OPINIÓN

Publicado el 17 de agosto 2026 en Prensa Libre

Por: Mario A. García Lara

Ciberseguridad: ni cerrojo ni coladero

La vida digital exige reglas inteligentes: seguridad, derechos, técnica y prudencia legislativa.

Hace no tantos años parecía que la ciberseguridad era un asunto reservado a especialistas en informática, bancos o agencias de inteligencia. Ese ya no es el caso: una falla o un ataque digital pueden impedir una transferencia bancaria, paralizar un hospital, interrumpir un servicio público, comprometer datos personales o afectar el suministro de electricidad. En una economía cada vez más digitalizada, la ciberseguridad no es ya solo un problema técnico, sino un asunto estratégico que afecta la vida económica, institucional y ciudadana.

Por eso cobra relevancia la discusión que actualmente tiene lugar en el Congreso sobre cómo regularla. Guatemala necesita un marco jurídico moderno que permita prevenir ataques, gestionar riesgos, proteger infraestructuras críticas, coordinar respuestas y perseguir eficazmente la ciberdelincuencia. Pero, como ocurre con casi toda buena regulación, el problema no consiste simplemente en emitirla, sino en diseñarla bien: una ley demasiado laxa puede dejar al país expuesto a riesgos crecientes, pero una demasiado restrictiva puede elevar costos innecesarios, obstaculizar la innovación, desalentar la cooperación privada e incluso abrir espacios para abusos sobre la privacidad. El desafío está en encontrar un equilibrio razonable entre seguridad y libertad, prevención y proporcionalidad, capacidad estatal y límites al poder público.

Aquí aparece el tema que tanto cuesta entender y afrontar en Guatemala: la institucionalidad. Una ley puede verse impecable en el papel y fracasar en la práctica si crea entidades sin capacidades, competencias confusas o mandatos traslapados. La autoridad que se establezca para regular la ciberseguridad debe ser técnica, flexible, profesional y suficientemente independiente de vaivenes políticos; tener funciones claramente delimitadas, recursos adecuados y mecanismos efectivos de rendición de cuentas. La ciberseguridad exige coordinación, no burocracia; especialistas, no improvisación.

La ciberseguridad exige coordinación, no burocracia; especialistas, no improvisación

Tampoco conviene inventar el agua azucarada ni empezar de cero. Existen mejores prácticas a nivel internacional. Y en lo local, algunos sectores como el financiero y el eléctrico han desarrollado capacidades, protocolos y mecanismos propios de prevención y respuesta. La regulación nacional debería aprovecharlos y articularlos, respetando las competencias de los reguladores sectoriales. Centralizar por centralizar puede destruir el conocimiento acumulado y generar costosas duplicidades.

Además, la ciberseguridad no puede tratarse como una isla normativa. Forma parte de un ecosistema más amplio que incluye, como mínimo, protección de datos personales, infraestructuras críticas, evidencia digital y prevención y sanción de ciberdelitos. De todos esos componentes, la protección de datos resulta especialmente urgente: proteger sistemas sin proteger adecuadamente la información de las personas sería construir una muralla con un boquete abierto.

Todo esto aconseja prudencia legislativa. Para emitir una regulación de naturaleza tan compleja, las prisas suelen producir leyes incompletas, contradictorias o imposibles de aplicar, por lo que precisa una discusión amplia, técnica y suficientemente pausada, que escuche al sector público, empresas, reguladores, academia, especialistas y sociedad civil. Guatemala necesita una buena ley de ciberseguridad pero, encima de eso, un sistema de resiliencia digital que funcione. Como tantas veces ocurre en política pública, el éxito no estará en la cantidad de artículos aprobados, sino en la calidad de las reglas, de las instituciones y de los incentivos que logremos construir.

Puede consultar esta y otras columnas en el siguiente enlace:
https://copades.com/monec/?page_id=63752