# Privacidad y seguridad digital: es posible

**Por: Enrique Amestoy. 23/03/2022**

Uno de los aspectos más importantes a cuidar en el uso de computadoras, celulares, dispositivos electrónicos e internet en general es el de la privacidad. Existen conductas y herramientas que nos permiten minimizar el riesgo de que nuestros datos queden expuestos. Contraseñas seguras, navegadores web y sistemas de mensajería alternativos, nos asegurarán estar a salvo de quienes se ocupan de sacar provecho de nuestra información.

Algunas empresas utilizan nuestros datos personales como parte de su modelo de negocios, para ganar dinero prediciendo nuestros comportamientos. ¿Qué le gusta comer? ¿Qué quiere comprar? ¿A quién quiere votar? ¿Qué necesitan sus hijos?, son interrogantes que han logrado convencer a la mayoría de los usuarios. Muchos razonan: “no tengo nada para ocultar”, “¿qué cosa de mí, que no soy nadie, les puede interesar?”.

De esa forma las empresas logran que estemos publicando el minuto a minuto de nuestra vida en redes sociales digitales: me desperté, estoy cansado, voy a desayunar, me gustan las tostadas, tomaré un taxi, foto con mis compañeros de la oficina, estamos en casa con nuestros hijos y el gato. Se pueden pensar millones de variantes.

Para comenzar a entender lo importante de la privacidad y el cuidado de nuestros datos personales, debemos saber de qué estamos hablando. Los datos personales son -entre otros- edad, sexo, gustos, costumbres, integración de la familia, lazos afectivos o cualquier otro dato que sea capaz de identificarnos. Respecto a la pregunta “¿qué puede interesarles de mí?”: alcanza con pensar cuántos clics hemos dado en publicidad en productos de Meta o Google (Instagram, Facebook, buscador de Google, Youtube) para enterarnos que, por cada uno de esos clics, hubo una empresa que pagó una fracción de dólar a quien nos la mostró.

Lo mismo si para utilizar una aplicación hemos tenido que visualizar un pequeño video o publicidad de algún patrocinador. También es bueno pensar si alguna de esas publicidades nos llevó a comprar un producto o servicio: en ese caso, habrán

logrado el objetivo de hacernos parte del modelo de negocio basado en datos personales.

Sin embargo, también podemos pensar en asuntos relacionados con el delito: ¿alguna vez llegaron a su estado de cuenta compras o retiros que usted no ha hecho? ¿Conoce al menos un caso de alguien a quien eso le haya sucedido? Bien: generalmente en estos casos hablamos de un delito denominado “phishing”; que básicamente se trata de un método que permite obtener contraseñas o números de tarjetas de débito o crédito de forma no autorizada.

Podemos pensar en riesgos aún más complejos como pueden ser el “cyberbulling” -o acoso por medios digitales-, el “grooming” -o acoso sexual a una persona menor edad en redes sociales, juegos o foros. También el “sexting” -envío de contenido erótico o sexual por medios digitales- que si bien puede no tener que ver con asuntos como la llamada “pornovenganza” o publicación de contenidos eróticos sin consentimiento, el solo hecho de conservar esos archivos guardados en nuestros dispositivos implica un riesgo muy grande para nuestra privacidad.

**Primeros pasos**

Hay elementos que nos permiten estar más seguros y con nuestros datos personales más protegidos en el mundo digital. En primer lugar, el uso de sistemas operativos actualizados a sus últimas versiones o parches de seguridad. Lo mismo con los antivirus. Un sistema operativo obsoleto contiene agujeros de seguridad que son explotados generalmente por software que denominamos “malware”, con el objetivo de cometer algún tipo de delitos similar a los mencionados anteriormente. El uso de Software Libre -desde el sistema operativo hasta la última de las aplicaciones- es el camino ideal para empezar a protegernos.

Cambiar Microsoft Windows por GNU-Linux (Debian, Arch, Ubuntu, Linux Mint o tantos otros) sería un paso enorme en este sentido. En los dispositivos móviles, por su parte, hay una excelente alternativa llamada LineageOS, si lo que queremos es cambiar el sistema operativo Android.

Es recomendable, sin dudas, que el cambio del sistema operativo sea realizado por técnicos. Pero también hay mucho material en internet para leer y hacerlo uno mismo. Si, fácilmente podemos cambiarnos de Microsoft Office a LibreOffice (que corre tanto en Linux como en Windows); o de Adobe Photoshop a Gimp (también en

Linux o Windows). Pero es necesario tener en cuenta que “gratis” o “pirateado” no es lo mismo que “libre”. Si descarga software gratis o freeware, o si instala software pirata, es altamente probable que junto con ese software vengan instalados programas malware, sistemas espías o de rastreo.

**Ábrete sésamo**

Sin importar el sistema operativo que utilicemos (Windows, Linux, Android, IOs) es fundamental utilizar contraseñas seguras, cambiarlas periódicamente y no utilizar la misma para todas las aplicaciones. Una contraseña mínimamente segura debería incluir letras, números, mayúsculas, minúsculas y símbolos, y tener una extensión de no menos de 8 caracteres. Por ejemplo: Cu3nt4_@ es una contraseña segura.

Algo que podemos poner en práctica para no tener que recordar decenas de contraseñas es utilizar un patrón común, “Cu3nt4_@”, por ejemplo; y agregar algo más que lo asocie con el uso que le estemos dando. Así por ejemplo podríamos tener para el banco “Cu3nt4_@BancO”, para el correo “Cu3nt4_@3maiL” y para Twitter Cu3nt4_@Tw1tt3r”. Es decir, un patrón común y luego otra parte de la contraseña que se genera por asociación con la aplicación que estemos utilizando.

En el caso de los dispositivos móviles, no es recomendable utilizar reconocimiento facial o el patrón, pues estos métodos tienen seguridad baja. Si el dispositivo lo permite, la huella digital es la que cuenta con mayor seguridad. Si utilizamos un PIN, tratemos de que no sean el cásico “1111” o “1234”. Lo mismo vale para las contraseñas: existen investigaciones que demuestran que “12345678” o “password” son de las más usadas en el mundo. Tampoco habría que utilizar en las contraseñas números que se asocien directamente con una identidad: como la fecha de nacimiento, el nombre, el número de cédula, etc.

Y recordar también que la clave del Wi-Fi de una casa o una oficina también es una contraseña, y debe cumplir con los mismos parámetros que aquí estamos planteando. Respecto al WiFi –de paso- lo ideal sería evitar utilizar datos sensibles cuando se hace uso de redes públicas (aeropuerto, plazas, transporte, etc). Se trata de espacios ideales para violar la privacidad. Por ello, mientras una persona se encuentre conectada a una red pública (por razones de estricta necesidad, pongamos por caso) no se aconseja que acceda a la cuenta bancaria o intercambie datos privados.

## ¿Qué buscás?

Un dato: el buscador de Google es el que menos cuida nuestra privacidad y el que recopila mayor cantidad de información personal. Tanto en la computadora como en el dispositivo móvil, quizás lo mejor sería cambiarlo por DuckDuckGo o StartPage: ambos cumplen el objetivo de la búsqueda sin que debamos pagarle con nuestros datos. También ayudaría utilizar Brave o Firefox, como navegadores, tanto sea en la computadora como en el dispositivo móvil. Al navegador mínimamente deberíamos agregarle un plugin (herramientas complementarias que agregan funciones a un programa) que ayude a bloquear ventanas emergentes de publicidad no deseada, phishing y malware en general. Una buena opción es el plugin uBlock Origin.

En todos los casos el uso de la “navegación segura” -que los navegadores actuales posee- nos da un plus de seguridad. Si queremos ir un poco más allá en materia de privacidad,  podemos utilizar el navegador Tor que, además de no almacenar datos personales, navega a través de distintos puntos y de esa forma también protege nuestra dirección IP del rastreo con fines comerciales o delictivos.

En todos los casos jamás debemos poner datos personales o contraseñas en sitios que no utilicen el protocolo seguro HTTPS (identificado con un candado al lado del nombre del sitio). Tampoco es aconsejable enviar contraseñas por herramientas de mensajería como Whatsapp, ya que pueden ser capturadas y utilizadas por terceros. Es recomendable la utilización de herramientas de mensajería que cuiden nuestra privacidad. Para ello cambiar a Telegram es un gran paso, e ir hacia Signal sería lo ideal. Los mapas de Google pueden ser sustituidos por OpenStreetMap o en la versión móvil por OsmAnd~ en Android.

En el caso del correo electrónico, siempre está la “tentadora” oferta de los 15Gb gratis de Google. Usar Gmail asegura un cliente del correo (en la computadora y móviles) así como en otras herramientas como la edición de documentos online con Google Docs. Se ofrece almacenar documentos como fotos u otros archivos en la nube, que no es otra cosa que los discos duros de Google. Pienso, categóricamente, que cuando el producto es “gratis” es porque el producto es usted y sus datos personales.

Una muy buena alternativa de correo en Uruguay es el que provee ANTEL: los que antes conocíamos como @adinet.com.uy y que hoy día se convirtieron en

@vera.com.uy. Es seguro, sus servidores alojados en territorio nacional, cumple con el cometido, se accede desde un navegador o cualquier herramienta para leer correo que instale en su computadora (Mozilla Thunderbird es una de las mejores) o dispositivo móvil (K9-Mail entiendo es una muy buena opción para Android).

Si buscamos aún más seguridad sugiero ir por el lado de ProtonMail, una herramienta de correo electrónico que pone el énfasis en el cifrado y la seguridad. Proton también tiene una opción de VPN (una forma de anonimizar nuestro tráfico en la web) llamada ProtonVPN. Otra excelente opción es Disroot, que ofrece correo electrónico encriptado y seguro, block de notas compartido, foros, alojamiento temporal de archivos para compartir o almacenamiento en la nube con NextCloud (otro servicio para almacenar archivos).

Usted mismo puede instalar su propia nube Nextcloud en su computadora, o un VPS (Virtual Private Server) que puede conseguirse por una pequeña mensualidad. Nextcloud es la opción para sustituir Google Drive, Dropbox y otras.  En general, los servicios más populares de Google pueden sustituirse por alternativas más seguras. Puede cambiar –por ejemplo- las reuniones virtuales a Jitsi Meet, en lugar de Google Meet o Zoom. Tendrá de ese modo una herramienta de software libre que, además de cuidar su privacidad, no le pondrá límites, tarifas, etc. Puede usarse en el navegador o descargar la aplicación en su dispositivo móvil. También puede agregarse como un plugin de NextCloud, si es que ha decidido tener su nube privada segura.

**Estáte atento**

Respecto a las redes sociales digitales hay algunos aspectos importantes a cuidar. Debemos tener en cuenta que una vez que algo se sube a internet, allí se queda (ya sea en los discos duros de Meta, Google o Twitter) aun cuando los eliminemos. También los datos quedan, alojados en lo que denominamos “caché” de Google o en otros espacios como el sitio www.archive.org.

Por ello se insiste con la idea de pensar antes de publicar datos personales. Cuando hablamos de datos personales me refiero a los que comentaba al comienzo del artículo: documento de identidad, cuenta bancaria, cualquier fotografía donde aparezca usted, su familia o amigos, etc.

La herramienta “bonita” que tiene Facebook de identificar rostros en fotos y etiquetar

a las personas es una sofisticada herramienta de control y reconocimiento, que sumado a otras formas de reconocimiento facial pueden colectar datos altamente valiosos.

Las aplicaciones “inofensivas” como FaceApp que nos muestran cómo será nuestro rostro dentro de algunos años, o como éramos cuando más pequeños, no son más que instrumentos para afinar las herramientas de inteligencia artificial que reconocen rostros y les harán más fácil reconocernos dentro de algunos años. (Pequeño paréntesis: “Coded Bias” -o “Sesgo Codificado” en español- es una muy buena película para entender sobre algoritmos de identificación facial. “The Great Hack” -o “El gran hackeo”- es un documental muy bueno para comprender sobre datos personales y su uso por parte de corporaciones con fines comerciales y políticos. “The Social Dilemma” -o “El dilema de las redes sociales”- es otro interesante material donde encontrar información sobre privacidad en internet. Las encuentra en plataformas de streaming).

En Uruguay contamos con una muy buena ley de datos personales. La Ley 18.331 de Protección de Datos Personales y acción de “Habeas Data” es muy abarcativa y es posible llevar cada uno de sus artículos al espacio digital. Algo que también debemos cuidar en redes sociales es el uso que las y los menores de edad hace de ellas. Pero sobre todo, lo que hacemos los adultos e involucra a menores de edad, como es el caso de la publicación de fotografías.

Esas fotos, que no se borrarán jamás de internet, pueden convertirse en un problema en la vida adulta, o directamente un peligro enorme si pensamos que la pornografía infantil es uno de los delitos que más dinero mueve en la web y por ello existen cientos de herramientas de malware para captar el material y comercializarlo en sitios prohibidos. Abrir cuentas en Facebook, Instagram o TikTok para menores de edad no está dentro de las cosas aconsejables. ¡Tampoco prohibir! Es importante que sepamos donde están los más chicos cuando navegan en el mundo virtual. Con quienes se relacionan, cuáles son los espacios de vinculación (juegos en línea, chats, etc); de la misma forma que pretendemos saber si están en la plaza o la escuela.

Resulta complejo proponer una alternativa a cada una de las herramientas que hoy día usted utiliza. Investigue antes de instalar, sabiendo que no todo lo que se encuentra en internet es verdad. A modo de ejemplo: la israelí Kape Technologies, empresa propietaria de ExpressVPN, también es propietaria de las otras tres o

cuatro mejores VPN’s del mercado. Al menos eso dicen decenas de sitios especializados en la materia. Sin embargo hay algo no nos dicen: Kape también es la dueña de los sitios especializados que nos sugieren cual es la mejor.

Pongamos el foco en la importancia de cuidar nuestra privacidad, saber qué hace la empresa proveedora de la herramienta con nuestros datos y los eventuales riesgos en el mundo digital. Leer los términos y condiciones o los acuerdos de servicio de las aplicaciones, por tedioso que parezca, nos llevará a elegir con mayor seguridad. Siempre –o en lo posible- busquemos herramientas de software libre y aquellas que en sus condiciones expresamente indican que no hacen uso de datos personales con fines comerciales. Intente siempre asesorarse con especialistas de confianza y ante la duda, elija no instalar un programa o aplicación. Una vida digital más segura y privada es posible.

**** Socio de la primera Cooperativa de Tecnologías Libres en Uruguay Libre.Coop. Fundador del Centro de Estudios de Software Libre Uruguay (CESoL) y la Red Iberoamericana de SL (RISOL). Ex asesor en TIC del MRREE de Uruguay y miembro del Consejo Asesor Honorario de Seguridad AGESIC. Colaborador del Centro Latinoamericano de Análisis Estratégico (CLAE)***

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: Nodal

**Fecha de creación**
2022/03/23