



Proponen reconocer los ataques cibernéticos como amenazas a la Seguridad Nacional

La diputada María Eugenia Hernández Pérez, de Morena, presentó una iniciativa que propone reformar la Ley de Seguridad Nacional para que reconozca a los ataques cibernéticos como amenazas a la Seguridad Nacional, crear una estrategia de defensa a los ataques cibernéticos, y fomentar la cooperación internacional en torno a la ciberseguridad como política exterior.



“Se busca reconocer los ataques cibernéticos como amenazas a la Seguridad Nacional, teniendo en mente que la mayoría de las instituciones de gobierno, incluyendo a la Secretaría de Seguridad y Protección Ciudadana (SSPC), la Marina (Semar) y la Secretaría de la Defensa Nacional (Sedena), tienen una tendencia a la digitalización de sus servicios y operaciones diarias y se han vuelto altamente dependientes de la disponibilidad de sus infraestructuras críticas”, detalla el documento.

La propuesta plantea clasificar como amenazas a la Seguridad Nacional los actos que tiendan a dañar, interrumpir u obtener acceso no autorizado a la Infraestructura Crítica del Estado a través del ciberespacio, con el propósito de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno o infraestructura de computación, destruir la integridad de los datos o robar la información controlada.

Y determina el concepto de ciberespacio como un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de TI, incluido Internet, redes de telecomunicaciones, sistemas informáticos y procesadores embebidos y controladores.

“La presente iniciativa se enmarca en los objetivos generales de la Estrategia Digital Nacional que contempla a la ciberseguridad como uno de los nueve ejes de acción”, señala la propuesta de la diputada Hernández Pérez.

Entre los riesgos que pueden comprometer la Seguridad Nacional, enlista la legisladora, están: la filtración de datos confidenciales de la nación, la intervención de las comunicaciones privadas del Estado, así como la vulneración de activos informáticos críticos para la provisión de servicios vitales como el agua, la luz y el Internet.