PROYECTO DE DECLARACION

La Honorable Cámara expresa su preocupación por los constantes ataques informáticos y vulneraciones de ciberseguridad sufridos por diversos ministerios, organismos públicos y entes estatales de la República Argentina en los últimos años, los cuales han puesto en riesgo la integridad de bases de datos oficiales, la privacidad de los ciudadanos, el funcionamiento del Estado y la soberanía tecnológica nacional.

Asimismo, insta a las autoridades competentes a reforzar las medidas de prevención, detección y respuesta ante incidentes cibernéticos, a implementar estándares internacionales de ciberseguridad en la infraestructura pública, y a garantizar la protección de la información crítica del Estado y de los datos personales de la ciudadanía.

Firmante: Gerardo Milman.

Co firmante:

-Silvana Giudici.

FUNDAMENTOS:

Señor presidente;

El presente proyecto de declaración tiene por objeto manifestar la preocupación institucional del Congreso de la Nación ante la creciente frecuencia y gravedad de los ataques cibernéticos dirigidos contra dependencias del Estado nacional, muchos de los cuales han implicado la filtración, secuestro o destrucción de información sensible.

Casos mas destacados en nuestro país:

En el año 2020, en plena cuarentena por el coronavirus, un ransomware (en la jerga, un secuestro virtual de datos), afecto el sistema de ingresos y egresos de la Dirección Nacional de Migraciones (DNM). Los ciberdelincuentes solicitaban una millonaria suma en dólares para no hacer públicos los registros que tenían en su poder.

Al año siguiente, el Registro Nacional de las Personas (RENAPER), sufrió un ataque al filtrarse más de 60 mil datos de su base.

El año pasado, también ocurrió un hecho similar cuando la Agencia Nacional de Seguridad Vial (ANSV) advirtiera que un usuario de la red social X (ex Twitter) comentaba que en un canal de la aplicación de mensajería Telegram se ofrecía para la venta un lote de 1,2 terabytes de información.

Dicho lote incluía los datos de las licencias de conducir que fueron extraídas de la Dirección Nacional de Registros de la Propiedad Automotor (DNRPA), incluían los datos del presidente de la Nación, ministros y otras personalidades públicas.

Asimismo, se registraron otros ataques, que han tenido diversos grados de repercusión mediática, como han sido la filtración de datos de los afiliados de la Obra Social de las Fuerzas Armadas o el secuestro virtual de datos PAMI. El ciberataque o hackeo a la Comisión Nacional de Energía Atómica (CNEA) fue detectado el 27 de noviembre de 2024, afectando sus

sedes en todo el país y provocando la pérdida de información en el Centro Atómico Bariloche.

También el sitio web Argentina.gob.ar / Mi Argentina, junto con SUBE y otros sitios estatales, fue víctima de un ataque de tipo *defacement* el 25 de diciembre de 2024, con mensajes ofensivos y desconexión de servicios durante más de una hora.

Mas recientemente, en mayo del presente año, se abrió una investigación por un posible acceso ilegal a datos de aproximadamente **50.000 agentes del Ejército Argentino**, incluidas identificaciones personales; continúa la pesquisa sobre su veracidad y alcance de este.

En el día de la fecha, sitios que alertan sobre incidentes, vulnerabilidades o ataques virtuales, alertan sobre la filtración de datos de la Secretaria de Niñez y Adolescencia (PBA) que contienen 460.000 archivos de casos, incluyendo registros de menores.

En enero de 2025, desde el Ministerio de Seguridad Nacional, se lanzó el programa de Fortalecimiento en Ciberseguridad e Investigación del Cibercrimen (ForCIC). Este plan, oficializado mediante la Resolución 19/2025, tiene como objetivo central mejorar las capacidades de prevención, detección e investigación de delitos informáticos. La medida, impulsada por la ministra de Seguridad Dra. Patricia Bullrich, apunta a responder a los recientes episodios de incidentes cibernéticos que evidenciaron fallas de seguridad graves en la protección de infraestructuras críticas y datos sensibles.

Según un informe de Fortinet estima que durante el primer trimestre de 2024 Argentina recibió más de **260 millones de intentos de ciberataque**, ubicándose como el **tercer país de América Latina** con mayor cantidad de ataques virtuales.

Estos hechos ponen de relieve vulnerabilidades persistentes en la infraestructura digital del Estado, con potenciales impactos sobre la

privacidad ciudadana, el funcionamiento institucional y la seguridad nacional.

Este fenómeno no es exclusivo de nuestro país, pero la falta de inversión sostenida, la obsolescencia de sistemas, y la fragmentación de las políticas de ciberseguridad han dejado a muchas dependencias estatales en situación de extrema vulnerabilidad. A ello se suma la escasa cultura organizacional en torno a la seguridad digital, el bajo cumplimiento de protocolos mínimos de protección, y la dificultad para retener talento especializado en el sector público.

Los ciberataques representan hoy una amenaza directa a la seguridad nacional, afectando no solo a estructuras administrativas, sino también a áreas sensibles como defensa, salud, justicia, finanzas, y registros de identidad. La filtración de bases de datos personales, la exposición de expedientes judiciales o la manipulación de sistemas de control estatal, no sólo erosionan la confianza pública, sino que debilitan al propio Estado frente a actores criminales o intereses externos.

En este sentido, corresponde que esta Honorable Cámara exprese su preocupación por los reiterados incidentes, y exhorta a las autoridades competentes en la materia, a adoptar medidas urgentes, sostenidas y coordinadas, como la centralización de estándares de seguridad, la capacitación del personal público en seguridad digital, y la implementación de infraestructura soberana y resiliente.

Por lo expuesto, solicito a mis pares el acompañamiento del presente proyecto de declaración.

Firmante: Gerardo Milman.

Co firmante:

-Silvana Giudici.