

Ciberseguridad al alcance de todos: cómo proteger tu vida digital

.....
| Por la traductora pública Valeria Cecilia Esterzon,
secretaria de la Comisión de Recursos Tecnológicos

La era digital en la que estamos inmersos nos ofrece múltiples posibilidades y comodidades gracias a la comunicación y la tecnología, pero al mismo tiempo nos enfrenta a un universo virtual repleto de retos y riesgos. Cada vez que los usuarios interactúan en línea, hacen clic o descargan un archivo, se pone en riesgo su privacidad. Así, debemos ser extremadamente precavidos ante esta situación. En esta nota, adquiriremos habilidades para navegar por internet con seguridad y confianza.

Creación de contraseñas seguras

Las contraseñas son como llaves de seguridad que resguardan nuestra información más confidencial, que abarca desde correos electrónicos y cuentas bancarias hasta perfiles en redes sociales y archivos personales. No obstante, a pesar de su relevancia, en ocasiones quedan en un segundo plano.

¿Qué debemos tener en cuenta al seleccionar nuestras contraseñas? Por ejemplo:

- Crear contraseñas fáciles de recordar y difíciles de adivinar. Una opción puede ser usar frases en lugar de palabras sueltas.
- Definir contraseñas utilizando ocho caracteres como mínimo y combinar mayúsculas, minúsculas, números y caracteres especiales.
- No incluir datos personales, datos fácilmente deducibles o secuencias de números o letras.
- No escribirlas ni dejarlas accesibles a otras personas, y modificarlas si existe alguna sospecha de robo.
- Cambiarlas periódicamente, aun cuando no se nos solicite hacerlo.
- No usar la misma contraseña para todas las aplicaciones.

Cómo inventar o recordar contraseñas

Si nos cuesta inventarlas o recordarlas, podemos usar un gestor de contraseñas, es decir, una herramienta que las almacena y organiza de forma segura todas juntas en un solo lugar. Permite crear contraseñas fuertes y únicas para cada cuenta sin necesidad de recordar todas, ya que solo se debe memorizar una contraseña maestra. Las opciones incluyen, entre otras, LastPass (<https://www.lastpass.com/es>), que es gratuita para la mayoría de las funciones esenciales; 1Password (<https://www.1password.com>), que se destaca especialmente entre los usuarios de macOS e iOS y es de pago en dólares; Bitwarden (<https://bitwarden.com>), que tiene una opción gratuita y una de pago. Usar un gestor de este tipo ayuda a mejorar la seguridad en línea y reduce el riesgo de reutilizar las contraseñas o perder el acceso a las cuentas.



Correo electrónico

Los correos electrónicos, no importa cuál tengamos, guardan una gran cantidad de información personal, aunque muchas veces no nos demos cuenta. Los traductores, en especial, manejamos mucha información confidencial de nuestros clientes y, en la mayoría de los casos, por ese medio recibimos los documentos para traducir. Además, es uno de los medios preferidos en la actualidad para generar estafas. Por lo tanto, no podemos pasar por alto su importancia a la hora de protegernos.

Estas son algunas recomendaciones básicas:

- Borrar los correos electrónicos de procedencia dudosa y, si se leyeron, no abrir nunca los archivos adjuntos ni acceder a los enlaces que contengan.
- No responder cadenas de correo ni reenviar *spam*.
- Tener cuidado incluso con los correos provenientes de personas conocidas. Si el asunto del correo no concuerda con lo que habitualmente envía ese remitente, no abrirlo y, si se abrió, no responderlo.
- Si recibimos un correo de un banco o alguna empresa, corroborar el correo electrónico del remitente letra por letra para detectar alguna diferencia con el oficial, porque las estafas suelen provenir de correos muy similares a los ya conocidos por el usuario.

Resguardo de la información

Es crucial hacer copias de seguridad periódicas de los datos importantes, para asegurar su protección en caso de cualquier contratiempo. Lo ideal es guardar estas copias en un dispositivo externo, como un disco duro externo o una unidad USB, o utilizar servicios de almacenamiento en la nube que ofrezcan una capa adicional de seguridad. Algunos ejemplos son Google Drive, Dropbox, Microsoft OneDrive, iCloud Drive, entre otros. La frecuencia con la que es conveniente hacer estas copias de seguridad puede variar según la cantidad de datos que se generen y su importancia, pero, en general,



se recomienda hacerlas al menos una vez a la semana. Estas medidas protegen al usuario frente a la pérdida de datos que podría resultar de un ataque cibernético, un fallo inesperado del sistema o incluso un error humano. También es recomendable guardar el disco en el que se haga el respaldo de datos lejos de la computadora, para evitar la pérdida total de datos si se rompe o la roban.

Acceso y uso de internet

El acceso y uso seguro de internet es fundamental para proteger la información personal y financiera. A continuación, se presentan recomendaciones clave para navegar de forma segura, identificar sitios confiables y evitar riesgos comunes al hacer transacciones en línea o utilizar redes públicas:

- Evitar hacer transacciones en sitios no seguros. Los sitios seguros se representan con un candado en la parte superior izquierda del navegador de internet.
- Utilizar conexiones seguras (https) al navegar por sitios web. Verificar que la dirección web comience con <https://> en lugar de <http://>. Evitar hacer clic en enlaces sospechosos o descargar archivos de fuentes no confiables.
- Evitar acceder a información sensible o hacer transacciones financieras en redes wifi públicas no seguras. Si es necesario, utilizar una red privada virtual (VPN) para cifrar la conexión y proteger la información.
- Utilizar un cortafuegos para controlar el tráfico de red entrante y saliente. Esto ayuda a prevenir el acceso no autorizado a los dispositivos porque crea una barrera de seguridad. Por ejemplo, Windows tiene un cortafuegos integrado en sus sistemas operativos, llamado Microsoft Defender (anteriormente Windows Defender).
- Antes de proporcionar información personal o financiera en línea, asegurarse de que el sitio web sea legítimo. Verificar la URL y buscar señales de autenticidad, como sellos de seguridad.
- Utilizar un navegador web que sea conocido por su enfoque en la seguridad y considerar la posibilidad de instalar complementos de seguridad que bloqueen anuncios y rastreadores maliciosos. Existen bloqueadores de anuncios gratuitos como Adblock Plus (<https://adblockplus.org/>) y pagos como Malwarebytes Browser Guard (<https://www.malwarebytes.com/browserguard>), entre otros.

— Descargar aplicaciones y *software* solo desde tiendas oficiales y sitios web confiables. El *software* descargado de fuentes no verificadas puede contener *malware*.

— Evitar hacer transacciones bancarias o compras en línea que involucren información financiera confidencial mientras se está conectado a redes wifi públicas.

Resguardo de la información en teléfonos móviles

Los teléfonos móviles se han vuelto fundamentales en nuestras vidas y guardan una gran cantidad de información personal y sensible. Desde datos de contacto hasta fotografías y contraseñas, estos dispositivos almacenan una vasta cantidad de datos valiosos. Sin embargo, con la creciente conectividad y el aumento de las amenazas cibernéticas, es crucial abordar el tema del resguardo de la información en teléfonos móviles de manera adecuada. En este contexto, vamos a ver cómo prevenir posibles riesgos que podrían comprometer la integridad de nuestros datos personales:

- Mantener todos los dispositivos actualizados con las últimas versiones y parches de seguridad. Esto ayuda a proteger los dispositivos contra vulnerabilidades.
- No conectarse a redes inalámbricas desconocidas.
- Deshabilitar los medios de conectividad que provea el equipo (ejemplo: wifi, Bluetooth, etc.) cuando no se usan.
- Utilizar bloqueos de pantalla, PIN o autenticación biométrica (huellas dactilares o reconocimiento facial).
- Tener cuidado con las aplicaciones que solicitan acceso a datos personales.

En un mundo digital cada vez más conectado, la ciberseguridad no es solo cosa de expertos en tecnología, sino una responsabilidad que también tienen los traductores. Es fundamental manejar bien los archivos confidenciales, usar plataformas seguras y seguir buenas prácticas digitales para proteger nuestro trabajo y la confianza de nuestros clientes. Estar al tanto de los riesgos y adoptar medidas de prevención no solo mejora nuestra seguridad personal, sino que también eleva los estándares de toda la profesión. ■