitaria –nos sentimos más seguros con la mascarilla puesta y un bote de gel, y todopoderosos tras vacunarnos–.

QUE NO PERCIBAMOS EL RIESGO COMO TAL O QUE NOS SINTAMOS SEGUROS, NO QUIERE DECIR QUE NO EXISTA. EVITA LOS SUSTOS.

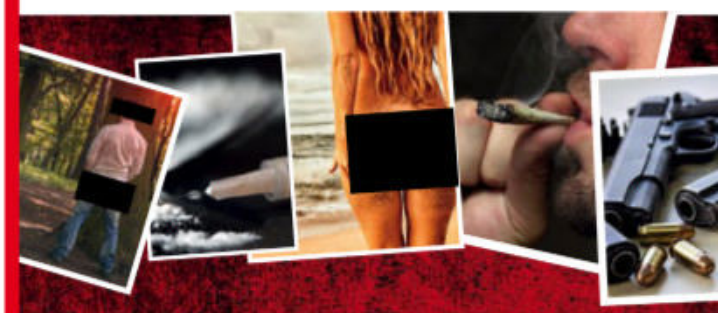
A todo ello hay que sumar que el simple hecho de presenciar a otra persona tomando (o no) precauciones aumenta potencialmente la probabilidad de que corramos un mayor riesgo. Producto de ese exceso de confianza, tenemos el "Tranquilo, que yo controlo" o el "Confía en mí". Y, si hablamos de Internet, debemos añadir el "No me preocupa la seguridad y privacidad porque no tengo nada que pueda interesar o necesite ocultar". Y entonces es cuando vienen los sustos. Recuerda, los sesgos cognitivos se alimentan de nuestra ignorancia sobre ellos: que no percibamos el riesgo o que nos sintamos seguros, no quiere decir que no exista.

carlos.gombau@axelspringer.es | **@cgombau**

Tu opinión cuenta...

Computer Hoy.com			YouTube	STORE
computerhoy.com	ComputerHoy	@computerhoy	ComputerhoyTV	store.axelspringer.es

No te pierdas...

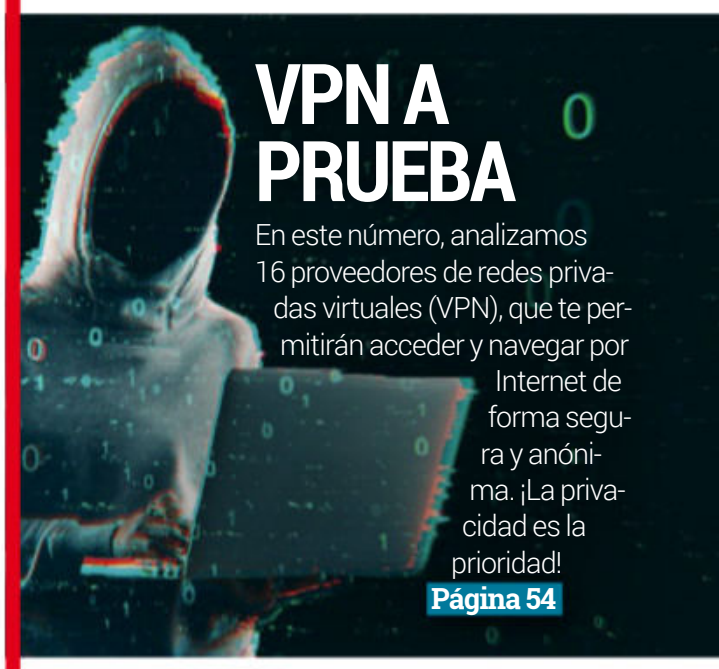


¿ESTAS SON TUS FOTOS?

Es mucho lo que se puede encontrar en los discos duros de segunda mano: fotos privadas, DNI, pornografía, documentos... Un material sensible que algunos podrían usar para chantajear a sus antiguos propietarios. **Página 10**

¡QUE NO TE ESPÍEN!

Mejorar la privacidad en tu ordenador y móvil es posible. Aprende a prevenir el espionaje en este tipo de dispositivos. **Página 22**



VPN A PRUEBA

En este número, analizamos 16 proveedores de redes privadas virtuales (VPN), que te permitirán acceder y navegar por Internet de forma segura y anónima. ¡La privacidad es la prioridad! **Página 54**

SUMARIO

ACTUALIDAD

UN ESPÍA EN EL BOLSILLO

Aprende a protegerte de los programas que pretendan vigilar tu teléfono móvil. Página 14

ROBO DE IDENTIDAD

Un robo de este tipo causa grandes daños y es un lastre para las víctimas durante mucho tiempo. Página 16

PRÁCTICO

A SALVO EN INTERNET

Hay muchas amenazas acechándote en la Red. Aprende a protegerte cada vez que te conectas a Internet o compras online. Página 32

CON DOBLE VERIFICACIÓN

Te explicamos cómo funciona la verificación en dos pasos y cómo te ayuda a garantizar un acceso seguro para tus cuentas online. Página 42

TEST

MANTÉN TU PRIVACIDAD CON UNA VPN

¿Sientes como que te vigilan cuando estás navegando en la Red? Entonces, un servicio VPN que te permita mantener el anonimato y la privacidad en Internet puede ser la solución para ti. Analizamos varios proveedores de redes privadas virtuales. Página 54

SABER MÁS

EL ENEMIGO INVISIBLE

Robo de datos, interrupción de la actividad empresarial... los ataques cibernéticos tienen muchos objetivos. Página 66

CRIPTOGRAFÍA Y CIFRADO DE INFORMACIÓN

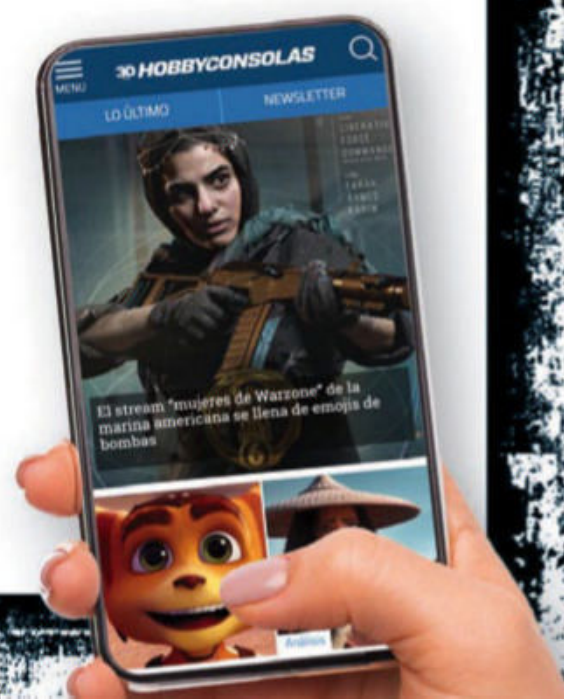
La confidencialidad de los datos es vital y la criptografía cobra ahora mucha importancia. Página 70

La revista de videojuegos nº1 en España

Y todos los días en la web
hobbyconsolas.com

1991 2021 30 AÑOS

Desde 1991 Hobby Consolas es la revista de videojuegos más vendida en nuestro país. Todos los meses la tienes en el kiosco llena de reportajes, análisis, reviews y mucho más. Un contenido exclusivo que no vas a encontrar en otra parte. Y durante todo 2021, **celebramos los 30 años** de la marca. **¿Te lo vas a perder?**



ESTA CAJA PROTEGE TU PRIVACIDAD

El eBlocker es una pequeña caja que protege tu privacidad cuando estás navegando. ¡Ahora puedes crear tú mismo este dispositivo tan práctico!

Por supuesto, puedes instalar un programa como TOR para **navegar de forma anónima**, equipar tu navegador favorito con diversos complementos (add-ons) para protegerte del seguimiento publicitario e instalarte otro programa de control parental para que los niños no vayan a parar a las páginas web que muestren contenido sexual o violento.

Pero ¿no sería mucho más práctico si instaláramos un pequeño dispositivo en la red doméstica y tuviéramos todas estas funciones de inmediato y sin tener que instalar tropecientas cosas adicionales? ¡Antes había un aparato de este tipo! Se llamaba **eBlocker** y ofrecía exactamente eso: una vez que se adhería al router, la pequeña caja protegía automáticamente todos los dispositivos de la red doméstica frente al espionaje a través de Facebook y Google, ante rastreadores publicitarios, contenidos no deseados de la red y mucho más. No obstante, aunque el eBlocker era muy práctico, cuando un posible inversor retiró sorprendentemente su ayuda económica, el fabricante de la caja tuvo que declararse en quiebra.

> Gran protección y privacidad al alcance de todos: esta cajita es realmente genial.
>
> **Andreas Sauerland**
> Redactor

Un eBlocker de fabricación casera

En vez de dar carpetazo por completo al proyecto, se decidió convertir el sistema operativo de la caja en un programa de **código abierto** y, de esta forma, ponerlo a disposición del público gratis. La consecuencia es que ahora puedes crear tú mismo tu propio eBlocker. Lo único que necesitas para ello es una Raspberry Pi. Puedes adquirir este miniordenador a través de Internet o en las tiendas informáticas especializadas por unos 70 €. Asimismo, necesitas una carcasa en la que acomodar tu Raspberry Pi, además de una tarjeta microSD en la que instalar el sistema operativo gratuito. Después, conecta tu eBlocker casero a tu router y el resto lo hará la caja prácticamente por sí sola. El software para el eBlocker te lo puedes descargar de Internet y, en las siguientes páginas, te explicamos de forma detallada cómo **montarlo y configurarlo**.

La caja, a prueba

Pero ¿la caja cumple lo que promete? En Computer Hoy hemos examinado a conciencia el eBlocker que hemos creado en el laboratorio de pruebas y nos ha convencido, sobre todo, la fácil configuración y manejo del dispositivo. Los diferentes ajustes del eBlocker se pueden llevar a cabo a través de una interfaz web en el ordenador. La **anonimización** mientras se navega funciona correctamente y de manera fiable gracias a la integración del programa TOR. Asimismo, nos ha causado una grata impresión el control parental que ofrece diferentes modos operativos y un sistema de control del tiempo. Lo que no resulta tan convincente es la protección frente al seguimiento publicitario y las inserciones en páginas web: aquí hemos echado de menos contar con más opciones de configuración personalizada.

TUYA POR SOLO 70 EUROS

CONCLUSIÓN

¿La protección de la privacidad en tus manos? El concepto del eBlocker con software de código abierto es estupendo. Una vez que está conectado al router, la pequeña caja te sorprende ofreciéndote una gran cantidad de funciones de protección para que puedas navegar de forma segura y a cambio de muy poco dinero. En las siguientes páginas te explicamos cómo funciona y, si necesitas más información, ve a la página del proyecto de eBlocker en eblocker.org.

NAVEGA DE FORMA ANÓNIMA

PROTÉGETE DEL SEGUIMIENTO PUBLICITARIO

FILTROS PARA EVITAR CONTENIDOS PORNOGRÁFICOS Y SPAM

PROTECCIÓN INCLUSO DEL MÓVIL

Así era eBlocker. ¡ahora puedes construirlo tú mismo!

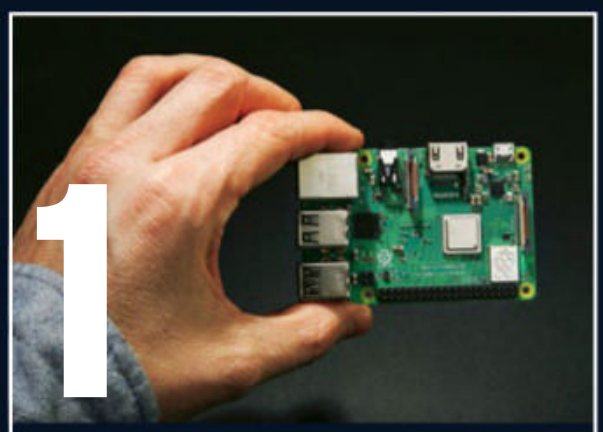
Esto es lo que necesitas:

Raspberry Pi

Carcasa

Software y tarjeta microSD

CREA TU eBLOCKER E



CONSTRUIR LA CAJA

Para poder construir el eBlocker, necesitas, en primer lugar, el corazón de tu dispositivo, el popular, versátil y económico ordenador Raspberry Pi. Hay diferentes versiones en las tiendas especializadas y también a través de Internet, por ejemplo, en Amazon. Elige el modelo que quieras: tienes el software más conveniente a tu disposición para todos los modelos de Raspberry Pi (2, 3, 3 B+ y 4) en la página web **eblocker.org**. Por supuesto, gratis.

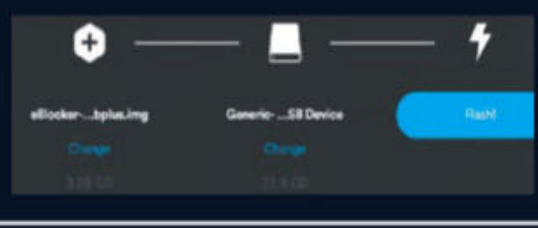
- **Montaje:** el montaje de la caja es sencillo. Solo tienes que colocar la placa Raspberry Pi en una carcasa adecuada. La carcasa la puedes conseguir por separado donde hayas adquirido la Raspberry Pi o puedes adquirir un conjunto completo de Rasberry y ya te vendrá incluida. Hay muchas configuraciones, incluso sets que incluyen los periféricos, adaptador de red, etc. para facilitar tu estreno. Cierra la carcasa y encájala bien.

INSTALAR EL SISTEMA

Ahora tienes que instalar el sistema operativo que corresponda. Hazlo con el ordenador en una tarjeta microSD que tenga al menos 8 GB de capacidad.

- **Preparación:** en primer lugar, visita la web **eblocker.org/en** y, en la página de inicio, selecciona la opción de ***eBlockerOS download***. Te llevará a otra página. Elige ahí ***eBlockerOS for Raspberry Pi 2-4 (565 MB Download)***. Para instalar el sistema operativo, lo mejor es descargarse una herramienta gratuita que te facilitará la tarea, llamada Etcher, desde su web **www.balena.io/etcher**.

- **Instalación del sistema operativo:** transfiere el sistema operativo de eBlocker con Etcher a la tarjeta microSD. Importante: no basta con copiar el archivo del sistema operativo en la tarjeta, se debe instalar, pero el proceso es muy sencillo. Inicia Etcher, selecciona con un clic en el icono de la izquierda el archivo del sistema operativo. Haz clic a continuación en el icono del centro y selecciona la unidad de destino, es decir, la tarjeta microSD que hayas conectado previamente. Haz clic ahora en ***Flash!*** y deja que Etcher instale el sistema operativo de eBlocker en la tarjeta. Cierra, a continuación, la ventana del programa.



CONECTAR

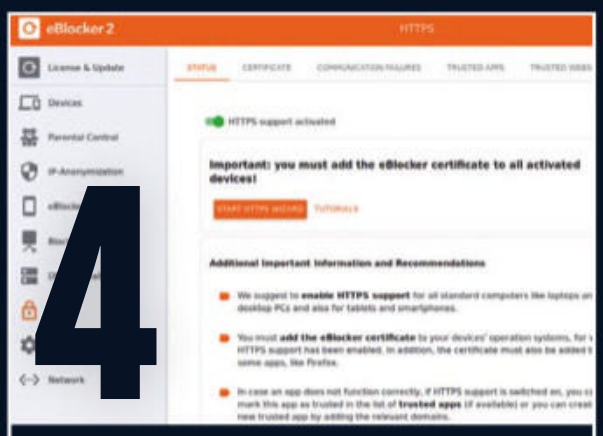
En el siguiente paso, convertirás tu Raspberry Pi definitivamente en un auténtico eBlocker que se encargará de proteger tu privacidad al navegar por Internet.

- **Instalación de la tarjeta microSD:** saca la tarjeta microSD con el sistema operativo ya instalado del ordenador. Introduce la tarjeta en tu Rasberry Pi. En función de la carcasa, puede ser necesario que saques el dispositivo de nuevo de la caja. En el caso de la Rasberry Pi 3 B+, la ranura para la tarjeta tiene este aspecto:

- **Conexión del eBlocker:** casi lo tienes listo. Enchufa ahora un cable LAN en el conector correspondiente de tu eBlocker y

conecta el cable, a continuación, con un puerto libre de tu router de Internet. Enciende la Raspberry y espera al menos cinco minutos hasta que se ponga en marcha el sistema operativo y se haya configurado. Importante: usa para tu eBlocker una fuente de alimentación separada de, al menos, 10W (15W para Rasberry Pi 4), ya que la gran mayoría de conectores de USB estándar de los ordenadores o routers no disponen de suficiente electricidad y pueden conllevar fallos en el funcionamiento del sistema.

EN 5 PASOS



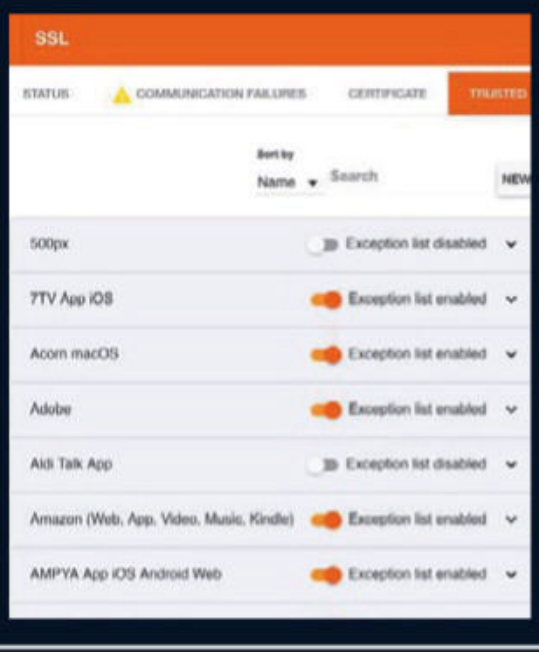
4 CONFIGURAR

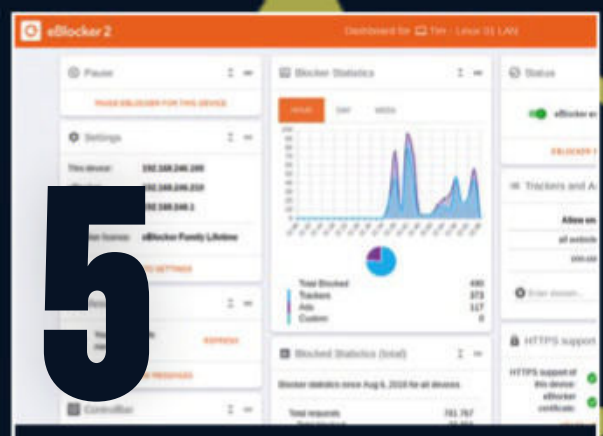
Ahora, tienes que configurar correctamente tu eBlocker. Para ello, vas a utilizar una interfaz web en tu nuevo ordenador.

- **Iniciar interfaz:** accede a la web ***setup.eblocker.com***. Si todo funciona bien, verás el icono de eBlocker en la esquina superior derecha de la pantalla. Ahí reconocerás que el sistema operativo de eBlocker está activo y que se protege tu privacidad. Con un clic en el icono, se abrirá la interfaz de usuario del sistema operativo de eBlocker. Tu vista general de eBlocker la encuentras en **eblocker.box** en cuanto esté el eBlocker activo.

- **Registrarse:** la primera vez que lo pongas en marcha, tendrás que introducir una clave de licencia. Introduce en el campo correspondiente la siguiente clave: FAMLFT-OPENSOURCE

El eBlocker instalará primero las actualizaciones, se reiniciará y estará listo.





5 A NAVEGAR

El eBlocker te protege de inmediato de los rastreadores publicitarios, anonimiza tus visitas a Internet e impide que tus hijos accedan a web con contenido pornográfico o violento mediante listas de filtros.

- **Recibir más información:** la mayoría de funciones de la interfaz de usuario son muy intuitivas. Ve haciendo clic en una u otra. ¿Necesitas más información o tienes una pregunta? Entonces ve a la página web oficial del proyecto eBlocker: **eblocker.org** y encontrarás un manual de uso detallado que podrás descargar, intuitivo como el mismo eBlocker y gratis.

- **Apoyar a eBlocker:** aunque el software de eBlocker es gratuito, ciertas cosas como la licencia de la lista de filtros o el desarrollo de las actualizaciones cuestan dinero. ¿Te gusta eBlocker? En la web de **eblocker.org/en/donate-and-contribute**, podrás ver cómo apoyar con un donativo este interesante proyecto.

EL ESCÁNDALO DE LOS DATOS

¿ESTAS SON TUS FOTOS?

Fotos privadas, pornografía, DNI y documentos personales: todo eso lo puedes encontrar en los discos duros de segunda mano en eBay.

Si compras un portátil nuevo o cambias de disco duro, no necesitas tirar el dispositivo viejo a la basura. Muchos de ellos pueden tener una segunda vida y encontrar un nuevo propietario en las plataformas de subasta. Pero, en muchos casos, el comprador no solo se alegrará por el nuevo hardware, sino porque también recibirá directamente un vistazo gratis a la vida del propietario anterior. Porque muchos de los dispositivos de almacenamiento de datos **no se borraron** o no se hizo bien. La frecuencia con la que eso pasa la muestra el sorprendente estudio de Kaspersky: en la mayor prueba realizada hasta el momento, el especialista de seguridad ha comprado casi 200 soportes de datos usados de particulares en la plataforma eBay y los ha analizado en el laboratorio. Y Computer Hoy tiene los resultados en exclusiva.

Un vistazo a la vida íntima de una persona

La dimensión del problema sorprendió incluso a los expertos. Pudieron echar un vistazo a los **datos más íntimos** de los antiguos propietarios: encontraron copias de recetas de medicamentos, documentos de identidad, declaraciones de la Renta o extractos bancarios, así como muchas fotos explícitas de parejas, fiestas o del cultivo privado de marihuana en el comedor. También son habituales las copias de tarjetas de crédito, listas de contraseñas, chats privados de WhatsApp o conversaciones de email, incluso cartas que narraban íntimas tragedias familiares. No hay nada que los almacenes de datos digitales analizados no contuvieran.

Lo que da miedo es que "para ver los datos en muchas ocasiones no necesitamos ni software especial", dice Marco Preuss

Fotografías y documentos personales pueblan los discos duros de segunda mano y apenas cuesta recuperarlos.

de Kaspersky. “En el 16% de los discos evaluados ni siquiera se habían borrado los datos o se encontraban en la papelera, sin vaciar”. Un clic sobre Restaurar es suficiente en estos casos para poder acceder de nuevo a ellos. Otros vendedores al menos habían intentado borrar sus datos formateando el disco. Pero está claro que muchos usuarios no saben que un simple formateo no significa que los datos realmente se hayan eliminado, porque pueden recuperarse por cualquier usuario mediante programas sencillos y gratuitos, y sin grandes conocimientos de informática.

Fallos de la tecnología

El trasfondo tecnológico es el siguiente: al formatear y borrar los datos normalmente solo se elimina la referencia a ellos en una especie de índice del disco. Pero **los datos siguen** donde están, hasta que sean sobrescritos. Mucho software especializado aprovecha esto para volver a hacer visible esa información. Estos programas fueron desarrollados para recuperar datos que se hayan borrado por error, lo que los profesionales llaman ‘File Carving’. Pero claro, estos programas también se pueden utilizar con fines maliciosos.

¡Hubo suerte!

Por suerte para los propietarios de los datos, el material acabó en las manos de Preuss y su colega Christian Funk. Siguiendo reglas

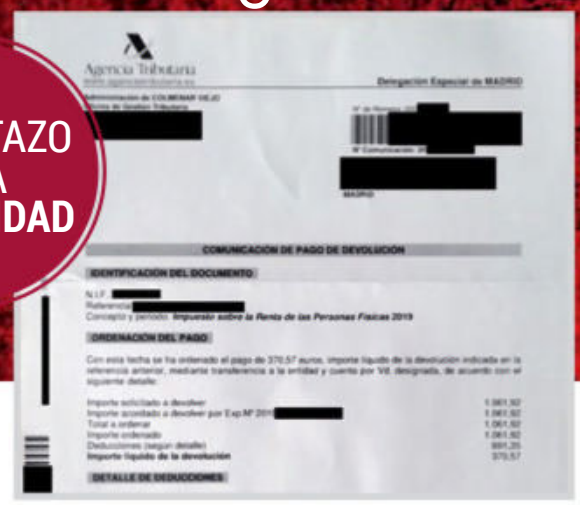
40%

de los usuarios realiza el borrado que restablece el estado de fábrica, lo que no elimina todos los datos. Y el 47% cree que así borra la información de forma definitiva.


装箱单(Packing List)

订单号 (OrderNo)	SDS20[redacted]	邮政编码 (PostCode)	28411	收件人 (Consignee)	[redacted]
国家 (Country)	ES	地址(Address)	[redacted]		

序号 (No)	EAN	物料号(Item)	物料名称(Item Name)	数量 (Qty)	
1	[redacted]	CP.MA.0000[redacted]	[redacted] Combo (EU)	1	[redacted]
2					
3					
4					
5					
6					


Agencia Tributaria

Delegación Especial de MADRID

[redacted]

COMUNICACIÓN DE PAGO DE DEVOLUCIÓN

IDENTIFICACIÓN DEL DOCUMENTO

N.I.F. [redacted]

Referencia [redacted]

Concepto y período: Impuesto sobre la Renta de las Personas Físicas 2019

ORDENACIÓN DEL PAGO

Con esta fecha se ha ordenado el pago de 370,57 euros, importe líquido de la devolución indicada en la referencia anterior, mediante transferencia a la entidad y cuenta por Vd. designada, de acuerdo con el siguiente detalle:

Importe solicitado a devolver	1.061,92
Importe acordado a devolver por Exp.Nº 201[redacted]	1.061,92
Total a ordenar	1.061,92
Importe ordenado	1.061,92
Deducciones (según detalle)	691,35
Importe líquido de la devolución	370,57

DETALLE DE DEDUCCIONES

UN VISTAZO A LA **PRIVACIDAD**

estrictas evaluaron los materiales siempre entre los dos, almacenaron los discos de forma segura y los destruyeron tras el análisis. Algunas fotos y documentos que mostramos son de ese estudio, pero se han anonimizado de forma que no se pueda identificar a nadie. Pero ¿qué podría hacer alguien con ellos si quisiera emplearlos para **extorsionar**, en lugar de investigar?

Material para chantajistas

Las fotos y documentos que aparecieron en el estudio realizado por Kaspersky hubieran sido muy adecuados para chantajear a los anteriores propietarios de los dispositivos analizados. ¿Quién sabe dónde pueden acabar las fotos comprometedoras? Seguro que a nadie le gustaría ver sus fotos de la última fiesta en los buzones de email de toda la empresa. Igual que el estado de sus cuentas bancarias o su situación familiar.

Naturalmente, está claro que no todos los compradores de discos son, automáticamente, chantajistas. Pero al mismo tiempo también es obvio que en las plataformas de subasta hay personas de todo tipo. Incluidas aquellas a las que les gusta **espiar la información** de otros.

El peligro es real: en una encuesta realizada a 1.000 usuarios, casi un 15% admitió que, si se encontraran datos personales por casualidad, al menos les echarían un vistazo. Y la cifra real seguro que es más alta. Además, el 9% de los encuestados admitieron que en el pasado **encontraron datos ajenos** en dispositivos usados.

El laboratorio confirma el alarmante análisis

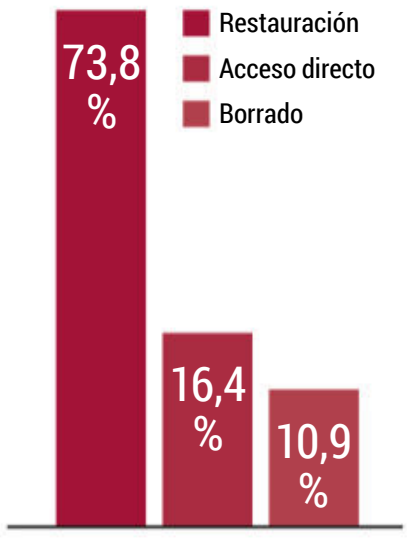
Los chocantes resultados de Kaspersky también preocuparon a la redacción de Computer Hoy. ¿Realmente es un problema tan agudo? La propia redacción hizo la prueba y compró cuatro discos duros al azar en la plataforma eBay. El responsable de los análisis, Mathias Otten, utilizó un software estándar para recuperar los datos: "¡Encontramos información a la primera!". Pieza a pieza apareció la vida de una docente de universidad, con una mezcla de sus emails personales y laborales, cálculos de costes, fotografías de estudiantes, vídeos privados y documentos copiados, así como comunicaciones con personal médico. "Este caso es especialmente grave, porque los **datos profesionales** deberían estar siempre cifrados", opinó Otten. Naturalmente, tras finalizar la prueba, Computer Hoy destruyó lo encontrado.

¿Mejor no venderlos?

¿Así que es mejor no vender tu hardware usado? No necesariamente, ya que casi todos los programas antivirus incluyen una función para borrar tus datos de forma segura, por ejemplo, en Kaspersky o Avira. Si

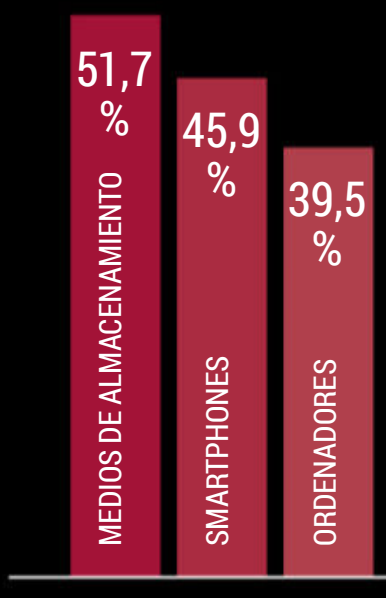
¿CÓMO SE ENCONTRARON LOS DATOS PERSONALES?

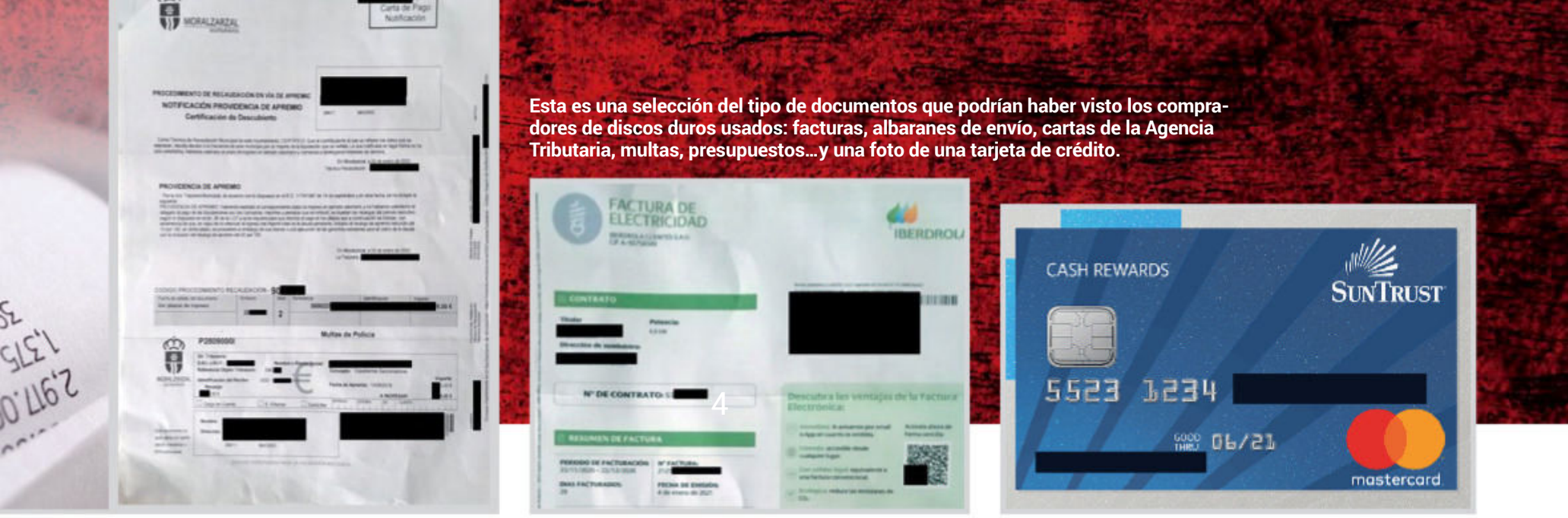
Más del 16% de los soportes de datos no habían sido borrados antes de realizar la venta. En el 74% bastó con un software para la restauración. Y solo el 10% de los soportes estaba 'limpio' y se había borrado correctamente.



DISPOSITIVOS USADOS QUE TIENEN DATOS

La encuesta de Kaspersky demuestra en qué dispositivos los compradores han encontrado datos personales alguna vez.





Esta es una selección del tipo de documentos que podrían haber visto los compradores de discos duros usados: facturas, albaranes de envío, cartas de la Agencia Tributaria, multas, presupuestos…y una foto de una tarjeta de crédito.

quieres vender tu disco duro con seguridad, también puedes arrancar el ordenador desde un DVD especialmente preparado o con una unidad USB e iniciar la destrucción de los datos desde ahí. Incluso el propio sistema operativo Windows viene con un programa para el borrado seguro de datos, la herramienta de seguridad Cipher.

A nivel de tecnología, todos estos programas tienen un modus operandi muy similar: **sobrescriben** las zonas de los datos borrados (en algunos casos también las zonas vacías) con datos aleatorios y lo hacen múltiples veces. De esta forma, un posible comprador solo recuperará ficheros sin sentido si empleara un software de ese tipo.

Y por cierto, también deberías preocuparte del destino de tus datos más preciosos cuando el hardware se hace tan viejo que solo sirve para el reciclado. Porque los dispositivos de la chatarra aparecen una y otra vez en lugares oscuros, y no siempre aquellos a los que estaban destinados. Para estar completamente seguro de que tus datos no caen en otras manos, desmonta el dispositivo y **destrúyelo mecánicamente**. Por ejemplo, un simple martillo puede ser el final definitivo de un disco duro o un USB.

¿Qué pasa con teléfonos móviles y tablets?

Los smartphones y tablets no formaron parte del estudio de Kaspersky. Pero en la conversación mantenida con Computer Hoy, el experto Christian Funk indicó que en este tipo de dispositivos se producen problemáticas similares. Porque, con la ayuda de un ordenador y unos cables, también puedes acceder a ellos mediante programas de software especiales.

En el caso de los iPhone y iPad, es suficiente con un reset de fábrica para obtener un borrado seguro de los datos, ya que Apple tiene la buena costumbre de **cifrar los datos** de los dispositivos desde hace años. Puedes encontrar esta opción en los ajustes bajo *General*, *Restablecer* y *Eliminar todo el contenido y la configuración*. En los smartphones y tablets Android deberías descargar una app de borrado específica de Play Store, como por ejemplo iShredder o CB Erazer. Primero cierra sesión en todas las apps de banca o de email, y también en redes sociales y apps de mensajería como Facebook o WhatsApp. Solo entonces inicia la app de borrado. Finalmente, resetea el móvil al estado de fábrica desde los ajustes, en *Sistema*, *Restablecimiento*, *Restablecer el teléfono*. Tras el reinicio automático, habrás terminado el proceso.

En los dispositivos Android acuérdate, además, de extraer cualquier tarjeta de memoria que haya insertada. En ella también puede haber datos privados o imágenes personales.

PERO ¿NO HEMOS APRENDIDO NADA?

“Las intenciones y la realidad son muy diferentes”.
Marco Preuss y Christian Funk Kaspersky

Computer Hoy: Todo el mundo sabe que es posible recuperar datos, pero da la impresión de que a la hora de la verdad, los usuarios dejamos de lado las buenas prácticas, ¿verdad?
Marco Preuss: Habíamos esperado, al menos, que se conociera más esta problemática, al fin y al cabo llevamos hablando sobre ello desde hace años. Pero los resultados del análisis demuestran, sobre todo, que la realidad y lo deseable no se parecen demasiado. Mientras que, en nuestra encuesta, la mayoría de los consultados dice conocer el borrado seguro, por otro lado hemos encontrado esa enorme cantidad de datos personales. Dicho de forma breve: falta mucho por concienciar todavía.

Algunas fotos reflejan situaciones que son embarazosas, pero no realmente peligrosas. ¿Dónde está el problema en lo que respecta a los documentos copiados?
Christian Funk: Puedes averiguar más a partir de los documentos de lo que el propietario puede pensar. Un ejemplo: hace poco un político envió un tuit con su billete de avión. Debido a una vulnerabilidad en el sistema de reservas, los atacantes pudieron averiguar datos personales como el número de móvil y de pasaporte a partir del código impreso en el billete. Siempre hay que tener cuidado, porque nunca se sabe qué puede hacer alguien con una información que parece inocua.

Para realizar este informe, en Kaspersky han manejado dos centenares de dispositivos que, en la mayoría de los casos, contenían algún tipo de información privada. ¿No resulta extraño construir una investigación en base a los datos personales de otros usuarios?
Marco Preuss: Por este motivo hemos empleado, sobre todo, métodos automatizados y no mirado los ficheros. Hacemos este tipo de estudios para mostrar que existe un problema y para explicar cómo evitarlo. Al término de la investigación, todos los datos fueron borrados.

CON UN ESPÍA EN

Los programas de vigilancia para el teléfono ganan terreno. El uso de apps de espionaje no solo no es ético sino que, además, se trata de un asunto bastante espinoso desde el punto de vista legal.

Qué detalles querríamos saber si pudiéramos echar un vistazo al móvil de nuestra pareja y amigos? Sobre esta idea, versa la comedia de Alex de la Iglesia 'Perfectos desconocidos', protagonizada por Belén Rueda y Eduardo Noriega, en la que unos amigos quedan para cenar y proponen un juego en el que tendrán que leer en alto todos los mensajes que reciban en el móvil y atender delante de todos las llamadas, de forma que se descubrirán sus secretos más sórdidos. No obstante, la vida real es menos divertida, ya que las personas celosas sí pueden espiar los móviles de sus parejas, mediante el uso de ciertas apps. Estas **registran en secreto todo lo que la víctima hace en su móvil** y reenvían la información automáticamente. Aunque resulta difícil de creer, estas peligrosas apps de espionaje, conocidas por el nombre de 'stalkerware', están a disposición de todos.

El espía accede a la información del móvil de la víctima cómodamente, a través de una interfaz online, y puede ver todas las conversaciones y llamadas.

Todo público: chats, Tinder, fotos...

El autor del delito coloca discretamente el stalkerware en el móvil, como si fuera un micrófono oculto, pero este 'micrófono oculto' no solo escucha conversaciones... los espías acceden a todos los mensajes de WhatsApp, la actividad en Tinder, la lista de llamadas, las citas del calendario, las fotos, los lugares en los que se ha estado y mucho más. La demanda de estas apps es alta. Un análisis de Kaspersky arrojó que el número de intentos de instalación de stalkerware ya había superado el récord de 37.000, tan solo de enero a agosto de 2019. Esto significa que el aumento a nivel mundial fue del 35%. No obstante, esto solo es la punta del iceberg de acuerdo con el investigador jefe de seguridad de Kaspersky, David Emm, ya que esta cifra procede solo de los móviles que incluyen alguna solución de seguridad de Kaspersky. Por tanto, el número real será bastante más alto.

En una zona gris

No es de extrañar la amplia expansión del stalkerware, ya que está al alcance de cualquiera.

EL BOLSILLO

Los vendedores de dudosa moralidad venden productos como FlexiSpy, PhoneSpector o mSpy, a modo de suscripciones temporales de lo que en apariencia son programas legales, a los hiperpadres o padres helicóptero para vigilar a los menores, justificando que lo hacen por proteger a sus propios hijos. En la letra pequeña, aparece el aviso de que, a partir de los 14 años, solo se puede utilizar este servicio **con el consentimiento expreso de la persona vigilad**a. Efectivamente, estas aplicaciones se encuentran en una especie de zona gris en lo que respecta a su legalidad, pero el stalkerware no solo no es ético sino que, además, es un asunto espinoso desde el punto de vista legal ya que, sin consentimiento, el espionaje está estrictamente prohibido. Si te pillan, te arriesgas a ser castigado con penas de prisión de uno a cuatro años y a multas de doce a veinticuatro meses, de conformidad con el artículo 197 del Código Penal español.

Vías para el espionaje

Pero ¿cómo instala el autor del delito el stalkerware en el móvil? Hay varias posibilidades:

- **Acceso físico:** si conoce el PIN para desbloquear el móvil, algo que no es nada raro entre parejas, puede instalarlo como cualquier app. Esta funcionará discretamente en segundo plano.

- **A modo de descarga:** el espía envía un enlace o un adjunto en un email, en el que se esconde el stalkerware.

Por lo general, es más complicado infiltrarse en un iPhone mediante una app de espionaje, si tienes la versión actual de iOS (como mínimo, la versión 12) y si no tienes el dispositivo liberado, es decir, si no usas otro sistema operativo alternativo. No obstante, el peligro es real si el atacante conoce la ID de Apple además de la contraseña de la víctima, ya que con ellas podrá acceder a las **copias de seguridad iCloud** que crea el iPhone cada día. Con estas copias, no habrá foto, chat o datos de ubicación que se le resistan.

Así puedes defenderte

Si como usuario de Android quieres ir sobre seguro, debes instalarte una buena aplicación antivirus, ya que estas suelen detectan de forma fiable las apps de espionaje. Son recomendables algunas de pago como Kaspersky, Bitdefender, Norton o ESET. Si te topas con apps de espionaje, tienes que restablecer los valores de fábrica del dispositivo. Asimismo, para que nunca llegues a ser objeto de un ataque, no deberías compartir tu PIN o contraseña de móvil con nadie.

AL HABLA CON EL ABOGADO

Christian Solmecke
Abogado

¿Es un delito el uso de aplicaciones del tipo stalkerware?
Sí, se incurre ya en delito con solo el intento: si instalas una aplicación de este tipo y después entregas el móvil a alguien que no sepa que está instalada. En cuanto se transmiten los datos, se aplican diversas sanciones por el espionaje de datos y por el uso de los datos interceptados (artículo 197 del Código Penal).

¿Cuáles son las sanciones?
Por interceptar las comunicaciones o utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, se castiga con penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. Las mismas penas se imponen si te apoderas, usas o modificas datos de carácter personal o familiar de otro que estén registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en registros públicos o privados, o si accedes sin autorización a los mismos y los alteras o usas en perjuicio de su titular. En el caso de que difundas los datos, te puedes enfrentar a penas de prisión de dos a cinco años. La pena, además, será la mitad superior de las nombradas si el que comete el delito es el cónyuge o pareja del titular.

¿Y en el caso de menores?
Muchos fabricantes de stalkerware venden productos a padres para vigilar a sus hijos. Sin consentimiento de los menores, solo se puede hacer hasta que cumplen 14 años. El consentimiento debe ser libre y los padres no pueden obligar o amenazar para que se lo dé. ■

ESTAFAS ONLINE
ROBO DE IDENTI

Si te roban la identidad en Internet, puede que tu doble se convierta en un gamberro por la Red y que eso te acarree problemas en la vida real. Aquí descubrirás cómo protegerte de esos robos de identidad.

Te apetece ahora realizar un pequeño experimento? Vale, entonces, desde tu página de perfil de Facebook, haz clic en tu nombre de usuario de la parte superior y, a continuación, pulsa en los tres puntos que aparecen justo a la derecha de ***Registro de actividad***, para así elegir la entrada ***Ver como***. Así, verás ahora tu perfil de Facebook, tal y como lo visualizan tus contactos. ¿En esta vista, puedes ver tu nombre y fecha de nacimiento? Entonces, tienes un problema.

Dobles odiosos

Para los delincuentes, tus datos personales son muy apetitosos. Con el nombre y la fecha de nacimiento, a veces es suficiente para poder comprar en Internet en tu nombre. Además, los datos personales no solo se guardan en Facebook, sino también en, por ejemplo, foros y tiendas online. Si los ciberdelincuentes se hacen, a su vez, con tu dirección, número de tarjeta de crédito o del carné de identidad, estás perdido. Los estafadores pueden, incluso, hacer contratos en tu nombre. El delito más habitual es, no obstante, **la estafa del crédito comercial**, que funciona de la siguiente forma: con tu nombre y fecha de nacimiento, los delincuentes realizan compras online contra reembolso. Como dirección de entrega, utilizan un punto de entrega, buzón o apartado de correos y, para la factura, utilizan una dirección falsa, por lo que la recibe de vuelta el vendedor. Este localiza tu dirección correcta mediante el nombre y la fecha de nacimiento, y encomienda a una empresa dedicada al cobro de impagos que te persiga para que pagues la factura.

Las tres prácticas más habituales

Además de **aprovecharse de los descuidos del usuario** para realizar la fuga de información, los estafadores se hacen con los datos personales principalmente de estas tres formas:

Técnicas phishing

Las posibles víctimas reciben correos electrónicos que parecen reales, por ejemplo, del banco, de un proveedor de pagos como PayPal o de empresas como Amazon. Normalmente, estos correos te piden que, por motivos de seguridad, hagas clic en un enlace e inicies sesión en algún sitio web. El enlace te lleva a una página online falsa, que guarda todos los datos personales que introduzcas allí

Técnicas spoofing

Este método es una variante del phishing. La diferencia es que, en vez de recibir un correo de un proveedor supuestamente serio, lo recibes de un remitente al que conoces personalmente y en el que confías pero que, por supuesto, es falso.

Técnicas pharming

Con este método, los estafadores no llevan a la víctima a una página falsa, sino que **instalan malware en su ordenador**. Lo hacen de tal forma que pasa desapercibido. El software malicioso redirecciona a los in-

Un manejo descuidado de los datos personales puede conllevar grandes daños

DAD

genuos usuarios del equipo, cuando consultan por ejemplo la página de eBay, a una versión falsa de la misma. Ahí, las víctimas introducen sus datos personales que van a parar a las manos de los delincuentes.

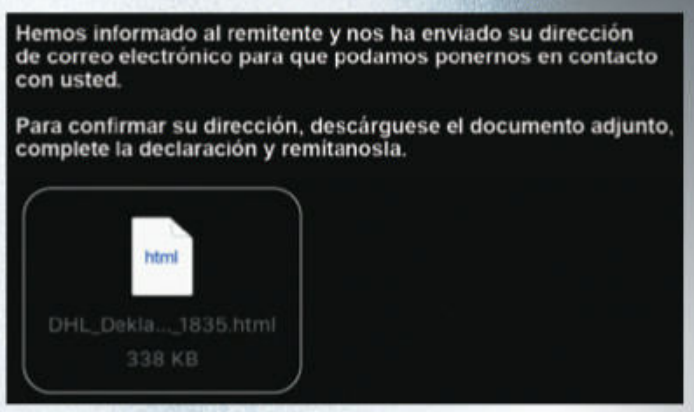
Grandes daños y nada de protección

Un robo de identidad causa grandes daños y **puede ser un lastre para la víctima** durante mucho tiempo. Los centros de protección al consumidor estimaron, en 2016, que el promedio de los daños financieros era de más de 1.300 € por afectado y, como muchas partes están involucradas, como tiendas, empresas dedicadas al cobro de impagos y autoridades, los procesos de esclarecimiento suelen ser bastante largos. Asimismo, resulta complicado e incluso imposible demostrar que uno mismo no ha cometido el delito. En la columna de la derecha, encontrarás varios consejos para protegerte del robo de identidad. Si eres víctima de una de estas estafas, deberías hacer lo siguiente:

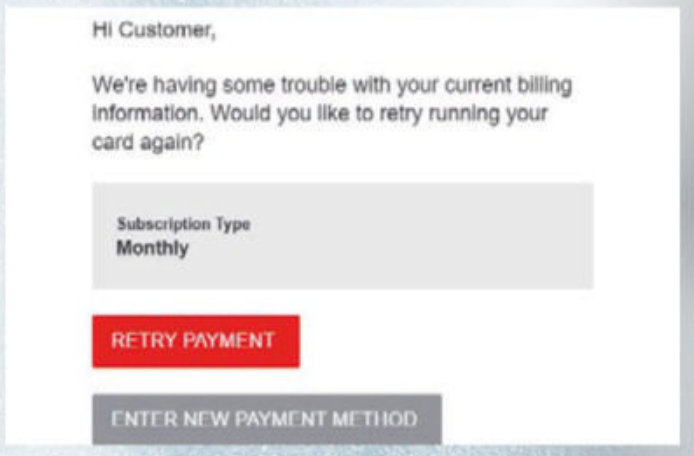
- **Presenta una denuncia:** ve de inmediato a la policía y presenta una denuncia. Aunque no haya ninguna ley sobre los robos de identidad, sí que la hay en relación a los delitos que se realicen a continuación, a partir de ella.

- **Bloquea tu cuenta:** si es necesario, pide al banco que bloquee la cuenta afectada de inmediato en cuanto notes movimientos raros. Así, evitarás problemas asociados.

- **Ponte en contacto con otros involucrados/perjudicados:** informa a los acreedores o a la empresa de cobro de impagos implicada sobre el robo. Puede venirte muy bien contar con un seguro de ciberriesgos, si afecta a tu empresa. En Internet, encontrarás ciberseguros de las aseguradoras conocidas y foros de perjudicados. ¡Échales un vistazo!



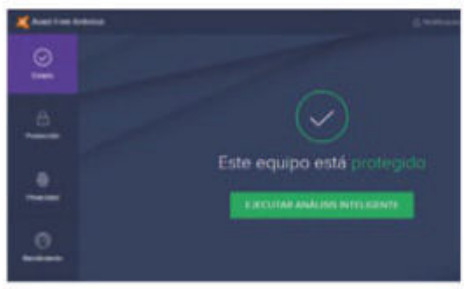
Pharming: el fichero adjunto del mensaje de correo es, en realidad, un software malicioso que roba datos.



Phishing: un supuesto email de Netflix, que te invita a hacer clic en el enlace para que introduzcas tus datos bancarios.

5 CONSEJOS PARA EVITAR EL ROBO DE IDENTIDAD

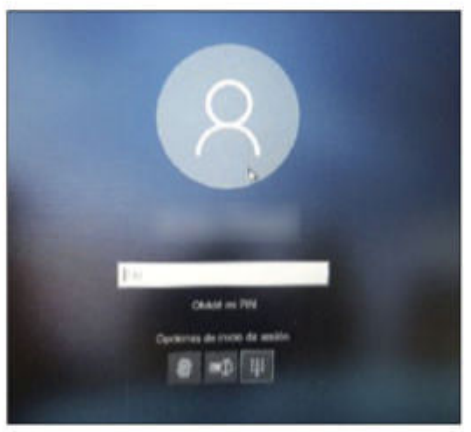
1 Instala siempre las actualizaciones recomendadas de los programas de tu ordenador y móvil, y usa un programa antivirus actual.



2 Utiliza contraseñas diferentes y complejas para cada tienda, plataforma o página web en la que inicies sesión. Puedes usar programas como KeePass para gestionar tus datos de acceso.

3 No abras nunca los adjuntos de los correos electrónicos si no estás seguro de que son fiables. Comprueba los emails que, aparentemente, proceden de conocidos. Y pregunta al remitente personalmente, si no estás seguro.

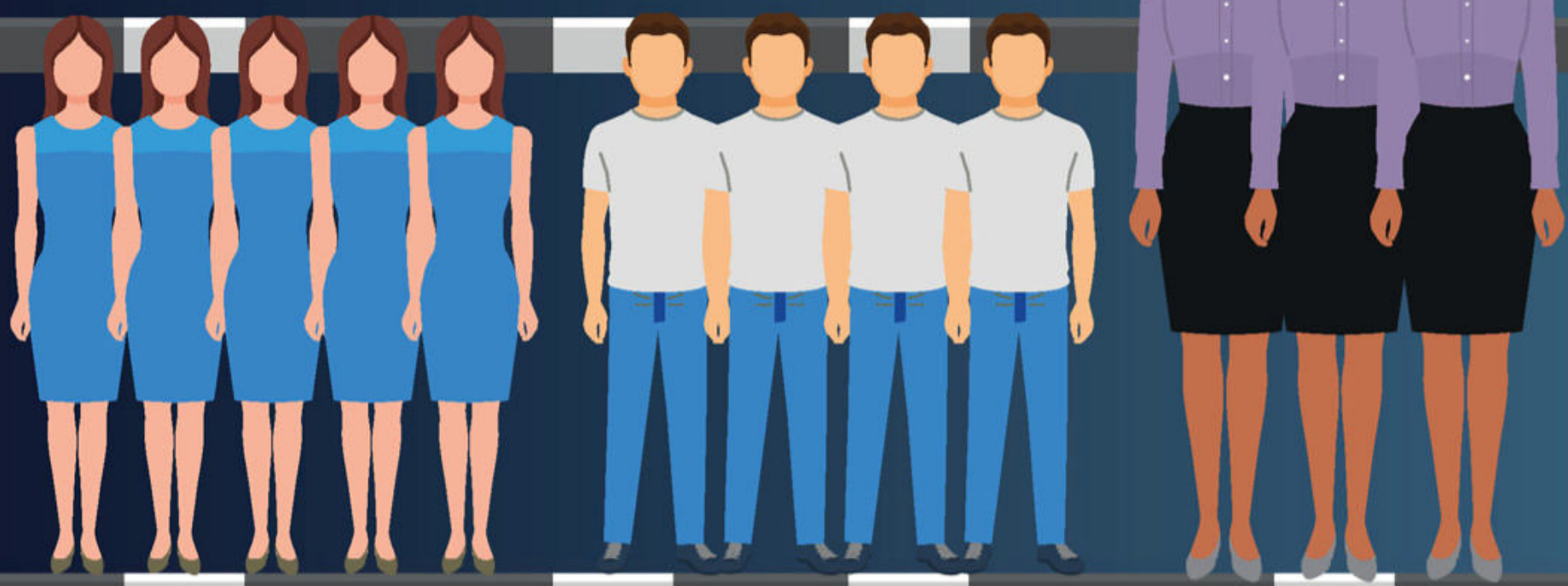
4 Inicia sesión con una cuenta de usuario normal con derechos limitados y nunca con la cuenta de administrador, si vas a navegar por Internet. De esta forma, podrás evitar fácilmente que el malware se instale en tu ordenador.



5 No proporciones demasiados datos personales por Internet. Si usas redes sociales, utiliza seudónimos siempre que sea posible y no introduzcas nunca tu fecha de nacimiento o dirección de casa. O, al menos, ocúpate de que solo tú y tus familiares y amigos puedan acceder a esa información personal. ■

CLONES EN EL SUPERMERCADO

¿Datos de acceso robados? Los hay en cualquier lugar en Internet, pero el Genesis Market maneja este negocio de forma especialmente pérfida.



Cuando se escucha la palabra 'cibercriminales', la mayoría de las personas piensan en talentos tecnológicos que, en algún momento, se han pasado al lado oscuro. Y eso ha ocurrido, sí, pero las cosas han cambiado bastante: si ahora quieres timar a tus congéneres a través de Internet, puedes ir simplemente al supermercado y comprar los datos de tus víctimas. Suena extraño, pero así es: Genesis Market ofrece en su plataforma **dobles digitales robados** en Internet. Computer Hoy ha echado un vistazo a este irreal mercado de los traficantes de datos, junto con el proveedor de soluciones cloud y de seguridad F5. Y hemos hablado con una víctima.

Sencillo y diabólico

El funcionamiento de este mercado ilegal es tan sencillo como inquietante: si te vas por él de compras, puedes buscar víctimas de determinados países o según diversos criterios. Para cada víctima hay **perfiles detallados** y te indican de qué servicio de Internet (por ejemplo Netflix, eBay o proveedores de Internet) es cliente el escogido.

Si compras su perfil, recibes toda la información, así como los datos de acceso, y puedes descargar todo eso en un cómodo contenedor. Este paquete se puede modificar con unos clics y utilizarlo en un navegador Chromium modificado que también puedes obtener en el Genesis Market. Y con ello se completa el círculo: porque el comprador ahora puede moverse por Internet con el navegador modificado **como si fuera la víctima**, ya que el paquete imita el equipamiento de su hardware y software, así como la ubicación aproximada.

Y, con ello, muchos de los mecanismos de seguridad de los servicios de Internet se pueden engañar. Porque, además de los datos de acceso, estos comprueban si el ordenador 'les suena'.

Los precios de los perfiles dependen de la actualidad, del número de servicios empleados y de las contraseñas disponibles. El precio final se paga en Bitcoins, en equivalentes de hasta varios cientos de euros.

¿Qué hay detrás?

Tremendo: el mercado ilegal se puede encontrar de forma totalmente abierta. Pero solo los miembros 'recomendados' pueden comprar en él. El antiguo empleado del FBI y la CIA Dan Woods estuvo observando este mercado durante bastante

tiempo. “Ya hace unos años que existe este mercado”, nos asegura Woods, que actualmente está trabajando para la compañía de seguridad F5.

Pero hasta el momento no se ha conseguido llegar hasta los responsables. “No todos los Estados colaboran en la persecución de los culpables”, explica Woods. Además, no es tan sencillo descubrir a estos ciberdelincuentes Es cierto que hay muchas pistas que apuntan a Rusia, pero también hay un ‘soporte de atención al cliente’ en este mercado criminal que contesta a las preguntas en un inglés perfecto. Hasta el momento, dice Woods, tampoco queda claro cómo se coleccionan los perfiles. Solo está claro que las víctimas caen mediante **malware** en algún momento. Es, por tanto, una caza muy difícil.

Búsqueda fructífera

Pero entonces, ocurrió algo decisivo para la investigación: un informante le pasó uno de los perfiles a Computer Hoy y comenzamos a indagar. Y, efectivamente, al cabo de un tiempo localizamos una de las víctimas: un hombre joven de Hamburgo. Este se mostró sorprendido cuando le llamamos y ofreció su colaboración de inmediato: “Hay que ayudar, para así poder avisar a otros”.

El experto de Computer Hoy, Mathias Otten visitó a la víctima y juntos le echaron un vistazo al portátil. Los datos en Genesis Market mostraban **accesos de varios familiares y conocidos** con diversas cuentas de Internet. Datos bancarios, contraseñas de eBay y más. “El ordenador es utilizado por varias personas” explicó la víctima, confirmando que la información era correcta. “Un golpe tremendo”, confesó. “Con eso cualquiera podría haber ido de compras”. Su perfil en Genesis Market es tan detallado que incluso contiene pistas sobre cuándo pudo comenzar la vigilancia. Una suerte para nosotros que la víctima nunca borró el historial de sus excursiones por la web y pudimos comprobar las páginas que se visitaron el día que comenzó el espionaje.

Genesis Market: aquí se negocian abiertamente conjuntos completos de datos de las víctimas, y el pago se realiza en la popular criptomoneda Bitcoin.

Es probable que el hermano de la víctima se bajara un programa ese día para convertir ficheros MP3. Desde una página que da de todo, menos confianza. Y este programa es el que seguramente incluía el malware. ¿Y el antivirus? Funcionando. Lo que demuestra que ninguna protección es perfecta.

Sigue la emoción

Ahora la víctima tiene que cambiar todas las contraseñas, porque si los datos cayeran en manos de criminales estos tendrían todas las puertas abiertas. Él se ha librado, pero hay miles de otras víctimas que pueden ser robadas de múltiples formas. Para que eso no ocurra, el joven colaborador le ha cedido el portátil a Dan Woods para que este pueda analizar el malware. La esperanza es que con el conocimiento sobre la tecnología puedan evitarse en el futuro nuevos ataques.

> **Un supermercado para criminales: ¿por qué nadie detiene esta locura?**
>
> **Dirk General-Kuchel**
> Redactor

LO QUE DICE EL EXPERTO

Dan Woods
Vice President Shape Security Intelligence Center en F5

¿Por qué se ocupa tanto del Genesis Market?
Nosotros nos dedicamos a apoyar empresas para que se defiendan del robo de datos. Por ello nos movemos por las plataformas ilegales. Queremos entender qué ocurre en ellas y observamos el Geneis Market desde hace un año.

¿Por qué es tan especial este mercado?
Genesis Market es más que un mercado para datos de acceso robados. Los criminales han encontrado un camino para imitar identidades digitales completas y así evitan hasta los mecanismos de seguridad más ingeniosos. Todos los conjuntos de datos solo se venden una vez pero, según su calidad, pueden costar varios cientos de dólares. Aunque parece mucho, imagina lo que puede hacer un atacante con acceso al email, al monedero Bitcoin, Netflix, Spotify o eBay. Lo que más miedo da es la simplicidad del sistema: cualquiera, sin demasiados conocimientos, puede abusar de estos datos. ■

MILES DE CLIENTES EN RIESGO

¿ES ILEGAL MI LICENCIA?

El negocio de las licencias de Windows y Office a precios por debajo de los oficiales sigue manteniendo tintes opacos. ¿Están sus clientes amenazados con un repentino cierre?

Windows 10 Pro al precio de 259 €? Quien quiera comprar el sistema operativo directamente a Microsoft probablemente se esté frotando los ojos al ver su precio oficial. Porque, si aún no lo ha visto por sí mismo, puede que alguien cercano le haya contado que el mismo producto cuesta en eBay y otros sitios de Internet **menos de 5 €**.

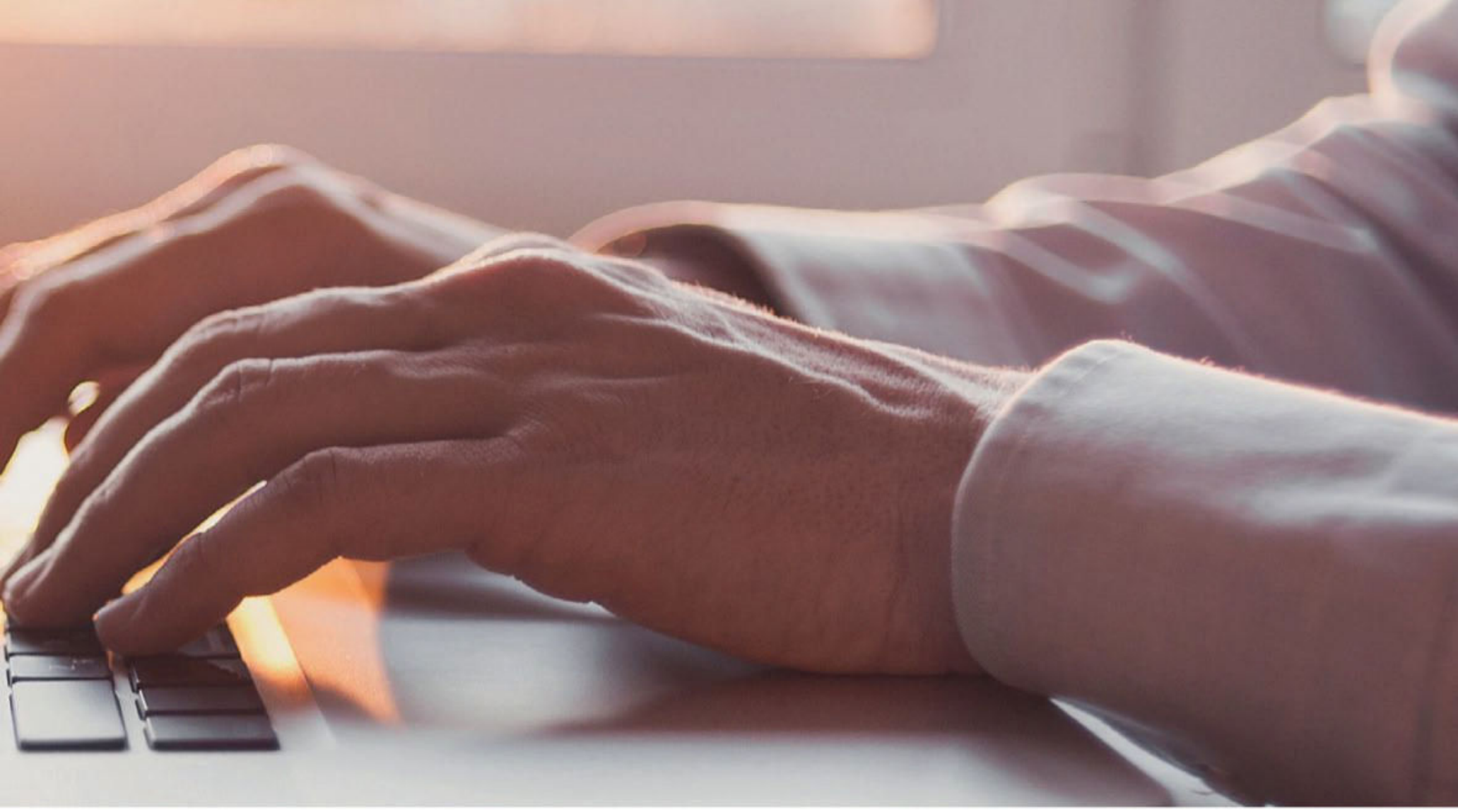
La descripción de estas ofertas puede sonar un tanto sospechosa, pero la mayoría de los clientes informan de una instalación exitosa, y por otra parte muchos pueden pensar que en una plataforma tan seria todo tiene que ser de fiar. Pero las dudas permanecen: ¿cómo se pueden explicar esta **diferencia de precios** tan radical? ¿Podría ser que, después de todo, haya gato encerrado?

Un mercado creciente

La cuestión de qué es legal y qué no cuando se intercambian licencias de software es tan antigua como complicada. Además de muchos comerciantes pequeños, unos pocos 'grandes' también han terminado por establecerse en el mercado de las licencias baratas de programas informáticos en los últimos años. Uno de ellos es la empresa alemana Lizengo, que también comercializa sus licencias de software en nuestro país.

Y de todos esos lugares tan económicos, fue precisamente en Lizengo donde se realizó hace poco un registro tras una denuncia de Microsoft. Sin embargo, por el momento la policía no ha colocado precinto alguno y Windows 10 Pro sigue disponible ahora mismo por menos de 50 €. Según manifestó Lizengo a Computer Hoy, actualmente está en marcha un **proceso civil**, pero rechazaron ofrecer más detalles. Microsoft no se muestra tan hermético en este caso: "Recientemente, han comprobado una serie de claves de producto que fueron vendidas por Lizengo a través de tarjetas de códigos de software o diferentes tiendas online (...). Se descubrió que las claves de producto ya **habían sido transferidas** a compradores anteriores y en algunos casos ya habían sido utilizadas para activar software original de Microsoft.

Esto se refiere a las tarjetas de la cadena de supermercados EDEKA en Alemania, aún disponibles hace unos meses. Tras hacerse pública la incertidumbre sobre la legalidad de su venta, Lizengo terminó por suspenderla, pero insistió en que el



modelo de negocio era sólido. Pero, ¿cómo pueden los comerciantes vender las licencias tan baratas? El origen de muchas de todas esas claves de producto provienen de las llamadas **licencias por volumen**.

Licencias por el mundo

Pongamos un ejemplo: la compañía ficticia Caleda compra un paquete de 2.000 licencias para los ordenadores de todos sus empleados. A cambio de alcanzar esta cantidad, la compañía recibe un precio por unidad muy bajo. Como Caleda no necesita todas esas licencias, vende las que han quedado sin utilizar a un concesionario. En la práctica, sin embargo, rara vez se trata de la compañía española Caleda, sino más bien de empresas chinas o de Europa del Este. En otras palabras, países en los que los licenciadores cobran **precios mucho más bajos** que en España, así que comprar allí es bastante lucrativo. El Tribunal de Justicia de la Comunidad Europea confirmó en un fallo de 2012 que las licencias por volumen pueden venderse individualmente, pero en ese momento se refería a programas informáticos destinados al espacio económico europeo.

Cruce de claves

Por lo tanto, Microsoft está buscando pruebas de una mala conducta y parece haber obtenido algo: claves de producto de la gama Lizengo ofrecidas por las **universidades china**s solo estaban originalmente destinadas a este mercado. En otro caso, las licencias fueron destinadas a una universidad danesa, pero esta institución negó haberlas comprado cuando fue interrogada por Microsoft.

Y también se encontraron claves de universidades búlgaras que fueron vendidas por Lizengo y estaban, según Microsoft, destinadas a ser activadas una sola vez. En otras palabras: todo el asunto es una complicada mezcla de cuestiones que al final tendrán que ser examinadas por un tribunal de justicia.

¿Qué puedo esperar?

Microsoft ha sido bastante indulgente con los consumidores finales. Si has adquirido una licencia de Lizengo o de otros vendedores y canales a un precio reducido y te parece dudosa, no hay que temer consecuencias. No se conoce ningún caso en el que el comprador haya sido procesado legalmente por estas compras.

Sin embargo, esto no tiene por qué seguir siendo así. Es concebible, por ejemplo, que un fabricante simplemente desactive el software con licencia dudosa a distancia o bloquee las actualizaciones. ¿Quieres comprobar la legalidad de tu licencia? Microsoft ofrece el llamado 'PID Checker', donde los clientes pueden hacer que se **compruebe la autenticidad** de su versión de Windows u Office. ■

> La compra de licencias es, a veces, como el Salvaje Oeste.

Carlos Gombau
Redactor Jefe

ORDENADOR Y MÓVIL SIEMPRE SEGUROS

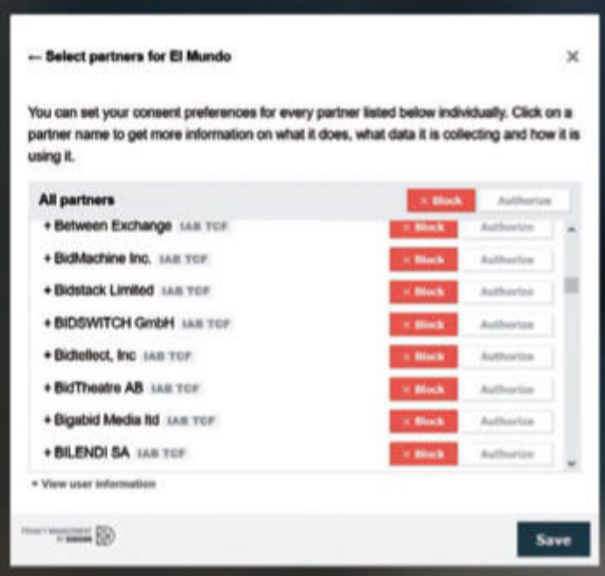
¡QUE NO TE ESPÍEN!

Nos pasamos el día rodeados de dispositivos tecnológicos conectados a Internet. El escenario perfecto para cualquiera que quiera 'saber' más sobre nosotros. ¡Evita que te espíen!

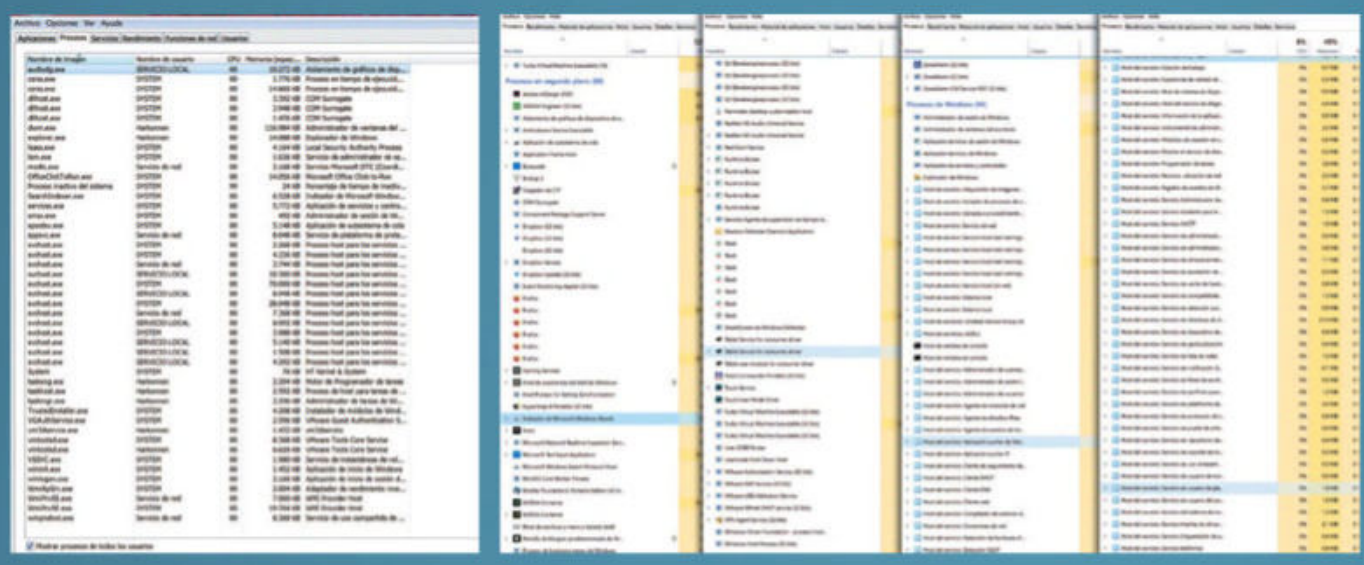
Aprende a...

Mejorar la privacidad en tu ordenador y teléfono móvil. Te proponemos una serie de herramientas que te ayudarán a prevenir el espionaje en este tipo de dispositivos.

Nadie quiere prescindir ya de su teléfono móvil, portátil o PC. Estos dispositivos se han convertido en parte fundamental de nuestras vidas y tareas cotidianas. El problema radica en que los creadores de estos dispositivos, o del software que empleamos en ellos, también se han dado cuenta de esto y lo aprovechan para aprender más sobre nosotros, con el fin de **enviarnos publicidad perfectamente adaptada** a nuestros gustos y así asegurarse el mayor número de ventas.



Para ver una noticia con una relativa privacidad, primero has de bloquear más de 300 redes de marketing y publicidad interesadas en tu actividad online.



Fíjate en estas dos imágenes. La de la izquierda es una captura del Administrador de tareas de Windows 7. La de la derecha es de Windows 10 y, en realidad, faltan algunos procesos al final de la lista. Los de Windows 10 son casi 100 (94) y son procesos internos que no dependen de cuántas aplicaciones tengas abiertas. Muchos solo están para saber qué haces.

En los últimos años, la privacidad personal online se ha visto perjudicada por las redes de publicidad. Si alguna vez te has molestado en decir 'No' a las ventanas de cookies que aparecen en todas las webs, te habrás fijado en que bajo 'Nuestros partners' puede haber 300 o 400 empresas... estas son las pueden recibir tus datos. Además, muchas de estas cookies son permanentes y de tipo 'tracking', lo que quiere decir que son capaces de **seguirte por varios sitios para saber qué camino online recorres**, cuánto tiempo le dedicas a cada sitio y cada cuánto regresas. Y eso se multiplica por decenas de miles, en cuanto varias redes colaboran.

El móvil, el gran rastreador

Hoy en día, basta con echarle un vistazo al móvil para saber de todo (y más) sobre ti. Ya sea el fabricante del teléfono, el desarrollador del sistema operativo o alguna de las apps que tienes funcionando en segundo plano en el terminal: todos pueden saber dónde estás y a dónde vas gracias al GPS, a qué velocidad te desplazas, si lo haces andando o en coche, cuántas veces usas el smartphone, si estás sentado o de pie (gracias al giroscopio)... Y, si tienes un reloj inteligente que te mide el pulso y los pasos, apaga y vámonos... hasta pueden saber si tienes alguna enfermedad latente, si eres deportista o sedentario, si sufres estrés... Y **da igual si eres de Apple o Android**, el resultado es el mismo.

El ordenador también te espía

A veces parece que la meta principal del sistema operativo no sea hacer funcionar el ordenador, sino **controlar lo que haces en él**. En ese sentido, Microsoft sabe lo que te conviene en cada momento e intenta hacerlo por ti. Pero eso no es lo peor. Ahora, Windows viene directamente preparado para esto y no es fácil desactivar estas funciones. Tu Windows sabe exactamente lo que haces en cada momento y lo registra con todo detalle, para así contárselo a Microsoft en cuanto puede. Y, si se te ocurre modificar tu Windows para evitar ese espionaje, llegan las actualizaciones permanentes que arreglan ese problemilla si llegara a presentarse, dejando las cosas como estaban antes de que tú, el usuario, tocara la configuración del sistema operativo.

Procesos y más procesos

En Windows 10 tienes, en todo momento, decenas y decenas de procesos funcionando en segundo plano, aunque en realidad no estés trabajando en Windows. Bajo **esta aparente inactividad**, se esconden procesos que se encuentran en marcha para Microsoft y que se encargan de recolectar datos sobre cómo usas tu ordenador, cuánto tiempo lo mantienes en marcha, qué aplicaciones usas, cuántos emails recibes, etc.

La buena noticia es que, tras su presentación, aparecieron las primeras aplicaciones para configurar los ajustes de seguridad de Windows y desactivar así el seguimiento de actividad, registro y estadísticas que el sistema implementa. También puedes hacer algo similar en tu móvil, para lograr que no te espíe. Nosotros te damos todas las claves.

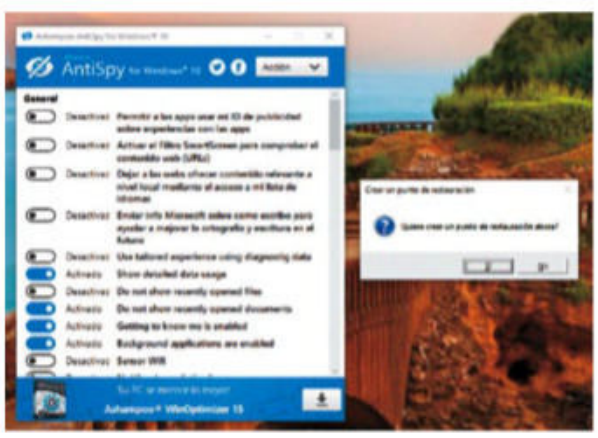
ASÍ EVITAS QUE WIND

Con Windows 10, Microsoft se ha subido al tren de las grandes empresas tecnológicas y recoge datos de los usuarios. Ahora, el sistema operativo también te espía.

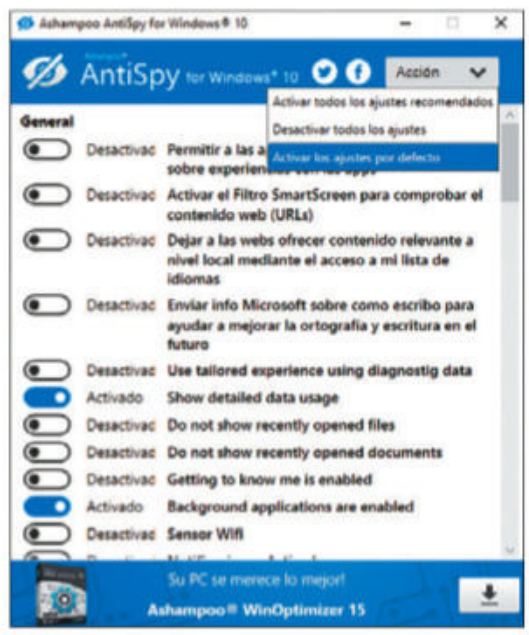
01 DESCARGA, INSTALA Y APRENDE A UTILIZAR ASHAMPOO ANTISPY

Como ya hemos mencionado antes, nada más salir Windows 10 al mercado, en 2015, aparecieron también aplicaciones para limitar la cantidad de procesos que funcionan en el sistema y cuya única finalidad es recolectar datos. La intención es evitar que toda esta información se envíe a Microsoft. Una de estas aplicaciones es Ashampoo AntiSpy. Es gratuita y, a continuación, te contamos cómo debes usarla para liberar el sistema de ojos y oídos atentos.

1 En primer lugar, descarga AntiSpy desde la dirección **bit.ly/3sjfBfv**. Pulsa luego sobre ***Download*** y descarga el fichero ejecutable. Verás que es extremadamente pequeño (menos de medio megabyte) y, además, no requiere instalación. Antes de ejecutarlo por primera vez, cierra el resto de programas, para así facilitar el trabajo de la aplicación. En su primera apertura, te sugerirá la creación de un punto de restauración. Esto es altamente recomendable, de modo que haz clic en ***Sí***. De esta forma, si tu equipo acabara configurado de algún modo erróneo o si algo empezara a funcionar mal, siempre podrás restaurar ese punto y todo volverá al estado actual de manera automática. Dicho esto, debemos decir también que Ashampoo AntiSpy es un programa muy seguro. Sin embargo, debido a que interfiere directamente con los ajustes del sistema, toda precaución es poca.



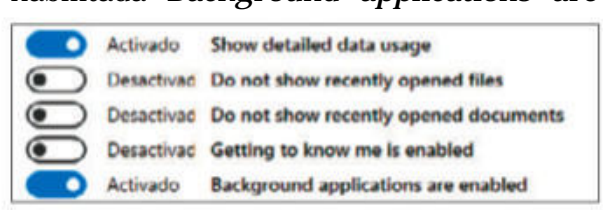
2 Una vez creado el punto de restauración, verás la interfaz principal del programa, que es extremadamente sencilla. Observa que simplemente se trata de una lista de opciones, que puedes activar y desactivar. El programa se ajusta automáticamente al español (o el idioma del sistema), con excepción de algunas entradas que siguen en inglés porque aún no están traducidas. En la parte superior derecha, aparece disponible una lista desplegable con algunas opciones para seleccionar grupos de ajustes. Por el momento, nada más iniciar la aplicación, déjalos como están.



3 Si te fijas, las opciones solo pueden estar activadas o desactivadas; el estado más recomendable puede variar en cada caso, según la función de la que se trate y del momento concreto. Nosotros te vamos a ofrecer ahora los ajustes recomendados de la redacción, pero cada caso puede ser diferente y es posible que quieras activar o desactivar alguna de las entradas, aunque nosotros digamos lo contrario. En general, de las primeras cinco opciones disponibles, la única que deberías mantener

habilitada es la denominada ***Activar el Filtro SmartScreen***. Esta se encarga de comprobar los sitios web antes de que accedas ellos y siempre que uses el navegador Edge. Naturalmente, para ello, ha de enviar la información de navegación a Microsoft. Si no quieres esto, desactiva también esta opción.

4 Por otro lado, verás que no hay ninguna opción para guardar los cambios. Se debe a que estos se realizan en el mismo instante en el que utilizas el regulador. Las siguientes opciones que te interesan son ***Show detailed data usage***, que te permite ver con detalle cómo usas las conexiones de datos de Windows, así como ***Do not show recently opened files*** y ***Do not show recently opened documents***. Estas dos desactivan la lista de documentos y de aplicaciones recientes en el menú Inicio de Windows 10; si prefieres conservar estas listas, deberás dejar activadas las dos opciones. Por último, es importante que dejes habilitada ***Background applications are***



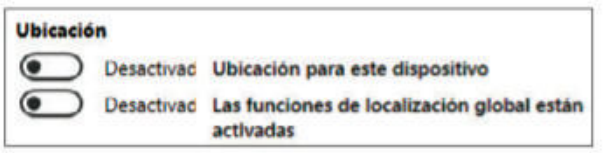
OWS 10 TE ESPÍE

enabled ya que, de lo contrario, se desactivará la posibilidad de mantener aplicaciones en segundo plano, y eso impide que la multitarea de Windows funcione correctamente. Solo en casos específicos querrás desactivarla (como un Windows en modo quiosco).

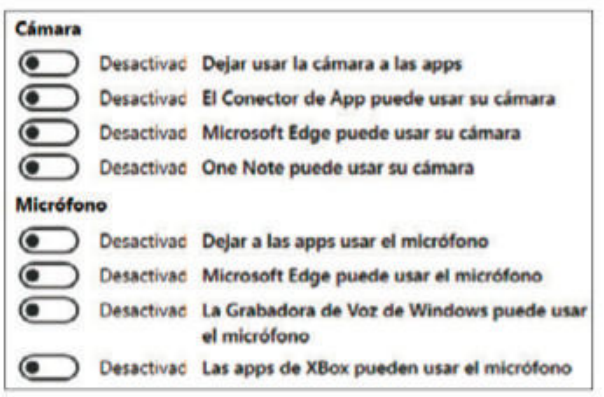
5 El próximo grupo de opciones es especialmente sensible, de modo que debes desactivarlas todas. La única que podría salvarse es ***Actualización automática de controladores***. Sin embargo, las cinco últimas, que empiezan por ***Let,*** son muy espías: uso de datos de diagnóstico, de datos

de email, de tareas y de contactos... Desactívalas y evitarás que tu lista completa de contactos acabe en manos de cualquiera.

6 A continuación, aparecen dos opciones que tienen que ver con la ubicación. No es imprescindible que se trate de un dispositivo móvil para que esta desactivación tenga sentido. Muchas aplicaciones utilizan los nombres de las redes WiFi que tienen a su alcance para cruzarlas entre sí y obtener una ubicación aproximada, aunque el equipo no tenga GPS. Eso, junto con la dirección IP que tienes asignada, puede situarte bastante bien en un mapa. De modo que, si no usas aplicaciones que necesiten tu ubicación, apaga ambos reguladores.



7 Seguidamente, verás dos grupos dedicados a la cámara y el micrófono. Si se trata de un portátil o un All-in-One, ambos estarán integrados; si es un ordenador de sobremesa, dependerá de lo que tengas conectado. En cualquier caso, con estas ocho opciones, puedes elegir si las aplicaciones recibirán o no acceso a la cámara y micró-



fono. Hoy en día, con el auge del teletrabajo y de aplicaciones como Meet y Zoom, es probable que tengas que activar algunas de estas opciones para poder trabajar y asistir a videoconferencias o reuniones remotas. Si no es así, puedes dejarlo todo apagado.

8 El próximo bloque contiene la configuración para el sistema de anuncios y publicidad integrado en Windows. En este caso, 'publicidad' también puede incluir consejos sobre cómo usar el sistema y sugerencias sobre nuevas apps. En principio, las siete opciones pueden estar apagadas y, especialmente, las dos últimas. Así, ***Receive ads by Bluetooth*** te permitiría recibir anuncios de tipo broadcast (para todos los que estén al alcance) mediante Bluetooth

(por ejemplo, en un centro comercial, evento o similar). La última entrada, ***Enable advertising ID***, es la que activa tu ID de publicidad. Ese es un número único con el que se te identifica, a la hora de mostrarte anuncios que te resulten más relevantes

¿QUÉ ES TU FINGERPRINT O HUELLA DIGITAL?

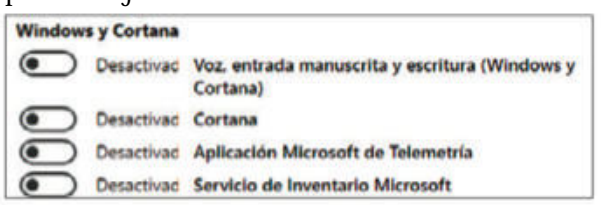
El término 'fingerprint' en inglés significa 'huella dactilar'. De modo que 'fingerprinting' es algo así como 'reconocimiento de huellas dactilares'. Sin embargo, ¿qué tienen que ver las huellas dactilares con el mundo de los ordenadores o teléfonos móviles? Pues mucho. Si tenemos en cuenta que las huellas dactilares permiten reconocer a alguien (ya que suelen ser únicas en cada ser humano, aunque hoy en día ya se hayan encontrado algunas duplicidades), el fingerprinting digital pretende lograr lo mismo, es decir, crear una especie de huella digital de ti.

¿Y por qué querrían hacer esto? Muy sencillo: para no contravenir las regulaciones de privacidad que indican que no pueden salir datos personales de un dispositivo, si no has dado permiso para ello. No obstante, la resolución de tu pantalla no es un dato que te pueda identificar, ni el tamaño de la ventana del navegador, ni los plugins que puedas tener instalados en el mismo, ni el tipo de navegador que usas, ni el número de iconos de la Barra de tareas, ni los programas residentes, ni la velocidad del procesador o el modelo de tu gráfica... nada de todo esto, así de manera individual, puede decir algo sobre ti. No obstante, si lo reúnes todo, resulta muy difícil que haya muchas más personas con exactamente ese mismo conjunto de datos. Especialmente, porque esa combinación de información suele ser mucho más extensa de lo que te hemos indicado antes. Existen cientos de parámetros 'inocuos' que, combinados, solamente aparecen en tu equipo. Así que a lo mejor no conocen tu nombre ni tu dirección, pero sabrán que eres tú en cuanto accedas a cualquier sitio web que

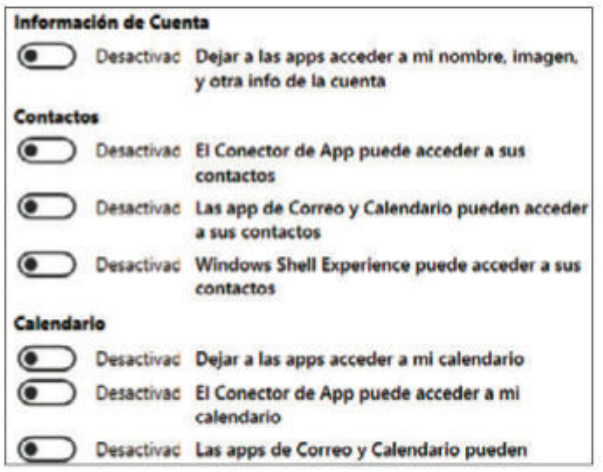
identifique algunos de esos datos. De esta forma, te podrán seguir en tus viajes por la Red. Y, aunque nunca facilites tu DNI, cuenta bancaria o datos personales, sí que sabrán lo que te gusta, lo que ves, cuánto tiempo juegas o trabajas... Y, si se cruza la información de múltiples bases de datos, ¿puedes imaginar cuál sería el resultado?

en función de tus gustos. Si desactivas el ID, las redes de publicidad lo tienen más difícil para saber quién eres (a menos que usen 'fingerprinting', ver recuadro de la página anterior). Esto no quiere decir que no verás anuncios, sino que los que aparecen serán al azar y no específicos para ti.

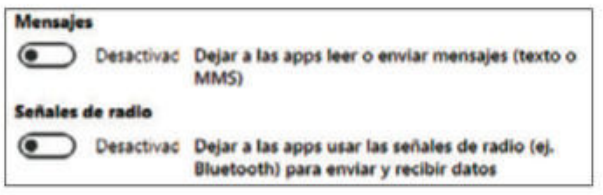
9 Un poco más abajo, tienes las opciones relativas a Cortana y otras dos especialmente peliagudas. Si no utilizas Cortana para nada, puedes desactivar los dos reguladores superiores. La función de 'telemetría' se encarga de mantener informado a Microsoft de cómo funciona tu equipo y, además, envía todo tipo de detalles técnicos para 'mejorar el sistema'. En cuanto al servicio de inventario, hace justo eso: llevar el control de todo el software que utilizas. Si no quieres que Microsoft se entere cada vez que instalas o actualizas algo, desactívala.



10 Y llegamos ya a la recta final. Los siguientes tres apartados son bastante autoexplicativos. Excepto el primero, que permite a las apps acceder a la información de la cuenta de Microsoft con la que has iniciado sesión, los demás se pueden activar o desactivar, según lo necesites. El peligro de dejar que cualquier aplicación acceda a los datos de tu cuenta de Microsoft es que, si has usado tu nombre real o una foto, te podrán identificar de inmediato.



11 Los reguladores ***Mensajes*** y ***Señales de radio*** deberían estar deshabilitados. El primero permite que las aplicaciones envíen SMS (si el dispositivo tiene una tarjeta SIM, por ejemplo) y el segundo es similar al que ya hemos visto para recibir información por Bluetooth. Sin embargo, en este caso se trata de información de cualquier tipo, no necesariamente anuncios. Así que, solo si vas a transmitir información por Bluetooth a un dispositivo móvil o electrónico, deberás activar esta opción.



RECUPERA UN PUNTO DE RESTAURACIÓN

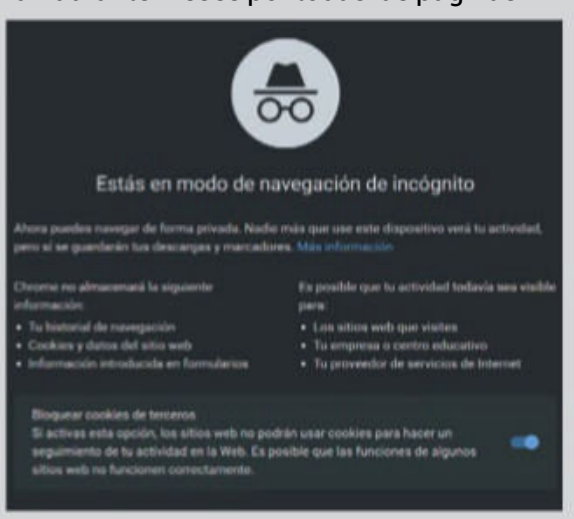
Si has creado un punto de restauración, ya sea con Ashampoo AntiSpy o O&O ShutUp (ver apartado de la siguiente página) y quieres volver a él, haz esto:

1. Abre el menú *Configuración* de Windows con las teclas Ctrl + I.
2. Escribe *recuperación* en la casilla superior y haz clic en *Recuperación*.
3. Pulsa en *Abrir restaurar sistema* y, a continuación, sobre *Siguiente*.
4. En el cuadro de diálogo que se abre, selecciona ahora el punto de restauración que te interese y continúa con otra pulsación en *Siguiente*.
5. Pulsa en *Finalizar* y espera a que termine el proceso de restauración.

12 El siguiente regulador se puede quedar apagado, si no vas a sincronizar varios dispositivos con los mismos datos. Por ejemplo, un sobremesa y un portátil, para que cuando copies algo en el portátil aparezca en el portapapeles del PC o similar. El caso de ***Microsoft OneDrive*** es especial: si usas OneDrive, debes dejar esta opción activada; si no, por ejemplo porque empleas Dropbox, Google Drive o similar, puedes desactivarla. Finalmente, ***Compartir actualización Windows*** es una descripción muy inocente que, en realidad, describe un ingenioso sistema para que los servidores de Microsoft no colapsen: si has actualizado tu equipo, Windows guarda una imagen del update en tu disco y, si alguien cerca de ti la necesita, se conectará a tu PC y la descargará desde ahí, en lugar de hacerlo desde un servidor de Microsoft. Si no quieres servir como centro de distribución de actualizaciones para el fabricante, desactiva el regulador.

VENTANAS PRIVADAS Y DE INCÓGNITO

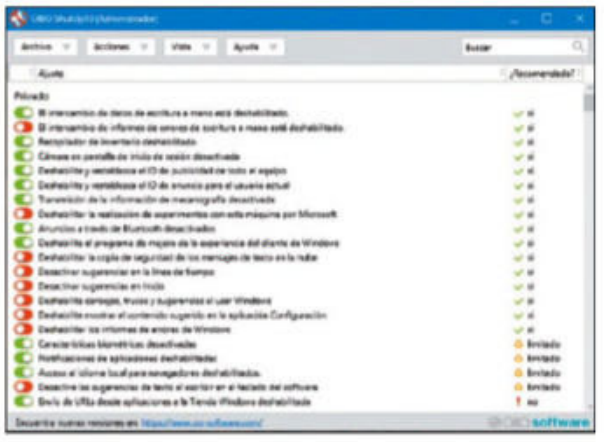
Todos los navegadores modernos incluyen este tipo de ventanas. Sirven para 'mejorar tu privacidad' porque, en cuanto se cierra una de estas ventanas, desaparece todo lo que hayas hecho en ella. No obstante, si navegas por Internet, la mayoría de los sitios te identificarán sin problema, con ayuda del fingerprinting (ver recuadro de la página anterior). De modo que no debes creer que, por usar una ventana privada, el sitio en el que estás no sabe quién eres. La única ventaja de esta función es que tu ordenador no acaba lleno de cookies innecesarias de webs que solo vas a visitar una vez, ya que el navegador las borra en cuanto cierras la ventana o pestaña de incógnito. En los tiempos del RGPD en la UE, en los que la mayoría de sitios web te piden confirmación del rastreo (lo que implica que pases algunos minutos configurando opciones, antes de ver lo que realmente quieres), las ventanas privadas representan una gran ayuda. Simplemente abre una ventana privada, di que aceptas todas las cookies, consulta lo que quieras y, cuando cierres esa ventana, las cookies desaparecerán. De este modo, no tienes que configurar nada y, al menos, no llenas el equipo de cookies rastreadoras que te perseguirán durante meses por todas las páginas.



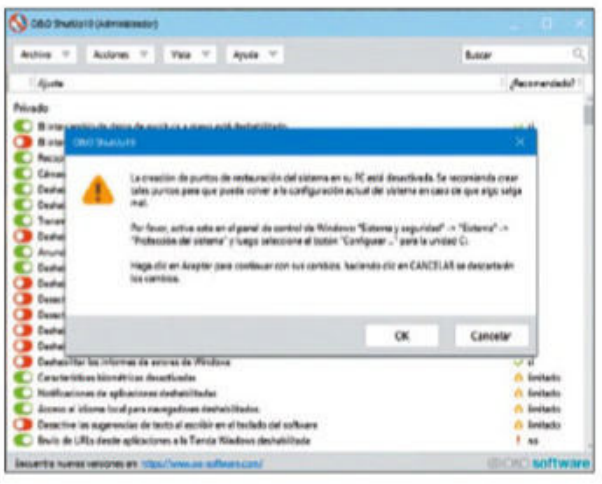
02 EVITA EL RASTREO EN WINDOWS CON AYUDA DE O&O SHUTUP 10

Otra alternativa para proteger tu privacidad y 'cortarle las alas' al sistema operativo es O&O ShutUp 10. Se trata de una aplicación gratuita con una finalidad idéntica a la de Ashampoo AntiSpy, aunque incluye algunas funciones únicas. Así que, si quieres estar realmente seguro en Windows, lo mejor es usar ambas. Utilízala sobre todo después de las actualizaciones, ya que es muy posible que con ellas Windows deshaga tus cambios para restaurar el sistema a un 'estado correcto'.

1 Descarga el programa desde **www.oo-software.com/en/shutup10** y ejecuta el archivo que obtendrás. Igual que en el caso de Ashampoo AntiSpy, no es necesario instalarlo y podrás usarlo directamente. Aunque su interfaz es muy similar a la de Ashampoo AntiSpy (con reguladores que activan o desactivan funciones), a la derecha hay más información que te indica si esa opción está recomendada o si es mejor que no la actives, a menos que haya una razón de peso.

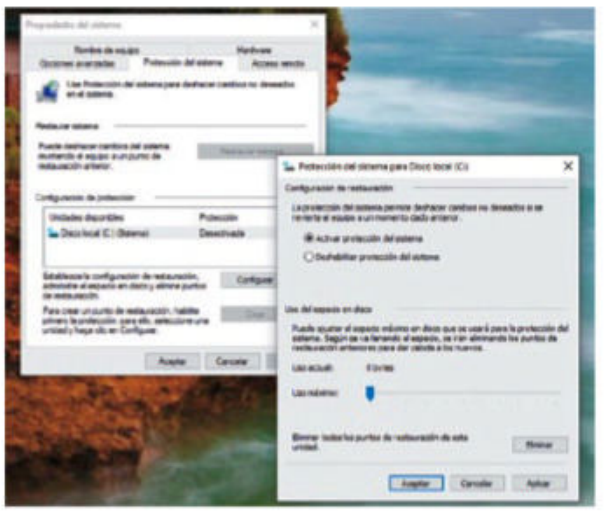


2 El primer paso consiste en crear un punto de restauración del sistema. Para ello, haz clic en ***Acciones*** y ***Crear un punto de restauración***. Si aparece un aviso, es



que tienes desactivados los puntos de restauración en Windows, pero eso se arregla en un momento, sigue leyendo.

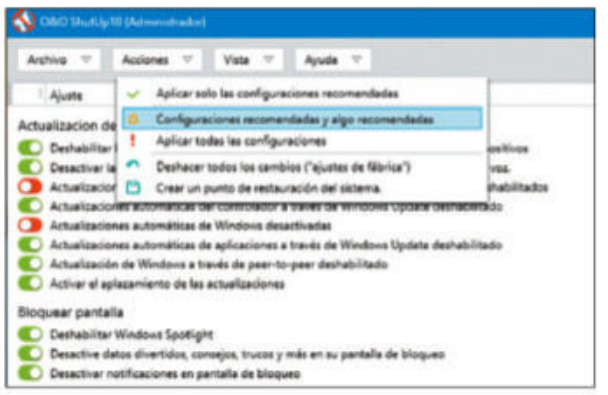
3 Abre la configuración de Windows con ⊞ + I y luego pulsa en ***Sistema*** y ***Acerca de***. A la derecha, localiza la entrada ***Protección del sistema***, asegúrate de que está seleccionado el disco ***C:*** en la lista central y haz clic en ***Configurar***. Luego, selecciona ***Activar protección del sistema*** y acepta todos las ventanas abiertas.



Ya puedes iniciar de nuevo la creación del punto de restauración desde O&O ShutUp. Haz clic en ***Sí*** y espera a que se cree el punto. A partir de ahora, podrás volver al estado actual si algo saliera mal o si no te gustan los cambios realizados.

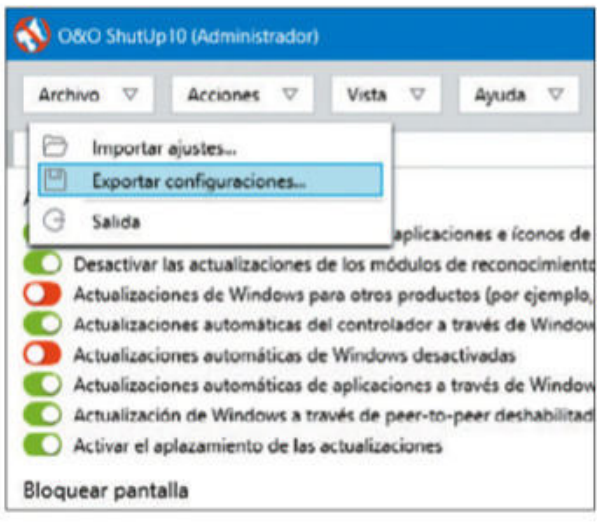
4 Una diferencia respecto a Ashampoo AntiSpy, es que O&O ShutUp incluye ayuda y te explica un poco para qué sirve cada opción. Simplemente, haz clic sobre la función que te interese (en nuestro caso ***Recopilador de inventario***) y se desplegará un texto de ayuda que, junto al icono de sugerencias, te ofrece bastantes pistas sobre si deberías o no modificar esa opción.

5 En general, puedes fiarte de la clasificación de opciones que ha hecho O&O ShutUp. Así que despliega el menú ***Acciones*** y selecciona ***Configuraciones recomendadas y algo recomendadas***. Esto ac-



tivará todos aquellos reguladores que pertenezcan a esas dos categorías. Al igual que en Ashampoo AntiSpy, tampoco tendrás que guardar nada, ya que los cambios se aplican inmediatamente en el Registro de Windows o donde sea necesario en cada caso. Solo en algunas circunstancias, al salir de O&O ShutUp, tendrás que reiniciar.

6 Otra ventaja de O&O ShutUp es que, si no estás del todo conforme con la selección de ajustes que hace el programa, puedes modificarlos a mano y luego guardar esa configuración en un fichero para más tarde poder volver a aplicarla en cuestión de segundos. Para ello, una vez que hayas realizado la configuración que te guste, pulsa en ***Archivo*** y ***Exportar configuraciones***. Asigna un nombre descriptivo al fichero y pulsa sobre ***Guardar***. Más adelante, si por ejemplo tu Windows se actualiza y quieres volver a aplicar la misma configuración que tenías antes, pulsa en ***Archivo*** y esta vez elige ***Importar ajustes***. ¡Listo!

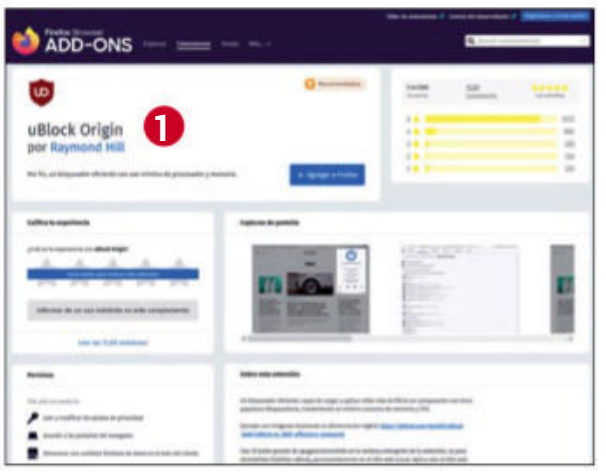


03 BLOQUEA EL SEGUIMIENTO AL NAVEGAR POR INTERNET

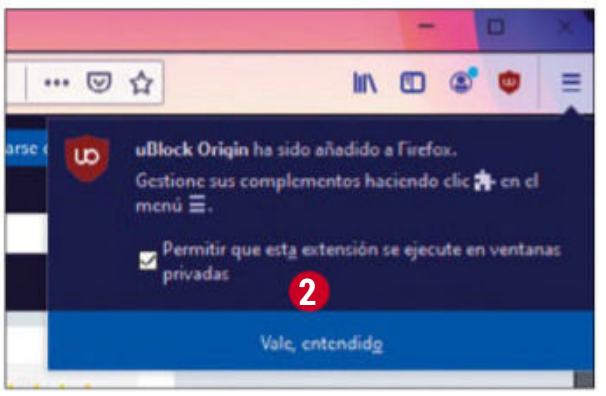
Aunque ya lo hemos mencionado en otras ocasiones, las cookies que utiliza tu navegador al visitar prácticamente cualquier sitio web se pueden utilizar para seguir tus pasos por Internet. Si diferentes sitios tienen acceso a una cookie en particular (por ejemplo porque usan la misma red de publicidad) y saben de qué página anterior vienes, pueden ir creando el rastro poco a poco. Y, como también te hemos dicho, es muy fácil crear el rastro de una u otra forma, ya que se utilizan cientos de redes. Google, Amazon, Twitter, Facebook y algunos otros son los indiscutibles reyes del seguimiento, precisamente porque viven de saber qué haces y de la publicidad que te muestran. Sin embargo, puedes poner freno a esta actividad, instalando complementos especiales en el navegador que impidan la persecución.

Uno de ellos se llama uBlock Origin y no es el típico bloqueador de anuncios, sino más bien un filtro de espectro amplio que analiza contenidos y bloquea aquellos que están marcados como publicidad o sirven para rastrearte. Está disponible para Firefox, Chrome, Edge, Opera y Safari. Vamos a ver ahora un ejemplo con Mozilla Firefox.

1 Abre el menú de las tres líneas y haz clic en ***Complementos***. Luego, escribe ***ublock*** en la casilla superior y selecciona ***uBlock Origin*** 1. Pulsa sobre ***Añadir a Firefox*** y ***Aceptar***. Por último, haz clic en ***Vale***, ***Entendido***, arriba a la derecha.



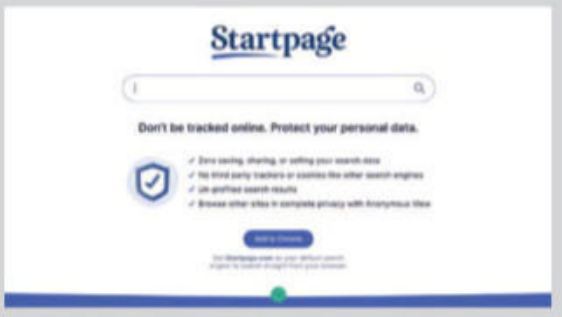
2 Si quieres que uBlock Origin también funcione en ventanas privadas, marca ahora la casilla correspondiente 2. A partir de este momento, ya tienes activada la protección y no tienes que hacer nada más.



BUSCADORES DE INTERNET ANÓNIMOS

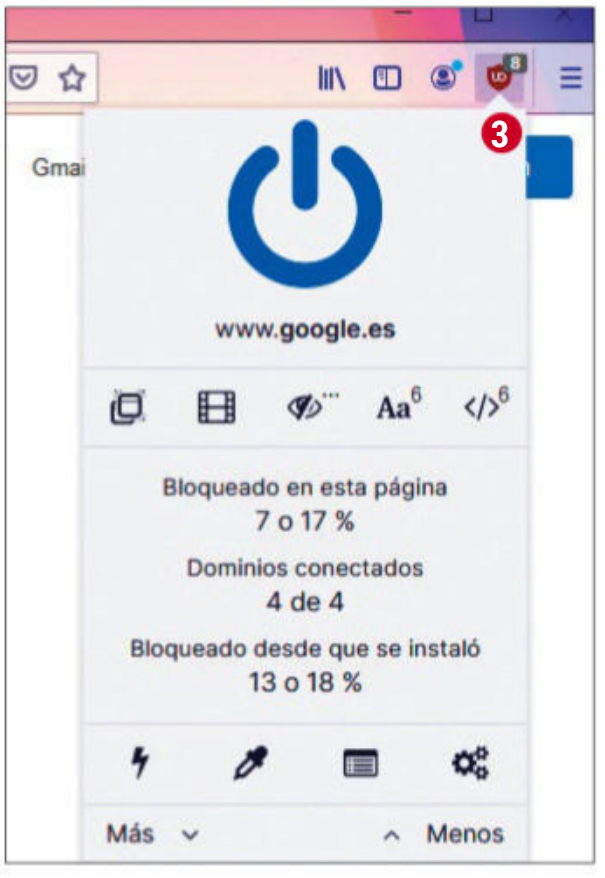
Cada vez que abres Google para buscar algo, sabes que miles de 'ojos virtuales' te están observando por encima del hombro. Si alguna vez te has fijado en la URL del resultado que se genera al realizar cualquier búsqueda en Google, habrás comprobado que no aparece directamente algo del tipo **www.unsitioweb.com**, por el contrario se utiliza una enorme ristra de letras, números y símbolos que le sirven a Google para identificarte, para etiquetar la búsqueda y poder medir el éxito que tiene eso que quieres localizar. Si no quieres que el 'Gran Hermano' te vigile así, puedes usar buscadores alternativos, que no realizan ese trazado exhaustivo de tus actividades. Dos ejemplos de ello son DuckDuckGo y StartPage.

- **DUCKDUCKGO duckduckgo.com**
  Se trata de un buscador propio, con su propia 'araña' (que recolecta datos en la web). Sin embargo, DuckDuckGo no almacena datos sobre ti, con lo que evitas la burbuja de información de Google, que siempre te enseña lo que cree que quieres ver (en base a lo que sabe de ti), en lugar de ofrecer resultados agnósticos y relevantes no tendenciosos. Además, no usa cookies y analiza más de 400 fuentes de datos, pero excluye a Google.



- **STARTPAGE startpage.com**
  En realidad, estás utilizando a Google, aunque de forma indirecta y filtrada. Es decir, StartPage envía tu búsqueda a Google para obtener los resultados, pero elimina todo lo que te pueda identificar y lo sustituye por datos aleatorios. Así, Google no sabe quién eres. Y ni siquiera el fingerprintig sirve, ya que StartPage genera estos datos al azar. Consigues resultados limpios y sin ser sustituidos por lo que Google cree que te va a interesar más.

3 Para configurar el complemento u obtener información de protección para la página actual (rastreadores bloqueados, etc.), pulsa el icono del escudo rojo, arriba a la derecha en la barra de direcciones 3. Recuerda actualizar la lista de filtros a menudo. Otra alternativa es Disconnect.



EVITA QUE TE ESPÍE EL TELÉFONO MÓVIL

Ya lo hemos mencionado anteriormente: tu smartphone es la máquina perfecta para espiarte. Lo sabe todo sobre ti y siempre te acompaña allí donde vayas. Ponle fin a eso de una vez por todas.

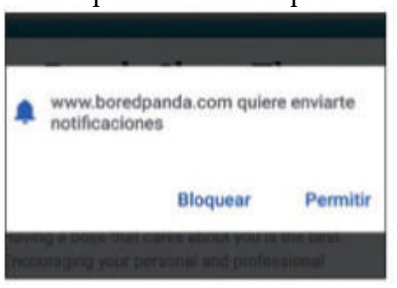
01 INSTALA ADBLOCK BROWSER Y CONTROLA LA PUBLICIDAD

Este navegador con privacidad, desarrollado por eyeo GmbH 'limpia' las páginas web antes de enseñártelas en pantalla, analizando el código HTML y de programación y eliminando la mayor parte de los anuncios. Si lo usas, en lugar de tu navegador habitual del móvil (como Chrome o Firefox), verás muchos menos anuncios mientras viajas por la web. Así es cómo lo puedes utilizar:

1 Para empezar, descarga la app desde el store y ábrela. En la primera pantalla te ofrece la posibilidad de renunciar a que tus datos se compartan con la app. Sin embargo, la herramienta funcionará igual aunque desmarques esta casilla. Una vez hayas tomado la decisión que consideres oportuna, pulsa en ***Continuar***.

2 Verás la típica pantalla de navegador móvil. La barra de direcciones está en la parte superior y debajo tienes ya ocho marcadores de sitios web populares, que te sugiere AdBlock Browser directamente 4. Aquí puedes colocar los que quieras y sustituirlos por tus sitios favoritos.

3 Ahora, si navegas por cualquier sitio web y este intenta cualquier cosa como, en el ejemplo, convencerte de enviar notificaciones, podrás bloquearlas de inmediato y para siempre. También podrás observar que la mayoría de los anuncios de ese sitio, si no la totalidad, han desaparecido.



4 Si quieres configurar el bloqueo de los anuncios, simplemente toca en el icono de AdBlock Plus y, desde el menú que se despliega, podrás activar o desactivar el bloqueo de anuncios con el regulador ***Bloquear anuncios molestos***. Con la entrada ***Interrumpir el bloqueo de anuncios***, podrás ver los anuncios de las webs durante un tiempo, pero luego se volverá activar la función automáticamente.

5 Si deseas configurar el programa con algo más de precisión, toca en ***Más ajustes de bloqueo de anuncios*** y llega-

GOOGLE APUESTA POR LA PRIVACIDAD

Las cookies son archivos que se generan con la actividad de navegación que haces en Internet. Esa información sirve a las empresas para crear anuncios personalizados. Ahora, Google va a eliminar las cookies en busca de una web más privada y segura. En el blog de Google se hace referencia a un estudio realizado por Pew Research Center donde comentan que el 72% de los usuarios sienten que casi todo lo que hacen en Internet está siendo observado por los anunciantes y empresas. A su vez, el 81% cree que los riesgos de esta dinámica superan los beneficios que se puedan obtener con la publicidad personalizada. ¿Cuándo se llevará a cabo el cambio por parte de Google? No hay datos al respecto, solo las intenciones de eliminar las cookies de seguimiento y no volver a adoptar ninguna medida similar. No son los únicos del sector que van a eliminar las cookies. Lo que diferencia al navegador Chrome de otros es que la competencia sustituirá las cookies de terceros por identificadores alternativos a nivel de usuario. Google, en cambio, afirma que ellos no seguirán esos pasos.

rás a esta pantalla 5, en la que se te ofrecen posibilidades adicionales. Una de ellas es ***Anuncios aceptables***. Observarás que, a pesar de usar este navegador, todavía verás algunos anuncios. Estos son los que están marcados como 'aceptables' por organismos internacionales (no son de juegos de azar, sexo, etc.). Si tampoco quieres ver este tipo de anuncios, desactiva esta opción y desaparecerán. Las demás funciones están bastante bien explicadas en el propio menú, con lo que puedes hacerte una idea de para qué sirve cada una de ellas.

LA SEGURIDAD EN ANDROID VS. APPLE

Desde siempre, el sistema operativo móvil de Apple ha tenido la fama de ser más seguro que Android. Y eso es así porque iOS es un sistema operativo cerrado y propietario, no como Android, que es Open Source. De este modo, les resulta mucho más difícil a los hackers encontrar posibles vulnerabilidades en los dispositivos iOS.

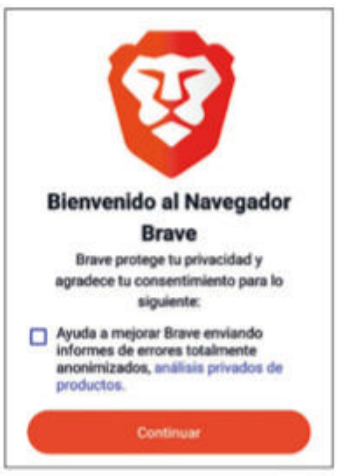
Por otro lado, Android es mucho más popular como sistema operativo para móviles que iOS, lo que lo convierte en la diana favorita de los hackers. Y es que, ya que se van a tomar el esfuerzo de encontrar una vulnerabilidad, al menos que afecte al máximo número de dispositivos.

Sin embargo, esto no quiere decir que iOS te proteja del seguimiento cuando navegas ni te asegura que tus datos no puedan caer en manos extrañas. Para la próxima versión, Apple ha anunciado que incluirá un sistema de bloqueo del tracking de Facebook, pero eso está por ver. Hasta entonces, usar un navegador con mayor privacidad siempre ayuda. Incluso en un iPhone.

02 NO DEJES RASTROS NI PISTAS CON BRAVE PRIVATE BROWSER

Con este nombre tan sugerente, este es otro navegador que quiere ofrecerte una navegación 'limpia', eliminando la mayor parte de los anuncios así como popups u otros elementos intrusivos que dan la lata cuando intentas navegar desde el móvil. Al igual que AdBlock browser, también intenta detener a todos los rastreadores posibles, para que así no te puedan seguir la pista de una web a otra. O, al menos, dificultar esa tarea todo lo que sea posible.

1 También en el caso de Brave, una vez hayas instalado la app en tu dispositivo móvil y la ejecutes por primera vez, verás una pantalla en la que se te pide que permitas el envío de datos anónimos de uso. Puedes consentir o no, eso no afectará al funcionamiento del navegador. Pulsa sobre ***Continuar*** cuando hayas acabado con todo el proceso.



2 La siguiente pantalla que verás también es similar a la de Brave. En este caso, puedes activar los llamados ***Informes de privacidad***. Esto significa que cada semana obtendrás un informe sobre aquellos sitios que visitas y que más anuncios tienen o más rastreadores emplean, para invadir tu privacidad. En este caso, el programa asegura que ningún dato sale del móvil, de modo que las estadísticas se generan a nivel local, en tu propio dispositivo. Si te parece útil la información que te ofrece, puedes activar estos informes con ***Activar informes de privacidad***: si no es así, cierra el cuadro de diálogo desde el aspa superior.

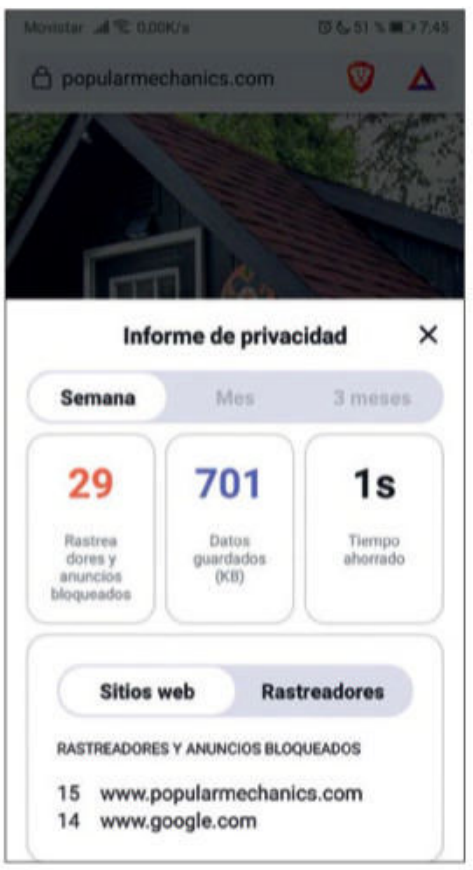
3 La primera vez que pulses en la barra de direcciones, podrás elegir el motor de búsqueda que quieras. Si valoras tu privacidad, deberías elegir ***DuckDuckGo***, ***Startpage*** o

Qwant. Aunque también puedes recurrir a Google o Bing, si así lo deseas. Pulsa sobre ***Guardar*** cuando te hayas decidido.

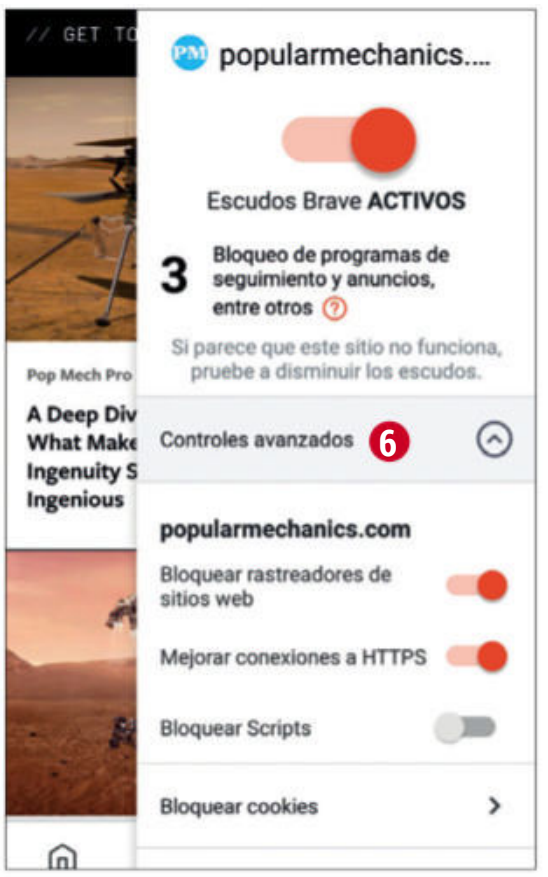
4 De forma parecida a AdBlock Browser, al tocar sobre el icono del león que hay en la esquina superior del programa, a lado de la barra de direcciones, podrás ver tanto

las estadísticas de bloqueo de la página actual, como activar o desactivar el bloqueo de los anuncios, por si quisieras verlos.

5 Con la opción ***Consultar todo el informe de privacidad*** (si activaste esta función durante el paso anterior), también verás las estadísticas de bloqueo que llevas hasta el momento. Además, desde la parte superior, puedes elegir el periodo de tiempo para las estadísticas que quieres ver. Así, puedes elegir entre la semana actual, el último mes o los últimos tres meses. También verás, en la parte central inferior, qué sitios son los más insistentes y curiosos, y qué rastreadores los más frecuentes.

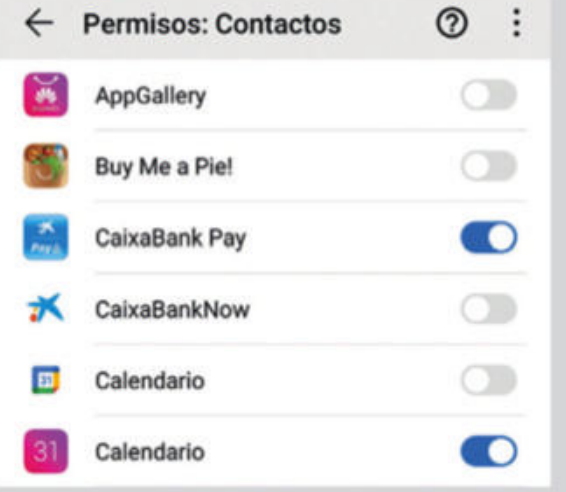


6 Por otro lado, si accedes a la función ***Controles avanzados*** 6 del menú anterior, tendrás acceso a controles más detallados, que te ofrecen la posibilidad de bloquear de forma independiente los rastreadores, los posibles scripts que se ejecuten en una página, las cookies o los fingerprinters. No obstante, ten siempre en cuenta que, según los ajustes que lleves a cabo en este cuadro de diálogo, es posible que algunas páginas no funcionen o que lo hagan incorrectamente. En ese caso, deberás ir asignando permisos hasta conseguir el equilibrio entre una web funcional y la máxima privacidad posible.



LAS APLICACIONES DE PC Y MÓVIL

Esto es algo que todos conocemos: instalas una app en el móvil y, antes de ver siquiera la primera pantalla, aparecen varias ventanas que te piden permiso para acceder a la ubicación, lista de contactos, llamadas, hacer fotos, recibir o enviar SMS en tu nombre, etc. La lista es infinita y su longitud depende solo de la imaginación de los desarrolladores, en lo que se refiere a espiar tus actividades con el móvil. Ten en cuenta que, en muchos casos, las apps piden por pedir. Y lo malo es que, si deniegas algún permiso, aunque no tenga nada que ver con el funcionamiento de la app, es muy probable que esta no funcione.



Es lógico que una app de cámara te pida permiso para acceder al almacenamiento, ya que necesita guardar las fotos; y, claro, también necesita acceso a la cámara y al micrófono. Pero ¿para qué quiere ver mi lista de contactos o enviar SMS? O esa app de recetas, que quiere acceso al GPS... ¿para qué? ¿Para sugerirme dónde comprar las patatas más cerca de casa?

Y luego está el envío de datos 'anónimo'. Sí, es perfectamente posible que no se envíe tu nombre o número de teléfono o IMEI al proveedor de turno, pero eso no significa que no te puedan identificar en cuestión de décimas de segundo: tu marca y modelo de móvil, las apps que tienes instaladas, número de contactos... ¿cuántas personas crees que tienen el mismo conjunto de datos que tú en el mundo? Así que, si alguna otra app ya ha enviado esa información a una de las múltiples bases de datos de marketing que hay en la Red, y lo ha hecho con tu nombre o número de móvil, todos sabrán ya quién eres. Y eso aunque la mayoría no envíe realmente tu nombre o número (ver el recuadro 'Fingerprinting').

Y lo peor es que en el PC la cosa empieza a ser cada vez más parecida. El sistema operativo crea permisos (micrófono, cámara, etc.) para que te sientas seguro a la hora de denegarlos pero, si realmente lo haces, el software no funciona. Aunque sea un permiso absurdo que nada tiene que ver con el propósito del programa. La única solución a este dilema es buscar un programa distinto, que no sea tan codicioso a la hora de recoger tu información personal.

LA GUÍA DE SEGURIDAD DEFINITIVA

A SALVO EN INT

El mundo conectado es una verdadera bendición, pero estar online tanto tiempo tiene sus propios peligros. Te explicamos cuáles son los riesgos en Internet en 2021 y cómo protegerte de ellos.

Aprende a...

Protegerte cada vez que te conectas a Internet: compras online, sistemas de protección infantil, envío de datos de forma cifrada, conexión WiFi segura, antivirus, firewall...

Voy a comprar" ya no implica necesariamente salir de casa. "Cojo un Uber" o "Hazme un Bizum" de pronto tienen sentido, y "¡búscalo en Google!" es una especie de encantamiento universal para encontrar lo que sea. Fuera de una película distópica, es difícil imaginarse ya un mundo sin Internet. La Red de redes ha venido para quedarse y, de hecho, si hoy en día te quedas sin conexión, es realmente difícil seguir tu vida normal. No tienes tele, no puedes leer noticias, escuchar música, comprar, pedir cita en el dentista, saber el tiempo que va a hacer mañana o jugar. Pero t**ambién tiene su lado oscuro**. Está claro que un medio de comunicación universal atrae al crimen. Resulta tremendamente atractivo para aquellos que buscan hacer dinero fácil o, simplemente, sembrar confusión: hackers malos y cibercriminales.

¿A qué amenazas te enfrentas?

¿Por qué hemos dicho 'hackers malos' específicamente? Porque el término 'hacker' está muy devaluado en el idioma común y normalmente tiene connotaciones negativas y criminales. Pero un 'hacker' no es más que alguien que 'utiliza una cosa de una forma para la que no estaba prevista'. Es decir, que le busca una funcionalidad nueva y alternativa. No mala. Claro que los 'Black Hat Hackers' (hackers de sombrero negro) utilizan estas artes para el mal y su propio beneficio. Y son ellos los que han creado todo el malware al que te enfrentas hoy en día:

- **Virus:** programas cuya meta es **destruir ficheros o el ordenador completo**, pero no antes de multiplicarse todo lo que puedan, para esparcirse al máximo. Una versión del virus es el 'gusano', que tiene más interés en replicarse que en hacer daño.

- **Troyanos:** aplicaciones que aparentan ser una cosa cuando en realidad son otra. Normalmente **quieren robar tus datos, contraseñas** o abrir puertas traseras en el equipo para cometer un delito.

- **Phishing:** mensajes de email, SMS o similar que parecen proceder de una fuente de confianza y que te instan a pulsar en un enlace para 'reactivar tu cuenta', 'impedir el bloqueo', 'recibir un regalo gratis', etc. En realidad, te conducen a un sitio en el que puedes infectarte por un virus o, peor, en el que introduces tus datos que, de inmediato, son usados por el hacker.

- **Ransomware:** los 'cryptolockers' son programas muy traidores. Cifran el contenido de tu equipo para que no puedas usarlo sin una contraseña. Esta la tiene el hacker y te la dará a cambio de un pago en Bitcoin (que no se puede trazar). O a lo mejor no te la da... pero con el dinero se va a quedar seguro.

¿Dónde está el malware?

Malas noticias: en cualquier sitio. Basta un descuido o una imprudencia, y ya puede ser demasiado tarde. Los lugares más comunes donde encontrarlo son estos:

Foto: depositphotos.com

Como el caballo de Troya, los troyanos son aplicaciones que aparentan ser una cosa cuando en realidad son otra, para así poder engañar al usuario.

- **En la web:** y no es necesario que sea una web extraña, de piratería o similar. Puede ser la más inocente del mundo, porque el propietario **no se haya dado cuenta de que está infectada**. Y, con las últimas técnicas, no es necesario ni que pulses en enlaces o similar. Según tu configuración de seguridad o tipo de navegador, es posible que el código malicioso se ejecute sin más.

- **En un email:** es el lugar más común. Un clic sobre el enlace equivocado y acabas en una web que te infecta. O bien ejecutas un programa que en realidad es un virus, troyano, gusano, cryptolocker o similar.

- **En redes sociales:** un lugar en el que hay mucha interacción entre personas y muchos clics. No hay nada como publicar algo atractivo o viral para que miles de personas pulsen sobre ello. ¿El resultado? Lo has leído en el primer punto.

- **Vulnerabilidades de software**: es de los más insidiosos, aunque el más sencillo de resolver. Hoy en día, el software y los sistemas operativos son muy complicados. Y, si no los mantienes al día, puede haber errores que los hackers **aprovechan para entrar en tu sistema**, colarte un virus o cosas más ingeniosas y malvadas.

ERNET

APRENDE A PROTEGI

Con seguridad, conoces algunas formas de protegerte, porque hoy en día ya son parte de la sabiduría popular. Una suite de antivirus o un firewall son las más comunes y, probablemente, las más efectivas. Sin embargo, hay otras formas de defenderte mientras estás online. Te hablamos de todas ellas.

01 MANTÉN TU SISTEMA OPERATIVO Y EL SOFTWARE ACTUALIZADO

Este es uno de los métodos más sencillos y efectivos de proteger tu equipo de ataques. Un software actualizado tiene menos vulnerabilidades y, por lo tanto, les pone las cosas más difíciles a los hackers. ¿Eso significa que tu sistema es impenetrable? Para nada. Pero los hackers van a lo fácil y prefieren atacar sistemas con más vulnerabilidades, porque les ofrecen más probabilidades de éxito. ¿Para qué molestarse con un sistema más seguro, si hay miles desprotegidos un poco más adelante?

1 En Windows 10, debes asegurarte de que tienes activadas las actualizaciones automáticas. Para ello, abre el menú ***Configuración*** con ⊞ + I y haz clic en ***Actualización y seguridad***. En las versiones recientes de Windows, no puedes desactivar las actualizaciones, aunque sí retrasarlas o desactivarlas durante un tiempo. Para lograrlo, pulsa en ***Opciones avanzadas*** 1.

2 A continuación, verifica que en ***Pausar actualizaciones*** se encuentra marcada la opción ***Seleccionar fecha*** 2. Esto quiere decir que no tienes las actualizaciones pausadas. De paso, verifica que está activada la opción ***Recibir actualizaciones para otros productos de Microsoft***.

3 Por otro lado, comprueba también regularmente que tus programas habituales están actualizados. En especial tus navegadores. Normalmente, puedes ver el estado de actualización en el menú ***Acerca de*** (como por ejemplo en Firefox, en la imagen 3). Esto te asegura que tu herramienta principal para navegar por la Red es todo lo segura que se puede. En otros programas, se corrigen fallos y vulnerabilidades.

¿PUEDO SUBIR MIS DATOS A LA NUBE SIN PROBLEMAS?

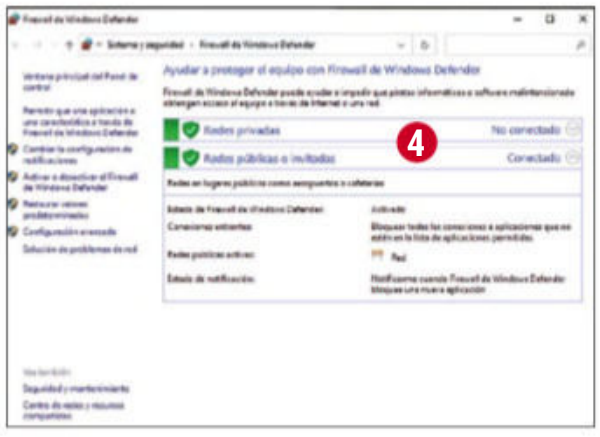
La respuesta corta es sí. Sin embargo, como siempre, es cuestión de tener un poco de sentido común y de tomar precauciones. Si subes las nóminas del mes de la empresa, las fotos de tus hijos o la escritura del piso, deberías tener cuidado y cifrar esos datos. Aunque la mayoría de los servicios cloud realizan el cifrado por su cuenta, cualquier precaución es poca. ¿Cuántas veces hemos oído en las noticias que se han 'escapado' cientos de miles de datos de cuentas de usuario de algún servicio? No obstante, si utilizas servicios online como Dropbox, Google Drive, iCloud, WeTransfer y similares, en general puedes estar tranquilo. Sin embargo, intenta siempre que esa no sea la única copia de tus datos, sino que también tengas una en local. Y cifra también los datos importantes, por si acaso (ver apartado 05). Son unos segundos adicionales al usar esa información, pero tienes la tranquilidad de que los ficheros estarán mucho más seguros.

ERTE EN INTERNET

02 UTILIZA SIEMPRE UN FIREWALL Y TAMBIÉN UNA SUITE ANTIVIRUS

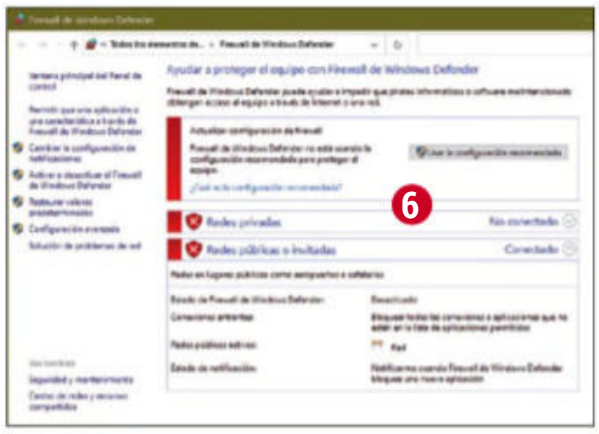
La misión de un firewall no es otra que la de bloquear los posibles accesos desde fuera al PC y controlar las conexiones de salida. Es decir, es una especie de 'portero' que vigila todo lo que entra y sale, y lo permite o no según unas reglas que estableces. ¿Cómo te protege esto? De entrada, evitando que alguien se pueda conectar a tu PC sin que lo sepas. Así no podrá aprovechar una vulnerabilidad (ver apartado 01), para conseguir el control del equipo. Si no usas un firewall de terceros, comprueba que el de Windows está activo.

1 Para ver que el firewall de Windows está actualizado y funcionando como es debido, abre el menú ***Configuración*** del sistema con + , escribe ***fire*** en la casilla superior y selecciona luego ***Firewall de Windows Defender*** en la lista. Si ves una imagen como la de la figura 4, con todo en verde, es que estás protegido. Si te fijas, puedes establecer dos niveles de protección: uno para la red local de casa (***Redes privadas***) y otro para Internet.



2 Como alternativa, puedes usar un firewall de los que vienen integrados normalmente en los antivirus, o bien uno independiente como ZoneAlarm Free Firewall, que es gratuito y protege tu PC de intrusiones de una forma más dirigida que el firewall de Windows. Puedes descargarlo desde **www.zonealarm.com**. La instalación y configuración es muy sencilla, especialmente si utilizas el modo automático. A partir de ese momento, cuando un programa quiera acceder a Internet, ZoneAlarm te preguntará si quieres permitirlo o no. Así tienes un control completo 5.

3 Si, por casualidad, visitas la pantalla del firewall de Windows cuando tienes otro firewall instalado y funcionando, no debes alarmarte de verlo todo en rojo 6. Eso es porque el firewall de Windows está apagado, ya que no es posible que ambos funcionen a la vez, porque se 'pelearían'. No obstante, lo importante es que sigues estando protegido perfectamente.



4 Por su parte, los antivirus modernos, prácticamente de cualquier fabricante, ofrecen una capa de seguridad imprescindible para tu sistema si te pasas mucho tiempo online. En realidad, lo que llamamos 'antivirus', hoy en día son en realidad suites de seguridad muy completas que cubren numerosos aspectos de la seguridad. No obstante, si no quieres comprar un antivirus comercial por el motivo que sea, debes saber que, desde hace un par de versiones, el antivirus que viene con Windows ya es medianamente decente. No se puede comparar con un producto de los grandes fabricantes, pero cumple con su cometido de forma razonable, para ser gratis. Si quieres comprobar el estado de este antivirus o modificar su configuración, puedes hacerlo de la siguiente manera.

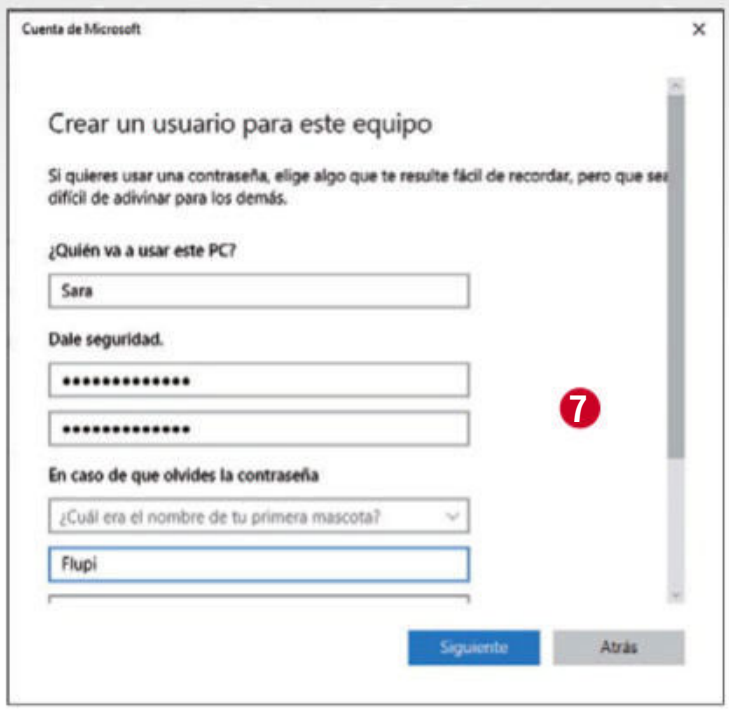
Abre la configuración de Windows y luego pulsa en ***Seguridad de Windows***. Acto seguido, en la izquierda, haz clic sobre ***Protección antivirus y contra amenazas***. A la derecha, verás todas las opciones de importancia. Por ejemplo, cuál es el resultado del último examen y si tienes que hacer algo o no. Luego, más abajo, aparecen las distintas opciones. Lo importante es que veas el mensaje ***No se requiere ninguna acción*** en todos los apartados o que todo está actualizado. De lo contrario, el sistema te guiará por lo que tienes que hacer.

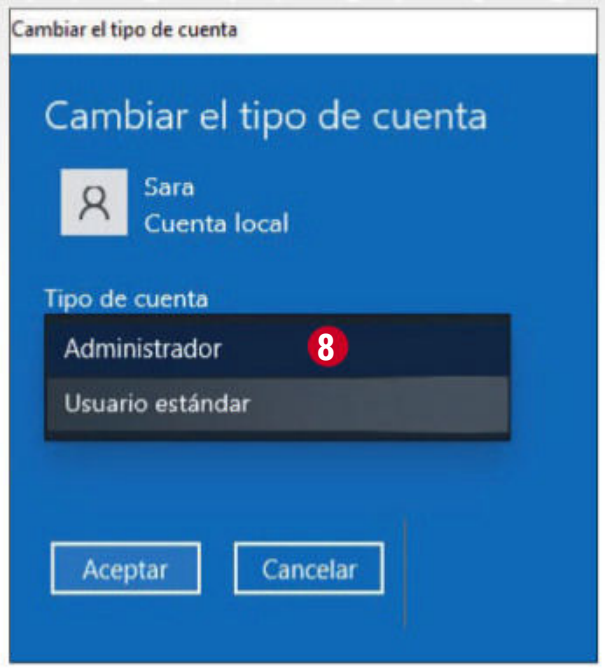
03 EMPLEA CUENTAS DE USUARIO Y NO ADMIN EN TU WINDOWS

En Windows hay dos tipos de cuentas: las de Administrador y las de Usuario. Las primeras tienen acceso a todas las funciones del sistema y permisos especiales. Por ello, están pensadas para gestionar el equipo, cuando es necesario. Si tu sistema es atacado por malware con una cuenta de Administrador, puede hacer más daño que con una cuenta de usuario, ya que esta no tiene acceso a tantas opciones y no puede realizar tantos cambios en Windows. Por eso, es recomendable que emplees siempre tu Windows con una cuenta normal. Así es cómo se gestionan o crean las cuentas en Windows.

1 Para crear una nueva cuenta, abre la configuración de Windows y haz clic en ***Cuentas*** y en ***Familia y otros usuarios***. Luego, pulsa en ***Agregar a otra persona a este equipo***. Si no tienes cuenta de Microsoft, haz clic en ***No tengo los datos*** y ***Agregar un usuario sin cuenta Microsoft***. A continuación, rellena los datos del usuario (nombre, contraseña y pistas para recuperar la contraseña) 7 y, finalmente, haz clic en ***Siguiente***.

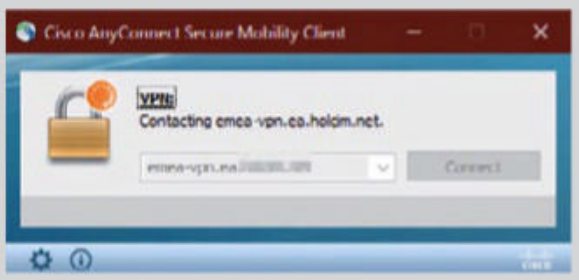
2 Eso creará una nueva cuenta. De forma predeterminada, Windows la crea de usuario, con menos permisos. Y eso es lo que quieres. A partir de ahora, inicia sesión con esa cuenta y guarda tus ficheros en ella. Si por algún motivo quieres conmutar el tipo de cuenta de usuario a Administrador o al revés, vuelve al mismo cuadro de diálogo de antes, haz clic sobre la cuenta y en ***Cambiar tipo de cuenta***. En el cuadro de diálogo que se abre, selecciona el tipo que quieres 8, pulsa en ***Aceptar*** y listo.



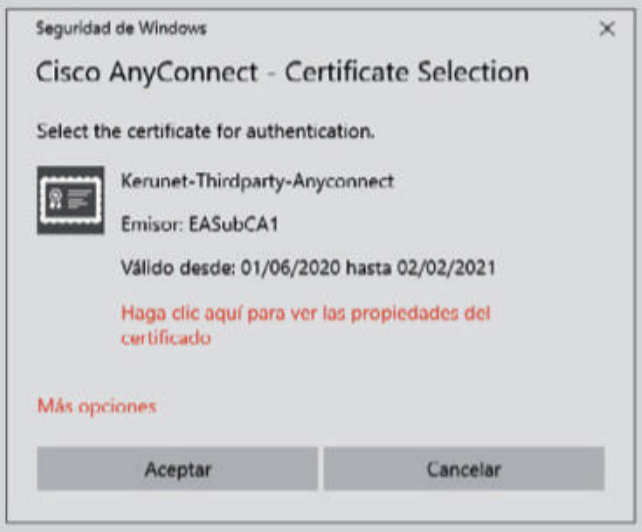


TRABAJA DESDE CASA DE FORMA SEGURA A TRAVÉS DE VPN

La pandemia por la COVID-19 ha sido la causa de la explosión del teletrabajo desde casa. Sin embargo, en función de los distintos empleos, en ocasiones nos podemos apañar con las herramientas informáticas que tenemos en el PC o portátil de casa, pero en otras necesitamos el acceso a uno de los sistemas de la empresa. Estos accesos tienen que ser seguros y especiales, para poder impedir que la información empresarial acabe en equipos privados o incluso fuera de ellos. Por eso, las conexiones remotas se suelen realizar a través de un cliente VPN (Virtual Private Network), que crea una conexión privada y cifrada con el sistema, por la que todos los datos viajan de forma segura. Basta con instalar el cliente VPN que emplee la empresa (como es, por ejemplo, Cisco AnyConnect, **bit.ly/3jgtTd1**) y que nos creen una cuenta y un usuario desde el que conectarnos. Además de eso, normalmente, la compañía nos tiene que enviar un certificado de seguridad, que deberemos instalar en el ordenador y que se encargará de cifrar las comunicaciones de forma apropiada. Este certificado se cargará antes de cada conexión y ayuda a autenticarnos ante la empresa, para de este modo poder demostrar que somos nosotros. Una vez que se haya establecido la conexión, podremos trabajar con los sistemas de la compañía, igual que si estuviéramos allí. Porque, de hecho, a nivel de red, lo estamos.



Con sistemas como AnyConnect, es posible el acceso remoto a una red de manera segura.



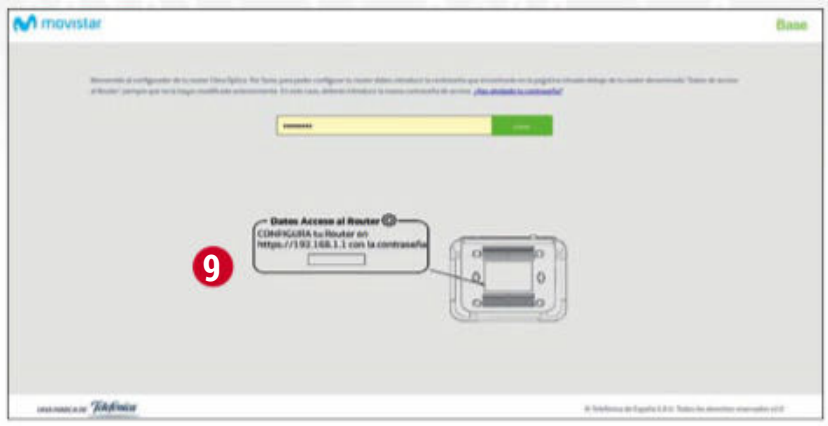
Al usar una VPN, debemos tener asignado un certificado digital, que permite identificarnos de forma segura.

Por esto, es extremadamente importante que no enviemos documentos de trabajo si no estamos conectados a la VPN, porque esta es la principal forma de asegurar que las comunicaciones son privadas.

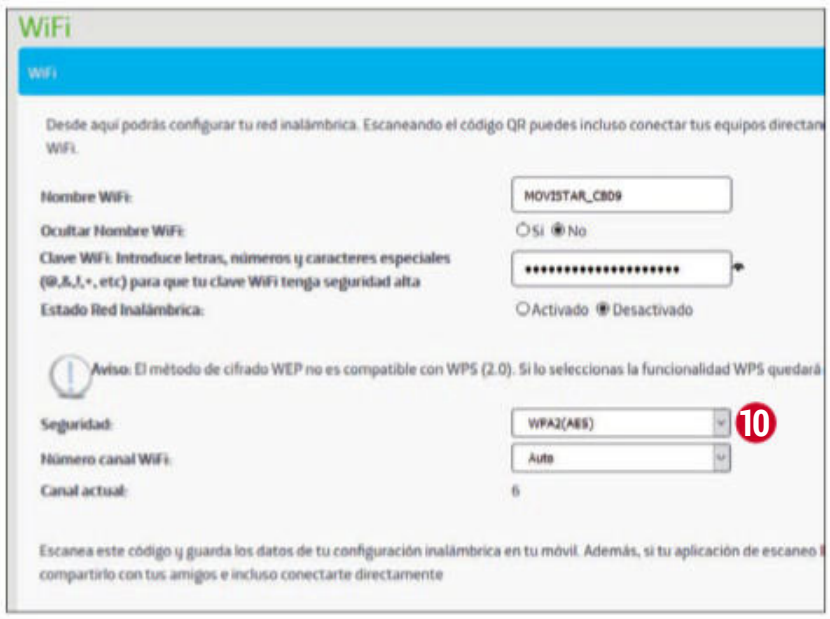
04 HAZ QUE TU CONEXIÓN WIFI SEA REALMENTE SEGURA

Un punto de ataque muy común a una red doméstica, son las WiFi no seguras. Como las ondas de radio atraviesan las paredes, es posible que ataquen la WiFi de tu casa sentados cómodamente en un banco del parque que hay cerca de donde vives. Pero, aún así, sin pensar en ataques, es importante que protejas tu WiFi de accesos no autorizados, para que nadie use tu línea sin tu permiso. Esto es especialmente importante en los routers que vienen configurados directamente desde tu proveedor de Internet. De modo que echar un vistazo nunca está de más. Hazlo así:

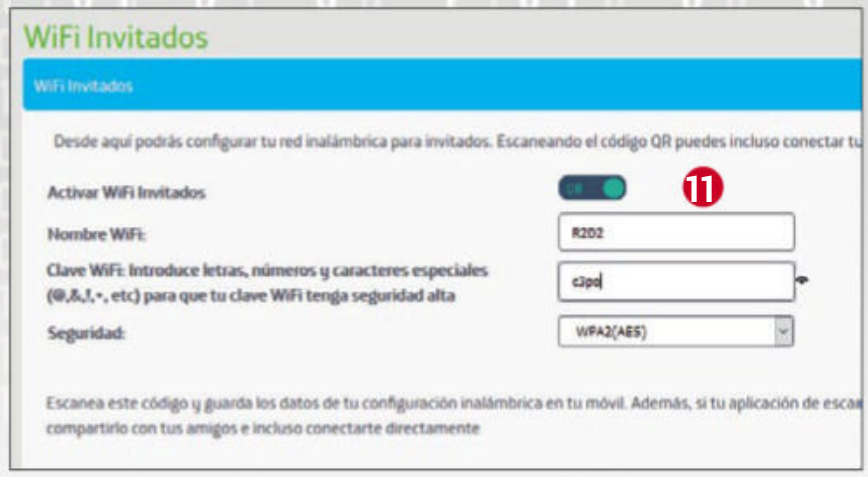
1 Vamos a usar como ejemplo un router de uno de los principales proveedores. Otros modelos tendrán otro aspecto, pero las funciones principales serán similares. Para conectarte al router, abre un navegador y emplea la dirección IP *192.168.1.1* (también puede ser *192.168.0.1*, consulta el manual del router). Escribe la contraseña que te dieron con el router (o que está en la etiqueta de la parte inferior 9) y pulsa ***Entrar***.



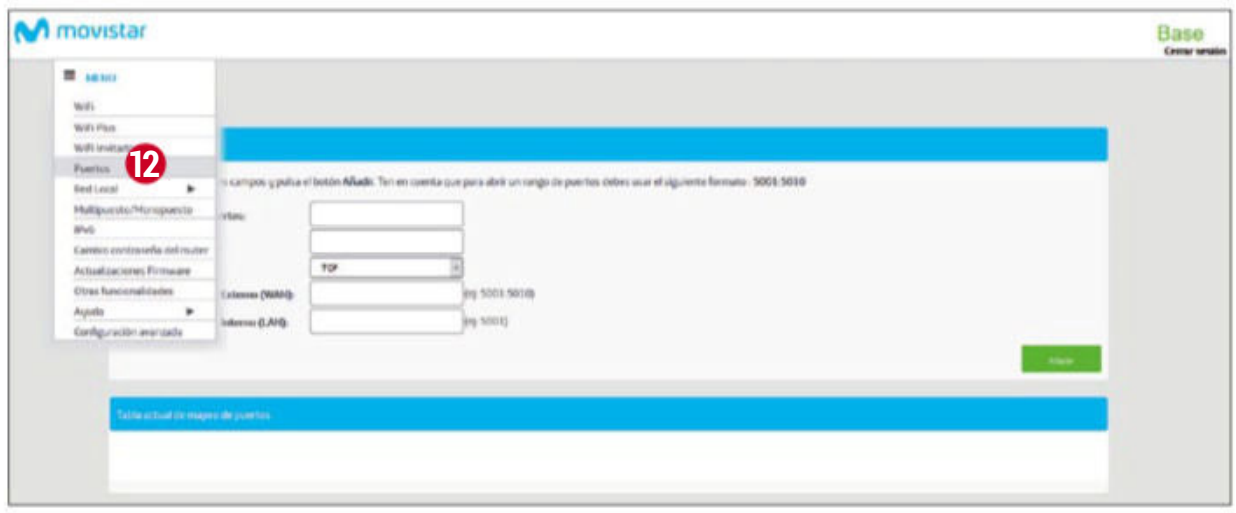
2 En el menú principal, normalmente verás directamente el resumen de las características de tu WiFi. Lo que más importa ahora es el apartado ***Seguridad*** o ***Cifrado***. Ahí debes ver el valor ***WPA2*** o ***WPA2(AES)*** 10. Esto hace referencia al sistema de cifrado que usa la conexión WiFi al enviar los datos por el aire para que, aunque alguien los intercepte, no pueda leer lo que contienen. Cualquier otro sistema de cifrado previo, como ***WPA*** o ***WEP***, es anticuado y ha sido roto ya. Si los utilizas, te expones a que cualquiera, con una app de móvil o un portátil, pueda conectarse a tu red doméstica y averiguar la contraseña en un momento.



3 Otro detalle importante es que uses lo que se llama 'red de invitados' para cuando vienen visitas a casa. Esta es una WiFi independiente que puedes activar y desactivar cuando quieras, con su propia contraseña. Así puedes darle la contraseña de la red de invitados a cualquiera que venga, pero no tienes que darle la de tu WiFi normal. Y, cuando acabe la visita, simplemente apaga la red de invitados. Sueles encontrarla en el menú directamente bajo ***WiFi Invitados*** o en el menú ***WiFi***. Asigna un nombre de red que sea fácil de identificar y una contraseña sencilla 11, para que todo el mundo pueda escribirla en el móvil sin problemas. Actívala con ***On*** y luego pulsa en ***Aplicar cambios*** para encenderla.



4 Hay otro detalle que también deberías comprobar: si tienes puertos abiertos en el router. Esto permite que determinados servicios puedan cruzar desde Internet hasta la red doméstica sin freno. Por ello, solo debes tener abiertos aquellos puertos que realmente necesites (por ejemplo para programas de videoconferencias o aplicaciones especiales que no vayan por HTTP). En el menú, localiza la función ***Puertos*** 12. En la tabla de puertos no deberías ver nada, y esta debería estar vacía. Si no es así, averigua para qué se usa ese puerto o desactívalo. Si algún dispositivo o programa deja de funcionar, puedes volver a activarlo. Al menos ya sabrás a quién pertenece.



05 ENVÍA FICHEROS DE FORMA SEGURA MEDIANTE CIFRADO

CONTRASEÑAS, UN MAL NECESARIO

Ya lo sabemos: teclear y recordar contraseñas es muy pesado. Sobre todo en el mundo actual, en el que tienes muchísimos servicios online de todo tipo. Pero, aunque sea así, debes respetar algunas reglas en la gestión y el uso de las contraseñas, para mantener tu seguridad y tus cuentas intactas fuera del alcance de personas no deseadas:

- **No uses la misma contraseña para todo:** sí, es mucho más cómodo tener que acordarse solamente de una contraseña, pero, si alguien la descubre por cualquier motivo, habrás comprometido todas tus cuentas a la vez. Como ayuda, puedes utilizar un gestor de contraseñas como **lastpass.com**, que te permitirá no tener que recordarlas o anotarlas.

- **No uses las típicas:** un estudio reciente demostró que el 40% de las contraseñas de Internet son ***123456***, ***123456789***, ***qwerty***, ***1234567***, ***12345678***, ***12345***, ***111111***, ***123123***, ***abc123*** y ***qwerty123***, lo que no dice mucho a favor de la imaginación de los usuarios. Y le facilita el trabajo a los hackers sobremanera. Usa el gestor anterior, **lastpass.com**, que también genera passwords seguras como puede ser, por ejemplo, ***98\%vd3y<EwJ[H^9***.

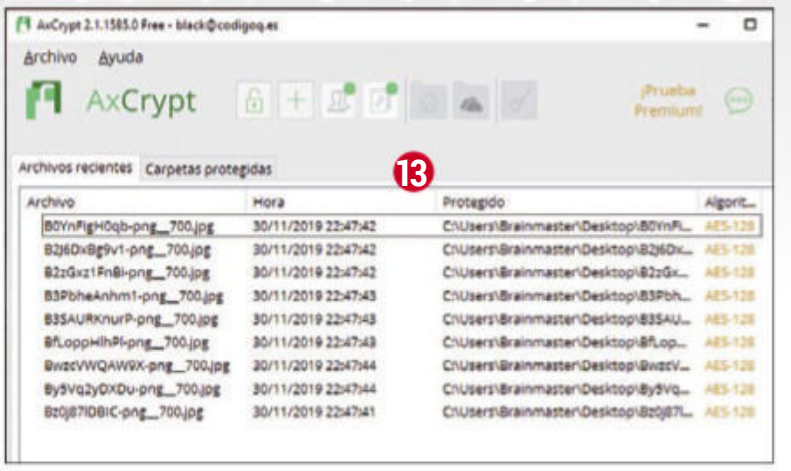
- **Nunca dejes las contraseñas de fábrica:** por ejemplo, en el router de casa. Tómate cinco minutos y elige ahora una contraseña segura que realmente proteja ese dispositivo.

- **No las apuntes en papel:** el PIN del teléfono móvil dispuesto en una pegatina al dorso del mismo puede ser cómodo, pero obviamente no es un sistema seguro, evítalo siempre que puedas.

Enviar datos a otras personas ya es una tarea de lo más común y, seguramente, la realizas cada día. Sin embargo, hay ocasiones en las que los datos que pretendes enviar son de naturaleza sensible y prefieres no mandarlos alegremente por email, no sea que ese mensaje acabe en manos de alguien que no quieres. La mejor manera de asegurar las comunicaciones es cifrando la información. Te presentamos dos formas diferentes. Y una de ellas te sorprenderá.

1 El método más convencional es emplear un programa de cifrado de ficheros. Es el sistema más seguro, porque tienes un control total sobre todo el proceso. El 'inconveniente' es que el receptor ha de tener el mismo programa y saber la contraseña. Para ello puedes emplear un programa como AXCrypt, que cifra los ficheros con el sistema que elijas. Accede a la web **www.axcrypt.net** y haz clic en ***Descarga***. Luego, haz doble clic en el archivo ***AxCrypt2-setup.exe*** que has descargado y tendrás que dar una dirección de email. Te llegará entonces un mensaje con un código de verificación que deberás escribir.

2 Ahora solo te queda introducir una contraseña, arrastrar los archivos a cifrar sobre el programa y definir la password que quieres utilizar para cifrar los ficheros a enviar en esta ocasión. Esta es la que tendrás que darle al destinatario del email, para que pueda extraer el contenido original. Ten en cuenta que los ficheros se cifrarán directamente, en el mismo lugar. Es decir, que se eliminan los originales. Si los necesitas tal cual, obtén una copia antes del cifrado. Cualquiera que reciba estos archivos, no podrá hacer nada con ellos sin la contraseña, ya que se encuentran codificados de una forma muy segura 13.

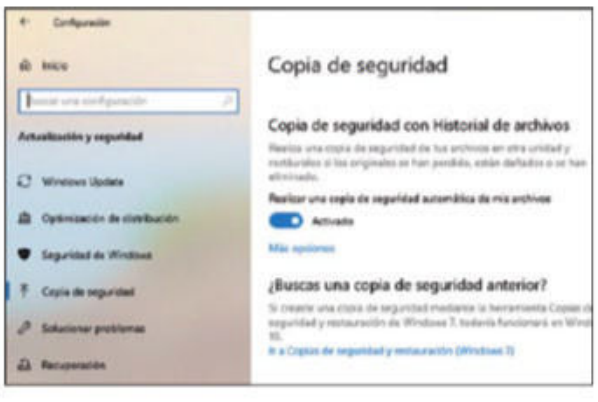


3 Una forma menos convencional de enviar información de forma segura a alguien, y en un instante, es utilizar WhatsApp. Hace años que este programa de chat emplea un sistema de cifrado extremo-a-extremo, lo que significa que los datos en tránsito están cifrados en todo momento y, aunque se intercepten, no le servirán de nada a nadie. De modo que la forma más rápida de compartir imágenes, archivos PDF o de Word o similares con otra persona es abriendo una sesión de WhatsApp Web (**web.whatsapp.com**) en tu navegador y siguiendo las instrucciones. Una vez tengas WhatsApp en el navegador, podrás arrastrar ficheros desde el PC hasta WhatsApp y se transferirán de inmediato. El tamaño máximo de los ficheros es de 64 MB.

06 HAZ COPIAS DE SEGURIDAD DE TODOS TUS DATOS IMPORTANTES

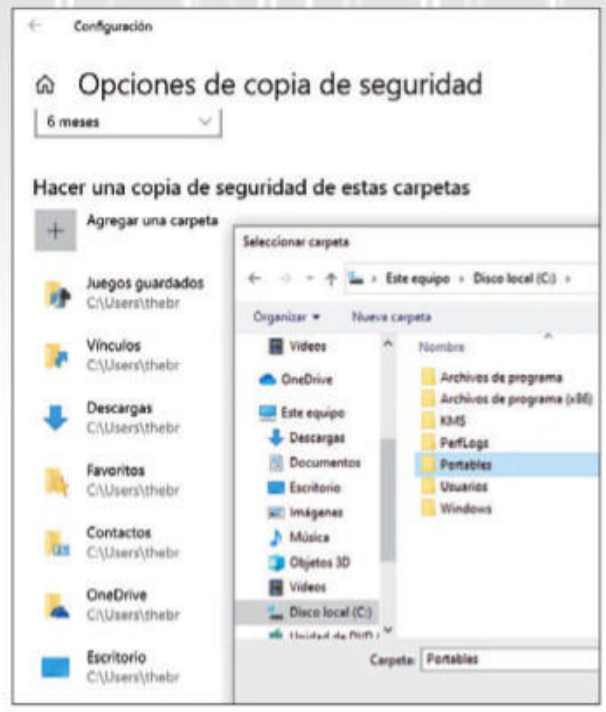
No hay nada mejor que tener un 'Plan B'. Y, en el caso de la informática, ese Plan B normalmente se llama 'copia de seguridad'. Cuando todo sale mal, siempre puedes recurrir a ella y recuperar tus datos y esa información importante que has guardado con antelación. Existen muchas aplicaciones pensadas especialmente para ello como KLS Backup (www.kls-soft.com), EaseUS Todo Backup Free (bit.ly/2GmaYyT), Cobian Backup (www.cobiansoft.com) o Paragon Backup & Recovery (bit.ly/3l6xN8P). Sin embargo, desde el propio Windows 10, también puedes llevarla a cabo de una manera sencilla. Hazlo así:

1 Comienza por abrir el menú ***Configuración*** y luego haz clic en ***Actualización y seguridad***, seguido de ***Copia de seguridad***. En el apartado ***Copia de seguridad con Historial de archivos***, pulsa sobre ***Agregar una unidad***, una vez que hayas conectado un disco externo o tengas preparada una unidad interna libre que quieras dedicar a las copias de seguridad. Cuando aparezca la unidad y se haya activado la copia de seguridad, podrás iniciar la configuración.



2 Para ello, haz clic sobre ***Mas opciones*** y podrás determinar con qué frecuencia se hacen las copias y de qué exactamente. Si tienes tiempo, comienza por ***Hacer ahora una copia de seguridad***, para realizar la primera. Luego, determina con qué frecuencia quieres hacer las copias. El valor que aparece, ***Cada hora***, puede ser excesivo si no trabajas tanto con el ordenador, de modo que ajústalo a, por ejemplo, ***Cada 6 horas***. Pero lo que es más importante es la lista inferior ***Mantener las copias de seguridad***. Ahí deberías establecer un valor razonable como ***6 meses***. Si no es así y guardas todas las copias de seguridad desde el primer día, el disco se llenará con cierta velocidad. Según tu estilo de trabajo, incluso puedes acortar este periodo.

3 Por otro lado, si necesitas hacer la copia de seguridad de una carpeta que no aparece en la lista predeterminada de Windows, puedes añadirla fácilmente con ***Agregar una carpeta***. Selecciónala entonces en la ventana que se abre, pulsa en ***Elegir esta carpeta*** y ya será tenida en cuenta en la próxima copia de seguridad. Puedes añadir tantas carpetas como quieras.



EL PELIGRO DE LOS JUEGOS ONLINE

¿Es peligroso jugar online? Más de un padre seguro que se ha hecho esta pregunta. Y la respuesta, como tantas otras veces en la vida, es 'depende'. Jugar online no es peligroso per se, pero jugar 12 h seguidas, todos los días, obviamente es un problema. Sin embargo, si dejamos de lado las componentes psicológicas, los juegos online pueden tener varios peligros:

- Los títulos pirateados suelen contener virus en su gran mayoría e infectar el ordenador o, incluso, la red local de casa.
- Lo mismo se aplica a los parches y 'hacks', los cuales añaden funcionalidades especiales, pero pueden proceder de lugares poco claros y nada seguros.
- Los MMOG (juegos multijugador masivos online) pueden terminar siendo un entorno de Bullying para el menor, si por ejemplo grupos de otros jugadores se reúnen siempre para enfrentarse a él en el mundo virtual, haciendo que pierda y produciendo frustraciones constantes.
- Jugar con personas de otros husos horarios, puede provocar que el menor (normalmente adolescentes) se quede hasta altas horas de la madrugada despierto, para coincidir con sus amigos de otro continente, con el consiguiente impacto en el ritmo del sueño o rendimiento en el colegio.

Los juegos online pueden provocar que pequeños y mayores perdamos la noción del tiempo.

07 APRENDE A REALIZAR COMPRAS ONLINE DE FORMA MÁS SEGURA

Hoy en día, comprar online es de lo más común. Y, en la mayoría de los casos, es completamente seguro. Todo el mundo ha comprado alguna vez en Amazon y esta plataforma gigantesca se toma muy en serio la seguridad. Lo mismo ocurre en las webs de centros comerciales grandes como Carrefour, El Corte Inglés, etc. Pero ¿qué pasa en otros sitios? Veamos algunos de ellos.

Portales eBay y Wallapop

En ambos casos, lo mejor es que pagues con PayPal. ¿Por qué? Porque PayPal aísla a los compradores y vendedores, en el sentido en que ninguno de los dos conoce los datos financieros del otro y, además, las transacciones no se realizan hasta que la parte compradora haya recibido el artículo. El vendedor, a su vez, sabe que el comprador ha pagado, aunque no recibirá el dinero hasta que el producto haya cambiado de manos. Las dos partes ganan en seguridad.

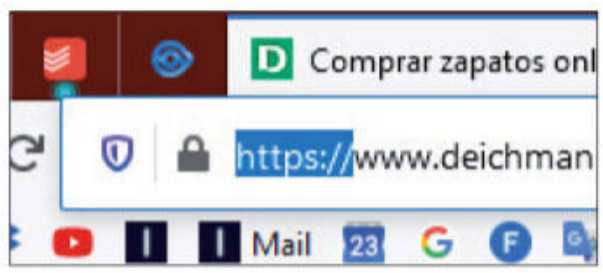
AliExpress, Alibaba, Banggood...

Las tiendas online chinas están muy de moda. El motivo es que puedes encontrar referencias interesantes a precios ridículamente bajos. Y, si buscas un poco, puedes llegar a encontrar productos de calidades muy razonables. Sin embargo, volviendo a la pregunta de si las compras son seguras, debes tener en cuenta que, siempre que te mantengas en las grandes tiendas, no hay problema. AliExpress (14), por ejemplo, tiene su propio sistema de pago, que funciona de forma similar a PayPal. Y lo mismo ocurre con Banggood. Y no hay problema con el reembolso, en caso de que los productos no lleguen antes de 60 días.

Sin embargo, otras tiendas chinas pueden presentar problemas. Por ejemplo, en lo relativo a la calidad de los productos o relacionados con el método de pago o las devoluciones. De modo que si te sales de las grandes y populares compañías, deberás tener cuidado y, a ser posible, pagar con PayPal. De este modo, tu información financiera estará salvaguardada y, en caso de problemas, podrás recuperar tu dinero.

Tiendas más pequeñas

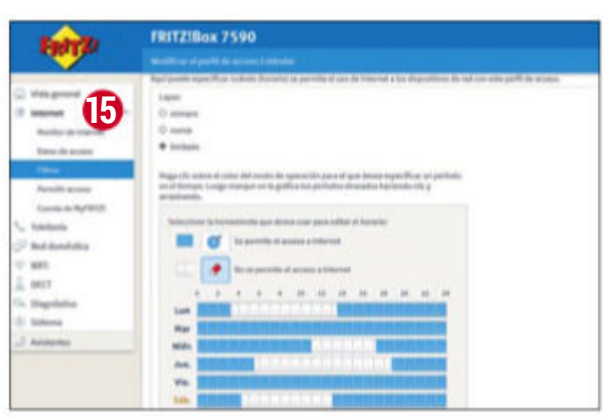
Muchos negocios pequeños también tienen su propia web. No obstante, el hecho de que sean pequeños no tiene que ver con su seguridad. Lo más importante en este caso es que conozcas el negocio personalmente o por referencias fiables, y que tus pagos o datos personales solo se introduzcan en páginas cifradas por SSL (cuya URL comienza por ***https://***). Si no es así, será mejor que nunca escribas tus datos personales en una web sin tecnología SSL (***http://***).



08 ACTIVA Y USA SISTEMAS DE PROTECCIÓN INFANTIL

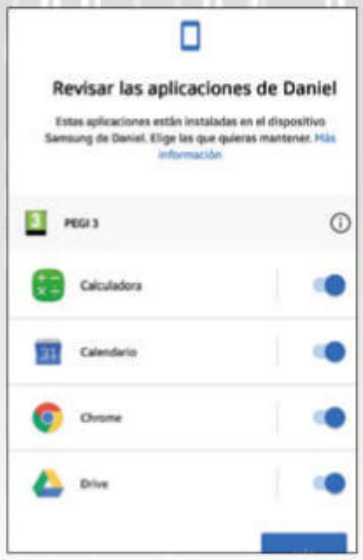
Sin duda alguna, los más pequeños son los más vulnerables en lo que se refiere a Internet. Es extremadamente sencillo que se tropiecen con contenidos que no son aptos para su edad, bien sea por accidente o por curiosidad. Por esta misma razón, lo mejor es que actives un sistema de protección infantil. Puedes hacerlo en Windows o también en el router. Veamos ambas opciones.

1 Muchos routers modernos tienen la posibilidad de crear planes horarios para la conexión de dispositivos. Con ellos, puedes controlar cuándo los niños pueden acceder a Internet y cuándo no. En función de la marca y el modelo del router, estas funciones pueden encontrarse disponibles para su uso en diversos lugares, pero normalmente las encontrarás bajo los menús *Internet* (15) o *Seguridad*.



2 Por otro lado, en el propio Windows tienes opciones de control parental a través de Microsoft Family, que son muy sencillas de configurar. Para acceder a ellas, abre el menú ***Configuración***, pulsa sobre ***Actualización y seguridad***, luego sobre ***Seguridad de Windows*** y, abajo a la derecha, sobre ***Opciones de familia***. Esto abrirá el cuadro de diálogo de la figura 16. Desde él, pulsa sobre ***Ver configuración de familia*** y sigue los pasos que se indican para crear un grupo familiar y asignar permisos de uso de todos los equipos e Internet a los distintos miembros de la familia.

3 Otra opción es que emplees la solución Google Family Link, que te permite no solo controlar la actividad del menor en el PC, sino también en el teléfono móvil. Podrás controlar y limitar horarios, ver las búsquedas que realiza, qué productos de Google emplea, vídeos de YouTube que ve, etc. La configuración no es complicada, pero requiere un rato. Puedes iniciar el proceso y consultar cómo usarlo desde la página **families.google.com/intl/es/familylink**, con tu cuenta de Google.



4 También puedes usar servicios como Qustodio (**www.qustodio.com**) que ofrecen todo un abanico de funciones de control y limitación para numerosos dispositivos y sistemas, con avisos por email cuando sucede algo extraordinario. Además, tiene la capacidad para localizar al menor a través del móvil.

LOS 10 FRAUDES MÁS COMUNES EN INTERNET ACTUALMENTE

Naturalmente, hay cientos de formas de engañar a alguien por Internet y todo depende del ingenio que desarrolle el cibercriminal y de lo ingenua que sea la víctima. En la siguiente lista, hemos reunido las 10 que te puedes encontrar con mayor frecuencia.

1 Phishing

Es una grafía distinta de 'fishing', que quiere decir 'pescar'. El phishing se compone normalmente de un mensaje que parece venir de un sitio que conoces (banco, operador de telefonía, Netflix, etc.), en el que te piden que verifiques tus datos de cuenta. Sin embargo, el sitio al que te conduce es de los hackers, que se quedan con tus datos, para aprovecharse fraudulentamente de ellos.

2 Contactos

Este timo se aprovecha de la soledad de algunas personas. Una mujer, con mucha frecuencia rusa, entra en contacto con un hombre europeo en una de las plataformas de citas. Se hace su amiga, muestra interés por él y quiere verlo. Pero 'necesita el dinero para el billete' o cualquier otra cosa. Una vez que envías el dinero, adiós muy buenas.

3 Príncipes Nigerianos

En esta ocasión, recibes un email de un alto cargo del gobierno que te ha elegido milagrosamente, para evadir millones de su país a través de ti. A cambio recibirás una generosa compensación. El gran problema es que tienes que pagar la transferencia primero... pero ¿qué son unos cuantos cientos de euros comparados con las riquezas prometidas? Obviamente, perderás tu dinero.

4 Tiendas online falsas

Se resume en cuatro palabras: 'Compras algo, nunca llega'. Como te hemos dicho, asegúrate que su dirección web comienza por ***https://*** y, si dudas, pregunta a otros usuarios, por ejemplo en foros.

5 Ingeniería social

Probablemente la amenaza más difícil de detectar y de evadir, ya que tiene que ver con la habilidad de una persona para hacer que te creas que es alguien que conoces y al que, al final, le confías datos personales. Te utilizará además para engañar a alguien por encima de ti y así continuará hasta que llegue hasta donde realmente quiere.

6 Bitcoin

Este timo circula con insistencia estos días. Personas conocidas, famosos, presentadores de televisión, jugadores de fútbol, etc. te cuentan (a ti casualmente) su secreto para hacerse ricos negociando con Bitcoin y ganar miles de euros cada día. Pero, como en todas las pirámides, hay muchos que ponen el dinero y solo es uno el que se lo lleva.

7 Encuestas con premio

Tal y como suena. Te hacen preguntas de todo tipo con la promesa de que te puedes llevar un magnífico premio que, naturalmente, no existe. Lo único que quieren, como en otras ocasiones, son tus datos.

8 Trabajo desde casa

Esta es una versión del timo de Bitcoin, pero ofreciéndote un trabajo maravilloso que puedes hacer desde casa, ganando miles de euros al mes y solo trabajando unas pocas horas al día. Trabajar igual trabajas, pero lo que es cobrar... olvídate.

9 Timos de la letra pequeña

Estos siempre han existido, aunque con Internet han aumentado una barbaridad. Contratas un servicio aparentemente inocuo de cualquier sector, pero muy escondido en la letra pequeña hay todo tipo de cláusulas con respecto a la cesión de tus datos, cargos adicionales por las cosas más absurdas y todo lo que puedas imaginar.

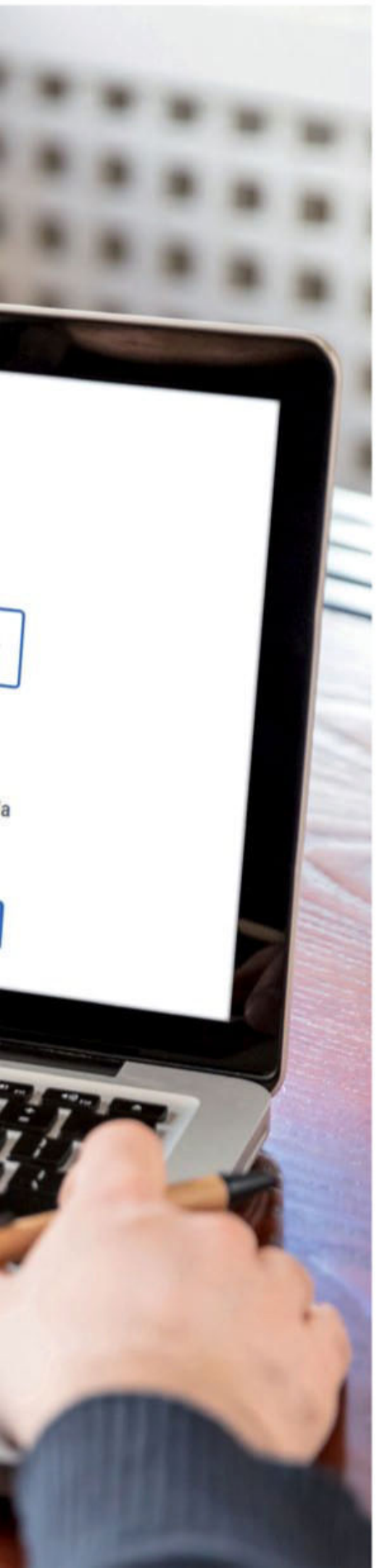
10 Webcam secuestrada

El timo de los contactos de rusas del que ya te hemos hablado antes se aprovechaba de la soledad, este en cambio lo hace de la vergüenza. Recibes un email en el que te muestran la información que tienen sobre ti (tu nombre y a veces tu dirección) y te dicen que tienen el control remoto de tu webcam y que te han pillado viendo una web y haciendo cosas comprometedoras. Te indican que pagues una cantidad de euros en Bitcoin o se lo mandan a tu mujer/marido/familia/amigos. Por supuesto, no hay grabación, pero siempre hay usuarios que pican.

MANTÉN A SALVO TUS PERFILES EN INTERNET

AUTENTICACIÓN

EN DOS PASOS



Disponer de un acceso seguro para tus cuentas online es algo fundamental. Pero, muchas veces, las contraseñas simples ya no son suficiente. Te explicamos cómo funciona la verificación en dos pasos.

Email, cuentas bancarias, acceso a Hacienda, redes sociales, tiendas online... estamos rodeados de cuentas digitales que nos proporcionan servicios, nos hacen la vida más fácil y nos divierten. No obstante, siempre hay que tener en cuenta que, en todas ellas, se gestiona información personal y privada. Y, por esa razón, todos los servicios tienen **contraseñas que permiten el acceso y garantizan la seguridad**. En este artículo, no vamos a centrarnos en cómo crear contraseñas seguras, sino que daremos un paso más allá, hacia la autenticación de dos factores o verificación en dos pasos. Esto no es nuevo, pero sí comienza a ser algo imprescindible en este mundo basado en la vida online.

¿Por qué necesito la doble autenticación?

Ya sea en forma de ordenador, teléfono móvil o de cualquier otro dispositivo electrónico (como un cajero automático, por ejemplo), estamos rodeados de electrónica. Y para muchas de las operaciones que realizamos en el día a día, **se necesita que nos identifiquemos**. Esta es la única manera de demostrar que nosotros somos quien decimos ser. Antes, ibas al banco y el cajero ya te conocía, porque te había visto muchas veces. Ahora, el cajero automático, **necesita alguna prueba de que tú eres tú**, antes de darte dinero o de facilitarte el estado de tus cuentas. Es decir, necesitas autenticarte. Para entrar en tu cuenta de correo de Google, ocurre lo mismo: necesitas demostrarle a la máquina que eres tú, mediante el conocimiento de una contraseña. Este es uno de los llamados 'factores de autenticación'.

En cualquier caso, todos hemos escuchado noticias sobre robo de datos por parte de los hackers, o relativas a descuidos en los que la información de miles de usuarios quedó al descubierto. Y aquí es donde se genera el problema: con solo un factor de autenticación, la seguridad de lo que se protege tras ese factor (normalmente una contraseña alfanumérica), queda anulada. Y, por esto, está tomando fuerza la autenticación de múltiples factores.

MFA o Multi Factor Authentication

La autenticación de múltiples factores (MFA) se basa en un principio de seguridad que es muy sencillo y que **diversifica los riesgos**. Para acceder al elemento protegido (una cuenta, un servicio, etc.) necesitas disponer de tres factores:

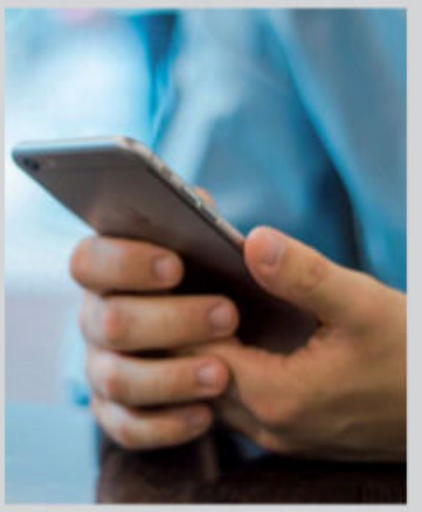
Safe ID es un pequeño dispositivo que representa un token de hardware de un solo uso, basado en el tiempo.

- **Algo que eres:** el primer factor se basa en algo propio de ti. Por ejemplo, tus huellas dactilares, iris ocular, altura, voz, etc. Un factor que solo tú tienes y que ayuda a definirte de forma más o menos clara.

- **Algo que tienes:** el segundo factor tiene que ver con algo físico que solamente tú posees y que te identifica como quien eres. Para acceder al autobús,

EL CUARTO FACTOR

Desde hace ya un tiempo, se emplea también un cuarto factor: dónde estás. Es importante que, si quieres entrar en tu empresa, te encuentres en la puerta de la misma y no en tu casa. Esto último sería bastante extraño y, por ello, algunos servicios empiezan a tener en cuenta el lugar en el que te encuentras, antes de concederte, por ejemplo, acceso. La idea es impedir la activación remota de puertas, de cajeros, etc.



por ejemplo, tienes que presentar tu bonobús o abono de transporte. O, para entrar en tu casa, necesitas la llave correcta.

- **Algo que sabes:** este es, posiblemente, el factor con el que estés más familiarizado, porque las contraseñas son precisamente eso, algo que únicamente tú conoces (o deberías).

El conjunto de estos tres factores es lo que se denomina 'autenticación multifactorial'. Por poner un ejemplo, no hay más que acordarse de las películas de espías en la que acceden a algún lugar secreto del gobierno, para distinguir todos estos factores en acción: un escáner de retina, una llave de seguridad y una contraseña. Solo si poseen todo eso podrán acceder allí. En realidad, hoy en día, ya hay un cuarto factor (ver cuadro inferior), pero únicamente se usa en circunstancias específicas.

A día de hoy, todavía muchos usuarios apuestan por contraseñas sencillas, que pueden ser averiguadas en minutos con programas especiales.

Pues bien, un subconjunto de la autenticación multifactorial es la autenticación de 2 factores (2FA, 2 Factor Authentication). Solo **emplea dos factores y, normalmente, se usan dos totalmente distintos**, para así incrementar la seguridad del sistema. Un ejemplo: igual no te lo has planteado nunca, pero usas la autenticación de dos factores cada vez que vas al cajero automático, ya que tienes que presentar algo que tienes (la tarjeta de crédito) y también algo que sabes (el PIN de la tarjeta) para poder operar. Debido a los peligros que amenazan a las cuentas digitales, para el mundo online se han desarrollado varios sistemas de doble autenticación.

LOS DEFECTOS DE 2FA

Como todo en la vida, tampoco la autenticación 2FA es perfecta. Existen algunos métodos ideados para obtener todos los factores, con la finalidad de acceder a la cuenta o servicio de la víctima. De hecho, un estudio reciente de Forbes indica que el 74% de los ataques parten de que ya poseen el nombre de usuario y la contraseña de la victima, con lo que solo les falta el segundo factor de autenticación. Estas son algunas de las vulnerabilidades:

Phishing

Los ataques de phishing representan el 93% de todos los que tuvieron éxito el año pasado, y la cifra sigue creciendo. Por una parte, el phishing se aprovecha del comportamiento humano, así como de los defectos existentes en la seguridad. Es posible que ya hayas sufrido algún intento de phishing: por ejemplo, el típico email que te insta a que cambies rápidamente la contraseña de tu banco (u otro servicio) porque si no te van a cerrar la cuenta. En el propio correo aparece un enlace que te llevará a una página falsa desde la que intentarán interceptar tus datos.

Redireccionamientos

Como la mayor parte de los códigos 2FA de hoy en día están basados en móviles, un hacker avanzado podría redireccionar el tráfico de tu teléfono a uno de sus dispositivos, para desde él ver todo lo que recibes. Y, si tiene acceso físico al dispositivo, incluso podría obtener un duplicado de tu SIM, con lo que vería lo mismo que tú, sin intervenir en el tráfico del teléfono.

Preguntas secretas

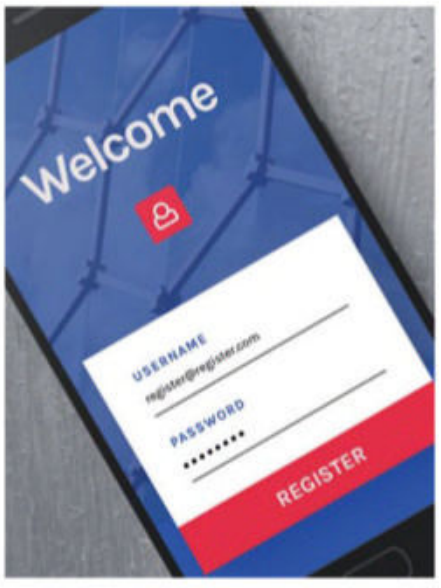
Las típicas preguntas acerca de '¿Cuál fue tu primer profesor de primaria?' o 'El nombre de tu primera mascota' se pueden averiguar con relativa facilidad, mediante técnicas de ingeniería social. O, aún más sencillo, siguiendo tus feeds de Facebook, Instagram, etc. porque muchas personas publican esos detalles sin pensar en las posibles consecuencias.

En 2016, fueron robados 16.000.000.000 de dólares online de usuarios estadounidenses.

Estos suelen complementar una simple contraseña con algo más.

Sistemas y tipos de 2FA

Hay diferentes tipos de autenticación de dos factores. No todos son iguales y **algunos ofrecen mejor protección que otros** o son más complejos. Sin embargo, sea como sea, resultan mucho más efectivos que emplear solo una contraseña. Estos son los tipos más importantes:



En la mayoría de los casos, un sistema de autenticación de un solo factor (por ejemplo, el acceso con una password) no es realmente seguro.

- **Tokens de hardware:** en informática, un 'token' es un identificador único. Los tokens de hardware son, probablemente, la forma más antigua de 2FA. Hace muchos años, los programas de pago realmente caros, como los de CAD, venían con una memoria USB especial (o con un conector de puerto serie, hace aún más años) que generaba un código específico cada cierto tiempo. Si no había código, no era posible acceder al software o a la cuenta relacionada. Otros muestran un número en pantalla, que has de introducir.

- **SMS:** seguro que ya conoces este tipo de sistemas si has visitado determinados sitios web como, por ejemplo, los sites bancarios. Una vez que accedes a tu cuenta (con nombre de usuario y contraseña), como último paso de comprobación te envían un SMS al teléfono móvil con un código único que has de escribir. Aún con todo esto, los SMS no se consideran un método muy seguro como segundo factor, y cada vez se usan menos.

- **Notificaciones Push:** en este caso concreto, el sitio web o la app a la que intentas acceder te envía una **notificación al ordenador o móvil**. Basta con que la apruebes para poder acceder. Este método no requiere que escribas códigos o contraseñas adicionales.

- **OTP o Tokens de software:** las siglas OTP significan One Time Password, es decir, con-

traseña de una sola vez. En realidad, los SMS que hemos visto antes, son un tipo de OTP. Sin embargo, en el caso de OTP, se suele necesitar también una aplicación especial (normalmente gratuita) que **genere los códigos, y que esté vinculada con el servicio** en cuestión al que quieres acceder (ver el práctico en las siguientes páginas). Cuando accedes al sitio, te pide un código de varios dígitos, que tienes que generar en la app. Este código suele durar unos segundos y después se invalida.

- **Tokens biométricos:** aún no se usan demasiado, pero ya están disponibles. En este caso, tú mismo eres el token. Ya sean las **huellas, iris**, etc. se usan como segundo factor. Gran parte de los móviles actuales ya incorporan, por ejemplo, un sensor de huellas, pero vendrá mucho más.

El iris de los ojos, los latidos del corazón o el olor corporal son algunas de las contraseñas biométricas que se están poniendo a prueba en estos momentos.

¿CUÁLES SON LAS MEJORES PRÁCTICAS DE SEGURIDAD?

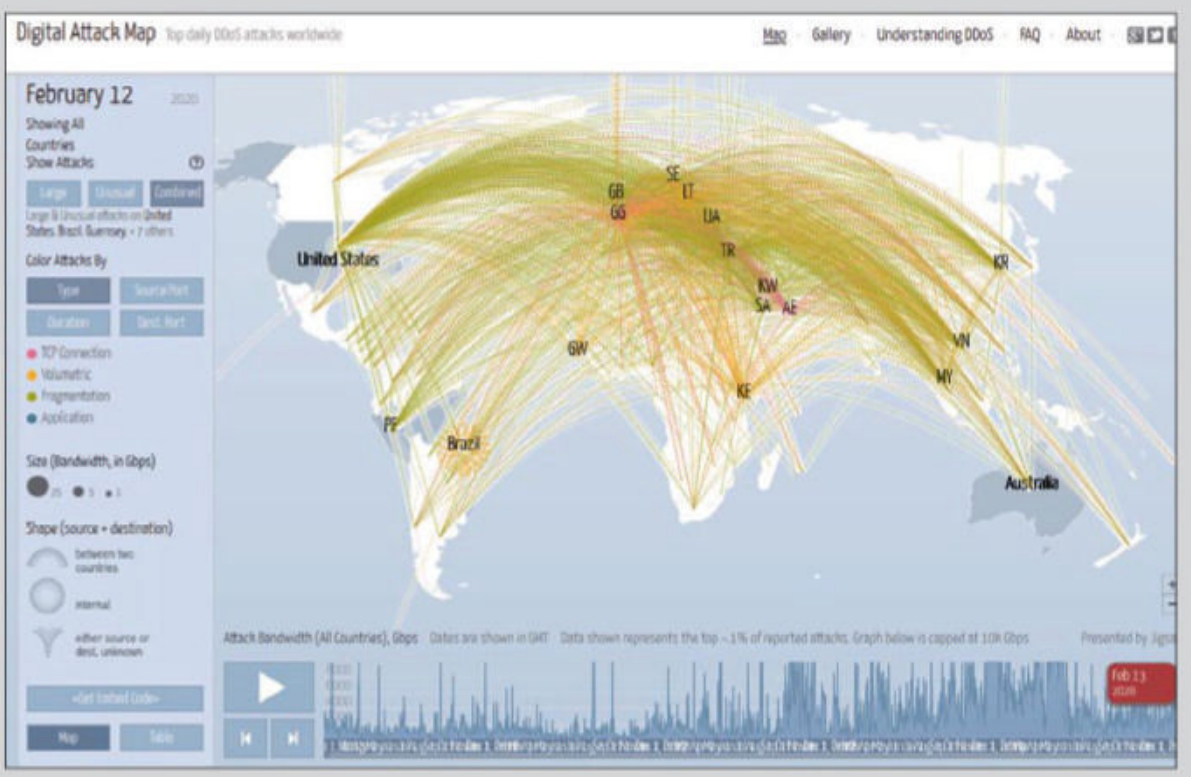
En la mayoría de los casos, el eslabón más débil suelen ser los usuarios y no los dispositivos o servicios. Por ello, hemos reunido aquí algunos consejos de mejores prácticas, que puedes aplicar cuando se trata de temas de seguridad.

- **"A mí no me puede pasar" no es la filosofía más apropiada.** Sí, eres uno entre muchos usuarios de Internet, pero los bots no distinguen y van uno por uno. Al final, te tocará.
- **Cuidado con el phishing.** Los mensajes que te apremian y amenazan con cancelar o cerrar algo suelen ser falsos. No pulses sobre los popups o botones que hay en los emails o páginas webs de origen dudoso. Escribe siempre la dirección del servicio en cuestión con el teclado, en la barra de tu navegador, para estar seguro de que vas al lugar correcto.
- **Usa contraseñas seguras además de la autenticación de dos factores.** Emplea contraseñas largas, que incluyan símbolos y mayúsculas, y evita obviedades como 1234, abcd, qwerty, etc. Pon las cosas difíciles a los hackers, directamente desde el principio.
- **Nunca dejes tus dispositivos sin vigilancia.** Si un atacante consigue acceso a uno de ellos, no sabes lo que puede llegar a hacer. Evita siempre esas situaciones.
- **Protege tus datos sensibles.** Lo mejor es que utilices algún sistema de cifrado. De esta forma, aunque alguien consiga tus datos, no poco o nada podrá hacer con ellos.

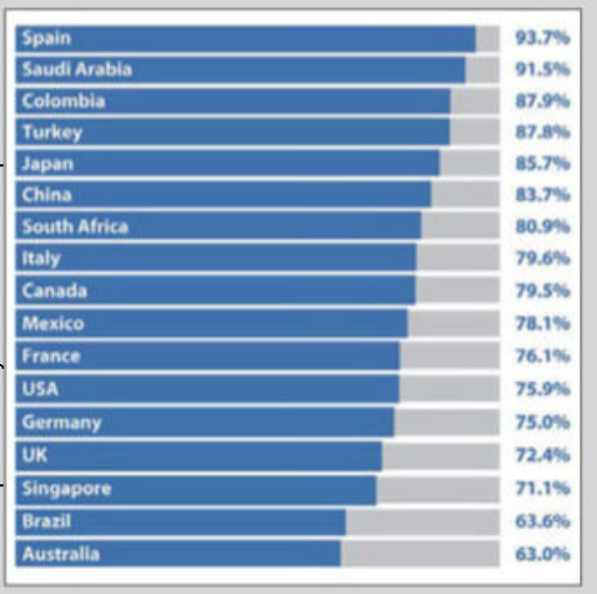
ESTADO DEL CIBERCRIMEN EN LA ACTUALIDAD

El daño que causará el cibercrimen en 2021 se estima en 6 billones de euros al año, a nivel mundial. ¡Y estamos hablando de billones españoles (millones de millones)! En el año 2018, aparecieron 137,5 millones de nuevos tipos de malware. Además, los dispositivos que se infectan por primera vez suelen reinfectarse antes de un año.

Con todos estos datos en mente y sabiendo que, durante el año pasado, el 50% de los crímenes cometidos en el Reino Unido fueron cibercrímenes, la importancia de proteger tus cuentas de forma seria queda patente. Es más, en el mismo 2018, España fue el país más atacado (ver gráfico) del mundo. Si quieres conocer el estado, en tiempo real, de los ciberataques que se están produciendo ahora mismo a nivel global, puedes visitar **www.digitalattackmap.com** y verás qué países están atacando a otros.



Digital Attack Map es una útil herramienta que permite mostrar, en tiempo real, los ataques DDoS que están teniendo lugar en todo el mundo. La información que muestra se recopila de forma anónima.



Fuente: Imperva 2019 Cyberthreat Defense Report.

Porcentaje de sitos comprometidos por, al menos, un ataque con éxito en los últimos doce meses.

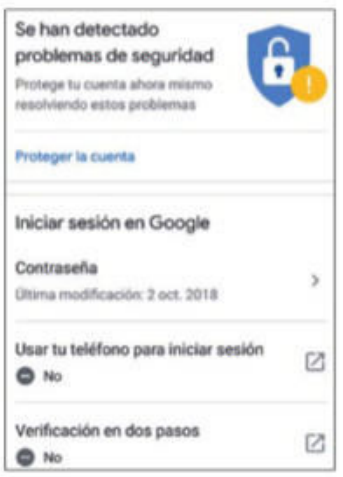
01 MAYOR PROTECCIÓN PARA TODAS TUS CUENTAS ONLINE

Prácticamente todo el mundo emplea servicios online o cloud para su vida cotidiana. Y todos se protegen mediante el uso de una contraseña. Pero, como en muchos de ellos guardas datos personales (como fotos o documentos), es importante que toda esta información no caiga en manos de personas no autorizadas. Por ello, en las próximas páginas, te indicamos cómo puedes proteger algunos de los servicios más populares con un sistema 2FA. Impedirás así accesos no autorizados, aún en el caso de que la contraseña quedase comprometida.

Protege tus servicios de Google

Email, programas de ofimática, almacenamiento de fotos y de ficheros, YouTube... todos sabemos que Google es una parte importante de nuestra vida online. Por ello, el hecho de proteger estas cuentas está más que justificado. Así es como activas la autenticación de doble factor en Google:

1 Puedes hacer esta operación tanto desde el ordenador, como desde el móvil. Nosotros nos hemos decantado por esta última opción. Abre los ajustes de tu teléfono Android y localiza el icono de Google. Luego, toca sobre tu nombre de usuario y pasarás a la pantalla de la derecha. Toca en ***Usar tu teléfono para iniciar sesión***.



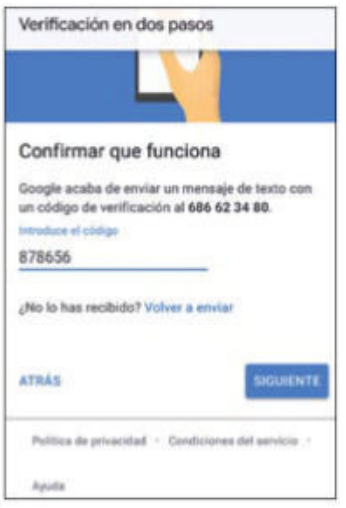
2 Ahora, tendrás que escribir tu nombre de usuario y contraseña de nuevo, e irás a parar a la pantalla ***Verificación en dos pasos***. Desliza hacia abajo, para ver el final de esa pantalla y pulsa sobre el botón ***Empezar*** que se encuentra ahí.

3 Una vez más, tendrás que identificarte, y pasarás a la lista de dispositivos que tienes asociados a esa cuenta de Google. Podrás utilizarlos todos para recibir las notificaciones, aunque es mejor que emplees tu teléfono principal. De modo que pulsa sobre el dispositivo que quieras y luego sobre ***Intentarlo ahora***.

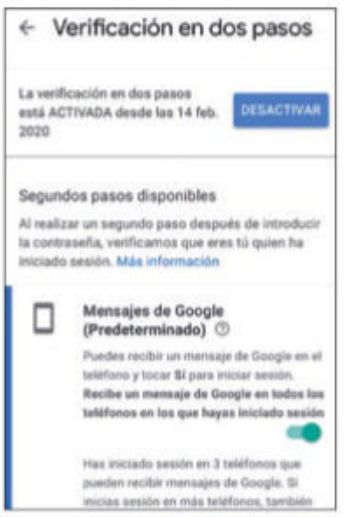
4 Acto seguido, aparecerá una pantalla en la que Google te pregunta si estás iniciando sesión. Este paso es necesario en el dispositivo en cuestión, para que puedas identificarte correctamente. A continuación, pulsa ***Sí***

5 Ahora, añade tu número de teléfono, para así asegurarte de que puedes recibir códigos de recuperación (en el caso en que no puedas realizar la autenticación en dos pasos). En el próximo paso, elige si quieres recibir esa información con un mensaje de texto o mediante una llamada de voz.

6 Como en todos los sistemas OTP, verás ahora una serie de datos que ofrecen como respaldo: una lista de códigos de seguridad que debes apuntar o guardar, porque te ayudarán a desbloquear la cuenta, en el caso de que pierdas el teléfono principal que utilizas como doble factor para la autenticación. Luego, recibirás un SMS con un número que debes escribir en la casilla. Ahora, toca sobre ***Siguiente***.



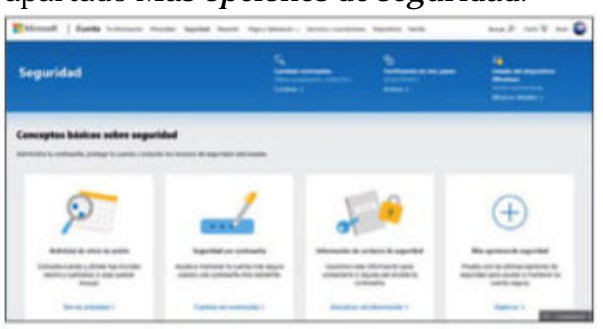
7 Ya solo te queda pulsar sobre el botón ***Activar*** para poner ya en marcha la doble autenticación. Google registra el día y la hora en que se ha activado, como referencia para el futuro. Si te fijas, también puedes volver a desactivar la doble autenticación con el botón ***Desactivar***.



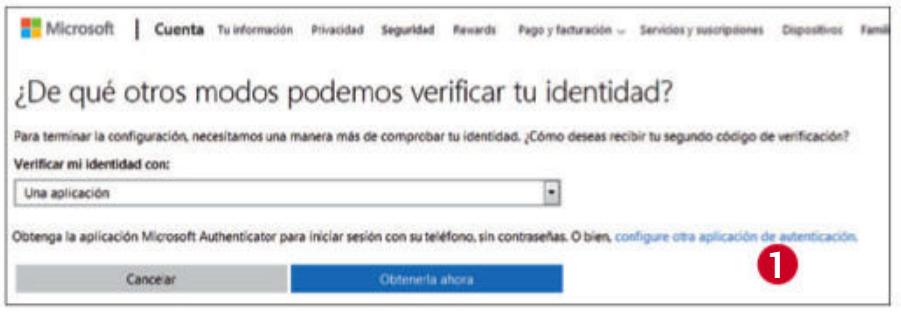
Más seguridad en Outlook.com

Naturalmente, el servicio de correo Outlook.com también soporta la autenticación de dos factores. Así que, si tienes una cuenta de Outlook, Windows o Hotmail, es recomendable que la actives. Hazlo así:

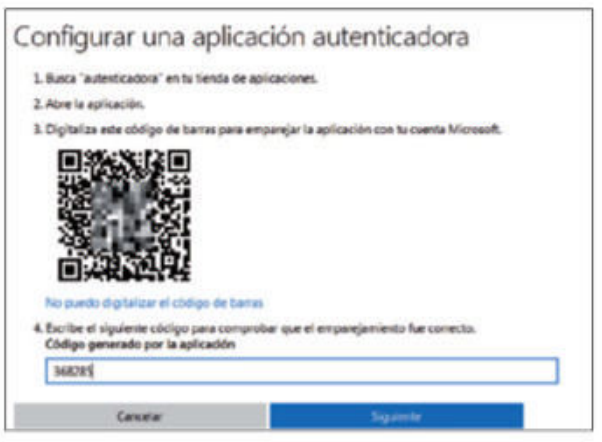
1 Inicia sesión en tu cuenta y pulsa sobre tu imagen, arriba a la derecha, seguido de un clic en ***Mi cuenta de Microsoft***. Luego, desde la barra superior, haz clic en ***Seguridad***. Ahora verás varias opciones disponibles. Haz clic en ***Explorar***, en el apartado ***Más opciones de seguridad***.



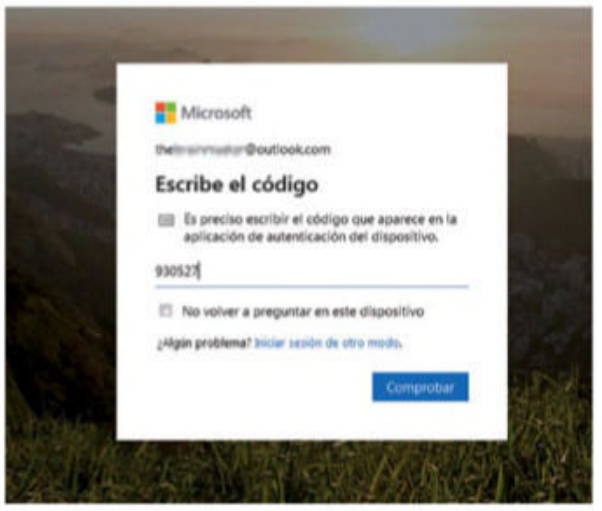
2 En la siguiente pantalla, pulsa ***Configurar la verificación en dos pasos*** y luego en ***Siguiente***. Ahora tienes tres opciones de autenticación: ***Una aplicación***, ***Un número de teléfono*** o ***Una dirección de correo alternativa***. Si no usas el autenticador de Microsoft, para emplear una app como FreeOTP, Authy, etc., pulsa el enlace ***configure otra aplicación de autenticación*** 1.



3 Seguidamente, abre tu app, por ejemplo FreeOTP, y escanea el código QR que aparece en el navegador, para enlazar la app con Outlook.com. Una vez que la entrada de Microsoft aparezca en FreeOTP, toca sobre ella para así poder generar un número, que debes escribir en la casilla de la web. Pulsa el botón ***Siguiente***.



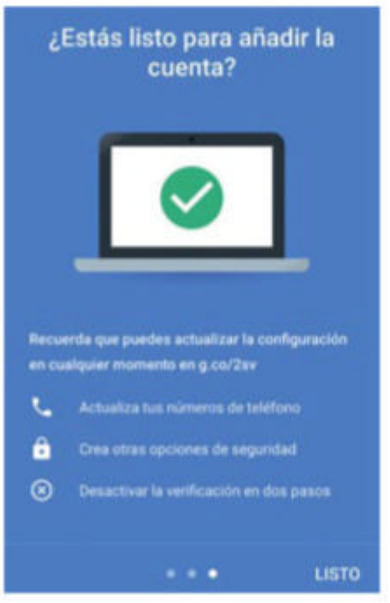
4 Outlook te mostrará un código de recuperación, que debes apuntar y guardar en lugar seguro. Haz clic en ***Siguiente*** y continúa por el resto de pantallas, hasta el final. A partir de ahora, cuando inicies sesión en tu cuenta de Outlook, verás una pantalla adicional, que te pedirá el código 2FA que has de generar en tu app.



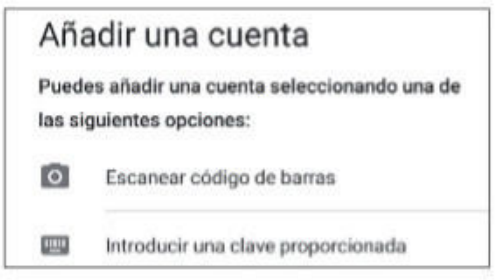
Dos factores en Dropbox con Google Authenticator

Google Authenticator es otra aplicación OTP, aunque esta vez de Google. De hecho, FreeOTP es una derivación de Google Authenticator, que se generó cuando Google convirtió a Authenticator en propietario, así que la funcionalidad es muy similar. Vamos a ver cómo puedes proteger tu Dropbox con un segundo factor OTP basado en Google Authenticator. Naturalmente puedes usar Authenticator para cualquier otro servicio en el que necesites contraseñas OTP.

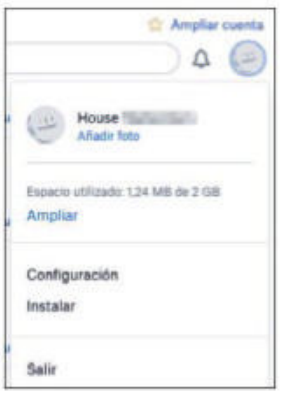
1 En primer lugar, instala la app de Google Authenticator desde tu store y ábrela. Lo primero que verás son unas breves líneas de instrucciones a las que conviene que eches un vistazo. Sobre todo, porque en la última pantalla hay un enlace que puedes usar más tarde para cambiar la configuración, si así lo quieres.



2 Tras pulsar sobre ***Listo***, verás dos opciones. Ahora, vamos a usar la primera que, por cierto, no está correctamente explicada. No se trata de un código de barras, sino de un código QR que, como sabes, no tiene barras, sino puntos. Por el momento, deja el móvil en espera, porque tienes que pasar a tu cuenta de Dropbox.

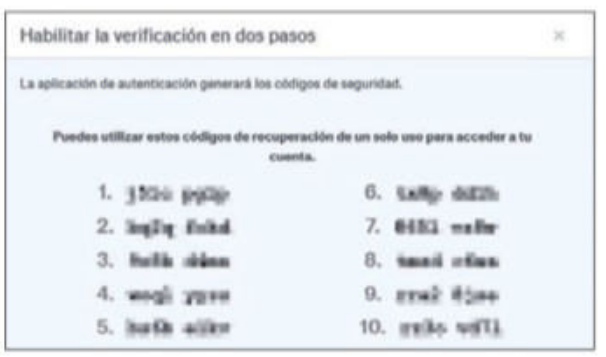


3 Seguidamente, abre Dropbox en el navegador del ordenador e inicia sesión con tus credenciales en tu cuenta. Arriba a la derecha, tienes disponible el icono (o la foto, si la has subido) de tu cuenta. Haz clic sobre él y, seguidamente, pulsa una vez sobre ***Configuración***. Luego, pulsa en ***Continuar*** y, en la siguiente ventana, verás dos opciones para utilizar la doble autenticación: ***Mensajes de texto SMS***, o bien ***Usar una aplicación móvil***. Esta última es la que nos interesa, y la que vamos a usar con Google Authenticator (o FreeOTP o cualquier otra app OTP). Haz clic en ella y en ***Siguiente***.



4 Ahora, vuelve a la app Google Authenticator, que debería estar en modo de cámara, y enfoca el código QR que ha aparecido en la pantalla del ordenador. En él, se encuentra toda la información necesaria para que no tengas que realizar la configuración del sitio manualmente.

5 En la pantalla del teléfono, aparece ahora un número de seis dígitos. Pulsa ***Siguiente*** en la ventana de Dropbox que hay en el ordenador y verás una casilla, en la que debes escribir ese número. Luego, haz clic en ***Siguiente*** de nuevo, y tendrás la posibilidad de introducir tu número de teléfono si quieres. Si no, continúa y verás una lista de códigos que debes apuntar o imprimir, ya que sirven para recuperar la cuenta si pierdes el móvil o no te funciona.



6 A partir de ahora, cada vez que inicies sesión en Dropbox, no solo tendrás que

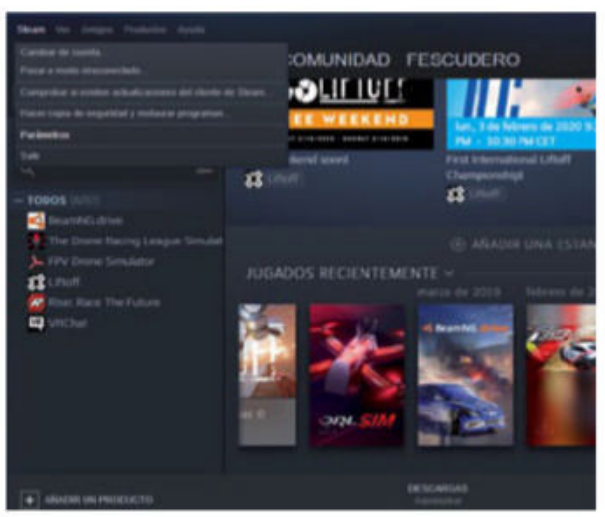
escribir tu contraseña, sino también introducir el número OTP que te proporciona Google Authenticator (o cualquier otra aplicación OTP que hayas elegido). Con esta acción, te aseguras de que el acceso a tu cuenta sea, a partir de ahora, mucho más difícil.

Asegura tu cuenta de Steam

Si eres aficionado a jugar en el ordenador, es muy probable que tengas una cuenta de Steam, para poder acceder a los miles de juegos que ofrece esta plataforma. Como sabrás, el acceso a Steam se realiza de forma habitual: con un nombre de usuario y una contraseña. Por ello, es recomendable que protejas tus inversiones en juegos y tus avances en los diferentes títulos con algo mejor que la pareja 'usuario/contraseña'.

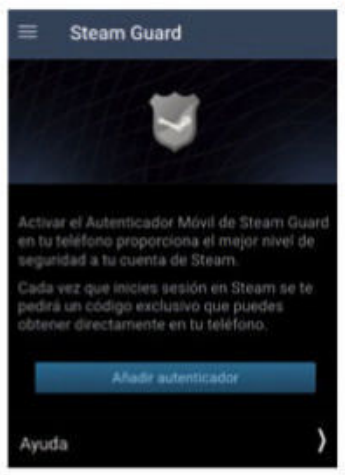
Por suerte, Steam ya ha pensado en eso y cuenta con su propio sistema. Este no necesita de aplicaciones OTP de terceros como Google Authenticator o similares. Puedes hacerlo todo con ayuda del ordenador, de tu móvil y de la app de Steam:

1 En primer lugar, abre la aplicación de Steam en el ordenador e inicia sesión si fuera necesario. Luego, haz clic en el menú ***Steam*** y, seguidamente, en ***Parámetros***, para así acceder a los ajustes de Steam.



2 En el apartado ***Cuenta*** de la izquierda, haz clic sobre el botón ***Administrar la protección Steam Guard de la cuenta***. Esto te llevará a una nueva ventana, con varias opciones. Pulsa sobre la superior, llamada ***Obtener códigos de Steam Guard desde la aplicación de Steam de mi teléfono***.

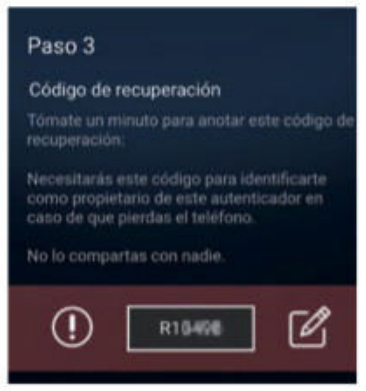
3 Ahora, pasa a la app Steam del teléfono y abre el menú lateral (las tres líneas). Selecciona entonces la entrada ***Steam Guard***, para así activar la autenticación de dos factores. En la primera pantalla que aparece, toca sobre ***Añadir autenticador***.



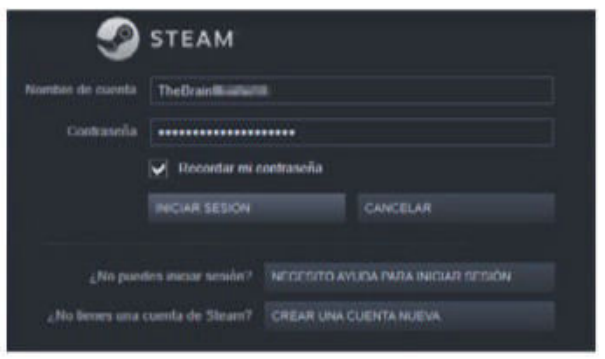
4 Acto seguido, deberás introducir tu número de teléfono, a fin de poder recibir los SMS del sistema. Luego, toca también en ***Añadir teléfono***. Pero antes de que eso ocurra, recibirás un email en la cuenta de correo vinculada con Steam. Haz clic en el enlace que aparece en ese email y luego en el botón ***Siguiente*** desde el teléfono.

5 Este proceso es un poco lioso, pero sirve para asegurarse de que tú eres realmente quien dice ser. Una vez que hayas confirmado el mensaje de correo y toques sobre ***Siguiente***, recibirás un mensaje SMS con un número que debes introducir en la siguiente pantalla. De alguna forma, este proceso es, en realidad, un sistema 2FA para llevar a cabo el proceso de 2FA. Escribe el código recibido en la casilla correspondiente y toca sobre ***Enviar***.

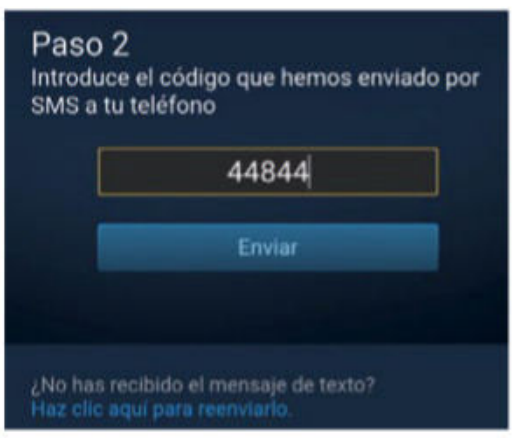
6 Ahora, por fin, recibirás un código de recuperación en pantalla. Es importante que apuntes ese código, ya que será lo único que te permita recuperar tu cuenta en caso de problemas; por ejemplo, si pierdes el teléfono y no puedes conseguir el segundo factor, para autenticarte.



7 A partir de este momento, si inicias sesión en tu cuenta de Steam de la forma habitual desde el ordenador, deberás escribir primero tu nombre de usuario y contraseña, de la forma acostumbrada.



8 Pero, ahora, aparecerá una nueva ventana que te solicita un código de 5 dígitos, que debes obtener en la app móvil de Steam. Verás que, debajo del código hay una barra azul que se va encogiendo. Ese es el tiempo de validez restante. Si el código cambia, no podrás usarlo y tendrás que escribir el nuevo. A partir de ahora podrás acceder a tu cuenta de Steam y a todos tus juegos e información personal de forma segura.



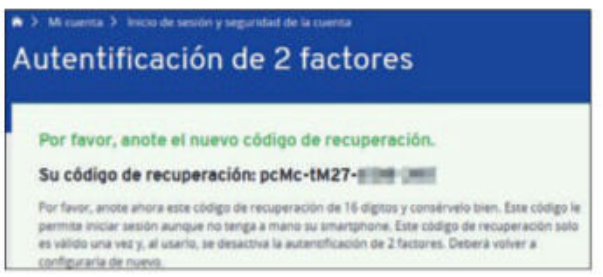
02 USO DE FREE OTP: PROTEGE TU ALOJAMIENTO WEB DE ATAQUES

FreeOTP es un programa similar a Google Authenticator, es decir, genera contraseñas únicas y válidas solo durante cortos periodos de tiempo. Ahora, vamos a ver un ejemplo de uso de esta app para un alojamiento web que soporta esta función. ¿Y por qué es importante proteger tu alojamiento web? Porque en él guardas no solo tu página (por ejemplo, si eres una empresa o autónomo) sino que también tienes ahí el servicio de email, que será donde recibas todas las confirmaciones de acceso de otros sitios. Por ello, este servicio es extremadamente importante y requiere de una buena protección que vaya más allá de una simple contraseña que se podría hackear. Como ejemplo, vamos a usar IONOS (antes 1&1), aunque otros proveedores disponen de servicios similares.

1 Comienza por acceder a tu panel de control y escribe tu nombre de usuario y contraseña habituales. Si te fijas, esto es lo único que te separa de todos tus ficheros online, sitio web, correo electrónico, acceso FTP, etc. De modo que activar 2FA es realmente importante, en este caso.

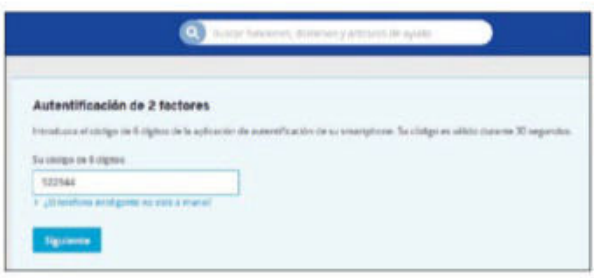
2 A continuación, pulsa sobre el icono de la persona en la esquina superior derecha, para, de este modo, poder acceder a los ajustes de tu perfil **2**. Continúa con un clic en ***Autentificación de 2 factores***. Luego, pulsa de nuevo sobre ***Autentificación de 2 factores*** y tendrás que escribir entonces tu contraseña de acceso al servicio.

3 Una vez que hayas activado la autenticación de 2 factores, es imprescindible que generes un código de recuperación. Este te servirá en el caso de que no tengas acceso al teléfono móvil para generar un código OTP, porque se ha roto, te lo han robado, no funciona, etc. Apunta este código en un lugar realmente seguro, porque si lo pierdes y no tienes acceso al teléfono, no podrás entrar en tu cuenta. Esto se aplica para cualquier otro servicio que admita OTP. Está claro así que, si no tienes ninguno de los factores de comprobación, no te van a dejar acceder de ningún modo.

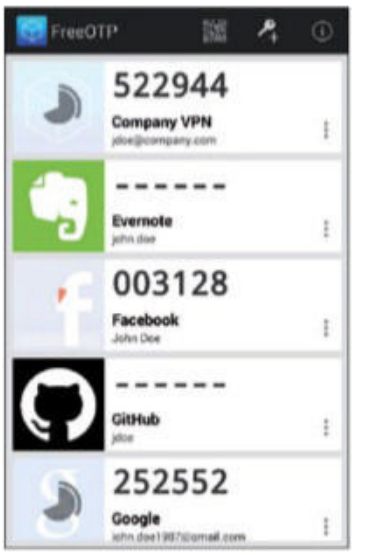


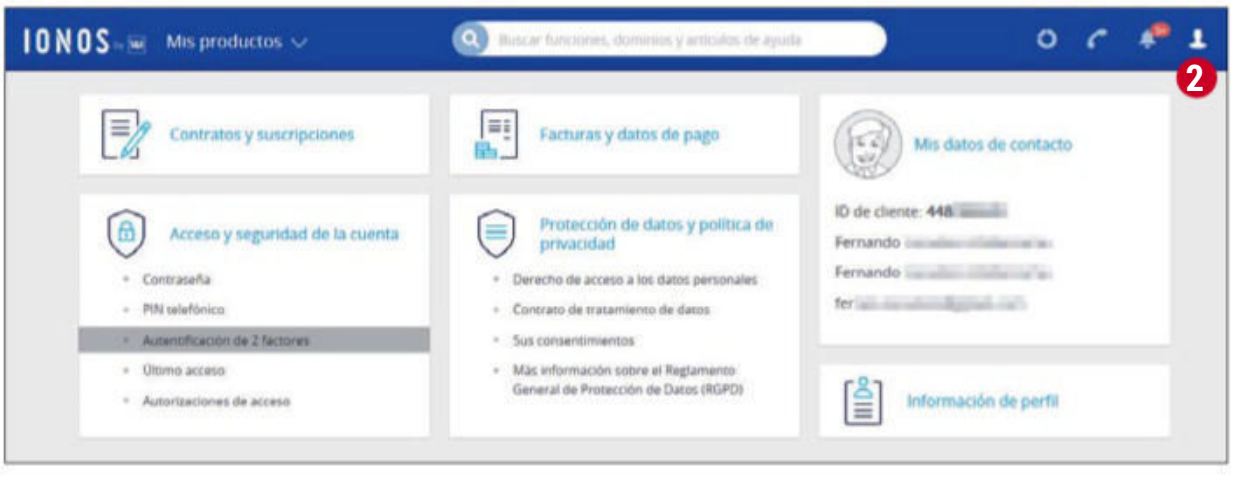
4 Ahora, descarga la app FreeOTP desde el store e instálala. Luego, ábrela y pulsa sobre el icono del código QR que hay arriba a la derecha. Pulsa en ***Configurar autentificación de 2 factores*** en la web de IONOS y aparecerá un código QR **3**. Este es el que debes escanear con FreeOTP y se configurará una nueva entrada para este servicio. En la app, puedes tener múltiples servicios disponibles y pulsar sobre el que necesites en cada momento, para obtener el código correspondiente. Luego pulsa en ***Confirmar*** y ya podrás vincular el acceso del sitio al segundo factor, mediante OTP.

5 A partir de ahora, cuando quieras acceder a tu alojamiento web, deberás escribir tu nombre de usuario y contraseña, como siempre, pero acto seguido aparecerá la pantalla que te pide un código OTP de 6 dígitos. Abre la app de FreeOTP



y pulsa sobre la entrada correspondiente, con lo que se generará un código. Observa que, al lado, hay un reloj en forma de gráfico de pastel que va disminuyendo. Si el pastel desaparece, el código ha dejado de tener validez y ya no lo podrás usar. Tendrás que generar uno nuevo. Así que escribe rápidamente el código en la casilla de la web y podrás acceder a tu hosting.





03 2FA EN LA AGENCIA TRIBUTARIA Y OTRAS ADMINISTRACIONES

Como vivimos en un estado social, los impuestos son necesarios y, por ende, no tienes más remedio que interactuar, al menos, una vez al año con Hacienda al año. Y, si eres autónomo te tocará hacerlo varias veces cada año. Por suerte, también la Agencia Tributaria se ha renovado y, hoy en día, puedes realizar prácticamente todos los trámites online, lo que agiliza muchísimo todas esas gestiones. Pero por otro lado, para que todas estos beneficios no dejen de serlo, está claro está que necesitas estar completamente seguro de que nadie puede hacer esos trámites en tu lugar o puede 'echar un vistazo' a tus datos fiscales. Actualmente, hay dos formas de realizar operaciones con la AEAT:

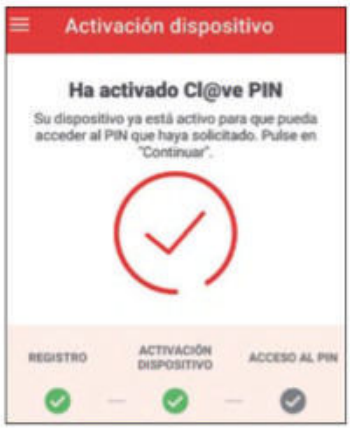
- **Un certificado digital: este se instala en el ordenador y firma todas las operaciones digitalmente. El inconveniente, es que siempre tienes que usar el mismo ordenador para operar.**

- **Cl@ve. Este sistema, que se puso en marcha hace unos años, emplea precisamente un método 2FA. Para poder usar Cl@ve, necesitas ir personalmente a tu delegación de Hacienda y solicitarla. Una vez dado de alta, descarga la app y sigue los siguientes pasos:**

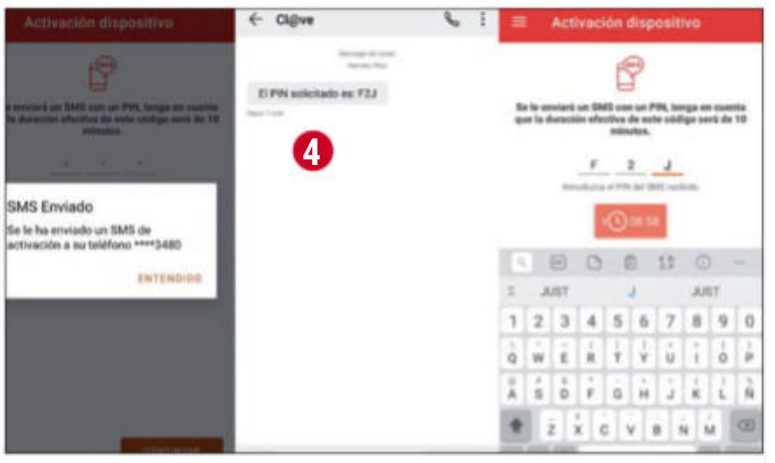
1 Abre la app y comienza por escribir tu DNI. Toca en *Aceptar* y la app te pedirá la fecha de caducidad de tu DNI. Búscala e introdúcela en el calendario que aparece. Toca de nuevo en *Aceptar*.

2 Como durante el alta en Hacienda de Cl@ve has tenido que dar tu teléfono móvil, ahora recibirás un SMS en ese número, para activar la app Cl@ve 4. De modo que mira ahora el PIN que acabas de recibir y escríbelo en la pantalla apropiada de la app, que aparece tras tocar sobre el botón *Entendido*. Ahora tienes 10 minutos para realizar esta operación.

3 Hecho todo esto, ya tienes lista la app en tu teléfono móvil para realizar operaciones con la AEAT y otros organismos oficiales que soporte el sistema Cl@ve. Pulsa sobre *Continuar* y pasa a tu navegador, bien en el móvil o el ordenador, para así iniciar el trámite en cuestión.



4 Para llevar a cabo esto, pulsa ahora sobre *Sede Electrónica* (en la página del a Agencia Tributaria) y deberás escribir tu DNI, así como su fecha de caducidad. Haz clic en *Continuar* 5 y, en la próxima página, pulsa en *Obtener PIN*.



5 Esto hará que el servidor de Hacienda contacte tu app de Cl@ve y te enviará un PIN, que es el que deberás escribir en la casilla correspondiente. Ten siempre en cuenta que, cada vez que necesites realizar un trámite, te hará falta un PIN. Y, a estas alturas, ya sabes que este PIN es, en realidad, una contraseña OTP. ¡Más fácil imposible!

TOKEN HARDWARE GOOGLE TITAN KEY

Ya hemos hablado de los Tokens de hardware, y el Titan Key de Google es justamente un representante de esta categoría de elementos de autenticación de dos factores. Se trata de una especie de llave USB que puedes conectar directamente al ordenador; así como otra que funciona mediante Bluetooth/NFC, por ejemplo para el teléfonos. Puedes ver los detalles en **cloud.google.com/titan-security-key?hl=es**. Funciona como todos los dispositivos de este tipo: cuando inicias sesión en uno de los servicios que aceptan Titan Key (actualmente son Google, Facebook y algún servicio cloud como Dropbox) insertas la llave y esta genera un código OTP que te identifica. Estos códigos cambian cada pocos segundos, para garantizar la seguridad. En el caso de los móviles, el método es el mismo, solo que tienes que acercar la llave al teléfono para que la detecte cuando inicias sesión en un sitio compatible y así te puedas identificar correctamente. Hasta hace poco, solo se podían comprar en Canadá, Estados Unidos, Francia, Japón y el Reino Unido, pero ya están disponible en España

Con las llaves Titan, puedes autenticarte en Google, Google Cloud y en otros muchos dispositivos.

04 CONTRASEÑAS SEGURAS EN TU NAVEGADOR CON AUTHY

Ya sabes que los navegadores tienen una función para guardar tus contraseñas de los distintos sitios y, además, permiten sincronizar tus marcadores favoritos, historial de navegación etc. Todo eso es información sensible que necesita ser protegida. Y también en este caso solo se interpone una contraseña entre los datos y un potencial hacker. Por esta razón, también los navegadores, como por ejemplo Firefox o Chrome, soportan autenticación 2FA. Vamos a ver un ejemplo con la ayuda de Firefox Sync, que es el sistema de sincronización de información personal de Mozilla. Y, en esta ocasión, vamos a ver otra app distinta para 2FA, llamada Authy, y que es de las más conocidas.

1 Abre el navegador Firefox y haz clic en el icono de tu cuenta, arriba a la derecha. Luego, pulsa en ***Ajustes de la cuenta*** y en ***Administrar cuenta***. Se abrirá la pantalla de la imagen. Pulsa sobre ***Activar***, al lado de ***Autenticación en dos pasos***.

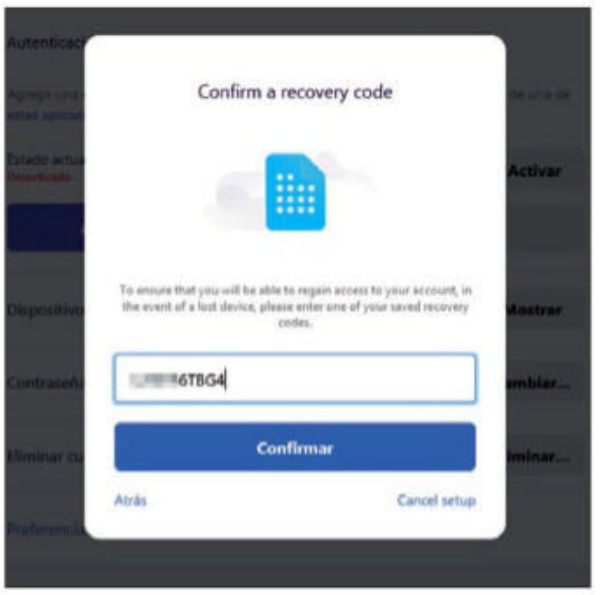
2 Si todavía no tienes la app Authy, descarga e instálala desde el store. Iníciala y te pedirá tu número de teléfono. Este paso es necesario, ya que sin ese dato no puede enviarte SMS de confirmación. De modo que escribe el número y pulsa luego en ***OK***.

3 A continuación, aparecerá una ventana de selección, en la que puedes elegir si quieres recibir el código de confirmación mediante un mensaje de texto SMS o, si lo prefieres, mediante una llamada de voz que te dictará el código de autenticación.

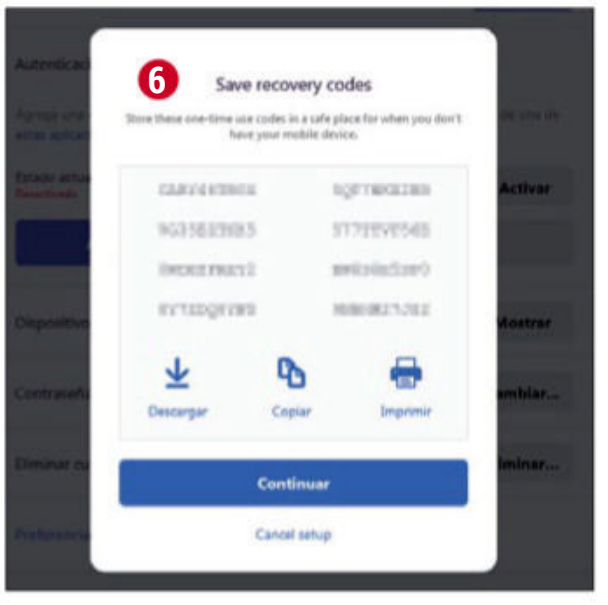
4 Ahora vuelve al navegador y verás que hay un código QR esperando ser escaneado. Desde la app de Authy, habrás llegado a la pantalla de la imagen, de modo que pulsa sobre ***Escanear código QR*** y escanea el QR que Firefox te está presentando para vincular la cuenta de Firefox Sync a Authy.

5 Antes de seguir, quedan un par de tareas que realizar. En primer lugar, Firefox te presenta una serie de códigos de recuperación, que debes apuntar, descargar o imprimir. Una vez hecho eso, pulsa directamente en el botón ***Continuar*** 6.

6 Además de lo anterior, deberás verificar al menos uno de los diferentes códigos. De modo que elige uno y escríbelo en la siguiente ventana. Luego, pulsa en ***Confirmar***. Este paso es necesario para comprobar la secuencia de códigos.



7 Con ello, finalmente, quedará activada la autenticación en dos pasos para acceder a tu cuenta de Firefox y, como prueba, verás la confirmación en pantalla. Otros navegadores cuentan con sistemas similares y el proceso, en su mayor parte, suele ser muy parecido al explicado.



¿PUEDES PROTEGER TU

Servicio/App	SMS	Llamada de voz	Email	Token hardware	Token software (App)
Almacenamiento online					
Apple iCloud	✔	✔	✘	✘	✔
Dropbox	✔	✘	✘	✔	✔
Google Drive	✔	✔	✘	✔	✔
Microsoft OneDrive	✔	✘	✘	✔	✔
Comunicaciones					
Google Hangouts	✔	✔	✘	✔	✔
Skype	✔	✔	✘	✔	✔
Slack	✔	✘	✘	✘	✔
Telegram	✔	✔	✘	✘	✘
WhatsApp	✔	✔	✘	✘	✘
Correo electrónico					
Google Gmail	✔	✔	✘	✔	✔
Microsoft Outlook	✔	✘	✘	✔	✔
Yahoo Mail	✔	✔	✘	✘	✘
Entretenimiento					
Deezer	✘	✘	✘	✘	✘
Electronic Arts (Origin)	✔	✔	✔	✘	✔
Google Play	✔	✔	✘	✔	✔
Netflix	✘	✘	✘	✘	✘
Playstation Network	✔	✘	✘	✘	✘
Spotify	✘	✘	✘	✘	✘
Steam	✘	✘	✔	✘	✔
Vimeo	✘	✘	✘	✘	✘
YouTube	✔	✔	✘	✔	✔
Salud y deporte					
Endomondo	✘	✘	✘	✘	✘
FitBit	✘	✘	✘	✘	✘
Google Fit	✔	✔	✘	✔	✔
Runtastic	✘	✘	✘	✘	✘
Strava	✘	✘	✘	✘	✘
Hoteles y hospedajes					
Airbnb	✔	✘	✔	✘	✘
Booking.com	✔	✘	✔	✘	✘

US CUENTAS CON 2FA?

Servicio/App	SMS	Llamada de voz	Email	Token hardware	Token software (App)
Sistemas de pago					
Amazon Pay	✔	✘	✘	✘	✔
Google Pay	✔	✔	✘	✔	✔
PayPal	✔	✘	✘	✘	✔
WePay	✔	✘	✘	✘	✔
Plataformas eCommerce					
AliExpress	✘	✘	✘	✘	✘
Amazon	✔	✘	✘	✘	✔
Apple	✔	✔	✘	✘	✔
eBay	✔	✘	✘	✘	✔
Seguridad					
Avast	✘	✘	✘	✘	✘
Bitdefender	✘	✘	✔	✘	✔
ESET	✘	✘	✘	✘	✘
Kaspersky	✔	✘	✘	✘	✔
McAfee	✘	✘	✘	✘	✘
Norton	✔	✔	✘	✔	✔
Sophos Central	✘	✘	✔	✘	✔
Redes sociales					
Facebook	✔	✘	✘	✔	✔
Flick	✘	✘	✘	✘	✘
Instagram	✔	✘	✘	✘	✔
Linkedin	✔	✘	✘	✘	✔
Pinterest	✔	✘	✘	✘	✔
Snapchat	✔	✘	✘	✘	✔
Twitter	✔	✘	✘	✔	✔
Otras					
Bitly	✔	✘	✘	✘	✘
Firefox	✘	✘	✘	✘	✔
Kickstarter	✔	✔	✘	✘	✔
Microsoft Office 365	✔	✔	✘	✔	✔
Opera	✘	✘	✘	✘	✔
TeamViewer	✘	✘	✘	✘	✔
Wikipedia	✘	✘	✘	✘	✔

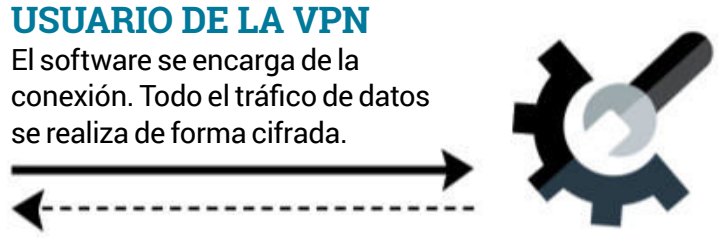
TEST 16 Servicios VPN

ASÍ FUNCIONA UNA VPN

Una VPN permite ocultar la actividad del usuario en Internet. No se puede conocer la dirección IP real y el flujo de datos está cifrado.

DISPOSITIVO DEL USUARIO DE LA VPN

El software se encarga de la conexión. Todo el tráfico de datos se realiza de forma cifrada.



16 SERVICIOS VPN A PRUEBA

A SALVO EN INTERNET

¿Quieres acceder a Internet de forma segura y anónima? Computer Hoy ha puesto a prueba 16 proveedores de redes privadas virtuales para ti. Aquí están los resultados.

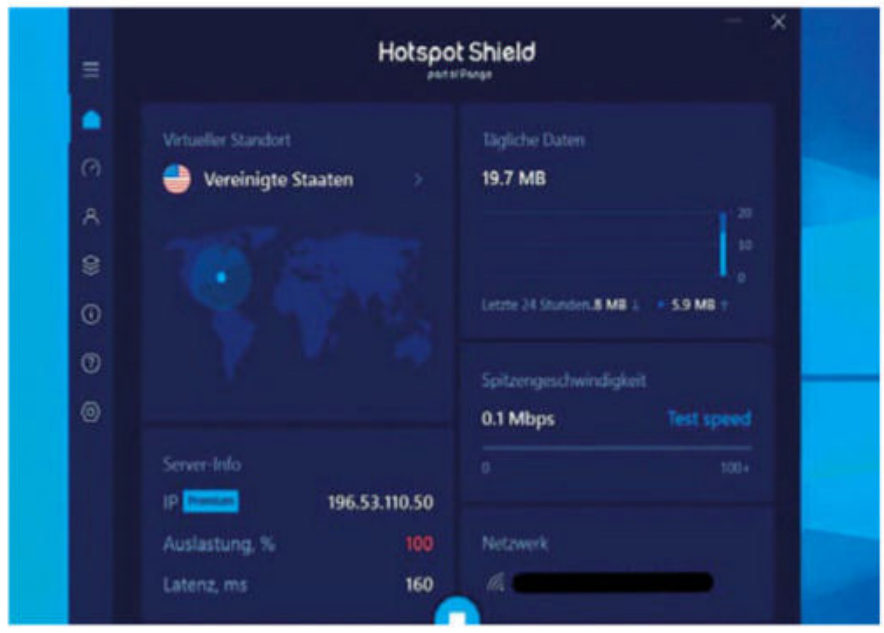
A veces sientes como que te están vigilando cuando estás online? Seguramente **estés en lo cierto**, porque en Internet hoy en día nadie tiene verdadera privacidad. Así que el deseo de ocultarse aumenta a cada día que pasa y, con él, un mercado que promete proporcionar justo eso. Hablamos de los servicios VPN. Y en Computer Hoy hemos probado 16 proveedores a fondo. Te descubrimos cuál ofrece más seguridad y velocidad de carga y descarga.

¿Qué es una VPN?

Cuando accedes a Internet obtienes una dirección IP que es **única para tu dispositivo**. Es como un número de identificación o de teléfono. Cuando abres una página web, esta preguntará (y posiblemente registrará) esta dirección IP. Y precisamente es a ese número al que el servidor enviará todos los datos que son necesarios para ver la página web.

La desventaja de esta clara identificación es que, como hemos dicho, **queda registrado con precisión** qué páginas web ve cada usuario y cuándo lo hace. Y con ello, es posible sacar conclusiones acerca de las aficiones, enfermedades, orientación política, estado financiero, ubicación, empleo...

Estos son los rastros que elimina un programa VPN, abreviatura de Virtual Private Network (red privada virtual, en español). Si un usuario se conecta con este tipo de red y realiza excursiones por Internet, el sitio web ya **no ve la dirección IP del usuario**, sino la del proveedor de VPN. Por decirlo de alguna forma, el programa crea un túnel seguro, a través del que puedes navegar por la red de forma casi anó-



Hotspot Shield ofrece un entorno con mucho estilo e información.

PROVEEDOR DE INTERNET

Como la conexión a través del proveedor de Internet al servicio VPN está cifrada, este no puede ver los datos enviados y recibidos por el usuario.

SERVIDORES VPN

Los servidores VPN son los encargados de acceder a las páginas que el usuario solicita y reenvían los resultados cifrados al equipo de este.

INTERNET

Las páginas visitadas solo ven la dirección IP del servidor VPN y no pueden averiguar la verdadera IP del usuario.

MÁS PELÍCULAS, MÁS NETFLIX AMERICANO CON UNA VPN

Para los fans del streaming puede merecer la pena el otro lado del charco. Porque la oferta americana de Netflix es mucho mayor que la biblioteca de streaming española. Y solo para clientes de EE.UU., porque Netflix utiliza la tecnología denominada Geoblocking (bloqueo por ubicación). Con ella, los proveedores de streaming limitan el acceso a ciertos contenidos, aunque con una VPN puedes saltarte esa limitación. Pero ¿está permitido? Las condiciones generales de Netflix no son claras al respecto. Sea como fuere, no es un delito, aunque en el peor de los casos te pueden bloquear la cuenta.

En general, cualquier servidor ubicado en los EE.UU. es adecuado para reproducir desde Netflix americano. Algunos proveedores como CyberGhost o Windscribe incluso ofrecen servidores especiales para este propósito, pero el acceso a los contenidos exclusivos en ocasiones es cuestión de suerte, porque el gigante del streaming ha cambiado su forma de proceder. En lugar de bloquear completamente a los usuarios de VPN, estos solo pueden ver el catálogo internacional, que es igual para todos los países. Solo cuando veas los contenidos específicos del país habrás conseguido saltarte el bloqueo con éxito.

En la página Flixwatch.co puedes ver los contenidos exclusivos de EE.UU.

nima. El gráfico de la primera página te muestra en detalle cómo funciona una VPN.

¿Para qué puedes utilizar una VPN?

Es un prejuicio el que las VPN se utilizan principalmente para usos criminales como, por ejemplo, descargar ficheros ilegales o comprar drogas en rincones oscuros de Internet. En realidad, los servicios VPN son muy **útiles en muchas situaciones cotidianas**. Aquí hay algunos ejemplos del día a día con los que te identificarás:

- **Proteger la privacidad:** ya estés comprando en la red o leyendo noticias, puedes estar seguro de que todas las páginas web están recolectando datos. Pero cada vez más personas quieren dejar el menor rastro digital posible, y una VPN les puede ayudar.

- **Más seguridad WiFi**: si lees tus emails en una cafetería o un hotel, estás en peligro. Cualquier atacante podría leerlos también. Aquí un servicio VPN protege tus datos.

- **Uso en el extranjero:** en países como China o Rusia el acceso a Internet, Facebook, Twitter y otras redes sociales está limitado. Si quieres tener acceso a todos los contenidos online, necesitas una VPN.

- **Streaming:** ver series de Netflix o desde mediatecas es algo normal para muchas personas. Pero si, en el extranjero no puedes ver ese partido o Netflix no te quiere mostrar tu serie favorita, te puede ayudar una VPN. Los servicios VPN buenos incluso 'liberan' los contenidos extranjeros de las plataformas de streaming –puedes averiguar más en el cuadro de la parte superior–.

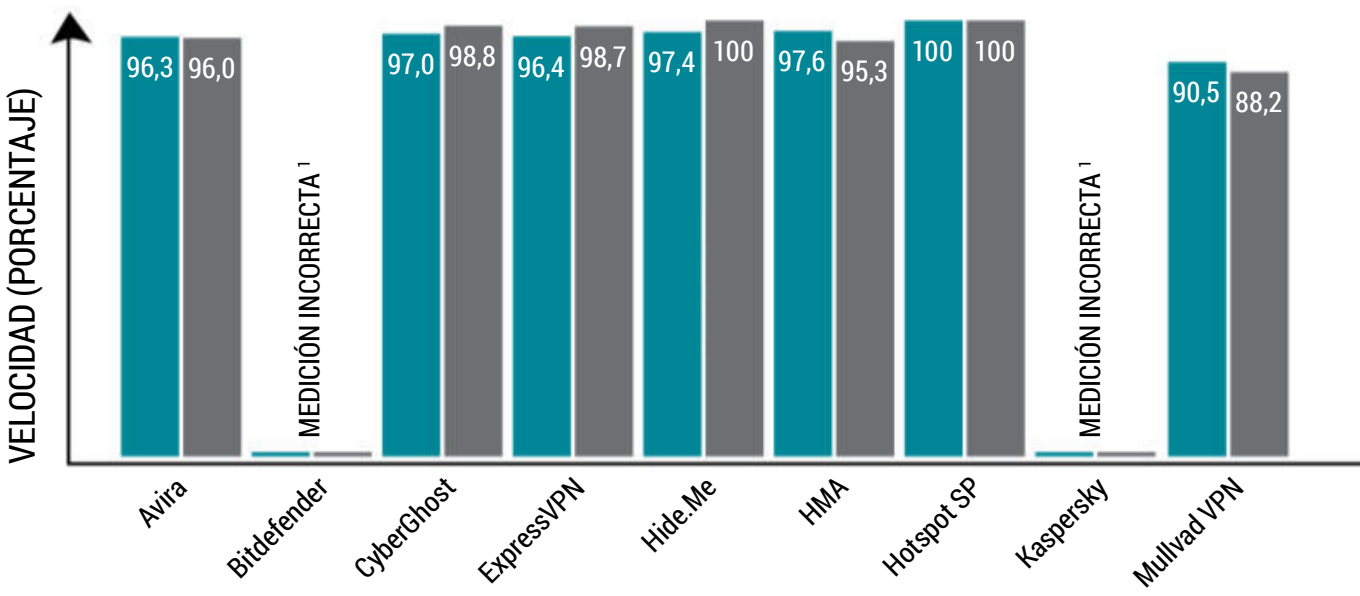
- **Compras más económicas:** las VPN también son interesantes si buscas gangas, porque muchas veces las tiendas online solo muestran los mejores precios a los visitantes de ciertos países. Los usuarios españoles suelen tener que pagar más, pero estas limitaciones se pueden anular con un servicio VPN de pago.

La seguridad tiene prioridad

Para que esta 'Protección para Internet' se merezca ese calificativo, ha de ser segura. Por suerte, hoy en día cualquiera de los servicios VPN que hemos probado tiene un Kill-Switch ('apagado de emergencia'). Y, con excepción de Hotspot

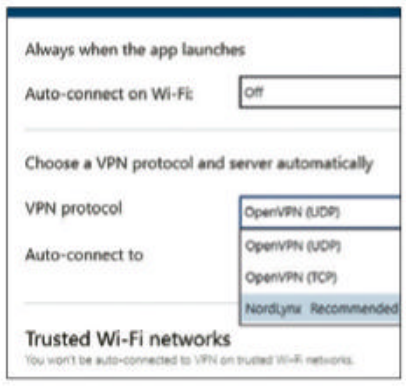
PRUEBA DE VELOCIDAD: RÁPIDOS EN GENERAL

Los resultados muestran qué porcentaje de la velocidad normal (sin VPN) han alcanzado de media los servicios con la VPN activa. Hotspot Shield es el que ofrece la mayor velocidad, PureVPN la más lenta. Las mediciones de Bitdefender y Kaspersky no se pudieron realizar debido a las interrupciones del servicio.



¿EL FUTURO DE LAS VPN?

Wireguard es una tecnología de VPN que, desde hace un tiempo, causa revuelo. Este protocolo VPN Open Source ofrece alguna ventaja con respecto a soluciones establecidas como OpenVPN o IKEv2: por un lado tiene funciones de cifrado nuevas y especialmente potentes; por el otro es muy ligero y rápido, porque necesita poco código de programación. Wireguard incluso es capaz de gestionar un cambio de red (por ejemplo de WiFi a LTE) mientras la conexión VPN sigue funcionando. Algunos proveedores ya han integrado Wireguard en sus servicios, como NordVPN.



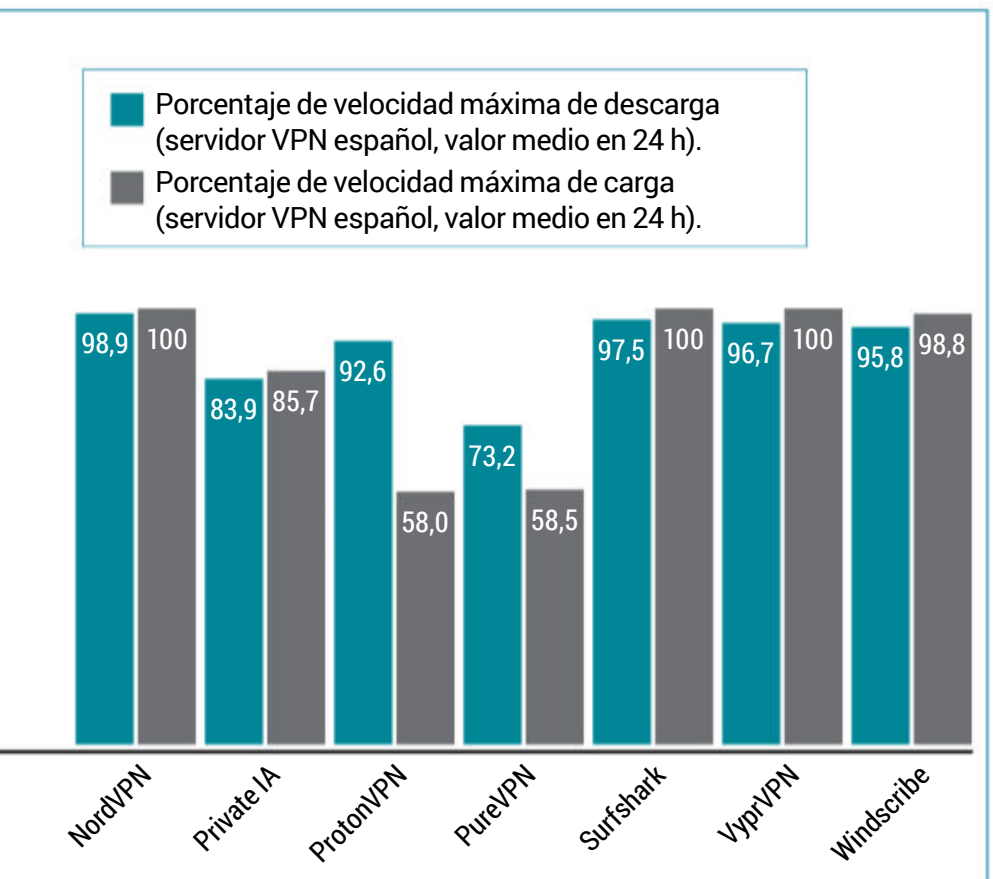
NordVPN tiene una versión propia de Wireguard llamada NordLynx.

Shield, Bitdefender y Kaspersky, todos emplean, al menos, el protocolo OpenVPN y un cifrado AES-256. Las tres excepciones apuestan por un desarrollo de Hotspot Shield, que se llama Catapult Hydra y que está optimizado, sobre todo, para rendimiento. A diferencia de OpenVPN, Catapult Hydra no es Open Source, así que **no se puede comprobar** lo que realmente esconde el código.

Por su parte, el protocolo VPN Wireguard es nuevo y ya durante su fase beta causó revuelo. En la actualidad ya se utiliza (ver cuadro superior) y NordVPN y Mullvad VPN son los primeros en integrar Wireguard en sus servicios. Otros como Hide.Me, Windscribe y VyprVPN se han apuntado también. CyberGhost, por ahora, solo usa Wireguard para Linux y Android, y también Wireshark ha anunciado la implementación del protocolo Wireguard de forma inminente.

Más siempre es mejor

Para obtener más seguridad algunos proveedores utilizan conexiones VPN de cifrado múltiple. La tecnología que hay detrás se llama Multi-Hop. La



[1] Interrupciones importantes del servicio durante las mediciones.

EN QUÉ DEBERÍAS FIJARTE EN UN SERVICIO VPN

1. ¿DÓNDE ESTÁ LA SEDE DEL SERVICIO VPN?

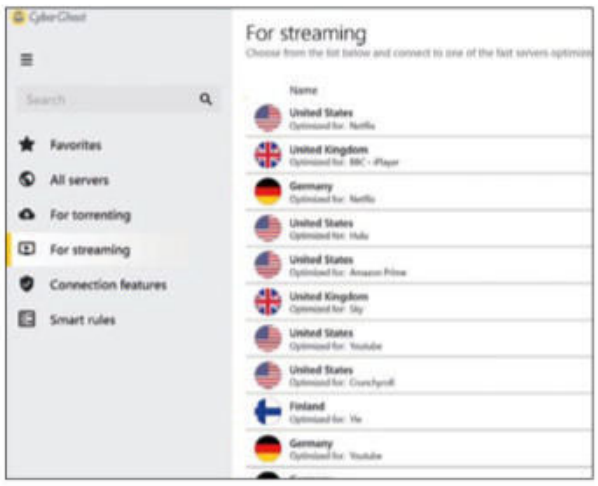
¿En qué país tiene su sede el proveedor? Esto tiene importancia debido a los servicios secretos. Porque ya no es un secreto: los servicios de inteligencia internacionales tienen acuerdos entre ellos con el fin de recolectar datos e intercambiarlos. Sobre todo los EE.UU. y el Reino Unido son los más activos de la alianza llamada 'Five Eyes', que forman junto a Canadá, Australia y Nueva Zelanda. Una colaboración que existe desde poco después de terminar la Segunda Guerra Mundial, 1946. En ella se organizan los servicios secretos que, actualmente, se han especializado en la escucha de redes electrónicas y en el análisis de la información. Los miembros tienen amplios poderes para la recolección y transferencia de datos privados y estos servicios de información incluso pueden obligar a las empresas a la entrega de datos. Por ese motivo muchos proveedores de VPN suelen tener su sede fuera del ámbito de acción de estas alianzas, para escapar de la obligación de tener que entregar los datos personales de los usuarios. Los Estados Unidos y el Reino Unido fueron los artífices principales, pero con el tiempo esta alianza se ha ido ampliando. Las nuevas alianzas ('Nine Eyes' y 'Fourteen Eyes') suman socios secundarios y terciarios que no tienen los mismos derechos que los fundadores. No obstante, los servicios secretos comparten información entre todos ellos. España, por ejemplo, pertenece a los 'Fourteen Eyes', es decir, no a los miembros principales, pero no obstante el servicio de inteligencia español, el CNI, colabora estrechamente con la agencia NSA americana.

2. ¿GUARDA MIS DATOS?

Las regulaciones de privacidad del servicio suelen indicar qué datos recolecta y qué hace con ellos. En principio todos los proveedores anuncian que no crean registros, la llamada 'No-Log-Policy'. Eso está bien, porque lo que no tienes, no lo puedes entregar. Pero esa promesa no siempre es del todo cierta. Así, algunos proveedores recogen datos estadísticos como horas o usos de ancho de banda, con el argumento de que de esta forma pueden mejorar el servicio. Desde un punto de vista técnico esto tiene explicación y no es una intervención seria. El problema lo representa el registro de las actividades del navegador, de la IP propia o del propio registro en el servicio, que permiten deducciones con respecto al usuario registrado.

3. CONFIABILIDAD

El tema de la confianza tiene gran importancia al elegir un proveedor VPN. Por ello, algunos de los servicios tienen informes de transparencia en su página web, los llamados 'Warrant Canary'. Se trata de una declaración publicada de forma regular que garantiza que el proveedor no ha recibido peticiones de ningún gobierno. Este curioso modo de proceder tiene su origen en una ley de los EE.UU., que obliga a las empresas a colaborar con el gobierno y además les prohíbe hablar sobre ello. Con la Warrant Canary las empresas pueden evitar ese 'bozal', porque si la declaración falta alguna vez o no es accesible, esto puede indicar que ha habido peticiones gubernamentales.



CyberGhost ofrece toda una armada de servidores especiales para servicios de streaming.

VyprVPN trabaja con servidores DNS propios, para proporcionar aún mucha más privacidad.

Surfshark: el modo 'No Borders' permite acceder a sitios y servicios censurados en un determinado país.

idea es que, si alguien consigue un acceso no autorizado a un servidor VPN, **no puede hacer nada** con la información, ya que los paquetes de datos entrantes y salientes nunca provienen del mismo servidor VPN. Multi-Hop está indicado, sobre todo, para la comunicación de información sensible de activistas o whistleblowers. De los proveedores de la prueba solo NordVPN, Surfshark, Hide.Me, Mullvad VPN y ProtonVPN soportan estos saltos múltiples. El resto apuesta por VPN simple.

Dos fallos totales en la prueba de velocidad

En la prueba de velocidad medimos los valores de descarga, carga y ping. Hotspot Shield y Nord VPN fueron muy rápidos y Hotspot Shield no mostró ninguna diferencia con respecto a la velocidad normal, impresionante. Pero también Surfshark, CyberGhost, Hide.Me y VyprVPN fueron rápidos. No ocurrió lo mismo con Bitdefender y Kaspersky: a pesar de muchas repeticiones de la prueba, **no conseguimos una medición** decente. El motivo es que la conexión VPN se interrumpía por completo y con frecuencia. En Kaspersky, incluso fue necesario reiniciar el ordenador para que la VPN funcionara de nuevo. Este grave fallo de la función principal llevó, en ambos casos, a una reducción de la nota hasta el 'Insuficiente'. También HMA tuvo que luchar con interrupciones, pero volvía a restaurar la conexión de forma automática. Aún así, le descontamos un punto, a causa de la frecuencia de las molestas interrupciones.

Confort y extras

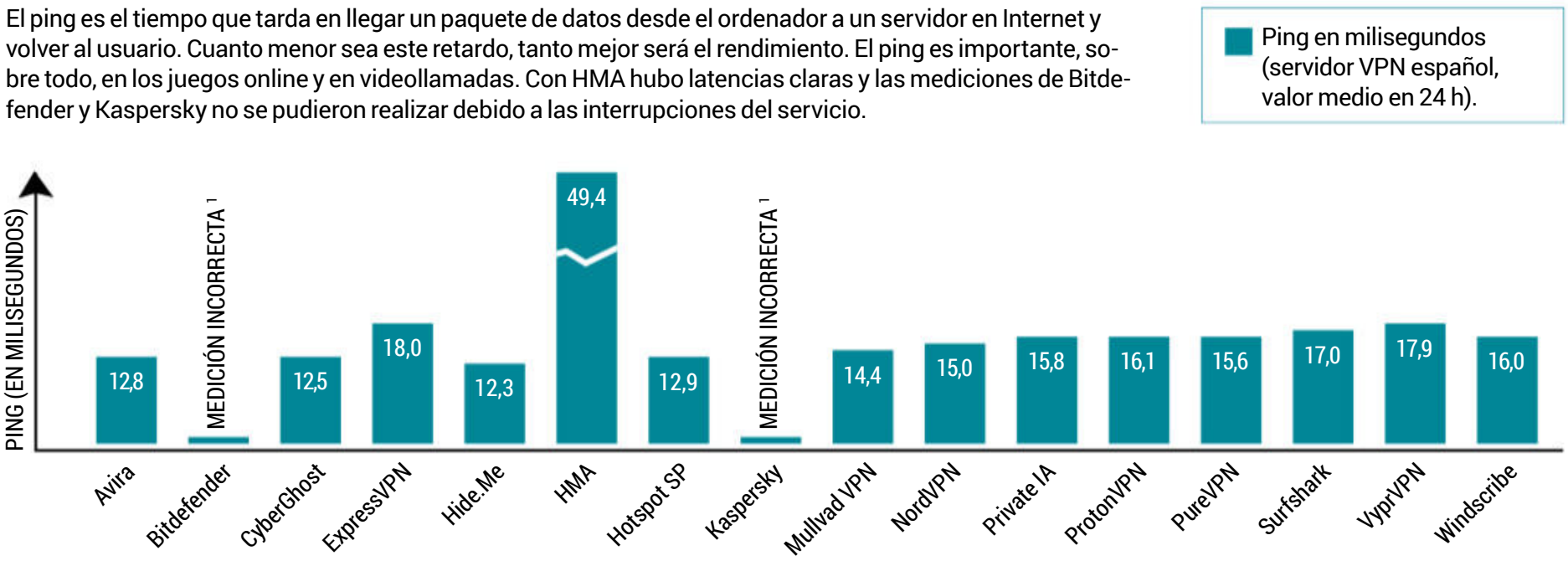
Ya no es suficiente con 'solo' crear una conexión VPN para convencer a los clientes. Por ello, los proveedores desarrollan constantemente nuevas funciones, para sobrevivir en el concurrido mercado de VPN. Algunas de ellas son solo extras agradables, otras extensiones con sentido (por ejemplo, la protección frente a malware, el acceso a la red Tor o el Split-Tunneling). A la derecha verás definiciones de algunas de estas funciones. Lo bueno es que en el manejo de la mayoría de los servicios VPN hubo **poco que criticar**. Solo PureVPN dio una impresión negativa con un entorno algo complicado.

CONCLUSIÓN

NordVPN consigue de nuevo el primer puesto y convence con una oferta muy completa. Muy cerca, y también con sobresaliente, está Surfshark, que comparte el calidad/precio con Windscribe. La mayor funcionalidad la tienes en ExpressVPN y, en general, la seguridad de todos es muy elevada. En realidad, solo Bitdefender y Kaspersky decepcionaron.

PING DE RESPUESTA MEDIO EN EL LABORATORIO: CASI TODOS BIEN, PERO TRES DE ELLOS FLOJEAN

El ping es el tiempo que tarda en llegar un paquete de datos desde el ordenador a un servidor en Internet y volver al usuario. Cuanto menor sea este retardo, tanto mejor será el rendimiento. El ping es importante, sobre todo, en los juegos online y en videollamadas. Con HMA hubo latencias claras y las mediciones de Bitdefender y Kaspersky no se pudieron realizar debido a las interrupciones del servicio.



[1] Interrupciones importantes del servicio durante las mediciones.

TERMINOLOGÍA VPN Y FUNCIONES SEGURAS: ¿QUÉ SIGNIFICA...?

PROTOCOLOS DE COMUNICACIÓN VPN

Un protocolo VPN define las reglas y los procesos con los que los servicios VPN pueden realizar una conexión segura. Los paquetes de datos se convierten a un protocolo VPN y luego se transfieren ('VPN Tunneling').

- **Protocolo IKEV2**
  Con el Internet-Key-Exchange-Protocol Version 2 se presentó un protocolo de seguridad que funciona igual de bien tanto en plataformas Windows como en Linux. Este protocolo VPN destaca, sobre todo, por estándares de seguridad muy elevados y diversos cifrados fuertes.

- **Protocolo OPEN VPN**
  El protocolo VPN basado en Open Source es actualmente la tecnología más potente y común con un cifrado de 160 a 256 bits. Es muy seguro y extremadamente rápido, incluso en grandes distancias.

- **Protocolos PPTP y L2TP/IPSEC**
  Hace tiempo que se consideran inseguros ya que están bajo la sospecha de vulnerabilidad. Sobre todo L2TP, del cual se tienen una y otra vez indicios de que la agencia NSA estadounidense conoce perfectamente los puntos débiles de este protocolo VPN.

- **Protocolo SSTP**
  El Secure Socket Tunneling Protocol tiene origen en Microsoft y está integrado en Windows de serie. El protocolo emplea cifrado SSL y la tecnología se parece mucho a HTTPS. Aunque SSTP es seguro, una y otra vez aparecen especulaciones acerca de que Microsoft haya incluido puertas traseras para poder extraer datos de las transmisiones.

- **Protocolo SOFTETHER**
  Protocol VPN Open Source desarrollado en Japón que reúne protocolos conocidos como OpenVPN, IKEv2 y SSTP bajo un mismo techo y que se define por una buena velocidad y un buen cifrado.

GPS-SPOOFING

Esta tecnología oculta el posicionamiento GPS real del usuario, creando una ubicación virtual. Las páginas y servicios solo ven el lugar virtual.

KILL-SWITCH

Esta funcionalidad no es otra cosa que un interruptor de emergencia que corta la conexión con Internet si el túnel VPN falla o se interrumpe momentáneamente la conexión. También está la opción App Kill-Switch, que solo desconecta de Internet un programa previamente definido y no todo el tráfico hacia y desde la Red.

CONEXIÓN MULTI-HOP

También conocida como VPN en cascada, no solo envía los datos como normalmente a través de un servidor VPN, sino que realiza la conexión en serie a través de servidores en varias ubicaciones. El usuario puede definir qué servidores se utilizan y los datos se cifran de nuevo en cada salto de ubicación. La ventaja es que en ninguna de las paradas intermedias es posible asignar el flujo de datos a un usuario determinado e incluso los ficheros de registro no dan pistas sobre la identidad de este. Ahora bien, es mucho más seguro pero hay que tener en cuenta que la conexión en cascada afecta a la velocidad de carga y descarga.

IP ALEATORIA Y DEDICADA

Si el proveedor ofrece la primera opción, el usuario recibe una dirección IP nueva a intervalos regulares para mejorar su anonimato. En el segundo caso recibe una IP dedicada que no comparte con otros usuarios. Esto tiene ventajas, por ejemplo, en compras y banca online, ya que estos sitios suelen calificar una IP cambiante como actividad sospechosa.

NEURO-ROUTING

Este avanzado sistema, desarrollado por Perfect Privacy, es muy similar a la función Multi-Hop, pero la Inteligencia Artificial integrada busca constantemente rutas seguras por Internet. A diferencia del Multi-Hop clásico, los servidores VPN varían constantemente y permiten, además, una conexión más directa y optimizada con el servidor de destino.

ONION OVER VPN

Con este método de conexión los datos primero se envían a un servidor VPN convencional y luego por la red anónima TOR. De esta forma, el proveedor de Internet no puede identificar al cliente como un usuario de TOR.

SMART DNS

Se trata de una tecnología que se emplea para evitar el Geoblocking, es decir, el bloqueo de contenidos en función de la ubicación. Gracias a esta función, un Proxy especial envía las peticiones al destino, de modo que el servicio correspondiente cree que estás en el mismo país. Los datos no se cifran, a diferencia de con una VPN, pero no pasas por DNS de terceros.

SPLIT-TUNNELING

Con esta función los usuarios pueden decidir qué datos se envían por el túnel cifrado VPN y cuáles no. De esta forma, puedes ver el Netflix americano con la VPN encendida, mientras que navegas por páginas locales sin VPN.

STEALTH VPN / OBFUSCATION

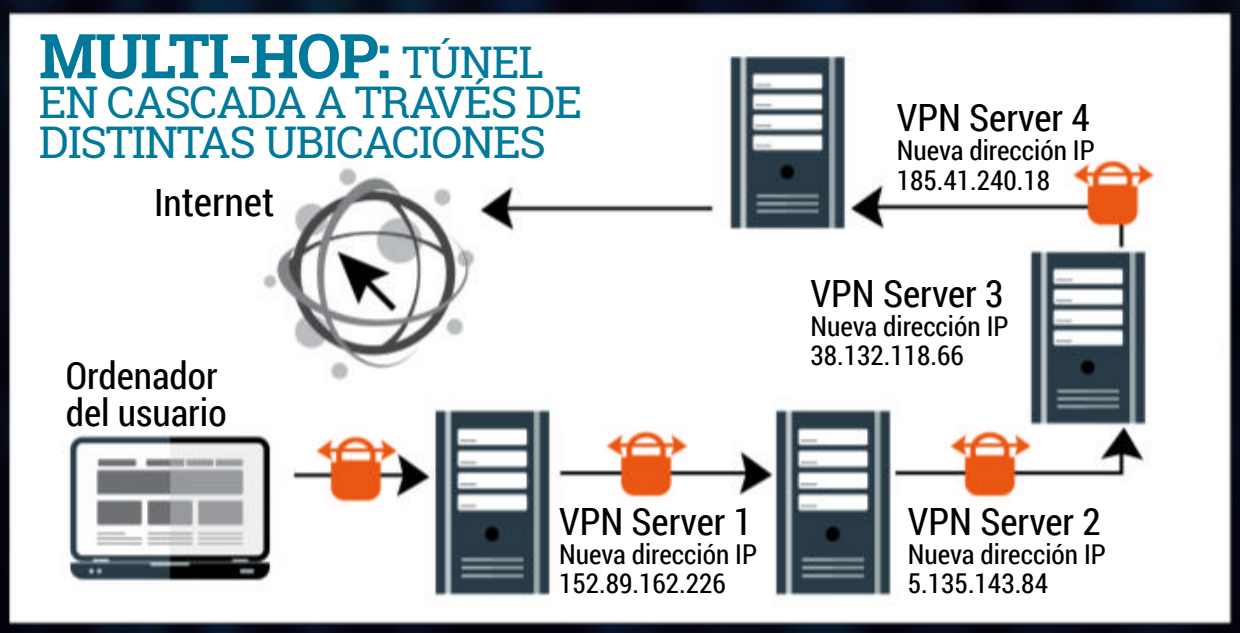
Modo de ofuscación que oculta el tráfico de datos. El flujo de datos parece tráfico normal a través de HTTPS y con ello escapa al control de los vigilantes que pueden reconocer el tráfico VPN y bloquearlo. Esta ocultación funciona con diferentes tecnologías. Para un camuflaje adicional se utiliza, por ejemplo, OpenVPN.

PROTECCIÓN WIFI

La VPN se activa automáticamente si te conectas a una WiFi no segura, por ejemplo, pública.

INVISIBILITY ON LAN

El ordenador permanece invisible para otros dispositivos que estén en la misma red local.



LA PRUEBA EN DETALLE

Computer Hoy GANADOR CALIDAD — NordVPN

1 NORDVPN
PRECIO/AÑO: 161,41 EUROS

NordVPN vence a la competencia con unas funciones más que convincentes. Aparte de unos generosos 5.400 servidores en casi 60 países, la seguridad de primera, las rápidas velocidades, el buen rendimiento en streaming, así como interesantes funciones adicionales apenas dejan nada más que desear.

Computer Hoy GANADOR CALIDAD/PRECIO — Surfshark

2 SURFSHARK
PRECIO/AÑO: 50,16 EUROS

El tiburón de las VPN Surfshark enseña los dientes y, además, presenta un precio muy económico. Los extras como la protección frente a malware, funciones especiales de ocultación y Split-Tunnelling no son habituales en esta gama de precios. Surfshark puntúa, sobre todo, con su manejo intuitivo.

CyberGhost

3 CYBERGHOST
PRECIO/AÑO: 49,50 EUROS

Si quieres utilizar tu VPN sobre todo para disfrutar de contenido en streaming de Netflix y otros proveedores disponibles en otros países, es difícil que evites CyberGhost. Este proveedor tiene toda una serie de servidores especiales, que superan cualquier frontera. Y también los extras del servicio son encomiables.

Nombre completo		NORDVPN		SURFSHARK		CYBERGHOST VPN	
Dirección web del fabricante		www.nordvpn.com		surfshark.com		www.cyberghostvpn.com	
Sede de la empresa		Panamá		Islas Vírgenes Británicas		Rumanía	
Sistemas		Windows, macOS, Linux, Android, iOS, Chrome, Firefox, SmartTV Android		Windows, macOS, Linux, Android, iOS, Chrome, Firefox, Fire TV, Apple TV, SmartTV, PS4, Xbox		Windows, macOS, Linux, Android, iOS, Chrome, Firefox, Fire TV, Apple TV, SmartTV, PS4, Xbox	
Protocolos		WireGuard (NordLynx), OpenVPN		OpenVPN, IKEv2/IPSec		WireGuard, OpenVPN, IKEv2/IPSec	
RENDIMIENTO	**25,00%**		**9,60**		**9,20**		**9,20**
Retardo medio al descargar datos (durante 24h)		1,10%	9,40	2,50%	8,80	3,00%	8,40
Retardo medio al cargar datos (durante 24h)		0,00%	10,00	0,00%	10,00	1,20%	9,40
Tiempo medio de respuesta (durante 24h)		15,0 ms	9,20	17,0 ms	8,80	12,5 ms	10,00
FUNCIONALIDAD	**20,00%**		**7,80**		**9,00**		**9,20**
Número de países		59	6,20	63	6,60	90	10,00
Número de servidores		5.400	10,00	1.700	10,00	6.200	10,00
Número de dispositivos por licencia / conexiones simultáneas		6 / sí	5,00	Ilimitado / sí	10,00	7 / sí	6,00
Soporte de descarga mediante Torrent / redes Peer-to-peer		Sí	10,00	Sí	10,00	Sí	10,00
PAGOS, FIABILIDAD Y SEGURIDAD	**25,00%**		**10,00**		**9,00**		**7,80**
Protección frente a vulnerabilidades (leaks): DNS / IP / WebRTC		Sí	10,00	Sí	10,00	Sí	10,00
Funcionalidad Kill-Switch		Sí	10,00	Sí	10,00	Sí	10,00
Conexión de datos Multi-Hop		Sí	10,00	Sí	10,00	No	0,00
Soporte WireGuard		Sí	10,00	No	0,00	Con limitaciones	6,00
Proveedor fuera de alianzas '5 Eyes' / '9 Eyes' / '14 Eyes'		Sí	10,00	Sí	10,00	Sí	10,00
Sin registros de actividad (No-Log Policy)		Sí	10,00	Sí	10,00	Sí	10,00
Informe de transparencia o Warrant Canary		Sí	10,00	Sí	10,00	Sí	10,00
Métodos de pago		Tarjeta de crédito, PayPal, transferencia inmediata, Bitcoin	8,00	Tarjeta de crédito, PayPal, Giropay, transferencia inmediata, Bitcoin	10,00	Tarjeta de crédito, PayPal, transferencia inmediata, Bitcoin	8,00
FUNCIONALIDAD GEOBLOCKING Y STREAMING	**20,00%**		**9,00**		**9,00**		**10,00**
Conexión con Netflix Estados Unidos		Sí	10,00	Sí	10,00	Sí	10,00
Conexión con Netflix España desde el extranjero		Sí	10,00	Sí	10,00	Sí	10,00
Servidores dedicados para streaming		No	0,00	No	0,00	Sí	10,00
Soporte geoblocking en streams en directo / mediatecas		Sí / sí	10,00	Sí / sí	10,00	Sí / sí	10,00
MANEJO	**10,00%**		**10,00**		**10,00**		**9,40**
Uso y configuración		Muy sencillo, muchas posibilidades de ajuste, diseño elegante de mapamundi	10,00	Muy sencillo, muchas posibilidades de ajuste, diseño moderno	10,00	Sencillo, muchas posibilidades de ajuste, versión móvil simplificada	9,00
Funciones adicionales		Bloqueador de publicidad, protección frente a tracking, Stealth VPN, protección WiFi, Onion over VPN, SmartDNS	10,00	Bloqueador de publicidad, protección frente a tracking, malware y phishing, Split-Tunneling, Stealth VPN, invisibility on LAN	10,00	Bloqueador de publicidad, protección frente a tracking, Split-Tunneling, protección WiFi, compresión de datos	10,00
CALIDAD		**Sobresaliente**	**9,26**	**Sobresaliente**	**9,15**	**Sobresaliente**	**9,03**
PRECIO		**161,41 €**		**50,16 €**		**49,50 €**	

4 HIDE.ME
PRECIO/AÑO: 99,99 EUROS

Hide.me de Malasia es, cada vez más, una opción muy recomendable para los usuarios que buscar salvaguardar su privacidad. Las funciones de anonimización son estupendas, las indicaciones transparentes y no todos los servicios VPN emplean servidores DNS propios. Aunque eso se nota en el precio.

5 WINDSCRIBE
PRECIO/AÑO: 41,36 EUROS

La selección de servidores es limitada y Canadá como sede de la empresa no debe ser la primera elección cuando se trata de proteger la identidad. A cambio, Windscribe está en primera línea a nivel técnico y, además, tiene muchas funciones útiles. El paquete completo convence con su precio realmente económico.

6 EXPRESSVPN
PRECIO/AÑO: 84,37 EUROS

El servicio que ofrece ExpressVPN está disponible para muchos sistemas operativos y dispositivos, y ofrece una buena funcionalidad. Con ExpressVPN puedes evitar bloqueos por ubicación (Geoblocking) y hacer streaming de Netflix y mediatecas extranjeras. Pero a nivel técnico el servicio ya no está a la última.

7 HOTSPOT SP
PRECIO/AÑO: 95,88 EUROS

Servicio con estilo y, sobre todo, increíblemente rápido, que también se lleva muy bien con Netflix y compañía. Pero al fijarte bien, la elegante fachada tiene algunos defectos a considerar: el manejo es bastante complicado y el proveedor guarda sorprendentemente muchos datos durante el registro como usuario.

8 VYPRVPN
PRECIO/AÑO: 45,00 EUROS

El servicio suizo VyprVPN ofrece un magnífico paquete para principiantes con streams de contenidos rápidos, ya sea de Netflix, contenidos de TV españoles o de mediatecas. El manejo es sencillo y a ello se añade el cifrado Chameleon y estupendas funciones de anonimización con VyprDNS. El precio acompaña.

HIDE.ME	WINDSCRIBE	EXPRESSVPN	HOTSPOT SHIELD PREMIUM	VYPRVPN
hide.me	esp.windscribe.com	www.expressvpn.com	www.hotspotshield.com	www.vyprvpn.com
Malasia	Canadá	Islas Vírgenes Británicas	Suiza	Suiza
Windows, macOS, Linux, Android, iOS, Chrome, Firefox, Fire TV, router	Windows, macOS, Linux, Android, iOS, Chrome, Firefox, Opera, Fire TV, Kodi, Nvidia Shield	Windows, macOS, Linux, Android, iOS, Chrome, Firefox, Fire TV, SmartTV, PS4, Xbox, router	Windows, macOS, Linux, Android, iOS, Chrome, SmartTV Android, Fire TV, router	Windows, macOS, Linux, Android, iOS, SmartTV, router
WireGuard, OpenVPN, SoftEther, IKEv2	WireGuard, OpenVPN, IKEv2/IPSec	OpenVPN, IKEv2/IPSec	Catapult Hydra, IKEv2/IPSec	WireGuard, Chameleon, OpenVPN
9,40	**9,10**	**8,60**	**9,80**	**9,00**
2,60% 8,60	4,20% 7,80	3,60% 8,20	0,00% 10,00	3,30% 8,40
0,00% 10,00	0,20% 9,80	1,30% 9,40	0,00% 10,00	0,00% 10,00
12,3 ms 10,00	16,0 ms 9,00	18,0 ms 8,40	12,9 ms 9,80	17,9 ms 8,60
9,20	**6,20**	**10,00**	**8,40**	**6,40**
72 7,80	63 6,60	94 10,00	80 8,80	70 7,40
1.800 10,00	110 0,60	3.000 10,00	3.200 10,00	700 4,60
10 / sí 9,00	Ilimitado / sí 10,00	Ilimitado / sí 10,00	5 / sí 4,00	5 / sí 4,00
Sí 10,00	Sí 10,00	Sí 10,00	Sí 10,00	Sí 10,00
9,60	**8,20**	**6,60**	**5,40**	**7,40**
Sí 10,00	Sí 10,00	Sí 10,00	Sí 10,00	Sí 10,00
Sí 10,00	Sí 10,00	Sí 10,00	Sí 10,00	Sí 10,00
Sí 10,00	Sí 10,00	No 0,00	No 0,00	No 0,00
Sí 10,00	Sí 10,00	No 0,00	No 0,00	Sí 10,00
Sí 10,00	No 0,00	Sí 10,00	Sí 10,00	Sí 10,00
No, recopila algunos datos estadísticos 8,00	No, recopila algunos datos estadísticos 8,00	Sí 10,00	No, recopila algunos datos personales 4,00	Sí 10,00
Sí 10,00	Sí 10,00	No 0,00	No 0,00	No 0,00
Tarjeta de crédito, PayPal, transferencia inmediata, Bitcoin 8,00	Tarjeta de crédito, PayPal, Bitcoin 6,00	Tarjeta de crédito, PayPal, Giropay, transferencia inmediata, Bitcoin 10,00	Tarjeta de crédito, PayPal 4,00	Tarjeta de crédito, PayPal 4,00
7,40	**10,00**	**9,00**	**9,00**	**9,00**
Sí 10,00	Sí 10,00	Sí 10,00	Sí 10,00	Sí 10,00
No 0,00	Sí 10,00	Sí 10,00	Sí 10,00	Sí 10,00
Sí 10,00	Sí 10,00	No 0,00	No 0,00	No 0,00
Sí / sí 10,00	Sí / sí 10,00	Sí / sí 10,00	Sí / sí 10,00	Sí / sí 10,00
9,00	**9,40**	**9,00**	**8,00**	**8,40**
Sencillo, diseño moderno, versión móvil simplificada 9,00	Sencillo, muchas posibilidades de ajuste, diseño minimalista 9,00	Sencillo, diseño limpio, versión móvil simplificada 9,00	Complicado, diseño elegante, versión iOS reducida 7,00	Sencillo, diseño sencillo y limpio 9,00
Split-Tunneling, Stealth VPN, Firewall, servidores DNS propios, IPv6-Support 9,00	Bloqueador de publicidad, protección frente a tracking, Split-Tunneling, Port-Forwarding, GPS-Spoofing, IP dedicada 10,00	Split-Tunneling, servidores DNS propios, Leak-Tests, optimizador de velocidad 9,00	Protección frente a malware y phishing, protección WiFi, Split-Tunneling, prueba de velocidad 9,00	Protección frente a malware, protección WiFi, servidores DNS propios (VyprDNS) 8,00
Notable 8,97	**Notable 8,51**	**Notable 8,50**	**Notable 8,08**	**Notable 8,02**
99,99 €	**41,36 €**	**84,37 €**	**95,88 €**	**45,00 €**

LA PRUEBA EN DETALLE

9 PROTONVPN
PRECIO/AÑO: 96,00 EUROS

El proveedor ProtonVPN valora, sobre todo, la seguridad y la confianza. Con 'Secure Core' y un Multi-Hop mejorado, los datos se transfieren de forma especialmente segura y, además, se ofrece soporte para la red Tor. Pero en la prueba de velocidad el servicio mostró debilidades que lastran su nota final en la comparativa.

10 PRIVATE IA
PRECIO/AÑO: 37,19 EUROS

PIA ofrece buenas funciones de seguridad y otros proveedores deberían tomar ejemplo de la transparencia de la estricta política 'No-Log-Policy' de este proveedor. Ahora bien, que su sede esté en los EE.UU. no es ideal para la privacidad. Y, por otro lado, el servicio también tuvo problemas de velocidad importantes.

11 PUREVPN
PRECIO/AÑO: 69,74 EUROS

La gran cantidad de servidores son un punto a favor de PureVPN, de los que hay muchos optimizados para disfrutar de contenidos en streaming de Netflix y similar. Pero el servicio no es adecuado para descargas, ya que la velocidad fue la peor de la prueba. El manejo poco claro también genera muchas dudas.

Nombre completo		PROTONVPN PLUS		PRIVATE INTERNET ACCESS		PUREVPN	
Dirección web del fabricante		protonvpn.com		www.privateinternetaccess.com		www.purevpn.com	
Sede de la empresa		Suiza		Estados Unidos		Hong Kong	
Sistemas		Windows, macOS, Linux, Android, iOS, router		Windows, macOS, Linux, Android, iOS, Chrome, Firefox, Opera		Windows, macOS, Android, iOS, Chrome, Firefox, SmartTV Android, Fire TV, PS4, Xbox, router	
Protocolos		OpenVPN, IKEv2/IPSec		WireGuard, OpenVPN		OpenVPN, IKEv2/IPSec	
RENDIMIENTO	**25,00%**		**4,20**		**3,60**		**1,60**
Retardo medio al descargar datos (durante 24h)		7,40%	6,20	16,10%	2,00	26,80%	0,00
Retardo medio al cargar datos (durante 24h)		42,00%	0,00	14,30%	2,80	41,50%	0,00
Tiempo medio de respuesta (durante 24h)		16,1 ms	9,00	15,8 ms	9,00	15,6 ms	9,20
FUNCIONALIDAD	**20,00%**		**6,60**		**9,20**		**9,80**
Número de países		54	5,40	74	8,00	140	10,00
Número de servidores		1.048	7,00	12.343	10,00	2.000	10,00
Número de dispositivos por licencia / conexiones simultáneas		5 / sí	4,00	10 / sí	9,00	10 / sí	9,00
Soporte de descarga mediante Torrent / redes Peer-to-peer		Sí	10,00	Sí	10,00	Sí	10,00
PAGOS, FIABILIDAD Y SEGURIDAD	**25,00%**		**8,60**		**7,00**		**6,20**
Protección frente a vulnerabilidades (leaks): DNS / IP / WebRTC		Sí	10,00	Sí	10,00	Sí	10,00
Funcionalidad Kill-Switch		Sí	10,00	Sí	10,00	Sí	10,00
Conexión de datos Multi-Hop		Sí	10,00	No	0,00	No	0,00
Soporte WireGuard		No	0,00	Sí	10,00	No	0,00
Proveedor fuera de alianzas '5 Eyes' / '9 Eyes' / '14 Eyes'		Sí	10,00	No	0,00	Sí	10,00
Sin registros de actividad (No-Log Policy)		No, recopila algunos datos estadísticos	8,00	Sí	10,00	No, recopila algunos datos estadísticos	8,00
Informe de transparencia o Warrant Canary		Sí	10,00	Sí	10,00	No	0,00
Métodos de pago		Tarjeta de crédito, PayPal, Bitcoin	6,00	Tarjeta de crédito, PayPal, Giropay, transferencia inmediata, Bitcoin	10,00	Tarjeta de crédito, PayPal, Giropay, Bitcoin	8,00
FUNCIONALIDAD GEOBLOCKING Y STREAMING	**20,00%**		**9,00**		**9,00**		**10,00**
Conexión con Netflix Estados Unidos		Sí	10,00	Sí	10,00	Sí	10,00
Conexión con Netflix España desde el extranjero		Sí	10,00	Sí	10,00	Sí	10,00
Servidores dedicados para streaming		No	0,00	No	0,00	Sí	10,00
Soporte geoblocking en streams en directo / mediatecas		Sí / sí	10,00	Sí / sí	10,00	Sí / sí	10,00
MANEJO	**10,00%**		**9,00**		**9,00**		**7,00**
Uso y configuración		Muy sencillo, diseño moderno de mapamundi	10,00	Sencillo, diseño plano y moderno, versión móvil simplificada	9,00	Complicado, selección del servidor más rápido solo en móvil	6,00
Funciones adicionales		Split-Tunneling, Onion over VPN	8,00	Bloqueador de publicidad, protección frente a tracking, Split-Tunneling, SOCKS5-Proxy	9,00	Bloqueador de publicidad, Split-Tunneling, protección WiFi	8,00
NOTA PARCIAL	**100,00%**		**7,22**		**7,19**		**6,61**
Corrección positiva/negativa							
CALIDAD		**Notable**	**7,22**	**Notable**	**7,19**	**Bien**	**6,61**
PRECIO		**96,00 €**		**37,19 €**		**69,74 €**	

12 AVIRA
PRECIO/AÑO: 59,95 EUROS

El experto en Antivirus Avira nos propone Phantom VPN Pro, un servicio que ha demostrado tener una buena velocidad, no comprometer nuestros datos ni tampoco limitar el número de dispositivos. Por lo demás, la cantidad de países y selección de servidores es algo baja, Netflix no funciona y la funcionalidad es reducida.

AVIRA PHANTOM VPN	
www.avira.com	
Alemania	
Windows, macOS, Android, iOS, Chrome, Firefox, Opera, Safari	
OpenVPN	
	8,70
3,70%	8,20
4,00%	8,00
12,8 ms	9,80
	5,20
38	3,40
46	0,20
Ilimitado / sí	10,00
Sí	10,00
	5,40
Sí	10,00
Sí	10,00
No	0,00
No	0,00
No	0,00
No, recopila algunos datos estadísticos	8,00
Sí	10,00
Tarjeta de crédito, PayPal	4,00
	5,00
No	0,00
No	0,00
Sí	10,00
Sí / sí	10,00
	6,00
Sencillo, diseño algo parco, versión móvil simplificada	8,00
Protección frente a malware	4,00
	6,17
Bien	**6,17**
59,95 €	

13 MULLVAD VPN
PRECIO/AÑO: 60,00 EUROS

Mullvad VPN flojea en cuanto a funcionalidad se refiere, opciones de streaming y velocidad del servicio. Una pena, porque este proveedor se toma su tarea de anonimización muy en serio y ofrece una magnífica seguridad al usuario. Además, Mullvad es el único de la prueba que no obliga a atarse a una suscripción.

MULLVAD VPN	
mullvad.net	
Suecia	
Windows, macOS, Linux, Android, iOS, router	
WireGuard, OpenVPN	
	5,40
9,50%	5,20
11,80%	4,00
14,4 ms	9,40
	5,20
36	3,20
737	4,80
5 / sí	4,00
Sí	10,00
	7,80
Sí	10,00
Sí	10,00
Sí	10,00
Sí	10,00
No	0,00
Tarjeta de crédito, PayPal, Bitcoin	6,00
	6,40
Sí	10,00
No	0,00
No	0,00
Sí / sí	10,00
	5,40
Muy sencillo, diseño sobrecargado, versión móvil simplificada	7,00
Split-Tunneling (solo con herramientas adicionales)	4,00
	6,16
Bien	**6,16**
60,00 €	

14 HMA
PRECIO/AÑO: 52,88 EUROS

Sobre el papel HMA es uno de los proveedores del tercio superior, gracias a una gran selección de ubicaciones, su política 'No-Log-Policy' y muchas funciones adicionales. Pero en la práctica HMA falla, sorprendentemente, en el Netflix americano y ha de luchar con frecuencia con incómodas interrupciones del servicio.

HMA (HIDEMYASS!)	
www.hidemyass.com	
Gran Bretaña	
Windows, macOS, Linux, Android, iOS, Chrome, Firefox, SmartTV Android, Apple TV, router	
OpenVPN, IKEv2/IPSec	
	6,80
2,40%	8,80
4,70%	7,60
49,4 ms	0,20
	8,00
190	10,00
1.100	7,40
5 / sí	4,00
Sí	10,00
	5,20
Sí	10,00
Sí	10,00
No	0,00
No	0,00
No	0,00
Sí	10,00
No	0,00
Tarjeta de crédito, PayPal, transferencia inmediata	6,00
	5,00
No	0,00
No	0,00
Sí	10,00
Sí / sí	10,00
	9,00
Sencillo, diseño sobrecargado, versión móvil simplificada	9,00
Split-Tunneling, App-Kill-Switch, selección aleatoria de IP, protección DDOS, servidores DNS propios, prueba de velocidad	9,00
	6,50
Cortes frecuentes	-1,00
Bien	**5,50**
52,88 €	

15 BITDEFENDER
PRECIO/AÑO: 29,99 EUROS

El 'Premium' del nombre no se lo merece el servicio VPN de Bitdefender porque, como mucho, es normal. No sería nada a destacar en vista del precio, si no fuera porque el servicio ha fallado de forma insalvable en las pruebas de velocidad: la conexión VPN se cayó por completo en múltiples pruebas en el laboratorio.

BITDEFENDER PREMIUM VPN	
www.bitdefender.es	
Rumanía	
Windows, macOS, Android, iOS	
Catapult Hydra	
	0,00
Cortes en la conexión	0,00
Cortes en la conexión	0,00
Cortes en la conexión	0,00
	6,00
27	2,20
1.300	8,60
5 / sí	4,00
Sí	10,00
	6,20
Sí	10,00
Sí	10,00
No	0,00
No	0,00
Sí	10,00
No, recopila algunos datos estadísticos	8,00
No	0,00
Tarjeta de crédito, PayPal, Giropay	6,00
	6,40
Sí	10,00
No	0,00
No	0,00
Sí / sí	10,00
	6,00
Sencillo, pocos ajustes, versión móvil simplificada	6,00
Protección WiFi, protección automática en P2P	6,00
	4,63
Fallos importantes	-1,64
Insuficiente	**2,99**
29,99 €	

16 KASPERSKY
PRECIO/AÑO: 20,96 EUROS

El por qué Kaspersky se esfuerza en participar en el mercado de las VPN es algo que no está muy claro, en vista de los resultados: la conexión VPN se interrumpió constantemente en las pruebas. Y, por lo demás, Kaspersky es el que ofrece el peor rendimiento de todos los proveedores de VPN de la prueba de este número.

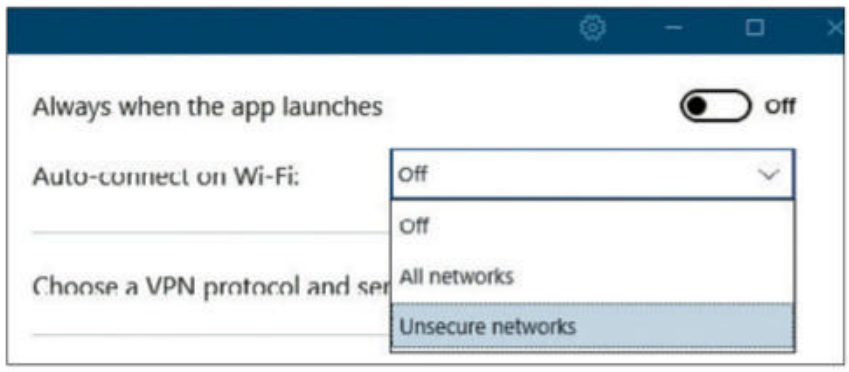
KASPERSKY SECURE CONNECTION	
www.kaspersky.es	
Rusia	
Windows, macOS, Android, iOS	
Catapult Hydra	
	0,00
Cortes en la conexión	0,00
Cortes en la conexión	0,00
Cortes en la conexión	0,00
	3,40
24	1,80
27	0,20
5 / sí	4,00
Sí	10,00
	6,20
Sí	10,00
Sí	10,00
No	0,00
No	0,00
Sí	10,00
No, recopila algunos datos estadísticos	8,00
No	0,00
Tarjeta de crédito, PayPal, Giropay, transferencia inmediata	8,00
	6,40
Sí	10,00
No	0,00
No	0,00
Sí / sí	10,00
	6,00
Sencillo, envío de datos preseleccionado	7,00
Protección WiFi	5,00
	4,11
Fallos importantes	-1,12
Insuficiente	**2,99**
20,96 €	

6 TRUCOS PARA

BLOQUEA EL MALWARE

Si al iniciar el programa por primera vez te saltaste la opción para activar ***CyberSec***, no te preocupes, puedes configurar la protección de malware ahora. Para ello, haz clic en el engranaje y luego en los ajustes del programa. Allí, ajusta la entrada ***CyberSec: block ads and malicious websites*** como ***On***.

CONFIGURA LA PROTECCIÓN WIFI Y CREA PERFILES

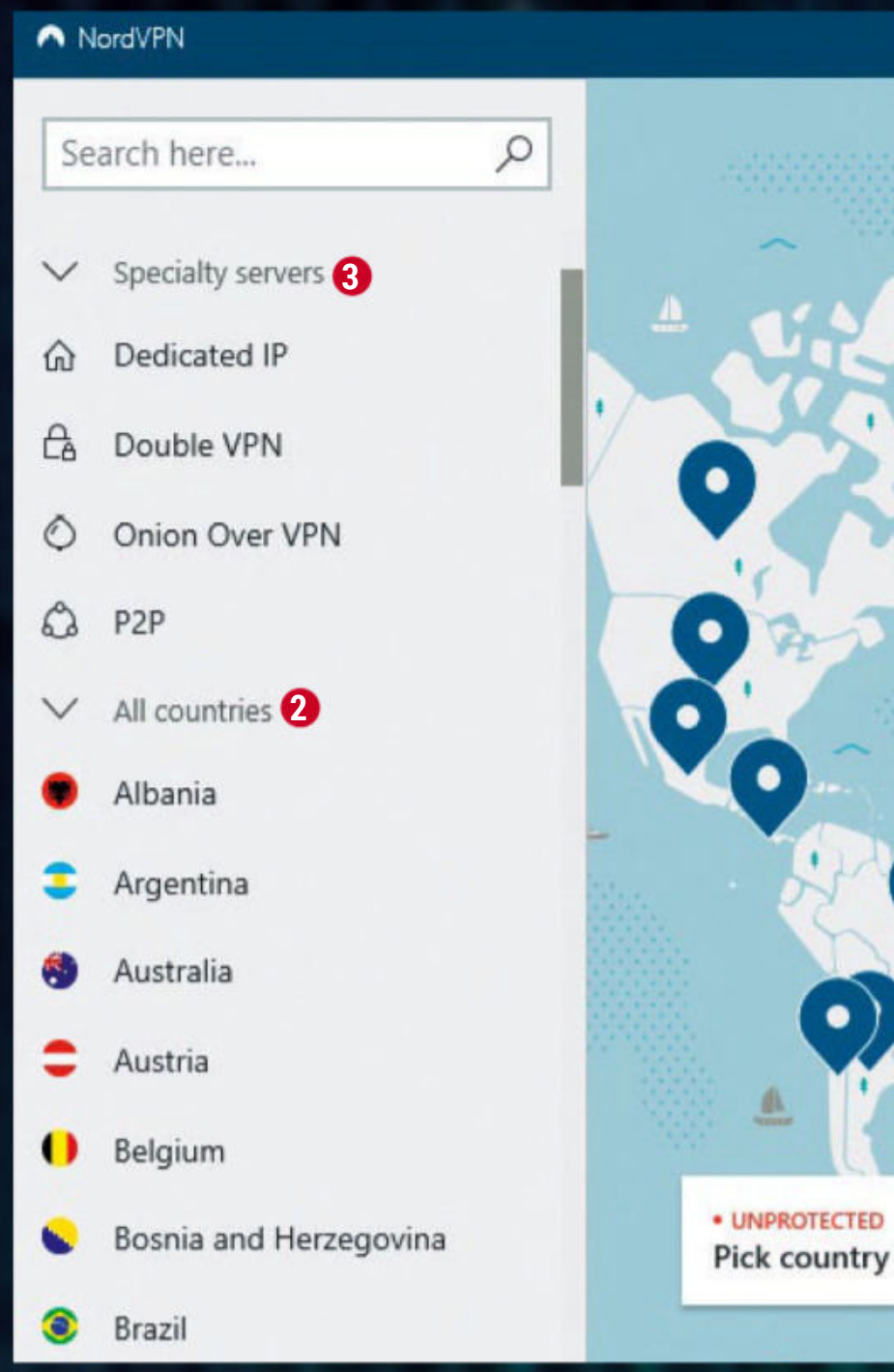


En el menú *Auto-Connect* puedes configurar el comportamiento que desees para las redes WiFi. Los ajustes del protocolo VPN permanecen en *On*.

Si eres usuario habitual de redes WiFi públicas, potencialmente inseguras, en restaurantes o hoteles, es especialmente importante que protejas tu conexión a Internet por medio de una VPN. Para ello, la aplicación NordVPN tiene un sistema automático que, no obstante, no viene activado de serie. Para configurarlo pulsa sobre el engranaje y, en el menú ***Auto-Connect on Wi-Fi,*** selecciona la entrada denominada ***Unsecure networks*** (redes inseguras); o, si quieres proteger todas las conexiones inalámbricas por WiFi, elige la opción ***All Networks***. Con esto, en cuanto abandones los ajustes con la flecha hacia atrás, se creará una conexión automática con el servidor VPN más rápido, cuando te encuentres conectado a Internet de forma inalámbrica por WiFi.

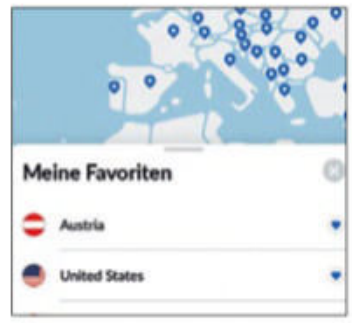
Crea perfiles WiFi

Navegar en tu red doméstica a través de la VPN no siempre tiene sentido. Por ello, NordVPN permite excluir las redes WiFi de las que te fíes. En el menú ***Auto-Connect*** selecciona ***Trust this network*** al lado de la red en la que confíes. Un clic sobre ***Remove*** la vuelve a proteger.



CREAR FAVORITOS EN iOS

Bajo el sistema operativo iOS puedes guardar los servidores frecuentes de forma más elegante que en las versiones de escritorio o Android. Al lado del país, toca sobre los tres puntos y luego en el icono del corazón. A continuación, encontrarás el país en la selección rápida de tus favoritos.



NORDVPN

La VPN perfecta se encuentra a tan solo unos clics de ratón: con estos trucos, puedes sacarle todo el provecho al servicio NordVPN.

SELECCIONA LA UBICACIÓN DEL SERVIDOR

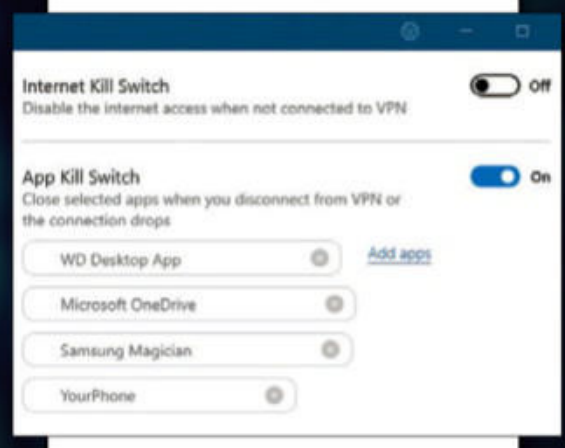
Si pulsas sobre uno de los marcadores del mapamundi, NordVPN creará una conexión de inmediato a través del país elegido. Y con la lista lateral de la izquierda tienes aún mucho más control. Ahí puedes pulsar sobre los tres puntos al lado del país, para poder seleccionar una ciudad determinada (solo disponible en algunas regiones). Con clics sobre ***Disconnect*** puedes pausar o cerrar la conexión VPN de forma rápida.

Servidores especiales

NordVPN ofrece muchos servidores especiales. Y es que, en algunas situaciones, puede ser recomendable usar uno de estos. La opción ***Dedicated IP*** está indicada para realizar compras o trámites bancarios; en el caso de que selecciones ***Double VPN*** se enviarán los datos cifrados a través de dos servidores en cascada, para dificultar aún más la identificación; con ***Onion over VPN*** el tráfico se redirigirá por la red Tor; para terminar, ***P2P*** te ofrece una protección especial al descargar ficheros desde redes peer-to-peer.

ACTIVA EL KILL-SWITCH

La función Kill-Switch, común entre este tipo de servicios, permite automatizar la desconexión inmediata de Internet cuando la conexión a través del servidor VPN se detiene y pueden verse comprometidos tus datos. NordVPN ofrece dos tipos de ajustes Kill-Switch en el menú de configuración: con ***Internet Kill Switch*** en ***On*** y ***Yes*** solo puedes conectarte a Internet si estás conectado a una VPN. Mientras tanto, si tan solo activas el ***App Kill Switch***, podrás seleccionar los programas que desees con ***Add Apps*** y ***Add*** para que estos solo se puedan conectar con Internet si la VPN está activada. De lo contrario, NordVPN cerrará el software iniciado automáticamente.

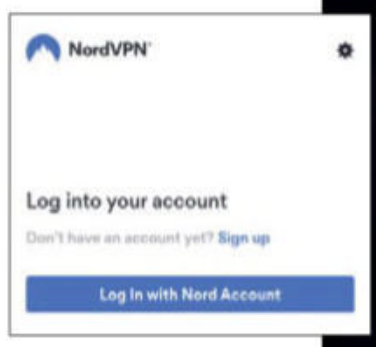


INSTALA EXTENSIONES EN TU NAVEGADOR DE INTERNET

Si no quieres proteger todas las conexiones a Internet que realizas desde tu equipo, sino solo tus excursiones con el navegador, simplemente recurre a la extensión correspondiente para Firefox, Chome y los demás.

- **Firefox:** busca la extensión ***NordVPN #1 VPN Extension*** e instálala. Antes de iniciar la extensión marca la casilla para que pueda funcionar en ventanas privadas y luego pulsa en ***Aceptar***. Tras un clic sobre el icono de NordVPN, escribe tus datos de acceso y pulsa en ***Log In***. Ahora ya tienes la extensión activada en Firefox.

- **Chrome:** añade la extensión ***NordVPN - #1 VPN Proxy Extension for Chrome*** y pulsa tres veces sobre ***Agregar***. Luego haz clic en el icono de las extensiones y en NordVPN. Tras escribir tus datos de acceso y un clic adicional sobre ***Log In,*** ya habrás configurado la extensión para Chrome.



SEGURIDAD CIBERNÉTICA

EL ENEMIGO

La clave para una seguridad cibernética eficaz reside en anticiparse allí donde sea posible y, en caso contrario, estar preparado para reaccionar con rapidez a fin de neutralizar cualquier amenaza.

Algunas de las batallas más agresivas y ofensivas que se están llevando a cabo hoy día, no están teniendo lugar sobre el terreno en algún país remoto, sino más bien entre bastidores, en los circuitos internos de nuestros sistemas de información. Los **ataques cibernéticos** se llevan a cabo de distintas formas y, además, pueden tener una **variada gama de objetivos**. "La mayor parte de los ataques cibernéticos están diseñados para robar información, en su mayoría propiedad intelectual y secretos industriales o comerciales. El robo de datos y la interrupción de la actividad empresarial representan las amenazas cibernéticas más costosas", explica Cynthia Provin, presidente de Thales eSecurity, Inc.

El impacto mediático de WannaCry en 2017

Uno de los ejemplos más recientes de infección masiva de equipos informáticos (mayo de 2017), que sonó fuerte en los medios de comunicación, fue **la amenaza WannaCry**, que afec-

O INVISIBLE

tó a gigantes tecnológicos como Telefónica o al servicio nacional de salud de Reino Unido. Estuvo en boca de todos durante varios días, pero... ¿qué es WannaCry? En pocas palabras, un ransomware que fue capaz de explorar errores de seguridad presentes en sistemas no actualizados para propagarse y afectar a miles de equipos. En cualquier caso, el ransomware no es nada nuevo. Ha habido amenazas anteriores de este tipo que también adquirieron renombre en los medios, como el famoso 'virus de la policía', CryptoLocker o TeslaCrypt. Sin embargo, lo singular de WannaCry no es que sea ransomware, sino la escala que alcanzó: se cuentan en cientos de miles de infectados.

Otro agujero de seguridad relativamente reciente en el que se vieron afectados sitios web y miles de apps, fue el conocido como **Heartbleed**, consistente en una vulnerabilidad que afectaba a la **biblioteca OpenSSL**. Lo grave de la cuestión es que OpenSSL se usa en la mayoría de servidores de Internet, por lo que se llegó a estimar que hasta dos tercios de la red podrían estar expuestos al error.

Foto: Depositphotos.com

La seguridad cibernética se está convirtiendo en un ingrediente fundamental en la planificación de los gobiernos en todo el mundo

Las empresas y la seguridad cibernética

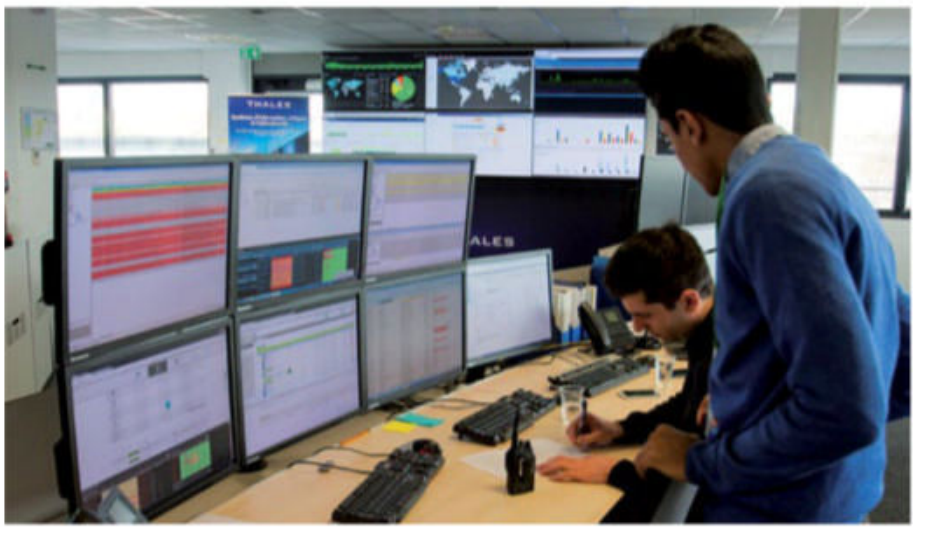
Las empresas pueden ser blanco de 'hacktivistas' o actores maliciosos cuyo objetivo es desfigurar o desactivar sitios web. Los ciberdelincuentes atacan instituciones financieras con el objetivo de **extraer información sensible** como, por ejemplo detalles de las tarjetas de crédito; y, a un nivel más sofisticado, las empresas pueden ser blanco de rivales o gobiernos extranjeros como parte de campañas de espionaje industrial.

La gama de atacantes cibernéticos se ha ampliado con el tiempo y sus motivaciones han evolucionado, de manera que existen hoy en día organizaciones más estructuradas que producen ataques más sofisticados.

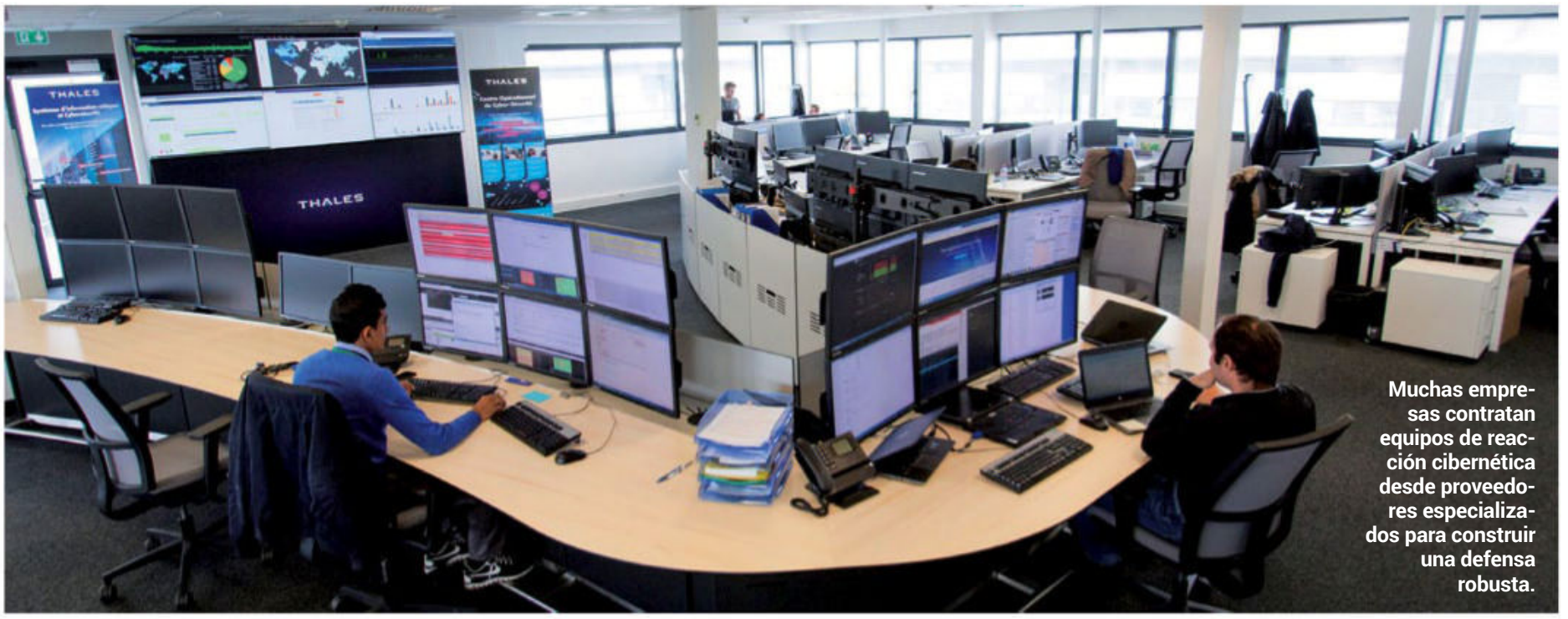
En efecto, las amenazas cibernéticas apuntan a blancos cada vez mayores, no solo empresas, sino gobiernos y ejércitos. La evolución de esta amenaza ha pasado "del cibercrimen al ciberespionaje, y de ahí al cibersabotaje, terminando por la ciberguerra", explica Daniel Ventre, del Centre National de la Recherche Scientifique de Francia. "Parece que las capacidades cibernéticas de los actores que componen el ecosistema de conflictos cibernéticos están aumentando y eso impacta en las amenazas cibernéticas en términos de violencia y volumen".

Los sistemas de autoentificación y cifrado son pilares básicos.

La mayoría de las personas y empresas son conscientes de la **necesidad de proteger sus sistemas** contra el software malicioso, aún cuando los sistemas de seguridad desplegados no son más que cortafuegos y detectores de virus. Y, según Ventre, la mayoría de los ataques puede ser



Para poder contrarrestar el efecto del adversario y mantener controlados a los atacantes, es necesario prevenir la entrada en los sistemas más críticos.



Muchas empresas contratan equipos de reacción cibernética desde proveedores especializados para construir una defensa robusta.

contrarrestados mediante **procedimientos de seguridad relativamente básicos**.

"El ochenta por ciento de los incidentes podría evitarse mediante la aplicación de sencillas reglas de seguridad: cifrado de datos y no guardar la información sensible, profesional y personal en el mismo dispositivo de almacenamiento", explica. "Sin embargo, las empresas deben tomar decisiones sobre el nivel de protección que estimen necesario según los fondos".

La seguridad de los sistemas informáticos debe cubrir, actualmente, tanto las amenazas externas como las internas

"Construir un muro virtual para prevenir la entrada de atacantes es solo la primera línea de defensa que, de por sí, tiene pocas probabilidades de mantener a raya a los atacantes más sofisticados", según Ross Parsell, director de cuentas del departamento de Gobiernos y Comercial y especialista en cibernética de Thales. Algunas empresas gastan cantidades relativamente altas de dinero en seguridad cibernética, pero enfocan una parte demasiado grande de su presupuesto a prevenir que los hackers penetren en su sistema, asegura Parsell.

"Lo primero que tienes que asumir es que los chicos malos ya están dentro o lo estarán muy rápido", explica. "Los hackers son muy rápidos a la hora de encontrar vulnerabilidades y compartir éstas en línea, y trabajan de una manera muy dinámica". Para contrarrestar este ágil adversario, las empresas deben adoptar **soluciones más integrales**. "En efecto, existen cuatro premisas", continua. "Está el extremo de la protección, es decir, muros altos y cifrado; detección, para ser proactivo y observar quién se acerca, teniendo un anillo exterior de defensa proyectado hacia fuera; un mecanismo de respuesta que pregunte, una vez que encuentre una anomalía, con qué voy a responder; y luego está el riesgo residual, sobre el que tienes que pensar, ya que los chicos malos se mueven más rápido que nosotros".

Foto: Depositphotos.com

En la actualidad, los ataques cibernéticos se llevan a cabo en una gran variedad formas y, además, pueden tener una variada gama de objetivos.

Las empresas deben aceptar la noción de que la seguridad cibernética "no versa sobre la idea de no ser atacado nunca", explica Marfaing. "Tiene que ver con la forma en que mitigas las consecuencias de un ataque a tu sistema". Describe este enfoque como una postura de defensa activa, al contrario del enfoque estático que contempla solo erigir cortafuegos. "Estás en una posición de monitorización, con sensores instalados en los elementos de tu red generando muchos datos y correlacionándolos. Ello implica un conocimiento considerable del dominio. Te alejas del mundo de la TI genérica para adentrarte en un grupo de gente profesional de naturaleza ciberreactiva".

Ciberdefensa robusta

Esto se está convirtiendo en un **área muy especializada**, hasta el punto de que muchas empresas carecen de la capacidad interna necesaria, contratando así a equipos de reacción cibernética desde proveedores especializados, para construir una defensa cibernética que resulte suficientemente robusta.

Otro servicio implica la entrega de lo que Marfaing describe como "equipos atacantes éticos". "Resulta necesario estar al tanto de las técnicas de ataque", comenta, "de manera que disponemos de equipos de atacantes éticos para realizar ensayos de

penetración. Testamos la robustez de su sistema atacándolo".

Una alta cualificación

Proveer **un nivel avanzado de protección resulta costoso** y requiere de considerables recursos humanos: el proceso de monitorización no puede automatizarse, ya que precisa de analistas humanos altamente cualificados para interpretar las tácticas e intenciones de los atacantes humanos. Ello obliga a elegir nuevamente las estrategias de defensa, comenta Parsell, quien aboga por un enfoque mediante el cual se otorguen diferentes niveles de protección a distintas partes de la red.

"Debe haber un cambio cultural respecto a qué es lo que guardas en tu red. Parte de tu información es de naturaleza crítica, y parte no. Lo que necesitas proteger es, por ejemplo, tu próxima gran invención y su propiedad intelectual".

Costes muy elevados

En la empresa privada, la inversión en seguridad puede convertirse, no obstante, en un asunto problemático. "La seguridad no es gratuita," apunta Marfaing, "y existe un intercambio entre la seguridad y la eficiencia. La seguridad viene siempre acompañada de una pérdida de eficiencia y velocidad: no es una inversión en productividad desde el punto de vista intrínseco y actualmente solo las organizaciones maduras son capaces de sopesar este equilibrio". Este intercambio se torna particularmente grave cuando las empresas privadas gestionan suministros y servicios de los que depende la sociedad, sobre todo cuando los atacantes pueden causar pérdidas considerables de vidas humanas, además de daños económicos, al penetrar en la red de infraestructuras que regulan el agua en las ciudades o los sistemas de energía, por ejemplo. Algunos gobiernos pueden llegar a sentir que hace falta legislación que fuerce a las empresas de suministro a protegerse a sí mismas mediante **sistemas de seguridad cibernética avanzados**, aunque el apoyo gubernamental podría ser suficiente para ayudar a estas empresas a contrarrestar la amenaza por iniciativa propia.

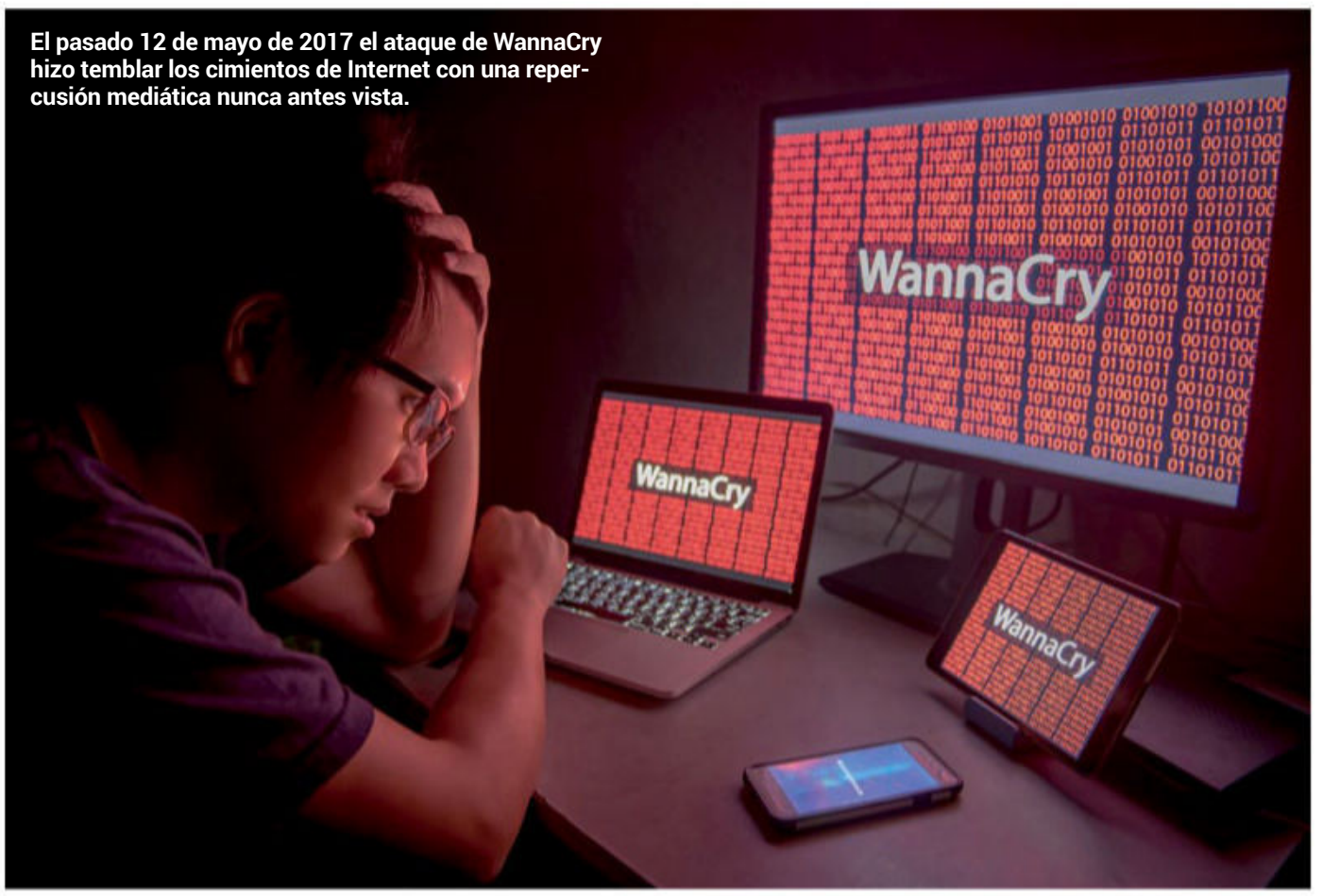
La mayoría de los expertos en seguridad cibernética están de acuerdo, no obstante, en que los gobiernos occidentales llevan la delantera al sector privado en cuanto al modo de tratar la amenaza de ataques cibernéticos con la seriedad que merece.

"Los crímenes cibernéticos contra los gobiernos van en aumento en todo el mundo" destaca Provin. "Aún cuando la mayoría del gasto público en el ámbito de defensa se reduce, la inversión en seguridad cibernética continua creciendo." No obstante, se observa un cambio de tendencia hacia la adquisición de capacidades ofensivas. "En el caso de las infraestructuras militares de comunicación, el desafío [de la defensa cibernética] sigue siendo complejo, debido a que el impacto de los ataques cibernéticos puede tener consecuencias letales", explica Ventre. "Esta es una de las razones por las que los gobiernos barajan estrategias de disuasión. La conclusión de que una seguridad cibernética realmente robusta es un objetivo no alcanzable justifica las nuevas políticas: las estrategias ofensivas se ven como un elemento disuasorio contra la violencia cibernética internacional."

La creciente competencia en la guerra cibernética está generando inevitablemente temores de que una carrera armamentística virtual está ya en marcha. ■

OTRO TIPO DE ESPIONAJE

Los robos de información a través de Internet están a la orden del día, pero no lo está tanto el espionaje electromagnético. Tu ordenador no deja de emitir todo tipo de señales que nada tienen que ver con la red de redes. Y todas ellas son susceptibles de intercepción y descifrado. De entre todas estas señales 'no digitales', destacan cuatro fuentes principales: radiación electromagnética, microvibraciones, impulsos térmicos y ultrasonidos. En el caso del teclado, cada tecla emite un pulso electromagnético característico que puede ser descifrado por un atacante en un rango de hasta 20 metros, según asegura un estudio publicado en la web **lasec.epfl.ch/ keyboard**.



El pasado 12 de mayo de 2017 el ataque de WannaCry hizo temblar los cimientos de Internet con una repercusión mediática nunca antes vista.

Foto: Depositphotos.com

CRIPTOGRAFÍA ¡NO OLVIDES T

Cabría pensar, y con cierta razón, que la criptografía es coto exclusivo de espías y gobiernos. De hecho, ha sido así durante muchos años, sin embargo todo eso ya se acabó.

Según afirma Dietmar Hilke, director de Desarrollo de Negocio y Ciberseguridad de la compañía Thales en Alemania, "En el pasado, solo las personas con autorización de acceso a los equipos de transmisión altamente sofisticados de la empresa podían dedicarse al espionaje. Por tanto, eran casos relativamente aislados. En cambio, ahora todo el mundo puede transmitir datos". Indica, "puedo ir a cualquier sitio con WiFi e intentar captar transmisiones. Por ejemplo, puedo lanzar ataques intermediarios y conseguir códigos PIN, información de tarjetas de crédito y datos bancarios, y puedo hacerlo con hardware estándar y software de código abierto que se encuentra en Internet. La amenaza ha evolucionado: ya no procede solo de un reducido grupo de expertos, sino de prácticamente cualquiera".

Para Dietmar Hilke, la digitalización de nuestras vidas implica un cambio en lo que él denomina el vector de la amenaza. Además, **no solo la transmisión de datos es vulnerable**, sino que se está utilizando software malicioso para obtener información valiosa sin que los afectados se den cuenta. La nube se utiliza para almacenar cada vez más datos en servidores de terceros: dicho de otro modo, estamos confiando nuestra información privada a sistemas de otras personas. Cuanto más conectados estamos, más vulnerables somos. "Ya no basta con proteger la información durante su transmisión. Las interacciones sociales en línea aumentan sin cesar y requieren la utilización de un cifrado de extremo a extremo", afirma Dietmar Hilke.

Criptografía y seguridad

La criptografía consiste en tomar información en formato de texto plano y cifrarla de manera que sea ininteligible. **El cifrado emplea un algoritmo de cifrado y una 'clave'** o información secreta. Los piratas pueden obtener el texto cifrado e incluso conocer el método de codificación, pero sin la clave les será imposible descifrar el código y leer el texto plano. Desde un punto de vista matemático, es como guardar un mensaje en una caja bajo llave. La dificultad radica en proteger la transmisión de la clave. Eric Garrido, jefe del equipo de criptografía de Thales Communications & Security, está especializado en el diseño y la evaluación de sistemas criptográficos. "Una cosa es tener una buena solución matemática, y otra es aplicarla con se-

TUS CLAVES!

guridad", explica. "Si el equipo o el software son malos, es como cerrar la puerta con llave y dejar una ventana abierta".

La televisión de pago constituye un caso especial: **las emisoras envían contenido cifrado a los abonados** y les proporcionan claves individuales para poder descodificarlo. La emisión transmitida es la misma, pero las claves son diferentes. Esta tecnología nació a principios de los años noventa, pero ahora necesita modernizarse, y precisamente ha sido objeto de una colaboración reciente entre la compañía Thales y la empresa suiza de medios digitales Nagra. "Todos los protocolos antiguos eran demasiado teóricos para que pudieran funcionar eficazmente en la práctica. Así pues, el objetivo era salvar esa distancia para darles una realidad práctica", explica David Pointcheval, responsable del equipo de criptografía en École normale supérieure de París, que ha participado en esta colaboración.

En la práctica, el coste del desarrollo de equipos y software es el mayor obstáculo en el diseño de sistemas eficaces de descifrado. Por ejemplo, el descodificador que se necesita para el descifrado de la televisión de pago debe ser fácil y económico de producir. Sin embargo, esto puede afectar a la calidad de la descodificación matemática y hacer que estos sistemas sean más fáciles de piratear por personas que no estén abonadas.

Ahora que tenemos cada vez más datos personales circulando por Internet, la necesidad de protegerlos es mayor que nunca

Y, cuanto más amplio sea un sistema, más probabilidades tiene de convertirse en el blanco de los piratas informáticos. Muchos sitios web y aplicaciones se jactan de ser capaces de piratear los sitios de las redes sociales como Facebook, Twitter e Instagram, poniendo en peligro nuestra vida privada. También aumenta el pirateo de blancos militares y gubernamentales.

Foto: Depositphotos.com

Con un cifrado homomórfico, los datos se envían a la nube cifrados. Los tareas se realizan con esos datos cifrados y el resultado se transmite también cifrado.

En 2010 se actualizó el programa Stuxnet, que atacaba los controladores lógicos programables (PLC) altamente precisos que sirven para controlar los parámetros de funcionamiento de ciertos sistemas industriales. Su objetivo consistía en **sabotear estos sistemas introduciendo comandos aleatorios** en las máquinas sin aparentemente levantar sospechas. Los controladores infectados se utilizaban en las centrifugadoras nucleares de Irán. Según la información que se hizo pública, el virus había provocado que un quinto de estos equipos se pararan haciéndolos girar a una velocidad superior al límite establecido. Según Dietmar Hilke, este ataque ha sido solo un pequeño anticipo de lo que nos espera. "Imaginaos un ataque contra un buque de guerra. Aunque hay muy pocas posibilidades de alcanzar el ultraprotegido sistema de mando del armamento, sí es posible acceder al sistema de regulación del motor y así tomar el mando de las turbinas para destruirlas. Pensad en la inversión que se necesita para causar unos daños así a un buque y pregun-

EL CIFRADO EN NÚMEROS

El estudio de 2015 sobre las tendencias mundiales en materia de cifrado y de gestión de claves, basado en una investigación independiente realizada por la empresa estadounidense Ponemon y patrocinada por la compañía Thales, ha revelado que el uso del cifrado no deja de aumentar en respuesta a las preocupaciones de los consumidores, los reglamentos sobre privacidad y a los ciberataques actuales. Según la encuesta, realizada en más de 4.700 empresas y responsables de informática de Estados Unidos, Reino Unido, Alemania, Francia, Australia, Japón, Brasil, Rusia, India y México:

- El 34 % utiliza mucho el cifrado.
- El 36% tiene una estrategia corporativa de cifrado.
- Casi la mitad piensa que utilizar técnicas de cifrado exime de la responsabilidad de denunciar infracciones observadas.
- Más de la mitad de los encuestados ve la gestión de claves como un obstáculo. Estas no pertenecen a la empresa, los sistemas están fragmentados y las herramientas son inadecuadas.
- Más de la mitad cree que los módulos de seguridad física son algo importante en la estrategia de gestión de las claves.
- Se cree que la principal amenaza que existe para la información son los errores de los empleados, más que los ataques.

Foto: Depositphotos.com

Las tres razones principales que impulsan la utilización del cifrado son: el cumplimiento de las obligaciones de protección de datos, la necesidad de contrarrestar amenazas de seguridad específicas y la reducción de las limitaciones asociadas a las auditorías de conformidad.

taos lo que pasaría en el caso de un misil de buque a buque", prosigue Hilke. La comparación es para echarse a temblar.

Normas de seguridad

En la actualidad, el **estándar supremo en materia de cifrado es el RSA**. Su nombre procede de las iniciales de sus tres creadores (Ron Rivest, Adi Shamir y Leonard Adleman), todos ellos profesores del Instituto Técnico de Massachusets (MIT), y esta norma, creada en 1977, se puede describir mediante la analogía siguiente: una persona envía una caja fuerte abierta a otra para que esta última deposite en ella un mensaje cifrado. La persona que ha enviado la caja fuerte es la única que tiene la llave para abrirla y leer el mensaje que contiene.

El algoritmo RSA se basa en la utilización de dos números primos grandes que, multiplicados entre sí, permiten obtener un número todavía más grande. Si tienes la clave es fácil factorizar el resultado; si no, resulta prácticamente imposible. "En la actualidad no conseguimos factorizar números compuestos de más de 600 cifras. Aunque tuviéramos ordenadores ultrapotentes, se necesitarían décadas para hacerlo", destaca David Pointcheval. ¿Es esta la solución? ¿Nuestros datos están completamente protegidos con este sistema? Por desgracia no. Aunque factorizar un número tan grande es imposible por el momento, los científicos e ingenieros están trabajando en la construcción de ordenadores cuánticos capaces de realizar cálculos de un modo completamente diferente. "Si se consigue perfeccionar un ordenador cuántico en los próximos años, todas las claves podrían quedar inutilizadas", afirma David Pointcheval. Por eso, Thales está trabajando en nuevos métodos de cifrado que resulten difíciles, si no imposibles, de descodificar hasta para los ordenadores cuánticos.

Otro de los objetivos consiste en **desarrollar lo que llamamos un 'cifrado completamente homomórfico'**, lo que Dietmar Hilke entiende por cifrado de extremo a extremo. Este tipo de cifrado permitiría garantizar la confidencialidad, manteniendo los datos codificados aun en caso de que sean procesados por un servidor remoto.

Actualmente, por mucho que cifremos los datos para transmitirlos, es necesario descodificarlos antes de poder evaluarlos. Así pues, los datos se vuelven vulnerables cada vez que se reconvierten a texto plano. Después del caso Snowden, que ha permitido comprobar el grado de intrusión por parte de ciertas agencias gubernamentales en los datos personales, la cuestión del respeto de la privacidad se ha impuesto como prioridad para las empresas de medios digitales. En este contexto, el cifrado homomórfico es el santo grial. "Un sistema homomórfico permite llevar a cabo diferentes operaciones sobre los datos cifrados sin recurrir a la de descifrado. Por ejemplo, alguien puede enviar datos cifrados a la nube. Todos los cálculos que quiera hacer se realizan con los datos cifrados, y **el resultado se transmite también de forma cifrada**. Siempre que esta persona sea la única que tiene la clave, también será la única que pueda leer el resultado. La nube nunca ve los datos no cifrados ni el resultado. Esto parece increíble, pero, con semejante característica, cualquiera podría hacer una búsqueda en Google sin que Google sepa lo que se está buscando. Es posible obtener respuestas sin que la persona a la que se pregunta sepa lo que buscáis", dice David Pointcheval.

Con todo esto, una cosa queda realmente clara: **la criptografía va a ser cada vez más importante** con el paso del tiempo. ■

Foto: Depositphotos.com

El cifrado usa un algoritmo y una 'clave' secreta. Sin la clave, nadie puede descifrar el código. Es como guardar un mensaje en una caja bajo llave.

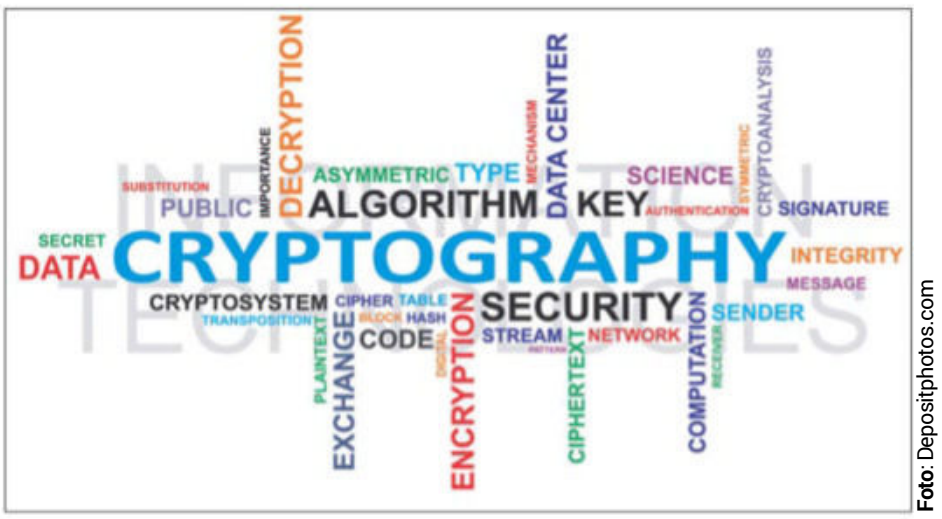


Foto: Depositphotos.com

La criptografía consiste en tomar información en formato de texto plano y cifrarla para que sea ininteligible. Cada vez es más importante en nuestras vidas.

Foto: Depositphotos.com

Un sistema más amplio tiene más posibilidades de ser el objetivo de los piratas informáticos. Y aumenta el pirateo de blancos militares y gubernamentales.

EN RESUMEN

1. Gracias a la revolución tecnológica, la transferencia de datos se ha convertido ya en una práctica muy generalizada.
2. La confidencialidad de estos datos se vuelve vital y la criptografía cobra una importancia fundamental.
3. La criptografía se tiene que adaptar permanentemente para, de este modo, contrarrestar las amenazas procedentes de cualquier parte del mundo.

AVANCE

A LA VENTA EL 3 DE SEPTIEMBRE

ESPECIAL WIFI

LA RED DOMÉSTICA PERFECTA

Los problemas con la red WiFi de tu casa pueden resultar un verdadero quebradero de cabeza. Te ponemos al día de los routers, repetidores WiFi y adaptadores PowerLine actuales, para que puedas sacarle el máximo partido a tu red inalámbrica. ¡Consigue más velocidad en tu red doméstica!

PROGRAMAS DE EDICIÓN

RETOQUE FOTOGRÁFICO

Conseguir la foto perfecta puede requerir un proceso de retoque. Probamos varios programas para lograrlo.

LUCHA DE ESTRELLAS

VALORACIONES EN AMAZON

En la lucha contra las valoraciones y reseñas falsas, Amazon, el gigante de las ventas online, promete ahora expulsar de su tienda a aquellos productos con valoraciones falsas de los usuarios. Y esto está llegando también a marcas populares...

25 AÑOS DE UN SHOOTER LEGENDARIO

DUKE NUKEM

En esta ocasión, el homenajeado es el conocido shooter Duke Nukem, que cumple 25 años en este 2021. Recordamos cómo fue la gestación de este clásico de Apogee Software, repasamos otros proyectos anteriores y posteriores de la popular saga y rememoramos a Duke, el antihéroe más malhablado de los 90.

Computer Hoy Staff

REDACCIÓN
Redactor Jefe: Carlos Gombau
Jefes de Sección: Fuencisla Mira y Tomás González
Redacción: Ana Abad y Fernando Escudero

MAQUETACIÓN:
Jefe de Maquetación: Dioni Juanas
Maquetación: Paula Cuesta
Fotografía: Depositphotos.com y Getty Images

CONTACTO REDACCIÓN
computerhoy@axelspringer.es

EDITA
axel springer

EQUIPO DIRECTIVO EJECUTIVO
Director General: Manuel del Campo Castillo
Directora Financiera y de Recursos Humanos: Rocío López
Director Comercial y Desarrollo de Ingresos: Daniel Chamorro
Director de Desarrollo Digital y Tecnología: Miguel Castillo

EQUIPO DE DIRECCIÓN
Directora de Área de Tecnología y Entretenimiento: Mila Lavín
Director de Área de Motor: Gabriel Jiménez
Directora del Área de Economía/ General News: Yovanna Blanco
Directora de Marketing: Marina Roch
Director de Arte: Abel Vaquero
Director de Vídeo: Igoe Montes

DEPARTAMENTO COMERCIAL
Sales Manager Tecnología: Estel Peris
Equipo Comercial: Beatriz Azcona, Javier Abad, Ainhoa Fernández-Checa y Valle Santos
Director Brand Content: Juan Carlos García
Brand Content: Susana Herreros y Sara González
Responsable de Operaciones: Jessica Jaime

SOCIAL MEDIA MANAGER
Nerea Nieto

SISTEMAS / IT
Director de Sistemas: José Ángel González

ADMINISTRACIÓN:
Jefa de Administración: Pilar Sanz
Bancos y proveedores: Cristina Nieto

Axel Springer España S.A.
Edif. Talent Garden. C/ Juan de Mariana 15
28045, Madrid
Tel. +34 915 140 600

CONTACTO PUBLICIDAD
publicidadaxel@axelspringer.es

CONTACTO SUSCRIPCIONES:
Tel. +34 915 140 600
suscripciones@axelspringer.es

CONTACTO MARKETING
marketing@axelspringer.es

DISTRIBUCIÓN EN ESPAÑA E HISPANOAMÉRICA
SGEL. Tel. +34 915 140 600

DISTRIBUCIÓN EN PORTUGAL
Urbano Press. Tel. +351 211 544 246

TRANSPORTE
Boyaca. Tel. +34 917 478 800

IMPRIME
ROTOCOBRHI. Tel. 918 031 676
Printed in Spain.
Depósito Legal M-37952-1998

Revista miembro de ARI

Computer Hoy

SÚPER OFERTA DE SUSCRIPCIÓN

26 NÚMEROS de Computer Hoy

1 año Edición en papel + edición digital (77,74€)

+

ESET Internet Security®

(44,95€)

~~Total: 122,69€~~

POR SÓLO

55€

AL AÑO Sin gastos de envío

Protección para banca online y pagos por Internet

Detección de páginas fraudulentas

Protección de la Webcam

El suscriptor recibirá su código de instalación por correo electrónico. Licencia 1 dispositivo / 1 año

Puedes suscribirte por cualquiera de estos canales:

En **http://store.axelspringer.es/tecnologia/revistas-tecnologia/computer-hoy/suscripcion-computer-hoy**

Por teléfono **915 140 600 /** Por email: **suscripciones@axelspringer.es**

Cada suscriptor tendrá acceso gratuito a la edición digital de Computer Hoy en Kiosko y Mas. Accesible desde PC, smartphones y tablets, con sistemas Windows 8, iOS y Android

UN DOCUMENTAL DE LA FUNDACIÓN JUEGATERAPIA CON LA COLABORACIÓN DE ALEJANDRO SANZ

En la soledad de una habitación de hospital, una videoconsola se convierte en una potente ayuda para que los niños ingresados sonrían, levanten la cabeza y descubran sus ganas de ganar. Cada partida jugada es una partida ganada si logra que el día pase sin dolor y sin miedo. Desde la Fundación Juegaterapia llevamos 11 años trabajando para demostrar que el juego predispone positivamente a los niños en su curación. Gracias al Dr. Mario Alonso Puig y al equipo médico del Hospital La Paz de Madrid, hemos podido demostrarlo científicamente. La voz de Alejandro Sanz, padrino de la Fundación, es el hilo conductor de esta bonita historia de amor a la vida y férrea lucha contra el cáncer infantil.

fundación juegaterapia

La Quimio Jugando se pasa Volando...

Disponible en:

FILMIN | prime video