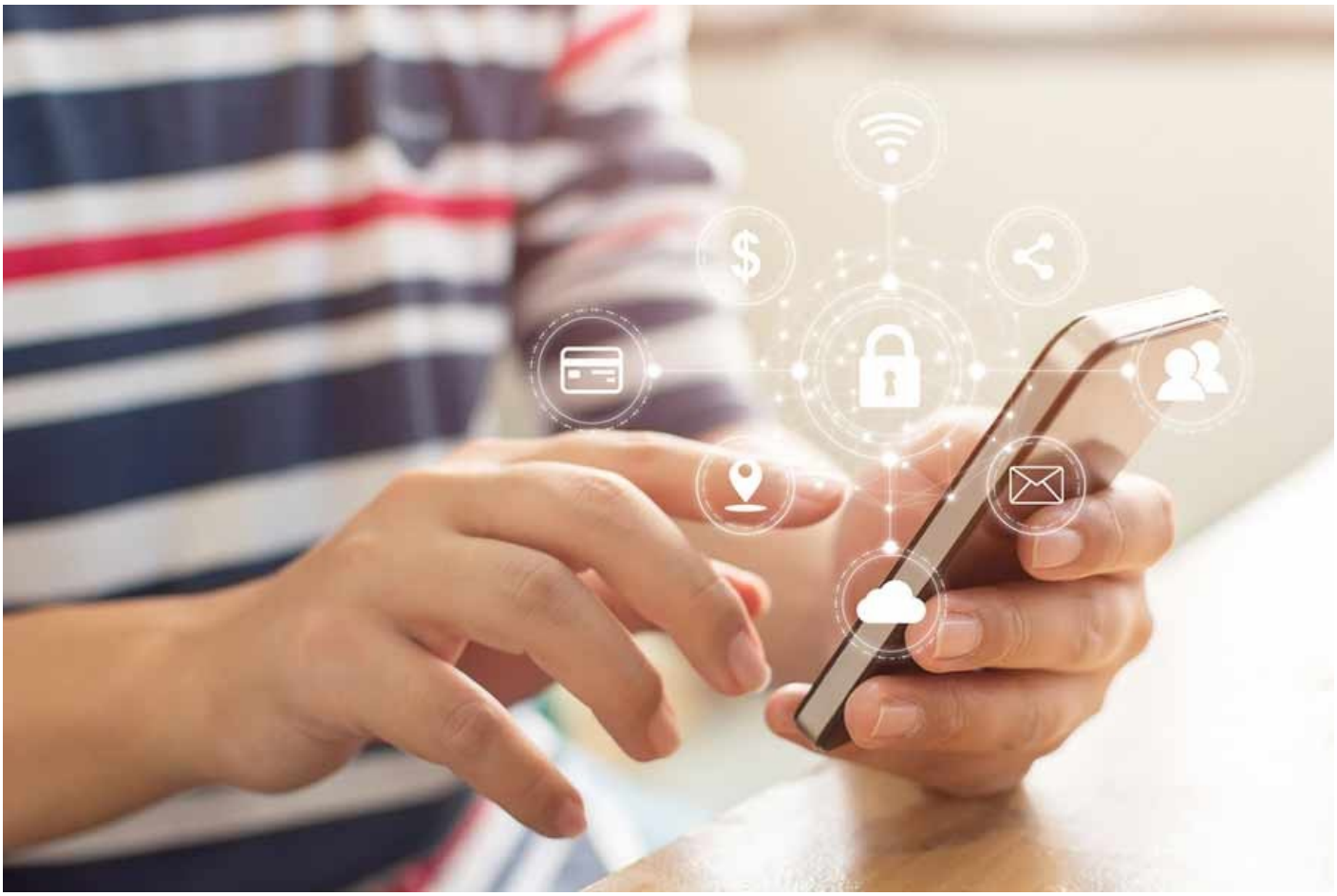
¿Proteges tu información? Sigue estos 8 consejos sobre ciberseguridad

*“Como usuarios estamos tan acostumbrados a compartir información que **pensamos que la seguridad está implícita**”.*

Así enfatiza **Anna Lee Montoya**, profesora de innovación del Tec de Monterrey campus Sinaloa, la importancia de **la ciberseguridad** en este 2020.

Precisamente, en su último informe, la **consultora de tecnología** a nivel internacional **GARNET** destacó que la ciberseguridad forma parte de las **10 tendencias tecnológicas** en este 2020.

La consultora explica que la **ciberseguridad** es la base con la que deben funcionar las otras tecnologías en tendencia, porque sin ella de poco nos sirve que todo esté conectado.


width="900" loading="lazy">

*“Vivimos en la **era digital** y nuestra **nueva normalidad** es estar conectados, así que todos queremos estar presentes ahí, por lo que incluso pudiera considerarse **una necesidad***”, señaló Ana Lee.

Además, indica que estamos en la **cuarta transformación industrial,** la cual persigue que todos los **sistemas informáticos** estén interconectados de **manera inteligente** y **tomen decisiones** por sí solos.

Entonces, la profesora señala que a **mayor digitalización** y **más presencia** en la red, aumenta el **tráfico de información** y **la ciberseguridad** toma más relevancia.

Debido a eso, la experta comparte algunas **medidas que puedes seguir para proteger tu información** y evitar los **ciberataques**.

1. Protege tu información al tener tus sistemas actualizados

*“Es muy común tener una lista infinita de **actualizaciones pendientes** y al no tener todos tus sistemas actualizados eres más vulnerable a un **ataque cibernético**”*, reconoció la profesora.

La profesora destaca que **las actualizaciones** tienen su razón de ser y especialmente estas son el primer **mecanismo de defensa** que tenemos ante **ataques maliciosos**.

Por esto, la profesora recomienda que si el sistema operativo de tus dispositivos te piden actualizarte, lo hagas lo más pronto posible.

2. Cuenta con un antivirus actualizado

La experta explica que **el antivirus** te ayuda a identificar aquellas páginas que son sospechosas y bloquea las ventanas emergentes que pudieran traer **“phishing**”, uno de los ataques cibernéticos más comunes.

*“**El phishing** llega como una alerta que dice que una de tus cuentas está teniendo problemas y te invita a darle clic, luego te pide compartir tu información para poder tener acceso”*, agregó Ana Lee.

Además, menciona que si **tu antivirus está actualizado**, le será más fácil **protegerte** porque estará preparado ante cualquier nuevo virus que pudiera surgir.

3. Sé consciente de los permisos que otorgas

De acuerdo con la experta, la mayoría de las personas con tal de avanzar, **cumplir el requisito** y estar ahí como todos los demás, le dan **aceptar a todo sin detenerse** mucho a pensar.

*“Tenemos confianza ciega en todas las herramientas que usamos, así que **le damos aceptar a sus términos y condiciones y permiso a todas sus solicitudes***”, declaró Anna Lee.

Entonces, propone **hacer conciencia acerca de los permisos** que se otorgan entrando al apartado de aplicaciones en cada dispositivo para revisar la lista de permisos que tenemos activados.

“*Pudieras llegar a sorprenderte de **la gran cantidad de permisos que tienes activados**, de los cuales muy probablemente **ni siquiera eras consciente** de que estaban ahí*”, señaló la profesora.


width="900" loading="lazy">

4. Cuida tus descargas

*“Si das clic o descargas cualquier cosa de **dudosa procedencia**, te estás exponiendo porque no puedes tener la certeza de que sea algo seguro”*, argumentó Ana Lee.

Además, afirma que **navegar en internet** para obtener **material multimedia r**equiere mucho expertis, porque antes de mostrarte el **botón correcto de descargar**, podría colocarte otros tantos falsos.

Por lo tanto, la profesora recomienda que **si recibes algo que no esperabas** y ves que es de procedencia desconocida, **no lo abras y si puedes, mejor elimínalo**.

5. Haz una buena gestión de contraseñas

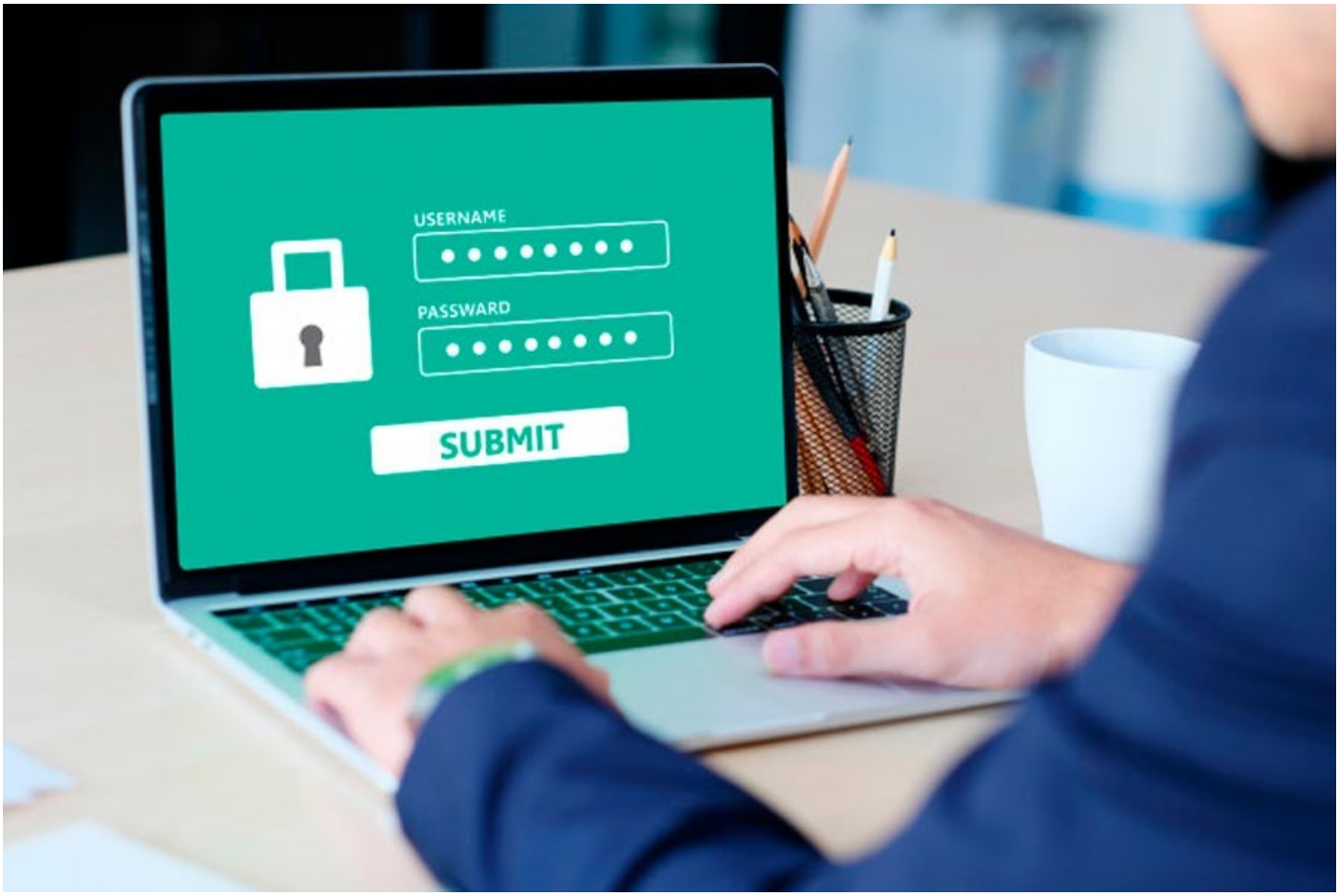
Según la experta, tenemos **cuentas para todo**, son tantas que cada vez se vuelve más difícil **administrar las contraseñas**, para lo cual indica que una contraseña fácil es poco confiable y una difícil se puede olvidar.

Si olvidas tu contraseña puedes **perder tu cuenta**, por lo que la profesora indica que es mejor **vincular tus cuentas** porque así son más **fáciles de rastrear y recuperar** en dado caso.

Sin embargo, en caso de ser necesario **crear una contraseña** sigue las recomendaciones que te hace la empresa, cumple los **requisitos mínimos** y verifica que el **medidor de confiabilidad** la

apruebe.

“Ahora las empresas buscan educar mejor al usuario para que realmente tome la responsabilidad de proteger su información y diseñe contraseñas fuertes difíciles de descifrar”, manifestó Ana Lee.



width="900" loading="lazy">

6. Cuida lo que abres en computadoras ajenas

La experta dice que todo lo que **abras o accedas** desde una computadora ajena podría quedarse guardado y **corres el riesgo** de que se queden ahí tus cuentas y la información de estas.

*“Evita usar computadoras ajenas o en caso de usarlas piensa bien que abrir o que no y tomar otras medidas necesarias para **borrar cualquier dato que se pudiera almacenar***”, recomendó Anna Lee.

7. Evita conectarte al Internet público

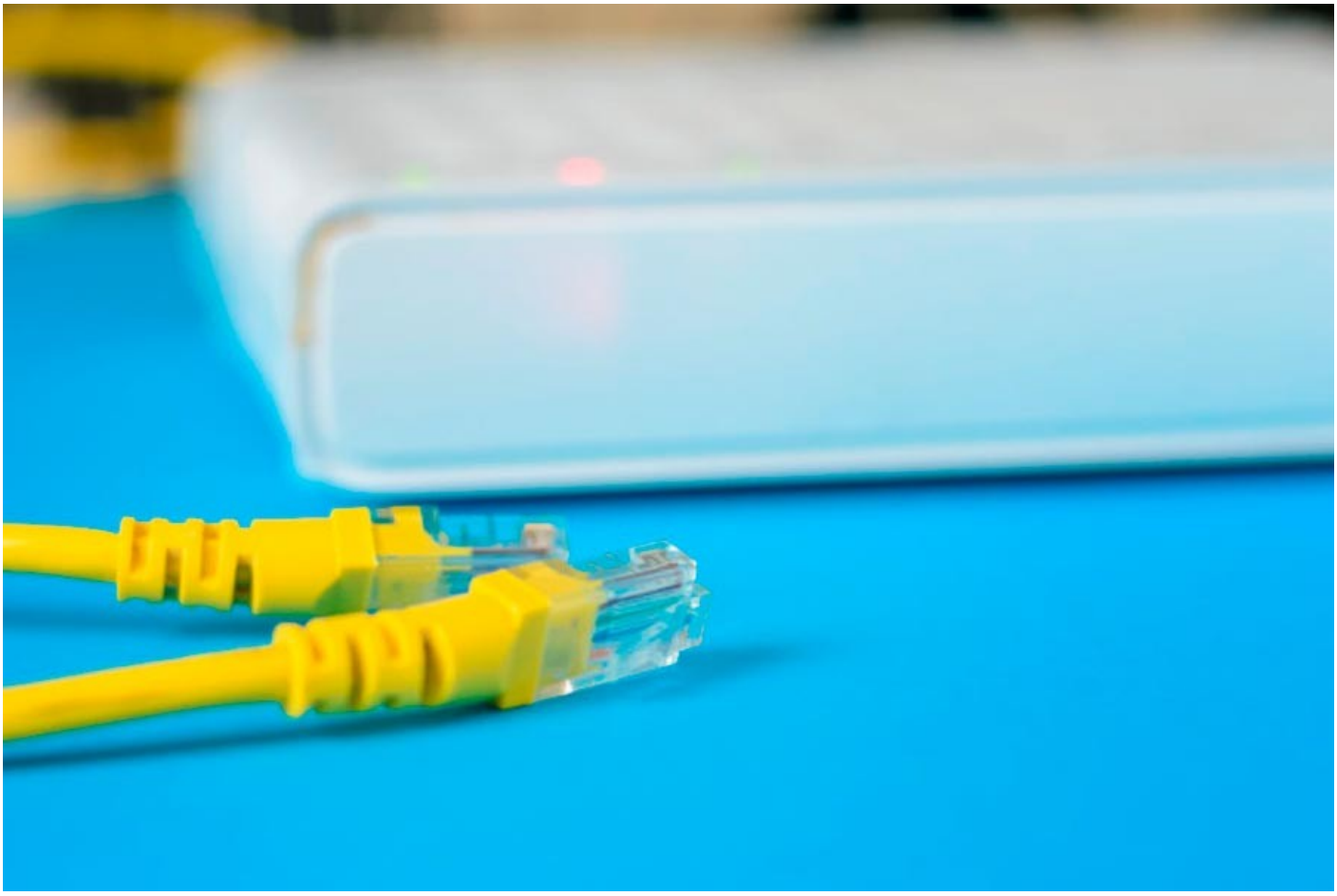
Aunque tengas muchas ganas de revisar tus redes sociales, la profesora dice que **no es nada recomendable usar los Wi-fi gratis**, ya sea el de un parque, un restaurante, un aeropuerto o un hospital.

Por muy atractivas que se vean **las redes abiertas**, la experta señala que en estas se comparten muchos datos y es donde **hay más vulnerabilidad** porque los hackers prefieren trabajar en ellas.

8. Si no vas a usar Internet, mejor apágalo

Si te vas a dormir, vas a salir o simplemente **no vas usar el internet, apágalo** porque según la experta, si alguien logra conectarse a tu red Wi-fi pudiera **tener acceso a todo lo que tengas conectado.**

*“Mantener el internet encendido cuando no lo estas utilizando permite **ciberataques** en momentos en los que es difícil que te des cuenta, algo que es posible **prevenir si lo apagas**”*, resaltó Ana Lee.



width="900" loading="lazy">

Finalmente, la experta resalta la importancia de **no subestimar el valor de tu información** o lo común que podrían llegar a ser los ataques cibernéticos, por lo que te invita a protegerte.

*“A pesar de que seguir estas recomendaciones requiere de **un esfuerzo extra** de tu parte es importante que tomes consciencia y seas más responsable sobre lo que aceptas y compartes”*, cerró Ana Lee.

SEGURO QUERRÁS LEER TAMBIÉN: