PROPOSICIÓN CON PUNTO DE ACUERDO, PARA EXHORTAR A LA SEDENA A HACER PÚBLICO UN INFORME SOBRE EL ESTADO QUE GUARDAN LAS INVESTIGACIONES RELATIVAS AL CIBERATAQUE QUE RECIBIÓ DICHA DEPENDENCIA, SUSCRITA POR LOS DIPUTADOS JORGE ÁLVAREZ MÁYNEZ Y SALVADOR CARO CABRERA, DEL GRUPO PARLAMENTARIO DE MOVIMIENTO CIUDADANO

Quien suscribe, diputado Jorge Álvarez Máynez, integrante del Grupo Parlamentario de Movimiento Ciudadano en la LXV Legislatura en la Cámara de Diputados, con fundamento en lo señalado en los artículos 6, numeral 1, fracción I, y 79, numeral 1, fracción II, del Reglamento de la Cámara de Diputados del honorable Congreso de la Unión, someten a la consideración de la está asamblea la siguiente proposición con punto de acuerdo, con base a la siguiente

Exposición de Motivos

I. El pasado 8 de agosto de 2022 en conferencia matutina se originaron las primeras declaraciones del Presidente de la República, Andrés Manuel López Obrador respecto a la presentación de la iniciativa para cambiar la adscripción de la GN:

> "Presidente Andrés Manuel López Obrador: Lo voy a analizar en el ámbito, en la esfera de mis atribuciones. Puedo modificar, si es necesario, el reglamento interno en el gobierno puede ser por decreto, puede ser una reforma a la Ley de la Administración Pública, independientemente de lo que resulte sobre la reforma constitucional, pero sí hacen falta estos cambios."

Para el día 26 de agosto de 2022, en la conferencia matutina, el Presidente declaró:

> "Entonces, para que se incorpore la Guardia Nacional a la Secretaría de la Defensa –que lo que queremos es que sea una rama de la Secretaría de la Defensa, con la idea de que perdure y que sea la institución por excelencia para garantizar la seguridad pública– bueno, esa propuesta requiere de una reforma constitucional."
>
> "Entonces, sin reforma constitucional, voy a enviar el día 1º una iniciativa de ley integral para que en los márgenes legales se pueda lograr este propósito."

El pasado 29 de septiembre de 2022 conforme a datos del reportaje del sitio de noticias Latinus, que dirige el periodista Carlos Loret, el grupo Guacamaya hackeó sistemas de la SEDENA y obtuvo seis terabytes de información con comunicaciones y documentos sobre temas como seguridad, contratos de obra pública y la salud del propio presidente. La Secretaría de la Defensa Nacional (SEDENA) sufrió un ciberataque que expuso presuntos correos y documentos sobre operativos de seguridad, así como contratos del Ejército.

Con esta filtración, se expusieron miles de documentos e informes de inteligencia sobre líderes criminales y personajes de la política, así como transcripciones de intervenciones telefónicas, fotografías, directorios y seguimiento a personajes como el embajador de Estados Unidos en México, Ken Salazar. También se filtraron bases de datos sobre el estado de fuerza de militares desplegados en el país, el uso de aeronaves y contratos al Tren Maya y al Aeropuerto de Tulum, en Quintana Roo.

En la primera entrega sobre información filtrada se hicieron públicos documentos sobre la salud del presidente López Obrador; las medidas tomadas por el Ejército en octubre de 2019, durante el llamado 'Culiacanazo', cuando se dio un enfrentamiento entre militares y narcotraficantes en Sinaloa para obligar la liberación de Ovidio Guzmán, hijo de "El Chapo"; y una carta entre el secretario de la Marina y el secretario de la Defensa Nacional, en donde se muestran diferencias en torno a sus criterios de seguridad sobre el Aeropuerto Internacional de la CDMX.

Asimismo, se difundió que, en la información obtenida, que equivale a 36 millones de documentos PDF y 1.5 millones de fotos o 3 mil horas de video, se tienen informes de inteligencia sobre líderes criminales y políticos, transcripciones de intervenciones telefónicas, informes extraoficiales sobre víctimas mortales en operativos militares y datos sobre presencia militar en diversas actividades a lo largo del país.

De acuerdo a especialistas en ciberseguridad de Seekurity, el grupo Guacamaya tardó alrededor de un mes para extraer la información de los servidores de SEDENA, además de que, de acuerdo a declaraciones de dicho grupo, ya se tenían códigos infiltrados para hackear a la Secretaría desde el 5 de julio, los cuales se utilizaron para estar descargando información. Además, esta vulneración ante ataques cibernéticos cree que está ligada con la reducción presupuestal que sufrieron las áreas de tecnología de la información cuando comenzó la presente administración

Esta intromisión a los sistemas de cómputo de la SEDENA da muestra de la vulneración y expone la seguridad de millones de personas que vivimos en el territorio nacional, así como las causas que nos han llevado a la militarización del país y del mando que tiene el Ejército en la actual administración. El hackeo a SEDENA revela uno de los riesgos de confiarle un número creciente de responsabilidades a dicha institución: crea un punto focal de vulnerabilidad para todo el gobierno federal.

En la mañana del 30 de septiembre de 2022, el Presidente Andrés Manuel López Obrador aceptó que el grupo de hackers denominado “Guacamaya” evidenció los documentos y la información antes descrita, y que esta fue obtenida por un ataque cibernético hacia la SEDENA.

II. La Secretaría de la Defensa Nacional es una dependencia del Poder Ejecutivo Federal, con la misión de organizar, administrar y preparar al Ejército y la Fuerza Aérea Mexicanos, con objeto de defender la integridad, la independencia y la soberanía de la nación; garantizar la seguridad interior y coadyuvar con el desarrollo nacional.

Desde 2013 a 2019 la propia Auditoría Superior de la Federación señaló deficiencias o vulnerabilidades relativas a la seguridad digital hacia la SEDENA, así como en el área de tecnologías de información. Además, se encontró que 18 de 20 controles tenían deficiencias y vulnerabilidades en materia de seguridad nacional, entre ellas:

- Deficiencias en los controles de ciberdefensa para la infraestructura de hardware y software de la Secretaría, relacionadas con las directrices, infraestructura y herramientas informáticas en esta materia, que podrían afectar la integridad, disponibilidad y confidencialidad de la información, poniendo en riesgo la operación de la SEDENA.

- Entre otras irregularidades graves, la Auditoría Superior de la Federación detectó falta de control en la configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores, evaluación continua de la vulnerabilidad y solución, así como protección de correo electrónico y navegador web.

- No se cuenta con evidencia documental acerca de las actividades realizadas por la SEDENA para verificar que los minutos que reportaba el proveedor fueran los utilizados por la secretaría.

- Los dictámenes técnicos carecen de documentación soporte que garantice que las cifras reportadas corresponden a lo efectivamente prestado por el proveedor.

- El administrador del contrato no elaboró, revisó o aprobó los dictámenes y oficios de aceptación parcial para ninguna de las partidas del contrato.

Factor crítico	Riesgo
Políticas y procedimientos institucionales	La carencia de políticas y procedimientos puede ocasionar que no se cuente con instrucciones, medidas de seguridad o mecanismos de control claramente definidos, causando confusiones, mal uso y manejo de los activos y herramientas de Tecnologías de Información y Comunicaciones (TIC) por parte de los usuarios finales y administradores de tecnologías, lo cual podría impactar en la operación de la Secretaría.
Mecanismos de control de incendios	La falta de implementación de dispositivos para el control de incendios puede ocasionar que en caso de presentarse algún incidente no se lleven a cabo acciones con oportunidad que permitan contener el fuego en su zona de origen reduciendo los daños en su entorno más inmediato y evitar la propagación a zonas adyacentes, y en consecuencia presentarse un daño a la infraestructura tecnológica de la SEDENA que pudiera impactar la operación de la misma.
Aire acondicionado y unidades UPS	El no contar con equipo de aire acondicionado y de respaldo para el suministro de energía en buenas condiciones, puede ocasionar que el centro de datos alcance niveles de temperatura elevados o tenga interrupciones de energía, lo cual podría afectar negativamente el rendimiento del equipo y acortar su vida útil; así como afectar la disponibilidad de los servicios e información de la SEDENA.
Replicación del almacenamiento a sitios alternos	Los respaldos están en el mismo predio que los servidores y no son probados sistemáticamente para detectar fallas en la grabación de los datos, aunado a que no son replicados a un sitio alterno fuera del centro de datos, en consecuencia, en caso de un evento o desastre, el punto objetivo de recuperación (RPO) de información sería mucho mayor al estimado.

Factor crítico	Riesgo
Políticas y procedimientos institucionales	La carencia de políticas y procedimientos puede ocasionar que no se cuente con instrucciones, medidas de seguridad o mecanismos de control claramente definidos, causando confusiones, mal uso y manejo de los activos y herramientas de Tecnologías de Información y Comunicaciones (TIC) por parte de los usuarios finales y administradores de tecnologías, lo cual podría impactar en la operación de la Secretaría.
Mecanismos de control de incendios	La falta de implementación de dispositivos para el control de incendios puede ocasionar que en caso de presentarse algún incidente no se lleven a cabo acciones con oportunidad que permitan contener el fuego en su zona de origen reduciendo los daños en su entorno más inmediato y evitar la propagación a zonas adyacentes, y en consecuencia presentarse un daño a la infraestructura tecnológica de la SEDENA que pudiera impactar la operación de la misma.
Aire acondicionado y unidades UPS	El no contar con equipo de aire acondicionado y de respaldo para el suministro de energía en buenas condiciones, puede ocasionar que el centro de datos alcance niveles de temperatura elevados o tenga interrupciones de energía, lo cual podría afectar negativamente el rendimiento del equipo y acortar su vida útil; así como afectar la disponibilidad de los servicios e información de la SEDENA.
Replicación del almacenamiento a sitios alternos	Los respaldos están en el mismo predio que los servidores y no son probados sistemáticamente para detectar fallas en la grabación de los datos, aunado a que no son replicados a un sitio alterno fuera del centro de datos, en consecuencia, en caso de un evento o desastre, el punto objetivo de recuperación (RPO) de información sería mucho mayor al estimado.

Además de la SEDENA, conforme a datos de EMEEQUIS, se encontró que en la violación de seguridad cibernética hay cuatro empresas responsables de la ciber vulnerabilidad**: "Decsef sistemas"**, "**Computadoras, Accesorios y Sistemas"**, "**Debug experts" y "M&F Rservices**". Al respecto el portal referido señala que "En una revisión rápida encontramos a tres de las cuatro empresas mencionadas en los contratos públicos que la Plataforma Nacional de Transparencia tiene disponibles".

En este sentido cabe mencionar que entre lo que encontró EMEEQUIS, se tiene que "Decsef sistemas" cuenta con 11 contratos: 9 para la SEDENA, uno para la Junta de Caminos del Estado de México y otro para el Instituto de Planeación Integral del Municipio de Chihuahua. Por otro lado, "Computadoras, Accesorios y Sistemas" tiene 63 contratos para diversas dependencias e instituciones como SEDENA, IPN, Banxico, Marina, UAM y Universidades Tecnológicas. "Debug Experts" no se queda atrás pues tiene 15 contratos con el Senado, el Consejo de la Judicatura Federal, el Tribunal Electoral del Poder Judicial y Coneval, todos ellos celebrados entre 2019 y

2022. Lo anterior, se traduce en una amenaza continua a la seguridad cibernética, económica y a la estabilidad democrática de nuestras instituciones.

Lo anteriormente descrito resulta preocupante no sólo por la afectación a las instituciones en materia de seguridad nacional, si no porque como ha quedado expuesto, las empresas involucradas en las omisiones a recomendaciones en materia de ciberseguridad prestan servicios a otras dependencias y entidades de la administración pública, lo que expone a millones de mexicanas y mexicanos que entregan sus datos personales a dichas entidades y que se encuentran vulnerables a ataques cibernéticos.

Por otro lado, cabe apuntar que el 16 de diciembre de 2019, la Secretaría de la Defensa Nacional negó la realización de todo tipo de contratos con la empresa Antsua o personas morales vinculadas a los proveedores del equipo de vigilancia y espionaje Pegasus. Esto pues, la Secretaría de la Defensa Nacional respondió dentro de la solicitud de información pública con folio 0000700340519 que "después de realizar una búsqueda exhaustiva en los archivos de esta Secretaría no se encontró evidencia documental que permita atender su requerimiento resultando aplicable el criterio 07/17, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales." Sin embargo, la información revelada por el grupo Guacamaya evidenció que en ese mismo año se compró equipo de vigilancia a una empresa proveedora de Pegasus. Es decir, la Secretaría de la Defensa Nacional faltó a la verdad.

Al respecto, el 4 de octubre de 2022, al ser cuestionado el presidente sobre las actividades de espionaje realizadas por las Fuerzas Armadas con el sistema Pegasus, si bien negó formalmente que el ejército espíe a periodistas, defensores de derechos humanos y opositores, reconoció expresamente que las Fuerzas Armadas intervienen comunicaciones en labores de inteligencia.

Lo anterior resulta ilegal puesto que, conforme a la Ley Orgánica de la Administración Pública Federal, no existe fundamento legal alguno que permita que las Fuerzas Armadas realicen trabajos de inteligencia e intervención de comunicaciones. Por el contrario, con fundamento en el artículo 30 bis, fracción XVII, es facultad exclusiva de la Secretaría de Seguridad y Protección Ciudadana "organizar, dirigir y supervisar bajo su adscripción al Centro Nacional de Inteligencia, el cual fungirá como un sistema de investigación e información, que contribuya a preservar la integridad, estabilidad y permanencia del Estado mexicano, así como contribuir, en lo que corresponda al Ejecutivo de la Unión, a dar sustento a la unidad nacional, a preservar la cohesión social y a fortalecer las instituciones de gobierno."

En este sentido, con base en las declaraciones del presidente, la SEDENA estaría actuando ilegalmente y violando derechos humanos de las personas cuyas comunicaciones han sido intervenidas. Lo anterior además implica que se desconoce si es que existen autorizaciones judiciales que hayan permitido la intervención de comunicaciones, conforme al marco jurídico vigente. Por tanto, es necesario que se informe si algún juez de control ha autorizado dichas intervenciones y bajo cuál marco jurídico; y, en caso contrario, deben informar si lo han hecho por cuenta propia, sin autorización y sin marco legal alguno.

De acuerdo con el National Cyber Security Index 2022, México está en el lugar 84 de 160 de los países y sus medidas de seguridad implementadas por sus gobiernos centrales. Un reporte de la compañía de ciberseguridad Fortinet reveló que, en el primer semestre del año, la región de América Latina y el Caribe sufrió 137 mil millones de intentos de ciberataques. De estos, México fue el país más atacado de la región con 85 mil millones.

Ante ello, las y los legisladores que integramos la Bancada Naranja consideramos que la filtración de 6 TB de información clasificada como confidencial de la Secretaría de la Defensa Nacional por parte del grupo de hackers denominado "Guacamaya", ha puesto en grave riesgo la seguridad nacional, por lo que exhortamos al Titular de la Secretaría de la Defensa Nacional a que haga público un informe detallado sobre el estado que guarda el reciente

ciberataque realizado a la Secretaría a su cargo. Asimismo, consideramos oportuno que el titular antes referido, comparezca a la brevedad ante esta Soberanía para que dé cuenta sobre dicho ciberataque ocurrido el pasado 29 de septiembre de 2022.

Por lo anteriormente expuesto, se somete a consideración de la Cámara de Diputados del Honorable Congreso de la Unión la siguiente proposición con:

Punto de Acuerdo

Primero. La Cámara de Diputados exhorta, respetuosamente, al titular de la Secretaría de la Defensa Nacional a que haga público un informe detallado sobre el estado que guardan las investigaciones relativas al ciberataque que recibió la Secretaría de la Defensa Nacional el pasado 29 de septiembre de 2022, así como sobre supuestas labores de inteligencia conforme a lo expresado por el Titular del Poder Ejecutivo, indicando el sustento legal de las mismas, así como las autorizaciones judiciales que se han obtenido para tales fines.

Segundo. La Cámara de Diputados exhorta, respetuosamente, al titular de la Secretaría de la Defensa Nacional a que tome las medidas de infraestructura y financieras necesarias para asegurar que el ciberataque no vuelva a suceder.

Tercero. La Cámara de Diputados exhorta, respetuosamente, a la Junta de Coordinación Política de la Cámara de Diputados para que, con base a sus respectivas competencias legales, cite al Secretario de la Defensa Nacional a sostener una reunión de trabajo con integrantes de los grupos parlamentarios de la Cámara de Diputados a fin de que dé cuenta sobre el ciberataque que recibió la Secretaría de la Defensa Nacional durante los meses pasados.

Cuarto. La Cámara de Diputados exhorta, respetuosamente, a la Comisión de Defensa Nacional de la Cámara de Diputados para que, con base a sus respectivas competencias legales, cite al Secretario de la Defensa Nacional a sostener una reunión de trabajo con integrantes de los grupos parlamentarios, a fin de que dé cuenta sobre el ciberataque que recibió la Secretaría de la Defensa Nacional durante los meses pasados.

Quinto. La Cámara de Diputados exhorta, respetuosamente, a la Secretaría de la Defensa Nacional a que cumpla con las recomendaciones emitidas por la Auditoría Superior de la Federación en cuanto a la ciberseguridad de la citada Secretaría y garantice los recursos humanos, financieros y materiales necesarios para evitar nuevas amenazas.

Sexto. La Cámara de Diputados exhorta, respetuosamente, a la Secretaría de la Defensa Nacional a que cumpla con las recomendaciones emitidas por Comisión Nacional de Derechos Humanos sobre violaciones a derechos humanos perpetuadas por militares y garantice que estas no vuelvan a suceder.

Notas

1 Hackean al Ejército: Latinus revela documentos sobre seguridad, contratos y salud de AMLO, Animal Político, 29 de septiembre de 2022, recuperado de:

https://www.animalpolitico.com/2022/09/hackean-ejercito- latinus-documentos/

2 Ibídem

3 Loret Capítulo 96, Latinus, 29 de septiembre de 2022, recuperado de:

https://latinus.us/2022/09/29/loret-capitulo-96/

4 https://m-x.com.mx/al-dia/que-es-el-grupo-guacamaya-y-que-datos-sensibles-filtro-de-la-sedena

5 “Varios hackers ya habían infectado a la SEDENA antes de Guacamaya”, El Economista, 2022

https://www.eleconomista.com.mx/tecnologia/Varios-hackers-ya-habian-infectado-a-la-Sedena-antes-de-Guacamaya-20221003-0070.html

6 Ibídem

7 Hackeo: desde 2021 ASF reprobó a SEDENA por deficiencias graves en ciberseguridad, EMEEQUIS, 30 de septiembre de 2022, recuperado:

https://m-x.com.mx/al-dia/hackeo-desde-2021-asf-reprobo-a-sedena-por-deficiencias-graves-en-ciberseguridad

8 Ibídem

9 @padaguan. (2022). Publicación de la red social Twitter. Twitter. Recuperado de:

https://twitter.com/padaguan/status/1577057428528824 320/photo/1

10 Versión estenográfica de la conferencia de prensa matutina del Presidente Andrés Manuel López Obrador, 4 de octubre de 2022, disponible en

https://lopezobrador.org.mx/2022/10/04/version-estenogra fica-de-la-conferencia-de-prensa-matutina-del-presidente-andres-manuel- lopez-obrador-826/

11 National Cyber Security, Inbox, octubre de 2022, recuperado de: https://ncsi.ega.ee/country/mx/

Dado en el Palacio Legislativo de San Lázaro, a 6 de octubre de 2022.

Diputado Jorge Álvarez Máynez (rúbrica)