

Declaración sobre el Uso Responsable de la Inteligencia Artificial en los Servicios de Seguridad

Junio 2025

Contexto

- La inteligencia artificial (IA) es una herramienta poderosa con el potencial de fortalecer la seguridad pública y empoderar a los servicios de seguridad. Sin embargo, también conlleva ciertos riesgos que la industria de la seguridad reconoce y está tomando medidas para abordar de manera responsable.
- Para las empresas responsables de proteger a las personas y los bienes, contar con regulaciones y definiciones claras es fundamental para que la IA pueda utilizarse plenamente en beneficio de la seguridad. Esto también permite que los proveedores de servicios de seguridad comprendan claramente sus obligaciones y puedan adaptar sus operaciones a marcos legales en constante evolución.
- Debido a la rápida transformación tecnológica, y a que distintos sistemas y casos de uso de IA implican niveles de riesgo diferentes, se justifica un enfoque flexible basado en el riesgo. Deben evitarse requisitos rígidos, prescriptivos y de tipo "talla única".

Oportunidades

La integración de la IA en los servicios de seguridad mejora la seguridad pública y aporta beneficios tanto a las empresas como a los trabajadores del sector. La IA transforma los conceptos tradicionales de seguridad al ofrecer herramientas innovadoras como sistemas de detección de comportamientos, identificación biométrica y drones habilitados con IA, mejorando los tiempos de respuesta y la toma de decisiones, y haciendo que las operaciones sean más seguras. Permite adaptar los servicios a las necesidades en tiempo real de los clientes, habilitando el análisis predictivo y la gestión de multitudes, lo que fortalece la resiliencia operativa. Mediante la automatización de tareas repetitivas, la IA libera al personal para concentrarse en tareas de mayor valor añadido, facilita decisiones basadas en datos y reduce la carga del trabajo rutinario. Además, la IA puede fomentar la inclusión, la diversidad y la creación de nuevas oportunidades laborales. También mejora la protección de datos y la ciberseguridad, promueve la eficiencia de costes y refuerza la competitividad empresarial, generando soluciones de seguridad más inteligentes y adaptativas.

Riesgos

Junto con las oportunidades, la industria de la seguridad reconoce que la implementación de IA también puede implicar riesgos. Estos pueden derivarse de una gestión inadecuada del riesgo, del uso de conjuntos de datos sesgados o poco fiables, de la falta de supervisión humana, de una resiliencia insuficiente frente a amenazas o de la ausencia de una gobernanza adecuada de la IA.

Entre los posibles daños se incluyen violaciones a la privacidad de las personas o vulnerabilidades en la seguridad, que pueden mitigarse mediante una adecuada gestión de riesgos.

Si bien muchos usos de la IA en los servicios de seguridad conllevan riesgos mínimos o nulos, algunas aplicaciones pueden implicar mayores riesgos y requerir niveles más altos de control y revisión.

- **Los casos de uso con riesgo mínimo** podrían incluir el análisis de datos no personales para evaluación de riesgos, eficiencia operativa o gestión de multitudes, permitiendo soluciones de seguridad más específicas, rentabilidad y mejoras ecológicas. Las aplicaciones de IA como la clasificación de alarmas y el análisis de objetos mejoran la eficiencia operativa y la toma de decisiones, mientras que la verificación biométrica mejora el control de acceso sin entrar en territorio de alto riesgo.
- **Los escenarios de riesgo elevado** pueden surgir cuando se incluyen datos personales, como en el uso de videovigilancia avanzada que los integra.
- **Los riesgos inaceptables** aparecen cuando un sistema o aplicación de IA vulnera derechos fundamentales, lo cual es rechazado por la industria de la seguridad. Ejemplos incluyen la creación de bases de datos de reconocimiento facial mediante métodos de recolección no autorizados (*scraping*), el uso de IA para generar puntuaciones sociales que conlleven tratos injustos, y la categorización biométrica basada en datos obtenidos de manera ilícita.

Comprender estas distinciones subraya que toda evaluación de un sistema de IA y su caso de uso es única, al igual que el potencial de la IA para mejorar los servicios de seguridad cuando se implementa de forma responsable dentro de marcos normativos flexibles.

Principios Éticos para el Uso Responsable de la IA en los Servicios de Seguridad

La *International Security Ligue* ofrece las siguientes consideraciones éticas a los proveedores de servicios de seguridad para el desarrollo e implementación de sistemas de IA:

- Identificar cada sistema de IA, su uso y propósito previsto, y verificar que aporte valor añadido garantizando una interacción complementaria y constructiva entre personas y tecnologías.
- Revisar las obligaciones legales y normas aplicables en cada caso de uso.
- Realizar una evaluación inicial de riesgos por caso de uso y gestionar los riesgos durante todo el ciclo de vida del sistema de IA.
- Mantener una supervisión humana adecuada sobre cualquier aplicación o sistema de IA, y capacitar al personal y al equipo directivo responsable de la IA cuando sea necesario.
- Realizar una debida diligencia al adquirir sistemas que utilicen IA, y limitar su uso a aquellos que se basen en datos y algoritmos confiables.
- Implementar medidas sólidas de protección física y cibernética para los sistemas de IA, asegurando la privacidad de los datos y la transparencia requerida para su uso.
- Establecer un equipo interno de gobernanza y liderazgo en IA; desarrollar códigos de conducta internos y planes de respuesta ante fallos o usos indebidos; y supervisar continuamente la gobernanza de IA y el entorno regulatorio.

Sobre la International Security Ligue. Fundada en 1934, la *International Security Ligue* ofrece una voz global a la profesión de la seguridad y trabaja activamente para elevar los estándares éticos y profesionales de la industria de la seguridad privada, así como para dar forma a códigos de conducta globales. A través de su grupo de trabajo *Tecnología y Sociedad*, la Ligue busca maximizar los beneficios de la tecnología para construir sociedades más seguras, promoviendo al mismo tiempo una implementación segura y responsable.

La *Declaración sobre el Uso Responsable de la IA en los Servicios de Seguridad* de la *International Security Ligue* fue elaborada por miembros del grupo de trabajo *Tecnología y Sociedad*, compuesto por representantes de empresas afiliadas a la Ligue. Con autorización, se inspira en la *Carta sobre el uso ético y responsable de la inteligencia artificial en los servicios de seguridad privada europeos* de CoESS. Esta declaración no necesariamente refleja las opiniones de todos los miembros; no constituye asesoramiento legal; y no debe considerarse como base de cumplimiento con ninguna normativa específica sobre el uso de la IA. Para una aplicación práctica de estos principios, los usuarios pueden consultar la *Lista de Verificación para la Aplicación de Principios de Uso Responsable de la IA en los Servicios de Seguridad* de la Ligue.