LITORALPRESS

Fecha: 27-01-2026
Medio: El Pingüino
Supl. : El Pingüino
Tipo: Columnas de Opinión
Título: **Columnas de Opinión: Ciberseguridad: el poder ya no se toma, se hackea**

Pág. : 9
Cm2: 239,1
VPE: $ 286.480

Tiraje: 5.200
Lectoría: 15.600
Favorabilidad: No Definida

La columna de...

GABRIEL BERGEL,
CEO 8.8 COMPUTER SECURITY CONFERENCE

Ciberseguridad: el poder ya no se toma, se hackea

La política sigue discutiendo de soberanía, de fronteras, de enemigos visibles. Mientras tanto, el poder real entra por el router, no por la aduana. Y lo hace sin pedir permiso.

La ciberseguridad dejó de ser un asunto técnico para transformarse en un tema profundamente político porque la estabilidad democrática, la confianza pública y la capacidad de gobernar dependen de sistemas digitales que son frágiles, permeables y, muchas veces, mal defendidos.

En el contexto político actual -polarización extrema, desinformación como estrategia y Estados lentos- la pregunta ya no es si habrá ataques, sino cuándo y con qué impacto.

Primer dato incómodo: hoy la mayor amenaza no suele venir de hackers encapuchados en países lejanos, sino de errores humanos, sistemas obsoletos y decisiones políticas cortoplacistas. La contraseña "admin" sigue siendo una metáfora demasiado real del Estado moderno.

Segundo dato aún más incómodo: la ciberseguridad no se resuelve con más control, sino con mejor inteligencia. En tiempos donde todo se graba, se filtra y se viraliza, la tentación autoritaria es espiar más. Clásico error. La seguridad digital no es vigilancia masiva; es resiliencia, prevención y capacidad de respuesta. Es asumir que el ataque va a ocurrir y preparar el sistema para no colapsar cuando pase.

La política, sin embargo, funciona al revés. Reacciona. Siempre tarde. Siempre con una comisión investigadora que llega cuando los datos ya están publicados. Se legisla después del escándalo, no antes del riesgo. Así no hay firewall que aguante.

A esto se suma el uso de la desinformación como arma electoral. Bots, deepfakes, que ensucian la discusión pública. No es solo un problema tecnológico, es un problema ético.

¿Cómo afrontar entonces la ciberseguridad en este contexto?

Primero, entender que la ciberseguridad es política pública. Requiere presupuesto estable, equipos profesionales bien pagados y autonomía técnica. No se terceriza la defensa de la democracia al proveedor más barato.

Segundo, cooperación. Ningún Estado puede solo. Los ataques no respetan ideologías ni banderas. Compartir información, estándares y buenas prácticas es más efectivo que competir a ver quién tiene el discurso más duro.

Tercero, alfabetización digital ciudadana. Sin ciudadanos informados, no hay sistema seguro. El votante que reenvía cualquier cosa también es parte del problema. Y sí, educar lleva tiempo, pero es la única alternativa para robustecer el sistema.

Cuarto, liderazgo político que entienda el tema, capaz de escuchar a quienes saben. La ciberseguridad no da votos inmediatos, pero su ausencia los puede destruir a todos de un día para otro.

La ciberseguridad no va a salvar la democracia, pero sin ella, la democracia no llegará al próximo mandato.

La pregunta final no es técnica, es política: ¿vamos a seguir improvisando hasta que el próximo ataque nos deje sin excusas, o vamos a asumir que el poder, hoy, también se defiende con código?