TDS 02/24
28/11/2024

Doctora
Rosalba Taboada Villasana

La seguridad de la infraestructura crítica y la usabilidad de los sistemas de inteligencia artificial

CURRICULUM VITAE

Rosalba Taboada Villasana cuenta con más de 20 años de experiencia en los sectores público, privado, social, académico, de investigación y organizaciones de interés público, así como es voluntaria en algunas organizaciones de la sociedad civil. Es una profesionista egresada de la UNAM, con formación de Licenciatura y Maestría en Relaciones Internacionales, Doctorado en Administración Pública y Posdoctorado en Estudios Latinoamericanos, Diplomados en Comercio Exterior, Seguridad Nacional, Prevención de las Violencias, Seguridad Ciudadana, Educación para la Paz y Derechos Humanos, cuenta con un conocimiento amplio en el campo social en la realización de diagnósticos, programas, proyectos, investigación y generación de información estratégica.

Ha realizado e implementado política pública en materia social, así como ha contribuido en los estudios y formación de profesionistas en materia de seguridad y sus diversas acepciones, así como en la prevención de la violencia y la delincuencia. Actualmente es Subdirectora de Área en la Subsecretaría de Desarrollo Democrático, Participación Social y Asuntos Religiosos de la Secretaría de Gobernación (SEGOB), en la cual realiza investigación en el campo de mejora regulatoria sobre las acciones para la sociedad civil organizada que lleva a cabo la Dirección General de Vinculación con Organizaciones de la Sociedad Civil (DGVOSC).

La DGVOSC, tiene sus instalaciones en Calle Abraham González N°48, Col. Juárez, Alc. Cuauhtémoc, C.P. 06600, Ciudad de México.

Tel. Of. 55 5128 0000 Ext. 34848

Móvil: 55 6319 9859

Email of. rtaboada@segob.gob.mx

Email pers. rosalba.taboada1301@gmail.com

Breve declaración. Declaró que la presente obra es primigenia, no ha sido publicada y no está siendo considerada para este fin en otro medio de difusión.

SINOPSIS

El evento del 19 de julio de 2024, que causó graves fallas en la infraestructura aeroportuaria debido a problemas en el sistema operativo de Microsoft, pone en evidencia la importancia crítica de la usabilidad de los sistemas de inteligencia artificial (SIA) y los riesgos asociados con su implementación, toda vez que pueden tener consecuencias significativas para la operación de infraestructuras críticas, afectando no solo la eficiencia, sino también la seguridad y la integridad de los procesos.

La relevancia de la usabilidad de los SIA se refiere a la capacidad de estos sistemas para funcionar de manera eficiente y segura en diversas aplicaciones. La integración de la IA en la infraestructura crítica requiere una planificación meticulosa para asegurar que los sistemas sean confiables y estén protegidos contra vulnerabilidades. La crisis mostró la necesidad de robustecer los mecanismos de seguridad y los protocolos de respuesta ante fallas para evitar interrupciones graves en servicios esenciales.

Este análisis resalta la importancia de abordar la usabilidad de los SIA con una combinación de buenas prácticas, regulación internacional, capacitación adecuada y preparación para emergencias, para garantizar que estos sistemas contribuyan de manera positiva a la operación de infraestructuras críticas y a la seguridad general. Dado el rápido avance tecnológico, es crucial que México adapte su estrategia digital de manera continua para abordar nuevas amenazas y oportunidades en el campo de la IA.

PALABRAS CLAVE

Infraestructura crítica, instalaciones estratégicas, seguridad nacional, seguridad internacional, defensa, inteligencia artificial, geopolítica.

ABSTRACT

The event of July 19, 2024, which caused serious failures in airport infrastructure due to problems in the Microsoft operating system, highlights the critical importance of the usability of artificial intelligence systems (AIS) and the risks associated with its implementation, today that can have significant consequences for the operation of critical infrastructures, affecting not only efficiency, but also the security and integrity of the processes.

The relevance of AIS usability refers to the ability of these systems to function efficiently and safely in various applications. Integrating AI into critical infrastructure requires meticulous planning to ensure systems are

reliable and protected from vulnerabilities. The crisis showed the need to strengthen security mechanisms and failure response protocols to avoid serious interruptions in essential services.

This analysis highlights the importance of addressing the usability of AIS with a combination of good practices, international regulation, adequate training and emergency preparedness, to ensure that these systems contribute positively to the operation of critical infrastructure and overall security. Given rapid technological advancement, it is crucial that Mexico continually adapts its digital strategy to address new threats and opportunities in the field of AI.

KEYWORDS

Critical infrastructure, strategic facilities, national security, international security, defense, artificial intelligence, geopolitics.

Los hechos se adelantaron a la prospectiva que había visualizado hace unos tres meses para la parte final del tema titulado: “La infraestructura crítica y la usabilidad de los sistemas de inteligencia artificial”, el desarrollo de la prospectiva sobre los riesgos y amenazas posibles por la usabilidad[1] de los sistemas de inteligencia artificial (SIA)[2], la cual fue presenciada por todo el mundo el pasado 19 de junio de 2024, con las afectaciones de la infraestructura crítica aeroportuaria.

Por lo que ahora partiré apoyándome en la metodología del método deductivo y descriptivo, exponiendo en primer lugar los acontecimientos del pasado 19 de julio de 2024 que marca un parteaguas en lo que se prepara y avecina como nuevo marco internacional en la aplicación de la inteligencia artificial (IA) en la gestión pública gubernamental contemplando las acepciones de la seguridad pública, seguridad nacional y seguridad internacional, principalmente el que brinda la Unión Europea (UE).

Por lo cual se abordará en primer lugar el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho, y en segundo lugar el Reglamento de la Inteligencia Artificial en la UE.

---

[1] Usabilidad en la IA, es comprender su uso, capacidades, funciones y tener el control y generación del mínimo de errores, así como es necesario que satisfaga las necesidades y requerimientos con el menor número de errores y facilidad para que las personas interactúen con los SIA.

[2] De acuerdo al Art. 2° del Convenio, los SIA son sistemas informáticos que deducen a partir de los datos que recibe/alimenta, y que cumplen ciertos objetivos para generar resultados como pronósticos, contenidos, recomendaciones o decisiones. Es probable que influyan en el hardware o en los entornos virtuales. Los diferentes SIA varía en sus niveles de autonomía y adaptabilidad después del despliegue.

En tercer lugar, se analizará el caso de México para abordar la continuidad de la Cuarta Transformación y la transición de México hacia un nuevo diseño institucional en las Fuerzas Armadas Mexicanas y cuerpos de seguridad, así como la seguridad de la infraestructura crítica y lo concerniente a la Administración Pública Federal del Gobierno de México y los retos que se presentan para diseñar una normativa acorde con los requerimientos y en la adopción de prácticas internacionales en la usabilidad y aplicación de los SIA.

Las fallas en la seguridad de la infraestructura crítica aeroportuaria (19 de julio de 2024)

Los acontecimientos del pasado 19 de julio del 2024, expuso los riesgos y amenazas que enfrentó la infraestructura crítica aeroportuaria en sus operaciones a nivel mundial, ocasionados por las fallas en los sistemas informáticos del sistema operativo de Microsoft.

Las afectaciones en la infraestructura crítica aeroportuaria mundial fueron incalculables, no sólo por los retrasos del servicio en el tráfico de personas y de mercancías tanto nacionales como internacionales, que es lo que a primera vista la gente presenció, sino, que va más allá de los despegues, aterrizajes y demoras de las aeronaves para viajar a diferentes destinos.

Los daños a la infraestructura crítica de los aeródromos nacionales e internacionales, se vio afectada en la operatividad de los sistemas migratorios y de comercio, el internamiento y salidas en los puntos de revisión aduanales, en los sistemas de comunicación e intercambio de información, las comunicaciones del tráfico aéreo así como en sus procesos se vieron bloqueadas y sin ningún plan de respuesta emergente de soluciones, más que el resolver de manera práctica los servicios que se ofrecen a las personas usuarias en las instalaciones estratégicas en donde interactúan tanto empresas, giros comerciales y financieros como el sector público gubernamental y oficinas de representaciones internacionales, lo cual, puso en riesgo no sólo la seguridad e integridad de las personas usuarias, sino también se vio vulnerada la seguridad nacional y la seguridad internacional de los Estados.

La infraestructura crítica es vital para el bienestar de la sociedad y la seguridad del Estado, ya que el transporte aéreo, marítimo y terrestre, la probabilidad de objetos e instrumentos espaciales, la producción de energía energética como petróleo, electricidad, centrales nucleares, el suministro de agua, distribución de alimentos, los sistemas de información tecnología que sustentan operaciones gubernamentales, de defensa, comunicaciones y servicios públicos, centros de investigación avanzada, plantas de producción de recursos críticos para la economía, infraestructuras de telecomunicaciones y nodos de conexión a Internet, son estratégicos y cruciales para mantener y preservar la estabilidad, la operatividad y el adecuado funcionamiento de un país. Esto, de igual manera en sus interacciones con el exterior.

Lo anterior, sin dejar de lado, la importancia de los recursos humanos, los cuales deben contar con los conocimientos, herramientas e instrumentos necesarios para el cumplimiento de sus funciones y responsabilidades de acuerdo a sus ámbitos laborales.

Es por ello, que teniendo como referencia este acontecimiento mundial del 19 de julio de 2024, el cual mostró las vulnerabilidades, los riesgos y las amenazas a la infraestructura crítica aeroportuaria. Estas últimas hasta el momento no visibles o dadas a conocer abiertamente hasta este momento en que escribo, dado que existe la posibilidad de que durante esta actualización del sistema operativo de Microsoft, pudiese haber sido aprovechado por personas del crimen organizado/delincuencia organizada y grupos terroristas para cometer varios delitos que son innumerables de describir en este espacio, pero como ejemplos, se encuentra la vulneración de la ciberseguridad, robo de información electrónica y digitalizada que compromete la seguridad y privacidad de los datos personales, robo de identidad, datos biométricos, datos dactilares, datos financieros, sistemas de datos de tráfico de personas y mercancías, seguridad estratégica militar y de defensa de las instalaciones estratégicas, operatividad y funcionamiento de la infraestructura crítica, así como la tecnología y las telecomunicaciones digitales y satelitales, entre otras.

Es a lo que nos enfrentamos ahora, no sólo de manera unilateral sino a nivel mundial, en donde tenemos retos que superar, toda vez que las velocidades en las que se mueve el mundo en el ámbito de desarrollo tecnológico y científico, tienden a ser diferentes y ajenas a los posicionamientos socio ideológicos que hacen mención sobre las características de los países Norte-Sur, Occidente-Oriente, capitalistas-socialistas, democracias-dictaduras, entre otras dicotomías, toda vez que estamos hablando en muchos casos de particulares, de empresas, de organizaciones, de países que invierten en ciencia y tecnología, de think tanks y de monopolios, así como de una nueva configuración geopolítica en el ámbito de la IA.

En este aspecto, la configuración geopolítica nos empuja a reflexionar en las capacidades y el poder nacional del Estado mexicano y los parámetros que está marcando Estados Unidos (EEUU) y la UE principalmente, seguido por Reino Unido, República de Corea, Canadá, Singapur, Brasil, Australia y Japón (ALERT, 2024), así como el sector privado, quienes se encuentran desarrollando ciencia y tecnología, haciéndolos ser los proveedores en la aplicación de los SIA en varios sectores para el desarrollo de las actividades tanto comunes para la sociedad como en los sectores estratégicos vitales para un Estado.

Lo anterior, también nos lleva a deducir que nos estamos acercando a un nuevo sistema de orden mundial en materia de seguridad internacional en relación a la usabilidad de los SIA y los riesgos que conlleva en materia de derecho internacional en la forma de hacer guerra, y lo que concierne en materia de seguridad internacional -como el terrorismo-, la seguridad nacional y la defensa de los Estados, así como los riesgos en los que se exponen.

Sin embargo, también existe otro aspecto importante y que va de la mano con los SIA, estamos hablando de la ciberseguridad, es necesario implementar medidas de seguridad específicas para prevenir y mitigar las vulneraciones, riesgos y amenazas asociadas con la tecnología.

Para abordar el complejo tema de la IA, es importante conocer cómo se ha abordado en otras latitudes -en este caso en particular en la UE- y cuáles son las características más importantes que son necesarias considerarse para una usabilidad de los SIA con responsabilidad, ética y protección de los derechos humanos.

Convenio marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho

El pasado 17 de mayo de 2024, se celebró en Estrasburgo, Francia la firma del Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho (EUROPA, 2024), en la 33ª Reunión de Ministros del Consejo Europeo.

El Convenio, es considerado el primer tratado internacional jurídicamente vinculante destinado a abordar los desafíos específicos que surgen a lo largo del ciclo de vida de los SIA y la importancia de considerar los riesgos e impactos de manera amplia la utilización de estas tecnologías en la salud humana y el medio ambiente, así como en los aspectos socioeconómicos y en las diversas actividades económicas como el empleo y el trabajo.

El Convenio es el resultado de dos años de trabajo, en que se analizaron las problemáticas y necesidades de la UE -que ahora al analizarse no son ajenas al resto de los Estados de la comunidad internacional-, ya que se expuso durante su desarrollo la mejora de la competitividad en sectores estratégicos; el tener una sociedad segura y fiable; el combatir la desinformación; garantizar que las personas tengan el control final en la utilización de la IA; el garantizar la supervisión humana; uso fiable y responsable de la IA; el establecimiento de salvaguardias; la garantía de transparencia; el uso de la IA y las herramientas digitales para mejorar el acceso de los ciudadanos a la información, incluidas las personas con discapacidad (EUROPEO, 2022), a través de un órgano intergubernamental y un Comité sobre Inteligencia Artificial (CAI) teniendo la oportunidad de reunir a los 46 miembros del Consejo Europeo[3].

[3] Además, reunió a 11 Estados no miembros, entre ellos México. Argentina, Australia, Canadá, Costa Rica, Estados Unidos, Israel, Japón, Perú, la Santa Sede y Uruguay, así como a representantes tanto del sector privado, de la sociedad civil y de la académica, quienes participaron como observadores.

El Convenio establece un marco jurídico que abarca todo el ciclo de vida de los SIA, ocupándose de los riesgos que pudieran suscitarse, a su vez, promueve la innovación responsable y adopta un enfoque basado en el riesgo para diseñar, desarrollar, usar y decomisar SIA, exigiendo considerar cuidadosamente cualquier posible consecuencia negativa del uso de estos sistemas.

Asimismo, dicta dos formas de cumplir con los principios estipulados y las obligaciones a las que se comprometen para regular el sector público -incluidas las compañías que actúan en su nombre- y el sector privado. Estos sectores pueden optar por seguir las disposiciones dictadas tal cual se enuncia en la norma, o en su caso, adoptar medidas para cumplir con estas, ya que existen diferencias en los sistemas jurídicos de cada Estado Parte del Convenio.

En cuanto al cumplimiento, se contempla la supervisión y riesgos específicos tomando en consideración la identificación de contenidos generados por SIA. Los Estados Parte deberán adoptar medidas para identificar, evaluar, prevenir y mitigar posibles riesgos y evaluar la necesidad de una moratoria, así como se podrán prohibir o tomar medidas apropiadas en relación con el uso de SIA, cuando los riesgos puedan ser incompatibles con las normas de los derechos humanos. En este aspecto, se deberá garantizar la disponibilidad de recursos legales y procesales para las víctimas, incluida la notificación a todas las personas que interactúen con SIA.

En lo que se refiere a los riesgos en la política, se deberán adoptar medidas para garantizar que no sean utilizados para vulnerar a las instituciones o transgredan los procesos democráticos, incluido el principio de separación de poderes, el respeto de la independencia judicial y el acceso a la justicia.

Los Estados Parte también deberán garantizar la rendición de cuentas y responsabilidad por el impacto negativo de los SIA, salvaguardando siempre la igualdad, el derecho a la intimidad y la prohibición de la discriminación. De hecho, el Convenio insta a que establezcan mecanismos de supervisión independientes para la plena vigilancia de las normas, así como se sensibilice y se estimule el debate público informado, y que se lleven a cabo consultas con múltiples partes interesadas, sobre cómo debería ser utilizada la tecnología de la IA.

En cuanto a los SIA aplicados en materia de seguridad nacional, es importante señalar que los Estados Parte, no están obligados a aplicar las disposiciones en las actividades relacionadas con la protección de los intereses de la seguridad nacional, siempre y cuando se garantice lo siguiente:

1) El respeto del derecho internacional.
2) La salvaguarda y seguridad de las instituciones, y;
3) Los procesos democráticos.

Por ejemplo, en lo que se refiere el primer punto sobre los riesgos que se pueden presentar en el derecho internacional, se refiere a la utilización de los SIA de manera malintencionada o para fines dañinos. Esto podría incluir su uso en ataques cibernéticos, la creación de armas autónomas o la manipulación de información para engañar, influenciar y manipular a las personas.

El segundo y el tercer punto se encuentran dentro de la categoría de los riesgos de la política, mencionados anteriormente.

Por otra parte, no se aplicarán las disposiciones en asuntos de defensa nacional, ni en actividades de investigación y desarrollo, excepto cuando las pruebas de los SIA puedan interferir potencialmente –o sean incompatibles- con las normas de los derechos humanos, la democracia o el Estado de derecho.

Ahora bien, ¿por qué no se aplicarán las disposiciones del Convenio en asuntos de defensa nacional? Hasta hoy en día es un tema de intenso debate a nivel internacional, si bien, los SIA ofrecen beneficios también pueden crear amenazas que son difíciles de predecir cuando su uso es malintencionado. Hemos tenido ejemplos de ciberataques basados en IA contra la infraestructura crítica, contra operaciones humanitarias y de mantenimiento de paz. El crimen organizado/delincuencia organizada/terrorismo han rebasado barreras técnicas y financieras, y ahora se torna más complicado de percibir cuando estas organizaciones criminales se proveen de SIA para conseguir sus fines. Ante esto, se contempla la contrainteligencia con IA, es un gran desafío por enfrentar ante las nuevas modalidades delincuenciales, y frente a los desarrolladores que se retan cada día para estar a la vanguardia en SIA. Por otro lado, se encuentran los Estados que puedan adquirir SIA o ampliar los esfuerzos en la cooperación o colaboración e intercambio de información en la lucha contra el crimen organizado/delincuencia internacional//terrorismo.

En cuanto a continuar ponderando los principios del derecho internacional y el mantenimiento de la seguridad internacional, se ha convenido en la prohibición de los SIA aplicados en armas autónomas letales que funcionen sin control humano, toda vez que pueden tener el potencial de que se haga un uso indebido o sea imprevisible su actuar, "…un SIA nos puede apoyar en comprender la ciencia de la biología, pero también puede servir para crear armas biológicas". La IA no debe utilizarse de forma directa para tomar decisiones de vida o muerte para los seres humanos, además aún no se ha encontrado la forma de protegernos frente a la posibilidad de que la IA pueda aprovecharse de las debilidades humanas. Por tanto, debe aplicarse un control humano eficaz y responsable para garantizar interacciones adecuadas entre el ser humano y la IA (UNIDAS, 2023).

Lo anterior, se ha discutido de manera amplia y exhaustiva en los organismos internacionales de Naciones Unidas, donde no se ha llegado todavía a un consenso para dotar a la comunidad internacional de un marco

normativo internacional. En este espacio no se aborda a fondo por lo extenso que da de sí, sólo el tratar una sola arista.

Pero retomando el Convenio marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho, el cual se encuentra a la vanguardia a nivel internacional junto con su Reglamento, toda vez como ya se mencionó contempla todo el ciclo de vida de los SIA, además de que no sólo es exclusivo para los miembros de la UE, sino que a partir del 05 de septiembre de 2024 -fecha de la Conferencia de Ministros de Justicia del Consejo Europeo en Vilna, Lituania (EUROPEO C., 2024)-, se encuentra abierto para que los países de distintos continentes que comparten los mismos valores, y deseen aprovechar los beneficios de la IA y mitigar sus riesgos, puedan adherirse al Convenio.

El Convenio[4] marca una oportunidad y una guía para el resto de la comunidad internacional, que no cuente hasta el momento con una normatividad en la materia y se encuentre en vías de crearla, o en su caso, integrar algunos aspectos que pudieran complementar las ya existentes.

Sin embargo, tanto el Convenio como el Reglamento repercutirán de manera global al considerar las buenas prácticas internacionales en la usabilidad de los SIA, así como contribuirán en la armonización normativa en la materia.

Es importante considerar que, a la UE le tomó de cinco a seis años el desarrollo de un marco jurídico, permitiéndole contemplar las aristas necesarias para enfrentar las diversas problemáticas en la utilización y aplicación de los SIA. Uno de sus primeros trabajos en la materia fue el desarrollo de una estrategia digital, aprobada el 07 de junio de 2019 (EUROPEO C. , CONSEJO DE LA UE, 2024), aunque existen hitos que fue desde la aprobación de la Declaración de Cooperación en Inteligencia Artificial, del 10 de abril de 2018 (EUROPEA C. , S/F).

[4] El Convenio contiene una introducción y un preámbulo, 8 capítulos y 36 artículos. A mencionar, Cap. I. Disposiciones Generales: Art. 1. Disposiciones generales; Art. 2. Sistemas de inteligencia artificial; Art. 3. Alcance. Cap. II. Obligaciones generales: Art. 4. Protección de los derechos humanos; Art. 5. Integridad de los procesos democráticos y respeto del Estado de derecho. Cap. III. Principios relacionados con las actividades dentro del ciclo de vida de los sistemas de IA: Art. 6. Orientación general; Art. 7. Dignidad humana y autonomía individual; Art. 8. Transparencia y supervisión; Art. 9. Rendición de cuentas y responsabilidad; Art. 10. Igualdad y no discriminación; Art. 11. Privacidad y protección de datos personales; Art. 12. Confiabilidad; Art. 13. Innovación segura. Capítulo IV. Recursos: Art. 14. Recursos; Art. 15. Garantías procesales. Cap. V. Evaluación y mitigación de riesgos e impactos adversos: Art. 16. Marco de gestión de riesgos e impactos. Cap. VI. Aplicación de la Convención: Art. 17. No discriminación; Art. 18. Derechos de las personas con discapacidad y de los niños; Art. 19. Consulta pública; Art. 20. Alfabetización y competencias digitales; Art. 21. Salvaguarda de los derechos humanos existentes; Art. 22. Protección más amplia. Cap. VII. Mecanismo de seguimiento y cooperación: Art. 23. Conferencia de las Partes; Art. 24. Obligación de informar; Art. 25. Cooperación internacional; Art. 26. Mecanismos de supervisión eficaces. Cap. VIII. Cláusulas finales: Art. 27. Efectos del Convenio; Art. 28. Enmiendas; Art. 29. Solución de controversias; Art. 30. Firma y entrada en vigor; Art. 31. Adhesión; Art. 32. Aplicación territorial; Art. 33. Cláusula federal; Art. 34. Reservas; Art. 35. Denuncia, y; Art. 36. Notificación.

Estos esfuerzos de la UE han sido parte de la carrera global para la regulación de la IA, en la generación de conocimiento, en los avances en ciencia y tecnología a través de los centros especializados de estudio e iniciativa privada aglutinados en los think tanks (EUROPEO P. , PARLAMENTO EUROPEO, 2024) llevando la vanguardia los estadounidenses y europeos.

Reglamento de la Inteligencia Artificial en la Unión Europea

El pasado 1° de agosto de 2024 entró en vigor el Reglamento de la Inteligencia Artificial en la Unión Europea (EUROPEA, 2024) del Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho, el cual tiene plazos para su aplicación, por ejemplo:

- A los seis meses, se aplicarán las disposiciones generales y las prohibiciones (1° de febrero de 2025).
- A los nueve meses, la publicación de los códigos de conducta para los SIA de uso general (1° de mayo de 2025).
- A los doce meses, los SIA de uso general puestos en el mercado después de esa fecha le serán aplicables todas las obligaciones previstas. Igualmente será de aplicación el régimen sancionador (1° de agosto de 2025). Además, a partir de esa fecha se establecerán los órganos de gobierno en los miembros de la UE y en toda la Unión.
- A los dos años, entrará en vigor la mayor parte del Reglamento a los SIA de Alto Riesgo. Tanto a los SIA de Alto Riesgo en virtud del Anexo III (EUROPEA U. , 2024) recién comercializados después de la entrada en vigor como a los sistemas que se modifiquen significativamente a partir de entonces (1° de agosto de 2026).
- A los tres años, la aplicación a los proveedores de modelos de IA de uso general, puestos en el mercado antes del primer año de la entrada en vigor del Reglamento. Igualmente, en esa fecha el Reglamento serán de aplicación las obligaciones previstas en él para los SIA de Alto Riesgo (1° de agosto de 2027).

Asimismo, el Reglamento tiene contemplado que para el 2030 -1°de agosto- sean de aplicación las obligaciones a los proveedores y responsables del despliegue de SIA de Alto Riesgo destinados a ser utilizados por las autoridades públicas, y se prevé que antes de que termine el 2030 -31 de diciembre-, que todos los sistemas que contengan componentes de sistemas informáticos de gran magnitud, establecidos por los actos jurídicos incluidos en el Anexo X(EUROPEA U. , EU ARTIFICIAL INTELLIGENCE ACT, 2024), y puestos en el mercado tres años después de la entrada en vigor del Reglamento tendrán que cumplir todas sus prescripciones.

El marco regulatorio define los riesgos y amenazas a la seguridad por la aplicación de los SIA. Las amenazas son consideradas en el marco europeo como prohibiciones (EUROPEA U. , EU ARTIFICIAL INTELLIGENCE ACT, 2024). Por ejemplo, la manipulación subliminal[5]; la explotación de vulnerabilidades[6]; la puntuación social[7]; la evaluación de riesgos y delitos[8]; las bases de datos de reconocimiento facial[9]; la inferencia de emociones[10]; la categorización biométrica[11], y la identificación biométrica en tiempo real[12], estás se consideran una clara amenaza para la seguridad, los medios de vida y los derechos de las personas.

En cuanto los riesgos para los SIA, se definen cuatro niveles.

1) Riesgos inaceptables. Se refieren a las prohibiciones.
2) Alto Riesgo. Los SIA están sujetos a estrictas obligaciones antes de poder comercializarse[13], y deberán cumplir con sistemas adecuados de evaluación y mitigación de riesgos; arrojar datos donde resulten ser discriminatorios; registrar las actividades para garantizar la trazabilidad de los resultados;

[5] Prohibido utilizar IA que manipule o engañe a personas a nivel subconsciente, afectando significativamente du capacidad de tomar decisiones informales y causando daños importantes.

[6] Prohibido utilizar IA que aproveche vulnerabilidades debidas a la edad, discapacidad, o situación socioeconómica, distorsionando el comportamiento y causando daños significativos.

[7] Prohibido utilizar IA para evaluar o clasificar personas basándose en su comportamiento social o características personales, resultando en trato perjudicial o desfavorable injustificado.

[8] Prohibido utilizar IA para predecir la probabilidad de que una persona cometa un delito basándose únicamente en perfiles o características personales. No se aplicará a los SIA utilizados para apoyar la evaluación humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva.

[9] Prohibido crear o expandir bases de datos de reconocimiento facial mediante el respaldo no selectivo de imágenes de internet o grabaciones de CCTV (Circuito Cerrado de Televisión).

[10] Prohibido utilizar IA para inferir emociones en lugares de trabajo o instituciones educativas, salvo por razones médicas o de seguridad.

[11] Prohibido utilizar IA para categorizar personas basándose en datos biométricos que infieran raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida sexual u orientación sexual. Esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos legalmente en el ámbito de la aplicación de la ley.

[12] Prohibido utilizar IA para identificación biométrica a distancia en tiempo real en espacios públicos con fines policiales, salvo que se aplique en: la búsqueda de victimas específicas (secuestros, trata de personas, explotación sexual) o personas desaparecidas; en la prevención de amenazas específicas sustanciales e inminentes contra la vida o seguridad física de las personas, o amenazas de atentados terroristas, y en; la detección, localización identificación o enjuiciamiento de un sospechoso o autor de un delito grave.

[13] Ahora bien, al ser comercializados los SIA al ser comercializados, las autoridades se encargan de la vigilancia del mercado. Los implementadores garantizan la supervisión y el control humanos. Los proveedores cuentan con un sistema de seguimiento posterior a la comercialización. Tanto los proveedores como los implementadores deberán informar sobre incidentes graves y fallos de funcionamiento.

generación de documentación detallada que proporcione toda la información necesaria sobre el sistema y sus fines para ser evaluadas en su cumplimiento; generar información clara y adecuada al implementador; tomar medidas adecuadas de supervisión humana para minimizar el riesgo, y contar con un alto nivel de robustez, seguridad y precisión.

3) Riesgo limitado. Se refiere a los riesgos asociados con la falta de transparencia en el uso de la IA. En este aspecto, los proveedores también deben garantizar que el contenido generado por IA sea identificable.

4) Riesgo mínimo o nulo. Cuando es de carácter gratuito la utilización o aplicaciones de IA (EUROPEA C. , COMISIÓN EUROPEA, 2024).

En los asuntos en materia de seguridad nacional las disposiciones en la aplicación de los SIA son consideradas de Alto Riesgo[14], entre ellos la infraestructura crítica, donde los componentes de los SIA están basados en su gestión, operación, funcionamiento y toda la cadena para proveer y distribuir los insumos y servicios que son vitales para el Estado, así como la protección e integridad física de las infraestructuras críticas y las instalaciones estratégicas, sin menoscabo de la salud, la seguridad de las personas y los bienes.

Asimismo, se encuentran los SIA destinados a ser utilizados por las instancias y autoridades competentes en materia de seguridad, como las fuerzas y cuerpos de seguridad y autoridades judiciales, asi como las instituciones, órganos u organismos responsables y coadyuvantes. Aunado a ello, las herramientas e instrumentos que se utilizan para su operación y funcionamiento. De igual manera los utilizados para realizar las responsabilidades y funciones de los recursos humanos involucrados de acuerdo a su campo laboral.

Lo anterior, obliga a repensar sobre un nuevo modelo de gobernanza, sobre el contrato social[15], la manera de hacer política, las formas de gobierno, los modelos educativos, los mercados laborales y la formas en las que se han caracterizado las guerras y las configuraciones geopolíticas en base a su poder nacional, en este caso, el construido en torno a la tecnología.

[14] De acuerdo al Anexo III, los SIA de Alto Riesgo son: los datos biométricos; las infraestructuras críticas; la educación y formación profesional; el empleo, la gestión de trabajadores y el acceso al autoempleo; el acceso y disfrute de los servicios privados esenciales y de los servicios y prestaciones públicas esenciales; fuerzas y cuerpos de seguridad; gestión de la migración, asilo y el control de fronteras, y; la administración de justicia y procesos democráticos.

[15] La UE considera que se ha vinculado el concepto de IA a los valores fundamentales que constituyen la base de las sociedades, como se refiere Dragoş Tudorache -representante de Rumania en el Parlamento Europeo-, es una manera de expresar el uso y la aplicación de la IA en actividades de desarrollo humano, toda vez, que las personas se hacen más dependientes de productos y aplicaciones digitales con IA, o los servicios digitales y electrónicos que ofrece tanto el sector público como privado.

La continuidad de la Cuarta Transformación y la transición de México hacia un nuevo diseño institucional en las fuerzas y cuerpos de seguridad y la seguridad de la infraestructura crítica.

En el caso de nuestro país, tenemos que desde 2019 con la administración del presidente Andrés Manuel López Obrador (1° de diciembre de 2018 al 1° de octubre de 2024) así como su predecesora la primera presidenta de México, Claudia Sheinbaum Pardo (1° de octubre 2024 al 1° de octubre de 2030), han otorgado nuevas funciones y responsabilidades a las dependencias y entidades de la Administración Pública Federal (APF), en particular a las instituciones militares. Las Fuerzas Armadas de México (Secretaría de Defensa Nacional (SEDENA) integrada por el Ejército y Fuerza Aérea Mexicana, la Secretaría de Marina y la Armada de México), instituciones primigenias de la seguridad nacional tanto terrestre, aérea y marítima, así como de sus límites territoriales.

Hay que recordar que desde el inicio de la administración del gobierno del Presidente Andrés Manuel López Obrador, como mando supremo de las Fuerzas Armadas de México (FAM) atribuyó a las instituciones militares nuevas funciones y responsabilidades en la realización de proyectos y obras asociadas a la infraestructura crítica, como la franja de 30 kilómetros a lo largo de la frontera norte de México; la construcción de la vía del tren para unir el Atlántico con el Pacífico; el desarrollo del Istmo de Tehuantepec con la reconfiguración de las refinerías de Minatitlán, Veracruz y Salina Cruz, Oaxaca; la construcción del Tren Maya; la construcción del aeropuerto internacional Felipe Ángeles; el plan de extracción de petróleo y gas; la modernización de las refinerías del país; la construcción de la refinería de Dos Bocas, Tabasco; la modernización de las plantas hidroeléctricas, y; el desarrollo del programa de energías alternativas, entre otras.

Lo anterior, por considerarse de interés público y de seguridad nacional, la realización de proyectos y obras a cargo del Gobierno de México asociados a infraestructura de los sectores comunicaciones, telecomunicaciones, aduanero, fronterizo, hidráulico, hídrico, medio ambiente, turístico, salud, vías férreas, ferrocarriles en todas sus modalidades energético, puertos, aeropuertos y aquellos que, por su objeto, características, naturaleza, complejidad y magnitud, se consideren prioritarios y/o estratégicos para el desarrollo nacional. (FEDERACION, 2021)

De igual manera, el nuevo diseño institucional que se está planteando en la APF se verá reflejado paulatinamente en el último trimestre de 2024 y en el transcurso del 2025. Toda vez, que las instituciones encargadas de la seguridad como la Guardia Nacional se integrará a la SEDENA, así como se definirán las funciones, facultades y responsabilidades para la consecución de los objetivos en la Secretaría de Seguridad Ciudadana y sus Órganos Desconcentrados, principalmente en el Centro Nacional de Inteligencia (CNI) y en el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SNSP), quienes coadyuvan en la

vigilancia y protección de las instalaciones estratégicas. De igual manera, se dilucirá el papel que desempeñarán las instancias competentes en la procuración de justicia.

Ante este nuevo diseño institucional tanto en su estructura como organización de la APF, en la consecución de los proyectos prioritarios y estratégicos, así como la continuidad y mejora de la Estrategia Digital Nacional (FEDERACION, 2021), se tendrá un impacto significativo en sectores como el transporte aéreo, terrestre, marítimo, espacial, la energías no renovables y renovables, la salud, la agricultura, el abastecimiento del agua de los alimentos -centrales de abasto- movilidad del transporte público y de uso particular, en el sector industrial y en la cadenas de producción, las telecomunicaciones y la tecnología. Todo ello necesario para la supervivencia y preservación de la nación y del Estado. Estas actividades interactúan directa e indirectamente con los ámbitos cívico-militares –de seguridad pública, seguridad interior, seguridad nacional e internacional, al conocerse alguna vulnerabilidad que pudiese impactar en la infraestructura crítica del Estado mexicano.

Por tanto, llegamos al punto nodal, la seguridad de la infraestructura crítica, sin dejar de lado la operatividad y las diversas funcionalidades de las instalaciones estratégicas, no sólo de manera física sino en su conjunto. Es necesario que se cuente con una amplia gama de soporte centradas en personas, sistemas operativos con el uso de tecnologías -máquinas-; soporte a altas densidades de tráfico de información; mantener alta calidad y eficiencia en la movilidad del transporte de personas y mercancías en todos los puntos de entrada y salida tanto terrestre, marítimo y aéreo, e incluso aeronaves no tripuladas -como los drones- el uso de robots y hubiese la probabilidad de objetos e instrumentos espaciales.

La Estrategia Digital en México, requiere avanzar en ciencia y tecnología y mejoras del entorno digital, así como en un marco normativo que acompañe su implementación en los servicios digitales, economía de

datos[16], fiscalidad digital[17], IA[18], conectividad[19], ciberseguridad[20], identificación digital[21], digitalización de la justicia[22] e intercambio digital de la información[23], sin dejar de lado, el respeto de los derechos humanos de las personas usuarias en esta nueva era digital y de SIA.

Conclusiones

Es crucial que se unan esfuerzos mediante la colaboración, cooperación y apoyo internacional para que sea posible desarrollar estándares internacionales que faciliten la interoperabilidad entre diferentes redes y dispositivos, promoviendo así una adopción más amplia de la tecnología.

Por tanto, para mantener, salvaguardar y proteger los intereses nacionales del Estado como se ha visto durante el desarrollo del presente trabajo, es primordial fortalecer el poder nacional en la disposición no sólo de infraestructura crítica sino de todo lo que se requiere para su operatividad y específicamente de las FAM, Marina y Armada de México, la Guardia Nacional y de las instituciones coadyuvantes en la materia.

Si bien, hasta el momento México no ha decidido adherirse a la normativa internacional como es el Convenio de la UE, con el tiempo nos alcanzará y se adoptarán las medidas para una armonización de la normatividad,

[16] La economía de datos se refiere a un mayor intercambio de datos y reutilización de datos entre sectores, entre ellos los estratégicos, como lo es la infraestructura crítica, así como la interoperabilidad de datos en las fronteras, contando con un alto nivel de seguridad, protección y privacidad de la información digital y electrónica.

[17] Adaptación a sistemas fiscales para que las normas rijan las cuestiones tributarias a nivel nacional e internacional y sean diseñadas para aplicarse a las empresas con presencia física en un país, toda vez que los impuestos no se gravan en el país donde se generan los beneficios.

[18] De acuerdo con el Consejo Europeo la inteligencia artificial (IA) es el uso de la tecnología digital para crear sistemas que puedan realizar tareas que por lo general se considera que requieren inteligencia humana.

[19] La conectividad se refiere a la expansión y cobertura de manera eficiente y rápida de gigabit en los sectores estratégicos y socioeconómicos, y cobertura 5G ininterrumpida para t las zonas urbanas y las principales vías de transporte terrestre, así como el acceso a la conectividad que ofrece al menos 100 Mbps para los hogares.

[20] La ciberseguridad debe de ir de la mano en los sistemas de aplicación de IA, toda vez que los riesgos, amenazas y los delitos en número y sofisticación van en aumento, por lo que se debe salvaguardar la integridad, la seguridad y la resiliencia de la infraestructura digital, las redes de comunicación y los servicios.

[21] La identificación digital, se dirige a un almacenamiento de datos de identificación electrónica, incluyendo las firmas digitales interoperables, que tengan el acceso a los servicios digitales públicos, privados y transfronterizos, lo cual coadyuvará en el desarrollo de una cartera digital.

[22] Se requiere para mejorar el acceso a la justicia y aumentar la eficacia y la eficiencia de los procedimientos judiciales a través del uso de las herramientas digitales, sin socavar principios fundamentales como la independencia e imparcialidad de los tribunales.

[23] El intercambio digital de información, particularmente en materia de justicia toda vez que en este caso la UE pone especial énfasis a los actos de terrorismo. Las herramientas digitales contribuirán a detectar los vínculos entre las investigaciones transnacionales y los enjuiciamientos en el ámbito del terrorismo, e informar proactivamente a los Estados miembros sobre los vínculos constatados. Asimismo, se busca simplificar la cooperación con terceros países concediendo a los fiscales de enlace adscritos a Eurojust acceso al sistema de gestión de casos.

toda vez que los flujos internacionales de personas, de mercancías, de servicios, así como el tráfico de información digital y electrónica que se maneja en las relaciones de cooperación, de colaboración, de intercambio de información en diversos aspectos -no sólo de seguridad- obligarán paulatinamente a cumplir con la normativa de la UE, como lo fue en su momento a raíz de los atentados terroristas del 11 de septiembre de 2001 en los Estados Unidos, que ante este acontecimiento provocó un despliegue de disposiciones a nivel internacional en materia de seguridad -infraestructura crítica, instalaciones estratégicas, controles fronterizos, de migración, entre otros-, comenzando con el reconocimiento de datos biométricos, que dio pie en el caso de México de signar en el 2005 una Alianza de Seguridad y Prosperidad de América del Norte en el 2005 -23 de marzo, en Waco, Texas, por Estados Unidos, México y Canadá-.

Por tanto, es un tema que amerita dar seguimiento para cumplir con las expectativas y compromisos internacionales de México con el resto de la comunidad internacional, pero sobre todo, continuar avanzando hacia la Transformación de la gestión de los asuntos públicos con Gobernanza a través de la Estrategia Digital que plantea la Primera Presidenta de México, Claudia Sheinbaum Pardo, así como los cambios a realizarse en el diseño tanto en estructura como organización de las fuerzas y cuerpos de seguridad que deberán adaptarse a las nuevas condicionantes. O en su caso, adoptar buenas prácticas internacionales en materia de la usabilidad de los SIA. Estamos a buen tiempo de configurar una normativa en la materia y una buena oportunidad para adherirse al Convenio, lo cual nos dará la oportunidad de avanzar con la asesoría, cooperación, colaboración e intercambio de información con los Estados Parte del Convenio.

BIBLIOGRAFÍA

ALERT, D. P. (2024). DIGITAL POLICIY ALERT.ORG. Recuperado el 13 de Agosto de 2024, de Regulación de la inteligencia artificial: https://digitalpolicyalert.org/threads/regulating-artificial-intelligence

DOF. (22 de Noviembre de 2021). *DIARIO OFICIAL DE LA FEDERACION*. Recuperado el 06 de Agosto de 2024, de ACUERDO por el que se instruye a las dependencias y entidades de la Administración Pública Federal a realizar las acciones que se indican, en relación con los proyectos y obras del Gobierno de México considerados de interés público y seguridad nacional,: https://dof.gob.mx/nota_detalle.php?codigo=5635985&fecha=22/11/2021#gsc.tab=0

EUROPEA, C. (26 de Junio de 2024). *COMISION EUROPEA*. Recuperado el 06 de Agosto de 2024, de Convenio Marco del Consejo de Europa sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho: file:///C:/Users/rtaboada/Downloads/1_ES_ACT_part1_v2%20(1).pdf

EUROPEA, C. (2024). *COMISIÓN EUROPEA*. Recuperado el 13 de Agosto de 2024, de Dando forma al futuro digital de Europa: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

EUROPEA, C. (S/F). *COMISIÓN EUROPEA*. Recuperado el 08 de Agosto de 2024, de Enfoque europeo de la inteligencia artificial: https://digital-strategy.ec.europa.eu/es/policies/european-approach-artificial-intelligence

EUROPEA, D. O. (13 de Junio de 2024). *Reglamento UE 2024/1689 del Parlamento Europeo y del Consejo de la Unión Europea*. Recuperado el 06 de Agosto de 2024, de DIARIO OFICIAL UNION EUROPEA: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401689

EUROPEA, U. (2024). *EU ARTIFICIAL INTELIGENCE ACT*. Recuperado el 13 de Agosto de 2024, de Anexo III: Sistemas de IA de alto riesgo contemplados en el apartado 2 del artículo 6: https://artificialintelligenceact.eu/es/annex/3/

EUROPEA, U. (Agosto de 2024). *EU ARTIFICIAL INTELLIGENCE ACT*. Recuperado el 13 de Agosto de 2024, de Anexo X: Actos legislativos de la Unión sobre sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia: https://artificialintelligenceact.eu/es/annex/10/

EUROPEA, U. (Agosto de 2024). *EU ARTIFICIAL INTELLIGENCE ACT*. Recuperado el 13 de Agosto de 2024, de Artículo 5: Prácticas de IA prohibidas: https://artificialintelligenceact.eu/es/article/5/

EUROPEO, C. (2024). *CONSEJO DE LA UE*. Recuperado el 07 de Agosto de 2024, de Cronología-Europa digital : https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/timeline-digital-europe/?taxonomyId=271842c3-2535-4f5a-a049-bcdab2758865&taxonomyId=c30a94f1-6111-478c-8572-941ee104fa6a&taxonomyId=6b7901c5-1094-4713-add8-3364400eee98

EUROPEO, C. (05 de Septiembre de 2024). *CONSEJO DE LA UNIÓN EUROPEA* . Recuperado el 06 de Agosto de 2024, de Reunión de ministros: https://www.consilium.europa.eu/es/meetings/gac/2024/09/05-06/

EUROPEO, P. (Mayo de 2022). *PARLAMENTO EUROPEO*. Recuperado el 06 de Agosto de 2024, de Conferencia sobre el Futuro de Europa: Informe Final: https://conference-followup.europarl.europa.eu/cmsdata/267106/Report_ES.pdf

EUROPEO, P. (27 de Marzo de 2024). *PARLAMENTO EUROPEO*. Recuperado el 2024, de Briefing. What Think Tanks are Thinking: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760389/EPRS_BRI(2024)760389_EN.pdf

FEDERACION, D. O. (06 de Sepriembre de 2021). *DOF*. Recuperado el 19 de Agosto de 2024, de ACUERDO por el que se expide la Estrategia Digital Nacional 2021-2024. 06 de septiembre de 2021: https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0

UNIDAS, N. (18 de Julio de 2023). *CONSEJO DE SEGURIDAD*. Recuperado el 16 de Agosto de 2024, de Mantenimiento de la paz y la seguridad internacionalesInteligencia artificial:

oportunidades y riesgos para la paz y la seguridad internacionales: https://documents.un.org/doc/undoc/pro/n23/210/52/pdf/n2321052.pdf