"ALEXA, OLVIDA TODO LO QUE SABES DE MÍ"

ACCEDE AL INFORME
EN NUESTRA EDICION DIGITAL

Son notorios los continuos escándalos por las brechas de privacidad de Facebook, cuyo cénit llegó con el caso Cambridge Analytica, que utilizó los datos de 87 millones de usuarios de la red social en campañas de *marketing* político; o la millonaria multa a YouTube por recoger información personal de niños con fines publicitarios sin el consentimiento de sus padres. Estos son solo algunos de los casos que más relevancia mediática han obtenido en los últimos meses, y que han situado en el punto de mira la privacidad de los usuarios en el entorno digital.

TEXTO **MARÍA JESÚS PÉREZ FUENTES** | ILUSTRACIÓN **ISTOCK**

Y lo que se vislumbra apenas es la punta del iceberg, porque cada día se ponen en marcha en todo el mundo numerosos contenciosos legales con motivo de la aparición de brechas de seguridad en los dispositivos móviles, apps o tecnologías *wearable* que, de todos es sabido, poseen mecanismos predeterminados para recopilar datos personales de los usuarios que las utilizan.

Lo que debería preocuparnos es el uso concreto que se hace de esos datos. Cada vez más, y sobre todo a raíz de los casos mencionados anteriormente, los usuarios somos más sensibles al uso que se hace de la información personal que proveemos a estas compañías, y se exigen más garantías de que esos datos no sean vendidos, utilizados o compartidos con terceros con fines poco éticos.

Es innegable que cada vez existe una mayor conciencia social sobre estos temas y la convicción de que la privacidad del usuario debería ser un aspecto primordial desde los inicios del desarrollo de una aplicación o dispositivo. Sin embargo, parte del problema reside en que las empresas se apresuran a lanzar su producto con el objetivo de conseguir la mayor cuota de mercado y vencer en la carrera a la competencia. Como consecuencia, al reducir el tiempo de desarrollo del producto, se favorece el aumento de la vulnerabilidad frente a las amenazas externas y, una vez que se ha lanzado, es realmente complicado corregir estos problemas o aplicar parches de seguridad.

"EL INFORME DE RIESGOS MUNDIALES 2020, ELABORADO POR EL FORO ECONÓMICO MUNDIAL, REVELA QUE **ENTRE LAS CINCO PRINCIPALES PREOCUPACIONES A NIVEL MUNDIAL SE ENCUENTRAN AQUELLAS RELACIONADAS CON LOS ATAQUES CIBERNÉTICOS"**

Pero no es cuestión de alarmarse. Quizás no podamos tener el control total del uso que se hace de nuestra información, pero sí podemos aplicar ciertos filtros para definir hasta qué punto las empresas lo sabrán todo de nosotros. A continuación te damos una serie de recomendaciones básicas, cuyo punto de partida es el uso del sentido común.

EN TU SMARTPHONE

Mantén siempre actualizado el sistema operativo de tu móvil. La mayoría de los dispositivos ya avisan automáticamente de las actualizaciones periódicas, aunque conviene realizar a mano la configuración de las opciones de privacidad.

Evita conectarte a wifi públicas. Sabemos que es tentador conectarse a una red gratuita, pero si lo haces estarás exponiendo tu identidad y dando acceso a tu dispositivo. Si no te queda más remedio que utilizar una wifi pública, utiliza una red privada virtual (VPN), preferiblemente de pago.

Instala solamente aplicaciones que provengan de una fuente oficial. Descargar e instalar apps de otras fuentes puede causar problemas en el dispositivo y dejar una puerta abierta a distintos tipos de malware.

Además, cuando te instales una aplicación, **presta mucha atención a los permisos que se te solicita aceptar.** Por ejemplo, si al instalar un traductor de idiomas se te solicita acceder a tus contactos, localización o cámara, pregúntate si es lógico. Si no lo es, esa app debería levantar tus sospechas.

Crea contraseñas fuertes. Evita usar la misma contraseña para varias aplicaciones. También es recomendable que cambies tus datos de acceso con frecuencia. Utiliza cadenas aleatorias de números, mayúsculas y símbolos, y si te sientes poco creativo, te recomendamos el uso de plataformas como **LastPass** o **1Password,** que crearán y recordarán todas tus contraseñas por ti.

EN TU **SMART TV**

A menudo olvidamos que estos televisores también tienen conexión a Internet y que por tanto, **conviene que seas precavido y configures tus opciones de seguridad.**

Todos los grandes fabricantes guardan un registro de comportamiento del usuario, de reconocimiento de imágenes o de voz, y que se justifica con la intención de ofrecer en un futuro una mejor experiencia de uso y generar mejoras en sus productos. Si no te encuentras cómodo con esta situación, decide qué información quieres compartir modificando las opciones de datos para diagnóstico. El lugar donde encontrarlo varía dependiendo de la marca y modelo del televisor, pero se suele encontrar en los apartados de Configuración y/o Privacidad.

EL **76%** DE LOS ENCUESTADOS OPINA QUE ESTE AÑO **AUMENTARÁN LOS CIBERATAQUES**

Y EL **69%** OPINA LO MISMO ACERCA DE LA **PÉRDIDA DE PRIVACIDAD ANTE LAS COMPAÑÍAS**

MÁS DEL **50%** DE LA **POBLACIÓN MUNDIAL** ESTÁ **CONECTADA A INTERNET.** APROXIMADAMENTE UN MILLÓN SE CONECTAN CADA DÍA POR PRIMERA VEZ. **DOS TERCIOS DE LA POBLACIÓN MUNDIAL POSEEN UN DISPOSITIVO MÓVIL**

TU ASISTENTE **DE VOZ**

Siri, Cortana, Alexa o Google Assistant ya son uno más entre nosotros, resultan de gran utilidad y nos hacen la vida más sencilla. No solo pueden responder preguntas o reproducir música, sino también controlar dispositivos inteligentes que sean compatibles con el sistema, como cámaras de videovigilancia. Sin embargo, cada vez que Alexa elige una canción para ti, o cuando controlas tus dispositivos de hogar con el comando de voz, **el sistema está almacenando una valiosa información sobre ti.**

Por eso, desde su lanzamiento en 2014, el asistente de voz de Amazon se ha situado en el centro de la controversia ante el

temor a que estos dispositivos graben las conversaciones privadas, las almacenen y analicen.

Pero, **Amazon no es la única que se enfrenta a estas acusaciones sobre la escucha permanente.** Google, Apple, Facebook o Microsoft también han admitido haber escuchado grabaciones realizadas con asistentes de voz inteligentes. Como consecuencia, estas compañías han lanzado al mercado modelos con mejoras en la configuración de la privacidad. Por ejemplo, los nuevos modelos de Echo (Amazon) ya incluyen varias capas de controles de privacidad, como un botón que desconecta el sistema de escucha. Incluso es posible poner límites a Alexa pronunciando frases como "borra lo que he dicho hoy" o "borra lo que acabo de decir". La compañía ha llegado a anunciar que estas características de privacidad también se incluirán en otros *gadgets* y *wearables* que Amazon tiene previsto lanzar próximamente.

Recuerda que en todos los dispositivos encontrarás una opción, como Ajustes o Mi Actividad, donde **podrás comprobar qué datos han sido recopilados,** con la posibilidad, en la mayoría de casos, de eliminarlos por completo.

TU PULSERA INTELIGENTE

El uso de la tecnología ponible o *wearable* conlleva algunos riesgos de seguridad inherentes, con el agravante de que **parte de la información almacenada por estos sistemas son relativos a la salud del usuario.**

Recientemente el anuncio de Google de que compraría Fitbit, llevó a que muchos usuarios expresaran su repulsa y se pasaran a la competencia, Apple Watch, todo pese a que Fitbit anunció que no vendería a Google los datos de sus 28 millones de usuarios ni los utilizaría para fines comerciales.

De momento los dispositivos portátiles de salud y los relojes inteligentes no se han visto implicados en ningún gran litigio relacionado con la privacidad, por lo que no existe constancia de protestas públicas sobre los riesgos de su uso.

Sin embargo, hay algunos casos que sí han salido a la luz por lo curioso de su naturaleza y por el debate que se abre ante la posibilidad de usar la información almacenada en estos gadgets como prueba en la detección de fraudes a las aseguradoras.

Dado que esta tecnología *wearable* seguirá sumando popularidad en los próximos años, es recomendable que nos acostumbremos a escoger **qué datos sobre nuestro estado físico o geolocalización queremos compartir con los demás.**

Debido al déficit actual de gobernanza tecnológica y de un marco común de regulación, seguirán existiendo riesgos inherentes de seguridad y privacidad relacionados con el Internet de las Cosas (IoT). Mientras tanto, depende de nosotros qué queremos compartir en un mundo cada vez más conectado y, sobre todo, qué riesgos estamos dispuestos a asumir.