PERIÓDICO	PÁGINA	FECHA	SECCIÓN
INDEPENDIENTE	5	09/02/2026	OPINION

CÁMARA DE DIPUTADOS
LXVI LEGISLATURA
SOBERANÍA Y JUSTICIA SOCIAL

BRÚJULA PÚBLICA

La seguridad no es crítica

POR RODOLFO ACEVES JIMÉNEZ

La infraestructura crítica está constituida por aquellas instalaciones relacionadas con la provisión de bienes y de prestación de servicios públicos esenciales y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la ley de la materia.

Un ejemplo de esta infraestructura crítica lo constituye los sistemas informáticos que proveen o alimentan de información en alguno los servicios que prestan los tres órdenes de gobierno de los tres poderes de la Unión, así como de las etapas de los procesos de producción o comercialización de bienes y servicios de los tres sectores de la economía.

Su importancia radica en que por sus procesos es posible que transiten gran parte de información sensible para el país o sus ciudadanos, como datos personales de los derechohabientes de algún servicio público que proporciona alguna institución gubernamental, de los usuarios de la banca, o transacciones y transferencias de sumas cuantiosas de dinero, y, por esta razón, es que son consideradas dentro de los parámetros de la seguridad nacional.

La violación a la seguridad de este tipo de infraestructura crítica ha sido el dolor de cabeza de diversas administraciones de los tres órdenes de gobierno.

Por ejemplo, en mayo de 2018 se tuvo conocimiento que los procesos en la infraestructura crítica que regula el Sistema de Pagos Electrónicos Interbancarios (SPEI) que opera el Banco de México (Banxico) afectó principalmente las transacciones en ese sistema que utilizan las instituciones Banamex, Banorte y BBVA Bancomer, cuyas últimas dos instituciones afirmaron que se trató de incidencias.

Esta falla pudo haberse extendido a todas las instituciones del sector bancario mexicano.

En la pasada administración la organización Guacamaya Leaks divulgó la sustracción de 6 terabytes de información a la Secretaría de la Defensa Nacional (SEDENA), y reveló que algunos servidores públicos de los gobiernos de Jalisco, Morelos, así como funcionarios federales tuvieron alguna relación con grupos de la delincuencia organizada. Hoy en día nuevamente sucede.

Se informa que los datos de unos 36.5 millones de personas fueron expuestos con el hackeo a por lo menos 25 dependencias públicas de los tres órdenes de gobierno.

Los sistemas informáticos del IMSS, SAT, Bienestar y Morena fueron vulnerados presuntamente por el grupo Chronus.

No sólo eso, en 7 días algunas de las instituciones de seguridad mexicana estuvieron vulneradas por ataque de hackers, cuando el portal de la policía de Tijuana fue atacado, lo que vulneró el sistema de reporte de incidencias cibernéticas y el sistema de cédulas de búsqueda de personas.

En la pasada administración la organización Guacamaya Leaks divulgó la sustracción de 6 terabytes de información a la Secretaría de la Defensa Nacional (SEDENA), y reveló que algunos servidores públicos de los gobiernos de Jalisco, Morelos, así como funcionarios federales tuvieron alguna relación con grupos de la delincuencia organizada. Hoy en día nuevamente sucede… Los sistemas informáticos del IMSS, SAT, Bienestar y Morena fueron vulnerados presuntamente por el grupo Chronus

Posteriormente hubo una ofensiva a nivel nacional, con la divulgación de los datos de más de 86 mil servidores públicos del gobierno de San Luis Potosí, de casi 49 mil expedientes de jóvenes en situación vulnerable atendidos en Centros de Integración Juvenil fueron filtrados, así como la sustracción de 40 giga bytes de información confidencial del gobierno de Nuevo León que contenían expedientes de trabajo y datos de impuestos, entre otros, fueron puestos a la venta por 50 dólares y hasta 320 dólares a quién quisiera adquirirlo.

Lo mismo ocurre en el sitio del gobierno de Coahuila cuando hackers vulneraron su seguridad para modificar la apariencia de su sitio web con textos e imágenes distintos a los oficiales, para humillar públicamente a su propietario.

Más allá de las excusas que dan a conocer las dependencias, el verdadero impacto de esta crisis recae en las personas.

El diagnóstico es, que algunas o muchas de las instituciones públicas operan sistemas informáticos sin protocolos de seguridad, policías cibernéticas que son hackeadas fácilmente, así como gobiernos estatales sin la protección más elemental, dando como resultado un paraíso para los cárteles de datos.

La amenaza digital ya está adentro.

No hay austeridad que valga para proteger la seguridad de los datos de la ciudadanía.

*Es Maestro en Seguridad Nacional por la Armada de México

racevesj@gmail.com

Twitter: @racevesj

Foto: Redes Sociales