

Ciberseguridad: un problema cultural

Durante años, hemos hablado de ciberseguridad como si fuera un asunto técnico, casi quirúrgico: más software, mejores firewalls, sistemas más robustos. Sin embargo, mientras la tecnología avanza, los incidentes siguen ocurriendo. No porque falten herramientas, sino porque fallan los hábitos. Y los hábitos no se parchean: se aprenden, se imitan y se normalizan. Por eso, cada vez resulta más evidente que la ciberseguridad no es, en esencia, un problema tecnológico, sino un problema cultural.

La mayoría de los ataques exitosos no comienzan con una vulnerabilidad sofisticada, sino con una acción cotidiana: un clic apurado, una contraseña reutilizada, un archivo abierto sin verificar, un mensaje reenviado “por si acaso”. El factor humano no es una excepción dentro del ecosistema digital; es su punto de entrada más frecuente. Esto no habla de ignorancia técnica, sino de cómo nos relacionamos con lo digital, de la confianza automática que depositamos en pantallas, enlaces y notificaciones, y de la idea instalada de que “si algo pasa, alguien más lo resolverá”.

En ese contexto, la ciberseguridad se parece menos a una disciplina informática y más a una práctica social. Tal como ocurre con la seguridad vial o la salud pública, no basta con que existan normas y sistemas: lo decisivo es si las personas internalizan conductas de cuidado. Podemos tener autos con airbags, pero si no usamos cinturón, el riesgo persiste. Del mismo modo, podemos tener plataformas seguras, pero si nuestros hábitos digitales son descuidados, el sistema

completo se vuelve frágil.

Esta fragilidad se vuelve especialmente visible en la vida cotidiana. La digitalización avanzó rápido, pero la cultura del autocuidado digital no avanzó al mismo ritmo. Muchas personas creen saber identificar fraudes, pero al mismo tiempo mantienen prácticas riesgosas: conectarse a redes WiFi públicas sin protección, usar la misma contraseña en múltiples servicios, ignorar configuraciones de privacidad, aceptar permisos sin leer. No es una contradicción individual; es una señal cultural. La conveniencia, la urgencia y la costumbre suelen pesar más que la seguridad, porque el riesgo se percibe como lejano, abstracto o improbable.

Un ejemplo particularmente revelador de esta tensión cultural es el uso de dispositivos personales con cuentas de empresa. Hoy, el trabajo, el estudio y la vida privada conviven en un mismo celular o computador. En el mismo equipo donde se revisa el correo institucional, se descargan aplicaciones, se comparan fotos familiares y se accede a redes sociales. Esta mezcla no es neutra: diluye fronteras, multiplica riesgos y convierte la ciberseguridad en algo que literalmente llevamos en el bolsillo. No es que las personas decidan conscientemente asumir más riesgo; es que el uso se normaliza sin reflexión, impulsado por la urgencia y la lógica del “responder ahora”.

Aquí aparece una paradoja incómoda: organizaciones que invierten en tecnología avanzada, pero cuya seguridad depende, en última instancia, de prácticas

cotidianas que nadie acompaña de forma sostenida. Políticas existen, documentos también, pero sin una cultura que las vuelva vivas, terminan siendo letra muerta. La ciberseguridad no falla porque la gente sea irresponsable, sino porque el sistema no está diseñado para fomentar hábitos seguros de manera realista y continua.

Si el problema es cultural, la respuesta no puede limitarse a controles técnicos o capacitaciones aisladas. Requiere educación, pero no solo en el sentido formal. Requiere formar ciudadanía digital desde temprano, entendiendo que navegar en internet, usar plataformas y gestionar datos personales es parte de la vida en sociedad. Enseñar a desconfiar de lo “demasiado bueno”, a verificar antes de compartir, a comprender el valor de los datos propios y ajenos, no es un lujo ni una especialización: es una competencia básica para vivir en el mundo actual.

Esta mirada obliga a elevar la conversación a nivel país. La ciberseguridad no es solo un tema de empresas tecnológicas o áreas de informática; es infraestructura social. Impacta la continuidad de servicios públicos, la confianza en las instituciones, la economía, la educación y, en última instancia, los derechos de las personas. Cuando un sistema cae o una base de datos se filtra, las consecuencias no se distribuyen de forma equitativa: afectan más a quienes tienen menos herramientas para protegerse o recuperarse. Tenemos un rol clave en promover alfabetización digital, establecer estándares claros y proteger derechos. Las organizaciones deben diseñar entornos que faciliten el comportamiento seguro y no lo conviertan en una carga adicional. El sistema educativo debe integrar la seguridad digital como parte de la formación ciudadana. Y las personas, finalmente, deben reconocer que su comportamiento en línea no es solo un asunto privado, sino parte del cuidado



Edgardo Fuentes
Director Ingeniería en Ciberseguridad UNAB

colectivo.

La cultura de ciberseguridad no se compra ni se instala con un software. Se construye cuando reportar un error no genera castigo, cuando la seguridad se conversa de forma cotidiana y no solo después de un incidente, cuando el cuidado digital se entiende como autocuidado y como responsabilidad social. Mientras sigamos tratando la ciberseguridad como un problema técnico, seguiremos buscando soluciones donde no está la raíz.

En una sociedad donde casi todo pasa por lo digital, la verdadera pregunta no es si tenemos tecnología suficiente, sino si tenemos la cultura necesaria para usarla con responsabilidad. Porque, al final del día, la ciberseguridad no se juega en los servidores: se juega en nuestras decisiones diarias, muchas veces invisibles, pero siempre determinantes.