INICIATIVA QUE ADICIONA EL ARTÍCULO 39 DE LA LEY ORGÁNICA DEL CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS, SUSCRITA POR EL DIPUTADO JUSTINO EUGENIO ARRIAGA ROJAS, DEL GRUPO PARLAMENTARIO DEL PAN

El suscrito, diputado Justino Eugenio Arriaga Rojas, integrante del Grupo Parlamentario del PAN, en la LXV Legislatura, con fundamento en lo dispuesto en el artículo 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; 6, numeral 1, fracción I, 77 y 78 del Reglamento de la Cámara de Diputados, somete a consideración de la Comisión Permanente la presente **iniciativa con proyecto de decreto por el que se adiciona la fracción XXVII, del numeral 2, del artículo 39, de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos, recorriéndose las subsiguientes en su orden, para crear la Comisión de Inteligencia Artificial y Ciberseguridad;** al tenor de la siguiente:

Exposición de Motivos

Objetivo de la iniciativa

La presente iniciativa tiene como propósito reformar el artículo 39, numeral 2, fracción XXVII, de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos, para crear la Comisión de Inteligencia Artificial y Ciberseguridad.

Antecedentes

A mediados del siglo XX, la computación surgió como un elemento innovador que pronto inició un cambio irreversible en la vida del ser humano.

Hasta antes de la década de los años cincuenta del siglo pasado, la computación no era conocida, ni se había extendido su uso en el común de la población y tampoco se vislumbraba, de manera generalizada, el enorme impacto que tendría en las décadas posteriores.

Hasta 1950, las pocas computadoras que existían tenían capacidades muy limitadas; eran de proporciones gigantescas que inhibían su comercialización; tenían costos estratosféricos que hacían imposible que la población las adquiriera y si bien podían ejecutar comandos, no podían guardar información, ni recordar lo que hicieron, ni aprender de esos procesos.

Pero hubo algunas personas visionarias que previeron que las computadoras tenían un brillante futuro y que advirtieron sobre la importancia que tendrían para la vida común. Uno de ellos fue Alan Turing, quien en 1950 inició un artículo intitulado *Computing machinery and intelligence,* preguntando: “¿Las máquinas pueden pensar?”**1**

Turing fue el primer científico en cuestionarse sobre la capacidad de las máquinas para procesar mecanismos de aprendizaje y de razonamiento. El inventor de Bombe, la máquina diseñada para desencriptar los mensajes del ejército alemán encriptados con la máquina conocida como Enigma, pensaba que las computadoras podrían dar, mediante procesos matemáticos, respuestas certeras a cuestionamientos concretos.

Bombe, además de haber sido pieza clave para que los aliados ganaran la Segunda Guerra Mundial, también fue la precursora de la computadora programable electrónica digital.**2**

Otros desarrollos en la materia fueron pronto implementados: a mediados de la década de los años 1950, específicamente en 1956, se llevó a cabo el Proyecto de investigación de verano sobre inteligencia artificial de Dartmouth (DSPRAI), que ayudó a que la innovación creciera y que las computadoras se volvieran más rápidas, económicas, accesibles y que tuvieran mayores capacidades. Este proyecto es considerado por muchos expertos como el fundador de la inteligencia artificial como campo de investigación y aplicación.**3**

Poco a poco, los siguientes veinte años, de la década de los años 50 a la de los años 70, la investigación en materia informática avanzó a pasos agigantados y se concretaron desarrollos importantes, mejorándose la capacidad de las computadoras de manera ostensible, así como mejorando los algoritmos de aprendizaje automático, pero sin lograr aún la plena consolidación de esquemas de inteligencia artificial, tal y como los conocemos en la actualidad.

Llegaron entonces los años 1980 y, con ellos, John Hopfield y David Rumelhart trabajaron en una de las principales dificultades que enfrenta la inteligencia artificial: que muchos de los factores de variación influyen en cada dato que podemos observar. Extraer características abstractas de tan alto nivel que no nos interesan de los datos sin procesar puede ser muy difícil. Hopfield y Rumelhart popularizaron, así, las técnicas de aprendizaje profundo que permitieron que las computadoras aprendieran usando la experiencia, pues encontraron que el aprendizaje profundo resuelve este problema central en representaciones que se expresan en términos de otros.**4**

Otro aporte importante fue el de Edward Feigenbaum, quien en 1992 introdujo los Sistemas Expertos, que imitaban la toma de decisiones de los seres humanos. Para Feigenbaum, la mayoría de las aplicaciones de inteligencia artificial son de un tipo llamado Sistemas Expertos:

> *"Most applications of the Artificial Intelligence (AI) science and technology are of a type called Expert Systems. An Expert System (ES) is a computer program that reasons using knowledge to solve complex problems. This overly brief caricature will be expanded upon below, but it serves to indicate an alignment of ES with AI's long term goals. Traditionally, computers solve complex problems by arithmetic calculation (not reasoning using logic); and the knowledge needed to solve the problem is known only by the human programmer and used to cast the solution method in terms of algebraic formulas."* **5**

A partir de entonces y en las siguientes dos décadas, el *software* de las computadoras evolucionó a pasos agigantados. En 1997, Deep Blue, desarrollada por IBM, logró lo que parecía imposible, derrotar en una partida de ajedrez, al campeón mundial Gary Kasparov.**6**

En las primeras dos décadas del siglo XXI, la computación, el internet, la inteligencia artificial, el *machine learning* y el *deep learning* han cambiado la faz de la tierra, creando aplicaciones que logran lo que el ser humano solamente podía soñar e, incluso, creando un ciberespacio y un metaverso que ha crecido de manera exponencial y, paradójicamente, sin control alguno.

Ciberataques, ciberdelincuencia y ciberseguridad

En todo el mundo se han incrementado los ataques cibernéticos, especialmente después del periodo de pandemia por Covid-19, en el que el uso de medios electrónicos se extendió de manera exponencial.

Por ello, existe una gran cantidad de expertos en la materia que han alertado sobre este incremento de ataques cibernéticos y de robo de información, tanto en empresas como en el sector público.

Un reportaje de la revista *Forbes México,* basado en datos de la multinacional Fortinet, indicaba el año pasado que México se ha convertido en un blanco importante para los ciberdelincuentes: "Tan solo durante el primer semestre del año (2021), dijeron, se registraron más de 91 mil millones de intentos de ciberataques en Latinoamérica, de los cuales más de 60,000 millones ocurrieron en México durante el primer semestre de 2021, lo que ubica al país en el primer lugar de la región frente a este tipo de amenazas."**7**

De acuerdo con la pieza periodística antes mencionada, "México ocupó el primer lugar de la región con 67 por ciento de intentos de ataque, seguido por Brasil con 17.8 por ciento y Perú con 5.1 por ciento, según Fortinet."**8**

En mayo de 2021, la Lotería Nacional sufrió un ciberataque, que tuvo como resultado la afectación de 44 sistemas y bases de datos, de los cuales cinco eran de criticidad alta (11.4 por ciento), 24 de criticidad media (54.5 por ciento) y 15 de criticidad baja (34.1 por ciento). Lo cual impidió la operación del organismo de 27 a 77 días.**9**

En 2022 se reveló que varias dependencias han sido atacadas por ciberdelincuentes. Entre los casos más difundidos y graves están los ataques a la Secretaría de la Defensa Nacional (Sedena), conocidos como *Guacamaya Leaks* y a la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT).

En el primer caso, a finales de septiembre de 2022, se hizo público que un grupo de *hackers* vulneró las ciberdefensas de la Sedena, obteniendo seis terabytes de información, documentos y correos electrónicos, que revelan detalles de la operación y alcances del Ejército Mexicano**10**

Esta información fue entregada a los medios de comunicación, los que tuvieron libre acceso a ella para investigar sobre cualquier tema que les interesara y, posteriormente, publicar reportajes.

En el segundo caso, la SICT fue atacada a finales de octubre de 2022. El 24 de octubre, la SICT difundió a través de su cuenta de Twitter que había “activado el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos y Plan de Contingencia, en apego a la normatividad, a fin de contener posibles vulnerabilidades a la información y datos derivado de accesos ilícitos a equipos informáticos de la SICT” y señaló que “Las investigaciones se encuentran en curso y de acuerdo con el resultado se denunciará y dará vista a las autoridades correspondientes”**11**

Este ataque parece haber sido del tipo *ransomware* , es decir, uno que busca acceder a los sistemas para bloquear el acceso a la información en ellos contenida y solicitar una cantidad en criptoactivos para liberar los datos secuestrados.

Esto obligó a que la SICT publicara en el Diario Oficial de la Federación del 1 de noviembre de 2022, un acuerdo que establece la suspensión de plazos y términos de diversos trámites y licencias de la propia dependencia y de la Agencia Federal de Aviación Civil, entre el 24 de octubre y el 31 de diciembre de este año.

Pero estas dependencias y entidades no son las únicas que han sido atacadas en los últimos años, pues en el gobierno federal, se han hecho públicos, al menos, ciberataques a los sistemas de la Secretaría de la Función Pública (SFP) y del Instituto de Seguridad Social al Servicio de los Trabajadores del Estado (ISSSTE).

Pero no todos los ciberataques o ciberdelitos consisten en el acceso ilícito a sistemas. Existe una gran cantidad de conductas delictivas que pueden ser ejecutadas por ciberdelincuentes a través del internet y las redes sociales.

Así, la pornografía infantil en el ciberespacio es el delito de mayor incidencia turnado a investigación cibernética a las autoridades competentes en México, sin que hasta el momento contemos con un marco legal robusto que permita prevenirlo, investigarlo y sancionarlo.

De acuerdo con información proporcionada por la Guardia Nacional a la Cámara de Diputados,**12** en el marco de la glosa del Segundo Informe de Gobierno del presidente de la República, entre el 1 de septiembre de 2019 y el 30 de junio de 2020, la pornografía infantil, fue el ciberdelito más denunciado en el país, con 28 por ciento de las investigaciones.

Lejos de la pornografía infantil, en el segundo lugar de incidencia de ciberdelincuencia se encontró el secuestro, con 14 por ciento; la trata de personas y la desaparición de personas, con nueve por ciento cada uno y los fraudes electrónicos con cuatro por ciento.

Esta alta incidencia de ciberdelincuencia enfocada en la pornografía infantil y la trata de personas generó que la Guardia Nacional implementara la “Operación Nacional Ciberguardián” y el “Operativo Salvación”, con el fin de prevenir e investigar estos delitos.

De acuerdo con los datos de la Guardia Nacional, de septiembre de 2019 a junio de 2020, hubo 12 mil 713 reportes ciudadanos de posibles ciberdelitos, pero el número de incidentes contra la seguridad informática se elevó hasta 98 mil.

En el mismo sentido, el Censo Nacional de Seguridad Pública Federal 2021, del Instituto Nacional de Estadística y Geografía (Inegi), coincide en que, durante 2020, la Guardia Nacional realizó mil 104 ciberinvestigaciones, en las que los casos de pornografía infantil y trata de personas fueron los más recurrentes.**13**

Además, de acuerdo con el informe de cibercrimen de América Latina, de Lexis Nexis, México ocupa la sexta posición de los países con mayores ataques cibernéticos.**14**

Todos estos datos y cifras son claramente indicativos de que la seguridad en el ciberespacio se ha convertido en una prioridad para el país y que su tratamiento requiere personal especializado en la materia, pues, aunque los ciberdelitos podrían considerarse un ámbito específico de la inseguridad, la realidad es que estas conductas tienen su propia dinámica, sus propias particularidades y hasta sus propias regulaciones a nivel internacional, como, por ejemplo, el Convenio de Budapest.

Por ello, contar con regulación jurídica adecuada y especializada para prevenir, investigar y sancionar estos delitos de ciberdelincuencia, es fundamental, pues de otro modo, las autoridades investigadoras y las jurisdiccionales se encontrarán en desventaja frente a las organizaciones de ciberdelincuentes que operan en todo el mundo a través del internet.

Inteligencia artificial

Pero este panorama se complica aún más cuando nos percatamos de que en las antípodas ciberseguridad-ciberdelincuencia la mera acción humana está dejando de ser el elemento principal, ya que el uso de programas de inteligencia artificial, *machine learning* y deep learning está cambiando por completo la correlación de fuerzas.

La inteligencia artificial se define, en su forma más general, como programas de computación diseñados para realizar determinadas operaciones que se consideran propias de la inteligencia humana, como el autoaprendizaje.

La inteligencia artificial está ligada, evidentemente, a los avances que han tenido los sistemas informáticos, la internet y el uso de dispositivos, sensores y herramientas que pueden ser utilizadas por las computadoras para detectar su entorno y decidir una acción determinada.

Dentro de las acciones y tareas que utilizan inteligencia artificial hoy en día, podemos encontrar, al menos, los siguientes:

- Las soluciones integradas;
- El procesamiento de habla y lenguaje;
- La videovigilancia y análisis de vídeo;
- La conducción autónoma;

- El reconocimiento facial;

- Entre otros.

La inteligencia artificial, como conjunto de técnicas predictivas y de autoaprendizaje está jugando un doble papel en la actualidad: por un lado, está ayudando a mejorar la ciberseguridad y por el otro, está ayudando a los ciberdelincuentes a vulnerar más fácilmente los sistemas informáticos y a cometer más fácilmente conductas consideradas dañosas o delincuenciales.

La inteligencia artificial aplicada en ciberseguridad-ciberdelincuencia "recurre a la calibración continua de los algoritmos a medida que se van exponiendo a nueva información. El grado de complejidad y dispersión de los sistemas con los que trabajan las empresas actualmente hace que los medios tradicionales y manuales de vigilancia, supervisión y control de riesgos se hayan demostrado insuficientes."**15**

Las aplicaciones de inteligencia artificial en materia de ciberseguridad son tan amplias como programas existen, pero, de manera resumida, pueden concentrarse en las siguientes:

Thead hunting: identificación de amenazas y neutralización de ciberataques. Las técnicas tradicionales que se apoyan en la identidad o la utilización de indicadores de compromiso (indicators of compromise) se pueden ver mejoradas, cerrando brechas de seguridad al gestionar e interpretar indicadores de comportamiento.

Gestión de vulnerabilidades *(Vulnerability Management).* El número de vulnerabilidades crece cada año y no es suficiente esperar a que los ciberdelincuentes las exploten para reaccionar ante ellas. User and Event Behavioral Analytics (UEBA) permite identificar comportamientos anómalos que señalen la actividad de ciberataques incluso antes de disponer de los parches que corrigen las vulnerabilidades.

Data centers. La IA, como en otros ámbitos en los que actúa, facilita la optimización y monitorización de centros de procesamiento de datos esenciales además de ayudar a detectar amenazas de comportamientos anómalos. Mejora el aprovechamiento de estos recursos y su evolución, con los consecuentes ahorros de costes y reducción de riesgos como, por ejemplo, la caída de los servicios o la ejecución de un software malicioso.

Seguridad en las redes. Tanto en el ámbito de las políticas de actuación frente al comportamiento de los usuarios como en el ámbito más topográfico a la hora de identificar qué procesos corresponden a cada aplicación, la IA permite aprender los patrones de comportamiento del tráfico en la red y recomendar la agrupación de cargas de trabajo, así como la aplicación de políticas de seguridad.

Identificación segura de usuarios *(Securing Authentication).* Tanto para la protección de los usuarios que acceden a nuestros servicios, como al conjunto de elementos que pasa a utilizar, la IA puede identificar el uso de identidades falsas o los ataques de fuerza bruta, confiriendo una barrera adicional al acceso fraudulento a nuestros servicios, más allá de la autenticación de usuarios o el uso de captcha.

Privacidad de la información y *compliance.* La IA ayuda a clasificar de manera automática la información por su nivel de criticidad de cara a distintas regulaciones como la GDPR. Esto implica ahorros respecto a los esfuerzos que actualmente se hacen de forma manual, evitando los riesgos que ello supone.

Bloqueo de bots a partir de su comportamiento. La actividad de los bot sin tener que ser maliciosa consume ancho de banda de nuestros servidores, perjudicando la experiencia de usuario de nuestros verdaderos clientes. La IA permite clasificar la actividad de estos visitantes para limitar su acción."**16**

Pero el uso de la inteligencia artificial no está limitado a cuestiones de ciberseguridad o de ciberdelincuencia, también existen cientos de miles de aplicaciones que están disponibles de prácticamente cualquier persona, por lo que cada día se vuelve más importante e indispensable en la vida común.

La inteligencia artificial y la ciberseguridad son dos grandes ramas del conocimiento que están íntimamente relacionadas y que están provocando cambios profundos en la vida de las personas y en la forma en que el mundo funciona.

Estos avances tecnológicos son fundamentales para mejorar la vida de la gente, pero también pueden provocar graves violaciones a derechos, sesgos discriminatorios y vulneraciones de datos personales y altamente sensibles como los datos biométricos o, incluso, delitos que pongan en riesgo incluso la vida de las personas o la estabilidad de una empresa o de instituciones gubernamentales.

En este contexto, es bastante evidente que, como se ha mencionado en el cuerpo de esta iniciativa, la gestión de riesgos y la prevención, así como la sanción de ciberdelitos, debe partir de una adecuada normativa y, para ello, se requiere que el poder que expide las leyes, el legislativo, cuente con órganos especializados en la materia.

En la actualidad, al revisar la composición de las comisiones ordinarias de la Cámara de Diputados del honorable Congreso de la Unión, podemos apreciar que no existe ninguna especializada en temas de inteligencia artificial ni de ciberseguridad y que ello provoca que las iniciativas y proposiciones sobre estos temas se puedan turnar de manera indistinta a las comisiones de Ciencia, Tecnología e Innovación; a la de Justicia; a la de Defensa Nacional; o a la de Seguridad Ciudadana.

Ante esta indeterminación, vale la pena reconocer que el desarrollo y cada vez mayor uso de la inteligencia artificial y la cada vez mayor incidencia de ciberataques y ciberdelincuencia, así como la imperiosa necesidad de garantizar la seguridad en el ciberespacio para todas las personas que habitan en este país y que acceden a aquél, nos exigen que la Cámara de Diputados del honorable Congreso de la Unión cuente con una comisión especializada en los temas relacionados con este campo.

Propuesta

Por lo anterior, la presente iniciativa propone crear una nueva comisión, denominada Comisión de Inteligencia Artificial y Ciberseguridad, en la Cámara de Diputados del honorable Congreso de la Unión.

Esto tiene como finalidad que dicha Cámara cuente con un órgano y con personal especializado en materia de ciberseguridad y de inteligencia artificial y todos los temas que le están relacionados, como el machine learning, el deep learning, las redes neuronales, el ciberespacio, el metaverso, etcétera, buscando que las propuestas legislativas que se presenten, que cada vez son más frecuentes, sean dictaminadas de manera congruente y consistente con una visión técnica que es indispensable en esta materia.

En esa tesitura, se propone adicionar una fracción XXVII al numeral 2 del artículo 39, de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos, recorriéndose las subsiguientes en su orden.

De aprobarse esta iniciativa, la Cámara de Diputados estará dando un paso muy importante hacia la construcción de un andamiaje jurídico especializado en esta materia y en estos temas de frontera.

Cuadro comparativo

Para ilustrar de mejor manera la propuesta, a continuación, se presentan las modificaciones en el siguiente cuadro comparativo:

Texto vigente	Texto propuesto
Ley Orgánica del Congreso General de los Estados Unidos Mexicanos	
ARTICULO 39. 1. Las Comisiones son órganos constituidos por el Pleno, que a través de la elaboración de dictámenes, informes, opiniones o resoluciones, contribuyen a que la Cámara cumpla sus atribuciones constitucionales y legales.	**ARTICULO 39.** 1. …
2. La Cámara de Diputados contará con las comisiones ordinarias y especiales que requiera para el cumplimiento de sus funciones.	2. …
Las comisiones ordinarias serán:	…
I a XXVI. …	I a XXVI. …
No existe correlativo	XXVII.- **Inteligencia Artificial y Ciberseguridad**;
XXVII.- Justicia;	**XXVIII**.- Justicia;
XXVIII.- Juventud;	**XXIX**.- Juventud;
XXIX.- Marina;	**XXX**.- Marina;
XXX.- Medio Ambiente y Recursos Naturales;	**XXXI**.- Medio Ambiente y Recursos Naturales;
XXXI.- Movilidad;	**XXXII**.- Movilidad;
XXXII.- Pesca;	**XXXIII**.- Pesca;
XXXIII.- Presupuesto y Cuenta Pública;	**XXXIV**.- Presupuesto y Cuenta Pública;
XXXIV.- Protección Civil y Prevención de Desastres;	**XXXV**.- Protección Civil y Prevención de Desastres;
XXXV.- Pueblos Indígenas y Afromexicanos;	**XXXVI**.- Pueblos Indígenas y Afromexicanos;
XXXVI.- Puntos Constitucionales;	**XXXVII**.- Puntos Constitucionales;
XXXVII.- Radio y Televisión;	**XXXVIII**.- Radio y Televisión;
XXXVIII.- Recursos Hidráulicos, Agua Potable y Saneamiento;	**XXXIX**.- Recursos Hidráulicos, Agua Potable y Saneamiento;
XXXIX.- Reforma Política-Electoral;	**XL**.- Reforma Política-Electoral;
XL.- Relaciones Exteriores;	**XLI**.- Relaciones Exteriores;
XLI.- Salud;	**XLII**.- Salud;
XLII.- Seguridad Ciudadana;	**XLIII**.- Seguridad Ciudadana;
XLIII.- Seguridad Social;	**XLIV**.- Seguridad Social;
XLIV.- Trabajo y Previsión Social;	**XLV**.- Trabajo y Previsión Social;
XLV.- Transparencia y Anticorrupción;	**XLVI**.- Transparencia y Anticorrupción;
XLVI.- Turismo;	**XLVII**.- Turismo;
XLVII.- Vivienda, y	**XLVIII**.- Vivienda, y
XLVIII.- Zonas Metropolitanas.	**XLIX**.- Zonas Metropolitanas.
3. Las comisiones ordinarias establecidas en el párrafo anterior, tienen a su cargo tareas de dictamen legislativo, de información y de control evaluatorio conforme a lo dispuesto por los artículos 26, apartado A, párrafo cuarto y 93, párrafo primero de la Constitución, y su competencia se corresponde en lo general con las otorgadas a las dependencia y entidades de la Administración Pública Federal.	3. …

Por lo antes expuesto, el suscrito, somete a consideración de esta Comisión Permanente, la siguiente iniciativa con proyecto de

Decreto por el que se adiciona la fracción XXVII, del numeral 2, del artículo 39, de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos, recorriéndose las subsiguientes en su orden, para crear la Comisión de Inteligencia Artificial y Ciberseguridad.

Artículo Único. Se adiciona la fracción XXVII, del numeral 2, del artículo 39, de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos, recorriéndose las subsiguientes, para quedar como sigue:

Artículo 39.

1. ...

2. ...

...

I a XXVI. ...

XXVII. **Inteligencia Artificial y Ciberseguridad;**

XXVIII. Justicia;

XXIX. Juventud;

XXX. Marina;

XXXI. Medio Ambiente y Recursos Naturales;

XXXII. Movilidad;

XXXIII. Pesca;

XXXIV. Presupuesto y Cuenta Pública;

XXXV. Protección Civil y Prevención de Desastres;

XXXVI. Pueblos Indígenas y Afromexicanos;

XXXVII. Puntos Constitucionales;

XXXVIII. Radio y Televisión;

XXXIX. Recursos Hidráulicos, Agua Potable y Saneamiento;

XL. Reforma Política-Electoral;

XLI. Relaciones Exteriores;

XLII. Salud;

XLIII. Seguridad Ciudadana;

XLIV. Seguridad Social;

XLV. Trabajo y Previsión Social;

XLVI. Transparencia y Anticorrupción;

XLVII. Turismo;

XLVIII. Vivienda, y

XLIX. Zonas Metropolitanas.

3. ...

Transitorios

Primero. El presente decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Segundo. Las erogaciones que se generen con motivo de la entrada en vigor del presente decreto, se cubrirán con cargo al presupuesto autorizado para los ejecutores del gasto responsables para el presente ejercicio fiscal y subsecuentes por lo que no se autorizarán ampliaciones a su presupuesto para el presente ejercicio fiscal ni subsecuentes como resultado de la entrada en vigor del presente decreto.

Notas

1 Alan Turing, el padre de la inteligencia artificial. Ministerio de Cultura Argentina. Disponible en https://www.cultura.gob.ar/alan-turing-el-padre-de-la-inteligencia-arti ficial-9162/

2 Ídem.

3 Ibid. Moor, James. The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years. AI Magazine, Volume 27, Number 4, American Association for Artificial Intelligence, 2006.

4 Duarte de Souza, Camila. Artificial Intelligence, Machine Learning and Deep Learning. Disponible en https://medium.com/analytics-vidhya/artificial-intelligence-machine-learning-and-deep-learning-4473dea47bca

5 Feigenbaum, Edward. Expert Sistems: Principles and Practice. The Encyclopedia of Computer Science and Engineering, 1992, pagina 1.

6 “Deep Blue venció a Kasparov en un campo donde el hombre no tenía rival.” Computer World España. Disponible en https://www.computerworld.es/archive/deep-blue-vencio-a-kasparov-en-un-campo-donde-el-hombre-no-tenia-rival

7 México, primer lugar en ciberataques en Latinoamérica. Forbes México. Disponible en https://www.forbes.com.mx/negocios-mexico-primer-lugar-en-ciberataques-en-latinoamerica/

8 Ídem.

9 Ataque cibernético a Lotería Nacional en 2021, por obsolescencia de equipos y sistemas vulnerables: Auditoría. Animal Político. Disponible en https://www.animalpolitico.com/2022/07/lotenal-ataque-ciberneticos-obso lencia-equipos/

10 Hackers obtienen información de Sedena; revelan enfermedades de AMLO. Política Expansión. Disponible en https://politica.expansion.mx/presidencia/2022/09/29/hackean-sedena-latinus-revelan-enfermedades-de-amlo

11 Todo lo que sabemos sobre el hackeo a la SICT del gobierno de México. El Economista. Disponible en https://www.eleconomista.com.mx/tecnologia/Todo-lo-que-sabemos-sobre-el-hackeo-a-la-SICT-del-gobierno-de-Mexico-20221102-0059.html

12 “Pornografía infantil, primer lugar en ciberdelitos: Guardia Nacional”. MVS Noticias. Disponible en https://mvsnoticias.com/noticias/nacionales/pornografia-infantil-primer -lugar-en-ciberdelitos-guardia-nacional/

13 Pornografía infantil entre los casos de ciberseguridad más investigados en México. NotiPress. Disponible en https://notipress.mx/tecnologia/pornografia-infantil-casos-ciberseguridad-mexico-9270

14 Ídem

15 Inteligencia Artificial: un nuevo hito para la Ciberseguridad. Enzyme. Disponible en https://enzyme.biz/blog/inteligencia-artificial-nuevo-hito-ciberseguridad

16 Ídem.

Dado en la sede de la Comisión Permanente, a 5 de enero de 2023.

Diputado Justino Eugenio Arriaga Rojas (rúbrica)