PERIÓDICO	PAGINA	FECHA	SECCIÓN
proceso	58 - 59	09/10/2022	LEGISLATIVO

El *hackeo* a la Secretaría de la Defensa Nacional (Sedena) por los ciberactivistas Guacamaya, por su extrema gravedad, no puede pasar inadvertido ni ser minimizado como pretende el presidente López Obrador, un mandatario y su gobierno que menosprecian la tecnología, cuyas consecuencias ya las hemos visto en varios incidentes previos.

No sólo se trata de una institución que procura la seguridad nacional, como la Sedena, sino de la indolencia que ha tenido México en materia de ciberseguridad en los años recientes.

Además, a partir de la pandemia de covid-19 hemos sido testigos de un aumento en los ciberataques, tanto en cantidad como en dimensión, sin que el gobierno haya actuado para atender el problema.

En este mismo espacio hace más de dos años urgimos a que el gobierno de la Cuarta Transformación tuviera su propia Estrategia Nacional de Ciberseguridad. Entonces la ciberdelincuencia ocasionaba pérdidas por 575 millones de dólares al año, 0.5% del PIB mundial. Los ciberataques a escala global, equivalentes a 3 mil millones de dólares anuales, rebasaron los ingresos del narcotráfico.

Distintos índices coinciden en señalar que somos un país de alto riesgo en materia de ciberseguridad, no sólo como objeto de ciberataques, también como generador de ciberdelitos.

Además, como parte del Diálogo Económico de Alto Nivel (DEAN) entre México y Estados Unidos, ambos gobiernos deberían estar coordinados para fortalecer las protecciones de seguridad cibernética.

Aunque EU brinda asistencia técnica a México para aumentar su capacidad

Continúa en la siguiente página

PERIÓDICO	PAGINA	FECHA	SECCIÓN
proceso	58 - 59	09/10/2022	LEGISLATIVO

Viene de la página anterior

JORGE BRAVO

"HACKEO" A LA SEDENA Y DESIDIA EN CIBERSEGURIDAD

para proteger el ciberespacio mediante diversas disposiciones, el DEAN parece más una carta de buenas intenciones que un compromiso serio en materia de ciberseguridad.

México tampoco ha signado el Convenio de Budapest sobre ciberdelincuencia, el primer tratado internacional vinculante que aborda los delitos informáticos y de internet para armonizar las leyes nacionales, mejorar las técnicas de investigación y aumentar la cooperación entre las naciones.

La ciberinseguridad y la cibercriminalidad en el entorno virtual son un reflejo fiel de la inseguridad pública que flagela a México en el mundo físico, por lo que se requieren normativas, acciones, estrategias, programas, presupuesto, instituciones y un responsable paralelo para afrontar el desafío.

El ciberataque a la Sedena no sólo compromete la seguridad de la información sensible y los datos personales que resguarda esa institución, sino que ha dañado seriamente su reputación en un momento en el cual el Ejército ha asumido labores civiles, como la construcción y administración del nuevo Aeropuerto Internacional Felipe Ángeles o la discusión de la adscripción de la Guardia Nacional a la Secretaría de la Defensa.

La pérdida de confianza en la Sedena en materia de ciberseguridad es ineludible, máxime cuando el presidente descartó una investigación del *hackeo*, uno de los procedimientos básicos para responder y reponer los sistemas afectados y minimizar cualquier daño.

La inseguridad cibernética es el lado oscuro de la conectividad, la digitalización, el mayor acceso a tecnologías de la información y la comunicación (TIC) y la transformación digital de la sociedad, los gobiernos y las organizaciones.

La mayoría de las actividades que realizamos dependen del uso de las TIC y de estar conectados a internet. La ciberseguridad no sólo protege la información, los equipos de cómputo, los sistemas y las infraestructuras, sino también las actividades que dependen de ellas, incluidas la seguridad nacional, las transacciones financieras, la integridad de las personas, sus datos personales, imagen y patrimonio.

México no tiene una ley específica sobre ciberseguridad, pero sí disposiciones en distintas normas. El artículo 211 del Código Penal prevé el delito informático. Sin embargo, estas disposiciones son limitadas, lo que dificulta la gestión del riesgo, la protección contra los ciberataques, la detección de incidencias en los sistemas de ciberseguridad, la minimización del impacto de los ataques y la implantación de una cultura de ciberseguridad.

La poco efectiva Estrategia Nacional Digital (EDN) promueve la implementación del Protocolo Homologado para la Gestión de Incidentes Cibernéticos entre Instituciones, que busca fortalecer la coordinación entre autoridades para mejorar la prevención de incidencias cibernéticas.

Concretamente, el objetivo 5 de la EDN incluye el deseo, pero no las acciones, para "promover una cultura de seguridad de la información que genere certeza y confianza a las personas usuarias de los servicios tecnológicos institucionales y gubernamentales".

En el marco de la EDN, en julio de 2021 se publicaron las Bases Técnicas de Seguridad Informática para las dependencias y entidades de la Administración Pública Federal: recomendaciones mínimas de seguridad informática, pero no una estrategia integral.

Lo que no existe es coordinación, porque la ciberseguridad es un tema transversal. El objetivo tendría que ser construir una base sólida e institucional de seguridad para asegurar que los organismos gubernamentales, las empresas y la sociedad cuenten con los mecanismos y herramientas adecuadas para manejar los riesgos, así como defenderse y responder ante los ciberataques.

Las funciones del gobierno, como la prestación de servicios públicos y la seguridad nacional, deben ser resistentes y resilientes a los ataques cibernéticos.

El Congreso de la Unión trabaja con parsimonia en la elaboración de una propuesta de Ley Federal de Ciberseguridad, a partir de 15 iniciativas de ley de diferentes partidos. Las comisiones de Ciencia, Tecnología e Innovación de la Cámara de Diputados y del Senado se comprometieron a presentar un borrador en septiembre de 2022.

Los legisladores vuelven a trabajar a marchas forzadas una vez que ha ocurrido un incidente de ciberseguridad grave, evidenciados en su falta de compromiso y enfoque de ponerse de acuerdo en lo importante para México. Ellos también son responsables del *hackeo* a la Sedena, junto con un gobierno que se resiste a entrar de lleno a la era digital, con sus oportunidades y retos. ●

Twitter: @beltmondi